Chapter 8

Defend and Collaborate: Information Security Considerations for Every Business Organization

Jacob M. Schmitt

Abstract

This research publication investigates multiple aspects of information and cyber security as it relates to all sizes of business enterprises. Because everyone utilizes technology that connects to the internet, all businesses are exposed to cyber security risks. This paper reviews basic principles of cyber security management for business leaders by investigating the human user security challenges in IT systems, new techniques of active defense and the nuances of cyber security insurance policies. The publication continues by highlighting ways that governments, businesses, and industry associations can and do cooperate with much success. The importance of obtaining industry certifications for more efficient coordination of responses to cyber intrusions are also discussed. The author emphasizes the need to focus on the human security aspect of access control because it is, universally, the primary weakness of any businesses' IT infrastructure even after utilizing other standard defenses like modern IT infrastructure and cyber security insurance to protect against catastrophic losses.

Introduction

Businesses of every size handle sensitive information such as transaction receipts, customer data and sensitive information pertaining to their business's decisions. Almost every business also utilizes technology that increases their efficiency

which also exposes them to increasingly extensive and pervasive risks. A 2017 report estimated global damages from cybercrime at $600 billion or nearly 1% of global gross domestic product (Economic Impact of Cyber Crime, 2018, p. 3). A joint report between Cybersecurity Ventures and the Herjavec Group projected an increase to $6 trillion in annual economic losses by 2021 (Morgan, 2017, p. 3). If a company's leadership fails to manage these risks properly, they face catastrophic losses to sales, reputation and assets. Powerful tools that were once wielded solely by sophisticated government actors are now relatively easily available on the internet as a standalone software program or as a service by talented criminals, often for a small fee. As governments grapple with regulating rapidly changing technology, businesses must take the initiative to protect themselves, cooperate with others in government and their industries, and work closely with their information technology (IT) service providers. Even if a small business does not sell goods or services outside their home country, connecting to the internet in any manner exposes them to malign actors who often operate in spaces of weak governance that can evade even the strongest domestic laws and regulations. The challenges of bringing justice to these offenders and receiving settlement for damages without international cooperation cannot be overstated. This publication will highlight cyber security management principles that are applicable to any sized businesses, highlight opportunities for security collaboration between public and private entities while stressing the need to take the initiative in defending one's own business interests in this complex and rapidly changing threat environment. Having read this publication, the reader will have a better understanding of the complexities of managing cyber security in businesses and will learn industry best practices that apply to every organization.

Defending Business Information

The sophistication of Enterprise Risk Management and Security vary greatly between organizations. Large multi-national corporations often require a large team of professionals to manage legal compliance, travel security, physical security, executive protection and internal investigations. Sole proprietors and small businesses don't have the same needs or resources when it comes to cyber security, but they face the same threats. The actors who look to exploit weaknesses do not discriminate in their targets if they have a way to benefit from it. In 2016, several small police departments in the United States experienced a ransomware attack on their outdated computers. The departments were using older computers and had failed to receive critical security updates. Some departments refused to

pay the ransom while one department was attacked twice and paid both ransoms (Francescani, 2016, p. 1–2). If a computer connects to the internet, there is always a security risk; even for smaller organizations and local law enforcement.

The Human Factor

The weakest link in many IT systems tends to be the human end users who have legitimate access to a given network as part of their jobs. Recent cyber security research by the University of Maryland summarized, "Humans are often identified as the weakest link in cyber security, since any technical security solution is still prone to failures by human error" (Gratian, et al., 2017, p. 345). Many companies invest vast sums of money on network security infrastructure and the latest automated protective software services only to be undermined by weak passwords and compromised email files.

The University of Maryland research team advanced research in the human elements of cyber security by identifying cyber security behaviors based on demographic factors, personality traits, risk-taking preferences, and decision-making styles (Gratian et al., 2017, p. 345). Their research added to Egelman, Harbach and Peer's Security Behavior Intentions Scale which investigated IT system user's security awareness, password strengths, timeliness of security updates, and the physical security of their devices (Egelman, Harbach, Peer, 2017, p. 5257–5261). Gratian, et al. concluded that technical minded people, like engineers, had better security awareness and stronger passwords than their humanities student colleagues. Interestingly, the data showed that women, between the ages of 18 and 25 years old who are humanities students tended to have weaker passwords and were more susceptible to phishing attacks (Gratian et al., 2017, p. 351–352).

This type of research helps organizations focus their finite security budgets on the most vulnerable aspects of their security infrastructure. A small business that has limited funds to invest in security can focus on training employees in cyber security practices to minimize these risks in the most economical manner. Such research could invite criticism if the training response is perceived as discriminatory, so security managers should act with prudence. Another weakness of this study is that the sample population was relatively small and exclusively students and faculty at a university. Nonetheless, this type of research provides valuable lessons and insight on one of the biggest security challenges of business organizations. Businesses must also focus on safeguarding portable devices like tablets and cell phones that are used to access their networks remotely.

Following the United States' Federal Bureau of Investigation (FBI) guidelines for business travelers, companies should educate their employees on simple but effective security practices of not leaving their devices unattended, clearing internet browsers after use, avoiding use of non-company provided electronic devices for work, and not connecting storage devices to phones or laptops (Safety and Security, 2016). "The company should also utilize Virtual Private Networks (VPNs) to establish secure connections to the company's servers whenever their employees are out of the office. The next greatest threat to business infrastructure is through "social engineering" attacks where an outside entity attempts to access the network by compromising a legitimate system user (Goldschmidt, 2018, p. 1–3).

The technical details of designing and developing security infrastructure is beyond the scope of this publication but assume that a professional IT team manages the infrastructure and subscribes to the latest malware and malicious software detection services. With such robust security, malign actors target legitimate employees who have regular access to a targeted IT system as a normal part of their employment. This type of threat seeks to circumvent individual security practices and exploit any gaps that are discovered. In the hacker's "approach", sensitive information is either manually obtained, "socially engineered" by manipulating a targeted person with legitimate access, or "reverse socially engineered" where a criminal gets an unaware person to come in to contact with them and then asks for a "favor" to lessen suspicions.

Criminals also use technical means of capturing a password and trying it in different websites or using "key logging" malware that transmits everything that is typed on a keyboard (Krombholz, et al., 2014, p. 114–116). All users should be aware of a usual form of attack called "phishing" where malicious attachments are sent to unsuspecting users who subsequently open these detrimental email attachments. This attack begins by gathering information on the victim by analyzing the victim's social media accounts and searching public records. In a classic example of a phishing compromise, the attacker finds an important friend or family member on Facebook and then sends a fake email from that person to trick someone into opening an infected file. Skilled attackers have learned what types of emails have the best success rate and repeatedly use that template in future attacks. These prosperous emails are constructed with an urgent call to action involving a request for help or disguised as an important business invoice. When the victim opens the malicious email attachment, it infects the target computer subsequently giving the hackers access to the network. The virus autonomously sends files back to the attacker or allows for remote access to the targeted system.

Again, cyber security awareness is essential in protecting businesses against these types of threats. In 2018, you cannot allow your employees to edit your companies' financial reports while chatting on Facebook from a hotel business center's computer, having logged in with the password "123456"! The attacks are obvious in hindsight, but it takes proactive training to help employees think about their actions on the company's IT system and recognize suspicious emails. Showing examples of other attacks and hacking methods helps to inoculate employees against this form of attack. After employing a capable and professionally managed IT infrastructure, strengthening employees against pervasive social engineering, some companies are taking an even more proactive approach to their information security management.

Active Defense

As cyber security attacks increase in number and sophistication, businesses are looking for ways to be more proactive in their responses. The idea of private entities "hacking back" to defend themselves raises numerous legal and ethical questions but principles of "active defense" have increased in popularity recently among IT infrastructure managers. The SANS Institute defines passive cyber security (PCD) as "systems added to the architecture to provide consistent protection against or insight into threats without constant human interaction" where an entity employs "firewalls, anti-malware systems, intrusion prevention systems, anti-virus, intrusion detection systems, and similar traditional security systems" that don't require constant IT system staff interaction (Lee, 2015, p. 8).

In contrast, Active Cyber Defense (ACD) is characterized by system responses that engage with the attacker once the traditional forms of cyber security have been breached. The SANS Institute explains this difference as "the process of analysts monitoring for, responding to, learning from, and applying their knowledge to threats internal to the network" (Lee, 2015, p. 10). Active defense calls for an analysis of the attack to understand the threat actor, attack vector, vehicle and malicious tools used to deliver the attack. An IT team using basic ACD principles will review the event, analyze system logs to disable accounts and update firewall criteria as each threat is identified (Overill, 2003, p. 163). A more dynamic ACD technique involves using a "honey trap" to draw a threat into an isolated "sandbox" where the threat can be observed and studied (Overill, 2003, p. 163).

The most aggressive and controversial forms of ACD call for "mount(ing) a Denial of Service (DoS) reprisal attack against the presumed source" or

"launch(ing) a retaliatory malicious software strike" (Overill, 2003, p. 164). The latter two types of responses are what most people think of when they hear the term "Active Defense" but business organizations are usually restrained by legal and moral operations against conducting such "hack backs". In any type of response, business leaders must consider numerous aspects of their responses including "(their) authority, third party immunity, necessity, proportionality, human involvement, and civil liberties" similar to the military's principles on the use of force (Denning, 2014, p. 111–112). Aggressive ACD could violate the Computer Fraud and Abuse Act (CFAA) of 1986 in the United States. The CFAA explicitly prohibits "knowingly cause(ing) the transmission of a program, information, code, or command… (that) intentionally causes damage and loss" ("18", 1986, p. 1030).

Becoming frustrated with these restrictions, private businesses in the United States encouraged their government representatives to enact legislature due to the challenges of these rapidly changing threats. In October 2017, the Active Cyber Defense Act (ACDA) was brought to Congress for consideration. This recognized updated ACD principles and would allow businesses to "not only identify the attackers, but even destroy information originally stolen from their network" (Kulik, 2018, p. 1–2). The bill has not been passed at the time of this writing, but many scholars and legal experts are concerned at the precedent it would set. Some argue that it would weaken law enforcement's ability to prosecute some entities for cyber intrusions citing dubious claims of self-defense. Other criticisms include the inability to precisely attribute an attack to one person or entity and varied skills among IT staff to carry out these aggressive counter-attacks skillfully without proper training (Kulik, 2018, p. 2).

Proponents of the bill say that the intent of the bill is to gather information to share with security researchers and law enforcement. Others argue these aggressive tools are necessary to counter emerging threats, especially when private organizations now face highly sophisticated attacks from foreign actors backed by nation-state level funding. This also begs the question: how does a business navigate the legal and moral complexities of defending against a foreign adversary that could be backed by another government? This is an ongoing challenge that has yet to be solved or even tested in international courts. To protect against these outsized risks, companies are now turning to sophisticated and specially designed insurance products as part of their comprehensive security policies.

Cybersecurity Insurance

While businesses continue to experience increasingly numerous and sophisticated cyber intrusions, Enterprise Risk Managers seek ways to reduce catastrophic economic losses from these events. Having employed talented IT personnel, invested in the latest secure infrastructure, and invested in training and awareness for their staff, business leaders still require additional safeguards to overcome crises. Insurance companies have responded by developing new insurance vehicles to transfer risk of cyber intrusions and data losses. The United States Department of Homeland Security (DHS) recognizes the benefits of these emerging products which are designed to "mitigate losses from a variety of cyber incidents, including data breaches, business interruption, and network damage" (Cybersecurity Insurance, 2016, p. 1). The DHS explains the benefits of Cybersecurity Insurance, "(1) promoting the adoption of preventative measures in return for more coverage; and (2) encouraging the implementation of best practices by basing premiums on an insured's level of self-protection" (p. 2). When a business purchases Cyber Liability Insurance Coverage known as "CLIC", they generally receive assistance with investigation of a malicious intrusion, compensation for business losses, privacy notification aid, and legal support against lawsuits and extortion (Lindros, Tittel, 2016, p. 2).

Research by Lloyds of London, one of the world's largest insurance providers, indicate that "92% of businesses experienced a data breach in the last 5 years" but only "73% of business leaders have limited knowledge of cyber insurance" (Cyber Risk, 2016, p. 7) Insurance industry experts recommend that companies use insurance brokers to obtain these policies because they are complex and available coverage varies significantly between insurance providers and policies. Secondary benefits of obtaining CLIC insurance policies is that the underwriters require a comprehensive audit and risk assessment of the policies' information security infrastructure and security protocols (Closing the Gap 2017, p. 32–35). Improvements are frequently required before a cyber security insurance policy is developed while companies benefit from these recommendations. The underwriters assess not only the current state of the system but also make predictions of future security needs while working with all stakeholders. These products should be considered when taking a holistic view of any companies' information security plan.

These new policies are frequently criticized due to their costs but the DHS is optimistic that they will become more affordable as they develop and more entities start using them. Another concern of Cybersecurity Insurance

is that companies will forgo spending in other areas of their information security plan and narrowly rely on their expensive insurance policies should a cyber intrusion or data loss occur. After all, we are paying for this expensive protection, why not use it? The moral hazard of this mindset is another downside of cybersecurity insurance. Critics warn that companies will either cut security spending in other areas to pay for insurance or will rely too much on their policy and act carelessly with customer's data because they are covered either way. Callous attitudes towards information security could become more common as insurance policies become more affordable. Business leaders will always look to minimize costs, especially on their security, because it does not add value to their profits; security is often viewed as an inconvenient expense. Companies can better manage emerging risks with new insurance policies but need to ensure they practice due diligence in obtaining policies so that they receive this essential coverage.

Cyber Security Collaboration

To confront an already extensive and growing risk of cyber intrusions, business leaders will have to work with resources outside of their immediate organizations. Using government resources, networking with other organizations in their industries and utilizing experts in information security is vital to combatting these rapidly changing threats.

Public-Private Cooperation

Government organizations in Europe and the United States have been established to assist private enterprises in protecting their information systems and data. The European Cyber Security Organization (ECSO), enacted by the European Commission in July 2016, aspires to "foster cooperation between public and private actors at the (initial) stages of…(the) research and innovation process… (and) allow people in Europe to access innovative and trustworthy European solutions" (About the cPPP, 2018). Through this organization, the European Union is investing €450 billion euros in their "Horizon 2020" initiative to expand European produced security solutions. Large European companies like Ericsson, F-Secure Corporation, NXP Semiconductors B.V., and many others, recently established working groups with European Union/Commission representatives. These working groups are divided into areas of expertise that work on challenges

in training, standardization, certification, research, etc. Recent accomplishments of the ECSO include supporting European Commission legislation on the Cyber Security Act, Industrial Cybersecurity Policy and establishing several Cybersecurity Competence Centers throughout Europe (ECSO Public Session, 2018). In the United States, the Department of Homeland Security is the main governmental organization tasked with defending against cyber security threats and performing post-incident analysis for governmental and non-governmental entities (Information Sharing, 2018). In compliance with the Cybersecurity Act of 2015, the Department of Homeland Security administers the Automated Information Sharing (AIS) system that "enables the exchange of cyber threat indicators between the Federal Government and the private sector at machine speed" (Automated Indicator Sharing, 2015, p. 1). Businesses can enroll in a program that automatically shares anonymized threat information with DHS while simultaneously receiving updates and information on emerging threats sourced through other businesses in the program. This system emphasizes speed and errs on the side of sending more information than less so that any potential threat can be reviewed (Automated Indicator Sharing, 2015, p. 2).

Another resource in the United States is the InfraGard public-private partnership between the Federal Bureau of Investigation (FBI) and "business executives, entrepreneurs, military and government officials, computer professionals, academia and state and local law enforcement; each dedicated to contributing industry specific insight and advancing national security" (InfraGard, 2003, p. 1). InfraGard gives focused assistance on critical infrastructure industries, maintains 82 chapters throughout the United States with regular information sharing events, publishes FBI news feeds, and boasts 400+ members from Fortune 500 companies (Partnership for Protection, 2003, p. 1). Considering the initial successes of European and American public-private collaborations, the model of closely coordinating government and private enterprise resources to combat cyber security threats should be expanded and encouraged by other countries.

External Resources

Sizeable government resources in intelligence and law enforcement are helpful to domestic enterprises but are limited by slow international coordination between governments and gaps in governance. Private enterprises are less constrained because they can react quickly and share information with international peers in their industry. Numerous innovations in the information technology space are created by private enterprises and organizations. International associations and

certifying organizations are great resources for businesses as well. Rapid sharing of information and standardized training allows IT professionals from different regions to work closer together using common language. One of the most recognized security certifications is the Certified Information Systems Security Professional (CISSP) issued by (IC)2 after demonstrating extensive knowledge and passing a threshold of work experience (Cybersecurity Certifications, 2018). The International Association of Privacy Professionals (IAPP) offers a Certified Information Privacy Professional (CIPP) certification to formalize their education in information privacy practices (International Association of Privacy Professionals, 2018). Both organizations offer numerous specialty certifications along with the widely respected Global Information Assurance Certifications (GIAC) that are board certified through the SANS Institute (Certifications, 2018). Companies should encourage their security staff in obtaining these certifications and to be active in their industries associations to continue learning and keep pace with the brisk speed of security threats.

Conclusion

When reviewing a business's cyber security policies, all stakeholders should focus on the human factors which constitute the biggest weaknesses in their systems. Making employees aware of best practices in cyber security is not only a cost-effective way of combatting cyber threats but will benefit employees in their personal cyber lives too. Everyone benefits from good cyber hygiene! After focusing on the greatest weakness in their systems, managers should focus on maintaining the best infrastructure that their budgets allow using active defense, automated threat detection services and well-trained staff members. A comprehensive security policy should also have a foundation of cyber liability insurance to protect against catastrophic loses. It is important for businesses and organizations to defend themselves first in the current environment of quickly changing measures and counter measures. Once sufficient local resources are established, business security leaders should seek out assistance from their respective industry associations and mean of cooperating with government entities who can offer unique support in responding to international actors and help investigate complex intrusions. Unfortunately, government tends to move slower than the threats in terms of cybersecurity laws and reactions to cyber security intrusions from abroad because they must consider wider international relations implications. To win in cyber security, leaders must proactively defend their organizations and collaborate as much as possible.