United States Secret Service
North Texas Electronic Crimes Task Force

CYBERSECURITY FOR EXECUTIVES

INTRODUCTION:

In the era of continuous compromises, business executives are faced with the growing threat of malicious actors targeting and successfully penetrating their defenses at an alarming rate. Cyber-attacks are making the news daily, especially when they target major retailers, banks, and government agencies[i]. Increasingly, businesses are relying on the connectivity (always online) and productivity (customization/remote access) of their information systems. Businesses are challenged with trying to deliver services to an expanding consumer base while trying to balance security with the convenience of usability. Connectivity, productivity and convenience are critical in the 21st century, but if not implemented properly, they can have devastating effects to security. Striking a balance between security and usability is not easy and is a constantly evolving process.

Cybersecurity touches nearly every aspect of business. It affects a company's opportunities for expansion, customers, markets, and is vital to most strategic plans. The only place where accountability for all of those domains is held and where there is a clear line of distinction and authority is at the executive level. Before any executive can determine the best balance for their company, they must first understand the threat. Unfortunately cybersecurity concerns are not always communicated in a meaningful way. Information technology often gets lost in translation because it is provided in a technical dialect and not in a business context.

Over the past several years the United States Secret Service North Texas Electronic Crimes Task Force has investigated numerous intrusions involving large and mid-sized businesses. The purpose of this guide is to provide information to executives based off of actual investigations to help track the risk and adopt the essentials of Internet Security within your enterprise system.

To assist with finding the right balance between security and usability the following three (3) key points are what every executive should want to know about their company's information technology presence.

1. Securing your data against a cyber-attack
2. Taking a holistic and layered approach to cybersecurity
3. Having a cybersecurity response plan

1. SECURING YOUR DATA AGAINST A CYBER-ATTACK

In today's environment new trends in cybercrime are emerging all the time and the cost of these attacks are in the billions of dollars. Malicious actors utilize the internet for cyber embezzlement, fraud, theft of intellectual property, and theft of personal or financial data.

A. What data do you have that others may want?

A data breach is an incident where private and sensitive financial or personal identifiable information (PII) has been compromised by unauthorized access[ii]. Organizations must identify their most valuable assets and devote the proper resources and security posture to protect them. What would be most detrimental if taken from your system?

A wide range of sensitive information and PII such as names, dates of births, and social security numbers can be taken from your systems. It is important to understand that data stolen from your systems may impact more than just your company. Stolen information can be used for a wide range of crimes, from identity theft, to compromised banking sessions, cyber extortion, to the theft of intellectual property which could include anything from trade secrets to proprietary products. If credit card data is a target, compromised card holder data is costing businesses in the United States billions of dollars in fraudulent transactions, regulatory fines, and investigation and recovery fees each year.

- Is your data confidential - could unauthorized disclosure cause financial harm to your company?

- Is your data restricted - could unauthorized disclosure impede or undermine operations of your company causing a competitive disadvantage?

B. Where is the critical data located?

As part of your risk assessment, you must inventory your network, both physically and logically (flow of data) before an incident occurs and keep pace with any internal and external environmental changes. Identifying critical assets and understanding your complete security posture across your entire IT ecosystem will help to prevent or mitigate future attacks against your security system. Understanding where the endpoint systems are located and how data flows through them is critical.

- Think about your data in motion – information moving through your network, such as emails and web traffic.
- Think about your data at rest – information sitting on endpoint devices like workstations or databases, applications and web servers.
- Think about your data in use – information that might be stored on portable devices such as laptops, smart phones, usb drives or printers.

C. What will happen if someone takes your data?

Will the exposure to your company have financial, competitive, reputational, or regulatory implications? Does it involve violations of Health Insurance Portability and Accountability Act (HIPPA), Health Information Technology for Economic and Clinical Health (HITECH) Act, Gramm-Leach - Bailey Act (GLBA), SEC Cybersecurity Disclosure Guidance, Fair Credit Reporting Act (FCRA), Payment Card Industry Data Security Standard (PCI DSS) or even state data breach notification laws? All require companies or individuals that maintain unique PII of individuals to notify those individuals, and the state's attorney generals, if such information is lost, stolen or otherwise compromised. Although the country suffers from breach fatigue, the loss of business and damage to your name brand or reputation can be enormous. Companies can also suffer from investigation expenses, fines, penalties, regulator fees as well as civil litigation.

- Will you experience a market share loss and increased shareholder scrutiny?
- Will assets be damaged or will you have an interruption of service?

D. Where are you getting your threat intelligence to protect your data?

In order to properly assess your cyber-security posture, your company must learn as much as it can about the possible risk, threats and vulnerabilities that currently threaten your business. Awareness of the latest trends in cybercrime and how they can affect your business's computer network is extremely important. Analytics (the making of structured or unstructured data meaningful) from cyber threat intelligence sources is crucial to understanding the current cyber threat environment and protecting your system. The discipline of cyber threat intelligence focuses on providing actionable information on adversaries, their tactics and techniques in ways your businesses can understand.

In order to develop a strategic plan on protecting your assets you must first understand the landscape; an active defense or offense being the best defense is the best way to understand the current threat environment. If you are attacked, you don't want to start from ground zero trying to react to the incident with limited trace events; such as finding malware that resolves back to an Internet protocol address or domain. You need an established practice of gathering advanced actionable information (ahead of time) that can lead you in the right direction and help you mitigate the damage and assist any affected customers.

Although every company on the internet must have an acceptable level of risk, an investment in cybersecurity before a breach is incalculable, however the amount of money spent after a breach is immeasurable[iii].

- Advanced analytics can be formed in house, outsourced or gathered from government, commercial or open source providers.

- Organizations must ensure that their cybersecurity strategy is aligned with their overall business strategy. Cyber intelligence spending will be most productive when the amount of money allocated is based off of an articulable set of risks.

E. What are you doing to protect your data?

This is where you begin the discussion on securing your enterprise. This is also where the resources spent on the investment of hardware and software is often debated. The key to any secure environment is to regulate the traffic that enters and exits a network, to understand which traffic entering your network is "good" and which is malicious. Access controls are used to filter the information coming in and out of your network. Systems that comply with your set of rules have access and get authenticated. The ones that don't are denied access or not authenticated. This is where you can plan for the correlation and automation of logs and other controls like firewalls, intrusion prevention/detection systems (IDS/IPS), data loss prevention (DLP) systems and the management of your software development life cycle (SDLC). Monitoring and controlling access into networks is the most difficult and by far the most challenging aspect of cybersecurity today.

While companies are doing a better job learning how to strengthen their programs, there are literally thousands of products and companies that are in the business of selling solutions and services geared towards securing and backing up your network. Determining which of these is the best for you, or the most cost effective is a never ending challenge.

In most large businesses the C-Level security personnel have the difficult task of controlling access, tracking risk and influencing senior executives on information security business decisions. However, they are too often not included in overall business planning. In order to ensure that businesses security decisions don't get lost in the overall business process and are aligned with business goals, security personnel must do the following:

- Understand the direction of (what drives) the business.
- Understand where the organization is going. Are they expanding or contracting?
- Get ahead of and stay engaged with the business, its peers and the environment.
- Become enablers and understand the problems.
- Read and stay current on business reports and strategic plans[iv].

2. TAKING A HOLISTIC AND LAYERED APPROACH

While we understand that there is no solution available that offers total assurance to preventing a cyber–attack, having the right balance of people, policies and technology can help adopt a holistic and layered approach to your organization's security posture.

- **Technology:** Technology is such a fast and changing space that the more data we can capture from our systems and automate, the better off we will be in devoting critical time responding to an incident. Technology can be used to enforce policies, monitor and alert on violations, and to provide data protection. Technological solutions can also be utilized as countermeasures to address the risk of data loss, whether it is intentional or human error. Technology comes in all forms, such as virtualization, cloud base services, content delivery networks and even risk management cycles. What amount are you willing to spend on both hardware and software to protect your system?

- **Policy**: Policy fills the gap between technology and people. The policies you put in place to protect your system will help to regulate your employee's and consumer's actions related to such things as bring your own device (BYOD), remote access, and the acceptable levels of use of your system. According to Symantec: The goal of corporate security policies is to define the procedures, guidelines and practices for configuring and managing security in your environment.[v] By enforcing corporate policy, corporations can minimize their risks and show due diligence to their customers and shareholders. Will the policies you but in place effect connectivity, productivity or security?

- **People:** Whether employee, customer, vendor, or outsourcer, education around security awareness is critical to the security of your network. The end user has always been, and will continue to be, the weakest link for any company's security posture. End user security awareness will have a major impact in protecting corporate data as they are the ones on the front line. [vi] Provide operational security training for employees to guard against insider threats and human error and make it informative, interesting and current. Empower employees to use data responsibly and educate them about the common threats vulnerabilities and risk of becoming a victim online. Stay mindful that vendors connected to your network can create a direct bridge into your organizations system and although outsourcing is a way to save money, you must take into account the state of their security environment. Have you established a security awareness program?

3. HAVING A CYBER-SECURITY RESPONSE PLAN (What to do when things go wrong.)

Having a comprehensive plan in place to address an incident when it happens is critical to cybersecurity. Organizations should have an incident response plan in place that is aligned with individuals who are trained on the various threats that may occur. A good incident response plan is one that understands that access controls and incident response are dependent on each other and the integration of the two affects the rapid detection of a security incident.

As cyber incidents spread across the nation's financial and critical infrastructure, an effective response requires close coordination with multiple stakeholders affected by the incident. A well-defined and organized response to a cyber-incident requires a team effort. Getting the right people involved is essential to properly responding, coordinating, mitigating, and investigating your incident. Plan for a worst case scenario with a defined clear path of escalation that includes a standard operating procedure.

Identifying who should be contacted and getting the right people involved is key to any successful response. A company must identify a central point of contact or leadership team that not only has the responsibility, but also has the authority to act. The leadership role must be empowered to perform the day-to-day analysis of the situation and make key decisions. A central point of contact should be established and be at the highest level in executive management, or have the backing of executive management.

Do you have a response team as part of your response plan? Does it involve in-house legal counsel, human resources personnel, corporate security, IT security, technical professionals and someone from your communications group to coordinate messaging? The response team must not only act as liaison within its own company, but also must coordinate and communicate with law enforcement, third-party forensic responders, outside legal counsel, media, and various state notification procedures. Synchronizing an effective incident response sometimes involves bringing in third-party entities. A well-organized and practiced response plan will have pre-established contacts for law enforcement and any needed third-party technical and legal support.

Cybersecurity planning should be flexible, enabling the organization to change with the environment. A strategic investment in a comprehensive incident response plan requires that an organization identify and invest in cybersecurity practices that are aligned with today's types of threats.

Contact information:

Any questions regarding this document can be directed to the United States Secret Service North Texas Electronic Crimes Task Force at (972) 868-3200 or email us at Dallas.ECTF@usss.dhs.gov.

References and Resources:

[i] http://anniesearle.com/webservices/Documents/ResearchNotes/ASA_Research_Note_ImpactOfDataBreaches_January2014.pdf

[ii] https://www.schneier.com/blog/archives/2009/02/balancing_secur.html

[iii] http://internetidentity.com/blog/cybersecurity-advice-id-give-ceo/

[iv] http://www.youtube.com/watch?v=DXtb1NPH9m8-Hacking Senior Management -- with Brian Honan

[v] Homeland security Cybersecurity Questions for CEO

[vi] SANS Institute InfoSec Reading Room People, Process, and Technologies Impact on Information Data
http://www.sans.org/reading-room/whitepapers/analyst/review-mcafee-039-s-total-protection-data-34770
http://www.merriam-webster.com/dictionary/cybersecurity
http://journal.georgetown.edu/cyber-iv-feature-taking-control-of-our-cyber-future/
https://www.schneier.com/blog/archives/2013/01/people_process.html
http://www.scottandscottllp.com/main/business_impact_of_data_breach.aspx
https://www.thales-esecurity.com/blogs/2009/december/banks-challenge-to-balance-security-with-usability
http://www.fcc.gov/cyberplanner
http://usa.visa.com/download/merchants/uscc-cyber-security-guide-2012.pdf
https://msisac.cisecurity.org/resources/guides/documents/Getting%20Started%20Guide.pdf
http://www.alvarezandmarsal.com/cyber-security-corporate-blind-spot
http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime
http://www.listcrime.com