Cybersecurity for Startups and Small Businesses

October 16, 2024

John Benninghoff
Cybersecurity Consultant
SECURITY-DIFFERENTLY.COM

Introduction

Organizations must make decisions on how to prioritize cybersecurity against all other investments and operational expenses. This is challenging for organizations of all sizes, but is a special challenge for startups and small businesses where leaders are rightly focused on growing and running their company. This paper describes simple habits that can reduce the largest areas of risk and help avoid taking on security technical debt that will have to be repaid later.

"I don't know what I don't know, what should I be worried about?"

All organizations face the risk of a security breach. Many criminals are opportunistic, looking for targets of opportunity that are vulnerable to attack, and security breaches have both an operational and opportunity cost. For many startups, the operational cost of a breach is low, especially when they have few or no customers. However, each hour spent in restoration and cleanup after a breach is an hour lost developing your business.

What risks do small businesses face? In fact, they are at risk of the same types of breaches as larger organizations. A recent report analyzing publicly available security incident data found that ransomware represented 37% of all losses, just ahead of accidental disclosure of sensitive data (36%) and system intrusion (24%). The report found that companies of all sizes have about a 1-in-10 chance of a ransomware event of $100K or more.

Can a cyberattack put your company out of business? While catastrophic breaches are rare, they do happen – an article published in 2023 covers six examples. Code Spaces, an online code hosting platform, was forced to shut down completely when an attacker took control of their cloud account and later deleted most of their data and backups. However, these cases are highly unusual, and there are often other factors that contributed to the failure of the business.

While the risk of a cybersecurity incident is real, there are several basic habits that have been shown to reduce your organization's risk, including choosing quality online services, managing technology, proactively updating technology, adopting good password practices, and backups. Each section presents a different habit, and the paper closes with a section on cybersecurity advice you *don't* need, along with advice for technology-focused organizations.

"What habits can I adopt that will reduce my cyber risk?"

Choose Quality Services

Startups and small businesses effectively outsource most of their security through the online products and services they consume, like Cloud, Web Hosting, Banking, Accounting,

Payroll, and others. In most cases, this is a good thing, as large online service providers are generally better equipped to secure their systems and include security features like Multi-Factor Authentication in their offerings. CISA, the government cybersecurity agency, recommends small businesses use cloud services over on-premises software for this reason.

When choosing a vendor, in general, high-quality services will have high-quality security. If you choose to do additional security vetting of your vendors, take advantage of the correlation Vivo Security discovered: organizations with a higher ratio of staff holding either of two key security certifications (CISSP and CISA) to total employees are less likely to experience a breach, and ask how many employees, CISSPs, and CISAs the vendor has.

Manage Technology Inventory

A recent academic paper found that an "organisation's attack surface was the strongest explanatory variable when it comes to predicting cyber risk outcomes." Small organizations can apply this principle by actively managing their hardware and software.

First and foremost, only install software you need and use, and expose services to the internet only when needed; this reduces the number of potential ways an attacker can get in (the "attack surface"). Typically, the default configuration for your computers and routers already does this, and we offer additional advice for technology-oriented companies in the last section. Additionally, keep an automatically maintained inventory of systems and services. Monitoring software and billing systems can provide a complete report of what you're running – turn off what you don't use.

Proactive Technology Updates

A habit of keeping *all* your organization's software and hardware up to date not only reduces your cyber risk, it improves system reliability, supports business growth, and keeps you from having to set aside time in the future to update and upgrade old, unsupported, and non-working systems (paying off technical debt). Underscoring the importance of updates, a survey conducted by Cisco found that a strategy of proactively refreshing technologies was most strongly correlated with security program success.

Since most security vulnerabilities are fixed by updating software, a habit of updating regularly significantly improves your cyber defense. Early in my career, our organization's diligent software updates prevented a hired security consultant from successfully breaching our *internal* network – the first and only time he did not gain full administrative control over a company's network. While it is uncommon, a strategy of "auto-update everything" is highly effective security.

For small organizations and individuals, this means turning on automatic updates for all software and systems, preferably on a schedule to automatically restart outside normal working hours if needed, so you're not tempted to click "update later." Advanced users should use a package manager, which is typically included with Linux (apt-get) and an add-on for macOS (Homebrew) or Windows (Chocolatey) to automate updates of software

without a built-in update mechanism. Using Homebrew Bundle, I'm able update *all* my software on my laptop with a single command, and can quickly download and install the complete set of software and tools I use on a new system.

When developing software, adopt a maintenance-first approach, by updating libraries and other dependencies before starting other work. As Sonatype discovered, most development organizations stay up to date on security by incorporating dependency management as part of their daily work, and proactively updating dependencies.

Passwords and Authentication

Of all the security technologies that are still in use, passwords are one of the oldest. Historically, managing password risk was challenging, but modern tools and technologies like passkeys, Multi-Factor Authentication (MFA), and password managers have made life easier.

The best way to secure your password is to not use one! While large enterprises can go fully passwordless, like Single Sign-On (SSO), doing so may require "enterprise" features that are too expensive for small businesses and individuals. For the rest of us, going passwordless means using passkeys (also known as FIDO). If passkeys aren't an option, multi-factor authentication is next best, and after that, using a unique long randomly generated password for each login. Using a full-featured password manager service helps with all these options. To sum up:

1. Use a full-featured password manager. A good product will generate, save, and automatically fill in details for passwords and other data, like name & address, credit card number, etc., will prompt you to turn on passkeys or MFA, and alert you about security issues, like compromised websites. They are available as a subscription service and allow you to sync passwords across all your devices and share passwords with family. Consumer Reports reviewed password managers in 2023.
2. Use passkeys when you can. Passkeys are resistant to phishing attacks and are the most secure authentication method today.
3. If passkeys aren't available, use MFA. Using an MFA application, including your password manager (as a time-based one-time password, TOTP), is more secure than text messages (SMS), but SMS-based MFA is still more secure than a password.
4. If you can't use passkeys or MFA, have your password manager generate a long, random password for each website or service you use.

Following this advice is generally easy, although occasionally a website will reject the password your manager generates – it might be too long, or not meet password composition requirements (if it doesn't contain the right combination of letters, numbers, or special characters OR contains disallowed characters). In the worst-case scenario, a site may silently fail or truncate your password. Thankfully, the National Institute of Standards and Technology (NIST) changed its guidance on passwords (SP 800-63-4) to specifically prohibit password composition rules, truncating passwords, and best of all: forcing periodic password changes, unless the password was compromised in a cyberattack. The newest

standard also states that passwords should be allowed to be at least 64 characters long, and allow any character, including space, in the password. Unfortunately, it may be some time before these new rules are fully adopted.

Backups

Regularly backing up your data and systems, *and* periodically testing a restoration, is a critical habit to develop as it provides resilience: the ability to recover from both known and unknown adverse events. While I've never had to deal with a cyberattack on my personal devices, I've had to restore from backups several times, due to hardware failures, accidentally deleting or overwriting a file, or just migrating data to a new device.

It's important to use a service or software that's specifically designed for backups – a cloud sync service like Google Drive, OneDrive, Dropbox, or iCloud Drive don't count, as they have a limited version history. (I recently had to restore a OneDrive file from backup, as the history had been accidentally overwritten). At a minimum, back up all your important files to a different storage location, and consider using some kind of full-device backup. A good way to think about backups is to ask yourself, "If I completely destroyed my laptop/phone/cloud sync service, how long would it take me to recover?" … Remember the case of Code Spaces, which had to shut down when an attacker destroyed both their production and backup data, which both resided on Amazon Web Services – backing up their data somewhere else, even to another cloud provider with a different login, would have allowed them to recover.

As with updates, automated backups are key – set up a regular schedule to run backups. For me, this is an hourly backup of my data files as well as my entire laptop. On macOS, Time Machine is an excellent choice for full-system backup as it runs backups hourly, automatically manages your backup history, offers some resistance to ransomware attacks, and is easy to set up. Backup services now exist that can provide a similar experience backing up cloud services, files, and full-system backups for Windows laptops.

Finally, it is important to periodically test the restoration process so you both know that it works and know what to do when you need it.

Other Considerations

For modern laptops, desktops, mobile devices, and most home networking devices (Wi-Fi and routers) the default configurations, firewalls, and built-in anti-virus (Windows Defender and macOS XProtect) are good enough – unless you have a specific business need, additional hardening or 3rd party security software, including VPNs, offers little or no extra protection, especially if you are diligent about keeping your software up to date.

You may have also heard advice to not use public Wi-Fi, and to never use public USB charging stations. This advice is wrong. While there was some risk to using public Wi-Fi years ago, that is no longer the case, as essentially all internet traffic is encrypted. Malicious USB chargers were never a real threat and there are no publicly known cases of a device being hacked by using a public USB charger (outside of hacker conferences).

Advice for Technology Organizations

For organizations that are technology-focused or have higher levels of technical expertise, we offer some additional advice. First, change the default ports for non-public internet services. As an example, by changing the SSH port for my home server from the default port 22 to a high numbered random port (above 10,000), I was able to reduce the number of SSH attacks I saw in my logs from multiple times per week (sometimes per day) to only about once or twice annually. While you should never completely rely on "security by obscurity" it can dramatically reduce the number of attacks you are exposed to. While this may not reduce your risk, it does reduce the amount of work needed to actively monitor your systems and investigate potential incidents.

Second, in addition to using password mangers, we recommend purchasing a product to manage secrets in the data center, either a cloud platform specific service like AWS Secrets Manager or Azure Key Vault, or a standalone product like HashiCorp Vault.

About Security Differently

Security Differently's mission is to replace the toil of security work with working securely by adapting lessons from safety to cybersecurity. Security Differently offers assessments and consulting services to organizations of all sizes, learn more at security-differently.com.