Securing Success: An Entrepreneur's Guide to Cybersecurity

Understanding the threat landscape and taking proactive steps to protect your business.

COMCAST BUSINESS | Entrepreneur

Table of Contents

CHAPTER 1

Introduction: Why Entrepreneurs Are Prime Cybercrime Targets

The digital landscape is crowded with a growing number of sophisticated threat actors who will attempt to access and exploit a company's data. For entrepreneurs, one thing should be clear about the targets of cyberattacks: being a startup or small company doesn't make you a less tempting target for cybercriminals.

Almost half of all companies (48%) reported a cyberattack in the past 12 months, up from 43% last year, according to Hiscox's Cyber Readiness Report 2022. Almost a fifth of companies (19%) reported a ransomware attack.

These numbers paint a clear picture of the risk that entrepreneurial companies face as cyber threats become more sophisticated. Cyber thieves know that even the smallest companies can have vast amounts of valuable data, and that smaller firms often lack sufficient cybersecurity measures and resources, leaving them more open to attack.

"Entrepreneurs who are just starting out are focused on their core business," says Sukhjinder Singh, Senior Director of Product Management at Comcast Business. "At the early stages, many are not thinking about risk, and they may consider cybersecurity an ancillary expense if they don't understand the true risk they face."

As threats grow, so does the need to get ahead of cyber

threat actors. This paper will explore the key elements to proactive protection—building a cybersecurity policy that ensures your company is focused on security best practices, having the right technology to help protect your data, providing effective employee training and education to be on guard for cyberattacks, and creating an effective incident response plan.

How Bad Actors Get in the Door

Many cyberattacks rely on psychological manipulation, tricking targets into providing confidential information or taking actions that can unknowingly put their data at risk. This technique is called social engineering.

The most common form of social engineering in cybercrime is phishing, which preys on the fear, trust, and curiosity of everyday users. Phishing leverages fake messages like emails, invoices, or shipping notifications to lure an employee to click on a corrupted link, which in turn downloads a piece of malicious software onto the company network.

Phishing is a common method for initiating ransomware attacks. In these scenarios, software will locate and encrypt a company's data, making it inaccessible unless they pay a ransom for a decryption key. According to the Identity Theft Resource Center, 44% of SMBs hit with a ransomware attack paid $250,000 to $400,000 for recovery costs, and 16% paid up to $1 million. One in six companies that suffered an attack struggled to survive.

Phishing can also secretly install a bot on a target network, allowing cybercriminals to remotely access, control, or extract data from devices on the network. These bots can steal vital information, launch Distributed Denial of Service attacks (DDoS), which flood a network with so much traffic it effectively shuts down, or engage in other malicious activities.

Types of Cyber Attacks

Cybercriminals attack small businesses in a range of different ways. Here are four of the most common techniques.

Phishing is the practice of sending emails or other messages purporting to be from reputable companies to trick someone into revealing confidential information, such as passwords and credit card numbers. Threat actors have many clever ways to make recipients think they are a trusted partner, customer, or even the employee's boss. For example, they might use email addresses that are similar to a legitimate company but use a different top-level domain, say verifyppal.xyz instead of verifypaypal.com.

Malware is a general term for a variety of malicious software that cyber threat actors use to steal data or destroy computer systems. Common types of malware include viruses, worms, Trojan viruses, spyware, and adware.

Ransomware is a form of malware that prevents users from using their systems or personal files. Once the hackers encrypt the systems, they demand a ransom to provide a decryption key so the infected company can access their data again.

Distributed Denial of Service Attacks (DDoS) flood critical computing resources and networks with so much traffic that employees, customers, and other intended users are unable to use machines or networks.

CHAPTER 2

Building a Cybersecurity Policy

Security should never be an afterthought. The businesses that are better able to protect against cyber threats have cybersecurity baked into their processes and culture. Having policies and procedures that codify key elements of your approach to cybersecurity will help ensure data security remains a top-of-mind priority for everyone at your company.

Every company needs a unique cybersecurity policy, stemming from an evaluation of specific risks and an accounting of data that requires protection. The first step toward creating a robust cybersecurity policy is a strong understanding of key assets and vulnerabilities. A cybersecurity threat assessment can help you identify your vulnerabilities and create a plan of action. In developing a cybersecurity policy, you should consider things like the types of data you manage, how the data is handled, who has access to it, and under what circumstances they have access.

The Federal Communications Commission (FCC) offers the Small Biz Cyber Planner 2.0, a tool that can help small businesses build a custom strategy and cybersecurity plan based on their unique business needs. The planner explores topics the policy should address, such as network security, website security, email, mobile devices, and facility security.

CHAPTER 3

The Right Technology

Given the complexity of cyberattacks, a strong defense should provide a good mix of security tools that fortify your network end-to-end.

"There is no single silver bullet when it comes to cyber defense, so you need to develop a defense-in-depth strategy," Singh says.

A defense-in-depth strategy uses a variety of security tools—including threat monitoring, firewalls, and anti-virus—along with good online hygiene practices.

Tools to Keep You Protected

Threat monitoring tools actively block malware, ransomware, phishing, botnet infections, and other malicious threats. They also prevent employees and guests on your network from accessing compromised sites and infected links, helping to prevent downloads of harmful software.

Threat monitoring should cover every connected device on the network. After all, culprits only need to find one point of entry to cause havoc. It's also imperative that the tools automatically update to monitor for the latest threats, as new attack methods are developed and launched daily. According to the 2023 Comcast Business Cybersecurity Threat Report, last year, over 26,000 new application and infrastructure vulnerabilities were added to the National Vulnerability Database, the U.S. government repository of standards-based vulnerability management data.

"There are always going to be these tried-and-true methods that cyber threat actors have used," explains Singh. "At the same time, there will also be new threats coming down the pike. And if you're not aware of these threats, or don't have partners who are aware of them, you can have blind spots in your security."

Anti-virus tools, another key type of security tools, detect and block malicious files. However, many anti-virus tools only block malware they recognize based on signatures that have been written into the anti-virus software. They are an important piece of the puzzle, but given their limitations need to be deployed in concert with threat monitoring.

Firewalls, a third common cybersecurity technology that many businesses employ, allow only authorized traffic or content on a network using configured controls, such as denying access to IP addresses that are known to deliver malware. Even if the malicious payload is delivered, firewalls can prevent it from communicating with control-and-command servers, reducing the damage the malware can do.

Companies can benefit from using technology that provides security and takes manual chores off employees' plates. One crucial area for automation is patch management. Software and system updates often close previous security loopholes. By automating software updates, small businesses can ensure they have the latest software or system version, reducing the number of known vulnerabilities that are available to hackers.

Finally, password management tools can generate strong passwords and store them securely for easy access. This helps provide a higher degree of protection to your network, without requiring employees to create and remember complex and effective passwords.

Using technology that removes the steps that employees need to take allows you to focus on the areas where you can have the greatest impact on reducing cyber risk, such as employee education and training.

"Security is such a complex story in itself that it's great if you can find tools that are easy to manage or have a partner that can help manage these cyber risks, so you can focus on growing your core business, especially in the early stages of your company when time and resources are precious," Singh says.

"Security is such a complex story in itself that it's great if you can find tools that are easy to manage or have a partner that can help manage these cyber risks, so you can focus on growing your core business, especially in the early stages of your company when time and resources are precious."

—Sukhjinder Singh, Senior Director of Product Management, Comcast Business

CHAPTER 4

Employee Education and Training

People—even well-intentioned employees—can often be the biggest cybersecurity vulnerability for small businesses. More than one third of security incidents (34%) were caused by non-malicious user error, according Foundry's 2022 Security Priorities Report. And these incidents can be costly and time-consuming. The Ponemon Institute's 2023 Cost of Insider Risks Global Report notes that it takes 86 days on average to contain an insider incident.

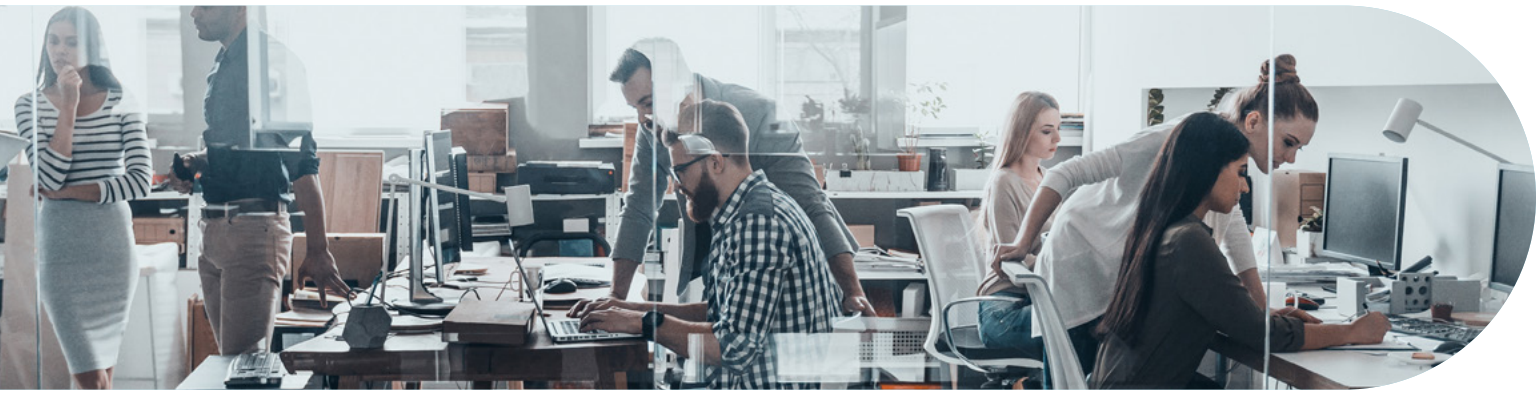
One of the strongest lines of defense against cybersecurity riskis keeping employees educated on current threats and steps they can take to avoid unwittingly becoming an aid to threat actors.

Cybersecurity training can never happen too early, or too often. If you begin cybersecurity training when you onboard a new employee and maintain an ongoing training cadence, it will clearly demonstrate how dedicated the business is to keeping its data and systems safe. You should steep new hires in your security policies and best practices from day one.

Areas to Cover in Cybersecurity Training

- **Learning the basics and be skeptical.** It's tough to spot a suspicious email without vigilance. Employees should know what to look for when it comes to suspect communications, even if they appear to be coming from a co-worker or manager. They should similarly learn to be careful about what information they share on social media, since threat actors often look at these feeds to gather information to personalize phishing schemes.
- **Maintaining mobile security measures.** Employees should understand that using mobile phones could increase the risk of a phishing attack. URLs may be shortened or less visible on a mobile web browser, making it difficult to assess their legitimacy. Employees on the go may also tend to be less focused on security. However, rigorous training that educates employees about such risks can help them remain mindful of cybersecurity best practices.
- **Developing good online habits.** As cyberthreats are constantly emerging and changing, employees should receive continual training on new types of attacks and scams as well as online hygiene, which includes best practices when using computers and other internet-connected devices. If you don't have someone on staff who can provide this function, consider bringing in an outside consultant or accessing free resources online.
- **Understanding business impact.** You want employees to understand the consequences to the company if their behavior leads to a data breach or ransomware attack. But also point out the personal benefits they'll receive from following sound practices. Good cyber practices protect their personal information just like it protects company information.

Cybersecurity should be everyone's business. Encourage employees to report attacks and threats, so you can keep your team in the loop about new threats.



CHAPTER 5

Creating an Incident Response Plan

While maintaining strong defenses for your network is essential, no defense is completely foolproof.

It's essential to prepare to respond quickly and efficiently in the case of a breach to reduce damage. Even for small businesses, it's critical to build that plan ahead and develop an incident response plan. The plan helps guide your company's response before, during, and after a confirmed or suspected security incident.

The plan should be as prescriptive as possible, starting with how an incident is defined. Some companies might consider an attempted, but unsuccessful hack, as an incident. Others may not. Based on your specific needs, your incident response plan should determine what circumstances require a coordinated response across your organization.

The value of a well-thought-out incident response plan is that it allows everyone in the company to know what they are supposed to do in the moment, rather than having to scramble to figure out what to do when tensions are running high and critical systems may be unavailable.

Well before a data breach occurs, every employee should know what their role in an incident response will be. The plan should designate cross-functional team members who should respond in the event of a breach, as well as any cybersecurity solutions providers and consultants who will be immediately available to assist. In addition to knowing their roles, it's critical that every employee has the correct access and authority to carry out their responsibilities during an incident response.

The steps for recovery in the plan also should be detailed and clear, accounting for different scenarios, such as what should be done if an attack occurs after hours or when response team members are on vacation and not reachable.

Responding effectively and quickly to an active cybersecurity threat can make a real difference—in revenue loss avoided, reputational risk averted, customer data protected, or even the survival of an organization. By thinking through worst-case scenarios well in advance and documenting actionable steps to take during an incident, you can help mitigate or avoid damage altogether.

About Comcast Business SecurityEdge™

Comcast Business SecurityEdge™ helps protect users and their connected devices against threats such as malware, ransomware, phishing, and botnets with advanced global threat intelligence that refreshes every five minutes. Monitoring activity can be done in real-time on a personalized dashboard using a single app. The customizable solution allows you to easily set web filters, block pages, manage network access, and schedule regular reports.

Learn more about Comcast Business SecurityEdge™ ***here***.

COMCAST
BUSINESS