April 04, 2022

Basic Best Practices for Boosting Your Small Business's Cybersecurity

Rodika Tollefson
Freelance writer and journalist

SUMMARY

With businesses around the world on high alert for cyberthreats, experts offer advice on how to prepare your company with better cybersecurity.

In response to cybersecurity concerns emerging from Russia's February 2022 invasion of Ukraine, the U.S. Cybersecurity & Infrastructure Security Agency (CISA) issued a unique alert – called "Shields Up" – recommending organizations of all sizes prepare for "disruptive cyber activity."

While improving cybersecurity is a multifaceted process that takes time, "Shields Up" is an opportunity for all small- and medium-size businesses to review their cybersecurity practices – and identify areas for better preparedness.

[Sound cybersecurity] just takes a commitment from the top down. You

need to pay attention to this stuff and commit a little bit of resources to it."

— Josh Moulin, Center for Internet Security

Understand Your Data

Boosting cybersecurity takes more than implementing some quick fixes, says Ron Gula, president of Gula Tech Adventures, which invests in cybersecurity companies and provides grants to cybersecurity nonprofits.

"There's no 'three easy things to do to secure your business and you're done.' You have to pay attention to it and be invested in it," says Gula, who also co-founded Tenable Network Security and worked at the National Security Agency doing network assessments.

Gula says that small- and mid-size business leaders need to start by caring about their data and customers. "They need to think what data they have that bad people could want," he says.

Josh Moulin of the Center for Internet Security (CIS) also says that data inventory is one of the first steps to ensuring a secure business. CIS is a nonprofit recognized globally for best practices, such as the widely used CIS Critical Security Controls, which include asset inventory.

"Create an inventory of your systems, software, vendors, and where your most important (and often most sensitive) data resides," says Moulin, a Certified Information Systems Security Professional (CISSP) who is the CIS acting general manager of operations and security services. "If you do suffer a cyberattack, the incoming incident responders will ask you for a few things – an asset inventory, software inventory, and network diagram or architecture will certainly be at the top of that list."

He notes it's common to discover corporate data across different vendor platforms or employees' personal cloud storage – and says that to get started, an inventory "can be as simple as a spreadsheet with a few tabs."

Adopt Basic Cyber Hygiene

Since every business is different, Gula says it's challenging to distill best practices into simple guidance. But for those working on the basics, he recommends starting with the four core cyber issues that the Cyber Readiness Institute (CRI) advocates for small and medium enterprises to focus on: ensuring strong passwords, keeping software up to date, creating awareness about phishing, and properly using USBs (including encrypting USBs and avoiding shared or found ones).

The following five basic steps represent a very short starting list based on recommendations from CRI, CISA, CIS and the National Institute of Standards and Technology (NIST), which establishes best practices for the public and private sectors.

1. Strong Passwords

CISA not only urges using strong passwords but also adopting a password manager to generate and securely store them. Weak or stolen credentials is one of the top vectors that threat actors use in cyberattacks. They can hack into your systems by cracking weak or predictable passwords or using compromised logins available on the dark web.

According to Verizon's 2021 Data Breach Investigations Report (DBIR), 61% of confirmed data breaches between November 2019 and October 2020 involved credentials. (Published annually, the DBIR for 2021 was based on an analysis of data from 79,635 incidents contributed by more than 80 cybersecurity companies and government agencies.)

2. Multi-Factor Authentication (MFA)

CISA advises using MFA as an additional layer of protection for all your accounts. Moulin says, "MFA alone significantly reduces the chances – by over 90%—of stolen credentials to be misused by an attacker." He adds that most cloud-based software applications offer MFA, and recommends enabling it as a company policy whenever it's available.

3. Software Updates

Cyberattackers commonly exploit security weaknesses in software, and many businesses take too long to patch those vulnerabilities. Moulin recommends enabling your systems to automatically download and install updates.

“Don’t forget third-party applications like browsers, [design software], and others that may need to be manually updated,” he says. “Create a company calendar appointment for all employees to check for updates on their systems and software at least monthly if you aren’t large enough to have this managed by IT.”

4. Security Awareness and Training

The 2021 DBIR found that 85% of confirmed breaches involved the human factor. Cybercriminals frequently use phishing or social engineering to trick employees to click on a malicious link or attachment, which enables the attackers to harvest credentials or install malware. According to CISA, more than 90% of successful attacks start with a phishing email.

An education and training program helps employees to recognize and defend against phishing and other threats.

“Recurring cybersecurity training is a must,” says Mark Kirstein, CISSP, vice president of customer success at Cosant Cyber Security, which provides cybersecurity advisors and virtual cybersecurity information officers (vCISOs) for emerging and midmarket businesses. “Companies should be doing it quarterly or continuously.”

5. Encryption

This best practice ensures unauthorized parties can’t access your data if a device is lost or stolen. Moulin notes that a great way to protect assets is by enabling built-in encryption.

Additionally, he recommends using cloud service providers that offer built-in security. “For example, having an email server inside the business that isn’t constantly monitored or scanned for vulnerabilities is highly susceptible to several cyberattacks, where commercial providers that offer business-grade email relatively inexpensively will be protected by 24/7 teams, have MFA built in, offer encryption at rest and in transit, and much more,” he says.

Moulin estimates that you could implement a host of baseline protections—including encrypted WiFi and laptops, centrally monitored endpoint tools (such as malware protection), and data stored with a secure cloud provider for about $30 a month per user, depending on the solutions you choose.

Beyond the Basics: Create a Plan

Kirstein says that developing an incident response plan needs to be a priority for all businesses because “even the best security can be defeated” and people can also make mistakes.

“You need a plan for when the incident occurs—who does what, in what sequence,” he says. “You can't make it up in the middle of an incident, and mistakes are costly.”

Incident planning should involve a cross-section of your business functions, including IT, HR, legal, public relations, and executives. "Test plans at least once per year by doing a tabletop exercise and make adjustments to the plan based on the lessons learned from the exercises."

The plan includes, among other things, a list of parties you'll need to contact in the event of an incident—and Moulin says it’s important to establish those relationships immediately.

“Begin a dialog with the necessary staff or outside organizations to plan for the very real potential that you will face some level of cyber disruption or attack in your business,” he says.

Getting Started

To help implement core best practices or advance to the next level, small and medium-size businesses can take advantage of a variety of free and low-cost resources, such as:

- The Global Cyber Alliance Cybersecurity Toolkit
- Free workshops from the Small Business Administration
- CISA’s Cyber Essentials Guide for small businesses and various free services
- Federal Communication Commission’s custom planning guide
- NIST small business cybersecurity website
- CIR’s starter kit
- Free publications for nontechnical audiences from CIS

Additionally, Gula advises reaching out to local or regional security crime task forces and similar groups that some states and other local entities have, as they often offer assistance to small businesses.

Ultimately, he says cybersecurity doesn’t have to be difficult. “It just takes a commitment from the top down,” he says. “You need to pay attention to this stuff and also commit a little bit of resources to it.”

The bottom line, according to Moulin: The more defensive layers you add between your business and attackers, the more protection you have. And, he says, it’s important to “not spend too much time admiring the cybersecurity problem.”

“Rather, pick one thing to improve and do it,” he says. “Then incrementally, as budget and risk dictate, implement the next step in the cyber program.”

Photo: Getty Images