Cybersecurity and Business Vitality

What Every Houston-Area Business Leader Needs to Know

Third Edition
October 2015

GINA LUNA
Chair of the Board

BOB HARVEY
President and CEO

UMESH VERMA
Cybersecurity Task Force Chair

GREATER HOUSTON
PARTNERSHIP
Making Houston Greater.

Chair's Letter

As you are aware, the issue of cybersecurity has drawn considerable discussion and captured numerous national headlines. In 2014 it was reported that 60 percent of all targeted attacks were aimed at small-and medium-sized organizations. It is pertinent that businesses understand how cybersecurity specifically applies to their industry so that they are able to be as prepared as possible.

National issues often times have local implications; therefore, we at the Partnership aim to provide members and the business community with the tools to create the best business climate in the nation. In this era of a globally connected economy supported by an infrastructure of electronic information systems and data, it is imperative that Houston-area leaders know what they can do to protect their business.

Gina Luna
2015 Chair of the Board, Greater Houston Partnership
Chairman, Houston Region at JPMorgan Chase

President's Letter

The Partnership is actively convening Houston-area businesses to address key issues facing the region, including cybersecurity. This issue impacts the economic engines that drive our region including businesses, government, health care providers and non-profit organizations. In today's technology-dependent business environment, information security is essential to preserving business vitality.

While many larger corporations already have systems and procedures in place to help safeguard their companies from cybersecurity attacks, the Partnership identified a strategic need to provide Houston's small to mid-sized businesses with information to make their businesses more resilient.

This guide includes valuable, first-hand advice from leaders of the Houston business community whose companies have benefited from implementing key steps for cybersecurity preparedness.

Bob Harvey
President and CEO, Greater Houston Partnership

Cybersecurity Task Force Chair's Letter

The Greater Houston Partnership created its Cybersecurity Task Force in 2012, comprised of leading experts across multiple industries, to address the issue of cybersecurity and provide their industry-specific recommendations and advice gleaned from first-hand experience. The task force explores how cyber-threats impact Houston's business community, with a purposeful focus on the needs of small to mid-sized businesses, which employ approximately one-third of Houston's workforce.

The third edition of the Cybersecurity and Business Vitality guide takes a complex issue and breaks it down into a digestible format, outlining simple strategies that can be implemented to protect businesses and organizations from cyber attacks. It includes information from leaders in key business sectors including energy, health care, legal, banking/financial services, education, retail, insurance, human resources and the public sector. I want to thank them all for their dedication and commitment to this issue and this 3rd Edition.

The cybersecurity issue is indeed complex, but this guide illustrates the benefits the business community can gain by taking a few extra steps. We hope you will find this guide to be a valuable resource – one worth sharing inside and outside your organization.

Umesh Verma
Chair – Cybersecurity Task Force
CEO BLUE LANCE, Inc.

GREATER HOUSTON
PARTNERSHIP
Making Houston Greater.

CYBERSECURITY TASK FORCE

Cybersecurity Task Force Chair

Umesh Verma
CEO, BLUE LANCE, Inc., Chairman-Cybersecurity Task Force

Cybersecurity Project Lead

Jesse Carrillo
Senior Vice President, CIO Hines

Cybersecurity Task Force Working Group Leaders

Phil Beckett, Ph.D., Chief Technology Officer, Greater Houston Healthconnect

Mary E. Dickerson, Executive Director, IT Security, University of Houston

Nicholas Economidis, Beazley

Geoffrey Graham, Strategy & Planning – Critical infrastructure BAE Systems

Luis Hernandez, Manager, Retail IT, NRG Energy

Bart W. Huffman, Partner Locke Lord - Austin

David LaPlante, ISO - Houston, City of Houston

Mel Nevarez, IT Manager, Cyber Security, CenterPoint Energy

Jason Ritchie, Operations Officer Federal Reserve Bank - Houston Branch,

Andy Sawyer, Director of Security, Locke Lord

Milind Sethi, Account Manager, Procom Services

Peter Thomas, CISSP CTO, BLUE LANCE, Inc.

Andy Woods, Director, Commercial Cyber Security BAE Systems

Cybersecurity Task Force Members

Adnan Amjad, Partner, Deloitte

William Carter, Vice Chancellor, Information Technology Houston Community College

Ray Cline, Ph.D., Information and Logistics Department Chair, University of Houston

Holli Davies, Regional Director, Office of U.S. Rep. Michael McCaul

Myra Davis, Senior Vice President and CIO, Texas Children's Hospital

Rhonda Festervand, Senior Vice President & Operations Director, Allegiance Bank Texas

David Hansen, Chairman, MIT Enterprise Forum of Texas

Angela Haun, Special Agent & Coordinator, InfraGard Federal Bureau of Investigation (FBI)

Gary Hayes, Vice President, IT & CIO CenterPoint Energy

Clive Hess, President, CompuCycle Inc

Kamran Khan, M.D. , Owner VP Consulting Services

Connie Miller, The Boeing Company

Kim Morris, Director, Bay Tech

Mike Phillips, CenterPoint Energy

Ken Redding, Vice President, Texas Retail IT NRG Energy

Jeff Reichman, Principal, January Advisors

Sah Sanjeev, Director, IS Risk & Controls (CISO) Texas Children's Hospital

S. Srinivasan, Ph.D., Distinguished Professor of Business Administration, Texas Southern University, Jesse H. Jones School of Business

Chuck Thomas, GIS Data Analyst, Center for Houston's Future

Charles T. Thompson, CIO, City of Houston - HITS

Massey Villarreal, President & CEO, Precision Task Group Inc.

Jeff Vinson, Chief Information Security Officer, Harris Health System

Mark D. Walker, DIrector, Alternative Channels, NRG Energy Inc.

John Wilburn, Director, Strategic Initiatives, Center for Houston's Future

Andrew Yang, Ph.D., Executive Director, Cyber Security Institute, University of Houston

Partnership Staff

Lilyanne McClean, Executive Vice President, Public Policy and Communications

Taylor Landin, Vice President, Public Policy

Joey Sanchez, Analyst, Public Policy

Regina Recinos Jr., Analyst, Public Policy

Myrna Cantu, Executive Assistant, Public Policy and Communications

Clint Pasche, Vice President, Communications

Damjana Alverson, Communications Manager

Marc Keosayian, Graphic Designer

Suzanne Morgan, Senior Graphic Designer

TABLE OF CONTENTS

INTRODUCTION

SONY Pictures, Home Depot, Target, JPMorgan Chase, Staples, U.S. Department of Homeland Security... These are just a few of the names recently associated with cyber-attacks and breaches.

Cybersecurity is a critical and growing concern for American businesses, government and families. From October 2011 through February 2012, more than 50,000 cyber-attacks on private and government networks were reported to the U.S. Department of Homeland Security, including 86 attacks against 'critical infrastructure networks.' These attacks likely represent a small fraction of cyber-attacks directed at the United States.

The Greater Houston Partnership created its Cybersecurity Task Force in 2012 to explore how cyber-threats impact Houston's business community, with a purposeful focus on the needs of small to mid-sized businesses. Small businesses employ approximately one-third of Houston's workforce, employing more people in the city's metro (682,501) than the total population of Boston. This group paid more than $29 billion in salaries in 2010, contributing greatly to the regional economy.[1]

The Task Force is comprised of leading experts across multiple industries, including consulting, education, energy, finance, real estate, health care, information technology, legal, retail, insurance, human resources and the public sector.

All members agreed that **the most important component of cybersecurity is awareness** – knowing that threats exist and that businesses need to secure their data and equipment.

Understanding the budgetary limitations for small and mid-sized businesses, the Task Force compiled concrete, specific steps for business owners to take in order to protect against the ever-changing cybersecurity threats. Those steps include:

- Zero-cost preventative solutions, based on Protection, Awareness and Responsiveness (P.A.R.)
- National standards created by a coalition of government and business leaders
- Guidelines for creating a cyber-attack containment plan
- A model crisis communication plan
- Industry-specific information for the largest sectors in Houston
- A self-review check-list for each business owner to review its current status
- A glossary of key terms

Finally, this guide includes valuable, first-hand advice from leaders of the Houston business community whose companies have benefited from implementing key steps for cybersecurity preparedness.

A free digital version of the cybersecurity report is available online at Houston.org/cybersecurity.

[1] U.S. Census Bureau, Statistics of U.S. Businesses, 2010. Small business/firm is defined as 1-99 employees

THINGS TO CONSIDER

In this era of a globally connected economy supported by an infrastructure of electronic information systems and data, cybersecurity has vaulted to the highest echelon of security concerns. Compromises in information systems may have tremendous impacts on virtually every aspect of life, economic markets and national sovereignty, impacting everything from personal health, safety, and finances, to national security, physical infrastructure and trade – and everything in between. Private industry and governments are legitimately concerned.

Cybersecurity risks are growing, with targets beyond government and major enterprise operations. Former Director of the National Security Agency and Commander of U.S. Cyber Command, General Keith Alexander, warned in 2012 that U.S. companies "lose about $250 billion per year through intellectual property theft, with another $114 billion lost due to cyber-crime, a number that rises to $338 billion when the costs of down time due to crime are taken into account."[2] And even the Department of Homeland Security was not immune to an attack through a partner company, US Investigations Services (USIS), which resulted in the theft of personal information about DHS employees. An April 2015 report demonstrated that in 2014 there was a 30 percent increase in targeted attacks, a 113 percent increase in ransomware attacks and a 70 percent increase in the number of phishing sites spoofing social networking sites. This report also found that **60 percent of all targeted attacks were aimed at small and medium-sized organizations** and 36 percent of all mobile threats steal information.[3]

One critical aspect of cybersecurity is protecting data any business gathers. Large businesses are able to withstand the financial loss due to a breach where as small and medium sized businesses are greatly affected and often they go out of business. As seen in the chart, we highlight the cost aspects of a data breach primarily for large businesses. However, the remedial measures needed are applicable to businesses of all types and so the per record cost given below would be applicable to small and medium sized businesses as well.

Ponemon Institute has been studying the cost of a data breach for several years. These results are borne out by other studies such as the Net Intelligence. The table summarizes per record cost of a breach.

Year	Average per record cost	Average total cost
2012	$188	$5.4 million
2013	$201	$5.9 million
2014	$217	$6.5 million

The increase in cost is attributed to steps taken for retaining customers. The customer churn rate has increased by 15 percent due to wide publicity. Heavily regulated industries such as health care, financial, energy and education tend to have higher cost due to data breach.

Cybersecurity's specific challenges continue to evolve with the evolution of technology. Cloud computing, mobile computing, applications-based computing, e-payment systems and increasing interconnection of devices, which the Federal Trade Commission (FTC) has called "the internet of things,"[4] each brings its own security issues. Traditional challenges such as third-party/supplier handling of information and insider threats are magnified as a boundless supply of data becomes more integral to a wider array of business functions.

It is imperative that business people know what they can do to protect their business. **The answer is reasonable diligence, not perfection**. Responsible information security measures that are regularly reviewed and updated will go a long way towards avoiding most attacks. However, in the event that cyber-attack succeeds in breaching these security measures, a containment plan is necessary to mitigate any damage that might result. Along with the containing the attack, a crisis communication plan for internal and external stakeholders will be necessary. Cyber insurance policies might help close the gap and coverage is likely to be more affordable to a business that is investing a reasonable, appropriate amount of time, attention and resources on this "new" fundamental aspect of business security.

We hope that this guide will provide useful points for you to consider.

[2] Rogin, Josh. "NSA Chief: Cybercrime constitutes the 'greatest transfer of wealth in history,'" Foreign Policy, 9 July 2012. http://thecable. foreignpolicy.com/posts/2012/07/09/nsa_chief_cybercrime_constitutes_the_greatest_transfer_of_wealth_in_history

[3] "Internet Security Threat Report 2015," Symantec Corporation, Volume 20, April 2015. https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf (emphasis added)

[4] Demboskly, April. "FTC targets 'internet of things' amid privacy fears," Financial Times, 4 September 2013. http://www.ft.com/intl/ cms/s/0/1eb3b2ca-15ac-11e3-b519-00144feabdc0.html#axzz2iOS28EW7

STATE OF CYBERSECURITY

NIST Framework

The National Institute of Standards and Technology (NIST), under the Department of Commerce, released its NIST Cybersecurity Framework discussing voluntary actions that can be taken to improve cybersecurity as directed by the Executive Order.[5] Under the NIST Framework, cybersecurity events are defined as "a cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation)."

The framework establishes five core functions, which are proscriptive, proactive or reactive in nature:

Identify: An understanding of which organizational systems, assets, data and capabilities need to be protected, determine priority in light of the organizational mission and establish processes to achieve risk management goals.

Protect: Appropriate safeguards, prioritized through the organization's risk management process, to insure the delivery of critical infrastructure services.

Detect: Appropriate activities to identify the occurrence of a cybersecurity event.

Respond: Appropriate activities, prioritized through the organization's risk management process (including effective planning), to take action regarding a detected cybersecurity event.

Recover: Appropriate activities, prioritized through the organization's risk management process, to restore the appropriate capabilities that were impaired by a cybersecurity event.

Excerpt from statement made by Homeland Security Secretary Johnson regarding Sony Cyber Attack and need for NIST framework:

".. This event underscores the importance of good cybersecurity practices to rapidly detect cyber intrusions and promote resilience throughout all of our networks. Every CEO should take this opportunity to assess their company's cybersecurity. Every business in this country should seek to employ best practices in cybersecurity. For businesses and other organizations that want to improve their cybersecurity, the (NIST) Cybersecurity Framework is a great starting point and a great tool. It lays out best practices developed together by government and the private sector."

NIST Framework: Practical Applications for Businesses

Created through a collaboration between industry and government, NIST's Cybersecurity Framework consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the Framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk.[6]

Businesses looking through the lens of the NIST framework should:

Identify information assets (data) and risks associated with these assets, including a business' own data, data of clients and other third parties. Custodial responsibilities may differ from ownership responsibilities and subject the business to specific responsibilities and obligations. Classify assets by sensitivity, criticality, value, shelf life, ownership, and custodial responsibilities. Assess risks to each asset in terms of likelihood, business impact, and loss expectancy. Steps to manage identified risks include:

- Avoid the risk by removing the asset or ceasing the behavior creating the risk.

[5] "Preliminary cybersecurity Framework," National Institute of Standards and Technology, 22 October 2013. http://www.nist.gov/itl/upload/ preliminary-cybersecurity-framework.pdf

[6] http://www.nist.gov/cyberframework/

- Mitigate the risk by implementing policies, procedures, and controls to reduce or remove the risk.
- Transfer the risk to an insurer or third party service provider.
- Accept the impact of the risk and communicate this policy to the data owner.

Protect the identified assets through implementing policies, standards, guidelines and controls to:

- Authenticate, authorize, and audit asset access.
  - » All access should be recorded or logged.
  - » Only those with a need to know or need to do are identified and given only necessary permissions
- Promote information security awareness within the business.
- Insure the confidentiality, integrity, and availability of data at rest and in motion.
- Protect data from unauthorized disclosure.
- Safely destroy obsolete data in all forms, electronic and physical, based on data and document retention requirements
- Implement incident recovery and business continuity plans to protect its interests and those of its clients.

Detect threats in real-time through implementing policies, processes, procedures, and controls to:

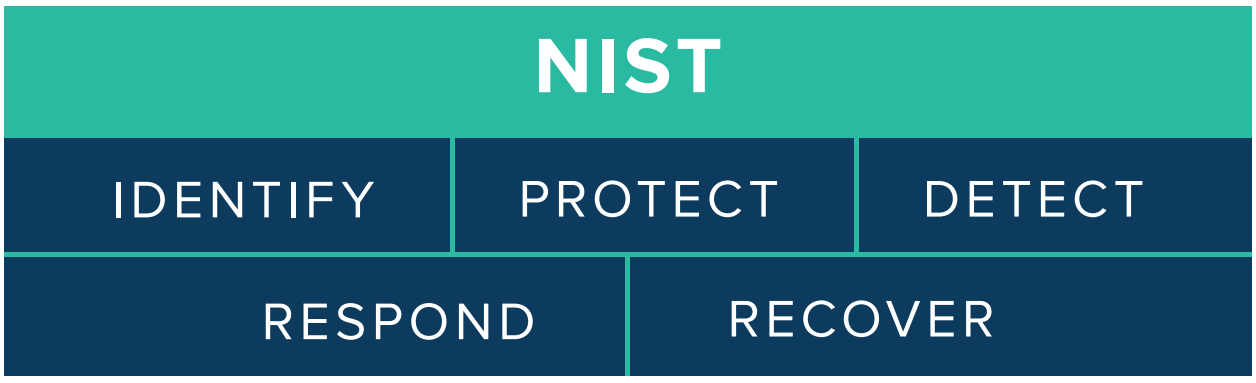
- Recognize malicious activity in a timely manner.
- Maintain continuous internal and independent vulnerability and penetration assessments to evaluate, maintain, and continually improve detective posture.

Respond to incidents effectively through implementing, testing, and maintaining a pro-active response plan that includes:

- Defined response team roles and responsibilities.
- A predefined notification list of:
  - » internal/external stakeholders,
  - » law enforcement/first responders,
  - » service providers,
  - » public relations/media.
- Contingency for communicating directly with clients and other external entities, if an obligation exists for a breach of data the firm has custody of but does not own.
- Isolate an incident, prevent expansion, and mitigate effects.
- Perform incident post-mortems to review and improve processes.

Recover: from incident and return to normal operations, including:

- Predefining recovery time objectives, the maximum tolerable time data, services, and operations can be unavailable. These objectives prioritize recovery operations.
- Predefining recovery point objectives, the maximum acceptable data loss as the result of an incident.
- Recovery time and point objectives determine if the business's key systems (e-mail, internet, document management) will be recovered at existing data centers, service providers, or failover/alternate sites.
- Ongoing recovery activity communications with internal/external stakeholders, data owners, service providers.



C³ Voluntary Program

In conjunction with the release of the NIST Framework, the U.S. Department of Homeland Security launched its Critical Infrastructure Cyber Community Voluntary Program (C3 Voluntary Program) to support the implementation of the Framework. The C3 Voluntary Program is working to promote the usage of the Framework, support the development of sector-specific Framework guidance, support organizations attempting to learn how to use the Framework and solicit feedback about the Framework.

In February 2014, NIST also released its "Roadmap for Improving Critical Infrastructure Cybersecurity." The Roadmap provides guidance on "NIST's next steps with the Framework" and identifies a number of "Areas for Improvement," including authentication, the cybersecurity workforce and data analytics.[7]

InfraGuard

InfraGard is a non-profit organization designed to promote collaboration between private industry and the Federal Bureau of Investigation.[8] The organization facilitates information sharing between businesses, academic institutions and state and local law enforcement agencies as well as other participants in regards to cybersecurity. There are branches of InfraGard across the country, including in Houston.[9] InfraGard provides industry and organization-specific threat reports and alerts as they are processed to their private partners. Other organizations provide more in-depth collaboration, such as the Cyber Technology and Information Security Laboratory (CTISL) at the Georgia Tech Research Institute (GTRI).[10]

Regulatory Activity

Various federal regulations reflect the importance of cybersecurity. For example,

- Federal Trade Commission (FTC) takes the position that its authority over "unfair" trade practices extends to the failure to adopt and maintain reasonable information security practices.11
- U.S. Health and Human Services (HHS) regulations pursuant to the Health Insurance Portability and Accountability Act of 1996 include stringent security requirements with respect to protected health information.12 The Gramm-Leach-Bliley Act's Safeguards Rule requires appropriate information security with respect to non-public information maintained by financial institutions and their suppliers.13
- U.S. Securities and Exchange Commission (SEC) issued guidance suggesting that public companies should disclose significant cyberthreats in regulatory filings.14

[7] "Roadmap for Improving Critical Infrastructure cybersecurity," National Institute of Standards and Technology, 12 February 2014. http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf

[8] "InfraGard," https://www.infragard.org/

[9] "InfraGard Members Alliance- Houston," http://www.infragardhouston.org/

[10] "Cyber Technology and Information Security Laboratory (CTISL)," Georgia Research Tech Institute. http://www.gtri.gatech.edu/ctisl

[11] "FTC Files Complaint Against LabMD for Failing to Protect Consumers' Privacy," Federal Trade Commission, 29 August 2013. ftc.gov/ opa/2013/08/labmd.shtm

[12] "Health Insurance Reform: Security Standards," Department of Health and Human Services, Federal Register, Vol. 68, No. 34, 20 February 2003. www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf

[13] "Standards for Safeguarding Customer Information," Federal Trade Commission, Federal Register, Vol. 67, No. 100, 23 May 2002. www.ftc. gov/os/2002/05/67fr36585.pdf

[14] "CF Disclosure Guidance: Topic No. 2: cybersecurity," U.S. Securities and Exchange Commission, 13 October 2011. www.sec.gov/divisions/ corpfin/guidance/cfguidance-topic2.htm

FEDERAL GOVERNMENT ACTIVITY

While Congress continues to work on cybersecurity legislation, the challenges of the undertaking – including fundamental privacy rights and concerns – have yet to be addressed. It appears that some form of federal cybersecurity legislation will be passed eventually. Future legislation could offer liability protections contingent on efforts to adhere to best practices, exempting companies from legal prosecution following a security breach and seek to promote information sharing and collaboration to advance defense against future attacks. However, privacy and civil liberty concerns exist regarding the sharing of information. Recognizing these concerns, President Barack Obama issued an Executive Order - 13636 on cybersecurity, directing the Department of Homeland Security to consult with the federal Privacy and Civil Liberties Oversight Board, in the hopes of developing a satisfactory medium.

Executive Order – 13636

Recognizing the importance of cybersecurity, President Obama issued an Executive Order for "Improving Critical Infrastructure cybersecurity," and announced it in his State of the Union Address on February 12, 2013.[15] The Executive Order directs federal agencies to take specific actions to improve cybersecurity communication and cooperation between the government and the private sector and develop and implement a voluntary national cybersecurity framework to strengthen infrastructure against cybersecurity threats.

As a result, the Departments of Homeland Security and Commerce worked with other federal agencies to develop potential incentives for private industry cooperation.[16] These incentives include (i) advantages in federal grants; (ii) preferential treatment in governmental processes and governmental service delivery; (iii) streamlined regulations; (iv) cost recovery through rate increases by utilities; (v) government research and development support; (vi) public recognition; (vii) fostering a competitive and informed cyber insurance market; and (viii) government agency support for liability-limiting legislation.

[15] "Executive Order – Improving Critical Infrastructure cybersecurity," The White House, 12 February 2013. http://www.whitehouse.gov/ the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[16] Daniel, Michael. "Incentives to Support the Adoption of the cybersecurity Framework," Department of Homeland Security, 6 August 2013. http://www.dhs.gov/blog/2013/08/06/

STATE GOVERNMENT ACTIVITY

In conjunction with the federal government, 47 states, including Texas, have enacted some form of cybersecurity legislation. Texas is keenly interested in the security of cyber-assets and systems, while viewing cybersecurity as providing important opportunities for statewide economic development.

Texas

In 2011, the 82nd Texas Legislature passed legislation authorizing the Texas Cybersecurity, Education and Economic Development Council (TCEEDC).[17] Consisting of members from government, academia and industry, the TCEEDC advised the legislature on Texas' cybersecurity infrastructure, government-business-academia partnerships, and the cybersecurity industry's development in Texas. Along with infrastructure and industry, the TCEEDC identified education, innovation and "cyber culture" to be extremely important to the state.

In 2012, the TCEEDC published "Building a More Secure and Prosperous Texas," which highlighted the themes of awareness, collaboration, training and education as critical components to accelerate the growth of cybersecurity as an industry within the State. The report recommended, among other things, the establishment of a Texas statewide Cybersecurity Coordinator, which was subsequently adopted in the 83rd legislative session.[18] The report's overall assessment highlights that cyber-attacks impact not just traditional computing systems, but also the growing universe of computer-connected devices.

Texas Cybersecurity Roadmap

In the years following the TCEEDC report and the appointment of the Texas Cybersecurity Coordinator, Texas has made good progress as a national cybersecurity leader through implementation of recommendations from the report. Critical to these efforts, the Texas Cybersecurity Coordinator has spearheaded several key initiatives.

Education and Workforce Initiatives

Bringing visibility to the State's established areas of excellence and forging collaborations between similar-focused organizations has been an initial objective. In addition to strengthening components of a state-specific cybersecurity education pipeline, Texas has partnered with several national organizations to promote learning programs directed toward middle and high-school students and teachers, as well as military veterans. These efforts, coupled with higher education programs such as the DHS/NSA Centers of Academic Excellence in Information Assurance are working to meet workforce challenges in innovative ways. They are also providing avenues for businesses of all sizes and industries throughout the State to become partners in solving these challenges through mentorship and sponsorship opportunities.

Policy Changes

Consistent with various initiatives on the Federal level, Texas has worked to align regulations, policies and recommendations toward NIST security controls, incident management and risk assessment. Using the NIST Framework, released in February 2014, as a foundation, the newly revised Texas Administrative Code (TAC) 202, defines how State agencies and higher education institutions deal with information security. Speaking the same language and following the same set of rules is making it easier for integrating control sets and encouraging security collaborations across industries and jurisdictions.

[17] "Texas cybersecurity Council," Department of Information Resources. www2.dir.state.tx.us/sponsored/SB988/Pages/overview.aspx

[18] Tex. S.B. 1102, 83d Leg., R.S. (2013) (amending Chapter 2504 of the Texas Government Code). www.capitol.state.tx.us/tlodocs/83R/billtext/ pdf/SB01102F.pdf#navpanes=0

CITY GOVERNMENT ACTIVITY

"Greater Houston" is a nine-county metropolitan area as defined by the Office of Management and Budget (OMB) with a population of over 6 million citizens.[19] **Since 2003, "Greater Houston" has been considered by the Department of Homeland Security (DHS) to be among the highest threat urban areas in the nation.** This designation qualifies the area to receive funding through the DHS Urban Area Security Initiative (UASI) grant program, established to enhance the preparedness level of high threat communities.[20]

Houston is one of the fastest growing metropolitan areas in the United States, but that growth also brings increased costs.

In a recent Houston Chronicle interview with Harris County Judge Ed Emmett stated, "If we are going to continue to accommodate growth - and I think that's a good thing - we are going to have to invest in the infrastructure to take care of it." With the "vast majority" of Harris County's growth occurring in unincorporated areas, a change in perception is needed. "[W]e have to make the Legislature understand that Harris is an urban environment and the county is not geared to urban issues," Judge Emmett said. "It is important that Harris County and Houston and other jurisdictions find ways to cooperate and do things together," the county judge said. "We need to look at things as a region, rather than at arbitrary county lines."

While Judge Emmett focused his comments on transportation, the same cooperation and collaboration is needed within the region's governmental entities to facilitate securing the systems and services the area's citizens rely on.

With support from the UASI and related homeland security grant programs, stakeholders in the Greater Houston area are engaged in a multi-disciplinary and multi-jurisdictional partnership to improve local capacity to prepare for, protect against, respond to and recover from natural or man-made catastrophic incidents.

Business Characteristics

The government sector cyber environment is probably one of the most complex. The business types and citizen services provided within the sector include: Public Safely (Police, Fire, 911, 311, Courts), Public Works (Utilities, Solid Waste), Transportation (Airports), Housing, Health Services and Emergency Management.

Legislative and Regulatory Requirements

As noted above, the numerous service types provided by the sector require compliance with Federal, State and local cybersecurity standards and regulations. Developing and implementing a solid Cybersecurity Framework can reduce the complexity and effort needed to comply with the various requirements.

[19] U.S. Census Bureau (April 5, 2012). http://www.census.gov/newsroom/releases/archives/population/cb12-55.html

[20] Houston Urban Area Security Initiative (UASI). http://www.houstonuasi.com/go/site/1532/

Information and Intelligence Sharing

While the availability of hardware and software tools to assist in detection capabilities are becoming more pervasive, it is unlikely that a single organization has the ability to detect more sophisticated attacks on their own. An essential element to assist in rapid detection is with information and intelligence sharing.

Some detection hardware and software vendors pool the detection information from their tools to provide an almost global repository of detection data from private and public sector cyber environments, giving their customers the expanded detection capabilities that result from the sharing of information.

Organizations must be willing to share security information for this capability to be effective. Gone are the days of secrets when it comes to security information. Requirements for reporting security incidents in many private and public sectors have been created through Legislative and regulatory action in an effort not only to provide for an informed public, but to promote the sharing of threat information.

Budget

As with any organization, the available budget for Information Technology in general and cybersecurity specifically is always a big consideration in deciding on strategies to secure your cyber environment. Since most, if not all funding for government sector operations comes from the public, the budget is generally more restrictive. With shrinking municipal budgets, municipal governments must be creative and use tools already in-house or find low-price or no-price alternatives.

There are open-source security tools for nearly every security task from protection to detection including: antivirus, firewall, log-management, network monitoring, vulnerability scanning, intrusion detection, and event management.

Some open-source tools require more labor to deploy and manage and may not provide the level of customer support needed by the organization, but could be used as a stop-gap while awaiting funding on a commercial tool that provides additional customer support, or may be sufficient to meet the organizations long-term needs.

Public Records Act

One of the challenges the Government Sector faces in respect to the cybersecurity program is the requirement to comply with Public/Open Records Requests. Many people have the expectation that any electronic documents produced within a public sector entity should be made available upon request, regardless of whether sensitive cybersecurity information is incorporated.

While the expectation of public information being available to all for the asking is part of a democratic system, there needs to be a better understanding that for cybersecurity reasons, some information should not be publicly shared. It is acceptable to most people that information such as personal information, confidential information, trade secrets and the like should not be shared, but sensitive information in respect to security processes and procedures and hardware and software to protect the government assets do not have the same consideration.

The Texas Public Information Handbook clarifies both the open records requirements as well as the acceptable exceptions to the requirements.

Section 552.139. Exception: Confidentiality of Government Information Related to Security or Infrastructure Issues for Computers

a. Information is excepted from the requirements of Section 552.021 if it is information that relates to computer network security, to restricted information under Section 2059.055, or to the design, operation, or defense of a computer network.

b. The following information is confidential:

    1. a computer network vulnerability report;

    2. any other assessment of the extent to which data processing operations, a computer, a computer program, network, system, or system interface, or software of a governmental body or of a contractor of a governmental body is vulnerable to unauthorized access or harm, including an assessment of the extent to which the governmental body's or contractor's electronically stored information containing sensitive or critical information is vulnerable to alteration, damage, erasure, or inappropriate use; and

    3. a photocopy or other copy of an identification badge issued to an official or employee of a governmental body.

c. Not withstanding the confidential nature of the information described in this section, the information may be disclosed to a bidder if the governmental body determines that providing the information is necessary for the bidder to provide an accurate bid. A disclosure under this subsection is not a voluntary disclosure for purposes of Section 552.007.[21]

It is important that Government Sector organizations implement data and documentation classification policy and procedure to insure that cybersecurity architecture, systems, tools, documentation, and data are protected by being exempted from public/open records requests.

The public publication or dissemination of Disaster Recovery/Continuity of Operations Plans, Security Policies and Procedures, Security and Network Architectures and Designs, Vulnerability and Threat information places the Government cyber environment and ultimately, the citizen at risk. Understandably, these documents should be identified as falling under the Section 552.139 Exemption and kept separate from information that falls under the Public Records Act.

[21] 2014 Public Information Handbook • Office of the Attorney General, https://www.texasattorneygeneral.gov/ag_publications/pdfs/publicinfo_hb.pdf

TASK FORCE RECOMMENDATIONS

Don't be Surprised: We Can All be on P.A.R.

After months of work comparing and evaluating industry standards and best practices, the members of the Cybersecurity Task Force drew several conclusions:

1. While cybersecurity is a complex issue, there are, in fact, many simple steps businesses can take to protect themselves from cyber-crime;
2. Many steps don't require a large financial commitment. Rather, what's needed most is a time commitment to understand the issues, take preliminary steps to continue to treat cybersecurity as a priority for the business; and
3. By aggressively working to aid Houston's business community, the Task Force could help protect the region's economic growth and prosperity.

The Task Force also identified a big challenge: how to reduce the complexities of cybersecurity preparedness into a framework that is immediately relevant to business people, easy to remember and to implement.

After extensive work, the Task Force agreed that virtually every business in our region can dramatically reduce the chance of experiencing a cyber-attack if it commits to "being on P.A.R.:"

- Adopting PROTECTIVE measures,
- Staying AWARE of changes to business operations that could indicate criminal cyber-activity, including industry trends, and
- Being immediately RESPONSIVE if criminal cyber-activity is detected.

In the next section, the Task Force outlines key aspects of the P.A.R. framework and provides implementation recommendations that have minimal cost (between $0 - $5,000).

PROTECTION: PREVENTING CYBER-ATTACKS

Security incidents are unavoidable. Preparations must be in place to quickly identify and respond to an incident. Whether it is a lost laptop or a malicious insider, organizations must be ready to respond. Having a plan available ahead of time is paramount to successfully managing the situation. To respond to an incident the organization must first be alerted to it. Alerting can come from any number of sources - from automated systems to reports from employees.

The good news is that protecting your business from cyber-attacks is easier than one might think. Although it does take time, there are things that business leaders can do with relative ease, such as determining roles and responsibilities for protecting the company's assets.

Small to medium-sized firms are unlikely to have security-specific positions. To bridge that gap, the Partnership Cybersecurity Task Force has identified 18 steps that help protect small and mid-sized business owners can take in order to thwart the majority of cyber-attack e-mails.

Protecting Your Business: General Guidelines

Protecting any business should follow a logical, deliberate method. Begin with an honest assessment of the organization's current security posture. This assessment should include an inventory of all critical systems, services and processes, as well as business priorities. This assessment will result in the institution's current security profile.

Once a baseline security profile is created, the next step is to assess the risks that businesses face to understand the specific threats and potential impact of those threats. With this information the organization can determine which risks can be reasonably mitigated and how long it will take. The outcomes of the risk mitigation strategy can be called the target security profile, or the desired profile. Then, a business can create a deliberate implementation plan comprised of actions required to move from the current security profile to the target security profile. This implementation plan can include the following steps:

1. Provide security awareness training

All employees should understand your organizational policies around security: why you have them, how you enforce them and the penalties for violations. Training should also include any federal and state regulations and industry specific requirements.

2. Encrypted data at rest and in motion

All sensitive data should be encrypted for transmission. This entails:

- Using secure socket layers (https or the padlock symbol on a web browser) or transport layer security with a password protected digital certificate either installed on both the sending and receiving side or over a virtual private network set up between two organizations.
- Encrypting data at rest by using built in tools to encrypt the entire hard dive (e.g. Bitlocker on Windows and FileVault on Mac).
- Password protect databases, and physically secure them behind a firewall, thus protecting them from the Internet while ensuring limited access based on business need.

3. Use firewalls

Firewalls block inbound internet traffic and protect your internal network from external access. Use a firewall to block all inbound ports and services except for the ones your hardened services need for inbound access.

4. Intrusion prevention services

Intrusion prevention services (internal/ external) automatically detect external threats to your network and provide notification before they damage your business.

5. Web security-restriction/monitoring/reporting

Filter and restrict websites, services and content that can be accessed from your business. Use this to block your employees from accessing inappropriate content and sites that are known to present a security risk to your business.

6. Data loss prevention

Monitor and block the sending of unencrypted confidential information by e-mail or file upload. Data loss prevention software reviews your outbound content for words and patterns that should be sent securely and automatically sends them encrypted.

7. Lock down desktops

Only certain individuals in your organization should be able to download and install software. Computers should be kept patched and virus scanning software should always be current.

8. Use strong passwords and force changes every 60-90 days

Set the required standard to at least a minimum of eight characters including at least one upper case letter, lower case letter, numeric and special characters. Also, advise employees to never write down or share passwords.

9. Classify data

Perform an assessment and determine what data is public, private and protected. Insure that your policies and systems treat data types appropriately, using the highest protection for the most sensitive data.

10. Data separation based on content

Use two internet services or a virtual local area network and isolate the systems that you use for secure data from those that access other internet services, such as e-mail and web browsing. This helps protect your data by reducing its exposure to internet threats that are initiated internally, whether by accident or on purpose.

11. Restrict access

Limit access to need to know/need to do. Limit user roles to only access data and systems that are essential for performing their duties. Also be sure to change their access when their responsibilities change, especially in the case where they no longer need access to specific data.

12. Whitelist applications if possible

This is an approach to only allow software that is verified (malware free) to run on your computers. This is a good strategy to include with your lockdown strategy, which only allows certain individuals in your organization to download and install software.

13. Wireless networks

- Change your default SSID (Name of the wireless network). The default name tells someone the brand of router (and any associated vulnerabilities).
- Do not broadcast your SSID if possible. This is an option on the wireless router. It requires someone trying to connect to your wireless network to know the name, as well as the password.
- Change your admin password immediately. The admin passwords for routers are available on the internet, making it very easy for someone to connect directly to your wireless network.
- Create a “public” and “private” Wi-Fi network. You may want to offer wireless access to your customers or clients. Do this through a separate guest wireless router that is on a different virtual network that only has access to the internet and does not have access to your internal network. The same SSID and password requirements apply to this guest wireless network.
- Encryption should be turned on.

14. Mobile device management

Require your employees to use a pin to lock their mobile device, have device tracking, have encryption turned on and set data boundaries.

15. Network Monitoring Tools

A technical defense used while an attack is in progress. These tools are for performance and security.

16. Vulnerability assessment

You should perform an internal assessment of your security risks and make sound business decisions based on risks, vulnerabilities and costs. Network routers and firewalls generate large amounts of log data that can provide the basic reports necessary for assessing vulnerability, including the number of connected devices, how much traffic those devices are generating, the amount of traffic traversing the border and what applications are sending the data as well. This data can be correlated and patterns can be established, showing what is normal for different times during the day. By creating this baseline, businesses can flag and investigate anomalies to mitigate cyber-attacks.

17. Security policy

Communicate the security policy to all personnel. Have detailed security policies that are reviewed and approved by your Board. Educate all employees on these policies (based on their role and access to data classification type). Review policy understanding at intervals and document training and reviews. Monitor adherence to policies and correct any violations appropriately.

18. Avoid free/public cloud storage and email accounts

Free cloud storage or email often has terms of service limitations and/or no service level agreements (SLAs).

AWARENESS: UNDERSTANDING THE THREAT

The Partnership Task Force members agreed that awareness is key to cyber safety. Business leaders and Boards of Directors need both the awareness that cybersecurity is necessary as well as a minimum understanding of the issue as it relates to their specific business, so they can evaluate the company's current vulnerabilities. This knowledge includes:

Why a company or organization might be a target.

- Sector-specific information, or the primary sources of cyber information key to a business' sector

What information the business has that is valuable.

- Understanding of "Bad Actors"
- Effective containment procedures

Cybersecurity Governance Recommendations and Guidance for Leadership

One of the primary challenges businesses experience in ensuring cybersecurity is understanding the company's current exposure to cyber-threats and its effectiveness in managing the risk. Due to the technical and specific nature of this threat, it is difficult for a business's leadership to learn enough about the issue in a short amount of time to provide effective governance over the cyber-threat. The required knowledge to assess the potential risk exposure and effectiveness of any potential plan includes specific language, metrics, and technology. A basic awareness of key elements in effective cyber-defense can help leaders understand their company's maturity in managing cyber-threat risk, and point to next steps that can help move the company toward a more proactive, preemptive and mature approach.

An educated, trained and practiced cyber-aware culture is the first step to mitigating the risk. In the same way that businesses communicate with their employees regarding safety and ethical behavior, it must also create a parallel communication avenue regarding cybersecurity – to establish a preventative cybersecurity culture.

Effective cyber-risk management needs leadership that guides or challenges all its management on the adequacy of cyber-risk management practices, particularly around risk appetite and cybersecurity strategy. Within this paradigm, the Board of Directors plays an important role. (see next page):

IS YOUR BOARD OF DIRECTORS ADDRESSING CYBERSECURITY?

	YES	NO
Is the Board cyber-aware or does the Board understand the opportunities and risks?	○	○
Does the risk committee of the Board provide adequate oversight over cybersecurity?	○	○
Does management have a senior executive overseeing cyber risks?	○	○
Has the Board reviewed and signed off on the risk appetite for cyber?	○	○
Has the Board reviewed and signed off on the cybersecurity strategy?	○	○
Has the Board reviewed the crisis management strategy?	○	○
Has the Board conducted an independent assessment?	○	○

Are Your Employees Aware and Capable of Handling Cyber Threats?

–Education is Key

"... even the most secure system, if operated by ill-informed, untrained, careless or indifferent personnel, will not achieve a significant degree of security."

– Information Systems Audit and Control Association (ISACA) Information Security Governance Guidance for Information Security Managers[22]

"Twenty years of experience in security and privacy risk management tells us that training is the single most effective tool to reduce risks."

– ePrivacy Group[23]

"I don't care how many millions of dollars you spend on hardware. If you don't have the people trained properly I'm going to get in if I want to get in."

– Susan Thunder, Former member of Cyberpunks Hacker Group[24]

Establishing a program supporting education and ongoing communication is critical to success. Available resources include the following from the Department of Homeland Security:

Training Programs for Infrastructure Partners
The Department's Office of Infrastructure Protection (IP) offers a wide array of training programs and resources, free of charge, to government and private sector partners. These web-based classroom courses and training materials provide government officials, infrastructure owners and operators the knowledge and skills needed to implement critical infrastructure protection and resilience activities.[25]

[22] "Information Security Governance: Guidance for Boards of Directors and Executive Management (2nd ed.)," IT Governance Institute, 2006. http://www.isaca.org/Knowledge-Center/Research/Documents/InfoSecGuidanceDirectorsExecMgt.pdf

[23] Cobb, Stephen and Schiavone, Vincent. "Practical Privacy: Responding to the Rising Cost of Privacy Incidents," ePrivacy Group, 2002. http://www.ehcca.com/presentations/compcongress6/schiavoneH.doc

[24] 0 Galley, Patrick. "Computer Terrorism: What are the risks," The Information Warfare Site, 30 May 1996. http://www.iwar.org.uk/cyberterror/resources/risks/index.html

[25] "Training Programs for Infrastructure Partners," Department of Homeland Security. http://www.dhs.gov/training-programs-infrastructure-partners

RESPONDING: COUNTERING A LIVE ATTACK

Cyber-crime is increasing at a significant rate across all business sectors. The Partnership's Cybersecurity Task Force concluded that two key elements in protecting businesses from criminal cyber-activity are: time management and communication.

Managing the time involved in responding to a cyber-attack is achieved through a well-constructed crisis response plan, designed to contain a cyber-attack. This response plan must be updated continuously to insure appropriate applicability to ever changing threats. Key personnel should be trained periodically on the response plan, and have access to review the plan as needed.

Along with countering the cyber-attack, a business must be prepared to talk about it, as well. Most small and mid-sized businesses do not pro-actively create crisis communications plans, and few have professionals on staff with the capacity to do so. To help the small and mid-sized business community in Houston achieve a solid readiness level, the Task Force developed the draft communications plan below to serve as a base plan for business people in any sector.

In addition, the industry sector chapters identify the appropriate law enforcement, regulatory and other entities that should be immediately involved to address a cyber-event.

Knowing the right call to make will save significant time as businesses work to protect the organization, its employees and its customers/clients.

Responsiveness: You Have Detected a Cyber-Attack – Now What?

Let's say your company's digital assets have been compromised and you are under a full-scale cyber-attack. You have only a few minutes to assess the situation and determine how best to combat the problem, while mitigating lost revenue, re-establishing operations, protecting brand equity and, if you are publicly traded, securing your share price.

The best way to insure sufficient responsiveness is to plan ahead and create a cybersecurity containment plan. There is no time for strategic thinking and planning once a cyber-attack occurs. Slow response time will only create additional company vulnerability.

Cybersecurity Containment: General Guidelines

While preventing cyber-attacks is preferable, there is a high likelihood that an attack of some kind will slip through. To prevent cyber breaches from becoming costly attacks, organizations need to have containment procedures in place that are triggered when a breach occurs, enabling business resilience and avoiding disastrous outcomes. Businesses must:

IDENTIFY	which critical assets require protection and management,
CONTAIN	breaches quickly through creating a *crisis response plan*, and
MINIMIZE	the risk by working in tandem with the appropriate stakeholders and partners in a structured and controlled manner

To help small and mid-sized businesses create their own cybersecurity containment plans, the Partnership Cybersecurity Task Force created the following guidelines and questions:

Identification/Scope

- Identify the source and path of the attack.
  - » Did the attack originate externally? What endpoints such as workstations, web servers, firewalls or spam filters were breached?
  - » Did the attack originate internally? What internal controls, processes, protocols or procedures were breached?
- What systems(s), processes or resources are affected?
- Is the attack still in progress? Are technical defenses such as network monitors, intrusion prevention systems, spam detectors or other automated alerts still reporting abnormal events? Are internal personnel reporting issues and outages not already identified?
- Make regular backups of systems and logs.
- After the attack, these will be used for forensic analysis of the attack to assess the damage and identify the attacker. They may also be used as evidence if legal action is taken.
- Are neighboring/similar systems affected?
- Can honey pots assist with ending the attack and/or attacker identification? A honey pot is a trap used to detect, deflect or counteract attacks. Generally, it is a computer that appears to be part of a network and contains information or resources that would be of value to an attacker, but, in reality, it is actually isolated and monitored.
- Has source code been changed or compromised?
- Have physical assets been compromised, disabled or broken?

Communications

- Provide ongoing communications to internal personnel.
- Keep detailed records of the incident and all actions taken.

Isolation

- Secure the system(s) so they cannot be accidentally changed.
- Should the system(s) be shut down?
- Should the system(s) be disconnected from the network?
- Should functions or services be temporarily disabled? Examples of services and functions to be considered include File Transfer Protocol (FTP), telnet, web browsing, web publishing, IP phones and e-mail.
- Should external sites be blocked as sources or destinations?
- Should remote access, such as Citrix or virtual private network (VPN), be temporarily disabled?
- Can passwords be changed immediately?
- What monitoring/remediation tools are available?
- What are the risks of continuing operations?

Data

- Has any data been obtained by the attackers?
- Has the confidentiality, integrity or availability of data been affected? If so:
  - » What are the reporting/notification obligations?
  - » What is the recovery point objective (RPO)? If data has to be restored from backup, how much data loss is acceptable? The recovery point represents the point in time up until which data can be recovered. For example, if the recovery point is four hours, this means that work that is more recent than four hours old will likely be lost, but work that was completed prior to the four hour threshold will be backed-up successfully.
  - » What is the recovery time objective (RTO)? The recovery time is the maximum tolerable length of time a computer, network or application can be unavailable after a disaster or attack.

Control the Story: Communicate

Your most important internal and external stakeholders including the media will expect expedient information about the breach as it unfolds. How you handle communications during and after the attack is paramount in decreasing chaos as your team counteracts and recovers from the cyber-attack.

One of the most critical, and sometimes overlooked, weapons in any organization's cybersecurity arsenal is its crisis communications plan and readiness of the team to move into action. In so many cases, organizations don't prepare in advance, let alone practice crisis communications drills. As employees, customers, news media and other

stakeholders learn of the cyber-attack, a company's response time and transparency in communicating what is known, are seriously scrutinized. In today's world of instant news, taking control of the situation is paramount to protecting a company's business reputation.

While a cyber-attack can cripple an organization, it doesn't have to be a public relations nightmare or cause significant harm to your brand. Formulating and practicing the crisis communications plan in advance is the best way to prevent further damage. If you don't have an in-house communications department, consider contracting with an experienced crisis communications firm or individual that can help you prepare, train and immediately deploy.

It's far easier to devise well-thought-out actions in a non-crisis environment versus trying to invent your communication approach when you are experiencing a real attack.

A well-constructed crisis communications "tool-box" includes company-specific communication templates and a step-by-step action list in the event of a cyber-attack. These steps should include:

- Designate an executive crisis team within your organization and define each individual's role and responsibilities. Bring all participants into your action plan, to insure that you've looked at all vulnerabilities you face during an attack, and create team cohesion to facilitate success in managing a real-time situation.
- Have your legal counsel brief your key executives on cyber-attack compliance mandates congruent to your line of business. Then outline who must be notified, how you will notify them, as well as communications requirements to assure compliance. This must be clearly delineated in your crisis communications plan and is critical if you are a publicly traded company.
- Outline your internal team notification process and an hour-by-hour timeline of each step to be taken once an attack is confirmed.
- Create an external communications section of your plan.
  - » Designate your official company spokesperson(s)
  - » Provide media training for crisis-style interviews
- Develop a media log to track all inquiries and coverage in chronological order. All media inquiries must be replied to in a timely manner or you will lose control of what is being said about your organization in the press. If you don't establish your voice quickly, someone else will do it for you. Likely, someone who doesn't have all the facts. Having inaccurate information "on the street" can create more work for you and your team, and more damage to your reputation and brand.
- Include a social media section in your plan that covers monitoring conversations on key platforms (i.e., Twitter, Facebook, etc.) to stay abreast of what's being said about your organization. Depending on your situation, you might also use these vehicles for issuing company-related responses as appropriate to your type of business.
- Create, and keep current, appropriate templates and scripts for use in a real situation. Remember with any correspondence during a crisis, keep it simple and focus only on the facts that can be released to assure you don't further jeopardize your position. These templates can include, but not be limited to:
  - » internal employee correspondence,
  - » website posts and updates,
  - » statements or press releases for the media,
  - » specific correspondence to investors,
  - » phone scripts for switchboard personnel,
  - » social media statements, and
  - » fact sheets on your company or organization with the basics of who you are, what you do, who you serve, where you do business and so on.
- Organizational review and approval of the crisis communications plan should include leadership within your organization, including C-suite executives, legal counsel, information technology, operations, finance, investor relations and of course, communications. Conduct internal drills or desktop training sessions for all involved staff once the crisis communications plan is complete. Make sure you're not implementing your plan for the first time during a real cyber-attack.
- Review and evaluate your plan several times a year to assure your processes still work, the information is accurate, contact lists are current, and crisis team roles and protocols are up to date.

By taking the time to prepare for a cyber-event you will be able to effectively react in the face of an actual attack – when minutes matter most.

SIX RISK AREAS FOR ALL BUSINESS SECTORS

Businesses face a variety of potential cyber-attacks. It is imperative that businesses are aware of the different types of cyber-attacks that may be used in order to understand how to avoid these attacks and mitigate the damage should an attack occur. We have discussed six of the most common types of cyber-attacks and have included the best practices available to businesses in order to thwart these malicious efforts.

1. Phishing: Most popular cyber weapon

It is estimated that 91 percent of data breaches occur with a "phishing" e-mail. Phishing is the act of attempting to acquire information such as usernames, passwords and non-public personal information (NPPI) by masquerading as a trusted entity in electronic communication. Phishing is typically carried out by e-mail spoofing or instant messaging. Spear phishing refers to highly targeted e-mails, often using detailed information about the recipient, obtained from social media.[26]

Phishing e-mails often contain malware known as Trojans. Like the Trojan Horse, once inside a company's firewall, they open the gates for other attackers. Phishing e-mails can also include keystroke loggers, which can record your entry of user IDs and passwords, and send this information to hackers. These e-mails seek to gain personal, often confidential, information about their targets by persuading people to click on a link, which installs a malicious code, circumventing security technology.

How Phishing Works

E-mail addresses are an important credential. It is a critical communication tool. Regrettably, it is also a target. Phishing companies purchase e-mail addresses from hackers, for up to $1 each. It only takes one e-mail address to allow a phishing company to successfully send an official-looking communication to an employee, enticing them to open the e-mail, click on a link or provide additional personal information.

Security breaches as a result of phishing e-mails are becoming more frequent, sophisticated and costly. Phishing e-mails attempt to leverage aspects of human nature in an effort to have people open them. They take advantage of people's trust by masquerading as banks, service providers and investment houses or as social networking friends, professional colleagues and business associates. Phishing schemes use people's natural curiosity against them. E-mails attempt to entice people by promising lottery winnings and deals that are too-good-to-be-true or imploring people to discover who has been searching for them online. Also, phishing attempts lure people in by creating the illusion that it is necessary to open them in order to avoid negative consequences, such as limiting a PayPal account or correcting an error like an e-mail with fake order confirmations from known online merchants or shopping sites citing alleged purchases. These e-mails even attempt to pose as charities often appealing for assistance involving disaster relief for victims.

Defending against Phishing:

Security awareness is the best defense against these pervasive, and increasingly sophisticated, attacks. Taking the bait in these e-mails circumvents most technology security safeguards. Therefore, training is the key to preventing security breaches from phishing schemes. Business leaders and employees must become human firewalls by being aware, skeptical and discerning. This cybersecurity defense is available to you at no cost. Training to prevent phishing attacks should include the following list of questions to help evaluate potentially suspicious e-mail:

- Did I receive the e-mail at an unusual time for the sender?
- Is the sender someone I ordinarily communicate with?
- If I know the sender, is the content out of character?
- Does the e-mail include an attachment?
- Does the e-mail contain grammatical or spelling errors?
- Does the content sound odd or illogical?
- Does the e-mail contain a hyperlink?
- After you've asked these questions, hover over the hyperlink and see if the website is consistent with the text. Then, copy and paste any links manually into the web browser to review prior to navigation.

Summary: Phishing e-mails give criminals access to personal information. Preventing their success involves no-cost staff training and awareness.

[26] "Spear-Phishing e-mail Most Favored APT Attack Bait," Trend Micro Incorporated, 2012. http://www.trendmicro.com/cloud-content/us/pdfs/ security-intelligence/white-papers/wp-spear-phishing-e-mail-most-favored-apt-attack-bait.pdf

2. Social Media: Don't "friend" your enemies

Social media sites and blogs have opened new avenues of attack. A Deloitte survey primarily of security and IT professionals in technology, media and telecommunications companies showed that "exploitation of vulnerabilities in Web 2.0 technologies" and "social engineering" were regarded as threats by 83 and 80 percent of respondents, respectively.[27] An internetnews.com article explained that attackers focusing on social media users were "attempting to trick [users] into downloading malware or divulging sensitive information."[28] That same article noted that the type of operating systems and browsers are irrelevant given that the user, not the technology, is being targeted.

Attackers use social media to identify, profile and compile personal identification data on potential targets. Data aggregation from multiple sites can lead to compromised passwords, data leakage and security incidents — or even lawsuits. Adversaries can use data extracted or derived from social media sites and various public information sources to build profiles of executives and board members for identity theft or cyber-attacks, via account access or spear-phishing. Some social media applications can be exploited by third parties to extract more data than users knowingly provide.

A related concern is managing collaborative computing environments. Some of these environments offer few barriers to inadvertent data sharing and can open avenues for loss of valuable IP.

Some enterprises go to great lengths to limit their exposure to social media. Others take a mixed approach, permitting marketers to use social media to monitor public opinion and HR professionals to check the backgrounds of potential hires. On the other hand, some companies do not have any well-defined approach. The best approach is to have a social media policy. The social media policy should consider the costs, benefits, risks and rewards to the enterprise and its stakeholders, ultimately determining the ideal way to balance them.

Summary: Social media sites and public information sources provide a platform for adversaries and attackers to extract or derive data and build profiles of business leaders for identity theft or cyber-attacks. Educated management of social media access is key to preventing business exposure.

STEPS TO CONSIDER

- Get smart. Understand the features and dangers of social media sites and collaboration tools.
- Create boundaries. Establish policies to govern social media, collaboration tools and data loss prevention.
- Educate your workforce. Training can promote proper use of social media and collaboration tools and limit inappropriate data sharing

[27] "The Future of Security: Evolve or Die," Deloitte, 2011. http://www.deloitte.com/assets/Dcom-MiddleEast/Local%20Assets/Documents/ Services/ERS/me_ers_future_of_security_0110.pdf

[28] Barrett, Larry. "Symantec's 'Unlucky 13' Security Trends for 2010," Internetnews.com, 20 November 2009. http://www.internetnews.com/ security/article.php/11803_3849371_1

3. Mobile Devices: Multiplying opportunities of attack

Mobile devices are pervasive and diverse in type, capability and risk. According to Pew Research Center, 15 percent of U.S. adults and 25 percent of young adults access the Internet mostly using on their cell phones.[29] In the business community, "mobile devices" includes the full range of smartphones, laptops, notebooks and tablets.

Mobile devices present relatively easy, low-risk points of entry to attackers, as enterprise security standards can be difficult to apply to the applications that are issued. Attackers can remotely monitor mobile devices for passwords, account numbers and personal identification data. These devices also open avenues of attack through social media sites and communication media.

Nevertheless, these devices can be outfitted with various levels of protection, although there are trade-offs between ease of use and security. Many of today's smartphones can be configured to lock down browser access, limit downloading of third-party applications and improve control over other functions. These security measures must always balance protection and productivity though.

Anti-virus protections are also available, yet they tend to be underused on mobile devices.

In addition, many users exercise a lower level of care with cell phones and Personal Digital Assistants (PDAs), and perpetuate these relaxed habits in their computer use in both their personal and professional lives.

Mobile devices have effectively become part of the corporate network and should be viewed as such and their risks addressed.

Summary:

Many of today's smartphones can be configured to lock down browser access, limit downloading of third-party applications, and improve control over other functions. Balance protection and productivity.

STEPS TO CONSIDER

- Leave it at home. Several enterprises restrict users' primary mobile devices to domestic use, and issue temporary devices with minimal data for overseas travel.
- Lock it down. Configure mobile devices to minimize the chances of being scanned, "sniffed", or tampered with; many can be encrypted selectively, for example for travel to high risk geographies — or just a trip to the local coffee house. .
- Employ dynamic policies. Policies such as application "white lists" are essential, as is considering the security capabilities of mobile devices in purchase decisions.

[29] "Teens and Technology," Pew Research Center, 13 March 2013. http://www.pewinternet.org/~/media/Files/Reports/2013/PIP_TeensandTechnology2013.pdf

4. Cloud Computing: Cloudy with a chance of infiltration

In 2015, use of public cloud accounted for nearly $100 billion in revenue. According to Forrester Research, it is expected to grow to $160 billion by 2020. Forrester also found that organizations increased their security spending in 2015 by 46 percent and for cloud computing this increase was an astounding 42 percent. Adoption of cloud based services is happening at a rapid pace and customers need to gain a clear understanding of risks associated with this service model.[30]

Security controls for cloud services are very similar to controls implemented for on-premises IT environments, however there is a clear division of responsibility between the customer and the cloud service provider (CSP). Operational control rests with the CSP and this introduces multiple levels of risk. Risks will vary with the type of cloud service (public, private or hybrid), its architecture and whether it is a software, platform, or total infrastructure service. On the flip side, cloud computing provides vastly improved security services when compared to security implemented on premises. This is a very important consideration for organizations, particularly SMB's that have limited resources to invest in skilled security personnel.

Customers need to ensure that the cloud service agreement (CSA) with a CSP has appropriate provisions for security and privacy that meet or exceed the customer's security policies. The agreement must help maintain legal protections for the privacy of data stored. Some of the key security risks that should be addressed are:

- Governance Loss – As operational control has shifted to the CSP, issues connected with service availability and problem resolution times need to be addressed.
- Authentication and Authorization. – As cloud services can be accessed ubiquitously from anywhere in the world, customers must analyze the CSP's capabilities for multi factor authentication and auditability.
- Compliance and legal risks – CSP's should hold multiple certifications such as SOX, HIPAA and FISMA. CSP's with SSAE 16 (Statement on Standards for Attestation Engagements 16) by the American Institute of Certified Public Accountants (AICPA) certification demonstrate adherence to strict audit guidelines by an independent third party.
- Allocation of Responsibility – Responsibility over aspects of security may be split between the provider and the customer. Allocation of security responsibility should be clearly defined to minimize security gaps.

STEPS TO CONSIDER

- Understand the configuration. Know where the cloud components and your data will be housed and who is responsible for which functions and risks.
- Apply your standards. To the extent possible, apply your standards to service providers, and remember that you can outsource functions but not risks.
- Trust but verify. Due diligence when selecting service providers and address each party's rights and responsibilities within the contract.

[30](http://www.forbes.com/sites/louiscolumbus/2015/01/24/roundup-of-cloud-computing-forecasts-and-market-estimates-2015/).

The Cloud Security Alliance (https://cloudsecurityalliance.org/) is an independent third party that has developed a set of security guidelines that every cloud customer would find useful. These guidelines include STAR (Security, Trust and Assurance Registry) and Cloud Controls Matrix.

One key question: Who is responsible for certain aspects of the systems and the data in the cloud? Other challenges center on service availability, access management, reliability assessment and risk management.

As with data centers, claims, or bill processing services, service level agreements (SLAs) and audit clauses can enhance control and transparency. Some cloud providers limit what customers can inspect, potentially placing the data center and other areas out of bounds. This can be cause for concern in a multi-tenant, highly virtualized world. If a breach or data loss occurs, the agreement may provide little protection or compensation. Providers typically do not accept the business and financial risks that cloud computing poses to the enterprise.

Given its stage of development and more open architecture, cloud computing can present serious risks. Data may reside anywhere in the cloud, in multiple locations, on shared devices and in foreign nations. Most enterprises more fully understand business and legal conventions in their domestic (as opposed to foreign) locations; therefore, when cloud components reside in foreign locations, the complexities and risks increase and must be managed aggressively. Additionally, businesses may need to produce an audit trail or specific data for tax or legal purposes, and must have access and capabilities that permit such retrieval. Thus, a number of issues must be addressed if cloud computing is to provide sufficient security.

Summary: Choose a cloud provider according to your business needs, and ensure that they are outlined in a service agreement contract.

5. Software Vulnerabilities: The underbelly of your IT environment

Software vendors regularly release patches, hot fixes and public announcements due to exploitation of their software products. With a growing number of applications being released for multiple platforms - including some, such as mobile applications, with very short build-test cycles - the number of software vulnerabilities has never been greater.

According to Forrester Research, social networks and Web 2.0 provide fertile ground for malware propagation.[31] That same report also saw a rise in "drive-by download exploits of vulnerabilities" and expected this tactic to expand as Rich Internet Application (RIA) technologies gain consumer acceptance. Pirated software, which fosters malware distribution, proliferates particularly in countries with lax intellectual property laws. The overlap between work and home life, the growing use of independent contractors and the sheer volume of pirated software make it easy for a virus, worm, or exploit to open a system to attack. Even legitimate software is at risk, given that freeware vendors, which rely on third party banners and advertisements for operating revenue, can be exploited.

No antivirus or firewall can guarantee protection. Collectively, attackers have almost unlimited time, skills and resources to devote to creating and exploiting vulnerabilities. That gives them an advantage over security teams with limited resources and a broad range of priorities. Even the leading security companies are often unable to keep pace with new threats. Although diligently implemented policies can greatly improve security, identifying all vulnerabilities can often prove to be nearly impossible. This underscores the need to anticipate incidents, take precautions, and prepare for an event in which the precautions taken were unsuccessful.

It is imperative that businesses employ vulnerability assessments, security design reviews, automated tools, and peer reviews whether they are creating software, implementing solutions, or developing in-house systems. These measures should be applied in the context of cost-benefit analysis. Although perfection cannot be achieved, the primary goal must be to have a consistent application of sound risk management processes.

STEPS TO CONSIDER

- Anticipate and defend. Anticipating cyber-attacks enables you to develop software procedures that facilitate damage control, system resiliency, rapid recovery, privacy protection and notification and public relations plans.
- Define normal to identify abnormal. In order to monitor unknown threats, develop heuristics, or techniques, that can detect unusual code or activity.
- Exercise vigilance. Develop baseline metrics and maintain situational awareness of network activity, monitoring your software for unusual spikes or traffic destinations.

Summary: Attackers have almost unlimited time, skills and resources to devote to creating and exploiting vulnerabilities. Active anticipation and assessment can detect abnormal activity and defend against cyber-attacks.

[31] Penn, Johnathan with Garbani, Jean-Pierre and Radcliffe, Edward. "Consumer Security Market Trends, 2009 to 2010: Evolving Threats and Defenses," Forrester, 12 November 2009. http://www.forrester.com/ Consumer+Security+Market+Trends+2009+To+2010+Evolving+Threats+And+Defenses/fulltext/-/E-RES55723?objectid=RES55723

6. Insider Threat

Organizations continue to face a variety of insider threats, as demonstrated by a string of high profile cases where employees in pursuit of validation or affirmation used their knowledge and access to physical and/or information systems to cause significant damage. These cases highlight vulnerabilities and underscore a historical, yet erroneous, perception that insider threat mitigation is predominately an information technology responsibility. This approach leaves an organization vulnerable to existing and emerging insider threats.

Few entities have a specific internal working definition of insider threats as security and IT budgets historically prioritize external threats. Defining the threats from within an organization and specific business environment is a critical first step to formulating a preventative program, as it will inform the size, structure, scope, and phasing plan, aligned to business risk priorities.

Define the critical assets (facilities, source code, IP and R&D, customer information) that must be protected and the organization's tolerance for loss or damage in those areas. Identify key threats and vulnerabilities in your business and in the way you do business. Tailor the protection program to address these specific needs, threat types and take into account your organization's unique culture.

Establish a cross-disciplinary insider threat working group to serve as change agents and ensure the proper level of buy-in across departments and stakeholders (e.g., legal, physical security, policy, IT security, human resources, ethics, etc.). The working group's support will be critical to building the insider threat mitigation capability and securing data needed for the program. It should assist in addressing common concerns (e.g., privacy and legal) and support the development of messaging to executives, managers and the broader employee population.

The insider threat challenge is a people-centric problem that requires a holistic, people-centric solution. Organizations should avoid the common pitfall of focusing on a technical solution as the silver bullet. Routine and random audits of privileged functions are commonly used to identify insider threats across a broad spectrum in a variety of industries. Organizations should trust their workforce but balance that trust with verification to avoid instances of unfettered access and single points of failure. This auditing is particularly essential in critical areas.

Case studies analyzed by Carnegie Mellon University's Computer Emergency Response Team (CERT) program reveal that insider threats are seldom impulsive.[32] Rather, insiders move on a continuum from the idea of committing an act to the actual act itself (e.g., fraud, espionage, workplace violence, IT sabotage, and intellectual property and research and development theft). During this process, the individual often displays observable behaviors (e.g., requests undue access, violates policies, and demonstrates disgruntled behavior) that can serve as potential risk indicators for early detection.

According to the FBI's Insider Threat Program, detection of insider threats should use behavioral-based techniques. Creating a baseline of "normative" activity of how people operate on the system and off-the network, will help identify anomalies. By correlating precursors or potential risk indicators captured in virtual and non-virtual arenas, organizations can gain insight into micro and macro trends in the high risk behaviors exhibited across the organization. Using advanced analytics platforms that ingest and correlate outputs from a variety of tools can facilitate this analysis. The resulting outputs can be used to identify insider threat leads for investigative purposes, while shedding new light on processes and policies that are either missing or could be improved upon.

As insiders' methods, tactics and attempts to cover their tracks constantly evolve, the insider threat mitigation program and precursor analysis must continuously evolve as well. This can be achieved through a feedback mechanism that includes an analysis of on-going and historical cases and investigations.

Workforce behavioral expectations need to be clearly defined, broadly communicated and consistently enforced policies (e.g., social media, removable media, reporting incidents, bring your own device (BYOD, etc.) to provide a basis for protecting a business from insider threats.

[32] Common Sense Guide to Mitigating Insider Threats, 4th Edition. CERT Program.http://resources.sei.cmu.edu/asset_files/TechnicalReport/2012_005_001_34033.pdf

Just as each business is unique, each organization's internal threat is unique. Still, each entity should train its employees based on the physical and network access levels, privilege rights and job responsibilities. Additionally, employees should be trained for the specific insider threat risks, challenges and responsibilities for each position (i.e., the data administrators' curriculum should be different from the sales representatives' curriculum).

Summary: The insider threat challenge is not a purely technical one, but rather a people-centric problem that requires a holistic and people centric-solution.

STEPS TO CONSIDER

- **Define your insider threats** — An insider can be an employee, a contractor, or a vendor that commits a malicious, complacent or ignorant act using their trusted and verified access.
- **Define your risk appetite** — Define the critical assets (e.g., facilities, source code, IP and R&D, customer information) to protect and identify key threats and vulnerabilities in your business.
- **Leverage a broad set of stakeholders** — The program should have one owner but a broad set of invested stakeholders.
- **Technology, alone, won't solve the problem** — An insider threat mitigation program should include key business processes (e.g., segregation of duties for critical functions), technical and non-technical controls (e.g., policies), organizational change management components, and security training programs needed to promote an environment of security awareness and deterrence.
- **Trust but verify** — Establish routine and random auditing of privileged functions.
- **Look for precursors** — Understand how insider threats emerge and use behavioral-based techniques to detect and prevent their attacks.[33]
- **Connect the dots** — Precursors or potential risk indicators captured in virtual and non-virtual arenas can identify insider threat leads and policy needs.
- **Stay a step ahead** — Continuous analysis and vigilance are necessary to meet ever-evolving threat tactics.
- **Set behavioral expectations** — Define workforce behavioral expectations through clear and consistently enforced policies (e.g., social media, removable media, reporting incidents, BYOD, etc.) and communicate consequences for violating policies.
- **One size does not fit all** — Customize training based on the physical and network access levels, privilege rights and job responsibilities.

[33] Common Sense Guide to Mitigating Insider Threats, 4th Edition. CERT Program.http://resources.sei.cmu.edu/asset_files/TechnicalReport/2012_005_001_34033.pdf

Other Things Business Leaders Should Consider

New Regulations Create Opportunities for Entrepreneurs, Startups and Small Businesses

Due to stricter cybersecurity mandates across all levels of government, there will be two big areas of attention for small businesses and startups:

- Companies that do business with the government soon will be subject to stricter cybersecurity measures, mandated in requests for proposals (RFPs) and purchasing terms. These new mandatory compliance measures will create a market of government contractors that need to upgrade software, hardware, and operating procedures.
- Because many of these government contractors are not in the business of cybersecurity, these new security measures create opportunities for service providers (startup and otherwise) to facilitate these upgrades.

For Governments: Ensuring Compliance across a Network of Contractors

Since 2002, over 173,000 businesses have downloaded bid specifications from the City of Houston.[34] This represents a massive network of businesses that all need a cybersecurity infrastructure in order to compete for a contract.

In order to create a competitive marketplace of contractors, municipal governments should implement new ways to encourage compliance, such as:

- Incentives. Provide a scoring bonus for voluntary compliance with cybersecurity recommendations.
- System for self-reporting. Define methods for self-reporting cybersecurity compliance, including what is part of the public record, what can be kept confidential, and what can be measured and reported by a trusted third-party.
- Random audits. Define a process for auditing a sample group of vendors, and provide clear scoring methods and steps for reconciliation. Random audits should be used as a check on vendor self-reporting.

For Startups: Understanding Opportunities within Compliance

Already, there is renewed interest in cybersecurity startups. Virginia's Center for Innovative Technology established an accelerator program specifically for cybersecurity startups, and Entrepreneur.com ran several articles on the issue earlier this year, addressing several areas of cybersecurity:

- "Fertile Ground for Startups: 10 Sectors of the $207 Billion Cybersecurity Industry Poised to Take Off" [35]
- "Cybersecurity a Growing Issue for Small Business"[36]

[34] Fell, Jason. "Cyber Security a Growing Issue for Small Business," Entrepreneur, 21 March 2013. http://www.entrepreneur.com/ article/226181#ixzz2fT4lL7kQ

[35] "Formal Bids & RFPs," City of Houston Strategic Purchasing, The City of Houston. https://purchasing.houstontx.gov/bid_download.aspx

[36] Clifford, Catherine. "Fertile Ground for Startups: 10 Sectors of the $207 Billion Cybersecurity Industry Poised to Take Off," Entrepreneur, 18 April 2013. http://www.entrepreneur.com/article/226455

Cybersecurity: Sector-by-Sector

It is imperative that businesses understand how cybersecurity specifically applies to their industry so that they are able to be as prepared as possible. The following sections focus on the energy, health care, legal, banking and finance, education, retail, insurance, and human resources sectors. These sections provide an overview of business characteristics, key statutes and government agencies that should be involved in the event of a cyber incident, internal roles and responsibilities and budget specific recommendations for these industries.

ENERGY SECTOR OVERVIEW

Houston is considered by many to be the "Energy Capital of the World." This city is the leading domestic and international center for virtually every segment of the energy industry –exploration, production, transmission, marketing, service, supply, offshore drilling and technology. In 2012, the Houston metropolitan area held 28.8 percent of the nation's jobs in oil and gas extraction - 53,900 of 186,800. The region has more than 3,700 energy-related establishments, both upstream and downstream. The logistics for moving much of the nation's petroleum and natural gas across the country are controlled from Houston. Sixteen of the nation's 20 largest interstate oil pipeline companies have a presence in the Houston region. These 16 companies control 69,866 miles, or 47 percent, of all U.S. oil pipeline capacity.[37] Seventeen of the nation's top 20 natural gas transmission companies have corporate or divisional headquarters in Houston, controlling 126,085 miles of pipeline, which is 64 percent of total U.S. gas pipeline capacity.

The Department of Homeland Security (DHS) has highlighted the energy industry as one of the primary critical infrastructure sectors that must be protected in order to secure our nation from cybersecurity attacks. Thus, it is critical that the energy industry is adequately prepared to deal with the threat of cyber-attacks.

"The U.S. energy infrastructure fuels the economy of the 21st century. Without a stable energy supply, health and welfare are threatened, and the U.S. economy cannot function . . ."[38] The Energy Sector is "uniquely critical because it provides an 'enabling function' across all critical infrastructure sectors. More than 80 percent of the country's energy infrastructure is owned by the private sector, supplying fuels to the transportation industry, electricity to households and businesses, and other sources of energy that are integral to growth and production across the nation.

"The energy infrastructure is divided into three interrelated segments, including: electricity, petroleum and natural gas. The U.S. electricity segment contains more than 6,413 power plants (this includes 3,273 traditional electric utilities and 1,738 nonutility power producers) with approximately 1,075 gigawatts of installed generation. Approximately 48 percent of electricity is produced by combusting coal (primarily transported by rail), 20 percent in nuclear power plants, and 22 percent by combusting natural gas. The remaining generation is provided by hydroelectric plants (six percent), oil (one percent), and renewable sources such as solar, wind, and geothermal (three percent). The heavy reliance on pipelines to distribute products across the nation highlights the interdependencies between the Energy and Transportation Systems Sector."[39]

Cybersecurity has emerged as a major new challenge to the energy industry.

- This issue occurs in "cyber-space", where information, business transactions and operational controls can be stolen, interrupted and manipulated. Threats from global "bad actors" are real and increasing. Cybersecurity requires strong collaboration and information sharing between the government and private industry, as well as every participant in the energy supply chain. This is where businesses are critical to the nation's cybersecurity success.
- The energy industry is increasingly dependent on partnerships and relationships for success. It is critical for employees and partners of companies to be cyber aware, knowledgeable and able to take action to prevent, mitigate and contain cyber-threats.

The purpose of this section is to communicate, educate and reinforce the actions that small and mid-sized energy companies can do to achieve cybersecurity readiness and resilience.

[37] Houston Facts, Greater Houston Partnership, 2013, 22

[38] "Energy Sector," Department of Homeland Security. http://www.dhs.gov/energy-sector

[39] Ibid.

Business Characteristics

The cyber environment in the energy industry is very complex. Often, cybersecurity is thought of as computer systems in a data center; however, this is not the only aspect that energy companies need to consider. All infrastructure systems used by energy companies are dependent on technology, from exploration sites, pipelines, and refineries, to power generation and energy distribution. This technology can be distributed throughout geographies in very remote locations to manage energy delivery. For this reason, the industry cannot separate physical security from cybersecurity. Physical and cyber-threats have to be considered in tandem as the industry looks to protect its infrastructures that provide the essentials of our economy, as well as the safety and expectations of everyday life.

Cyber-Attacks on the Energy Sector

Due to the nation's energy dependency and the importance of specific components of the energy delivery system, businesses in this industry are a target for cyber-attacks in the following areas:

Personally Identifiable Information

Many of the energy companies provide direct services to customers. Customer information, if breached, can provide for economic gain through fraud and other tactics.

Intellectual Property and Competitive Information

Energy companies, for the most part, are in a market-based economy. Intellectual property or competitive information has value on a global financial and political scale. Successful cyber-attacks could cause billion-dollar losses.

Critical Infrastructure Information

Extraction and exploitation of information regarding facilities and equipment in the energy supply chain can threaten safety, operational and national security.

Control System Accessibility

Engineered energy systems are built for safe operations across the entire energy supply chain. Safeguards are in place to address operational issues safely. For example, a system may systematically shut down due to unstable conditions. Protecting these control systems is paramount to ensuring energy supply reliability

Information Technology (IT)/Operational Technology (OT) Convergence

Traditionally the sensitive control systems in Operational Technology (OT) environments were physically isolated from the corporate IT systems. In today's hyperconnected world, that is not always possible. As companies look to leverage information sharing between IT and OT environments, they might unknowingly introduce an attack vector from the corporate IT environment into the sensitive OT equipment. When executing any IT/OT convergence projects, it is important to maintain proper network segmentation, and deploy sufficient safeguards to ensure the network segmentation between the IT and OT systems are enforced.

The Energy Sector and Bad Actors

Many "bad actors" thrive in cyber-space. They use a variety of approaches to attack energy companies in order to achieve their objectives. The following are explanations of some of those approaches:

Social Engineering

These attacks take on many forms. Many people in the business community are familiar with emails that attempt to entice people to click on a link, which will then deploy malware into a local personal computer or system. However, social engineering, a type of confidence trick for the purpose of information gathering, fraud, or system access, takes on many different faces. Private information can be obtained by calling personnel to "spoof" them into providing information about their identification (ID) or having them click on a link so they can record the entry of an ID. Attackers can also deploy malware into the local computer and/or the connected computer. Providing an ID and password, unknowingly, to attacker is handing the "keys to the kingdom" over to people who have nothing but malicious intent. Social engineering can also involve gaining access to secure areas to connect to or deploy malicious equipment or programs in an attempt to gain access to technology systems. Thus, physical security and cybersecurity must stay interconnected in order to insure effective mitigation.

STEPS TO CONSIDER

- Understand. Work to understand the threats and develop approaches, policies and processes to ready employees for cyber defense.
- Communicate. Provide information, education and training to employees regarding cybersecurity.
- Confirm. Validate through periodic surveys, inquiries or tests that your employees are demonstrating cyber defensive skills.

Summary: The greatest success for a cyber-attacker is through the resources within an organization. An employee's cyber skills are critical in a company that provides resources to many organizations.

Advanced Persistent Threats (APT)

As the name would suggest, Advanced Persistent Threats (APT) are systematic, long term attacks against technology systems that seek to create situations for very complex malware programs to be introduced or permitted access to critical systems or information. Often attributed to nation states, APTs are also used by organized crime groups. APTs are generally the accumulation of several strategies, including: phishing, social engineering, waterholes, exploratory hacking and others. It is estimated that the average APT occurs over a 14 month period.

APTs are not limited to technologically based attacks, but can include insider sabotage or espionage, as well. Nation states and other entities are training personnel and encouraging people to apply for jobs in energy and other industries with the implicit intent to extract information and content over time. Again, there is a strong correlation between physical security and cybersecurity as demonstrated by the need to perform background checks, monitor unusual traffic within a business system and not just the attempts to get into systems, and restrict physical access controls to certain areas of the company.

Summary: APTs are sophisticated, persistent attacks coming from well-skilled and well-funded bad actors. It is necessary to insure that cyber-based interactions are appropriately mitigated in order to assist in managing this threat.

Supply Chain

Technology components, operating systems and application codes are manufactured or developed across the globe. There is an ever-increasing demand to insure that there is security and integrity in these components across the supply chain. Once thought to be solely a hardware consideration, the supply chain includes the quality, integrity and security of the operating systems and application software. Security gaps can allow malicious code to be interjected or even embedded in hardware and devices which can be attached to desktop and laptop systems, like USB memory sticks. There are many examples of over-the-counter memory sticks embedded with malware - a reminder of the risks to cybersecurity throughout the supply chain.

Small and medium-sized companies are key to the success of energy companies in today's economy. As components of the energy sector's supply chain, they offer flexibility, innovation, economics and collaboration that lead to opportunity and benefit for both organizations. Often, these companies provide programming and development of technology components. Increasingly, securing the supply chain against these threats requires knowing the source of the parts and programming is a critical component of cybersecurity.

The cybersecurity landscape and demands present challenges for both parties going forward. Operational and legal requirements may seem like difficult barriers and the resulting safeguards and procedures may involve some extra complexities to "get the work done." However, the stakes are high, the risk is great, and the consequences are too serious for all parties involved. Therefore, all companies along the supply chain must meet challenge of cybersecurity and act as part of a team to protect the infrastructure supporting the safety, reliability, sustainability and economy of one of our nation's greatest resources – energy.

STEPS TO CONSIDER

- Prepare. Understand legal and regulatory requirements. Evaluate how to integrate those requirements into the supply chain to insure integrity and security.
- Integrity. Know the suppliers and partners; integrate cyber requirements into relationships and contracts.
- Confirm. Inspect, test, validate and/or confirm suppliers' and partners' compliance with cyber requirements.

Summary: Supply chain integrity is critical to successfully mitigating cyber-threats. It is vital to know who the suppliers are and the integrity of their products. An organization should be prepared for the legal terms and conditions related to cybersecurity. Although cyber-threats may increase the cost of doing business in the energy sector, taking the necessary precautions to prevent and mitigate cyber-attacks costs less than the potential larger costs of remediating successful cyber-attacks.

STEPS TO CONSIDER

- Prepare. Understand the threats and develop approaches, policies and processes to address APT's. Establish cyber information sharing so that as threat information is received, it can be acted upon simultaneously.
- Monitor. Establish monitoring and control processes and solutions to identify vulnerabilities, threats and mitigations.
- Respond. Don't wait – respond. Time is critical in cyber space. Work fast and take appropriate actions to "contain" the potential threat.

Energy: Top 4 Cyber Actions

Recognize and accept your responsibilities in this "cyber war." Become educated about cybersecurity. Based upon your risk profile and the services you provide, invest in the people, programs, procedures and perhaps technologies to mitigate cyber-threats for your company. This investment may sound expensive, but it involves exercising good, solid and proven cybersecurity practices – many of which are no-cost. Continuously mature your company's cybersecurity skills, processes and controls to insure future success.

1. Create a culture of cybersecurity within your company. Strong employees are the greatest opportunity to practice cybersecurity. Cyber-attackers "bad actors" will attempt to exploit employees if they are weak. Deflecting those attempted attacks relies on an educated, trained and practiced cyber aware culture. Communicate with your employees to establish a cybersecurity culture in the same ways that businesses build a safety culture. Create cyber requirements, policies, and procedures and train all employees to understand and incorporate them into their daily activity, including the ability to recognize activities by bad actors. Maintain updated, concise and easily understandable information on varying security topics presented in multiple vehicles, including posters, e-mail communications, videos or other readily available reference items. Engage in periodic reviews and tests to insure your cyber-curriculum remains effective. Be a model for cyber awareness and readiness.
2. Incorporate and apply the physical security and cybersecurity guidelines included in this guide. Implementing basic rules for password protection, anti-virus, data encryption, data protection and more is "just good cyber sense." Develop a plan to implement, monitor and test these guidelines in your organization. Be prepared to adapt – the cyber world is changing every day.
3. Create a baseline measurement of "normal" activity. Conduct an initial review of how all systems are used – and perform frequent reviews to find anomalies. Conduct quality assurance confirmation that your team is following the outlined cyber program. Report any observations, concerns or findings in accordance with those procedures. This includes any concerns regarding your company's systems. Sophisticated "bad actors" attempt to exploit relationships between parties. These could be attacks against interfaces originating in your shop, file exchanges and VPN access by your employees. Time is critical for cyber-response, so creating a system that reveals attacks quickly decreases response time, and enhances cybersecurity.
4. Assign cyber responsibility and accountability in your organization. Have a clear assignment, create procedures and confirm compliance. As with any emergency planning, preparedness prevents chaos and greater loss. Trained employees with clearly defined functions, who have practiced in their roles (through simulations) are the best way to mitigate the impact of a cyber-attack. Front-line defense through a culture of cybersecurity supported by education and ongoing communication is critical to success. Businesses should utilize resources such the Department of Homeland Security's "Training Programs for Infrastructure Partners."

Private and Public Sector Cooperation

The nature of cybersecurity, and its potential risk has led to greater communications between the public and private sector. Information sharing and collaboration are leading this effort and additional initiatives are underway between energy related agencies and private energy companies to strengthen this cooperation to combat cyber-threats against the energy industry. Energy companies must establish policies and procedures to meet regulatory compliance and extend these efforts to continue the safe, reliable delivery of energy to our nation. Critical to the success of cybersecurity along the entire energy industry supply chain is for small and medium-sized businesses within that structure to incorporate company requirements, policies, legal terms, procedures, and programs. This will insure maximum security of energy company operations.

HEALTH CARE SECTOR OVERVIEW

The health care sector is a major component of the Houston region's economy. The Houston region is home to over 12,400 health care establishments, including 132 hospitals, and the Houston Metropolitan Statistical Area (MSA) employs over 290,000 employees in the health care industry, including 15,315 physicians. Harris County alone has 12,551 physicians and 95 hospitals.[40]

Houston is home to the world's largest medical complex – the Texas Medical Center (TMC). TMC member institutions have been consistently recognized as some of the best hospitals and universities in the nation by U.S. News and World Report. Considered a prized asset and engine for economic growth, TMC is currently comprised of 54 institutions. These non-profit and for-profit entities within TMC are responsible for the discoveries of new therapies and treatments that provide training and employment for our nation's health care workforce and delivery of premier care and support services to tens of thousands of individuals each year. TMC currently employs 106,000 people and its teaching hospitals train and educate 50,000 students. TMC has over 160,000 daily visitors and over 7.2 million patients visit annually, including more than 16,000 international patients. TMC institutions combined total operating budgets are $15 billion per year. According to a 2010 survey conducted by the TMC, there are 9,700 ongoing research projects at various TMC institutions – an innovation investment estimated at $3.4 billion.[41] Cybersecurity is critical to protecting the sensitive information that exists within the health care industry, and in turn, maintaining the integrity and prosperity of the industry in the Houston region.

Business Characteristics

Health care is characterized by multiple specialties providing different services to patients. To provide those services, protected health information and personal identifiable information is accessed, stored and shared by multiple individuals and organizations. Health care organizational structures can be divided into three major types – large institutions, small physician groups and bio-tech companies. Large institutions consist of hospitals, multi-specialty group practices, pharmacies, ancillaries (labs and imaging) and health plans. These organizations often have large Information Technology (IT) infrastructure, in-house legal and compliance specialists and a high awareness of cybersecurity risks. Provider practices with between one and nine employees comprise almost 60 percent of physicians.[42] These small groups and solo practices in general do not have access to the same IT and security resources. Start up companies are flourishing as health care information becomes digitized, government incentives drive interoperability to reduce costs and improve outcomes, and consumers come to expect to manage the details of their lives through mobile devices. The one thing all of these sectors have in common is the struggle and burden of complying with HIPAA security regulations, earning the confidence of their customers, and avoiding a data breach that could/would put them out of business. Small to medium size organizations have the most difficulty ensuring good cyber hygiene and adhering to HIPAA regulations due, in part, to the extraordinary number of hours it requires to implement a comprehensive HIPAA Security program and the potential costs of ensuring adequate cyber protection. This section is focused on small to medium health care businesses and emphasizes how to protect themselves and their patients with limited resources. While it is important for covered entities to have an understanding of cybersecurity and HIPAA security regulations, it is imperative that providers address HIPAA compliance as whole and not in pieces. Technical cybersecurity defenses can provide the necessary security protections, however, when a breach occurs, it is the compliance documentation and complete HIPAA program that will provide the covered entity the protection from breach penalties and fines.

[40] Houston Facts, Greater Houston Partnership, 2013, 24.

[41] Emmons, David W. and Kane, Carol K. "New Data On Physician Practice Arrangements: Private Practice Remains Strong Despite Shifts Toward Hospital Employment," American Medical Association. http://www.ama-assn.org/resources/doc/health-policy/prp-physician-practice-arrangements.pdf

[42] Cline, Bryan and Hourihan, Chris. "A Look Back: U.S. Healthcare Data Breach Trends," Health Information Trust Alliance (HITRUST), December 2012. http://www.hitrustalliance.net/breachreport/HITRUST%20Report%20-%20U.S.%20Healthcare%20Data%20Breach%20Trends.pdf

Statistics: HIPAA incidents can and do happen everyday

- According to the Office for Civil Rights (OCR), more than 2 million patient records have been breached due to lost or stolen devices
- When a breach occurs, 54 percent of patients are very likely or likely to change providers
- Over 227,000 new viruses are created everyday
- More than 14,000 patient complaints filed in 2014 with OCR
- There were 164 HIPAA breaches in 2014 affecting approximately nine million Americans
- Over 3 million cell phones were stolen in 2013 according to Consumer Reports

What Do I Have of Value?

Patient information is extremely valuable. From names to addresses to insurance identification numbers; protected health information is actively sought by thieves and hackers. Patient information is valuable to both the thief and the provider protecting the record. When information is compromised, the value of that information changes. The cost of patient information can then be measured by the cost of the breach. According to the 2015 Ponemon Institute Research Report, Cost of a Data Breach Study: United States, the average breach cost is $398 per record. For example, a breach caused by a stolen laptop, containing 3,000 patient records, will, on average, cost the covered entity $1,194,000. In addition, providers in Texas are also subject to state level fines that can be added to the federal. Patient information is also valuable to the patients themselves. Compromised financial data, such as stolen credit card numbers, has a very short shelf-life. Within minutes, credit cards are canceled and stolen funds returned. Compromised protected health information can affect a patient for the rest of their life. From stolen identities to fraudulent insurance claims, patients can end up paying the price long after the breach has occurred.

Legislative and Regulatory Requirements

Two HIPAA rules that are most applicable in regards to cybersecurity are: the Privacy Rule, or “Standards for Privacy of Individually Identifiable Health Information”, which established national standards for the protection of certain health information, and the Security Rule, or “Security Standards for the Protection of Electronic Protected Health Information (ePHI)”, which established a national set of security standards for protecting certain health information that is held or transferred in electronic form. The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that health care organizations called “covered entities” must put in place to secure individuals’ ePHI, including the information gathered, maintained or transmitted electronically.

As previously mentioned, Texas is one of the states with state level penalties. In addition, Texas also has state level privacy and breach notification requirements. The 82nd Texas Legislature expanded the requirements and penalties for breaches by passing House Bill 300 in 2011. Although privacy and breach notification are not directly related to cybersecurity, it is very important for covered entities in Texas to be aware of the state level requirements, as they preempt the federal. For example, Texas differs from the federal HIPAA privacy and breach notification regulations in the following ways:

1. Employees must complete training within 90 days of hire
2. Covered Entities must provide patients with electronic copies of their electronic health records within 15 business days of the patient’s written request
3. Records of employee training attendance must be kept for 6 years

When a cyber-breach occurs, covered entities must be prepared to provide not only documentation proving their compliance with security controls, but they must provide documented proof of compliance for all regulations under HIPAA, including privacy and breach notification.

Main Components of a HIPAA Security Compliance Program

HIPAA Security compliance is an overwhelming process, especially when an organization does not have regulatory or cybersecurity expertise in-house – as most do not. For the purposes of this document, the compliance process can be stripped down to three main sections.

Risk Analysis

1. The Security Rule requires Administrative, Physical and Technical Safeguards. The Administrative Safeguard provisions in the Security Rule require covered entities to perform risk analysis as part of their security management processes. Risk analysis results determine which security measures are reasonable and appropriate for a particular covered entity, and affects the implementation of all safeguards that are contained in the Security Rule.
2. A risk analysis includes 3 parts:

- Risk Assessment – information related to all administrative, technical, organizational and physical procedures of a covered entity is gathered through a thorough questionnaire. The assessment is the foundation of the risk analysis. The more comprehensive the assessment the more complete the analysis.
- Compliance Analysis – compliance is reviewed for all 60+ safeguards and implementation specifications. The compliance portion or the risk analysis informs the covered entity which safeguards and implementation specifications are currently being met.
- Threat Analysis – reasonably anticipated threats must be analyzed. Threats include natural, human and environmental events. Evaluate the likelihood and impact of potential risks to protected patient information. Security controls that are reasonable and appropriate to the specific covered entity being analyzed are reviewed for their ability to reduce risk of threats.

Safeguards, Policies and Procedures

It is not enough just to identify areas of non-compliance. Safeguards must be properly implemented and documented to achieve compliance. How a covered entity implements the necessary cyber-security controls provides for the development of HIPAA security policies and procedures. Policies and Procedures must be custom to the organization. Template binders or document libraries are not policies and procedures and will not meet the regulatory requirement under the law. Unless using the services of a HIPAA compliance regulatory consulting company, organizations should carefully read the fine print of purchased policy binders. Key words such as “guide for creating policies” or “sample polices to be reviewed” indicate the policies, as is, are not the final version that represents the actual security policies of the organization. Template policies can increase HIPAA fines and penalties.

Risk Management

Documentation of compliance is required at the time of implementation and ongoing as part of a covered entity’s risk management plan. Without risk management, an organization cannot be compliant with the security rule. In addition to documented actions such as new hire paperwork and termination procedure verification, security controls must be continually reviewed and monitored to show on-going compliance. For example, review of audit logs and regularly updated security patches must be monitored and documented. When a breach occurs, risk management documentation provides the proof required to show adherence to an organization’s policies and procedures.

Enforcement and penalties are covered in the Privacy Rule.

Available Resources

There are resources to help providers comply with the regulations and respond in the event that a cyber-attack or data breach does occur. These resources include:

- Local medical society
- Texas Medical Association
- Department of Health and Human Services Office for Civil Rights
- HealthIT.gov and Office of the National Coordinator for Health IT
- Texas Department of State Health Services
- Regional Extension Centers (Gulf Coast Regional Extension Center at UTHealth - https://sbmi.uth.edu/gcrec/)
- HIPAA Risk Management and the Online HIPAA Security Manager

Top Four HIPAA Incidents for Small to Medium-Sized Organizations

Every day, in practices all over the country, HIPAA incidents occur. One HIPAA incident can result in an investigation by OCR. It is important for organizations to be prepared to respond quickly and accurately to these incidents. In order to do so, organizations must have not only a strong data security posture, but the regulatory process and documentation required in a comprehensive HIPAA security compliance program. Case studies involving recent or upcoming OCR enforcement action are listed below.

Incident #1: Lost Device

More than 500,000 laptops, smartphones and tablets are lost at airports each year. What happens if this incident occurs and an the organization cannot provide proof of compliance through documentation?

$1,975,220 HIPAA Fine

Incident #2: Computer Virus

Computer viruses, or malware, is the leading cause of data breaches for all industries. It is the easiest way for hackers to get into your network and steal your electronic protected patient information.

$150,000 HIPAA Fine

An institution was fined for failing to ensure that firewalls were in place with threat identification monitoring of inbound and outbound traffic.

Incident #3: Patient HIPAA Compliant

The most common type of HIPAA patient complaint is patient allegations of staff disclosing information. In 2014, there were more than 14,000 HIPAA patient complaints filed with OCR and, nearly one in four complaints resulted in corrective action.

“Indiana Court of Appeals upheld a $1.4 million verdict against a large pharmacy chain and one of its pharmacists who shared confidential medical information about a client that had once dated her husband”

Incident #4: Third Party Breach

Business associate breaches represent a very real risk for health care organizations mainly because they don’t have control or insight into their business associates security or policies. Business associates that store your patient data, like cloud based EHR or a billing vendor, can create breach scenarios that require action on the part of the covered entity. Even if the breach is caused by the business associate, the covered entity is responsible for :

Reporting the breach to the Department of Health and Human Services

Notifying the affected individuals by first class mail

Notifying the media (if more than 500 individuals are affected)

Provide information to affected individuals who have questions about the breach

In 2015, an EHR vendor had a breach involving more than 200 covered entities. The vendor is covering costs for each affected covered entity. However, if the business associate does not have the financial resources to cover costs associated with a covered entity’s notification costs, the covered entity is responsible for that financial burden.

Top Five Practical Cybersecurity Considerations, Guidelines and Recommendations

Health care providers will benefit greatly from adhering to the following five cybersecurity recommendations. It is important to get started right away as the cost of doing nothing could be enormous.

1. Assign a security and privacy officer and provide time for them to do the work your organization is legally required to do
   - » Perform a current self-assessment and target cybersecurity profile using the simple assessment tools developed by the Partnership and the NIST Framework for more granular details, as appropriate.
2. Take action where your organization is vulnerable
3. Develop, maintain and enforce organizational privacy policies and procedures.
4. Train personnel on legislation and organizational policies and procedures.
5. Review business associate agreements and their privacy policies.

THE PARTNERSHIP'S TASK FORCE RECOMMENDATIONS FOR ADDRESSING CYBERSECURITY IF:

YOU HAVE A $0-$500 BUDGET?

- One no-cost strategy is to implement a strong password policy that includes forced changes every 60-90 days. Another is to identify and train all staff (existing and new) on basic security and privacy procedures.
- Other low-cost strategies include installing and maintaining anti-virus software, encrypting hard drives and portable media along with encrypting all data during back-up procedures.

YOU HAVE A BUDGET OVER $500?

- Elevated strategies include developing comprehensive security policies with tracking of updates, enforcement and violations along with reviewing security policies of business associates and vendors.
- Hardware and software strategies include upgrading your router and firewall, creating isolated networks for protected information and implementing a consistent process of analyzing audit logs.
- Whether organizations have a budget of $50 or $5,000, all HIPAA related actions must be documented. A comprehensive HIPAA security compliance program, that includes current data security controls, is not only necessary to protect patient information but is required under HIPAA law.

ftware Advice, Austin, TX Data Breach Patient Survey 2015

PandaLabs Q3 2014 Quarterly Report http://www.pandasecurity.com/mediacenter/src/uploads/2014/11/QuarterlyReport-PandaLabs_Q3.pdf

Ponemon Insitute Research report, 2015 Cost of a data breach study: United States

Tex. H.B. 300, 82d Leg., R.S. (2011). http://www.legis.state.tx.us/tlodocs/82R/billtext/pdf/HB00300F.pdf#navpanes=0Trends.pdf

Department of Health & Human Services Press Release Stolen laptops lead to important HIPAA settlements http://www.hhs.gov/news/press/2014pres/04/20140422b.html

Software Advice, Austin, TX Data Breach Patient Survey 2015

Department of Health & Human Services Bulletin HIPAA Settlement Underscores the Vulnerability of Unpatched and Unsupported Software http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/acmhs/acmhsbulletin.pdf

Indy Star http://www.indystar.com/story news/2014/11/14/m-award-upheld-walgreen-pharmacist-shared-patientdata/19035783/

http://www.hipaajournal.com/2014-saw-25-increase-hipaa-breaches-201/

LEGAL SECTOR OVERVIEW

Business Characteristics

The Houston MSA employs over 25,000 employees in the legal services industry, up 2.5 percent over last year. Legal services is an expanding industry in Houston, with law firms handling an increasing amount of confidential work for their clients. This consists of approximately 20,000 employed in a variety of legal occupations, including nearly 12,000 attorneys. Also, the region has more than 3,500 legal services establishments and the Houston Bar Association, a nonprofit professional association of attorneys, is the fifth largest metropolitan bar association in the nation with nearly 11,500 members.

Trusted Third Parties

Law firms are seen as trusted third parties. In addition to providing single transaction legal services, many serve as ongoing outside counsel and trusted advisors. The legal industry must address cybersecurity in a dual manner. Legal professionals must take precaution in regards to both their own responsibility for regulated information as well as their client requirements.

And One-Stop Data Shops

Law firms are viewed by hackers as a one-stop shop for confidential information including identities, protected health information, merger and acquisition details, intellectual property, and trade secrets.

The Human Factor

Cybercriminals made a dramatic shift in the way they deploy malware in 2014, targeting law firms' greatest vulnerabilities, its people. While U.S. firms were spending $71 billion hardening technical defenses, attackers focused on the human factor. Social engineering and ransomware attacks increased 113 percent in 2014 compared to 2013. Attackers shifted to long-term phishing campaigns exhibiting the following characteristics:

- Focus – Identifying specific populations like technologists, data custodians, and professional service providers such as attorneys
- Familiarity – Cultivating or implying a relationship to build trust
- Patience – Not being in a hurry to deliver or activate malware
- Persistence – Continually sending emails with different exploits to targeted recipients until successfully deployed
- Diversity – Employ a variety of appeals to trust, hope, greed, fear, and curiosity recognizing that recipients have different emotional response/tolerance levels
- Delivery – Combine telephone, texting, instant messaging, social networking with email to improve email click rates

Making the right decision about suspicious email is the single most effective cybersecurity defense at our disposal

Each poor decision, each wrong click – and it only takes one – creates an opportunity for the cybercriminal to pounce.

10, Borderline 11

Borrowing a line from the Gone Fishing movie, on a scale of 1 to 10, the risks law firms are facing are an 11, according to a professor at George Washington Law School. Reinforcing this statement, 80 of the 100 biggest law firms in the U.S. have been hacked since 2011.

xas Workforce Commission

Occupational Employment and Wage Estimates (OES), Bureau of Labor Statistics, May 2012 Metropolitan Area.

"County Business Patterns", Census Bureau, 2011.

"2011 ILTA/InsideLegal Technology Purchasing Survey," InsideLegal.com. http://insidelegal.typepad.com/files/ILTAInsideLegalTechnologyPurchasingSurvey2011.pdf

"2011 ILTA/InsideLegal Technology Purchasing Survey," InsideLegal.com. http://insidelegal.typepad.com/files/ILTAInsideLegalTechnologyPurchasingSurvey2011.pdf

"ABA Commission on Ethics 20/20," American Bar Association. http://www.americanbar.org/groups/professional_responsibility/aba_commission_on_ethics_20_20.html

Ibid.

"Model Rules of Professional Conduct," American Bar Association. http://www.americanbar.org/groups/professional_responsibility/publications/ model_rules_of_professional_conduct/model_rules_of_professional_conduct_table_of_contents.html

Rule 1.1: Competence. "Model Rules of Professional Conduct," American Bar Association. http://www.americanbar.org/groups/professional_ responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence.html

Comment on Rule 1.1. "Model Rules of Professional Conduct," American Bar Association. http://www.americanbar.org/groups/professional_ responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence/comment_on_rule_1_1.html

All law firms, regardless of size are small businesses. Even the largest law firms consist of multiple practice groups made up of partners providing individualized client service. As firms increase in size, each attorney becomes more dependent on his or her colleagues to make good cybersecurity decisions.

Assume You Are a Target

Law firms are a cybercrime target because they are entrusted with client sensitive data including intellectual property, corporate transactions, mergers and acquisitions and lawsuit data that may include personal data. "It becomes a realization they may have a treasure trove of data outside of the primary organization that's being targeted. Cybercriminals now believe it's easier to go after a third party to gain access to an organization. Law firms as a secondary access point for criminal activity, due to the volume and sensitivity of data they deal with, are now viewed by their clients as both trusted partners and cybersecurity vulnerabilities.

Firms must recognize the need to take action, identifying the information assets that are targets. The data of most interest to cybercriminals is client data they have custody of, making it highly sensitive and requiring the strictest security controls. Allowing this data to be compromised while in a firm's possession may result in irreparable reputation loss. Clients now expect attention to cybersecurity from their law firms because their information and interests are at risk.

Assume You Will Be Successfully Attacked

Security experts maintain it's not a matter of "if" but "when" a firm will experience a cyberattack. Given the inevitability, it's also reasonable to assume the attack will be likely discovered only after the fact. Again, 80 of the largest law firms have been attacked since 2011.

Law Firms Must Bolster Defenses

Law firms must embrace the idea that they need to bolster their people, processes and technology defenses. Cybersecurity is an issue that simply cannot be ignored.

Ethical Obligations and Professional Conduct

The profession's ethical obligations and professional conduct rules provide governance guidelines. However, these guidelines alone are not sufficient to meet the firm's cybersecurity obligations. Federal and state laws, regulatory agency oversight, and, most importantly, client expectations require that law firms employ a cybersecurity framework based on industry standards and best practices. The framework provides structure as well as a roadmap through standards, guidelines and practices aimed at reducing and managing cybersecurity risk.

ABA Model Rules of Professional Conduct

Ethical rules are evolving to meet issues and requirements arising from new technology.

ABA Commission on Ethics 20/20

- Created in 2009 to review the ABA Model Rules of Professional Conduct "in the context of advances in technology and global legal practice developments."
- Released Resolution & Report 105A (Technology and Confidentiality) in May 2012.
- Resolution & Report 105A adopted, as revised, in August 2012 as discussed below.

The Competence Rule, MODEL CODE OF PROF'L CONDUCT 1.1

Rule 1.1 of the Model Code of Professional Conduct requires that a lawyer provide "competent representation to the client."

Comment 8 to that Rule directs that a lawyer should: "keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology,* engage in continuing study and education[,] and comply with all continuing legal education requirements."

*Amended upon adoption of Resolution & Report 105A

The Confidentiality Rule, MODEL CODE OF PROF'L CONDUCT 1.6(a)

Rule 1.6(a) of the Model Code of Professional Conduct directs that a lawyer "shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by [the next paragraph of Rule 1.6]."

New paragraph (c) in Rule 1.6: "[a] lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.*"

Amended Comment 18 provides guidance as to what constitutes "reasonable efforts" to prevent the revelation of a client's confidential information. Per amended Comment 18, factors considered in assessing reasonableness of efforts include, but are not limited to the following: "the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the [lawyer's] ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).*"

*Amended upon adoption of Resolution & Report 105A

The Rule on Responsibilities Regarding Nonlawyer Assistant, MODEL CODE OF PROF'L CONDUCT 5.3

Rule 5.3 of the Model Code of Professional Conduct requires attorneys, subject to some limitations, to "make reasonable efforts" to ensure that the conduct of nonlawyers retained by or associated with that lawyer is "compatible with the professional obligations of the lawyer."

Comment 3 to that Rule makes clear that the Rule applies to nonlawyers outside of a lawyer's firm who are engaged to assist on a particular matter, including, by way of example: use of a "document management company to create and maintain a database for complex litigation," the "sending [of] client documents to a third party for printing or scanning," and use of "an Internet-based service to store client information."

State Bar Opinions

Opinions of at least seventeen (17) state bars (including those of Arizona, Florida, New York, and Pennsylvania, which refer directly to Rules 1.1 and 1.6, above) have been issued concerning ethical permissibility of a lawyer's use of advanced technology such as cloud storage.

- So far, answer is a conditioned 'yes.'
- Lawyers and law firms are obligated to take competent and reasonable steps to assure that the confidential information in electronic form is not lost, destroyed, or disclosed through theft or inadvertence.
- New York State Bar Ethics Opinion 842: lawyers are required to stay abreast of technological advances to meet reasonable care requirements.
- Some state bar opinions discuss need for lawyers to ensure that they maintain unfettered access to client records in connection with their use of cloud storage.
- In general state bars are likely to follow the evolution of the ABA model rules (discussed above).

Personal Information Breach Notifications

Information security breach notification laws, such as TEX. BUS. & COM. CODE § 521.053(c) ("Any person who maintains computerized data that includes sensitive personal information not owned by the person shall notify the owner or license holder of the information of any breach of system security immediately after discovering the breach, if the sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person.") Also, such as those in Florida and Kentucky, require that entities holding information as service providers for an information owner or licensee to take action in the event of a security breach involving personal information. FLA. STAT. 501.171 ("In the event of a breach of security of a system maintained by a third-party agent, such third-party agent shall notify the covered entity of the breach of security as expeditiously as

"Model Rules of Professional Conduct," American Bar Association. http://www.americanbar.org/groups/professional_responsibility/publications/ model_rules_of_professional_conduct/model_rules_of_professional_conduct_table_of_contents.html

Rule 1.6: Confidentiality of Information. "Model Rules of Professional Conduct," American Bar Association. http://www.americanbar.org/groups/ professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information.html

Ibid.

Comment on Rule 1.6. "Model Rules of Professional Conduct," American Bar Association. http://www.americanbar.org/groups/professional_ responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/comment_on_rule_1_6.html * Amended upon adoption of Resolution & Report 105A

"Model Rules of Professional Conduct," American Bar Association. http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_5_3_responsibilities_regarding_nonlawyer_assistant.html

Rule 5.3: Responsibilities Regarding Nonlawyer Assistant. "Model Rules of Professional Conduct," American Bar Association. http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_5_3_responsibilities_regarding_nonlawyer_assistant.html

Comment on Rule 5.3. "Model Rules of Professional Conduct," American Bar Association. http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_5_3_responsibilities_regarding_nonlawyer_assistant/comment_on_rule_5_3.html

51" Ethics Opinion 842," New York State Bar Association, 10 September 2010. http://www.nysba.org/CustomTemplates/Content.aspx?id=1499

"ABA Releases cybersecurity Guide for Legal Professionals," North Dakota Supreme Court. 7 August 2013. http://www.ndcourts.gov/court/news/ cyber0813.htm

"Florida Information Protection Act of 2014 (FIPA)". The Florida Senate. http://www.flsenate.gov/Session/Bill/2014/1524/BillText/er/PDF

practicable, but no later than 10 days following the determination of the breach of security or reason to believe the breach occurred."); KY.14 R.S. H.B. 232 ("Any information holder that maintains computerized data that includes personally identifiable information that the information holder does not own shall notify the owner or licensee of the information of any breach of the security of the data as soon as reasonably practicable following discovery, if the personally identifiable information was, or is reasonably believed to have been, acquired by an unauthorized person."); see also Ariz. Rev. Stat. 44-7501(B) ("A person that maintains unencrypted computerized data that includes personal information that the person does not own shall notify and cooperate with the owner or the licensee of the information of any breach of the security of the system following discovery of the breach without unreasonable delay.")

These laws do not exclude lawyers or law firms from such requirements. Lawyers handling personal information should implement policies and procedures and should adopt their practices, as necessary, to prevent data breaches and to be ready to address them if they occur (including by notifying clients). As with other service providers, prudent practices include information security policies that are realistic and enforceable, control and oversight over vendors, and a security incident response plan.

Don't Reinvent the Wheel – Use a Cybersecurity Framework

The National Institute of Standards and Technology (NIST) has developed a cybersecurity framework consisting of five customizable functions. These are:

IDENTIFY

PROTECT

DETECT

RESPOND

RECOVER

Roles and Responsibilities

Larger firms may have a CISO or a director-level position responsible for security policy and implementation. This role may report to the CIO or COO. In larger firms, security is distinct from IT. Security has responsibility and exclusive administrative access for firewalls and security appliances, including Intrusion Prevention Appliances, Data Loss Prevention and web and e-mail security appliances. A typical security department in a large firm would consist of two to three persons, a director and one or two engineers with certifications including a security credential, such as the CISSP.

Small to medium-sized firms are unlikely to have security-specific positions. Medium-sized firms may have an engineer with firewall experience who typically assumes cybersecurity responsibilities. Small firms often rely on personal knowledge, colleagues and internet service providers for cybersecurity responsibilities.

"KY.14 R.S. H.B. 232". Kentucky Legislature. http://www.lrc.ky.gov/record/14rs/HB232.htm

"Ariz. Rev. Stat. 44-7501". Arizona State Legislature. http://www.azleg.gov/ars/44/07501.htm

"Business and Commerce Code". Texas Constitution and Statutes. http://www.statutes.legis.state.tx.us/Docs/BC/htm/BC.521.htm

THE PARTNERSHIP'S TASK FORCE RECOMMENDATIONS ON ADDRESSING CYBERSECURITY IF:

YOU HAVE A $0-$5,000 BUDGET?

Small firms typically do not have a separate budget item for security and may not have a budget item for IT either. On-premise security appliances, in the form of an all-in-one anti-virus, anti-spam firewall, typically are in the price range of $2,000-$5,000. Most small firms have their website hosted by an Internet Service Provider (ISP). E-mail is their key application and this is included in the hosting package. They tend to use free cloud services such as DropBox for client collaboration.

Medium-sized firms are likely to have on-premise IT servers and security appliances. Firms of this size are also candidates for co-location and managed hosting services provided by firms, such as Rackspace. Once they have performed the due diligence required, they are essentially outsourcing IT and security.

Some steps that small and medium sized firms can take include:

Participate in information sharing and industry forums to stay abreast of emerging threats. Join InfraGard, which has a Special Interest Group (SIG) for Legal Professionals.

Provide educational materials for customers, employers and board members. Execute anti-phishing and social engineering campaigns for your depositors and employees. Make positive pay and verification of wire transfers mandatory. Communicate risks and mitigating efforts to directors and key stakeholders.

Utilize resources available through the U.S. Secret Service Electronic Crimes Task Force and the FBI InfraGard to investigate a cybersecurity attack.

YOU HAVE A BUDGET OVER $500?

Large firms usually employ a hybrid solution, mixing outsourced and in-house security spending based on expertise and the focus of the firm's managing partner(s).

BANKING AND FINANCIAL SECTOR OVERVIEW

Business Characteristics

As of June 30, 2013, the Houston MSA's 110 Federal Deposit Insurance Corporation (FDIC)- insured institutions had local deposits of $208.033 billion. Commercial banks accounted for 99 institutions and $206.726 billion in deposits, while savings institutions numbered 11 with $1.307 billion in deposits. In 2013, the Houston MSA ranked 10th among U.S. MSAs in total deposits. That same year, 90,400 workers in the financial activities sector were employed in the Houston MSA. 14 of the nation's 30 largest FDIC-insured banks, as measured by domestic deposits, operate full-service branches or commercial loan offices in the Houston region. These 14 include the four largest banks in the nation. Also, according to the U.S. Census Bureau's 2012 County Business Patterns, the Houston MSA had 8,976 finance and insurance establishments with a total annual payroll of $8.129 billion.[43]

Due to the large sums of money at stake in the banking and financial industry, banks and other financial institutions in Houston face a tremendous risk of cyber-attacks and increased vulnerability. They must focus on the security of their own employees, as well as that of their customers.

According to a 2015 survey of global data breaches, financial services was the third hardest hit industry behind government and information technology. Out of all of the industries surveyed, financial services had the second highest number of confirmed data loss incidents, with the majority of these resulting in the loss of a large amount of data.[44]

Banks' vulnerabilities are impacted not only from their own networks but can be impacted by cyber-attacks against third-party vendors and even retailers. For example, it is estimated that banks and credit unions spent $200 million in the wake of the 2013 Target breach to reissue 21.8 million credit and debit cards.[45]

The nature and volume of customer transactions mandate that banks and other financial institutions have a higher level of requirements than many industries for information security, privacy and confidentiality. Additionally the legal liability in the event that a financial institution's customer fails to follow or implement the institution's security recommendations to provide protection against cybersecurity threats is an ongoing concern. If the customer is a company, Section 4A of the Uniform Commercial Code (UCC) suggests that it may be responsible for stolen funds if they had agreed to a security procedure with a financial institution, the institution followed the procedure, and the procedure was commercially reasonable. However, several court cases have indicated that the legal interpretation of this code is unclear as several banks have been deemed liable for lost funds.

Banks also face an evolving regulatory environment, which may include future provisions on cybersecurity. IT security regulations for financial institutions are defined by a complex series of legislation, Federal Financial Institutions Examination Council (FFIEC)[46] regulations and guidance, Federal Reserve-, OCC-, and FDIC-specific guidance, and FDIC financial institutions letters (FILs) along with state banking regulators. Each regulatory agency provides guidance on adhering to standards.

Federal regulators have also been actively working to tailor assessments and resources to meet the needs of financial institutions. In late spring of 2014, federal banking regulators began piloting a new cybersecurity assessment meant to help regulators gauge the level of cyber readiness of the nation's smaller banks. After the assessment was concluded, the FFIEC released "FFIEC Cybersecurity Assessment General Observations," which provides themes from the assessment and presents guidance on assessing firm's cybersecurity preparedness. The FFIEC also recommended that financial institutions participate in the Financial Services Information Sharing and Analysis Center (FS-ISAC), a non-profit organization that acts as a cyber and physical security information sharing forum. Additionally, since 2012, examinations by the Texas Department of Banking are placing a stronger emphasis on cybersecurity issues. These examinations are guided by an IT "Officer's Questionnaire," which presents specific areas for examination and provides regulatory references.[47]

[43] Houston Facts, Greater Houston Partnership, 2014, 17.

[44] tp://www.verizonenterprise.com/DBIR/2015/resources/

[45] "How Regulators are Shaking Up Small Bank Cyber Reviews," American Banker http://www.americanbanker.com/issues/179_124/how-regulators-are-shaking-up-small-bank-cyber-reviews-1068348-1.html

[46] tps://www.ffiec.gov/press/pr110314.htm

[47] Information Technology Officer's Questionnaire, FDIC, 2007, Texas Department of Banking, November 2012. http://www.banking.state.tx.us/ examproc/itexamquest.pdf

In June 2013, the FFIEC convened a working group to promote coordination across federal and state banking regulators on critical cybersecurity and infrastructure issues. As a result of this initiative, the FFIEC created a web page that acts as a repository of all current and future FFIEC materials related to cybersecurity. Additionally, the working group created the Cybersecurity Assessment Tool to assist financial institutions in identifying cyber risks and gauging levels of preparedness. Available online, this free tool incorporates standards from the information security examination handbook as well as the NIST Cybersecurity Framework. It seeks to provide a repeatable and measurable process for financial institutions to measure their cybersecurity preparedness over time.[48]

The largest contributor to regulations related to information security is section 501 (b) of the Gramm-Leach-Bliley Act. The largest and most detailed guidance on the interpretation of the GLBA can be found in the FFIEC's IT Examination Handbook.[49] A brief summary of key regulations and sources of guidance is included below.

Gramm-Leach-Bliley Act (GLBA) Section 501(b) [Federal Reserve Regulation H]

This provision charges federal financial regulatory agencies to establish regulations promoting electronic safeguards and is primarily enforced by the FDIC, the Office of the Comptroller of the Currency (OCC), state banking agencies and Federal Reserve IT auditors. FFIEC Information Security guidance can be found in the FFIEC's *IT Examination Handbook*.[50]

Federal Reserve Regulation P: Privacy of Consumer Financial Information

This pertains to protections and disclosure of private information. Information on compliance with Regulation P can be found in the *Compliance Guide to Small Entities*.[51]

FDIC Rules and Regulations Part 364-Standards for Safety and Soundness

This encompasses sections of the GLBA and the Fair Credit Reporting Act. It is the basis for which examination questionnaires are drafted.

Payment Card Industry Data Security Standard (PCI DSS)

Created by the PCI Security Standards Council (SSC) to protect cardholder data and prevent theft of personal information, these requirements are enforced by payment credit card brands (Visa, MasterCard, American Express and Discover) to all entities that transmit, store or process credit card information. For more information on PCI DSS, please consult the Retail section of this guide.

FFIEC Supplemental Guidance on Internet Banking Authentication

Issued in 2011, this is a supplement to the FFIEC guidance Authentication in an Internet Banking Environment, originally issued in October 2005. Its purpose is to reinforce the risk-management framework described in the original guidance and to update the FFIEC member agencies' supervisory expectations regarding customer authentication, layered security, and other controls in the increasingly hostile online environment.[52]

Uniform Commercial Code, UCC Article 4A (UCC 4A)

UCC 4A governs the rights of financial institutions and their corporate clients regarding funds transfers. Under UCC 4A, if a financial institution's corporate customer is the victim of a corporate account takeover, the company may be liable for funds stolen from its account if the corporate customer has agreed to a security procedure with the bank, the bank followed the security procedure and the procedure was "commercially reasonable". This premise has been put to the test in several court cases in the last few years, the verdicts in some of which have been in favor of financial institutions, while others have been in favor of corporate customers.

[48] Additional information on the FFIEC's cybersecurity and Critical Infrastructure Working Group can be found at https://www.ffiec.gov/cybersecurity.htm.

[49] ps://www.ffiec.gov/cyberassessmenttool.htm

[50] deral Financial Institutions Examination Council, FFIEC IT Examination Handbook http://ithandbook.ffiec.gov/it-booklets/information-secu¬rity.aspx . The Handbook is divided into booklets, several of which pertain here; e.g., E-Banking, Information Security and Outsourcing Technology Services.

[51] Ibid.

[52] Board of Governors of the Federal Reserve System, Compliance Guide to Small Entities, August 2, 2013 http://www.federalreserve.gov/bankinforeg/regpcg.htm

Payment Fraud Trends

Payment-related fraud remains a significant concern for both financial institutions (FIs) and non-FIs. According to a survey conducted by the Federal Reserve Bank of Dallas:

- For FIs, signature debit card is the payment instrument most vulnerable to attempted fraud and FI losses.
- Over half of FIs in the survey reported that signature debit card losses from fraud exceeded their investment in mitigation to prevent such fraud.[53]
- For non-FIs, checks continue to be the payment instrument most vulnerable to attempted fraud and losses.
- Corporate account takeovers can result in significant losses, but was not identified by respondents as a commonly occurring fraud scheme that affected a high percentage of respondents. However, those corporate account takeover cases that have been publicized typically involved large dollar amounts.
- Account takeovers are growing more common, as fraudsters go after smaller banks and businesses, where security is often weaker; many small business owners are not savvier about risks than the average consumer.
- Most FIs and non-FIs report total fraud losses that represent less than 0.5 percent of their annual revenues.
- A layered strategy using multiple mitigation methods and tools is required to detect and prevent fraud effectively.[54]

Because of the prevalence and associated cost of signature debit card fraud, financial institutions and others are now focused on alternatives to magnetic strip authentication technology to secure card payments. One of these alternatives is chip cards combined with Europay, MasterCard, and Visa (EMV) standards. Chip cards are plastic cards that contain a microchip that sends a dynamic, protected value unique to each transaction making fraud harder to commit. To encourage EMV adoption, Visa will institute a U.S. liability shift for domestic and cross-border counterfeit card-present POS transactions in the fall of 2015. With this liability shift, if a contact chip card is presented to a merchant that has not adopted, at minimum, contact chip terminals, liability for counterfeit fraud may shift to the merchant's acquirer, which will likely then be shifted to the merchant. For more information on EMV payments, please consult the Retail section of this guide.

Government Agencies

The government agencies and regulators with supervisory responsibility that might be involved in the event that a cyber-attack occurs against a financial institution include:

- Federal Reserve
- Federal Deposit Insurance Corporation (FDIC)
- Office of the Comptroller of Currency (OCC)
- Texas Department of Banking
- U.S. Secret Service
- Federal Bureau of Investigations (FBI)

[53] http://www.dallasfed.org/assets/documents/banking/firm/fi/fraud_survey.pdf

[54] As adapted from the 2014 Verizon Data Breach Investigations Report on Financial Services, "http://www.verizonenterprise.com/resources/factsheets/fs_2014-dbir-industries-financial-services-threat-landscape_en_xg.pdf"

Incident Classification Patterns

Four incident classification patterns cover 68 percent of security incidents in the financial industry. These include denial of service attacks (32 percent), crimeware (16 percent), web application attacks (14 percent), and card skimming (6 percent).

Denial of Service Attacks:

Denial of Service (DOS) attacks utilize botnets of computers to overwhelm systems and applications with malicious traffic. While DOS attacks rarely involve data theft, they can disrupt online banking or other platforms. The best practices in defending against DOS attacks include the following.

- Segregating key assets to keep critical systems on a separate network
- Testing anti-DOS services
- Having a plan to react to an attack and test it regularly

Web Application Attacks:

Web application attacks occur when attackers use stolen credentials or exploit vulnerabilities in web applications such as content management systems or e-commerce platforms. These attacks are difficult to defend against, but the following steps are recommended to decrease this vulnerability.

- Switch to a static content management system (CMS). Pre-generate pages to reduce the windows for exploits, instead of executing code to generate content for every request.
- Enforce lockout policies. Locking accounts after repeated failed log-in attempts will help to thwart brute-force attacks
- Monitor outbound connections.

Crimeware

Crimeware is the use of malware to compromise systems to gain access to confidential information or sensitive data. In the finance industry, 16 percent of all attacks were classified as crimeware in the 2015 DBIR, up from 4 percent in last year's report. In order to mitigate the risk of this threat, consider the following:

- Expect malware and monitor files or programs that have been introduced into your IT environment
- Monitor traffic
- Enable two-factor authentication
- Educate staff

Card Skimming

These attacks involve tampering with a card reading device to install a "skimmer" that automatically captures a customer's card data. The tactics and equipment used are often extremely sophisticated and can involve ATMs, gas pumps, cash registers and many other platforms. In order to mitigate the risk of this threat, consider the following:

- Use tamper-resistant terminals.
- Use tamper-evident controls.
- Encourage users to be vigilant.
- Inspect ATMs and card readers frequently.

Vendor Risk Management

Banks are impacted by cyber-threats against their own networks, as well as by threats against their vendors' networks. Cloud computing service providers, contract compliance providers, mobile application providers and many others may hold or have access to an institution's vital data, but may not share a similar level of security standards.

The following items are best practices or points for consideration when dealing with third-party risk management.

- Implement a vendor security management program that assesses the vendor, its risk classification and its policies and that manages any open issues.
- Consider that vendors may pose a risk to other avenues in addition to information security risk, such as business and legal risks.
- Consider whether your vendor utilizes other vendors to deliver services.

Roles and Responsibilities

Banks often outsource IT functions, including cybersecurity preparedness. If these functions are performed in-house, generally the CIO, network administrator and/or COO is responsible for implementing cybersecurity policies. Although it is rare for smaller institutions to have an employee dedicated to cybersecurity, the role appears to be growing more prevalent among mid-sized institutions.

Board members and bank officers should be educated on the state of cybersecurity and its impact to their organization. This will help avoid the risk of conflicting interests between cybersecurity policies and lending functions, which may pose a threat to the implementation and management of security policies.

Cybersecurity Considerations, Guidelines and Recommendations

Industry best practices include:

1. Conduct and/or update a risk assessment at least annually, including a section on corporate account takeover.
2. Provide cybersecurity awareness training for corporate customers. Emphasize that cybersecurity is not the sole responsibility of the financial institution nor of its customers, but a partnership between the two.
3. Use layered security for corporate accounts.
    - » Do not rely on tokens, passwords and "cookies" for authenticating customers; instead, use layered security, including software that flags unusual behavior (e.g., multiple transfers within minutes to new recipients).
    - » Require out-of-band verification for wire initiation and/or automated clearing house (ACH) origination services.
4. Offer positive pay or – even better – positive pay with payee verification, and encourage corporate customers to use it.
5. Recommend that corporate customers use a dedicated PC for conducting online banking with your institution.
6. Use fraud detection technology such as behavioral and fraud analytics.
7. Notify customers of suspicious activity (e.g., by offering them alerts).
8. If you provide merchant services, ensure that your corporate customers who are accepting credit cards (e.g., retailers) are adhering to the Payment Card Industry Data Security Standard (PCI DSS).
9. Consider utilizing a ".bank" domain.
10. Utilize the FFIEC Cybersecurity Assessment Tool to establish a baseline of cybersecurity practice and monitor preparedness over time.
11. Investigate and implement mobile wallets and tokenized payment methods (e.g., Apple Pay and Samsung Pay).

General guidelines similar to other industries include:

1. Whitelisting software programs
2. Frequent patching of operating systems and programs
3. Employee training
4. Limiting the number of employees with administrator privileges
5. Segmenting critical data for further protection from ex-filtration
6. Defining separation of duties and dual controls for processes impacting payments and receipts
7. Regularly testing the network using a simulated cyber-attack (penetration test)
8. Reconciling accounts and payments daily
9. Segregating accounts for different payment methods and types

THE PARTNERSHIP'S TASK FORCE RECOMMENDATIONS FOR ADDRESSING CYBERSECURITY IF:

YOU HAVE A $0-$500 BUDGET?

There are several low-cost and no-cost solutions to address some of the elements of cybersecurity.

Participate in information sharing and industry forums to stay abreast of emerging threats. Join InfraGard, which has a Special Interest Group (SIG) for the Banking and Finance industry that meets monthly.

Provide educational materials for customers, employers and board members. Execute anti-phishing and social engineering campaigns for your depositors and employees. Make positive pay and verification of wire transfers mandatory. Communicate risks and mitigating efforts to directors and key stakeholders.

Utilize resources available through the U.S. Secret Service Electronic Crimes Task Force and the FBI InfraGard to investigate a cybersecurity attack.

YOU HAVE A BUDGET OVER $500?

Implement the low- and no-cost strategies delineated above. This will provide a baseline for additional actions, depending on the institution's size.

All banking and financial institutions must comply to all regulations from the FFIEC and other governing bodies and must satisfy PCI standards, which requires expenses and resources well exceeding $500.

EDUCATION SYSTEM OVERVIEW

The Houston region has approximately 380,000 students in more than 60 degree-granting colleges, universities and technical schools. This includes 198,340 students enrolled in community colleges, 167,082 enrolled in universities and 12,010 enrolled in medical schools and colleges as of fall 2013.[55] Protecting and securing an educational institution's assets through cybersecurity is critical to maintaining the teaching, learning, research, scholarship and business aspects of higher education.

Higher Education

Higher education institutions depend on constant network reliability and access to all on and off site university data, systems, enterprise resource planning (ERP) (student registration, admissions, finance, financial aid, human resources, etc.), classrooms, e-learning and research data in digital format. These resources must always be fully functional, without interruption from attacks and breaches within and outside the campus environment. Additionally, most educational institutions receive federal financial support such as student loans and therefore, are governed by federal regulations on financial data security. The risks are high if attention to cybersecurity, best practices, awareness and training are not a high priority for such an institution.

Universities and colleges can suffer from the loss of data, stolen personally identifiable information, denial of services for student and faculty digital assets, loss of communications with vital constituencies, and loss of intellectual property and years of research that is crucially important to scientific discoveries. Research universities lead and power U.S. innovation, which translates to an economic benefit for the nation. Over time, this research yields new products that can improve the lives of millions of people, and results in millions of jobs created.

A cyber-attack can severely debilitate research projects, hindering the potential economic and societal benefits of those new discoveries. The cost associated with a breach can be high in both dollars and reputation for a university or college.

University leadership, CIOs and security officers should continuously plan and prioritize efforts to keep essential digital assets secure. However, an internal tension exists between the need to secure critical assets and the openness of a university's culture. Any security governance policy must balance these opposing forces, meeting the challenges of the rapidly changing cybersecurity needs while allowing for the maximum ability to collaborate and share in a de-centralized eco-system that is a hallmark of the university and college campus environments. There are additional decentralization issues associated with the overall technology trend of movement of data to the cloud. Establishing security governance in higher education and partnerships with a variety of agencies and departments is essential to the success of decision making pertaining to policy, protection, breaches and actions that need to be taken.

Developing a Security Program

As outlined in the general recommendations for all businesses, higher education institutions should begin with an honest assessment of the organization security profile, including an inventory of all critical systems, services and processes, as well as business priorities.

Once a baseline security profile is created, the next step is a standard risk assessment to understand the specific threats and potential impact of those threats. With this information the organization can begin to determine which risks can be reasonably mitigated, what steps to take and how long those steps will take to achieve the desired target security profile.

[55] Houston Facts, Greater Houston Partnership, 2014, 28.

Risk Areas

Higher education institutions have a variety of areas that may be targeted by attackers. These include research environments, web servers, student information systems and financial systems. These target areas are often vulnerable to attacks due to the diversity and inconsistent administration of these systems and configurations across departments. In fact, within the past year, several major academic institutions such as the University of Maryland, Indiana University and Butler University have experienced data breaches resulting in several hundred thousand records stolen.

In an effort to foster open communication, networks in many higher education institutions are often permissive in allowing traffic to and from the Internet as well as between systems on campus. This makes it easier for attackers to find vulnerable systems that would normally be protected by safeguards such as firewall blocks and intrusion prevention systems.

Federal Laws in Higher Education Compliance

To better understand the compliance landscape, the rules and regulations that cover protecting individual privacy and safeguarding information can be found at www. educause.edu/security/guide.[56] The following is a list of some of the important aspects of this landscape. Please note that compliance requirements associated with these items may only be applicable to certain types of data.

- Family Educational Rights and Privacy Act (FERPA)
- Financial Services Modernization Act of 1999 (Gramm-Leach-Bliley Act; GLB Act; GLBA Safeguards Rule
- Health Insurance Portability and Accountability Act (HIPAA) privacy and Security Rules
- Payment Card Industry Data Security Standard (PCI DSS)
- Human Subjects Research
- Fair and Accurate Credit Transactions Act of 2003 (FACT Act; FACTA) which amended the Fair Credit Reporting Act (FCRA), and amendments thereof, including Red Flags Rule (Identity Theft Prevention Program)
- Standard Non-Disclosure Agreement
- Higher Education Opportunities Act of 2008 (HEOA) Technology Mandates (Including: illegal peer-to-peer file sharing, emergency notification, and distance education student verification.)
- Standard Terms and Conditions (contractual terms) for Doing Business With a University

Working closely with university and college legal staffs, information technology departments, information security officers and administrators to better understand the access, movement and storage of digital assets in conjunction with the laws, rules and regulations has become a high priority, as the landscape is continuously evolving with cloud, e-learning and off-site campuses in the U.S., as well as abroad. Institutions must be aware of federal and state laws pertaining to the technology compromise of personal information, social security protections, breach and criminal intent. Federal and state agency briefings are great tools to help prepare for major incidents (breaches, attacks and weather related events) that require institutions to invoke crisis management procedures and disaster recovery plans. If your organization doesn't have crisis management procedures or a disaster recovery plan, it should create them.

[56] "Information Security Guide: Effective Practices and Solutions for Higher Education," www.educause.edu/security/guide

Government Agencies

Partnerships with government agencies and initiatives such as InfraGard can help inform institutions about the threats that they face as well as provide help in analyzing detected attacks.

Security Roles

Technology can only assist in backing up good practices and procedures. Developing and implementing a campus-wide security awareness program addressing identified risks is critical. This awareness program should include information on cybersecurity policies, expectations of employees, and necessary procedures to implement security strategies.

The role of Information Security management is related to the people, information, processes, compliance, standards, risk and governance structure within IT, as well as periodic reviews to make sure that the proper controls are in place. Effective Information Security management will lead to implementing the designs and architecture necessary for securing systems, developing capabilities for internal and external risk evaluation, ensuring that proper levels of privacy are maintained for individuals, and securing the institution's digital assets. CISOs should have a comprehensive understanding and expertise regarding institutional information work flow, the framework for implementing cost-effective compliance, the governing system that maintains security policies and the controls that are essential to reduce risk exposure.

Working in congruence with legal staff, the security office should define the scope of institutional security policies, identify and assess risks, select and implement controls, develop risk mitigation plans, and be pro-active. It is important to integrate information security into the institution's governance through the development of an information security governance framework and the reporting on internal controls. Emphasis should focus on internal and external threats, consistently and continuously planning, monitoring, reviewing and improving information security management.

Effective institutional governance of the information security function is critical to a successful program. An effective information security strategy for a higher education institution must take into account academic (including research), administrative (or business), clinical and residential environments. Even when focusing on critical processes and legal mandates, it is necessary to extend protective measures beyond the underlying IT systems and associated administrative staff. The governance of information security is based on well-defined organizational structure, roles and responsibilities, strategic planning, policy, compliance, risk management and measuring and reporting of performance.

It is important to have the organization's approach to the information security function reviewed periodically or when significant changes to security implementation occur. Such a review should include both assessing opportunities for improvement and the need for changes to the institution's approach to security. These reviews should be carried out by agencies independent of the area under review.[57]

[57] "Information Security Guide: Effective Practices and Solutions for Higher Education," www.educause.edu/security/guide

Protection of Personal and Institutional Data

Personally identifiable information (PII), data and media on which data resides and is accessed are key areas of concern. Data protection is especially paramount. Data comes from many places across the university –from admissions offices to research projects– and often includes PII, university-sensitive banking information and intellectual property (IP). Proper data ownership allows for an understanding of where data is located, who needs access to it and how it should be protected. Backing-up and disaster recovery of data is an essential part of the following guidelines and recommendations.

- Institutions should comply with Federal, State and local laws and regulations related to the protection of confidential or sensitive and personally identifiable information in conducting university business. Policies should cover students, employees, donors, alumni, prospects, applicants, research subjects and others. Confidential or sensitive information should be collected, secured, stored, transmitted and disposed of based on institutional elaboration of policy. This includes restrictions in distribution and accessibility as well as good internal control practices. Individuals should be informed of the applicable restrictions. Information can be properly secured by the use of such safeguards as secured file storage rooms, encryption and other technology tools. Also, the practice of disposal means that a systematic procedure should be in place for proper disposal of all hardware including: hard drives, portable media, CD/DVDs, etc.
- Confidential and/or sensitive data generated as part of the university business should be kept within the university network unless it is encrypted and fully secure in external clouds.
- Mobile tablets and smart phones used for conducting university business— including university e-mail—should be PIN protected. This protects the data should the device be lost or stolen. Remote wipe capabilities should also be set up and utilized on devices that have the option in the event that it is lost or stolen.
- Utilize encryption on all mobile vehicles: Thumb drives should be encrypted or password protected depending on the nature of the data.
  - » Provide secure network shares to store such data.
  - » E-mail is not a safe model of transport for confidential or sensitive information. If used, messages should be encrypted or password protected prior to sending.
  - » Laptops should be encrypted or in order to properly protect data.
  - » Keep strong password policies, requiring password changes every 60-90 days.
- A formal Incident Response Plan should document individuals who need to take action if a data breach occurs. All employees should be familiar with the plan and understand their roles.

Preparing for Security Events and Incidents

Security incidents are unavoidable. Preparations must be in place to quickly detect and respond to an incident. Whether it is a lost laptop or a malicious insider, organizations must be ready to respond. Having a plan available ahead of time is paramount to successfully managing the situation. To respond to an incident the organization must first be alerted to it. Alerting can come from any number of sources - from automated systems to reports from employees.

Network routers and firewalls generate large amounts of log data that report on more than just errors. They also can report on the number of connected devices and how much traffic those devices are generating. They report on the amount of traffic traversing the border and what applications are sending the data as well. This data can be correlated and patterns can be established, showing what is normal for different times during the day. Anomalies in this data should be flagged and investigated; many attacks do not affect operations and are otherwise unnoticed.

An organization's critical systems and servers also generate normal log data that can be used as a baseline for anomaly detection. A sudden increase in disk input/output (I/O) on a server may indicate a large file copy operation and a sequence of failed login attempts across various user ID's may indicate a brute-force attack attempt. Correlating these logs with those from the network devices can illuminate an attack that would otherwise be missed. Critical systems and servers should also undergo vulnerability assessments that are both regularly scheduled and occur when system components are changed or upgraded.

Public facing sites, such as a Domain Name System (DNS), e-mail and Web Servers, are often targets for remote attacks against an organization. These systems should be monitored and can be an early indicator of a larger attack that is coming.

As outlined above, organizations should create and maintain incident response plans for several scenarios. Many of these plans will have common elements, such as how to isolate systems on the network and preserve data needed for forensics. Another extremely important aspect is the communication plan. Understanding what to communicate and to whom is important to insure that the right information is delivered to the right people. Misinformation costs an organization time and reputation. Communication plans should also include an 'all clear', letting people know the system or service is back online and safe to use again.

All incidents should be reviewed shortly after resolution. An understanding of what happened and how it can be prevented in the future can help mitigate similar attacks in the future.

Throughout the incident management process, it is imperative to have clear roles defined for the different aspects of the response plans. People are better equipped to handle emergencies if they know their role and have had training and practice executing it.

Security and Process Recommendations from Educause[58] Include:

- Stewards/Stakeholders: Position the owners/stewards/stakeholders of the identified data set to take a leadership role in all decision making processes.
- Consultation: Consult with the appropriate Institutional Review Boards, data stewards, stakeholders, and subject matter experts. Research compliance, including HIPAA compliance, and consult with compliance offices and officers, including the General Counsel's Office, Information Security Office and Information Privacy Officer.
- Receiver agreement: Create a standard contract or service level agreement to be used with the receiver of the identified data.
- Due diligence: Due diligence should be conducted to determine the viability of the data de-identifier and the receiver. Consider such factors as reputation, transparency, references, financial (means and resources) and independent third-party assessments of safeguards and processes, particularly if you outsource the de-identification process.[59]
- Risk/benefit analysis: Identify and understand the risks and benefits of the service. Recognize that de-identification failures and re-identification efforts of receivers will potentially involve or at least reflect on the university. Compare costs of providing de-identification services, including costs to manage the receiver relationship, against the benefits of the intended use of the de-identified data.
- Lower risk candidates: When considering de-identification services, ideal candidates will be those that involve information with lower risk of re-identification or that are classified into a level that requires little to no protections. These are likely to represent the best opportunities for maximizing benefit while minimizing risk.
- Higher risk candidates: Data that is questionable as to whether or not it actually can be completely de-identified (such as network flow data, web traffic data, etc.) are higher risk candidates and require careful scrutiny and consideration, as well as stronger strategies for reducing the risk to acceptable levels. Data classified into levels that require medium to strong protections are higher risk candidates, as well. Also, small data sets are generally riskier, due to the increased chances that an individual could be identified.
- Centralized de-identification services: Consider leveraging internal services when looking for ways to provide data de-identification to university community members for university purposes (e.g., create a data lab or virtual server solution, with trained data de-identification experts). Develop an institutional standard for data anonymization.
- De-identifier safeguards: Insure the data handler doing the de-identification implements physical, technical and administrative safeguards appropriate to the risk. Areas to explore with the de-identifier include privileged user access, regulatory compliance, data location, data segregation, recovery or data availability, personnel practices, incident response plans and investigative or management support. You should scrutinize any gaps that are identified.
- Proportionality of analysis or evaluation: The depth of the above analysis and evaluation and the scope of risk mitigation measures and required assurances must be proportional to the risk involved, as determined by the sensitivity level of the information involved and the criticality or value to the universality of the usage of the de-identified data involved. Fewer steps and strategies for mitigating risk are necessary when the risk is low, whereas more are required when the risk is high.[60]

[58] http://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-initiative

[59] Ibid.

[60] Ibid.

Education Security Budgets and Resources

There are many resources regarding security and what is required to secure your environment. Many best practices for higher education exist on the web, through both for-profit and non-profit sources, that are of value to organizations with small budgets and limited resources. These resources assist with guiding institutions on essential security components that should be considered in securing the organization. It is important for institutions to partner, communicate, share security information and share information regarding up to date events and incidents with their peers.

The following sites are excellent resources to learn more about the best cybersecurity practices for educational institutions:

- Educause.edu[60]
- National Security Agency (NSA) – Reference: http://www.nsa.gov
- National Initiative for Cybersecurity Education (NICE) – Reference: http://csrc.nist.gov/nice
- Higher Education Information Security Council (HEISC)
- CERT[61]
- Information Systems Security Association[62]
- National Institute of Standards and Technology[63]
- Georgia Tech Information Security Center[64]

K-12 Cybersecurity Considerations

While dealing with a different user population, K-12 schools face many of the same challenges as Higher Education institutions and in many cases can leverage the same strategies as noted previously. Some specific considerations for K-12 schools:

Understand the privacy requirements for the specific user populations (minor students, employees, etc.) and implement appropriate technology controls

At the school district level as well as at individual school campuses, designate an information security officer responsible for overseeing a comprehensive information security program including employee awareness, business process review and technology controls. Encourage information sharing among the security officers throughout the District to leverage best practices and identify common threats. Classify critical data and prioritize resources to protect.

Educate school administrators as well as school board members as to information security concerns and strategies.

Develop incident response plans that include communications targeted to parents and other community stakeholders.

[61] http://www.cert.org/

[62] https://www.issa.org/

[63] http://csrc.nist.gov/csrc/professional.html

[64] https://www.gtisc.gatech.edu/

RETAIL OVERVIEW

Houston is home to half the Fortune 500 companies with operations in Texas. It also has 100,000 small businesses. With so many businesses within its economic core, cybersecurity has quickly become a topic of interest within the retail segment in our area. Many retailers make use of methods to take cardholder information, which makes credit card breaches a major concern. No matter the size, it has become more important to ensure this data is protected. With the help of new and future technologies, policies, and procedures, companies can have confidence that their information is secure.

Cyber-Attacks on the Retail Sector

In recent news, cybersecurity has been at the forefront for retail businesses. In the 2015 Data Breach Investigations Report, Verizon states that almost 90 percent of security incidents in the retail sector involved denial of service attacks, crimeware, or point-of-sale intrusions. Cyber criminals take advantage of being able to take large amounts of data and profit without ever stepping outside their home or office. Retail companies want to protect their investments, brand, data and the relationships they have with their customers. Measures are now being taken to ensure the security of data against cyber-attacks. The ease of using stolen credit card information has launched a change to increase overall security on the methods in which credit cards are used. For this reason, credit cards are now migrating to chip technology to prevent ongoing fraud. In 2014, dubbed “the year of the breach,” there were many reported breaches at U.S. retailers. Cyber criminals infiltrated systems containing secure information resulting in millions of credit card numbers, PII, and other sensitive data being stolen. Whenever evidence of a breach is found, the retailer must report it to the credit card brand.

Small retail businesses have as much risk as larger companies. When there is a card-present transaction, there are vulnerabilities that are often overlooked. They are susceptible to insecure remote access, weak or default passwords, lack of network segmentation, and malware deployed to capture card data. For card-not-present transactions, there are also vulnerabilities that are often exploited. Websites are attacked using SQL injections, cross-site scripting, malware, and could be made vulnerable by not using proper coding practices. Retailers can help mitigate risk by taking certain measures to provide safeguards against cyber-attacks like implementing network segmentation, changing default passwords, limiting remote access only when needed, and providing awareness training for employees. As a small retail business, having a complete security program can be overwhelming. There are many vendors that can provide services to insure proper security controls are implemented.

QUESTIONS TO ASK

Point-of-Sale Vendor

- What does your software automatically store?
- Does my network have a firewall installed to protect my POS from unauthorized access?
- Does the program have a broad set of invested stakeholders?
- Can you confirm that you do not use common or default passwords for my system?
- Have all unnecessary and insecure services been removed from my POS system?
- Do you deliver system updates through a secure method?

Software Vendor

- How often can I expect patches to software?
- How soon will I be notified of vulnerabilities?
- What are your software upgrade policies?
- Do you deliver system updates through a secure method?

Processing Vendor

- Are you PCI DSS compliant?

Global Point-of-Sale Counterfeit Liability Shift

EMV (Europay, Mastercard and Visa) is a standard set of specifications for smart card payments and acceptance devices. Smart (EMV) cards will replace the credit cards that are currently used. Effective October 1, 2015, card brands will institute a liability shift in the U.S. for domestic and cross-border counterfeit transactions. This will affect the merchant or the issuing financial institution that does not have the EMV technology. The policy encourages wider deployment of EMV cards and terminals to better protect all parties.

Visa has outlined three rules to determine where liability lies due to fraud and one exception:

- Rule 1: A traditional magnetic stripe is swiped at a magnetic strip terminal - If the purchase is a counterfeit transaction, the merchant is generally not liable, just like today.
- Rule 2: A chip card is used at a traditional magnetic strip-only terminal - If the purchase is a counterfeit transaction, the merchant generally holds liability, because the issuer has made the investment in chip technology to make transactions more secure while the merchant did not invest in upgrading to chip.
- Rule 3: A chip card is used at a chip-enabled terminal that has been activated by the merchant - if the purchase is a counterfeit transaction, the merchant is not liable, and the issuer will continue to bear the responsibility of counterfeit fraudulent activity. The good news is that when both parties adopt chip, overall in-store counterfeit fraud is virtually eliminated due to the security benefits of chip technology.
- Exception: Liability for automated fuel dispensers and ATM transactions shift in October 2017. The EMV liability shift does not apply to card-not-present transactions, lost and stolen fraud or Visa payWave transactions. In these cases, the liability remains subject to existing liability and chargeback rules.

Payment Card Industry Data Security Standard (PCI DSS)

The PCI DSS was created to protect cardholder data. The PCI DSS applies to all entities that store, process, and/or transmit credit card information. It covers technical and operational components included in or connected to these systems. If you accept or process payment cards, PCI DSS applies to you. PCI DSS applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers. PCI DSS also applies to all other entities that store, process, or transmit cardholder and/or sensitive authentication data. The validation requirements vary based on the amount of transactions per year.

PCI DATA SECURITY STANDARD – HIGH LEVEL OVERVIEW

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Level	Merchant Criteria	Validation Requirements
1	Merchants processing over 6 million Visa transactions annually (all channels) or Global merchants identified as Level 1 by any Visa region 2	Annual Report on Compliance ("ROC") by Qualified Security Assessor ("QSA") or Internal Auditor if signed by officer of the company The internal auditor is highly recommended to obtain the PCI SSC Internal Security Assessor ("ISA") certification Quarterly network scan by Approved Scan Vendor ("ASV") Attestation of Compliance Form
2	Merchants processing 1 million to 6 million Visa transactions annually (all channels)	Annual Self-Assessment Questionnaire ("SAQ") Quarterly network scan by ASV Attestation of Compliance Form
3	Merchants processing 20,000 to 1 million Visa e-commerce transactions annually	Annual SAQ Quarterly network scan by ASV Attestation of Compliance Form
4	Merchants processing less than 20,000 Visa e-commerce transactions annually and all other merchants processing up to 1 million Visa transactions annually	Annual SAQ recommended Quarterly network scan by ASV if applicable Compliance validation requirements set by merchant bank

If cardholder data is compromised, you can incur fines and the ability to accept payment cards. Immediate action should be taken if a merchant or service provider has experienced or suspected a security breach.

Steps for Compromised Entities		
1	Immediately contain and limit the exposure. Prevent further loss of data by conducting a thorough investigation of the suspected or confirmed compromise of information to preserve evidence and facilitate the investigation	Do not access or alter compromised systems (i.e., don't log on at all to the machine and change passwords, do not log in as ROOT). Do not turn the compromised machine off. Instead, isolate compromised systems from the network (i.e., unplug cable). Preserve logs and electronic evidence. Log all actions taken. If using a wireless network, change SSID on the AP and other machines that may be using this connection with the exception of any systems believed to be compromised. Be on "high" alert and monitor all systems with cardholder data.
2	Alert all necessary parties immediately.	Your internal information security group and incident response team. Your merchant bank. If you do not know the exact name and/or contact information for your merchant bank, notify Visa Fraud Investigations and Incident Management group immediately at (650) 432-2978. Your local office of the United States Secret Service.
3	Provide all compromised Visa, Interlink, and Plus accounts to your merchant bank within 10 business days. All potentially compromised accounts must be provided and transmitted as instructed by your merchant bank and Visa Fraud Investigations and Incident Management group. Visa will distribute the compromised Visa account numbers to Issuers and ensure the confidentiality of entity and non-public information.	
4	Within 3 business days of the reported compromise, provide an Incident Report document to your merchant bank. (See Appendix A for the report template.)	

Note: Visa, in consultation with your merchant bank, will determine whether or not an independent forensic investigation will be initiated on the compromised entity. For more information: http://usa.visa.com/dam/VCOM/download/merchants/cisp-what-to-do-if-compromised.pdf

Summary: **When an EMV card is used it helps identify that the owner of the card is the one using it. This will reduce the chances of a company from accepting any stolen cards.**

STEPS TO CONSIDER

Companies that have not upgraded their POS (point-of-sale) systems are encouraged to do so, due to the liability shift. The POS will need to have the ability to read the chip in credit cards.

Merchants should also review their POS systems.

- Physical Access: Verify no external devices are connected to the POS
- Reset any vendor supplied password
- Keep system and patches updated
- Segment the POS from other systems on the network

INSURANCE OVERVIEW

The Risk Management Perspective

In addition to insurance, there are a number of risk financing options available to organizations. These include: (1) funding losses from existing cash flows; (2) establishing funded or unfunded reserves to pay for loss; and, (3) establishing contractual (non-insurance) transfers for the cost of risk.

Insurance is the preferred risk financing mechanism for large and unpredictable loss events that are difficult or impossible to fund via normal cash flows or existing reserves. Cyber risk is often considered to meet these criteria because it is difficult to predict the frequency of loss, as well as the uncertain, unstable, and evolving legal environment that makes it difficult to predict the cost of legal liability arising from a data breach, or other cyber risk event.

The costs of such a data breach event may be significant. The 2015 Cost of Data Breach Study conducted by Ponemon Institute found that the average total consolidated total cost of a data breach was $3.8 million The 2014 netDiligence Cyber Claims Study found that the average claims payment for crisis services was $366,484, and the average claims payment for legal defense costs was $698,797

But again, insurance is not the only valid form of risk financing. Organizations should consider the purchase of Cyber Insurance, but the key point is that organizations should not default to retaining risk and funding the cost of loss from existing cash flows without giving due consideration to each alternative.

An Overview of Cyber Insurance

Cyber insurance, also frequently known as data security and privacy liability insurance or breach response insurance generally focuses on costs and expenses associated with a data breach event. With that said, cyber insurance is a new and rapidly evolving line of insurance coverage. Policies available in today's market are considerably different than policy forms available five years ago.

Furthermore, unlike General Liability or Workers' Compensation, there are no standard policy forms for cyber insurance. There are often significant coverage differences between policies offered by various carriers in the market.

Due to the rapidly changing nature of the coverage provided by such policies as well as the distinct differences between various policy forms, it is highly recommended that organizations work closely with a knowledgeable insurance broker. A knowledgeable insurance broker can assist the insured to understand the important differences between policies offered by various insurers that are easily overlooked.

Although there are distinct differences between various policies offered by different insurers, the vast majority of policies provide one or more of the following types of coverage:

1. Liability coverage: insurance coverage for the cost of defense and amounts that an insured entity is legally obligated to pay others as damages arising from a data breach or a failure of computer security. Liability coverage commonly includes the following components:
    - » Legal liability coverage for claims based on common law allegations. As an example, class action claims are often filed on behalf of consumers after large data breach events.
    - » Regulatory defense and penalties coverage for actions by governmental entities in their official or regulatory capacity. Data breach events may result in inquiries from state attorneys general or other governmental regulators. Health care entities may face regulatory inquires and fines from the U.S. Department of Health and Human Services (HHS) imposed under Privacy and Security Rules promulgated under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

- Payment Card Industry fines and expenses provides coverage for fines, expenses and damages that an insured may be contractually liable for under an agreement to accept payment cards.

2. Breach response and crisis management expenses: insurance coverage for the costs of notifying consumers and other expenses incurred to investigate and respond to a data breach event. Coverage for such loss generally includes the following components:
   - Notification costs: the cost to comply with laws requiring consumer notification after a data breach event.
   - Credit monitoring and identity restoration services: coverage for the cost of services to protect consumers impacted by a data breach event that is offered on a good will basis.
   - Computer forensic investigation expenses: coverage for the costs to retain computer experts to determine the existence and scope of a data breach event.
   - Legal assistance: coverage for the cost of retaining legal counsel to determine the entity's legal responsibilities after a breach event.
   - Crisis management and public relations: coverage to retain crisis management and public relations experts to assist with the response to a data breach event.
3. First party coverage: insurance for direct loss incurred by the organization arising from a failure of computer security. First party coverage options may include:
   - Cyber extortion: insurance for ransom or other costs to terminate a threat to release data that has been taken from an organization's computer system or a threat to damage/disable an organization's computer system.
   - Data recovery expenses: coverage for the costs to restore or recover electronic data that is corrupted or damages due to a failure or computer security.
   - Business interruption: coverage for loss of income and extra business expenses incurred as a direct result of a disruption to computer systems due to a failure of computer security.
   - Social engineering /theft of funds: coverage for a loss of funds arising from a fraudulent transfer from the organization's banking or other accounts. This may include losses arising from the voluntary parting of funds or property resulting from fraudulent social engineering techniques.

Finally, organizations considering cyber insurance should consider the expertise and assistance available from the insurer after a cyber-event occurs. Major insurers often handle thousands of incidents each year. Based on this experience, insurers may be able to offer important input into the proper handling and response to a cyber-event.

Putting It All Together

Because no set of risk controls can guarantee that an organization will not have a loss, the science of risk management prescribes that organizations should employ a combination of risk controls and risk financing techniques. Such techniques should not be intended to prevent a loss from occurring, but rather to minimize the organization's total cost of risk.

In the case of cyber risk, the entity should consider the purchase of cyber insurance as a part of an evaluation of various risk financing alternatives. The expenses to comply with data breach notification laws and respond to consumer's claims may be significant. Cyber insurance can provide important financial protection for the costs arising from a data breach event as well as other types of loss associated with computing systems. Furthermore, insurance buyers may find significant value in the expertise provided by insurance companies for these types of events.

"http://www.ibm.com/security/data-breach/

http://www.netdiligence.com/NetDiligence_2014CyberClaimsStudy.pdf

HUMAN RESOURCES OVERVIEW

Cyber-preparedness and assessing one's own risk levels can be a daunting task. The good news is there are many resources available to assist and the security field has become one of the most in-demand IT professions.

Cybersecurity is booming. Job postings have grown 74 percent in just six years—twice as quickly as other IT jobs. Opportunities in cybersecurity are growing faster than employers can fill them.

With the growing frequency of cyber attacks, the demand for information security analysts has never been higher. In fact, the Bureau of Labor Statistics (BLS) anticipates an employment growth of 22 percent from 2010 to 2020 for IT professionals involved in cybersecurity. But it takes a number of people to anticipate and design these technologies, and each position plays an important role in cybersecurity, earning a different salary range based on experience and skill.

FAST FACTS ABOUT THE CYBERSECURITY JOB MARKET

4 out of 5 Cybersecurity Jobs Require a Degree

Most positions in the cybersecurity sector require at least a bachelor's degree. A recent study found that 84 percent of cybersecurity positions require a bachelor's degree or higher.

Top Paying Cybersecurity Jobs

Based on median annual wages, compensation for cybersecurity professionals typically ranges from $70,000 to $118,000.

In-Demand Cybersecurity Job Skills

TOP 10 CYBERSECURITY JOB TITLES

1. Security Engineer
2. Security Analyst
3. CISO/ISO Director of Security
4. Web Penetration Tester
5. Security Auditor
6. Intrusion Analyst
7. Information Security Manager
8. Information Assurance Engineer
9. Senior IT Auditor
10. Security Administrator

IN-DEMAND SKILLS FOR CYBERSECURITY JOBS

Employers are seeking to hire employees with proficiency in:

- Firewalls
- Network Security
- LINUX
- UNIX
- CISA
- Cryptography
- Cisco
- Transmission Control Protocol/Internet Protocol (TCP/IP)
- System and Network Configuration
- Scanners

TOP 10 INFORMATION SECURITY CERTIFICATIONS:

#1 CompTIA SECURITY+

This is a basic entry-level certification for the curious security newcomer. It really introduces the candidate to many of the security concepts and touches on many basic topics to encourage the young generation to go for Information/IT security.

#2 CRISC

A great information risk certification that touches on various topics concerning information security and is definitely a natural progression for the information and business security practitioner to understand how to deal with risk and apply knowledge acquired in the realm of risk. This certification is mostly geared towards the risk practitioner and is mentioned and ranked here for its close relation to Information/IT security.

#3 CISM

This is a business-oriented certification focusing on management, design and risk. It is the information security professional's gateway to understanding the broad concepts of information assurance. It is geared towards security managers and business security architects, amongst others.

#4 CISSP

The CISSP is composed of 10 knowledge domains in various security topics ranging from physical security to management. It is more technically oriented and relates to some of the more complex topics like cryptography, network security, authentication and authorization. This certification is most appropriate for security analists.

#5 OSCE

This certification is considered one of the most complex certifications. In order to apply to the OCSE, the candidate has to go through two challenging ordeals. Due to the extreme challenge involved, this is considered a "cult certification" in many circles.

#6 LPT

Although this certificate has been around for sometime now, EC-council has restructured how it is attained. It now requires a practical exam in addition to achieving the CEH and ECSA. This is a must for the dedicated penetration tester.

#7 CREST ACE/ICE

Two very valuable certifications that are composed of various testing techniques such as long answers, multiple choice and a practical exam. ICE infrastructure and ACE application penetration testing are reserved for the novice penetration tester.

#8 GIAC Security Essentials

This inexpensive certification is a must-have for all security professionals. SANS courses are still the best, but somewhat expensive. This certification touches on many topics that range from basic to mid-range complexity. It is recommended for any security professional.

#9 CEH

Certified Ethical Hacker is a highly regarded certification in the industry. This is a qualification obtained by assessing the security of computer systems using penetration testing techniques. It is a great start for junior penetration testers.

#10 OSCP

This is an ethical hacking certification that teaches penetration testing methodologies and the use of the tools included with the BackTrack, now Kali Linux. The OSCP is a hands-on penetration testing certification requiring holders to successfully attack and penetrate various live machines in a safe lab environment. It is one of the few certifications that requires evidence of practical penetration testing skills.

A BRIGHT FUTURE AHEAD

Reflecting the diverse cyber threats in existence today, the field of cybersecurity is full of opportunities. In addition to the diversity of professions, careers in cybersecurity also range accross numerous industry sectors. Over the next five years, you should see more C-level positions being created for cyber professionals and the role of the CISO developing into an ever-increasing board room role.

CONCLUSION

Understanding that each business is unique in its size, technological requirements and vulnerabilities, the Partnership's Cybersecurity Task Force has sought to create a resource for all businesses to learn about the steps that they must take to secure their cyber environment. With ever-evolving technology, threats and resources, issues of cybersecurity can seem overwhelming for many small and medium-sized businesses. However, awareness, common sense and several no-cost or low-cost strategies can significantly protect a business against cyber-attacks

One final note: in the cybersecurity arena, lack of action is akin to a store owner leaving a retail store or warehouse unlocked. It is an invitation for theft, loss and hassle. Luck can only go so far, and eventually a negligent business owner will become a target. Likewise, leaving a business' online environment unlocked and workforce uninformed of the risks is an invitation for hackers, attackers and other bad actors to invade a business's cyber environment and wreak havoc on everything from personal information, proprietary information, to financial accounts and other such assets. The cost of recovery after such an attack can be devastating for a business – and potentially fatal. Prudent business owners will incorporate preventative cybersecurity strategies into the overall operations plans, along with other insurance and security prevention actions.

It is our hope that by collecting the information contained in this publication, and creating guidelines for businesses to follow to create and implement cybersecurity plans, we have made the process less daunting and easier for business-owners to address.

GREATER HOUSTON PARTNERSHIP NIST CYBERSECURITY PROTECTION ASSESSMENT

NIST Category			Negligible ⊗		Low ⊗	
Protect - Access Control	1	**Do you assess and monitor changes to user privileges?**	All user privileges monitored continuously, alerts investigated immediately.		All user privileges monitored continuously, reports analyzed weekly.	
Protect - Access Control	1	**Do you have an organization password strength policy?**			Multi factor authentication (something you know, like a password, plus something you have, like a badge or a finger print)	
Protect - Access Control	1	**Do individuals or third party organizations have access to your network?**			Over a virtual private network, restricted access vendor accounts, business associates agreement with vendor	
Protect - Awareness and Training	2	**Do you perform Security/Awareness training?**			Mandatory for all employees periodically with assessment of understanding. Third parties understand roles and responsibilities	
Protect - Data Security	3	**Do you manage assets?**			Formally managed through acquisition, update, transfer, removal and disposal	
Protect - Data Security	3	**Do your employees travel with laptops or other removable devices?**	No		Encrypted and no local data storage	
Protect - Data Security	3	**Do you have remote backup?**	No		Zero recovery encrypted	
Protect - Data Security	3	**Do you have wireless networks?**			No SSID (name of wireless network) broadcast, complex password, air defense system (blocks addition of wireless routers to network). User account and/or computer address access control. No public access	
Protect - Data Security	3	**Do you store personally identifiable information on your network?**			No	
Protect - Information Protection Processes and Procedures	4	**Do you have organizational security policies?**			Board approved, trained, monitored and enforced	
Protect - Information Protection Processes and Procedures	4	**Contracts with vendors**			Have copies of vendor security policies. Vendor has adequate cyber protection and insurance. Liability defined in contract	
Protect - Information Protection Processes and Procedures	4	**Do you perform personnel security and background checks?**			All employees have background checks. Physical access control to physical network and servers. Accounts disabled as soon as employee is no longer hired	
Protect - Information Protection Processes and Procedures	4	**How do you transmit personally identifiable information to third parties?**			Using mutual transport layer security with a BAA in place	
Protect - Information Protection Processes and Procedures	4	**Do you have a security function in your organization?**			Dedicated Security team. Reports to Senior leadership.	
Protect - Information Protection Processes and Procedures	4	**Do you have an incident response team and plan and recovery plan?**			24/7 response by multiple teams.	
Protect - Maintenance	5	**Do you perform logging and monitoring?**			Network and host base alerts responded in real time	
Protect - Protective Technology	6	**Do you have anti virus and malware software?**			All computers and servers, monitored	
Protect - Protective Technology	6	**Do you have Phishing protection?**			Monitored, no email/unrestricted internet browser access on network containing secure information	
Protect - Protective Technology	6	**Do you protect your network with a firewall?**			Monitored	

Count of risk level categories

Negligible: ____

x 0 = ____ (subtotal)

Low: ____

x 1 = ____ (subtotal)

Add subtotals to calculate RISK SCORE _____

In response to each of the questions, check the column that best describes your organization by entering an 'X' in the appropriate cell

	Moderate		High		Extreme	
	Only administrator accounts monitored. Reports analyzed at least monthly.		User privilege assessment scans performed and reviewed once in a while.		No	
	Only		Less than 8 characters, no special characters		No	
	Remote access tools to access secure network from outside		Physical access to hardware			
	For new hires only		None			
	Network, servers, devices and software documented		Purchased inventory only documented		No device or network management	
	Hard drive encryption		File encryption		Unencrypted	
	Encrypted		Unencrypted		Physically unsecured	
	Separate isolated guest wireless with no access to internal network		Published SSID, weak password			
	Yes, encrypted at rest and in transmission		Yes, unencrypted at rest and/or in transmission			
	On shelf		No			
	Liability defined in contract		No cybersecurity in contract			
	Background checks, but no physical access controls		No security or background checks			
	Over a virtual private network		Via secure/encrypted email to unvalidated recipient		Unencrypted, e.g. via email	
	Security functions shared within technical teams.		No Security function			
	Business hours response by some teams.		None			
	Network only / Host only (No real time alerting)		None			
	Computers with access to PHI only, not monitored		No			
	Yes, users trained		No			
	Commercial class router, complex password, ports open to the internet restricted to only those required for business applications		Residential class router, default password		No	
	Moderate:		High:		Extreme :	
	x 2 =		x 3 =		x 4 =	
	(subtotal)		(subtotal)		(subtotal)	

20 or less:	Good cybersecurity measures in place	**20-40:**	Perform risk/benefit analysis of enhanced security	**Over 40:**	High risk. At minimum, invest in basic protection

GLOSSARY

ABA
American Bar Association

APT
Advanced Persistent Threat

Audit logs
Security-relevant chronological record, set of records, or destination and source of records that provide documentary evidence of the sequence of activities that have affected at any time a specific operation, procedure, or event.

BAA
Business Associate Agreement

Card-present fraud
Card-present fraud occurs when a credit or debit card is used to make an unauthorized transaction in a face-to-face setting, such as a grocery store checkout lane. This type of fraud may involve the use of the actual stolen card or a fraudulent duplicated card made using a card number and magnetic stripe information.

Cardholder Data
At a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code. See Sensitive Authentication Data for additional data elements that may be transmitted or processed (but not stored) as part of a payment transaction.

CIO
Chief Information Officer

CISO
Chief Information Security Officer

CISSP
Certified Information Systems Security Professional

COO
Chief Operations Officer

CTISL
Cyber Technology and Information Security Laboratory

Data Anonymization
A process that removes or replaces identifying information from a record

Data lab/virtual server
A virtual server is hosted on physical hardware, called the host, and allows for multiple servers to run on that single host.

De-identified data
Data that has had the information that would allow for the identification of the source of the data deleted.

DHS
Department of Homeland Security

Drive-by download exploits of vulnerabilities
A drive-by download website serves as a host to exploits that target specific vulnerabilities in web browsers, and browser add-ons. Individuals and groups with malicious intent use various techniques in an effort to direct Internet users to these websites, which have been compromised. Users with vulnerable computers may have their computer become infected with malware simply by visiting such a website, even without attempting to download anything themselves.

e-PHI
Electronic protected health information

EMV
A set of specifications developed by Europay, MasterCard and Visa defining what is needed to ensure data exchange between payment chip cards and terminals.

EMV card
An EMV card, also called a chip-and-PIN card or smart card, contains a special computer chip to store card account data. Unlike magnetic-stripe cards, every time an EMV card is used for payment, the chip creates a unique transaction code that cannot be reused, thus stymying counterfeit card fraud. The initials EMV stand for Europay, MasterCard and Visa -- the three processing firms that in 2002 first agreed to the standards. EMV cards are widespread in Europe and other parts of the world, and are being rolled out in the U.S.

ERP
Enterprise resource planning

FACTA
Fair and Accurate Credit Transactions Act of 2003

FBI
Federal Bureau of Investigation

FCRA
Fair Credit Reporting Act

FDIC
Federal Deposit Insurance Corporation

FERPA
Family Educational Rights and Privacy Act

FFIEC
Federal Financial Institutions Examination Council

FIL
Financial Institution Letters

File Transfer Protocol (FTP) (p. 14, 52)
Standard protocol that is used to transfer files from one computer to another over a network, such as the Internet.

Firewalls
A firewall is a software or hardware-based network security system, which controls both the network's incoming and outgoing traffic. A firewall analyzes the data and determines whether it should be permitted through or not.

FRB
Federal Reserve Bank

GLBA
Gramm-Leach-Bliley Act

GTRI
Georgia Tech Research Institute

HEISC
Higher Education Information Security Council

HEOA
Higher Education Opportunities Act of 2008

Heuristics
Techniques used to solve a problem when the standard methods fail.

HIPAA
Health Insurance Portability and Accountability Act

Honey pots
A honey pot is a trap used to detect, deflect or counteract attacks. Generally, it is a computer that appears to be part of a network and contains information or resources that would be of value to an attacker, but, in reality, it is actually isolated and monitored.

Houston MSA
Houston-The Woodlands-Sugar Land Metropolitan Statistical Area (MSA) contains nine counties: Austin, Brazoria, Chambers, Fort Bend, Galveston, Harris, Liberty, Montgomery and Waller. The Houston MSA is 9,444 square miles and includes 124 incorporated communities.

ID
Identification

Intrusion Prevention Services (internal/external)
Intrusion prevention services are network security applications, which monitor the network's and system's activities in an effort to identify malicious activity, record information about this activity, attempt to block it and report it.

IP intellectual property
Intellectual property

IP Phones
IP Phones place and transmit telephone calls over the Internet instead of the traditional public switched telephone network (PSTN).

IPO
Initial public offering

IT
Information technology

Malware
Malicious software that is used to disrupt computer operations, gain access to private computer systems, or gather sensitive information.

NCSC
National Computer Security Center

NIST
National Institute of Standards and Technology

NSTISSC
National Security Telecommunications and Information Systems Security Committee

OCC
Office of the Comptroller of the Currency

Out-of-band verification
Out-of-band verification securely identifies a user who wants to access confidential information. Out-of-band signifies that the network used to obtain the information is distinct from the login gateway, which provides a more secure method of accessing data.

Patching
A repair job for a computer program in order to prevent the exploitation of data as a result of an attack.

PCI DSS
Payment Card Industry Data Security Standards

PDA
Personal digital assistant, which is a mobile device, or handheld computer, that functions as a personal information manager.

PHI
Protected Health Information

Phishing
Phishing is the act of attempting to acquire information such as usernames, passwords and non-public personal information (NPPI) by masquerading as a trusted entity in electronic communication. Phishing is typically carried out by e-mail spoofing or instant messaging. Spear phishing refers to highly targeted e-mails, often using detailed information about the recipient, obtained from social media.

PII
Personally Identifiable Information

Point-of-sale (POS)
The point-of-sale, or POS, is the location in a merchant's establishment at which the sale is consummated by payment for goods or services received. It is also where many retailers offer their store's credit card applications to consumers.

Ports
A port is a software construct that is specific for an application or process and serves as the endpoint for communications in a computer's operating system.

Re-identification
The process of combining data containing information that when correlated allows for the identification of the source of the data.

Recovery Point
The recovery point represents the point in time up until which data can be recovered. For example, if the recovery point is four hours, this means that work that is more recent than four hours old will likely be lost, but work that was completed previous to the four hour threshold will be backed-up successfully.

Recovery Time
The recovery time is the maximum tolerable length of time a computer, network or application can be unavailable after a disaster or attack.

RFP
Request for proposal

Sensitive Authentication Data
Security-related information (including but not limited to card validation codes/values, full track data from the magnetic stripe or equivalent on a chip, PINs, and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions.

Spoofing
A cyber-attack in which a person or program masquerades as another, falsifying data and gaining an advantage.

SSID
The name that identifies a wireless network.

Telnet
A program that runs on a computer, connecting the computer to a server on a network. This allows for remotely controlling Web servers.

TMC
Texas Medical Center

Tokenization
When applied to data security, Tokenization is the process of substituting a sensitive data element with a non-sensitive equivalent, referred to as a token, which has no extrinsic or exploitable meaning or value.

VLAN
A virtual local area network (VLAN) links computers as if they were connected to the same wire even though they may physically be located on different segments of the network.

VPN
Virtual private network

Waterholes
In a waterhole attack, a website that is frequently visited by an individual or a business is compromised in an effort to infect the user's network with malicious software.

White listing
A list of employees or applications that are provided a particular privilege, service, mobility, access or recognition. Only those on the list will be accepted, approved or recognized.

Underwritten by

BLUE LANCE

GREATER HOUSTON
PARTNERSHIP

Making Houston Greater.