FILE EDIT VIEW HISTORY BOOKMARKS TOOLS WINDOW HELP

THE SMALL BUSINESS GUIDE TO Cybersecurity

SCORE
FOR THE LIFE OF YOUR BUSINESS

TREND MICRO™

Initiative for Education
DIGITAL SAFETY OUTREACH

Do you think cybercriminals are too busy targeting the likes of Capital One, Citrix and Facebook to bother with your small business? Think again.

Some 76% of cyberattacks occur at businesses with under 100 employees. Cybercriminals know small businesses tend to be easy targets, and that accessing a small business's computer networks often gives them entrée to client and vendor networks, too.

For a small business the cost of a data breach can be devastating. The average cyberattack costs smaller companies an average $3,533 per employee. It takes an average 206 days to identify a risk and another 73 days to contain it, making the life cycle of a data breach 279 days.

No wonder nearly 60% of companies go out of business within six months of a cyberattack.

The stakes are high. Fortunately, there are some steps you can take to prevent a cyberattack—and survive one if you're hit. In this e-Guide, you'll learn about the biggest cybersecurity risks facing small businesses, the 3 most common cyberthreats to watch out for, how to secure your business, and how to respond to a data breach.

76%

OF CYBERATTACKS OCCUR AT BUSINESSES WITH UNDER 100 EMPLOYEES.

60%

OF COMPANIES GO OUT OF BUSINESS WITHIN 6 MONTHS OF A CYBERATTACK.

Cybercrime Grows During COVID-19 Crisis

The FBI reports that instances of cybercrime appeared to grow as much as 300% since the beginning of the coronavirus pandemic! The Bureau's Internet Crime Complaint Center (IC3) is receiving between 3,000-4,000 cybersecurity complaints a day, up from an average of 1,000 per day before the pandemic hit.

As America's daily activities increasingly moving online due to stay-at-home orders, the opportunities for cybercriminals grew due to:

- Employees, new to remote work, who were unaware of basic security measures
- Businesses struggling to keep externally-accessed systems secured
- Lack of social and workplace interactions

There are ongoing uncertainties, including:

- Supply chains (PPE and essential goods)
- Online orders and payments
- Medical help and COVID-19 testing
- High unemployment
- Fears and other factors

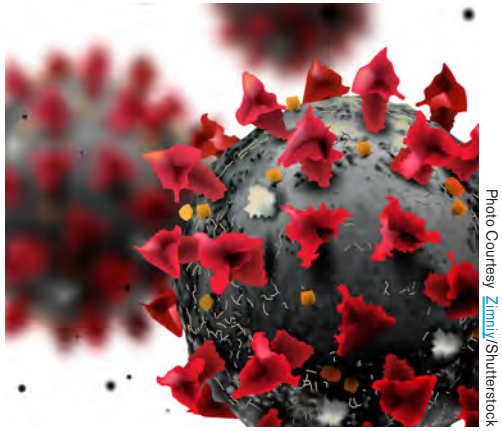

Photo Courtesy Zimniy/Shutterstock

Photo courtesy Benoit Daoust/Shutterstock

5 biggest cybersecurity risks

What's putting your business at risk? The answers might surprise you. The biggest cybersecurity risks for small businesses are:

1. **Human Capital Risk:** Hackers target employees, which is why you need a strong IT security staff. Educate your employees about your security requirements.
2. **Cyberthreat Risks:** These include phishing and social engineering (tricks cybercrooks use to make people do things they don't want to do); clickjacking (technique used by cybercriminals to hide malware and other threats under content of legitimate sites); botnets (a network of hijacked computers and devices infected with malware remotely controlled by a hacker to send spam and launch DoS attacks; fileless attacks (malware that doesn't drop a file on your disk, but can infect your computer, steal your data, etc.); and denial of service (DoS) attacks designed to disable, shut down or disrupt a network, website or service).
3. **Data Risk:** The exposure to loss of value or reputation caused by issues or limitations to an organization's ability to acquire, store, transform, move, and use its data assets.
4. **Infrastructure Risk:** Potential losses due to failures to protect business critical data assets and applications. It's key to make sure technologies, such as mobile, cloud, social media, and IoT devices are safe to use in the workplace.
5. **Operational Risk:** Protecting against data breaches and other cybersecurity threats.

The 3 most common cyberthreats

Cyberthreats grow more sophisticated every year. Here's what to watch out for.

1. **Ransomware:** Hackers get into your system and hold your data hostage until you pay a ransom. If you don't pay, your business is out of commission. Ransomware cost companies $11.5 billion in 2019. That's expected to rise to $17 billion in 2020 and $20 billion in 2021. Cybercrooks use various techniques to blend in, including:
   - **Obfuscation:** Cybercriminals use obfuscation to conceal information such as files to be downloaded, sites to be visited, etc.
   - **Critical System:** Attacks on critical infrastructure
   - **Legitimate Software:** Malicious files often coming from software downloaded from URLs that were not whitelisted.
   - **Distribution Model:** Popular websites housing malicious files. The digital extortion of businesses will continue. The value will be in ransoming Industrial IoT (IIoT). Attackers are discussing on underground forums to how to monetize IoT infections.
2. **Business Email Compromise:** BEC are scams targeting companies that conduct wire transfers and have suppliers abroad. Since 2016 over $9 billion has been lost to business email scams. Email accounts of executives or high-level employees are either spoofed or compromised through keyloggers or phishing attacks to do fraudulent transfers.
   - According to the FBI, there are 5 types of BEC scams:
     - **The Bogus Invoice Scheme:** Attackers pretend to be foreign suppliers requesting fund transfers for payments to an account owned by fraudsters.
     - **CEO Fraud:** Attackers posing as the company CEO or other executive send an email to employees in finance, requesting them to transfer money to the account they control.
     - **Account Compromise:** An employee's email account is hacked and used to request invoice payments to vendors listed in their email contacts. Payments are then sent to fraudulent bank accounts.
     - **Attorney Impersonation:** Attackers pretend to be from the law firm supposedly in charge of crucial and confidential matters. These requests often are done via email or phone, at the end of the business day.
     - **Data Theft:** Employees in HR and bookkeeping are targeted to obtain personally identifiable information

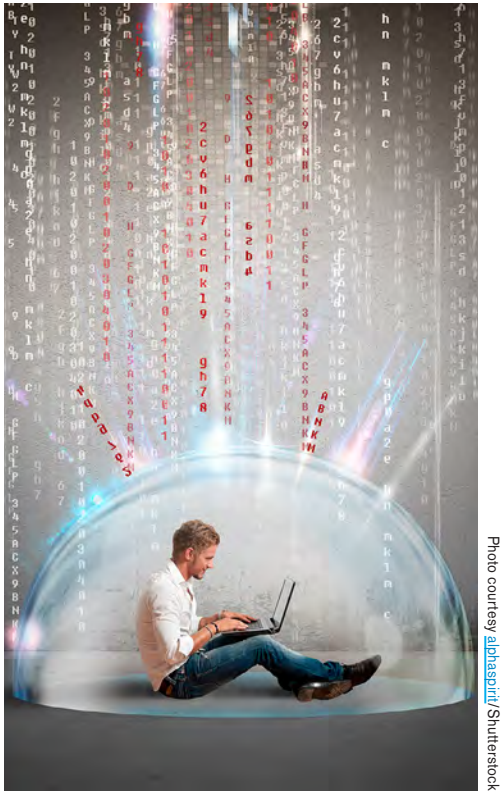

Photo courtesy alphaspirit/Shutterstock

Photo courtesy EtiAmmos/Shutterstock

(PII) or tax statements of employees and executives. Such data can be used for future attacks.

- Because these scams do not have any malicious links or attachments, they can evade traditional solutions. Employee training and awareness can help enterprises spot this type of scam.
- **FBI Warning:** The FBI has issued a warning anticipating a rise in BEC schemes related to the COVID-19 pandemic. "Fraudsters will take advantage of any opportunity to steal your money, personal information, or both. Right now, they are using the uncertainty surrounding the COVID-19 pandemic to further their efforts."

  According to the FBI, there has already been an increase in BEC frauds targeting municipalities purchasing personal protective equipment (PPE) in the fight against COVID-19. Most of the recent BEC attacks were targeted at financial institutions or banks.

3. **Cryptocurrency mining:** These hackers don't care about your data. They just want to get into your computer system and use its resources to mine cryptocurrency. These attacks target tablets, smartphones, routers, printers and IoT devices–any device with computing capabilities they can leverage.

How to protect your business

You have two areas of defense against cyberthreats: your users (you and your employees) and your devices. Follow best practices for both to keep your business safe.

Best practices for user security

Attackers prey upon:

- Human error
- IT security complacency
- Technical deficiencies

Create policies incorporating the following cybersecurity practices.

1. **Passwords**
   - Use a different password for every account or website. Most of us re-use the same password across multiple accounts, so a hacker who accesses an employee's Etsy account can try the same password on their business email account with a good chance of success.
   - Change passwords frequently–every quarter. Use long, complex passwords. A password manager can help by automatically creating and saving passwords. Popular password manager apps include:
     - Trend Micro Password Manager
     - LastPass
     - 1Password
   - Don't store passwords in an obvious place like a Post-it note on your computer monitor or under your keyboard.
   - Don't share the same password among users or tell others your password.
2. **Email security**
   - Watch for these clues that an email is fraudulent:
     - Look for obvious grammar and spelling mistakes; often hackers are from outside the U.S. and aren't fluent in English. Hover your mouse over links in the email to see if the link matches the link in the pop-up. For example, a link that shows as www.paypal.com in an email might actually be www.paipal.com when you mouse over it.
     - Examine the email sender's address to make sure it's correct. In the preview pane an email might look like it's from JohnSmith@yourbiz.com, but when you expand the header information, you see the actual email address is JohnSmith@youbiz.com.
     - Verify before responding to an email request for sensitive data. In CEO fraud, for example, the hacker may say their phone isn't working or they're in a meeting, so you need to answer by email. Don't! Call the person to double check before sharing sensitive information.

Photo courtesy zimmytws/Shutterstock

Photo courtesy Natali_Mis/Shutterstock

- Prohibit employees from opening outside email attachments. Instead:
  - Create a policy that any supplier must use a cloud-based option to share files instead of sending attachments.
  - If this won't work, require password-protected attachments only. Any others should be viewed as suspicious and deleted.
  - If neither of the above will work, have employees contact the supplier to verify that the attachment is legitimate before opening it.
- Conduct regular phishing awareness training. Free or low-cost tools that let you simulate phishing attacks and educate employees about cybersecurity include:
  - Trend Micro Phish Insight
  - Cofense
  - KnowBe4
- Use email encryption when sending sensitive data. Encryption is built into or can be enabled on most popular email clients, including Outlook, Windows, MacOS, Linux, Android and iOS.

3. Online safety

- When logging onto websites–especially for sensitive purpose, such as accessing bank accounts– use two-factor authentication for an extra layer of security.
- Verify links. Be careful of links in texts or emails, even if they seem to be from someone you trust. Hover over the link to see if it matches the link that appears in the email, or manually type in the URL instead of clicking on the link.
- Minimize use of cloud file-sharing. Be judicious about what you share with others on sites such as Dropbox and Google Drive.
- Never share customer information, intellectual property information or other core business data online..
- In general, don't overshare online–with anyone.

4. Outside the office

- Be cautious using public Wi-Fi. Keep work conversations private. Many networks are unsecured, meaning usernames, passwords, or files that you upload or download can be captured by crooks. Bring your own Wi-Fi access device instead; you can get one from any cell phone carrier.
- Restrict remote access to your business network to only necessary users.
- Close RDP ports and enforce VPN use.

THE FBI REPORTS THAT INSTANCES OF CYBERCRIME APPEARED TO GROW AS MUCH AS

300%

SINCE THE BEGINNING OF THE CORONAVIRUS PANDEMIC! THE BUREAU'S INTERNET CRIME COMPLAINT CENTER (IC3) IS RECEIVING BETWEEN 3,000-4,000 CYBERSECURITY COMPLAINTS A DAY.

Best practices for device security

Take the following steps to secure your devices.

1. Computers and servers

- Choose a centrally-managed, business-grade antivirus (AV) security solution so you can monitor all the devices on your network, restrict user access and enforce security policies. Consumer-grade products don't provide enough protection
- Implement multiple layers of protection. Installing AV software on your computers alone isn't enough. Look for an all-in-one cloud solution that provides endpoint, web security and email protection.

Photo Courtesy Chadchai Krisadapong/Shutterstock

Photo courtesy flydragon/Shutterstock

- Isolate payment systems. Separate your point-of-sale systems or credit card readers from the rest of your network by putting them on a separate network or firewall.
- Restrict both physical and digital access to servers. All it takes is one malicious employee to wreak havoc.
- Require two-factor authentication to log onto servers.
- Update software, hardware and firmware regularly; set updates to install automatically.

2. All devices

- Whatever device people are using be sure to:
  - ❍ Change default username /password.
  - ❍ Disable remote management
  - ❍ Restrict access to specific addresses.
  - ❍ Require two-factor authentication.
  - ❍ Update device software and firmware regularly.

3. Mobile devices

- Enforce passwords or passcodes on devices.
- Take advantage of biometric identification technology if available; it's more secure than using a password.
  - ❍ Install security software on devices.

4. Wi-Fi routers

- And other network-connected devices like printers and copiers, etc.
- Use a separate Wi-Fi network for guests.
- Enable encryption using (WPA2).

THE 3-2-1 RULE OF BACKUP

When making backups, experts recommend following the "3-2-1" rule:

3. **Have 3 copies** of backup at all times.
2. **Store backup** using 2 mediums (for example, on a hard drive and in the cloud).
1. **Keep 1 copy** offsite so a physical disaster at your location doesn't wipe out your only copy.

How to recover from a cyberattack

Despite your best efforts, what if you're hit by a cyberattack? Here's how to handle it.

Step 1: Respond

- Turning off your computer, disconnecting your internet connection, or shutting down your router until you can assess the damage.
- Restore your data from backup. (See "The 3-2-1 Rule of Backup," on left.)
- Bring in IT experts to help if necessary

Step 2: Recover

- Execute your disaster recovery plan. (If you don't have a disaster plan, now is a great time to create one. Look for free templates online that you can use as a starting point and adjust based on your business.)
- Attend to any breach notification requirements. Depending on your industry, you may be required by law to notify customers, vendors or employees affected by a security breach.
- Evaluate existing and new technologies you can use to prevent future breaches. Are your current cybersecurity practices effective? If not, what can you add to better protect your business?

Conclusion

Cybercriminals are crafty—but you can outsmart them by being aware of the risks and implementing cybersecurity best practices immediately. Educate your employees, implement a cybersecurity policy for your business, and put the proper protections in place. Taking these simple steps will help to prevent your business from becoming a statistic.

Photo courtesy Nagy-Bagoly Arpad/Shutterstock

RESOURCES

Use these resources to learn more about cybercrime, develop a plan to protect your business from cyberattacks, and report a cyberattack.

- SCORE
- Trend Micro Internet Safety for Small Businesses
- National Cybersecurity Alliance
- Federal Communications Commission
- Federal Trade Commission
- National Institute of Standards and Technology
- FBI Field Office Cyber Task Force
- Internet Crime Complaint Center