AT&T Business

Cybersecurity and protection playbook

What your small to mid-sized business must know

Tight budget? You can still assess your risks and make a cost-effective plan

AT&T Business

Size doesn’t matter. You’re at risk.

It’s not the size of your business that determines your cybersecurity threat. It’s your security maturity.

Small and mid-sized businesses are realizing that they, like big enterprises, are growing targets for cybercriminals. The reason is simple. It’s easier to break into smaller businesses than large ones that have dedicated security staffs.

Cybersecurity risk isn’t based on the size of your business; it’s based on security maturity. Recent research by AT&T Cybersecurity and Enterprise Strategy Group (ESG) helps small and mid-size businesses better understand what a mature cybersecurity program looks like and how that maturity influences security and business outcomes. This research found no correlation between company size and maturity level. Organizations of any size can achieve a mature cybersecurity program. See how you rank on security maturity with this free online assessment.

Small businesses want to focus on running their business and providing the best customer experience possible. They realize that fighting cybercrime is not their core competency and want help from a cybersecurity expert. But the reality is that smaller companies need the resiliency of larger companies. Fortunately, they can meet that goal even on a limited budget.

As digitization increases,

43%[1]

of cyberattacks target small businesses.

And very concerning

70%[1]

of small businesses are unprepared to deal with a cyberattack.

The economic fallout from COVID-19 is a stark reminder that small and mid businesses make up the vast majority of the nation’s businesses at the local level.[2]

[1] 2021 Cybersecurity Statistics, PurpleSec: https://purplesec.us/resources/cyber-security-statistics/#SmallBusiness.

[2] Infosecurity Magazine: “When It Comes to Cybersecurity the Small and Medium Business Community Needs to Do Better.”

Get to know your hacker

The “bad guys” come in several varieties, including automated bots. Either way, you’ll need to fight them all.

Ever wonder why a small business with a small geographic footprint and almost no online presence gets compromised? Chances are it had just the right combination of issues that an automated attack bot could exploit.

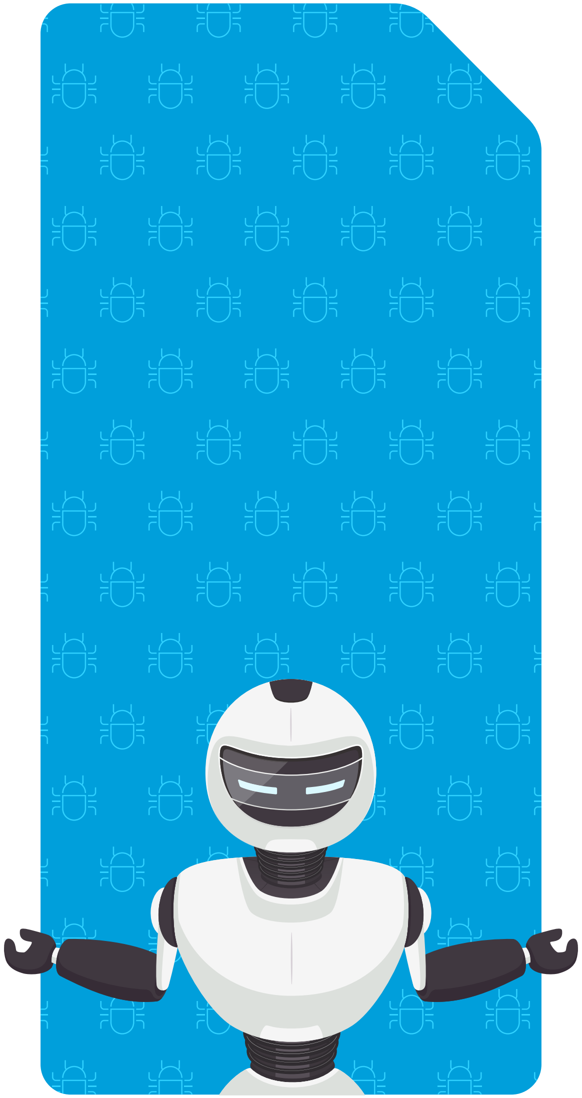
Two basic types of attacks exist: opportunistic and targeted. Opportunistic attacks are largely automated, low-complexity exploits against known vulnerable conditions and configurations. These kinds of events can potentially derail a small to medium business.

Targeted attacks are quite different. Cybercriminals can break into your network and lurk anywhere from a few minutes to hundreds of days. During this “dwell time” – the time between the attack and its discovery – intruders can go on a veritable shopping spree and steal sensitive data. Because the attacks are slow, persistent, and don’t raise red flags, a small or mid-size business may not notice until it’s too late and data is already compromised.

Not only is your business at risk from targeted attacks but so are your employees, partners, and third-party supply chains. (See next page for information on how to protect your supply chain.)

While targeted attacks may use some of the same exploitable conditions that opportunistic attacks use, they tend to be less automated in nature to avoid detection for as long as possible. In addition, targeted attacks may involve a more frequent use of emerging threats, aka “previously unknown exploit vectors” or **“zero-day attacks,”** to reach their goals or abuse trusted connections with third parties to gain access to your organization.

Ultimately, it doesn’t matter which of these kinds of attacks results in a compromise and potentially a breach. It’s important to think of both when aligning your people, processes, and technology to mitigate that risk.

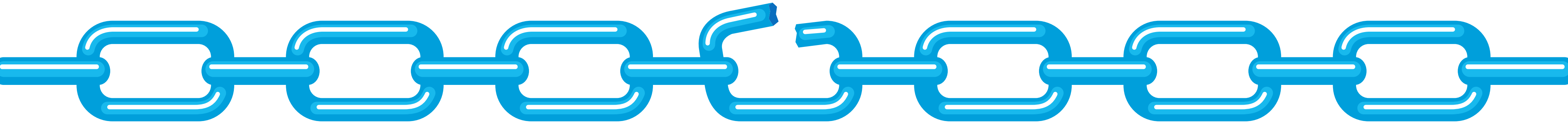


What’s the weakest link in your supply chain?

Partners and software are essential but can expose you to threats

Small and mid-size businesses using a third-party supply chain are unknowingly subject to areas of vulnerability from partners and software.

Partners. Small businesses are not always able to own or operate every step of their supply chains. They are often reliant upon third-party partners to handle essential elements such as logistics or the supply of raw materials. While these relationships are essential to how small businesses operate and are positive for all concerned, there is a risk of inconsistent cybersecurity protections across all third-party partners. If one link in the chain doesn’t have sufficient system protections, it can present the risk of a breach to all companies they are connected to and even expose customers themselves.



Software. Small businesses are unlikely to create and develop their own proprietary software solutions. It is most likely that small businesses use commercial off-the-shelf software (COTS) to run their business (for accounting, inventory management, etc.) While this can be an attractive option for many businesses, leaders are trusting that these third-party vendors are operating robust cybersecurity protocols and providing sufficient protection for data collection, sharing, and storage. Be sure to work with a trusted vendor for your business-critical applications to protect your business.

What you can do right now

Mitigate the risk of e-commerce

Preserving human connection with evolving digital strategy. The pandemic has shown marketers can't remain passive – reacting to a changing world – they must evolve proactive strategies that predict consumer needs and deliver the human connection they crave. This is what conversational commerce delivers.[3]

As you continue to lean heavily on online transactions, it's important to conduct online business carefully to protect company reputation and prevent data breaches. Cybersecurity starts with password security. Develop and enforce a password security policy and encourage employees to regularly change passwords and use complex ones. You may wish to invest in a password manager for convenience and to manage long and robust passwords. Encourage two-factor authentication, also.

[3] "Navigating the rise of digital commerce: Imperatives and impediments for CMOs."

How can I help protect online payments?

Get started with this checklist of 8 best practices

Keeping customers' personally identifiable information (PII) safe during transactions should be a top priority. Follow these steps to keep financial transactions smooth and decrease the likelihood of a security breach.

1. Be compliant

Make sure your payment system is compliant with the Payment Card Industry Data Security Standard (PCI DSS), an international standard for secure card payments with 12 security requirements. The PCI Security Standards Council (PCI SSC) was established in 2006 for regulating payment brands and helping merchants secure financial data of customers.

AT&T Cybersecurity Consulting offers a range of comprehensive, customized PCI compliance solutions to provide a holistic solution for your company. We provide assessments (PCI) and remediation consulting, program development, penetration testing, and code review services that help companies address specific areas of PCI compliance and security best practices. Learn more about security solutions for PCI compliance to help secure your cardholder data.

How can I help protect online payments? cont.

2. Use data encryption

Keep your customers' financial information private by adopting data encryption. Nowadays with open Wi-Fi networks, identity theft is prevalent and relatively easy for hackers to commit if the data is unencrypted. Websites that your business deals with for online transactions should be valid and have legitimate operators. Data encryption protects your sensitive information so that it can only be viewed by the authorized parties and does not fall into the wrong hands. It also helps reduce vulnerability to password-hacking. These features combined provide an additional protection layer for customers during transactions.

How can I help protect online payments? cont.

3. Keep your network updated

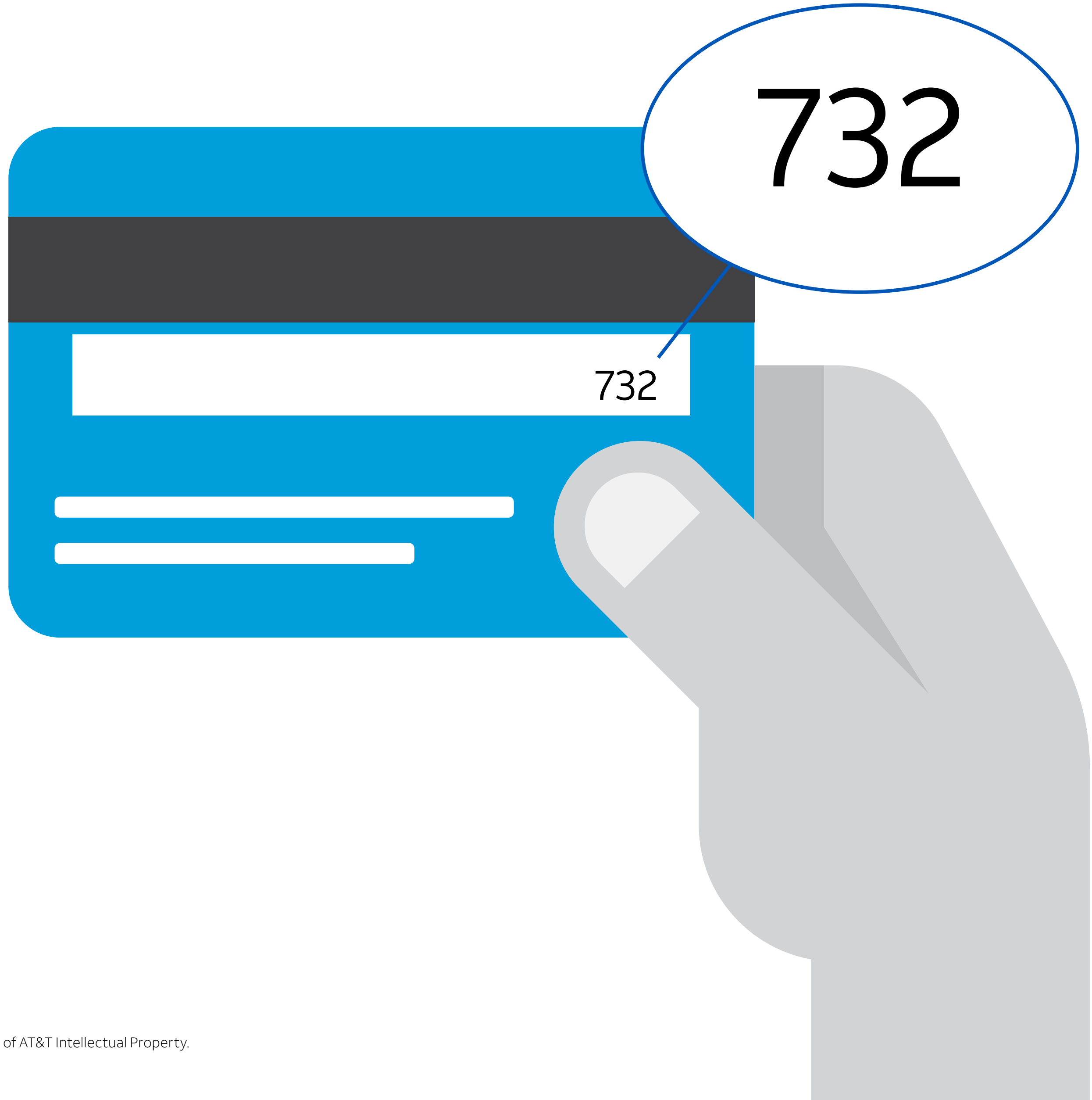
Hackers regularly invent new ways to infiltrate systems. For this reason, it is important to regularly install security updates on your business's computer networks. Sign up for automatic system updates to stay a step ahead. Automatic updates will install important safeguards so that your online transactions remain protected. They will also help reduce the chance of virus attacks on your system, which could harm your business.

How can I help protect online payments? cont.

4. Provide secure login

Make the customer's login process as secure as possible. If you don't, it's all too easy for cybercriminals to infiltrate your system and steal login information. If customers forget their passwords, they should have to enter an email address or username to retrieve their passwords by using the emailed link to change them. This safety protocol is simple but highly effective. Even better, use two-factor authentication for logins.

How can I help protect online payments? cont.



5. Enable Address Verification System (AVS)

An AVS verifies the customer's billing address against cardholder data from the issuing bank. It helps detect fraud because the hacker does not usually know the billing address of the real cardholder. These systems are used in combination with CVV2 verification, the three-digit code on the user's card. Asking for both AVS and CVV2 at checkout can better protect against fraudulent activity.

How can I help protect online payments? cont.

6. Carefully choose the right payment processor

Make sure to choose a reputable payment processor that prioritizes security and can accept credit and debit cards safely and securely. Besides security concerns, you also need to consider the type of payments it accepts, the fees it charges, and the transaction platforms it supports.

7. Install SSL certificates on your website

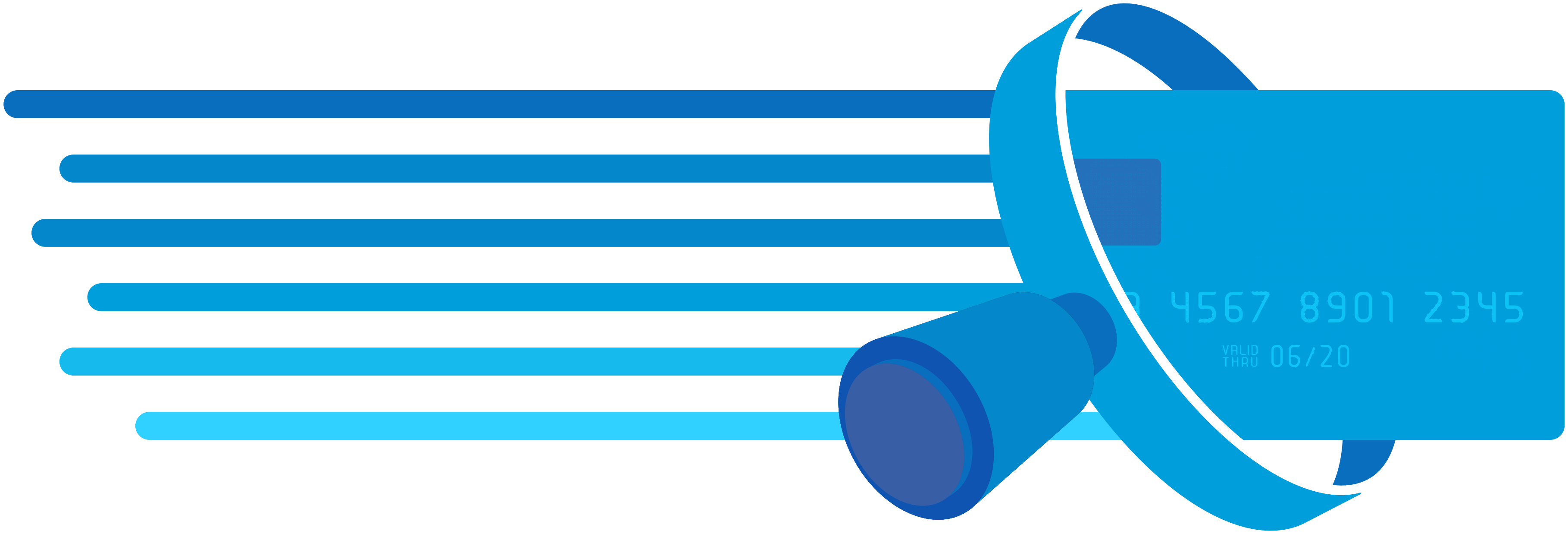
Small businesses are easy targets and can fall prey to online transaction breaches. Make sure to get a Secure Sockets Layer (SSL) certificate for your website to help protect your customers' valuable information.

How can I help protect online payments? cont.

8. Conduct regular security assessments

Lastly, tie up any loose ends with annual security assessments of your system conducted by experts who can perform penetration tests and vulnerability assessments to inspect your network like a hacker. They manually conduct tests, detect flaws that can be exploited, and provide suggestions to improve security. Additionally, they can discover unencrypted data leakage and loopholes in wireless and network security.

AT&T Cybersecurity Services can provide consulting and planning services that address the essentials of security with a multi-layered approach.



6 bonus tips to protect your business

- **Install updates.** Stay on top of patching, system/application updates, end of support/life platform migrations, user administration, and configuration management.
- **Secure your email.** Be aware that email and phishing are often used to deliver malware such as ransomware.
- **Protect your endpoints.** Use Endpoint Detection and Response (EDR) controls to protect "endpoints" such as desktops, laptops, mobile devices, Internet of Things (IoT) devices, servers, and routers from malicious web content.
- **Build a firewall.** Don't let hackers steal your customers' credit card information or company trade secrets. Use a firewall to establish a boundary between the internet and your own network.
- **Detect problems early.** Minimize the time it takes to detect and fix problems. Consider using a Security Information and Event Management (SIEM) system.
- **Use multi-factor authentication.** Most breaches involve the use of leaked authentication credentials. Always use strong, multi-factor authentication.

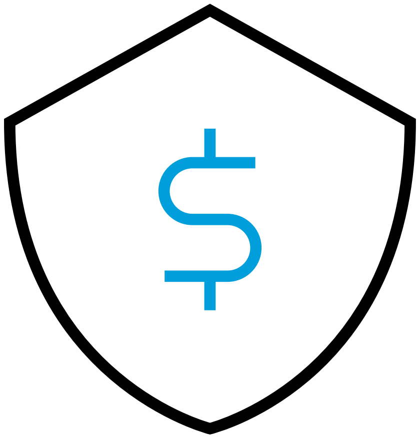
While many large businesses suffered breaches, small and medium businesses were an easier target for hackers because of their lack of resources and security expertise.[4]

[4] Forbes, Cybersecurity in 2022, https://www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity-in-2022--a-fresh-look-at-some-very-alarming-stats/?sh=64c54f766b61.

How to budget for cybersecurity

Learn to take a proactive approach

We get it. Small businesses are on tight budgets without much wiggle room. Although planning for a cybersecurity crisis may cost a company more day to day, it is still far more cost effective than being unprepared in a crisis, which can cost up to millions of dollars in mitigation and potentially hundreds of millions in reputation and shareholder value. Hear from a cybersecurity expert on how to create a cybersecurity budget.



All it takes is one employee to accidentally open a phishing email to create a company-wide data breach. Cybersecurity is a team sport and should be everyone's business. Consider budgeting for employee training on cybercrime.

Don't have time to become a cybersecurity expert? Consider hiring one. AT&T Business understands the challenges small businesses face. We can help you decide what products and services will work best for your business today in consideration of where you want to take your business in the future. See our Cybersecurity Consulting Services, which can help you tackle security essentials. And, visit AT&T Cybersecurity to learn more about our managed security services (MSS).

AT&T Business

Assess your cybersecurity risk

Take our quiz. Call for help if you need it.

Start with a free online assessment to understand where you are in your security maturity. This assessment, based on a survey of 500 security strategists, shows where your organization stands today. Based on your results, you'll see customized recommendations to help you improve your organization's standing. You can map your own cybersecurity maturity vs. others in your vertical such as financial services, healthcare, manufacturing, and retail.

AT&T Business is here to help small businesses in a big way. We have specialists focused on the technology and connectivity you need for businesses of your size in your industry – ready to share their knowledge with you. To learn more, contact your account team or visit the AT&T Business Cybersecurity site and we will contact you with more information.

AT&T named a

worldwide "leader"[5]

in the IDC MarketScape: Worldwide Managed Security Services 2020 Vendor Assessment

AT&T Cybersecurity ranked

No. 1

MSSP Alert's Top 250 MSSPs for 2020 list[6] and is a Finalist for SC Magazine's 2021 Best Managed Security Service[7]

Why AT&T?

Technology is complex and changes quickly. It can be difficult to know if you're making the right communication and connectivity choices. That's why we're with you every step of the way—offering insights, guidance, and solutions to uncover the right technologies to help your business thrive.

[5] IDC MarketScape: Worldwide Managed Security Services 2020 Vendor Assessment
[6] MSSP Alert's Top 250 MSSPs for 2020 list
[7] Finalist for SC Magazine's 2021 Best Managed Security Service.

AT&T Business