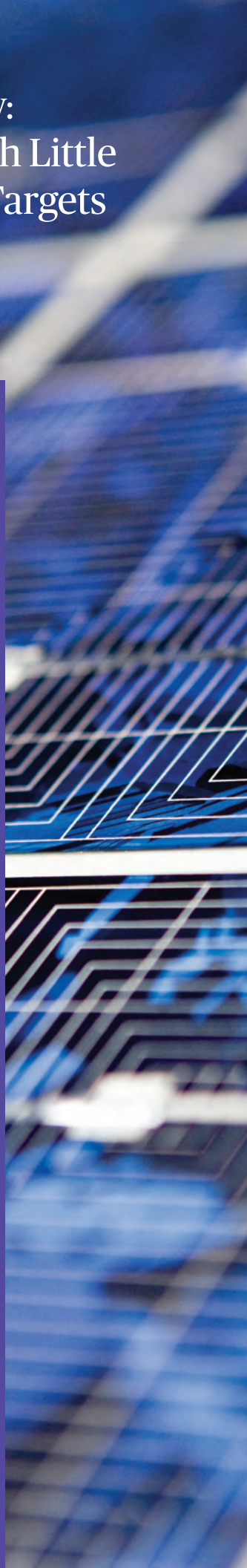
What All Cyber Criminals Know: Small & Midsize Businesses With Little or No Cybersecurity Are Ideal Targets

Authored by: Pascal Millaire, Anita Sathe, and Patrick Thielen

CHUBB®

Symantec™

COVERHOUND®



When Rokenbok Education's database was compromised by cyber criminals, the small, California-based company flat out refused to pay a hefty ransom to get it back. Instead, they went to work manually reconstituting their core systems and were back in business again four days later. That's not to say the company that designs toys to teach kids engineering skills didn't lose thousands of dollars in missed sales during the peak holiday season in 2015. But Rokenbok did fare far better than many small businesses facing similar ransomware and malware threats – among myriad other cyber risks that increasingly threaten companies of all sizes.

In fact, 93 percent of small and midsize enterprises (SMEs) that have experienced a cyber incident reported a severe impact to their business. Almost all reported a loss of money and savings. Thirty-one percent reported damage to their reputation, leading to a loss of clients, as well as difficulty attracting new employees and winning new business. And nearly half reported an interruption in service that damaged their ability to operate. In spite of those figures, less than 3 percent have cyber insurance.

What Is the Domino Effect?

Cybersecurity risks are uniquely challenging for small businesses due to the frequency with which these threats manifest into bona fide cybersecurity incidents, the severe business disruption and financial impacts they can have, and the limited resources that small businesses typically have at their disposal to respond and recover from an incident. This cascade can easily lead to bankruptcy due to a phenomenon we'll call "The Domino Effect."

The First Domino Cascade

When the websites or computer systems of SMEs are attacked and taken offline, their virtual storefronts and ability to process transactions can be destroyed. It's as if those businesses have gone out of business, even when their brick and mortar stores are still open. As a result, many customers and clients go elsewhere, and a large percentage of them never return.

The Second Domino Cascade

When attacks involve stolen personal information such as credit card numbers, a downward spiral of negative press and shaken customer confidence can lead to crippling brand damage and further customer attrition can become stampede-like.

The Third Domino Cascade

Computer ransoms can range from a few hundred dollars to six figures. While the decision to pay a ransom is typically case-specific (and officially discouraged by the FBI), there's no guarantee that, once a ransom is paid, cyber criminals will cooperate and decrypt the compromised data. Further, regardless of the type of cyber incident – whether involving ransom, malicious code, or another event, malicious or not – restoring digital data, software, and computer systems can require such a large investment of time and money that it can precipitate business bankruptcy.

The Fourth Domino Cascade

The last, but certainly not least significant possible outcome, is that SMEs may be sued for liability when an attack impacts customers, vendors, suppliers, or others. Such lawsuits are often extremely costly and time consuming to defend, regardless of the final outcome of the suit, and that's another way that a cyberattack can become an endgame event.

Significantly more than half of all cyberattacks are directed at SMEs, and that number is steadily increasing.

Why Are SMEs Targeted?

Given the all-too-common outcomes above, the logical question to ask is: Why don't SMEs do more to protect themselves with professional cybersecurity measures? There are two common reasons why they don't.

The First Reason

It is human nature to fear a risk that you or someone close to you has experienced. Although cyberattacks frequently make headlines, the big news is about big companies. The cyber threat simply does not feel real to most SMEs, but here's a stark reality: significantly more than half of all cyberattacks are directed at SMEs, and that number is steadily increasing.

What cyber criminals look for when scanning the Internet for new targets is a company that can be hacked with ease. They often accomplish this by using software that automatically scans the web and identifies companies with specific security weaknesses (e.g., outdated or unpatched software, poor password hygiene, open web ports, unencrypted data in transit, lacking

endpoint protection and the like), making the process nearly effortless for them. As a result, it's becoming increasingly likely that if an SME has a security weakness, it will be identified sooner rather than later. This is why, for cyber criminals, these businesses are the proverbial low-hanging fruit. Not only are such companies easy targets, they also offer a substantial cumulative payoff – in the form of ransom money, stolen credit card numbers, or bank account information, making it easy for the criminals to siphon off cash in a few digital seconds. As a final enticement, criminals can also avoid the increased effort and risk of hacking larger corporations or government entities. As a result, SMEs, with their low or no investment in cybersecurity measures, are actually the ideal, and subsequently the most common, target for online crimes.

The Second Reason

Large businesses spend enormous sums on corporate cybersecurity, often spending tens and sometimes hundreds of millions to institute very sophisticated, high tech defenses. SMEs face most of the same threats. However, most SMEs don't have the means to make anywhere near the investment required to implement comprehensive protection, leaving significant risk uncovered.

How Do Cyber Criminals Gain Entry?

There are all kinds of ways for criminals to access an SME's website or internal server. Here are the four most commonly used methods of attack:

- **Attacks on Physical Systems:** Cyber criminals can access an SME's internal server or hardware through insufficiently protected electronic devices that have legitimate access, such as laptops, desktop computers, tablets, and removable media like USB devices. They can also gain entry through a server room break-in or from internal network hacking, which then enables monitoring by criminal third parties. This can often be triggered by something as innocuous as plugging an infected USB drive into a computer or device that is connected to an internal network.

- **Authentication & Privilege Attacks:** Criminals can gain access to sensitive data when passwords used by those with legitimate access are very weak and easily hacked, or when some employees who are allowed access to information stored deep within the company's online data storage take a lax approach to password precautions. There is a vast repository of billions of compromised user ID and password combinations available today on the dark web. Given how frequently individuals reuse ID and password combinations, it may not be difficult for a cyber criminal to find valid credentials for a single employee in order to gain access. Another source might be deliberate sabotage by a disgruntled employee, or even allowing unnecessarily broad access to sensitive data by rank-and-file employees, which is known as "privilege creep."

- **Loss of Service:** There are two ways to lose service, meaning an SME's site cannot be accessed due to Internet service issues. One involves human action and the other involves service failures that lead to a lack of power or an inability to connect to the Internet. Distributed Denial of Service (DDOS) attacks typically involve flooding an SME's Internet service provider with so much online traffic that it suffers bandwidth exhaustion and stops working. Non-deliberate attacks involve single point of service failures, occurring because of an overdependence on a system or service provider without adequate redundancies. These types of cyber incidents may be caused by natural disasters or by simple failures of technology.

- **Malicious Internet Content Attacks:** This is the type of attack that Rokenbok experienced. In their case, their system was infested with ransomware, a form of malicious malware or software that allows criminals to reach in and lock up a company's database by encrypting everything and offering the decryption key for a ransom payment. There are many other kinds of content attacks. One of these, called phishing, involves sending an employee an email with a link that, when clicked on, automatically downloads malicious software onto the computer that employee is using. These are often combined with social engineering techniques to make these emails seem as if they are sent from a coworker or other internal source. Others involve so-called viruses, Trojans, and worms, along with "drive-by downloads" and web application attacks.

How Can SMEs Protect Themselves from Cyberattacks?

Although stopping cyber criminals from accessing SME funds and data may seem like a formidable task, there are a handful of simple measures that companies can use to create their own cyber risk management program and limit their exposure. After first ensuring that their antivirus and other security software is always kept up-to-date, and asking a cybersecurity consultant to identify high risk areas, SMEs can take the following five risk mitigation steps:

- **Develop and Enforce a Formal, Written Password Policy:** One of the quickest and easiest ways for cyber criminals to access SME assets is by walking through the virtual "open door" that employees provide when using weak or reused passwords. To correct that situation, it's a good idea for SMEs to establish a written password policy requiring strong passwords (e.g., a mix of letters, numbers, and symbols) that are frequently changed. Passwords should also be changed automatically or accounts marked inactive when employees leave the company in case a disgruntled employee later decides to harm the business, using his former password as access. Utilizing good password management software can assist in this critical step.

- **Educate All Employees Regularly on Cybersecurity Vigilance:** By the same token, SMEs should inform employees of the role they play in preventing a cyber breach. It's all too easy for malicious software to hitch a ride into the company server when company laptops or other devices are used offsite and later connected to the internal network. The best ways to establish positive and secure habits within your

Although stopping cyber criminals from accessing SME funds and data may seem like a formidable task, there are a handful of simple measures that companies can use to create their own cyber risk management program and limit their exposure.

company's workforce is with regularly scheduled training and education. Of equal importance is a policy that restricts sensitive information by only allowing trained executives, or those who require that information for company operations, to have access.

- **Update IT Equipment & Deploy Security Software:** Another area of easy-to-fix potential cybersecurity problems involves IT equipment. Outdated operating systems and computers can be a risk, as they are easily breached by criminals, being vulnerable to more sophisticated hacking techniques and newer forms of malware. At the same time, it's important for SMEs to monitor those who have legitimate access to their computer network, as well as to monitor the network itself, looking for abnormal activities that - if caught quickly - can limit company damage. Although SMEs do not typically have information security experts within their organization, they can access basic downloadable software offerings that deploy some of the same technology solutions used by Fortune 500 companies within minutes.

- **Create a Cyber Incident Response Plan:** While most SMEs do not have the internal expertise to successfully resolve a major cyber breach incident, there are less damaging incidents they can resolve with a dedicated and prepared team of cyber responders consisting of both employees and outside service providers. The advantage of an entire team working on an incident is that the response time will generally be shorter, and resolution – if it's within the team's capabilities – can occur more quickly.

- **Purchase Cyber Insurance:** In addition to the above steps, SMEs can more fully protect their assets and the viability of their businesses by purchasing cyber insurance. The cost of insurance will always be far less than the cost of shutting down a business in the wake of one or more cyberattacks. And cyber insurance can be prepackaged with some of the services mentioned above.

Why Is Cybersecurity Essential to SME Survival?

Unlike Rokenbok Education, most SMEs are not capable of doing what this specialty toy company did – restoring their core systems internally. In fact, the vast majority would not even know where to begin. But since statistics show that significantly more than half of all cyberattacks were directed against SMEs three years ago, and that this percentage is likely to increase, the risk to these companies is too great to ignore.

And yet, because of a general misperception about the enormity and severity of that risk, less than 3 percent of all SMEs have cyber insurance, compared to 40 percent of all big businesses. In fact, as a group, SMEs tend to devote inadequate resources, time, and funds to cybersecurity, with 67 percent having no data security policies. Of the 33 percent that do, 87 percent have no formal written policy in place. Should they become the target of a cyberattack, their vulnerability is only increased by their inadequate investment in cybersecurity and the fact that most also lack cyber insurance. It's no wonder that of those SMEs that suffered a cyber breach, 93 percent experienced a severe business impact.

In today's world, it behooves SMEs to ensure their company's future by incorporating common-sense cybersecurity measures. Fortunately for them, although cybersecurity has historically been a highly technical and costly challenge, such simple measures as those mentioned above can provide effective protection at a low level of cost and complexity.

About the Authors

Pascal Millaire is Vice President and General Manager, Cyber Insurance at Symantec. In this role, he is responsible for partnerships and product innovation at the intersection of security and insurance, as well as for creating underwriting and aggregation modeling tools for cyber insurers.

Anita Sathe, Chief Strategy Officer at CoverHound, is an insurance professional with more than 13 years of experience in the insurance industry. She holds a breadth of experience ranging from product and underwriting strategy to technology implementation and actuarial analyses. She is one of only twelve to hold actuarial fellowship credentials across P&C, Life and Health Insurance. Prior to joining CoverHound, Anita was a Senior Manager with Deloitte Consulting.

Patrick Thielen is a Senior Vice President with Chubb and is product lead for the Cyber and Technology E&O lines of insurance for North America. He is currently leading Chubb's efforts to expand the availability of cyber coverage for small businesses. Mr. Thielen can be contacted at Patrick.Thielen@chubb.com.

Endnotes

All data is derived from research completed by the **Janet & Mark L. Goldenson Center for Actuarial Research at the University of Connecticut.**

To download the full report, visit http://goldensoncenter.uconn.edu/cyber-risk/.

Chubb. Insured.℠

www.chubb.com/us/cyber