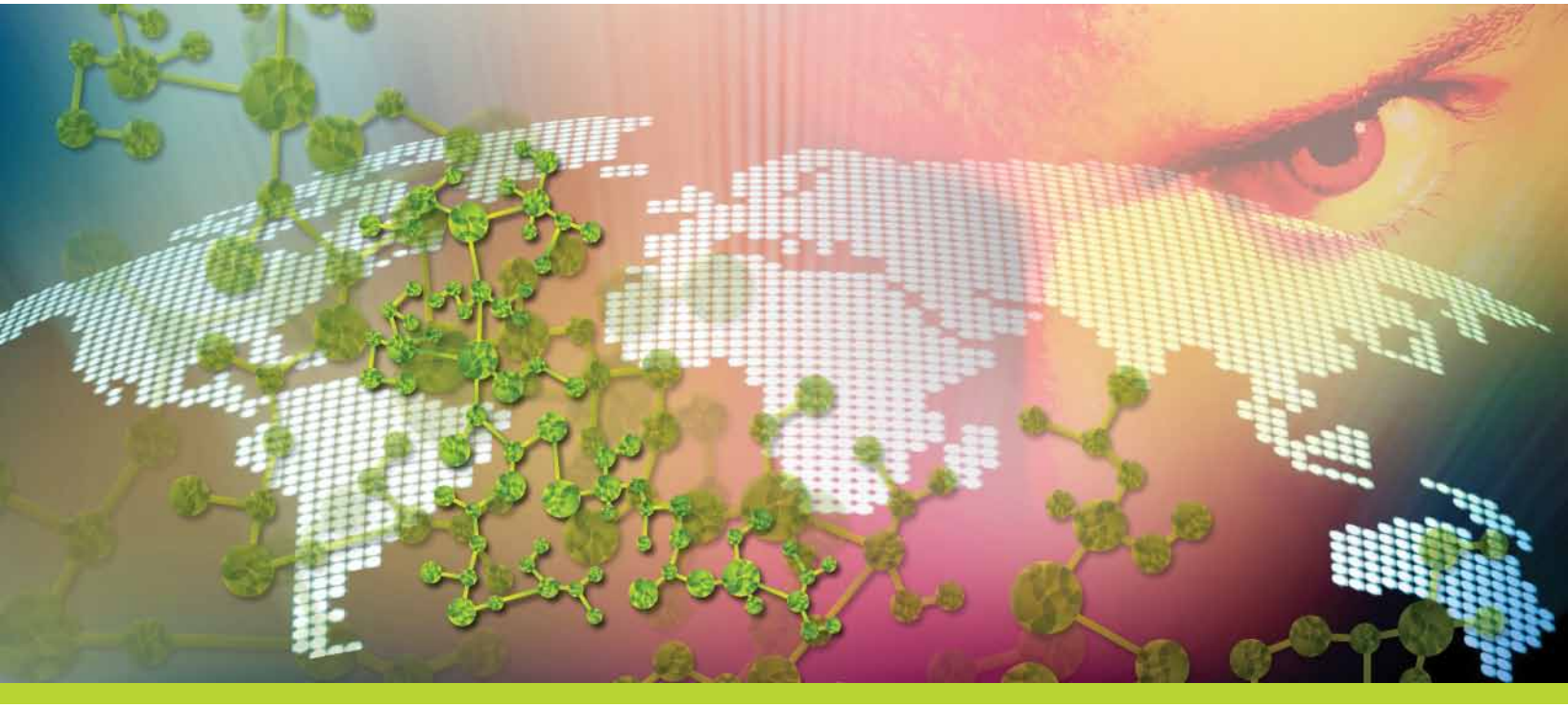
ADVISEN
Insurance Intelligence®



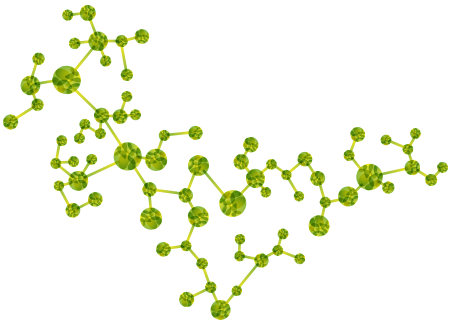
CYBER EXPOSURES OF SMALL AND MIDSIZE BUSINESSES – A DIGITAL PANDEMIC

October 2014

Sponsored by:

THE HARTFORD

CYBER EXPOSURES OF SMALL AND MIDSIZE BUSINESSES – A DIGITAL PANDEMIC



SMBs from all types of industries and all corners of the country are increasingly vulnerable to data breaches, privacy law violations, or other network security incidents.

Executive Summary

Gone are the days when data breaches, privacy violations, and other network security incidents were only a big business problem. Countless organizations of all sizes are now victimized daily, and in many cases with crippling effect. Yet many small and midsize businesses (SMBs), typically defined as firms with fewer than 250 employees, are not aware of the risks, or choose to ignore them. This can be likened to society simply ignoring a pandemic. This Advisen report, sponsored by The Hartford, will examine the cyber threat landscape of SMBs, explain the phenomenon surrounding their cyber-risk complacency, and offer actionable suggestions for effectively managing network security risks.

Introduction

For most employees, as they go about their daily work routines, network security is far from top of mind. Preparing for a meeting, making an impending deadline, or managing customer issues are more urgent concerns. Basic online security practices may routinely be followed, but in a busy corporate environment mistakes can easily be made – like clicking on a seemingly innocuous link in an email that allows a malicious file to infect the corporate network. For SMBs, this situation is potentially devastating and could turn a thriving company into a struggling one.

SMBs from all types of industries and all corners of the country are increasingly vulnerable to data breaches, privacy law violations, or other network security incidents. These events can result from malicious insiders, lost or stolen laptops, or employee error. More and more frequently, however, an attack originates from outside the company by individuals seeking to steal sensitive information, empty corporate bank accounts, or execute any number of fraudulent cyber schemes.

What many fail to realize is that cybercriminals are opportunistic and SMBs frequently present the better opportunity.

Many SMB owners and managers may find it difficult to believe that they are at risk. It seems counterintuitive that cybercriminals would focus on small businesses. Major news outlets, for the most part, only report on the largest incidents, which typically affect the largest companies. Furthermore, common sense suggests that the bigger the business, the more desirable the target due to the volume and scope of its operations. Think of U.S. retailer Home Depot, for example.

What many fail to realize is that cybercriminals are opportunistic and SMBs frequently present the better opportunity. Cybersecurity experts have repeatedly sounded the alarm about the vulnerability of smaller businesses. The Target breach, for example, was a result of malware introduced by a much smaller corporate partner that likely had far less sophisticated cyber defenses. [1] But a nationwide survey found that a majority of small business managers are not concerned about cyber threats – either external or internal.[2] The Hartford's annual Small Business Success Study, which focused on the truly small businesses defined as companies with fewer than 100 full-time employees and annual revenue of $100,000 or more, paints a similar picture, finding that 27 percent of small business owners do not believe a data breach represents a risk to their business. Furthermore, 31 percent of respondents said there would be no impact to their business if their company experienced a data breach.[3]

If cybercrime is a disease, these companies do not appear ready to find a solution. A disconnect clearly exists between the reality of the situation and the cyber threat perception of SMBs. However, with data, privacy, and network security risks at an all-time high, it is only a matter of time before SMBs recognize that the time has come to address this digital pandemic. Hopefully, most won't learn the hard way.

A 'not so' positive trend

In the past SMBs may have been able to neglect network security with little consequence, but this is not the case today. This is highlighted in Symantec's 2014 Internet Security Threat report which found that SMBs (defined as having fewer than 250 employees) accounted for more than half of all targeted attacks (61 percent) in 2013. This was an 11 percentage point increase from the previous year.[4] In another study by the National Cyber Security Alliance, it was reported that 20 percent of small businesses fall victim to cybercrime each year.[5]

As previously mentioned, cybercriminals tend to be opportunistic. Verizon defines opportunistic attacks as one where the victim is not specifically chosen as a target but identified and attacked

Historically speaking, of all the cyber incidents tracked by Advisen, SMBs represent approximately 60 percent of the total cases

because it exhibited a weakness the attacker knew how to exploit. According to the 2012 Verizon Data Breach Investigation Report, 85 percent of targets of opportunity are small businesses, which they define as organizations with fewer than 1,000 employees.[6]

Advisen data shows similar trends. Comprised of cyber intelligence collected since 2000, Advisen's database highlights where and how cyber-related losses are occurring. Defined as businesses with revenues less than $350 million, cyber-related incidents affecting SMBs have had an upward trajectory since 2004 (exhibit 1). Historically speaking, of all the cyber incidents tracked by Advisen, SMBs represent approximately 60 percent of the total cases (exhibit 2).

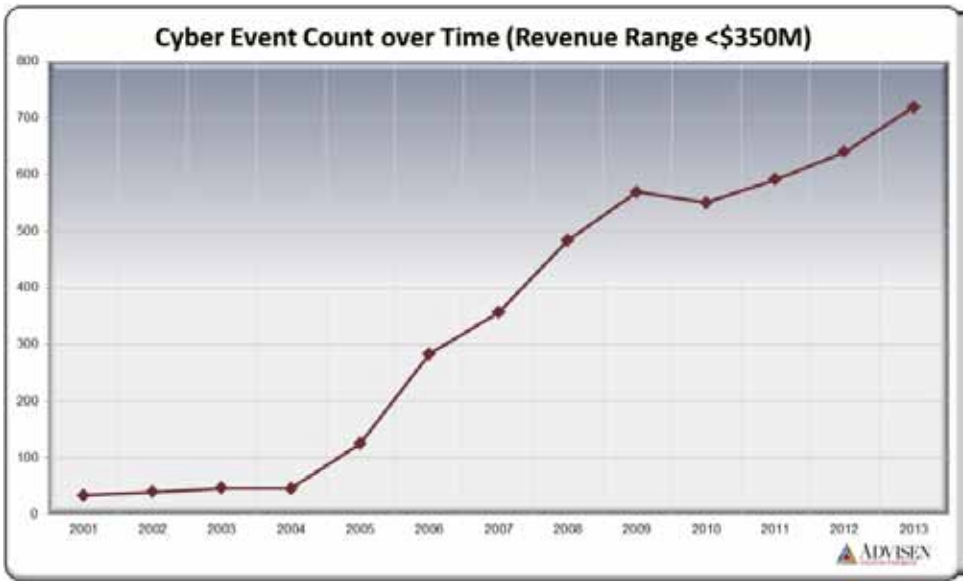
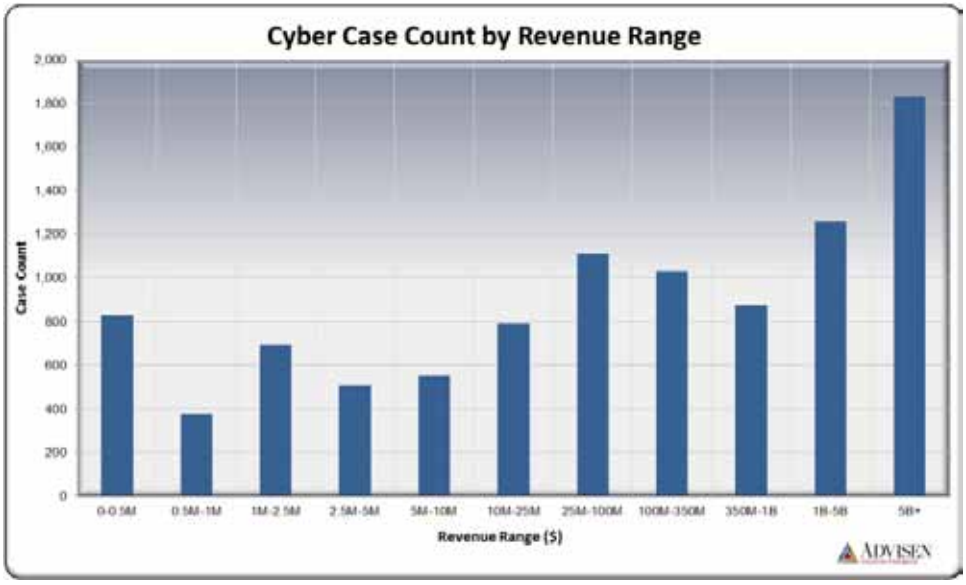


Exhibit 2:



In most cases larger companies are higher-value targets, but they also tend to have more sophisticated IT security systems.

Exhibit 1:

Even more frightening are the potential consequences for SMBs if they fall victim to a cyber-attack, the most severe of which include going out business. Yet many SMBs still choose not to make cybersecurity a priority. The question is "why?" Are they not educated on the threats and consequences? Is it complacency? Or is it a bit of both?

The easy target for the opportunistic criminal

In most cases larger companies are higher-value targets, but they also tend to have more sophisticated IT security systems. SMBs, on the other hand, frequently have less robust security systems and hackers can still gain tremendous value from exploiting their data.

SMBs generally have fewer IT resources and devote less time and money to cybersecurity than their larger counterparts. Some outsource their IT and security to a vendor and simply trust that the vendor's data management practices and network security measures are adequate. They are less likely to keep security software up to date, and are generally less knowledgeable of their overall cyber exposures. Security training is often nonexistent. Even companies that want to make cybersecurity a priority often believe they do not have the resources to develop, maintain, and execute comprehensive cybersecurity policies and procedures.

The Ponemon Institute estimates that nearly half of SMBs do not have an adequate security budget.[7] The study evaluated the security profiles of small and mid-size companies with fewer than 100 employees up to 5,000. According the National Cyber Security Alliance,"87 percent of SMBs do not have a formal written Internet security policy for employees while 69 percent do not have even an informal Internet security policy for employees." [8] In addition, employees are often not educated on basic cybersecurity practices such as updating anti-virus software, avoiding phishing scams and compromised websites, creating strong passwords, and not using public wi-fi. These factors make SMBs low-risk targets with potentially significant rewards.

It is important to note, however, that a lack of cybersecurity focus does not correlate with being less dependent on technology. According to the National Cyber Security Alliance Small Business Study, 87 percent of small businesses have at least one employee who uses the internet daily. According to the same study, 71 percent say their business is at least somewhat dependent on the Internet for daily operations.[9]

Costs arising from a data breach can include forensic IT expenses, fines, credit monitoring and identity restoration, crisis management activities and attorney fees.

Another study conducted by the National Small Business Association found that the vast majority of small businesses maintain an online presence via a website and increasingly use social media as part of their online strategies. The study also found that utilization of new technology platforms such as cloud computing, smart phones, and tablets are on the rise, and companies increasingly allow their employees to telecommute.[10] All of these factors have expanded the attack zone of SMBs and are exposing already vulnerable organizations to a greater degree of risk.

What are the stakes and who is most at risk?

The potential consequence of a data, privacy, and/or network security breach to a SMB is significant. According to the Ponemon Institute's 2014 Cost of a Data Breach Study, data breaches now cost $3.5 million on average, which is a 15 percent increase over 2013. The same study also found that the cost per lost or stolen record is on average $145, a 9 percent increase over the previous year.[11] Yet according to The Hartford's 2014 Small Business Success Study, 31 percent of small business owners think there would be no impact to their business whatsoever if it experienced a data breach.[12] But in reality, for many SMBs, sustaining a loss at these levels would severely cripple them, or even put them out of business.

Costs arising from a data breach can include forensic IT expenses, fines, credit monitoring and identity restoration, crisis management activities and attorney fees. One significant cost is notifying affected people of the breach. Presently 47 states, the District of Columbia, Guam, Puerto Rico and Virgin Islands have enacted data breach notification laws.

The logistics around notifying victims alone can be costly. According to the Ponemon Institute, U.S. organizations on average spend $565,020 on breach notification.[13] The cost and complexity of notification increases with the number of states in which a SMB does business since they are subject to the laws of each state where customers are located. Complying with the regulatory requirements of various states requires a tremendous amount of coordination, time, and resources, which many SMBs simply do not have.

The threat of a lawsuit by customers or other affected parties is also a risk. Although victims typically must prove they have sustained demonstrable losses in order to prevail in a suit, in a few significant cases judges have denied motions to dismiss if there was a possibility of future damages. In February 2014, a data breach class action with no claim of financial harm was settled, suggesting some companies may be more vulnerable to lawsuits than was

While the most targeted attacks in 2013 were against Governments and the Services industry, the industries at most risk of attack were Mining, Governments and Manufacturing.

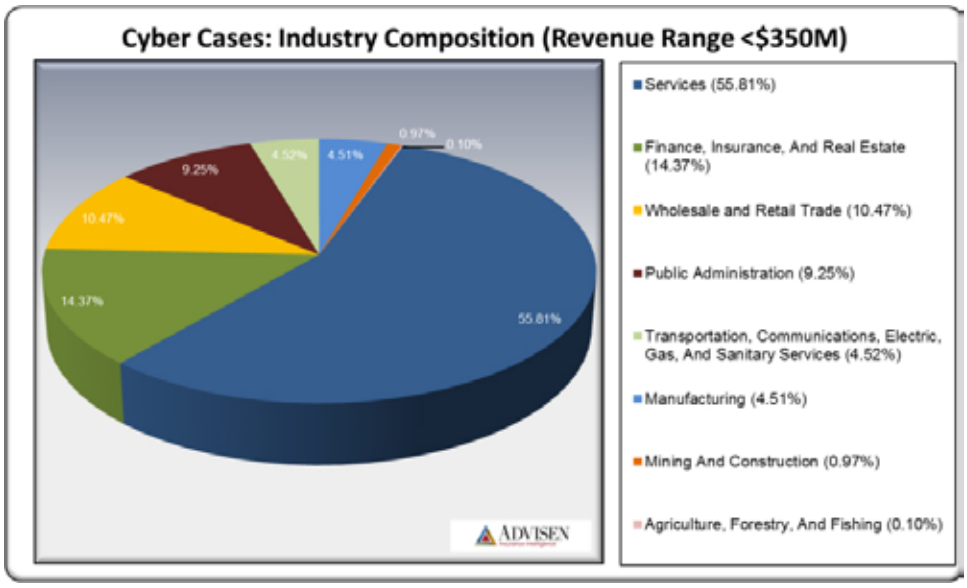
previously believed. [14]

Firms that collect valuable information such as payment card or healthcare information are not the only ones at risk. The intentions of cybercriminals vary. Some may seek trade secrets or other intellectual property, others may want access to a larger and potentially more profitable corporate partner, and yet others may want to use a compromised SMB's computers as part of a platform to launch other attacks. It was reported that on average 30,000 new websites per day – the majority of which belong to legitimate SMBs – are infected and unknowingly distribute malicious code for cybercriminals.[15] Inadvertent transmissions such as these reinforce the importance of network security and the risk of third party liability if an organization's negligence in network security leads to malicious code being transmitted to someone else.

Again, no business is immune from the threat of an attack. Nonetheless, certain industries are at greater risk than others. For instance, looking at businesses of all sizes, Symantec found that, "While the most targeted attacks in 2013 were against Governments and the Services industry, the industries at most risk of attack were Mining, Governments and Manufacturing. Their odds of being attacked were 1 in 2.7, 1 in 3.1 and 1 in 3.2 respectively."[16]

According to Advisen, SMBs in the services sector (e.g. healthcare, education, hospitality etc.) have been the most frequently targeted. This is perhaps not surprising since these companies typically collect and store vast amounts of valuable data. This valuable information not only makes them attractive to outside cybercriminals, but also more prone to insider threats, both accidental and with malicious intent. (Exhibit 3)

Exhibit 3:



Cybercriminals employ a variety of tactics against SMBs ranging from broad based malware attacks to more targeted attacks that utilize ransomware, mobile malware, botnets, DDOS attacks, and brute-force attacks.

Tactics and consequences

As they attempt to stay a step ahead of network defenses and find paths of least resistance, cybercriminals' tactics are constantly evolving. TrendMicro reported that a new threat targets small businesses every second.[17] The ability to execute such attacks has become increasingly simple thanks to underground marketplaces that offer cyber criminals almost every product or service they need to execute an attack. This is referred to as "cybercrime as a service" (CaaS). Among other things, these marketplaces make it possible to purchase malware, and even hire hackers to execute attacks.

Cybercriminals employ a variety of tactics against SMBs ranging from broad based malware attacks to more targeted attacks that utilize ransomware, mobile malware, botnets, DDOS attacks, and brute-force attacks.[18] Broad-based malware attacks are commonly executed via a phishing scheme whereby an employee of the targeted business is tricked into opening an email attachment or link within an email that covertly installs a malicious file onto the SMB's system. Once installed, cybercriminals can steal sensitive information, empty corporate bank accounts, or potentially gain access to corporate partners.

Ransomware is another tactic frequently used against SMBs. When installed on a network the cybercriminal blackmails the user into giving them what they want by either locking them out of their computer, or threatening to go public with secrete or embarrassing information.

Of all the cyber-related events affecting SMBs, attacks using these types of tactics are increasing as a percentage of total events. For example, according to Advisen data, 'Digital Data Breach, Loss, or Theft' has been in decline while 'System/Network Security Violation or Disruption' has been on the rise. In fact, 2013 saw the most system/network security violation or disruption events – both the absolute number and as a percentage of the total events – since Advisen started keeping records in 2005. (Exhibit 4)

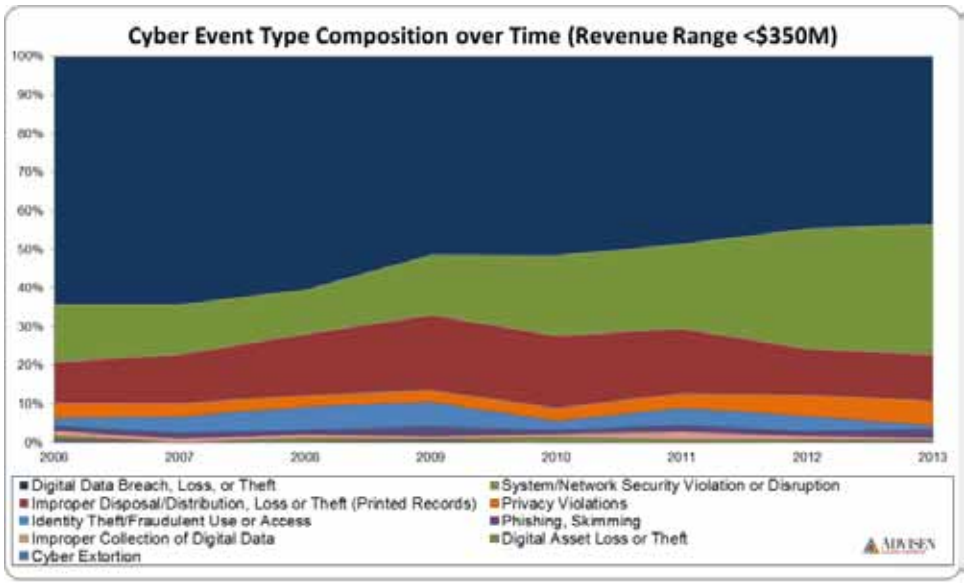
Coming to the realization that cyber risks are a serious issue for SMBs is a vital first step in implementing cybersecurity practices.

Advisen Defines:

Digital Data Breach, Loss or Theft as a Digital breach, distribution, loss, disposal, or theft of personal confidential information, either intentionally or by mistake, in such a way to enable the information to be used or misused by another.

System/Network Security Violation or Disruption unauthorized use of or access to a computer or network, or interference with the operation of same, including virus, worm, malware, distributed denial of service (DDOS), etc.

Exhibit 4:



Risk mitigation

Coming to the realization that cyber risks are a serious issue for SMBs is a vital first step in implementing cybersecurity practices. Although a determined hacker can penetrate almost any network, SMBs can avoid or repel the vast majority of attacks with a variety of cybersecurity protocols, many of which require minimal technical resources, time, or money. Here are some suggestions:

- **Keep up with the latest risks:** Managers who stay on top of the ways in which cybercriminals are affecting other businesses can make better informed decisions about network security.

Small and midsize businesses are in the midst of a digital pandemic. Every day across the country more are learning that they have become the victim of a data breach or other cyber-related incident.

- **Educate staff:** Every employee should be aware of how they can help protect the business. Establish basic security practices such as having strong passwords and adhering to internet use guidelines.
- **Hold employees accountable:** Establish consequences for employees who fail to follow the established security practices.
- **Utilize basic cybersecurity software and keep it up to date:** Cybersecurity software includes antivirus and internet firewall security.
- **Employ mobile device security procedures:** Accessing sensitive business information on employees' own mobile devices can create significant security challenges. Implement mobile device security procedures such as password protecting the devices, encrypting data, and installing security apps.
- **Use secure wi–fi networks:** Make sure the business wi-fi is secure, encrypted, and hidden. Discourage employees from using outside unsecured networks.
- **Be prepared to respond to a breach (incident response plan):** Without advanced preparation, a serious breach can quickly get out of control. Incident response plans can include what to do to limit the damage, who to contact (lawyers, law enforcement, regulators, affected companies etc.), and understanding what type of information is lost and the associated notification requirements.
- **Purchase Insurance.** In addition to providing indemnification for a wide array of privacy and network security losses, many insurers offer access to a variety of pre-breach and post-breach services.

Conclusion

Small and midsize businesses are in the midst of a digital pandemic. Every day across the country more are learning that they have become the victim of a data breach or other cyber-related incident. They have joined a group they likely knew existed but never believed they would be a member of. Many chose not to take even rudimentary steps to keep themselves safe and to prepare to respond to an attack. This general lack of cyber threat knowledge and overall complacency put these companies at risk. Some will not survive.

For those who have yet to become a member of this group, this is a call to action. The pandemic is spreading and the likelihood of being infected grows with every passing day. The good news is that even basic defenses can be effective against an opportunistic attacker, who will simply move on to the next less fortified victim. And if an attack is successful, being prepared can mean the difference between quickly gaining control of the situation with minimal impact and helplessly watching events spiral out of control. There is no excuse for any company to not implement basic cybersecurity measures, and every company should consider insurance protection. ■

This Report was written by Josh Bradford, Associate Editor, Advisen Ltd.

[1] Symantec 2014 Internet Security Threat Report, Volume 19, http://www.symantec.com/security_response/publications/threatreport.jsp see also statement of Fazio Mechanical Services, http://faziomechanical.com/Target-Breach-Statement.pdf

[2] Symantec and National Cyber Security Alliance, Press Release, "New Survey Shows U.S. Small Business Owners Not Concerned about Cybersecurity; Majority Have No Policies or Contingency Plans." http://www.symantec.com/about/news/release/article.jsp?prid=20121015_01

[3] The Hartford's 2014 Small Business Success Study,"

[4] Symantec, "Internet Security Threat Report 2014," http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

[5] National Cyber Security Alliance and Symantec, "2012 National Small Business Study"

[6] Verizon, "2012 Data Breach Investigations Report," http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf

[7] Ponemon Institute, "The Risk of an Uncertain Security Strategy: Study of Global IT Practitioners in SMB Organizations," (November 2013), http://sophos.files.wordpress.com/2013/11/2013-ponemon-institute-midmarket-trends-sophos.pdf

[8] National Cyber Security Alliance and Symantec, "2012 National Small Business Study,"

[9] National Cyber Security Alliance and Symantec, "2012 National Small Business Study,"

[10] National Small Business Association, "2013 Small Business Technology Survey," http://www.nsba.biz/wp-content/uploads/2013/09/Technology-Survey-2013.pdf

[11] Ponemon Institute, Press Release, "Ponemon Institute Releases 2014 Cost of Data Breach: Global Analysis," (May 5, 2014), http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis

[12] The Hartford's "2014 Small Business Success Study,"

[13] Ponemon Institute, "2013 Cost of Data Breach Study: United States," (May 2013),

[14] http://www.nixonpeabody.com/files/167884_Privacy_Alert_07MAR2014.pdf

[15] Sophos, Press Release, "Security Threat Report 2012," (January, 24, 2012), http://www.sophos.com/en-us/press-office/press-releases/2012/01/security-threat-report-2012.aspx

[16] Symantec, "Internet Security Threat Report 2014," http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

[17] TrendMicro, "Small Business is Big Business: 5 Things Every Small Business Should Know About Web Threats and CyberCrime," (2012), http://about-threats.trendmicro.com/smb-primers/small-business-is-big-business/files/assets/downloads/Small-Business-Is-Big-Business.pdf

[18] Dirk A. D. Smith, NetworkWorld, "Cybercrooks target SMBs with new types of attacks," (June 24, 2013), http://www.pcworld.com/article/2042809/cybercrooks-target-smbs-with-new-types-of-attacks.html