Cynet

THE STATE OF DENIAL

Thoughts of a former corporate CISO (turned vCISO) on mid-sized organizations' false sense of security and how they can efficiently confront their threat landscape.

By: Wade Richmond

Wade Richmond worked as the full-time Chief Information Security Officer for enterprises such as BJ's Wholesale Clubs, Ahold USA, Sensata Technologies, GTECH Corporation, Citizens Financial Group and CVS Pharmacies. In these roles, he was responsible for providing leadership and direction to all cybersecurity and IT risk efforts associated with information technology applications, communications and computing services.

INTRODUCTION

Cyberattacks have become a ubiquitous problem--regardless of company size or location. In fact, smaller enterprises have become a bigger target due to poor resourcing and skill set. According to a Verizon report, 61 percent of data breach victims were small businesses. In today's threatscape, the amount of effort required to get an effective defense up and running has become unattainable by most enterprises--large or small. Many organizations have neither the time nor the resources to implement technology to help automate some of these key functions. So they are trapped on the hamster wheel of pain, reacting without sufficient visibility, and without time to invest in gaining that much-needed visibility into threats.

LIVING IN THE STATE OF DENIAL

CYBER ATTACKS ARE EVERYWHERE. OR NOWHERE. DEPENDS ON WHO YOU ASK.

From reading headlines, its clear cyber attacks are a reality for many large firms. But what about smaller, resource-constrained companies? They aren't in the headlines--so somehow they're exempt from attacks. The reality, as Verizon points out, is that 61 percent of data breach victims were small businesses. Jeremy Grant, an advisor at the Department of Commerce's National Institute of Standards and Technology, says in the past two years he has seen "a relatively sharp increase in hackers and adversaries targeting small businesses."

Moreover, many smaller firms are essential parts of a supply chain. Clever attackers are going after supply chain partners since they are easier targets. In 2018, US intelligence warned small companies about supply chain dangers."Software supply chain infiltration is one of the key threats that corporations need to pay attention to, particularly how software vulnerabilities are exploited," William Evanina, the NCSC's director and the US's top counter-intelligence official said. "To get around increasingly hardened corporate perimeters, cyber-actors are targeting supply chains. The impacts to proprietary data, trade secrets, and national security are profound."

The lesson? The risks are the same. So, what is different? Smaller firms don't have the insights or funding to support a program. But, like Calvin points out above, many live in a state of denial. This is driven by a set of wrong beliefs:

1. I'm small and not important enough to hack.
2. I don't have what anyone wants.
3. I can't stop them even if I wanted to.

THE WAKE UP CALL

THE TYPICAL DATA BREACH COSTS SMALL BUSINESSES $117,000

The above false beliefs give comfort. Until they don't. The wake up call for little organizations? Primarily ransomware and ransomware or data theft breaches with implications most small organizations cannot afford. This could be directly, because of the entailed costs, or indirectly, if the breached organization operatesas part of the supply chain of a bigger organization, in which case it could get listed out, materially impacting its business operations.

The typical data breach costs small businesses $117,000, which can take a big chunk out of your operating budget. Plus, you have to account for the cost of disaster recovery, informing consumers about the breach, paying for security audits, and dealing with the reputation loss.

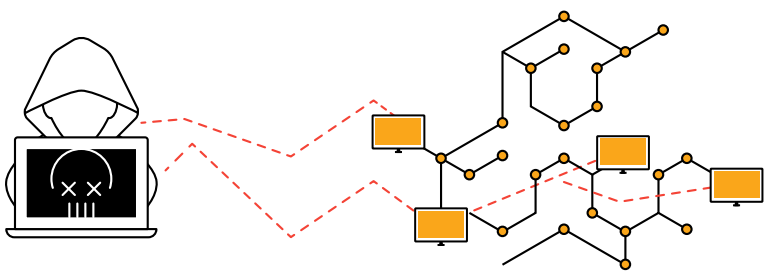
Then, to make things worse, about 60% of small businesses never recover from a cyberattack, instead going out of business. Understanding and proactively addressing small company cybersecurity threats puts you in a position to protect your business.

ATTACKING SMALL BUSINESS: A HACKER'S PERSPECTIVE

But let's look at the question from the attacker perspective. Cyber attackers have a whole world of organizations to choose from. Logically, the attractive targets are the ones you can make profit from. Larger firms tend to have more robust defenses in place. For that reason, attackers pick the little guys with little defense. They want to find the homes with no alarms on the house.

TODAY'S ATTACKS BROADLY TARGET ENDPOINTS AND NETWORKS.

At a minimum, a comprehensive defense requires at least a firewall, AV, SIEM, EDR, analytics, and much more. Yet many smaller firms lack basic controls. Small and medium enterprises, according to the BBB, rely mostly on firewalls (76%) and AV (81%)--but little else. In fact, the most common cyber defense measure behind technology, according to the same BBB survey, is employee training at 47%. Worse, existing tools are noisy and provide a siloed view: organizations have point tools in place that were purpose-built to solve a specific problem, but were not purpose-built to address cyber risk in a holistic way. Existing security point tools flag threats and anomalies but fail to look at the enterprise as a whole, understanding the hundreds of activities that take place each day and correlating it with a firm's intrinsic risk.



THE RESULT?

CONSIDER THESE CYBER INSECURITY REALITIES:

1.

Cybersecurity Ventures expects ransomware damage costs will rise to $11.5 billion in 2019 and that a business will fall victim to a ransomware attack every 14 seconds.This is up from 2016 levels where ransomware occurred “just” once every 2 minutes - a 300% jump.

2.

One in thirty emails are malicious.

3.

The typical dwell time is 146 days.

4.

Automation and bots characterize today’s security threat. SMB websites are attacked, on average, 44 times per day--almost twice an hour.

5.

About 45-50% of the workforce are employed by smaller firms. About half have been hacked.

These are just a few hard facts. Consider the “soft” side of attacking smaller firms:

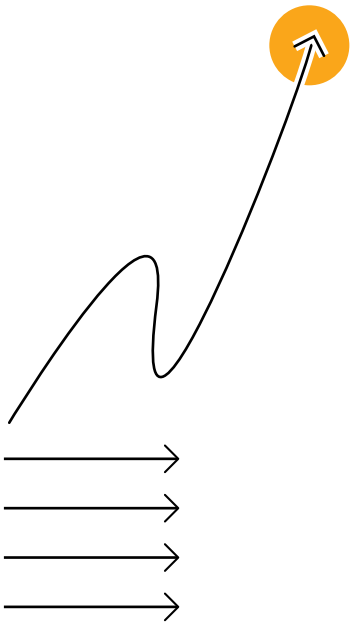
A. Attackers see their job as a full-time role and spend close to 100% of their focus on bad stuff to perfect their craft.

B. Nation states, criminal gangs and amateurs are all going after smaller firms.

C. Attackers live in a constant cycle of trying to improve and fine tune malware.

ESCAPING THE HAMSTER WHEEL

WITH 60% OF SMALL FIRMS GOING BANKRUPT POST A SIGNIFICANT CYBER-ATTACK, MAKING DEFENSE A PRIORITY SHOULD BE, WELL, A PRIORITY. WHAT DO YOU DO?



RECOGNIZE CYBER IS A LIFESTYLE CHANGE.

When someone experiences a heart attack, they undergo a lifestyle change marked by better diet and exercise. Others make that change proactive, trying to avoid the heart attack. The same holds for cyber security and breaches--only you can clean up your cyber hygiene. Here are some basic things any small firm can do:

WASH YOUR HANDS

Like washing your hands regularly with soap and water, performing backup and storage to a managed location offsite is essential.

GET SOME OUTSIDE HELP TO CLEAN UP

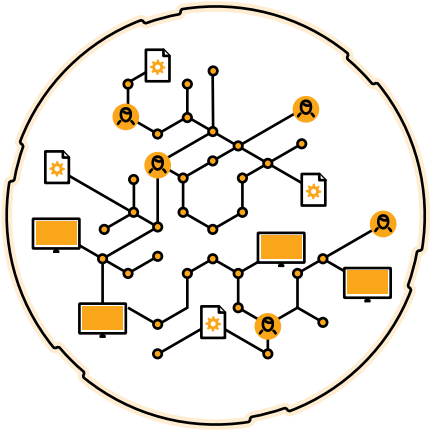
- Cyber insurance policies often come with access to pros who can help not just advise you on how to recover your business--but importantly, help you prevent issues.
- Figure out what you don't need to keep onsite. Others do a much better job of security if they outsource. Identify trusted cloud solutions, such as Office 365 or Google Mail. Why run in-house email?
- Perform regular patch management. Patching is basic and extremely rewarding in terms of reducing your exposed attack surface.

GET IN CONTROL OF CHANGE CONTROL

When things change, you open yourself up to security problems. Ensure that any changes made are tested and their impact is understood with proper change control procedures.

HAVE A CYBER PLAN

Organizations need a plan. After an operation, the surgeons' job isn't complete--they need to provide patients with a plan to get back to normal. In cyber, use NIST or some framework to identify, protect, detect and respond, as well as recover after an episode.



MAKE CYBER A DIFFERENTIATOR.

If you're part of a supply chain, make cyber a BIG part of your RFP response. For example, show some of the following:

- You have a virtual CISO. Many firms can't afford a full-time employee--a number of "consultancies" offer a virtual CISO to work part-time and direct risk management, recommending a defense strategy and helping with ongoing maintenance.
- Detail your plans to improve your organization's cyber posture and include technical steps you're taking to stay ahead.
- Demonstrate your organization's current defense approach showing tools and capabilities that include firewall, AV, training and other key tools.
- Implement breach protection technology that provides the fullest coverage of your environment--files, users, network and hosts.

If not part of a supply chain, the challenge is more difficult. In this case, smaller firms should articulate how cyber defense is a part of customer loyalty--protecting their private data is key. By taking this simple step, you show customers how you're focused on doing the right thing. The good news? As cyber crime becomes more public, making the case for a stronger cyber security posture will become easier. Also, the regulatory environment is changing to require more cyber controls.

INCORPORATE CYBER INTO DISASTER AND BUSINESS CONTINUITY MANAGEMENT.

Many small firms already perform disaster and business continuity management. The goal is to limit risk and get an organization running as close to normal as possible after an unexpected interruption. As cyber threats increase and the tolerance for downtime decreases, business continuity and disaster recovery gain importance. These practices enable an organization to get back on its feet after problems occur, reduce the risk of data loss and reputational harm, and improve operations while decreasing the chance of emergencies. The cyber-resilience trend of combining business continuity and disaster recovery with cyber reflects the growing recognition that business and technology executives need to collaborate closely when planning for incident responses for cyber security.

FINAL THOUGHTS

Despite the billions in venture money that has poured into security startups, the majority of new vendors focus on larger enterprises with bigger budgets. Today, big companies with million-dollar cyber budgets assemble a defense-in-depth strategy to block and mitigate a wide variety of attacks such as phishing, ransomware, DDoS, APT and so on. But little guys are left behind. By following the steps described in this paper, small companies can begin to tame the cyber security beast.

ABOUT WADE RICHMOND

Wade Richmond is the founder and CEO of CISO ToGo, a company that is the result of a long-held understanding that the growing level of global cybersecurity threats are no less impactful and critical for small to mid-sized organizations, than to large enterprises.

Prior to founding CISO ToGo, Wade worked as the full-time Chief Information Security Officer for such large enterprises as BJ's Wholesale Clubs, Ahold USA, Sensata Technologies, GTECH Corporation, Citizens Financial Group and CVS Pharmacies. In these roles, he was responsible for providing leadership and direction to all cybersecurity and IT risk efforts associated with information technology applications, communications and computing services.

To learn more, visit: www.ciso-togo.com

ABOUT CYNET

Cynet was founded by an elite group of seasoned security entrepreneurs, researchers and SOC practitioners to build a single, autonomous platform centralizing all aspects of breach protection. Cynet couples unmatched prevention, detection and response capabilities with extreme ease of operation, providing protectionto all organizations, regardless of the size and prior skill of their security teams. Cynet is the trusted partner of small to large enterprises worldwide, guiding them in their journey towards fully automated threat discovery and mitigation.

To learn more, visit: www.cynet.com