Lenovo™

GUARDING THE GATES

BUILDING THE RIGHT SECURITY PLAN FOR YOUR BUSINESS

Powered by Intel®
Intel Inside®. Powerful Productivity Outside.

1. Introduction: You’re Not Too Small To Be At Risk

News reports sound regular alarms about massive data breaches in which millions of people’s personal and financial data is captured in a single online attack. As the owner of a small or midsize business, you may breathe a sigh of relief at the thought that your company is too small to be the target of hackers. But that’s a dangerous misconception—one that could cost you your data, your reputation, and even your ability to remain in business.

The reality is that, for a variety of reasons, small business owners are at increased risk of being the victims of cybercrime. Seeing beyond the headlines and understanding the current landscape can help prepare you to protect your company from adding its name to the list of small businesses that have suffered an online attack.

2. Surveying the Hacker Horizon

One challenge is keeping track of cybercrime trends and recognizing the most prevalent current threats. A tactic known as “spear-phishing” is one example. You may not know the term, but you’ve almost certainly seen examples of it in your inbox. And Symantec, Inc. reports that 91 percent of cyberattacks are launched via spear-phishing emails.

To launch a spear-phishing attempt, cybercriminals first learn something about you and your business, such as the identity of your commercial bank, credit card company, or vendors. They obtain that by hacking into a network or by culling information that you or an employee posted on social media or other sites. Armed with these details about your company, they contact you with an email that at first glance looks legitimate: a notice that claims your account is past due or that the order you placed be fulfilled until you provide certain information. You’re urged to click on the link provided to take care of the matter immediately but the set-up is a sham, and if you respond in a panic, you can end up handing passwords, account information, and other key data to criminals.

According to the 2016 Internet Security Threat Report, published by Symantec, sole proprietors and companies with fewer than 250 employees were targeted in just 18 percent of spear-phishing attacks in 2011. By 2015, however, they were the target of 43 percent of those attacks.

Another threat is ransomware, which encrypts your data, blocks your access to it, or locks down your system entirely; you then receive a demand for money to get your access restored. It relies on a form of malware, the umbrella term for software installed on your computer without your permission or knowledge. And it can stop companies in their tracks—or force small business owners to choose between paying vast sums or losing their enterprises. “In 2014, more than 1,800 complaints were filed regarding ransomware, resulting in a loss of more than $23 million,” the FBI reports. “In 2015, that number grew to more than 2,400 complaints, with a reported loss of more than $24 million.”

To receive more articles like this, register for our small business updates here.

3. Fewer Resources, Lower Defenses

As these statistics demonstrate, when it comes to security, you're not paranoid; cybercriminals really are out to get you. "Given their role in the nation's supply chain and economy, combined with fewer resources than their larger counterparts to secure their information, systems, and networks, small employers are an attractive target for cybercriminals," the U.S. Small Business Administration notes. And the problem intensifies among those small companies that "lack sufficient resources or personnel to dedicate to cybersecurity."

The risks can increase if you work in—or have a connection to organizations that work in—ahigh-profile industry, says Larry Clinton, president and CEO of the Internet Security Alliance, a multi-sector trade organization focused on cybersecurity. To illustrate, he tells an incredible, yet true, story: "There was a defense facility that had very good cybersecurity. Sophisticated hackers wanted to get at it but couldn't. They found out that the employees at this secure facility liked to order lunch from the local Chinese restaurant, which had an online menu. So they loaded malware onto the Chinese menu and through that, got into the defense facility."

4. Cybersecurity and the Supply Chain

That incident points to the importance of thinking about cybersecurity in the context of your entire supply chain. Hackers may target your computer or network for your customer data, business plan, or proprietary intellectual property. But others may identify you as a conduit for gaining access to your vendors, corporate clients, or investors, says Sanford Moskowitz, chair of the Global Business Leadership Department at St. John's University/College of St. Benedict and author of Cybercrime and Business: Strategies for Global Corporate Security.

With that in mind, small business owners must "dominate the supply chain as best they can" by seeking information about cybersecurity quality when they assess any additions to the supply chain, he says. "Even if you have an excellent security system, a supplier that gives you good prices could be a disaster if you don't have control over that supply. It's got to be another factor in how you choose your suppliers and decide how your supply chain will be structured."

His research has identified another risk: companies that organize their departments and divisions into silos that impede communication about problems. While your own company may be too small for that kind of internal structure, it's worth keeping in mind if your clients include individual divisions of larger corporations.

Sensitivity to these issues will help to protect your company financially, but it could have an even greater impact on your reputation, Moskowitz notes. As a small player, you need to be known for reliability and security, and damage to your track record in data integrity could be devastating. On the other hand, being known as meticulous about security could give you an additional selling point and create a competitive edge.

5. Small Business Security Strategies

"Everything in security comes down to a risk assessment," says computer security expert Chuck Easttom, author of 20 books, including Computer Security Fundamentals. "You have to look at your organization and the threats to you. Decide what's really important to you in doing business, and focus your security efforts there."

Unless you're confident of your technology expertise, you may want to engage a consultant to assist in securing your company's electronic assets and minimizing its risks. Look for someone who can offer references and who has experience working with companies that have some parallels to your business. That can mean similarities in your industry, the verticals you serve, the way you do business, a comparable customer base, or even similar problems you just want some indicator that the consultant is well positioned to address the issues your company faces.

To receive more articles like this, register for our small business updates here.

At the same time, there are steps you can take on your own, such as making data backup a part of your daily routine. While automated backup is the easiest option, Steve Durbin, managing director of the Information Security Forum Limited, recommends doing a physical backup to an external hard drive, too. Multiple backups—known in the industry as redundancy—increase your chances of emerging unscathed if you're subjected to a ransomware attack or if you need to restore your data following a system recovery (a means of starting from square one if your computer suffers a serious operating error).

Durbin knows of a case in which ransomware affected not only the target computer but also its auto backup files. "Fortunately, the cloud provider had a 30-day rollback," he says. "But think about the amount of information you're pulling together in just a day. It's huge. So external backup is really fundamental, irrespective of whether you're using the cloud, and irrespective of all the auto backup systems that you've got on your device." Unplug the external hard drive from the computer after you've backed up and shut down so that hackers can't access the external drive.

6. Conclusion: It's Not "Set-It-and-Forget-It"

Once you have a plan in place, revisit it as you hit milestones that may change the security landscape for your company. "The general guidelines for revisiting your plan would be: if you significantly alter your network or IT infrastructure; or if you change anything, such as a new operating system, a new version of Windows, or a new router, so that your old measures may not still be applicable," Easttom says. In addition, although physical expansion is not generally a trigger, "moving into a new line of business or adding online features requires a second look to check whether security measures are still adequate."

By making a commitment to cybersecurity best practices, you optimize your company's ability to discourage and withstand online attacks. It's one of the best strategies you can use to protect your customer relationships, your business intelligence, and your prospects for achieving sustained performance, profitability, and growth.

Looking for more ways to protect your business? Consider biometrics hardware features, like the ones found on the ThinkPad X1 Carbon, as well as online backup services, like those offered by Lenovo.

To receive more articles like this, register for our small business updates here.

AN ANTI-CYBERCRIME CHECKLIST

TAKING THESE STEPS CAN HELP YOU PROTECT YOUR DATA, NETWORK, AND BUSINESS

Powered by Intel®
Intel Inside®. Powerful Productivity Outside.

□ 1 Establish a formal Internet policy. Put it in writing, and be sure that it covers privacy controls for handling customer data, addresses the use of personal devices, and provides guidelines for employees' social media use on computers or other devices used for work.

□ 2 Train your employees. "The number one vulnerability for cybersecurity is always people," Clinton says. "There's a whole range of inexpensive training that you can give to your employees. It doesn't have to be a big, complicated thing."

□ 3 Configure your vendor security updates for automatic installation, and upgrade your operating system as new versions are released. The same approach applies to keeping your antivirus and security programs up to date.

□ 4 If you're using cloud storage, make sure you know about the service provider's security measures and are satisfied with the level of protection they provide.

□ 5 Use password protection on sensitive or valuable data. This ensures that the files can't be opened except by someone who has the password. Clinton recommends using a service to manage and keep track of all those passwords.

□ 6 Consider encrypting your most critical information. Encrypted material is "scrambled" before it is stored as an extra measure of protection against hacking. It's more complicated to use than password protection and best employed only where that level of security is warranted.

□ 7 If you have a mobile or remote workforce and employees frequently need to access data from connections that the network doesn't recognize, implement an authentication system. "Authentication is a handshake," explains Steve Durbin, managing director of the Information Security Forum Limited. "It allows you to make sure that the people accessing your system are who they say they are." He also recommends creating policies against using unsecured Wi-Fi connections for transmission outside the office.

□ 8 Make use of free and low-cost resources that can aid you in implementing these strategies thoroughly and productively. (See the "Reference Shelf" sidebar for a listing of guidelines, tools, and support organizations available to help you.)

To receive more articles like this, register for our small business updates here.

Lenovo

REFERENCE SHELF

USE THESE ONLINE RESOURCES TO CREATE A STRONG CYBERSECURITY PLAN THAT PROTECTS YOUR BUSINESS

Powered by Intel®
Intel Inside®. Powerful Productivity Outside.

The scope of cybercrime and its potential to disable your business can feel overwhelming. But a network of government agencies, professional associations, not-for-profit organizations, and commercial enterprises offer extensive information and support.

These online resources provide you with the tools you need to educate yourself and your employees about the strategies best equipped to safeguard your company, its intellectual property, and its reputation:

- National Institute of Standards and Technology. A part of the U.S. Department of Commerce, the agency produced Framework for Improving Critical Infrastructure Cybersecurity. This 41-page report reviews the Cybersecurity Framework government initiative for "using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes."

- U.S. Small Business Administration. The website offers several resources that owners of small and midsize businesses can use to address their cybersecurity concerns and responsibilities. They include:
  - > Introduction to Cybersecurity
  - > Top Ten Cybersecurity Tips
  - > Top Tools and Resources for Small Business Owners
  - > Social Media Cyber-Vandalism Toolkit
  - > Additional Cybersecurity Resources

- Federal Trade Commission (FTC). The government agency created Protecting Personal Information: A Guide for Business, an online tutorial that business owners can use to help train their employees.

- Center for Internet Security. This nonprofit organization works with industry and government to combat "evolving cybersecurity challenges on a global scale and helps organizations adopt key best practices." Among the digital booklets it has published online are:
  - > Getting Started Guide
  - > Firewall Guide
  - > Acceptable Use Guide
  - > Erasing and Disposal Guide
  - > Guidelines for Backing Up Information
  - > Cyber Incident Response Guide
  - > Risk Management Guide
  - > Cyber Crime Technical Guide

- National Cyber Security Alliance. The organization, whose goal is to provide education and empowerment in safe, secure internet use, created StaySafeOnline.org. The site's extensive Keep My Business Safe section provides these overviews and tools:
  - > Assess Your Risk
  - > Workplace Security Risk Calculator
  - > Monitor Threats
  - > Implement a Cybersecurity Plan
  - > Protect Your Customers
  - > Train Your Employees

- Sophos. The company, which develops network and endpoint security products, teamed with the Center for Internet Security to publish Threatsaurus: The A-Z of Computer and Data Security Threats. From "Advanced Persistent Threat" to "Web Application Firewall," this 100-page book explains cybersecurity terminology in non-technological language. The resource also includes safety tips.

- Internet Security Alliance. Founded in collaboration with Carnegie Mellon University, the organization's goal is to "combine the thought leadership of a think tank with the advocacy of a trade association and the programs of a professional association." The Advanced Persistent Threat: Practical Controls That Small and Medium-Sized Business Leaders Should Consider Implementing was written with the goal of "providing small and medium sized-business leaders with practical recommendations to help protect their organizations" from cybersecurity threats to their intellectual property.

- Information Security Forum. This independent not-for-profit is "dedicated to investigating, clarifying, and resolving key issues in information security and risk management, by developing best practice methodologies, processes, and solutions." Tools available on its website include:
  - > The ISF Standard of Good Practice for Information Security
  - > Information Risk Assessment Methodology 2
  - > ISF Benchmark and Benchmark as a Service
  - > Threat Horizon 2018: Lost in a Maze of Uncertainty

To receive more articles like this, register for our small business updates here.