DECISION SCIENCES INSTITUTE

Cybersecurity and e-commerce risks: A model framework for small businesses

Mayur S. Desai

Texas Southern University

Email: desaims@tsu.edu

Kamala Raghavan

Texas Southern University

Email: raghavank@tsu.edu

ABSTRACT

Small businesses are becoming painfully aware that their small size does not provide them immunity from the risk of a cyber-attack. This paper discusses the SEC disclosure guidance for registrants that can provide a model framework for small businesses and offers steps to strengthen cybersecurity. It reviews the tools available currently on website security to help organizations protect critical data and build trust with customers such as Secure Sockets Layer (SSL) encryption, the need for data encryption offered by SSL, and additional measures such as authentication of website legitimacy and trust building with one's customer base.

KEYWORDS: Cybersecurity, Cyber-attack, (SSL) encryption, Cloud Computing

INTRODUCTION

Most small businesses are finding that a vital factor for success in e-commerce is to gain the online customers' trust in the security of their sensitive data. Customers are justifiably concerned about identity theft, and are reluctant to provide information such as their credit card and social security numbers, passwords, health details, and other confidential data. Many times this sensitive information is intercepted in-transit, or the destination website is operated by fraudsters with malicious intent. When businesses cannot provide customers assurance of their data being protected almost 21% of users abandoned their online purchase transactions, according to an AICPA online survey (Vien, 2015). Some customers make smaller than intended purchases for fear that the transaction will be compromised. Such consumer fears are documented in the study “11th Annual Online Fraud Report” which estimates $3.3 billion in fraud losses to U.S. and Canadian online retailers in 2009. However, online businesses can realize substantial benefit and increase potential incremental business revenue streams by taking steps to alleviate customer fears such as use of technology to protect sensitive customer data, authenticate their websites, and build consumer trust. Since consumers have the ability to shop at a wide range of trusted e-commerce sites, they can and will make the best choice that protects their private information.

Small businesses are becoming painfully aware that their small size does not provide them immunity from the risk of a cyber-attack. Today's highly sophisticated hackers can and will attack any target they choose. While most small businesses understand the need for cybersecurity, many still have not taken sufficient measures to protect themselves against hackers. A survey (NCSA, 2012) by the National Cyber Security Alliance (NCSA) found that 71% of security breaches target small businesses, about 50% of small businesses have suffered from cyber-attacks. The credit data provider, Experian reports (PwC, 2015) that 60% of small businesses go out of business 6 months after suffering a security breach. The Department of Commerce’s National Institute of Standards and Technology study also found a sharp increase in hackers and adversaries targeting small businesses in the past 2 years. Small businesses may be more attractive to hackers because they do not take the time to develop a contingency plan or response plan to cyber-attacks, and do not have the resources to recover from an incident when it happens.

According to Symantec's 2014 Internet Threat Report, 30 percent of all cyber-attacks last year targeted small businesses. A cybersecurity incident could shut an entire network for many days until the problem is researched and fixed. A small business may not be able to withstand the loss of income, or have insurance that helps to defray those costs or any liabilities that might occur as a result of the breach. A highly public breach could also damage the business's brand and lead to long-term loss of income (Home Depot, Target.). NCSA's research (NCSA survey, 2015) identified 3 major reasons hackers target small businesses: They are not well equipped to handle an attack due to lack of resources; their partnerships with larger businesses provide back door access to a hacker's true targets; and they do not guard the information that hackers desire such as credit card credentials, intellectual property, personal information, etc., effectively.

Problem, Significance and Purpose

Small businesses with e-commerce operations are increasingly using cloud services for expense savings, but they do not always ensure that the services use strong online security measures. This combination of cloud services and lack of strong online security provides the hacker the opportunity to easily access reams of sensitive data. More businesses are beginning to establish systems that monitor and alert when the probability of a particular scenario increases, setting up cross- functional crisis management teams, and identifying processes to quickly react to risks when they occur. A culture of risk awareness throughout the business is an essential platform for effective risk management. This paper discusses the SEC disclosure guidance for registrants that can provide a model framework for small businesses and offers steps to strengthen cybersecurity. It reviews the tools available currently on website security to help organizations protect critical data and build trust with customers such as Secure Sockets Layer (SSL) encryption, the need for data encryption offered by SSL, and additional measures such as authentication of website legitimacy and trust building with one's customer base. The next section discusses the current practices and status of online security in small businesses.

Current practices and status

Cloud computing enables today's small businesses and their employees to work from anywhere, anytime using multiple devices. They are able to transfer files using Drop Box, video-conference globally with Skype and other sites, and remotely access work from their smartphones and tablets. But as some small businesses have learned painfully, the price for these collaborative benefits is the potential for a serious data security breach. If the small businesses have Fortune 500 companies as customers, they provide an easy entry point to a much larger treasure trove of data. Examples of such breach are the incidents at Target and Home Depot where the hackers used the access of a relatively small vendor in the supply chain as the entry point to a major credit card data theft. As companies turn to digital technologies for business solutions, the risk of a security breach continues to rise. For the last 11 years, the security of information technology and data has been rated as a top technology initiative in surveys conducted and published by the AICPA (2014). In addition to concerns about the loss of data and sensitive information, the AICPA surveys (2014) identify controls for mobile devices and cloud computing as ongoing concerns.

Businesses of all sizes need to assume a state of compromise today, because not doing so can lead to considerable costs from loss of data or stolen intellectual property, interruption to business operations, and damage to the business's reputation which can lead to customers switching to competition. All businesses need to assess their cybersecurity weaknesses so that they can develop a strategy to safeguard sensitive data. A basic question to ask: what is the most sensitive data for the business? A pharmaceutical company might have the formula for a new drug in a document that is securely stored on its hard drive, but the data has also been shared by the researchers via email without encryption. Similarly government and non-profit agencies have large troves of sensitive taxpayer data in their files which are loaded onto employees' laptops or flash drives for work reasons without encryption. It is important to ask specific questions about how data is handled and transported, what media are used for data storage, where did the data originate from, and who has been granted access to the networks. The data most valuable to a hacker may not reside in business's own database, but it can provide access to their customers. Knowing the answers to these questions is essential for effective management of the cybersecurity risks**.**

The primary reason for the small businesses' failure to invest in cybersecurity appears to be the mistaken view that such investment is a discretionary spending item, and not understanding it to be an essential, defensive cost for staying alive. Studies (Pwc, 2015) have shown that 89% of consumers avoid businesses who do not protect their online privacy, as evidenced by the sales decline at companies like Target and Home Depot. Business partners also require proof that their interests and privacy are protected. Adequate security has become a requirement for companies to collaborate or outsource work. 54% of US businesses have baseline standards that they expect their external partners, suppliers, and vendors to meet (Ponemon survey, 2014).

While small businesses and non-profits lack resources and time to researching the most appropriate cybersecurity tools, a "one-size-fits-all" approach to cybersecurity by installing the bestselling package is not the answer. The businesses need to adopt new strategies for risk management focusing more on the consequences of a wide range of potential risk events and less on the probability of the events occurring. The new threats from trends of globalization, rapid technological changes, and re-alignment of economies are increasing volatility in the markets, and disrupting ideas about “black swan events”, i.e., low probability, high impact events. For small businesses making no change to their risk management by considering the security breach events as “black swans” may pose the biggest risk to their strategy and future growth. They need to review their current risk-management approach and decide whether it can take them to their desired future state. That may require a mindset change to viewing risk management as a business enabler that helps propel the organization forward, rather than a rigid structural shield.

To understand any cyber breach event, the motivation of the attackers needs to be understood. Most attacks are low-skill and low-focus i.e., hackers using low-end attacks by sending spam mails out to millions of email addresses, hoping that someone will click on the link. High-skill, low-focus attacks such as the ones on Target, Home Depot Chase and other commercial networks in the past year are more serious. They are sophisticated attacks using newly discovered "zero-day" vulnerabilities in software, systems and networks. The following tables show some of the top 10 data breaches in 2014, and the total data breaches in 2014 listed by Identity Theft Resource Center.

Top 10 business data breaches (Source: Identity Theft Resource Center)

Company	**State**	**Number of accounts affected**
Home Depot	GA	56 million
Michaels	TX	2.6 million
Neiman Marcus	TX	1.1 million
Goodwill	MD	868,000
Variable Annuity Life	TX	775,000
Spec’s	TX	550,000

Total data breaches in 2014 (Source: Identity Theft Resource Center)	**Number of breaches**	**Number of records**
Banking/ Financial	43	1,198,492
Business	258	68,237,914
Education	57	1,247,812
Government	92	6,649,319
Healthcare	333	8,277,991
Total	783	85,611,528

In all of the above incidents, the attacker is an opportunist who got access to large database of credit-card numbers from exploiting the weaknesses in cybersecurity. Any large retailer would have served their purpose. The low skill hackers who penetrate the networks of businesses do not care much about the individual entity, and if the business' security protocols are strong they will move on to the next weaker prey. Such low-focus attacks are easier to defend against by having strong protection of systems. All networks are vulnerable to attacks by a sufficiently skilled, funded and motivated attacker, but good security can make the attacks harder, costlier and riskier. In the case of low skill, low focus attacks, good security may protect the business completely. The next section discusses the requirements in the SEC disclosure guidance for registrants.

SEC Disclosure guidance for registrants

In the fall of 2011, the SEC's Division of Corporation Finance issued enhanced financial statement disclosure guidance directed towards public companies, which can serve as a model framework for small businesses. The guidance has led to a higher level of cybersecurity awareness, monitoring, and scrutiny by SEC registrants ("CF Disclosure Guidance: Topic 2," Oct. 13, 2011). The guidance was issued in response to the increase in number and severity of cybersecurity incidents experienced by SEC registrants, and the new disclosure obligations focus on cybersecurity risks and actual incidents. The SEC guidance recognized that cyber-attacks can be deliberate or can result from unintended events caused by outside hackers or by internal agents (e.g., employees, contractors, vendors). Examples of specific attacks mentioned by the SEC include: unauthorized access to sensitive data, industrial espionage, sabotage of hardware and software, infection of hardware and software with malicious software, theft of computer time and other denial of service attacks, and theft of mobile devices, such as laptops, notebooks, and cell phones. The SEC guidance is consistent with other disclosure requirements mandated by federal securities laws and suggests that disclosures should identify the unique facts and circumstances related to specific, material cybersecurity risk factors. For example, SEC financial statement disclosure obligations can arise from the following: cybersecurity risks and costs associated with a registrant's operations, or risks from outsourcing activities, or risks that were undetected for an extended period, or risks that lead to increased insurance coverage; past year's cybersecurity incidents that are individually or collectively material in nature. In addition to the potential risks, actual cyber-attack incidents must be disclosed with details on the nature, occurrence, potential cost, and related consequences. Such information on prior attacks can be helpful to users to understand the risks faced by the company and its remediation efforts. Realizing that estimating costs of potential breaches is very difficult, SEC offered guidance on costs that should be considered, which include: remedial costs associated with loss of data and business after an attack, costs of cybersecurity, loss of revenues due to a loss of data or customers, regulatory fines, litigation costs, and reputational damage that can lead to loss of customers and reduced investor confidence.

The SEC disclosure guidance requires management to explain the costs and other consequences of material cybersecurity incidents, and potential cybersecurity costs and risks in the management's discussion and analysis (MD&A) section of financial reports including needed disclosures about costs of material litigation, prevention of cyber-attacks, maintaining business relationships, loss of business and future cash flows, and impairment of goodwill and long-lived assets. Disclosures about the impact of cybersecurity risks on the business's information system and the integrity of financial reporting should be a part of management's assessment of internal controls and a potential internal control deficiency. The next section outlines preventive steps and recommendations for a model framework for online security for small businesses.

Preventive steps and recommendations: model framework

Security is a combination of prevention (protection), detection and correction (response). Prevention can defend against low-focus attacks and make targeted attacks harder, and detection can spot the attackers. Having a planned response strategy will minimize the damage and manage the fallout. In todays inter-connected, global marketplace individuals have to entrust businesses with intimate life details on email, Facebook, text messages etc., and entrust retailers with financial details. Increasingly, businesses and individuals use cloud services for storage and transactions (Green et al, 2014). Awareness about the risks and data vulnerability will prompt users to strengthen data security and response plans. Creating a culture of cybersecurity, having current security software, and creating an emergency response plan for a data breach are good first steps toward protecting the business in the long term. Broadband and information technology are powerful factors in small businesses reaching new markets and increasing productivity and efficiency making it critical for businesses to develop a cybersecurity framework to protect their own business, their customers, and their data from growing cybersecurity threats. **Some specific steps to take are outlined in Exhibit 1.**

Internal controls can strengthen companies' resilience against game-changing risks. Many businesses do not have formal processes in place to assess and prepare for game-changing circumstances that could have reputational, competitive, legal, or operational implications. Many cyber breaches result as much from weak spots in the technology as weak decision making processes that fail to account for the full range of potential business consequences of technology-related problems. The long term viability and reliability of a business depend on timely access to vital information and IT resources at all times. Effective internal controls can help a business maintain and test both the IT contingency and disaster recovery plans. Adopting a consequences-based approach to dealing with risk brings more focus on resilience and less on prediction. By establishing and testing scenarios, managers can determine if the businesses can be resilient at the times of greatest need. These scenario plans look beyond the individual business to include all players in the value chain including key vendors. More businesses are beginning to establish systems that monitor and alert when the probability of a particular scenario increases, setting up cross- functional crisis management teams, and identify processes to quickly react to risks when they occur. Ultimately the most successful risk strategies embed risk awareness through the company's entire culture.

Exhibit 1: Implementation steps

What Action?	How?	Why?
Set the tone at the top	Delegate responsibilities at	to monitor cybersecurity

	various levels of management, assign security team, and develop metrics & measures of risks	threats and corresponding protective measures, to focus on holes in the technology infrastructure, metrics will allow to measure and take actions for any abnormal risk levels
Raise employee awareness	Allocate funds to train employees in using technology	So that employees understand the importance of setting up various levels of passwords access to critical information on the servers.
Establish security policies, practices about Internet security practices, security policies for third-party security providers, and establish policies about physical access to computers and network hardware	Communicate them to employees on a regular basis along with the penalties for violating the business policies. Use of USB, social media, and personal devices on the workplace needs to be supervised. Establish the standards up front, spell out the desired security level, ensure that it is included in the provider's performance contract, and test them periodically.	To protect sensitive business data and practices rules for handling and protecting sensitive customer information and other vital data. When using third-party security it is important that a legal corporate contract is in place due to the liability issue Physical security of hardware components is inevitable for any business
Establish cross functional security teams	Include leaders from IT, HR, Finance, Risk and legal departments to meet on a regular basis to discuss and coordinate information security issues, run simulation exercises	The plans will help them to take an appropriate actions during and after security breaches. Communication between departments is integral to a successful security strategy. Companies that do not perform such scenario planning exercises for crises may end up looking like amateurs, making a bad situation worse.
Establish backup and recovery processes	Regularly backup data on all equipment used in the business.	In case of disaster the business can recover by using the backup data
Setup firewalls between internal and external networks and implement barriers to limit the	Teach employee to think about their irresponsible behavior	If not then employees may unintentionally expose the internal information to outside world

employees' irresponsible online actions		
Automate software updates	Software such as Systems, application, antivirus, anti-spam, antispyware	
Secure and manage the Wi-Fi networks	Provide restrictive password access and assign the access to networks with careful investigation of individual who can access Wi-Fi network	Since there are no hard connection it is critical to secure the access to Wi-Fi network so that no unauthorized individual can access
Use encryption	Categorize the information sensitivity levels and accordingly provide encryption key so that only authorized individuals can have access to information	In the global business environment trans-border dataflow is inevitable and to secure the information is more critical than ever
Instill trust in customers about the seriousness of security breaches	Via CRM the trust can be achieved	In the e-commerce environment this is more critical since all the customer activities occur online
Be alert to new, affordable technologies and cybersecurity innovations that can deter attackers by detecting intruders sooner	Proactive management style of the security official is necessary to keep up with the state of the art security technology	Staying one step ahead of the intruder minimizes the risk of getting security breach

Conclusion

Many small businesses are realizing that in the increasingly sophisticated and inter-connected global marketplace, investing in information security helps for more than just protecting the business. Strong cybersecurity can position the businesses for competitive advantage with their business partners and customers, as well as to allow them to take advantage of newer technologies to help their growth. New, affordable technologies are offering stronger protections to detect intruders sooner and help businesses to implement preventive and corrective measures. Progressive small businesses and non-profits understand that volatility will stay for years to come, and are rethinking their approach to risk management so that shocks to the system will not disrupt their strategy and future growth. A culture of risk awareness throughout the business is a necessary platform for effective risk management.

By adopting some of the recommended steps, small businesses can be resilient and be able to take calculated risks to pursue growth in the global marketplace. With the exponential increase in internet fraud, security of personal data transmissions is vital to e-commerce operations. A survey by AICPA in March 2015 found that 82% of the respondents said their fear of cybersecurity breaches has changed their shopping habits on internet, and 56% mentioned that they used cash and checks more often. The increased level of internet data theft has caused potential customers to become skeptical, and scared and want more assurance of the protection of their information. Investment in technology to protect customers and earn their trust is minimal compared to the overall cost of doing business and by the potential upside. Enhancing e-commerce site security with technological tools like SSL, and working with a reputable security vendor are essential choices for small businesses to be successful and earn customer trust.

REFERENCES

References available upon request.