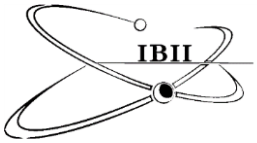


Journal of Management Science and Business Intelligence, 2017, 2–1
May 2017, pages 9-15
doi: 10.5281/zenodo.581691
http://www.ibii-us.org/journals/jmsbi/
ISBN 2472-9264 (Online), 2472-9256 (Print)

Managing Cybersecurity and e-Commerce Risks in Small Businesses

Kamala Raghavan[1], Mayur S. Desai, P.V. Rajkumar

[1]1Department of Accounting and Finance. Texas Southern University, Houston, TX 77004 [2] Department of Management Information Systems, Texas Southern University

*Email: raghavank@tsu.edu, desaims@tsu.edu, p.rajkumar@tsu.edu

Received on April 12, 2017; revised on May 09, 2017; published on May 20, 2017

Abstract
Cybersecurity is a topic of discussion at boardrooms of businesses of all sizes as recent breaches have shown that every sector is vulnerable. Small businesses are becoming aware that their size does not provide safety from breaches. This paper discusses the pattern of increase in cyber breach incidents in businesses of all sizes around the globe, the challenges to cyber resilience found by the Ponemon Institute 2016 survey, offers steps to strengthen cybersecurity and builds customer trust, and reviews available tools on website security to help protect critical data such as SSL encryption.
Keyword Cybersecurity, e-Commerce, small businesses

1 Introduction

Recent disclosures by FBI of a scheme by hackers to profit by distributing market sensitive information from firms that handle official press releases of corporations and the infiltrations into the databases of small companies like Ubiquiti networks and Car phone Warehouse drive home the urgent need to strengthen cyber security procedures. 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.

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, and 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, and many others). 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.

2 Problem and significance

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. 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. With the availability of many trusted e-commerce sites, consumers have the ability to shop for the best choice that protects their private information. More businesses are beginning to establish systems that monitor and alert as 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 offers steps to strengthen cybersecurity and cyber resilience. 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, 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 California Attorney General's office released its 2016 Data Breach Report which analyzes breaches that occurred from 2012 through 2015. The report stated that office received reports on 657 data breaches involving more than 49 million records of Californians. There were 131 breaches involving 2.6 million records of Californians in 2012, and the comparable numbers for 2015 were 178 breaches putting more than 24 million records at risk which equates to nearly three out of five Californians. The report cited that these cyber incidents occurred in all sectors- retailers, banks, medical services, spas, hotels, restaurants, government agencies, schools, and universities, mostly caused by both unintentional and intentional actions by insiders (employees and service providers). Although small businesses can increase revenues by accepting credit cards, but there are costs and risks.

The threat of having customers' payment card data stolen is real, but it can be reduced by adhering to the Payment Card Industry (PCI) Data Security Standard (DSS). A Symantec survey found that 77% of small businesses in the US think that they are safe from cyber threats, and 83% of them do not have security plan. However 40% of the cyberattacks Symantec prevented in 2012 targeted businesses with fewer than 500 employees (Symantec 2012). In 2014-15, several major private-sector and public-sector organizations suffered breaches including, Yahoo!, Anthem Blue Cross, the Home Depot, Target, Neiman Marcus, Adobe, RSA, Lockheed Martin, Oak Ridge National Laboratories, and the International Monetary Fund. A Ponemon Research survey conducted in 2012 of 583 U.S companies ranging from small businesses with less than 500 employees to companies with more than 75,000 employees found that 90% of the respondents admitted that their organizations' systems had suffered at least incident in the previous 12 months, and 60% reported more than 2 breaches.

The joint study by Ponemon Institute and IBM's Resilient Company on cyber resilient organizations around the world involving 2400 security and IT professionals from USA, UK, France, Germany, UAE, Brazil, and Australia during 2015 and 2016 found that:

- 66% of the respondents felt that their organizations were not prepared to recover from cyber-attacks,
- 75% admitted that they did not have a formal cyber security incident response plan (CSIRP),
- 41% said that time to resolve the cyber incident had increased from previous year, and
- 52% felt that complexity of business processes is a significant barrier to achieving cyber resilience.

Other key discoveries from the study were:

- 74% of the organizations said they had been compromised by malware and 64% by phishing,
- 66% of the organizations were not confident in own ability to recover from an attack,
- Only 25% of the organizations have an incident response plan applied consistently, 23% have no plan at all, and 14% test their plan for effectiveness.
- 70% of organizations felt that the time to resolve a cyber-incident has been the same or has increased from previous years.

The study respondents listed the top 5 barriers to cyber-resilience as insufficient planning, complexity of business processes, insufficient risk assessment, complexity of IT processes, and silos and turf issues. The same trend was observed by a subsequent 2016 study by Ponemon Institute and A10 Networks dealing with Indian organizations. India's economic growth rate combined with its adoption of digital technology has increased its vulnerability to malware attacks to be among the top 5 in the world. Sophos India found that 55% of the organizations surveyed (790) were reporting attacks by ransom ware, but only 5% of the spending in IT is earmarked for cyber security plans. The next section discusses the current practices and status of online security in small businesses.

3 Current 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.

Some small businesses have started using "penetration testers" to test the strength of their defenses. However, they are finding that such "counter-intelligence" measures have to be constantly updated to keep ahead of the thieves in the game of cyber security (Schumpeter Aug. 2015). One such technique is to sacrifice some of the convenience of integrated data, and keep sensitive information in separate groups. Such a strategy will require a lot of thought into the information needs of managers, and defining and enforcing rules for information sharing. Another technique used by counter-intelligence experts is to offer tempting targets as "Honey pots" to entice the attackers, and enable monitoring their moves (Martin, May 25, 2001). This technique is effectively used by some banking institutions who can alert the law enforcement agencies. A successful security system design must include a checklist of preventive, detective and corrective steps to increase the chances of success for designing and implementing a security system. Some examples would be:

Preventive- (1) understanding the landscape of computer and network security; (2) putting together the basic safeguards.

Detective- (1) identifying security threats; (2) identifying security measures and enforcement. Corrective- (1) understanding the services of computer emergency response team, (2) preparing a comprehensive security system, and (3) the business continuity planning.

Regardless of the strategy, managers must develop "constructive paranoia" and start thinking of ways in which data can be breached. They need to be ever vigilant to unusual incidents or patterns, and follow security protocol without fail.

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 that 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 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.

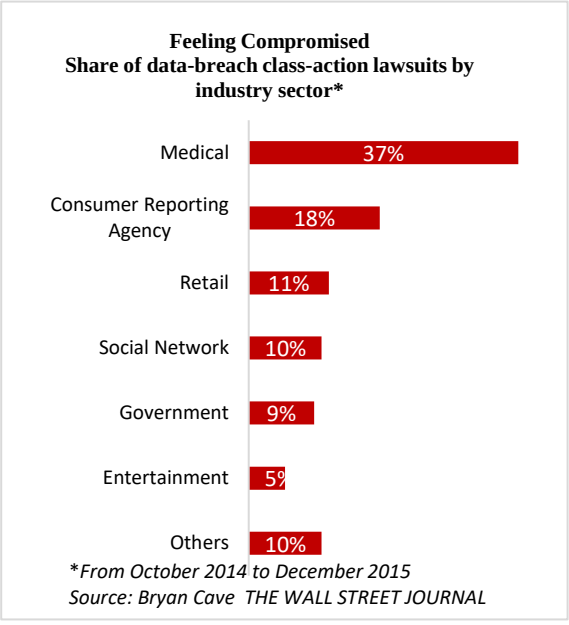
To understand any cyber breach event, the motivation of the attackers needs to be understood. Most attacks are low-skill and low-focus i.e., hackers using low-end attacks by sending spam mails out to millions of email addresses, hoping that someone will click on the link. High-skill, low-focus attacks 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

Cyber breaches can cause widespread damage to companies, and harm to customers. About 5% of data breaches in the U.S. have led to lawsuits so far, but high profile cyber breaches can spawn more than 100 lawsuits according to a study by law firm Bryan Cave LLP. None of these cases has yet gone to trial because the parties have either settled out of court, or the



courts have dismissed them. Target and Home Depot both ended up settling customers' claims, while Neiman Marcus, PF Chang's, and others are contesting. When judges allow class-action lawsuits to progress beyond their earliest stages, the businesses have to bear millions of dollars for expenses incurred to gather large volumes of data and documentation demanded by the plaintiffs, in addition to loss of business and reputational damage.

4. Cybersecurity Management Execution Flow

Cyber security management is a combination of both technology management as well as adequate employee training on secure handling of IT resources. In this section, we present an implementation process for cyber security management that includes both technology and employees who use the technology. Figure 1 depicts an execution flow of security management for small businesses. Even though this approach is equally applicable to businesses of all sizes, we emphasize that security of organization can be improved to a large extent by (1) training the employees and (2) appropriately hardening the computer and communication settings. More importantly, the investments required to implement these two steps would be affordable for small businesses.

4.1 Human Resources Management: A well-known weak link in security protection chain is human beings who handle the resources. Security of organizations largely depends on safe handling of data storage and computer resources.

Individual Training: Regularly assessing the individual's security awareness through routine short courses and quizzes. Such assessments would help the security trainer opt the materials and illustrations specialized for the individual employees. This would help in the improving the overall security protection organizations.

Group Training: Security training on recently discovered attacks on the products (both hardware and software) that are used by the organization's business solutions. Establishing cross functional security teams to identify the business consequences of potential attacks and develop resilience.

Customer Trust: Demonstrable security practices of people handling information system within an organization would improve customer trust.

4.2 Technology and Systems Management: Most of the cybersecurity attacks on businesses are low key and low focused. They often exploit the weakness in security settings of computer and communication devices. For example, it is more often the case that default settings of routers, firewalls, user privileges and credentials remain unchanged until such vulnerabilities are exposed by the attacker.

Hardening Security Settings: Configure firewalls, both computer and network level, to have up-to-date blacklisted websites. Enable the security features of all communication networks like Wi-Fi, Bluetooth, LAN etc. Configure the computer and mobile devices to run in lowest privilege mode as much as possible.

Explore the possibilities: Explore the possibilities of using pen source security tools for penetration testing, port scanning and anti-virus protections.

4.3 Real life practices: The corresponding author of this paper practiced the above flow while managing the operations area of a major financial services where employees had regular training on cybersecurity awareness. Annual simulation exercises were conducted involving cross functional teams to test the cyber resilience of the entire organization. The results of the simulation were analyzed and security practices were strengthened as needed. The organization's technology personnel used penetration testing using internal personnel and skilled outside testers to harden security settings as required. Anti-virus protection updates were installed promptly, and tested periodically by the IT auditors. Such preventive measures were critical for building customer trust and for preserving regulatory approvals.

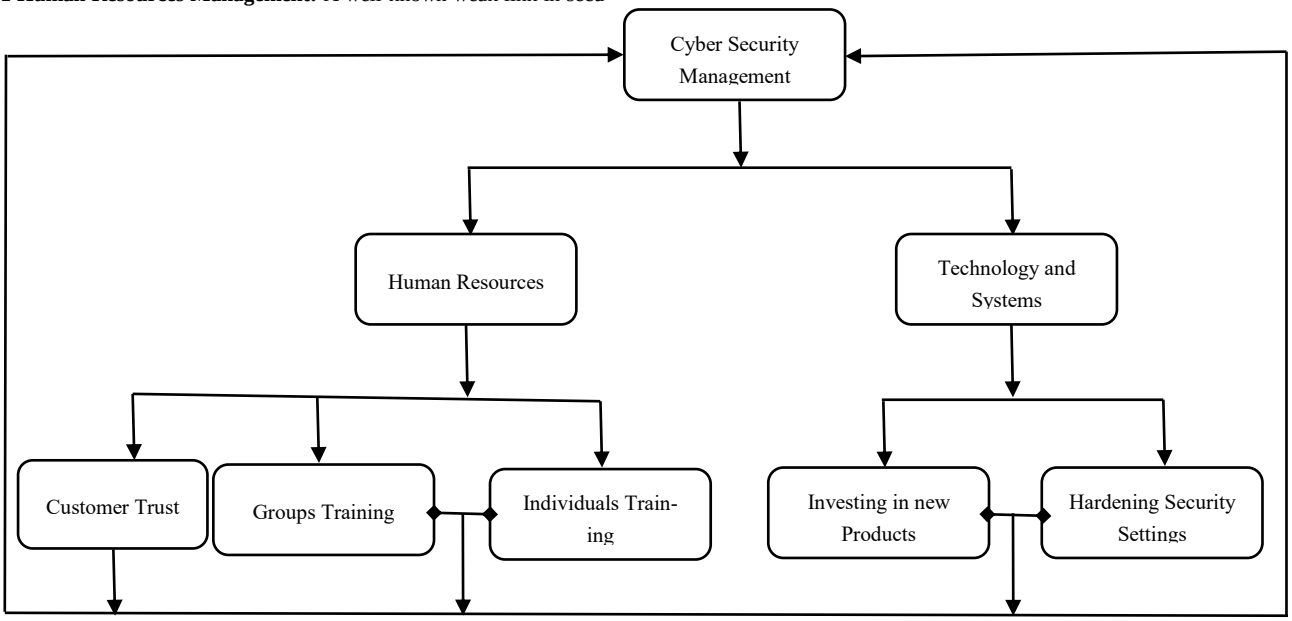


Figure 1: Cyber Security Management Execution Flow

The second author of this paper worked in the electronics and defense industry for over 15 years, and had first-hand experience of going through security training. During his employment and working on the government projects, he and his colleagues had to go through continuous training regarding data handling and level of sensitivity of the data for their assigned projects. Anytime they had a need to use new data, the employees were briefed by the HR professional and the training about the technical part of handling the data was managed by the project manager. The key highlight of the training was the emphasis on the ethical responsibility of employee in handling data. The employees were formally informed about what data they could access and how they needed to be modified and stored. They were assigned specific segments of data that they could either read only or read and edit, and provided training on using the applications they were not familiar with. They were required to refresh their familiarity with the

policy of how they could handle the data. Any data access by the employees was recorded in a log with information about the type of data, the reason for access, the reason for modifying and using data, and employee had to enter his or her employee id and the date to allow for monitoring by management. The policies for data handling and protocols were the same for governmental and non-governmental projects. Any employee working on government projects had to get security clearance which was paid for by the corporation, and the employees who left the company voluntarily or involuntarily were debriefed about their responsibility regarding maintaining the security and content of the data. They were also informed about the possible legal action that can be taken by the company in case of any breach of security and privacy of the data. Both of the above real-life examples in different sectors show the data security management execution flow in practice today.

Besides the training and education, the right set of incentives would motivate the employees to keep them up-to-date on best security practices. A study on relationship between leadership style and cyber security in small businesses by Bhattacharya in 2008 showed that there is a significant relationship between transactional and transformational style leaderships and cyber security concerns within the organization. We suggest that the cyber security management activities such as planning the training and assessments, designing a right set of incentives and setting overall security goals be explicitly integrated into the adopted leadership style of the organization to implement an effective cyber security protection.

The National Institute of Standards and Technology (NIST) provided a detailed guidelines for securing small business. Table 1 provides a brief summary of recommendations made in the NIST report.

Table 1: NIST recommendations (Source: Kissel 2009)

Absolutely necessary actions
1. Keep regularly updated anti-virus and anti-spyware software both in office and home computers as employees may access from home computers. 2. Install hardware firewalls between office/home computers and Internet. Change the default admin names and passwords of the firewalls. Secure Wi-Fi access points and networks. 3. Install and enable software firewalls in each computers. 4. Regularly patch OSs and applications; Make backup copies of important business documents. 5. Control physical access to computer and network components. 6. Require individual user account for each employee on business computers and business applications. 7. Limit the access to data and information, authority to install software.

Highly recommended practices
1. Do not open attachments, web links, social media messages that comes in email unless you are expecting them and you trust the sender. 2. Do not respond to popup windows by clicking Ok. 3. Use secure browser connections while doing online business or banking. 4. Do not surf the web using an administrative privilege. 5. Do not download software from any unknown web page. 6. While disposing computers remove the hard disk and destroy them.

Usage of mobile devices in small business is increasing rapidly as they are economically more viable than desktop and laptop computers. These devices often handle and carry sensitive business information. Device-oriented, user-oriented and management-oriented recommendations for usage of mobile devices in small business is listed in (Harris et al. 2014).

5. 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

Action step	**Method**	**Rationale**
Set the tone at the top	Delegate responsibilities at various levels of management, assign security team, and develop metrics & measures of risks	To monitor cybersecurity 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	To enable employees to 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	To help them to take 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.	To make sure that the business can recover by using the backup data from disasters
Setup firewalls between internal and external networks and implement barriers to limit the employees' irresponsible online actions	Teach employee to think about their irresponsible behavior	To prevent employees from unintentionally exposing the internal information to outside world
Automate software updates	Software such as Systems, application, antivirus, antispam, antispyware	To ensure prompt update of software
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	To ensure that the access to Wi-Fi network is secured 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	To secure trans-border dataflow in the global business environment
Instill trust in customers about the seriousness of security breaches	Via CRM the trust can be achieved	To promote customer confidence in the organization's commitment to privacy.
Be alert to new and 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	To stay ahead of the intruder and minimize the risk of getting security breach

The suggestions outlined in the above table are preventive or avoidance mechanisms. Since cyber security threats evolve over time, it is not practical to implement a fool-proof security protection at an organizational scale. We suggest deploying intrusion detection systems at various levels within the business to identify potential ongoing attacks. Effectiveness and applicability of various types of intrusion detection systems are measured in terms their detection methods, metrics used and their deployment models (Milenkoski et al. 2015). Table 2 provides an overview of common trends and business practices of Intrusion Detection Systems (IDSs) necessary and feasible for small organizations

Table 2: IDS trends and business practices (Source: Milenkoski et al, 2015).

IDS property	Types	Recommendations
Attack detection and accuracy, coverage	All	Use workloads that contain current attacks
Attack detection and reporting	Distributed IDSs	Measure time to notify all or designated nodes
Resource consumption	IDSs in resource constrained environments	Measure power consumption based on all nodes
Performance overhead	Host based IDSs	Evaluate workloads in executable form generated by workload drivers
Workload processing	Network	Monitor high rate workloads

We recommend that the small businesses employ a combination of host and network based intrusion detection systems to identify ongoing attacks. This would help them to reduce the business risk from the security breaches that could circumvent the implemented preventive measures.

6. 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 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

Anonymous. 2016. Current Developments, *Computer and Internet Lawyer*, 33 (5): 20-25.

Bidgoli, Hossein. 2016. Integrating Real Life Cases into A Security System: Seven Checklists For Managers, *American Journal of Management*, 16 (4) :9-25.

Bosworth, Seymour, Michael E. Kabay, and Eric Whyne. 2014. *The computer security handbook*, 6th Ed., New York, Wiley.

CBS. *60 minutes show*, 6 September 2015

Clapper, Danial, and W. Richmond. 2016. Small business compliance with PCI DSS, *Journal of Management Information and Decision Sciences*, 19 (1):54-67.

Eyden, Terri. 2013. "NSBA Survey: cyber-attacks concern small business owners", *Available at: http://www.accountingweb.com*, October 10.

Fallon, Nicole. 2014. "A Culture of Cybersecurity' Is Best Small Business Defense". *Business News Daily*, November 10.

Federal Communication Commission. 2004. Ten cybersecurity strategies for small businesses. *Available at: www.fcc.gov/cyberforsmallbiz/*

Grant, Gerry H., and C Terry Grant. 2014. "SEC cybersecurity disclosure guidance is quickly becoming a requirement", *The CPA Journal*, 84 (5): 69-71.

Green, Kelly Brian, and Brian P. Green. 2014. "Reining in the risks of cloud computing". *Internal Auditing*, 29 (5): 29-35.

Hagel, Jack. 2014. "Not for profits delve into risk management". *Journal of Accountancy*, 218(5): 24-25.

Lanz, Joel. 2014. "Cybersecurity governance: the role of the audit committee and the CPA*". The CPA Journal*, November: 6-10.

Martin, William W, 2001. "Honey Pots and Honey Nets - Security through Deception". Available at 25http://www.sans.org/reading-room/whitepapers/attacking/honey-pots-honey-nets-security-deception-41 *SANS Institute InfoSec Reading Room*, CISSP May - Accessed on September 7, 2015

Milenkoski, Aleksandar Marco Vieira, Samuel Kounev,,Alberto Avritzer, and Bryan D. Payne. 2015. "Evaluating Computer Intrusion Detection Systems: A Survey of Common Practices", *ACM Computing Surveys (CSUR) Surveys*, 48 (1), September.

PwC. 2012. Cyber Security: Why you can't afford to ignore it, *Growing Your Business PwC*.

Schneier, Bruce. 2014. "Hackers Could Expose Any of Us --- A focused, expert attacker will always get past security", *Wall Street Journa*l, 20 Dec: C.3.

Schumpter, Joseph. Aug 2015. "Manage like a Spymaster" (http://www.economist.com/news/business/21662540-counter-intelligence-techniques-may-help-firms-protect-themselves-against-cyber-attacks-manage) – Accessed on Sept 7, 2015

US Chamber of Commerce. 2004. *Commonsense guide to cyber security for small businesses*, Feb 2004, http://www.uschamber.com

Wyatt, Christy. 2014. "Is it safe? Be open about cyber threats", *Wall Street Journal*, Oct 20: R4

.