

10 ESSENTIAL BUSINESS CYBER SECURITY TIPS

Table Of Contents

| | |
|--|-----------|
| Introduction | 03 |
| <hr/> | |
| What Is Cybersecurity? A Quick Overview | 04 |
| <hr/> | |
| The Importance of Having Effective Cybersecurity for Your Business | 05 |
| <hr/> | |
| Top Cybersecurity Tips for Your Business | 06 |
| <ul style="list-style-type: none"> - Tip #1: Your People Are Your Weakest Link, Provide Them With Training | 07 |
| <ul style="list-style-type: none"> - Tip #2: Use Multi-Factor Authentication | 08 |
| <ul style="list-style-type: none"> - Tip #3: Warn Employees Against Phishing, Talk About Examples | 09 |
| <ul style="list-style-type: none"> - Tip #4: Train Users to Use Strong Passwords & a Password Management Tool | 10 |
| <ul style="list-style-type: none"> - Tip #5: Control & Monitor Your Internet of Things (IoT) Devices | 11 |
| <ul style="list-style-type: none"> - Tip #6: Monitor Your Domain on the Dark Web | 12 |
| <ul style="list-style-type: none"> - Tip #7: Work from Home? Use Zero-Trust Networking (ZTNA Networks) | 13 |
| <ul style="list-style-type: none"> - Tip #8: Follow Mobile Device Management Best Practices | 14 |
| <ul style="list-style-type: none"> - Tip #9: Have Managed Threat Response in Place | 15 |
| <ul style="list-style-type: none"> - Tip #10: Secure What You Can and Insure the Rest | 16 |
| <hr/> | |
| Additional Security Threats and Responses To Consider | 17 |
| <hr/> | |
| Final Thoughts from a Cybersecurity Professional | 18 |

Introduction

As a business owner, do you worry about keeping your data safe or your systems up and running? Did you realize that over half of small businesses that suffer from a cybersecurity attack go out of business within six months of the attack? Seriously, it's no joke.

Even enterprise level businesses can lose millions in cybersecurity breaches, and it may take years for them to restore their reputation. But what are the most common cybersecurity threats to smaller businesses?

Recent statistics show that some of the highest risks to a company's cybersecurity include:

- Data breaches from less secure home-based workstations of remote work employees.
- Lack of corporate security programs to fight ransomware attacks.
- Failing to regularly backup and secure data on external servers and in the cloud.
- Major IT service outages.

As cybersecurity networking professionals, Succurri recommends several tips to help my customers manage and mitigate threats to their IT infrastructure. In this ebook, we'll share the **top ten most important steps to take in order to protect your business from cybersecurity attacks**.

This is not a comprehensive resource for every business owner. Our goal is to highlight the importance of a complete cybersecurity solution with managed threat response, employee training, regular data backups, and VPN or ZTNA networks for businesses of all sizes.

No business is too small to need appropriate data protection. Succurri serves the greater Seattle area from Tacoma to Bellingham, WA and manages IT support, network management, provides cloud solutions, IT security, and phone systems for small, medium, and large businesses.



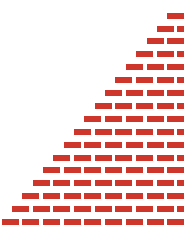
What Is Cybersecurity?

A Quick Overview

Cybersecurity involves putting together a plan that encompasses all of your best efforts to protect computer devices, networks, and systems from intrusion by unauthorized users attempting to steal, damage, interrupt, or lock out the system operations, data, transactions, and communications transferred on the network.

In layman's terms, cybersecurity is any step you could take to protect your organization's data and ability to operate your technology. This includes hardware, software, networking, and employee training.

In 2022 alone, there have already been several major cybersecurity breaches, affecting the conflict between Russia and Ukraine, extortion against Microsoft, Nvidia, Ubisoft, and other major companies, crippling blows to Costa Rica's infrastructure, and the theft of over \$1B in cryptocurrency. If entire countries, major corporations, and financial marketplaces are at risk, how do small and medium-sized businesses deal with the threats of cyberattacks? A cybersecurity strategy must examine and protect multiple weak points and factors to deter potential attackers from accessing confidential data and systems.



The Importance of Having Effective Cybersecurity for Your Business

The negative effects of a single data breach can close the doors on small and medium businesses for good. You can expect a host of problems stemming from a cyberattack on your business, including confidential data and systems.

- Fines and penalties by regulatory agencies for the breach.
- Forensic investigations into the causes of the data breach.
- Continuing credit and identity monitoring for victims of the data breach.
- Loss of customer trust.
- Diminished sales due to a damaged reputation.
- A tainted online reputation as stories of the data breach surface over relevant search terms.
- Lost income during a company shutdown due to non-operating systems during the attack.
- Reduced hiring interest to prospective employees, especially in IT.
- Threats to your business partners and vendors through your compromised system.

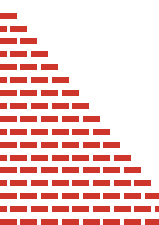
A breach affects four main categories of your business operations: internal, regulatory, vendor partnerships, and customer opinion.

By having effective cybersecurity strategies in place with a managed IT service provider you can reduce the opportunity that attackers have to disrupt your internal operations and controls. For example, ransomware attacks could lock you and your employees out of your systems until you pay a ransom to regain access so you can resume business operations. Weaknesses in your system could pose a risk to your business partners. Infection from a phishing scam could target partners your team regularly emails for invoicing, communications, planning, ordering, and more. Some types of businesses are more at risk than others.

Government agencies and financial organizations take data breaches extremely seriously, levying heavy fines for breaches that affect personal data and identification. If your business stores personal or business information, you'll want to read a little closer. Up to 69% of customers would avoid a business that fell victim to a data breach, and 29% would never visit that company again. So a data breach could have a real and lasting impact on your business.

Top Cybersecurity Tips for Your Business

While these tips are not a comprehensive list of every cybersecurity measure you should take nor do they represent a cybersecurity strategy, they do include several basic concepts you should address as soon as possible if you don't already have a solution in place

- Tip #1: Your People Are Your Weakest Link, Provide Them With Training
 - Tip #2: Use Multi-Factor Authentication
 - Tip #3: Warn Employees Against Phishing, Talk About Examples
 - Tip #4: Train Users to Use Strong Passwords & a Password Management Tool
 - Tip #5: Control & Monitor Your Internet of Things (IoT) Devices
 - Tip #6: Monitor Your Domain on the Dark Web
 - Tip #7: Work from Home? Use Zero-Trust Networking (ZTNA networks)
 - Tip #8: Follow Mobile Device Management Best Practices
 - Tip #9: Have Managed Threat Response in Place
 - Tip #10: Secure What You Can and Insure the Rest
- 

Tip #1: Your People Are Your Weakest Link, Provide Them With Training

Your human workforce presents the greatest threat to your company's security against data breaches. In 2021, 82% of data breaches were recorded as failings by human involvement. The most common attacks by hackers target human users on your networks and include:

- Phishing and social engineering attacks: 57%
- Stolen or compromised devices: 33%
- Theft of credentials or authorization: 30%

Many employees still fall for phishing attacks on their company email, potentially exposing your entire company's network to malware, ransomware, or disabling your email communications entirely. Social engineering attacks exploit user trust by presenting as an official resource to collect privileged information, such as by claiming to represent a bank, CEO, or vendor partner

A third of all attacks happen on devices, meaning device security is extremely important to protect data. Multi-factor authentication is essential to protecting device data.

Keyloggers, ransomware, and other malware can collect passwords, usernames, and spy on user screens to steal authorized login information. With this information, hackers can access financial systems, customer databases, transaction servers, and more to empty bank accounts, steal credit card information, and gain access to email systems to target your business partners.

Because your human employees are most susceptible to cyber threats, train them thoroughly on how to use multi-factor authentication, identify phishing threats, and generate and manage strong passwords.



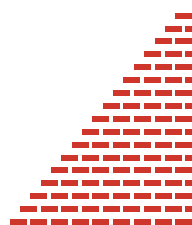
Tip #2: Use Multi-Factor Authentication

You can protect your transactions and network utilizing any of several multi-factor authentication (MFA) tools. At Succurri, we recommend AuthPoint by WatchGuard, but you may find another MFA provider that works better with your proprietary systems.

Many industry-standard devices and apps offer built-in MFA, including smartphones, banking apps, email systems, and more. Whether you prefer iPhone or Android, if you or your employees use their phones for business, you should all turn on MFA under your general settings.

Say you want to log in to an MFA-protected email account on a new company laptop. Once you enter the known password, the MFA window will pop up with a message saying that a special PIN was sent to the corresponding phone number for that account and to enter the PIN from the SMS message.

If you're a hacker, you don't have the phone with that number and can't access the account. If you own that phone (because it's your account), you simply enter the PIN that the MFA system texted to you to access your email on that computer.



Tip #3: Warn Employees Against Phishing, Talk About Examples

Phishing attempts account for the largest percentage of common data attacks, rising 11% in 2021 and making up 36% of all data breaches. Hackers deploying phishing attempts update their fraudulent claims to incorporate current events and appear more relevant to recipients, making your employees more likely to misidentify a major security risk. Train your employees at all levels to recognize phishing attempts. Some tools they can implement include:

- Learning about the most common and latest phishing scams, ranging from Nigerian princes to impersonations of colleagues.
- Learning how to read the sender's email address for fake emails.
- Learning to hover over a link to preview the link address before clicking on anything, even if it looks like an official corporate email.
- Forwarding suspicious emails to report a suspected phishing attempt.

Regular training sessions and phishing simulations can help prepare employees to recognize real phishing attempts and report them to the appropriate department when they encounter actual threats.

Tip #4: Train Users to Use Strong Passwords & a Password Management Tool

Succurri recommends Keeper Security to manage passwords for several high-risk industries, including:

- Healthcare
- Research
- Communications
- Government
- Military
- Engineering
- Finance
- Municipalities
- Education
- Construction
- Architecture
- Supply Chain Management

No matter which password management tool you choose for your business, you need to train employees on how to use strong passwords or a password generator to create unique, hard-to-guess passwords for their company profiles. A weak password strategy includes:

1. Using the same username and password across multiple applications.
2. Not using multi-factor authentication (MFA) in combination with strong passwords.
3. Not using a password management tool to generate and protect passwords.

Addressing these weak points can help you maintain your system security. Consider forcing password changes for users every 90 days and implementing a password management tool on all company devices.



Tip #5: Control & Monitor Your Internet of Things (IoT) Devices Management Tool

Internet of Things (IoT) devices include data-collecting chips, sensors, onboard computers, or GPS devices, among others, that are integrated with things like vehicles, building security, and personal devices. As this technology grows, breaches of these systems could become a major cyberattack threat.

For example, many hotels use digital door locks for guest rooms utilizing a keycard for entry. Electronic attackers could infiltrate the system to gain access to guest rooms, threatening the safety of guests and/or putting their belongings at risk.

IoT devices often do not have security as a primary concern by design, which makes their weaknesses highly exploitable. For anything your company uses, from a Ring doorbell to wearable remote health monitoring devices for patients, ensure that your systems use strong passwords, that you turn off unused features, and that you update the software and firmware frequently.

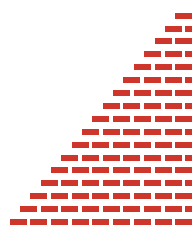
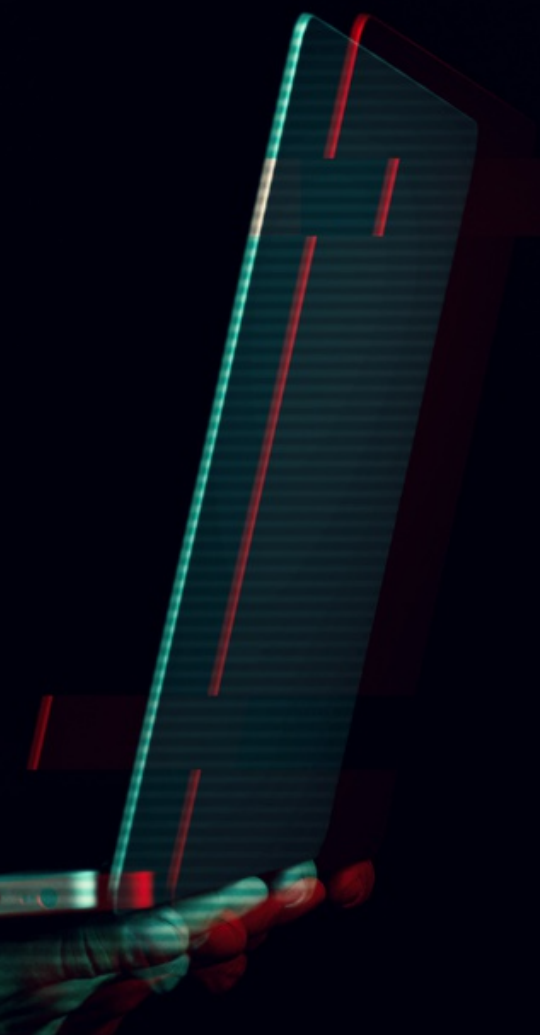


Tip #6: Monitor Your Domain on the Dark Web

The Dark Web is the seedy underground of illicit data trading for cybercriminals. You can protect your business with dark web monitoring and scans to look for compromised accounts, data breaches, and other weaknesses.

The problem with leaks on the dark web is that criminals can buy information to gain access to compromised passwords and accounts. Once you become aware of a potentially compromised account, you can force password changes for all employees to protect your network from additional attacks. However, without dark web monitoring, you may not discover the breach until you've already suffered a catastrophic cyberattack.

Succurri offers a dark web scan of your information if you are curious to know if your personal information is on the dark web.



Tip #7: Work from Home? Use Zero-Trust Networking (ZTNA Networks)

Since COVID-19 derailed most of society and enterprise for a time in 2020, and since we've learned to work around a global pandemic digitally, new threats have arisen to target businesses that adopted a work-from-home structure for their employees and independent contractors.

For your WFH (Work From Home) employees and contractors, a zero-trust network access (ZTNA) system is the latest in VPN (Virtual Private Network) technology. Where traditional VPNs have to back route data through the corporate VPN data center, ZTNA is local software on approved devices.

Think of ZTNA as creating a private island on the public internet. The only way onto your island is through the single front door entry. You lock your door with MFA (Multi Factor Authenticated)-protected passwords, and open-sea internet pirates can't access your private island network.

At Succurri we recommend iboss Zero Trust Edge for ZTNA protection.

Regardless of where an employee uses their ZTNA access, whether it's from home or the local coffee shop wi-fi, their ZTNA will always send data from the same IP address. By contrast, traditional VPNs may seek out local network addresses and change a user's IP address depending on their location.

ZTNAs are the most secure modern network management system for WFH, split-time, as well as on-site employees and independent contractors. While it can be time-consuming to ensure that users are authorized to access all essential corporate software using a ZTNA, the protection offered is second-to-none.

Tip #8: Follow Mobile Device Management Best Practices

Many of us spend hours each day working from our mobile smart phones. Whether you work in construction, administration, or a non-profit organization, you and your employees probably communicate vital company information across mobile devices every day.

With mobile device management, you and your employees can protect business data and keep it separate from personal data on mobile devices like phones and tablets. With mobile device management, you can ensure that:

- Employee phones are up to date with the latest security software.
- Company apps stay up-to-date with the latest software patches.
- Company data is wiped from any devices used by former employees.
- App use and mobile email accounts are secure through company monitoring.

While many business owners and employees are reluctant to put mobile device management onto their personal phones, this type of software can help protect personal devices from future company data breaches that could affect their private data.

Since not every business can implement best practices and provide all employees with company mobile devices, mobile device management is an excellent strategy to keep personal and business uses separate on a personal mobile device.



Tip #9: Have Managed Threat Response in Place

Managed threat response, event detection response, or managed detection response is a combination of AI, human alerting, and intervention software to block possible cyberattacks and digital threats.

At Succurri we prefer Sophos MDR Advanced for our managed threat response applications. Because the most expensive part of event detection and threat response is human monitoring, we recommend digital monitoring with AI intervention to reduce the need for a human response to a threat.

Your MDR software can actively hunt for threats in your systems, respond effectively with integrated AI intervention, and notify you about possible threats and weaknesses in your systems.



Tip #10: Secure What You Can and Insure the Rest

Even the latest and greatest cybersecurity measures can't offer a 100% guarantee that your data is safe, especially when hackers are increasing their attempts to breach company data. Due to the sensitive nature of the data affected and other costs, a single data breach can cost small and medium businesses over \$120k per incident.

InsuranceBee surveyed 1,300 small and medium-sized business owners to learn that over 91% don't have cyber liability insurance in case of a data breach. Effective cyber liability insurance should cover:

- Costs associated with investigating the data breach.
- Costs to inform customers, vendors, and partners about a breach.
- Electronic fund transfer recovery.
- Restoration of your systems and data.
- Credit monitoring for identity theft victims.
- High-risk financial data monitoring.
- Credit monitoring with all three bureaus.
- Legal fees to defend your company against claims made by victims of the breach.
- Costs to pay fines or penalties imposed by regulatory commissions.
- Lost income from operations halts due to the data breach.
- Reputation restoration and client relationship management services.

While many business owners and employees are reluctant to put mobile device management onto their personal phones, this type of software can help protect personal devices from future company data breaches that could affect their private data.

Since not every business can implement best practices and provide all employees with company mobile devices, mobile device management is an excellent strategy to keep personal and business uses separate on a personal mobile device.

If you want your business to survive a cyberattack, get cyber liability insurance from a reputable provider to protect your operations from costly fines, lawsuits, and damage to your reputation.

Additional Security Threats and Responses to Consider

These tips do not make up a comprehensive guide to everything you can do to protect your business from a cyberattack.

Other exploitable weaknesses come from unused apps, failing to update apps and other software, and not maintaining your backups.

You can mitigate your risks by doing some seasonal cleaning to improve your digital hygiene. The first thing you can do is remove unused apps or old software from your systems and devices. Old programs may not receive updates anymore, leaving openings for cyber attackers to infiltrate your systems and slowing down functioning processes.

Ensure that you update your software frequently. Most software and operating systems will search for updates automatically and pre-install the new features to run on your next computer restart.

However, some proprietary software may require manual updates. Instruct employees or your in-house IT team to run updates as they become available.

The most essential part of data recovery after a breach is having secure backups of all of your data. Data backup processes should follow the Rule of Three, meaning you need to back data up to two other locations besides the primary data location. For example, you may have your primary data location, a physical backup server, and a cloud backup.

You should also automate your backups to always have current data protection available. Do not rely on yourself or your employees to maintain an adequate backup schedule. Utilize a professional backup service or software to ensure that your data is safe and that you can access updated backup data when you need it after a breach.



Final Thoughts from a Cybersecurity Professional

An effective cybersecurity strategy utilizes an entire toolbox of smart policies, software, backups, and employee training. Overlapping security layers can balance each system's strengths and weaknesses to provide a strong defense against cyber threats.

Remember that no matter how many digital security systems you have, your people are your weakest link. Train employees effectively to recognize threats and report them to the appropriate department. Then, give them the digital tools they need to manage and secure their passwords with multi-factor authentication.

As a business owner, it's up to you to provide ZTNA access, automate backups, and implement mobile device management across your organization to protect your data.

If you want to know how effective your company's cybersecurity strategy is, contact us at Succurri to get a free IT & Cybersecurity assessment.

