Advisen
Transforming • Insurance™

THE EVOLVING CYBER RISKS TO SMALL BUSINESSES AND THEIR DATA

Sponsored by

CYBERSCOUT™
Formerly IDT911

September 2016

INTRODUCTION

Organizations of all sizes face cyber risks, but an attack on a small business can take a more significant toll than on a larger organization. While any entity that collects sensitive data—including personal and payment card information—can be breached, small businesses tend to be particularly vulnerable due to a combination of factors.

The majority of U.S. businesses—over 99 percent, according to federal data—fall into the category of "small business" with fewer than 250 employees.[1] While these businesses provide necessary goods, services, employment and community involvement, they often lack the awareness and resources to address growing cyber threats such as ransomware, social engineering attacks and third-party vendor risks.

Insurers, brokers, and cybersecurity vendors are working together to offer solutions and advice designed to help smaller organizations make the best, most secure choices. Having a plan and partners in place before an event occurs can mean the difference between keeping the lights on or shuttering a business permanently.

Cyber attacks on small business are on the rise in recent years, according to Symantec's 2016 Internet Security Threat Report.[2] Small businesses are ideal targets because they lack the resources, awareness and training to guard against such threats.

This paper will examine:

- Key reasons why small businesses are a target
- Types of attacks most likely to affect small businesses
- Tips and services that can help small businesses turn the tide against cyber crime.

"Small businesses are more susceptible to attacks that exploit weaknesses in the 'human firewall,'" commented Brian Huntley, chief information security officer at CyberScout. "They tend to be running at the speed of light and in many cases, they don't have the opportunity to step back and think about whether an email may represent a potential threat or not."

Trying to keep up with the pace of business can lead to just the type of mistakes cyber criminals hope businesses will make, including:

- Using weak passwords
- Opening email attachments
- Losing or not securing devices
- Failing to use two-factor authentication
- Failing to encrypt data.

Fast-paced business environments have created ideal circumstances for three primary problems for small businesses: social engineering, ransomware attacks, and third-party risks.

THREE PRIMARY PROBLEMS FOR SMALL BUSINESSES:

- SOCIAL ENGINEERING
- RANSOMWARE
- THIRD-PARTY RISK

[1] https://www.sba.gov/managing-business/running-business/energy-efficiency/sustainable-business-practices/small-business-trends; http://csrc.nist.gov/publications/nistbul/itlbul2014_05.pdf

[2] https://www.symantec.com/security-center/threat-report

SOCIAL ENGINEERING

Social engineering is the "easiest way for an attacker to penetrate the defense of an organization," according to the SANS Institute.[3] In this tactic, criminals get victims to divulge sensitive information by appearing as a trusted source. Then, they swindle the business out of funds.

Most people have long become familiar with Nigerian scams in which the scammer asks for financial assistance to transfer money and promises millions of dollars as a reward. These types of schemes persist and can occur by phone, letter, text or email. Sophisticated hackers using email work hard to trick recipients into giving up system credentials or other information to steal funds or data. A more targeted method of phishing known as spear-phishing involves emails that are so convincing because they often include details of a business that employees might not expect outsiders to know.

For small businesses, those hard-earned funds at risk in these scams are vital to the survival of the operation. The prevalence of social engineering and the skill of hackers in mimicking legitimate business communication demand vigilance on the part of small businesses.

"The watchword for those people should be 'do not trust and verify,'" Huntley said. "You have to take that extra half second to look for those anomalies. We've got to have more of that."

He added, "If something looks or feels wrong and out of place, it probably is."

PINPOINTING THE PROBLEM

Larger organizations often have more time and resources to train their employees and are more likely to have dedicated information security staff. However, smaller businesses face an even greater problem – many still don't realize that they could be targets of cyber criminals.

Recognition of the problem is imperative, and this is an area where insurers, brokers and their cyber partners can be invaluable in helping small businesses understand the true risk. As Eduard Goodman, CyberScout's chief privacy officer, put it, a breach "could be an extinction-level event."

RANSOMWARE: ONCE CYBER CRIMINALS INFILTRATE A SYSTEM, THEY CAN DEPLOY MALICIOUS SOFTWARE THAT BLOCKS ACCESS TO DEVICES, SYSTEMS OR FILES UNTIL THE USER PAYS A RANSOM, USUALLY IN BITCOIN, TO THE PERPETRATOR.

"There is a very glaring lack of awareness," said Goodman. "As a small business, your goal is to do whatever you do for a living. That's what you do, that's your passion. You're often just worried about making payroll and getting your taxes filed."

For some, information security and data backup "doesn't even occur to them."

Goodman reported seeing businesses hit by a cyber event using "systems that are woefully out of date."

He added, "They haven't backed up their data for over two years. It hurts because sometimes they're so far gone, and that's a difficult lesson to learn in the time of crisis."

[3] https://www.sans.org/reading-room/whitepapers/engineering/methods-understanding-reducing-social-engineering-attacks-36972

Christie Lucas, vice president and business insurance product manager at Erie Insurance, explained the mindset of many smaller businesses as, “It happens to everyone else, but not to me.”

RANSOMWARE

The fastest rising cyber trend, ransomware, cost victims over $24 million in 2015, according to the Federal Bureau of Investigation, which investigated 2,453 ransomware cases during 2015.[4] Once cyber criminals infiltrate a system, they can deploy malicious software that blocks access to devices, systems, or files until the user pays a ransom, usually in bitcoin, to the perpetrator.

While ransomware attacks can affect any businesses, smaller organizations feel a disproportionate impact.

“The bad guys committing the ransomware attacks don’t really care who they’re attacking,” said Tim Francis, enterprise lead for cyber insurance at Travelers. “They’re just looking to cast a wide net. And there are a lot of small businesses. Large businesses just tend to have more security, while smaller ones have less of the wherewithal to respond on their own.”

Goodman of CyberScout added, “It’s all about low-hanging fruit. Criminals are not looking for hard gains; they’re looking for easy.”

And one of the easiest ways to bring a business to its knees is to restrict its operations. CyberScout’s Huntley described the case of a transportation operator gripped by a ransomware attack. The firm had reservations in place for the next four days – and no way to access the system. Without a sufficient business continuity plan in place, the situation looked dire for the business.

Ransomware reflects the value of information to a business and the absolute need to protect access to that information. It also represents a quick payday for criminals who know that businesses might be forced to offer up the ransom in exchange for vital systems and data. A recent CyberScout survey found that most businesses don’t factor the potential cost of paying ransoms into their budget.[5] But one in three respondents indicated that they would be unable to go without access to critical business systems for any amount of time. Just three percent of respondents said they would pay more than $10,000 to regain access, while 10 percent would pay between $1 and $100.

Organizations invariably need outside assistance when it comes to addressing a ransomware attack. Experts say that they should look to vendors and software providers for advice on security. For example, if a small retailer has a point-of-sale terminal, the vendor should be able to provide support. In the case of cyber insurance, most insurers will offer value-added services to help policyholders develop the best possible cyber defenses.

“There’s no way to keep the lights on and the business running and resolve ransomware,” said Huntley. “They’ve got to reach out and get some trusted advice.”

Small businesses might see demands of $500 to $2,000, according to CyberScout’s Goodman. However, after paying a ransom, an organization might find itself targeted again.

“It’s the standard extortion scheme. It doesn’t end at the first time,” he said. Some businesses plan ahead, prepare, back up their data, and are ready to respond if hit with ransomware.

“This is not something that’s out of reach. For them, it’s an inconvenience but then they’re up and running,” Goodman said.

---

[4] https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise

[5] http://cyberscout.com/company/press-center/press-release/majority-of-american-business-owners-unlikely-to-pay-off

BACK UP YOUR DATA

If an organization takes the sensible course and plots out a business continuity plan, one of the first tasks should be to analyze the operations and safeguard all business-critical data and systems.

"Think of a cybersecurity incident as a disaster, as a business continuity event," Huntley advised. Plans should be flexible, extendable and scalable, he added. A call tree used to alert employees to contingency plans for a snowstorm could also be used in the event of a cyber attack. Temporary office space and data backup at a separate location in case of a storm could provide an equally necessary haven when an organization is hit by ransomware.

And, according to Goodman, the term "back up" might not be fully understood by business owners.

"They might think that they do good, iterative, non-network-connected backup," he said. However, in reality, a business might have only backed up its data several months before a cyber event, or stored it on the same servers that get locked up with ransomware. Depending on how dynamic a business' system is, older data might be fine. For others, even yesterday's data might be old news.

"You probably can't get by on 15-month-old data," he said.

Small businesses should back up all data and systems on all business computers on a weekly basis at a minimum, according to the National Institute for Standards and Technology (NIST), which issued guidance on the fundamentals of information security for small businesses.[6]

Given how long malware can lurk quietly on a system, organizations run the risk of having backed up a malicious virus along with data and key systems needed in order to effectively use the backed-up data, Goodman said.

"We're talking about backing up the data, but also really understanding what you need to do to make sure it's usable," said Goodman. "Make sure it's working. I hear this all the time. They've never tested it; they just assume it works. If it goes dark, they need to have a way to turn the lights back on."

CyberScout's survey found that business owners may be overconfident when it comes to backing up their data, with most (65 percent) not planning to allocate more of their budget to securing data. In fact, 22 percent said they weren't sure how to back up their systems and files, or didn't realize the need, or the extent to which data must be secured.

"They have to make sure it's a removable hard drive. I've seen more and more injections that get onto a system, go in and encrypt the data, and then actually look for network backups to go and poison them, too," Goodman said.

"We've seen more than our fair share of businesses pay [ransom] because they had no other choice, and it was literally that or close up shop," said Goodman. "It's not an enviable position."

BASIC CYBER HYGIENE

Just as few business owners would fail to lock their office doors at the end of a work day, cybersecurity involves some simple strategies that any business can implement. It may just take some education.

"Most of these people are very good at running their own businesses, but they're not computer experts," said Lucas of Erie Insurance.

---

[6] http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf

Organizations don't need to be striding ahead in security, according to Goodman. They do need to do their due diligence on security.

"It's not about being the fastest, it's just about staying with the herd," he said.

It all comes down to "basic cyber hygiene," according to Ondrej Krehel, founder and chief technology officer at LIFARS. For example, computer systems must be maintained a minimum of four times a year, he suggested. The process should ensure that all systems have been reviewed and updated. Business owners should ask their vendors of any systems such as point-of-sale devices for checklists to keep the equipment secure.

THIRD-PARTY RISK

Krehel highlighted another avenue of risk for small businesses—the franchisee/franchisor relationship. Major chain restaurants, for example, involve well-known franchised brands. The franchisees can be seen as providing access to the larger corporate infrastructure, just as smaller third-party vendors can be seen as a throughway to bigger businesses.

"It is a big brand, but the franchise is really driving the value," Krehel said. "There were four cases last year with four big chains. The reality is that small businesses that are part of larger enterprises are targets."

Often, the corporation will provide the technology and the systems, but the franchisee must maintain the security.

"There's a disconnect between the cybersecurity governance from the corporation to the franchisee," Krehel said. "[The hackers] only have to conquer one system. They just have to go around to the franchise and see who is detached from the company."

While small businesses can be viewed as an entry point into larger organizations, they can also be at risk of a breach with their own vendors. Most small businesses rely on third parties to operate. A security event for a third-party vendor can also affect their business partners.

LIFARS' Krehel noted that small businesses frequently lack the awareness and ability to insist upon good cybersecurity practices from their vendors. PricewaterhouseCoopers' annual Global State of Information Security indicated that only 52 percent of all businesses have standards in place for vetting the security of their third-party partners.[7]

TRANSFERRING THE RISK

In the CyberScout survey, over half (52 percent) of respondents admitted not carrying cyber insurance, but millennials ages 18 to 34 were more likely to purchase cyber coverage. A recent Fitch Ratings report found that U.S. cyber insurance premium volume rose to $1 billion in 2015.[8] Cyber insurance is big business, but greater adoption is needed in the small business sector.

"The insurance industry is helping to make them aware of the risks," Goodman said. He explained that the insurance underwriting process itself can be a "wake-up call" for businesses that didn't previously realize the degree of risk they faced from cyber issues.

"If they don't have any insurance or financial risk backup, they're risking everything and they can go out of business. Insurance is the way to go for [small businesses] as long as they don't have high deductibles and they get educated on the product itself," said Krehel of LIFARS. "The challenge is that there needs to be more expertise."

---

[7] http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html

[8] http://www.businesswire.com/news/home/20160824005973/en/Fitch-U.S.-Cyber-Insurance-Premiums-Total-1B

Expertise on cyber insurance is increasing, but insurers acknowledge that agents and brokers working with smaller businesses need to do more outreach and education for their clients.

“It can be complicated,” said Francis of Travelers. The insurer underwriting processes vary for cyber, but have become more streamlined over the years, he added.

Francis countered the contention from businesses that feel they’ve implemented all the cybersecurity they need to avoid breaches by noting that property owners still buy insurance even when they have smoke alarms and sprinkler systems to prevent fires.

“You buy insurance just in case those measures fail,” he said. “You can do all the right things but no solution is foolproof. We’ve seen cases where businesses found themselves on the short end of a cyber event.”

“I think agents are a little nervous about their knowledge of the cyber industry,” said Lucas of Erie Insurance. “Unless you’re pretty commercial-savvy, this coverage may be foreign to them.”

Erie Insurance, a smaller regional commercial carrier, writes data breach response, identity theft and computer fraud coverage for its customers—many of them mom-and-pop businesses—and is working on rolling out coverage for ransomware and social engineering.

Erie partners with CyberScout on a co-branded website dedicated to cyber risk, Lucas said, and has found that customers appreciate risk calculators offered through the firm. The calculators illustrate the risk, based on the type of data and number of records a business holds, and assist insureds in selecting appropriate coverage limits. It is helpful not only for clients, but agents as well, Lucas explained.

Policyholders have the option of embedding lower-limit cyber cover into their business owner’s policies (BOPs), or buying higher limits via standalone coverage. The take-up rate for higher limits is quite low, she added.

“We have had a few clients that have not had adequate limits and probably were surprised at how costly it was to do a response,” Lucas said. However, Erie has made outreach a focus, offering frequently asked questions about cyber and webinars for agents and clients, who they have found are more likely to ask about the coverage.

“Today’s agents face a drain on their employee’s time and resources as to where they want to focus their continuing education,” Lucas said. From an errors and omissions standpoint, agents know they need to offer cyber coverage.

“The penetration rate is very low, so there’s room to grow,” she said. “We actually feel that all of our customers have an exposure to data breach.”

Organizations do need to understand the coverage they purchase and many observers see a problem in both the variations between policies, the buyers’ grasp of their own risk, and the insurance industry’s evolving understanding of information security concerns.

“I do think it is still a little bit of a buyer beware market,” said Goodman. “It’s important to find a broker that really knows this stuff.”

He highlighted surprise potential gaps in coverage that concern smaller organizations, citing lack of payment card assessment coverage in policies that cover other fines and penalties. Some older policies might not offer third-party coverage vendors or ransomware coverage.

"I ask, how fresh is this coverage?" he said. "I really encourage people to look around, shop around until they're comfortable."

Francis reported plenty of competition for small to mid-size enterprises in the cyber insurance market, with many different product options. In return, small businesses appear to understand that buying the coverage may not be as expensive as they thought—and not as expensive as remediating a breach on their own would be.

"It's not the case that they'll have to pay what a larger company would," he said, calling coverage for breach response "critically important" for smaller businesses.

"They can comply with regulations, but almost more important than complying is offsetting the cost—particularly for forensics, which can be prohibitively expensive." Francis said. "We can all rattle off a handful of very sophisticated companies and governments that had the wherewithal and still were hit."

LIGHT ON THE HORIZON

The ability of a small business to bounce back from a cyber event depends on how well it prepares for and mitigates all types of business disruptions. Applying basic risk strategies to cyber risk and recognizing the mission-critical systems and information necessary to operate will serve any organization in good stead. The resources exist for small businesses to understand how cyber risk affects them, just as they do for fires, floods, theft, accidents, and other perils.

"Risk is risk when it comes to business," said Goodman. "They're really all connected. Before you start stressing about technical gobbledygook, start with the basics."

He added, "It's a journey, not a destination."

This is good news for small businesses. Those that have thought about their risks and worked with an IT or information security provider on continuity planning have better outcomes, according to Huntley.

"While those people are usually upset by being violated by a thief, the vast majority survive after assuming some impact," he said. "It's about pre-planning and knowing that a cyber attack might be no different than a fire in their building. Any business can do that."