PDI TECHNOLOGIES

5 Common Security Challenges and 5 Steps to Solve Them

White Paper | 2022

Executive Overview

Cybersecurity is a serious matter, but you shouldn't feel afraid or overwhelmed thinking about it. This paper covers five common challenges that can impact your organization's cybersecurity posture, along with five steps to mitigate those issues.

Even if you don't have the in-house expertise to accomplish these steps on your own, rest assured that there are many options to supplement your cybersecurity strategy with a wide range of managed security services, solutions, and partnerships.

Can You Avoid the Predictable Disaster?

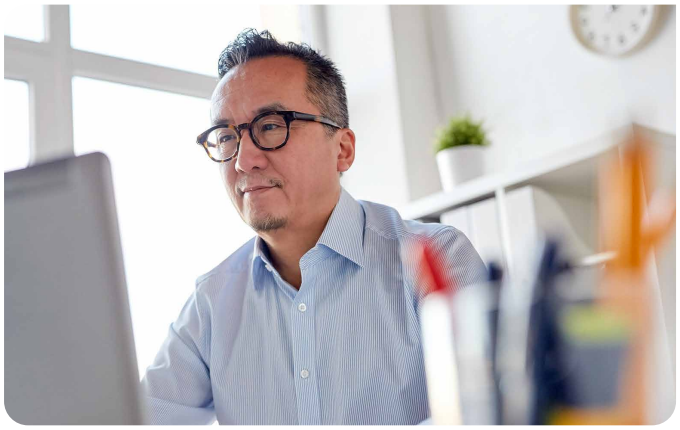
If you manage a business, you already face enormous pressure to optimize your operations, reduce costs, and continually improve your customer experience. Accomplishing that in the best possible market conditions can still be difficult. But when you factor in the additional challenge of having to worry about the rising number of cyberthreats, your job becomes exponentially more challenging.

While some business conditions and disruptions aren't predictable—such as the global COVID-19 pandemic—cyberthreats are just the opposite. It's no longer a question of "if" you'll experience an attack. It's more about "when" you'll get hit and how large the impact will be.

The good news is that a predictable event—like a ransomware attack—is something you can prepare for, which is why it's so critical to prioritize cybersecurity right now.

From the largest companies to the local convenience store, every business must prepare for cyberattacks. Even if you can't ever completely prevent an attack from happening, you can at least take steps to minimize the impact on your business.

Today, it's more a question of when, not if, you'll experience a cyberattack.



When you consider how sophisticated cyberattacks have become:

- How confident are you that your organization is prepared for this challenge?
- How much risk are you willing to accept?
- How effective do you think your cybersecurity strategy is?

If you're not sure how to answer these questions, it might be time to re-evaluate your approach to cybersecurity so you don't become just another statistic. Start by reviewing some common cybersecurity challenges to see where your business stacks up.

How to protect sensitive data

- Define a holistic cybersecurity strategy with clear processes and best practices
- Train your employees about cyberthreats and how to avoid them
- Leverage modern detection and response tools to minimize risk
- Perform and test regular data backups, keeping them at an offsite location in case your production data is encrypted

5 Common Cybersecurity Challenges

If you know that your business is being targeted for attack, what are the key factors holding you back from enhancing your security posture?

The most common obstacles are some combination of:

1. An ill-defined cybersecurity strategy
2. Outdated or disjointed cybersecurity tools
3. IT budget constraints
4. A lack of in-house expertise
5. Coverage gaps

Challenge 1: An ill-defined cybersecurity strategy

If you don't have a holistic approach to cybersecurity, you'll inevitably have gaps and vulnerabilities. It's critical that you have a willingness to prioritize cybersecurity from the executive level on down. With the recent string of high-profile ransomware attacks, business leaders are now much more willing to discuss cybersecurity.

Your strategy must account for budgeting, tools, staffing, and risk management. This is especially the case with the shift toward the remote working model, where more critical workloads and data are getting pushed to the edge of the network. In particular, highly distributed companies with many remote sites need a solid cybersecurity foundation with a central point of control and standardized policies to provide a minimum level of protection.

Challenge 2: Outdated or disjointed cybersecurity tools

If your business still relies on purely detective measures—and/or legacy security systems—you aren't adequately prepared for today's advanced cyberthreats. Although useful for controlling incoming and outgoing network traffic, basic firewall implementations aren't always enough to protect an IT network from increasingly sophisticated attacks. Moreover, in today's remote working world, there are many cases where a robust corporate firewall doesn't even exist between users and the Internet anymore.

Because every device and system connected to the Internet is a potential point of vulnerability, you need reliable tools for malware prevention, Web content filtering, secure VPNs and Wi-Fi, and much more. However, throwing together a hodgepodge of unrelated tools can often create a bigger problem. Multiple, independently functioning security tools can place an additional management burden on your already overtaxed IT staff.

Challenge 3: IT budget constraints

Even if securing your IT networks and sensitive data is a necessity, many organizations have difficulty finding the money for security-related investments. That's often the case even for those with a sizable IT staff and budget. And if your IT staff are already overworked, adding cybersecurity to their plate isn't going to help.

If you have the means to find and hire qualified IT security experts, salary remains one of the largest expenses. Add to that the recurring training to stay on top of evolving security threats, and the costs quickly add up. The same applies to security tools and infrastructure management activities such as software/firmware upgrades and appliance health monitoring. The overall cost can often feel overwhelming if you want to follow best practices.

Challenge 4: A lack of in-house expertise

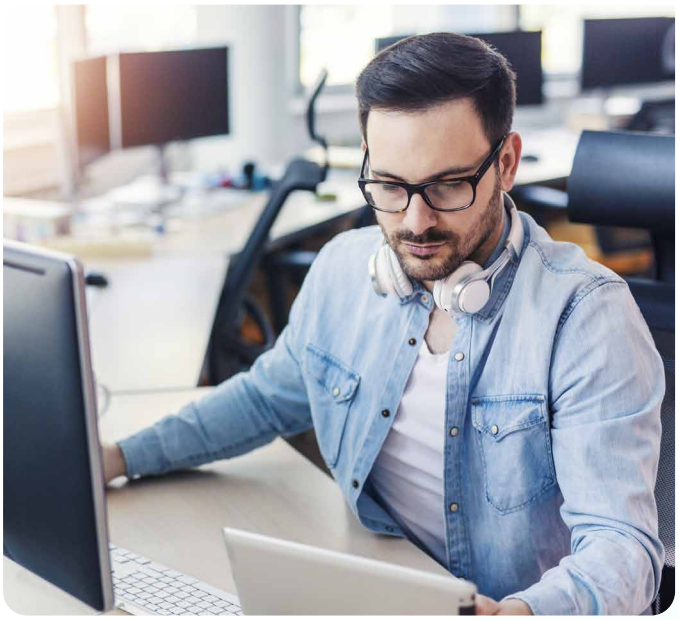
Apart from enterprise-class businesses, most organizations simply don't have the means to bring in full-time IT staff dedicated strictly to cybersecurity. Often, cybersecurity is handled by a few IT personnel already focusing on numerous other projects. They're less likely to know the latest threat tactics or the tools that can help prevent those threats.

A lack of expertise can also lead to an over-reliance on tools (whether or not they're the right tools for your particular needs). Unfortunately, a "set-it-and-forget-it" cybersecurity approach simply doesn't work. Proper installation and configuration are essential, but even more importantly, continued monitoring and management are required to help ensure that your security tools remain current and perform optimally.

Challenge 5: Coverage gaps

If cybersecurity gets lost in the flow of day-to-day IT activities, a data breach could take months to discover. But while employees take vacations and days off, cybercriminals and their automated attacks don't. That's why it's so important to maintain a vigilant watch 24/7/365. However, continuous security is more than just threat management—it involves proactively evaluating and updating policies to keep up with changes in your business.

That's one reason why many smaller businesses find it difficult, if not impossible, to maintain a high level of security on a continual basis. But if you don't have IT staff monitoring your systems on a 24/7/365 basis, you'll have gaps in coverage. And it might take only minutes for an attack to infiltrate and spread across your IT systems. Moreover, if you lack cohesive security technologies and processes, criminals will view you as "low-hanging fruit" that's ripe for attack.



MSSPs can help streamline your IT processes by:

- Troubleshooting connectivity issues faster
- Monitoring and updating security policies and user access
- Investigating, responding to, and reporting on security events
- Performing regular audits to meet regulatory and compliance requirements
- Proactively monitoring your overall security posture

If your business lacks internal cybersecurity expertise, a Managed Security Services Provider (MSSP) can supplement your IT team.

5 Steps to Boost Your Cybersecurity Profile

Once you understand the challenges you face, it's good to think about ways to increase your cybersecurity profile.

Start with these five steps:

1. Honestly assess your security posture
2. Fine-tune your security strategy
3 Prioritize threat prevention
4. Dive deeper on threat detectionand response
5. Conduct ongoing security awareness training

Step 1: Honestly assess your security posture

You can't understand your true cybersecurity readiness or define your strategy until you know what you're working with. In this case, that means getting an honest assessment about your IT systems and overall environment. A vulnerability scan helps identify weaknesses in your IT environment and predict the effectiveness of implementing countermeasures. You can conduct the scan yourself or bring in an outside vendor. The DIY approach is less expensive, but hiring an external consultant helps ensure a neutral third-party perspective.

A penetration test (also known as "white hat testing" or "ethical hacking") goes much deeper in probing your IT infrastructure. This process actively attempts to find security vulnerabilities that an attacker could exploit. It typically involves collecting information about the targets, identifying possible entry points, exploiting vulnerabilities, and reporting on the results. There are two key items to remember:

- The primary goal isn't to "pass" the test. It's to learn about your environment.
- It can be a very humbling experience, but the goal is to identify what you need to fix, even if it leaves you feeling exposed.

Step 2: Fine-tune your security strategy

After you discover where your business might be vulnerable, decide what risks you're willing to live with. This requires a discussion at the highest level of your company, because a cyberattack can take down your business with immediate and comprehensive impact. Every business must make practical tradeoffs in terms of cost, resources, and risk management.

When determining how much to prioritize security, be realistic about the financial threat you could be facing. For example, it's increasingly common for ransomware victims to pay as much as $10,000 per device just to get their business up and running again. Meet with your business leaders to find out how much risk they're willing to accept, then define a cybersecurity strategy (including tools, processes, and personnel) to support your needs. Create a budget that allows you to fix what you need today and also cover what you'll need for ongoing management.

Step 3: Prioritize threat prevention

No one has yet created a 100% impenetrable system. Although you can't prevent every threat, you can take steps to minimize the impact on your business. To elevate your security posture, you need prevention methodologies that block a wide range of application and system exploits. Make sure all your systems have up-to-date patches and the right software updates, especially for anything connected to the Internet.

To avoid data loss, you should also have a solid disaster recovery and business continuity plan. And be sure to regularly back up your data and maintain as many versions as necessary. Backups that are stored separate from your production workloads can be critical for getting your business up and running in the event of a ransomware attack that locks down your production systems.

Step 4: Dive deeper with threat detection and response

It's important to know that you can't account for human behavior, so the notion of completely preventing attackers from getting inside your organization is unrealistic. That's why you must be able to detect and respond to advanced threats and malicious actors when a breach occurs. Typically, this requires the right mix of cybersecurity tools and human expertise.

For example, it's a good practice to act as though you have less than two hours from the time of infection to the point when a cybercriminal can exfiltrate or encrypt your data. This is why you must be able to quickly sort out real threats from false flags and anomalies. If you find a credible threat, real-time response is often the difference between isolating the threat, minimizing the blast radius, or experiencing an actual breach.

Step 5: Conduct ongoing security awareness training

As much as you need the right cybersecurity tools and processes, you can't neglect the human factor. If an employee opens the wrong email attachment, the best tools in the world won't always stop a threat. Despite how unintentional any process gaps or human error might be, both can have serious consequences on your business.

Ongoing security awareness training and easy-to-understand security policies are vital, especially for non-technical employees. Every employee (part-timers and seasonal workers included) must be aware of the potential threats and know what to do if they encounter one. This training extends to business leaders, because they must have a ready-made plan for how to deal with a significant cyber incident.

Supplement Your Cybersecurity Strategy with Outside Help

Maintaining cybersecurity best practices can feel like a heavy burden for organizations with limited IT expertise or budgets. Fortunately, there are a wide range of vendors that offer managed security services and solutions to supplement your own security measures.

These vendors can serve as an extension of your internal IT staff, managing critical cybersecurity monitoring and detection tasks while lending expertise to reduce IT complexity and costs. In the meantime, these vendors free you up to focus on what you do best.

In fact, working with a reputable vendor is often the safest and most cost-effective option to:

- Reduce the number of IT security personnel you need to hire, train, and retain
- Decrease downtime with faster incident response and containment
- Access a team of highly trained experts in a 24/7/365 security operations center (SOC)
- Simplify your compliance and regulatory processes
- Continually benefit from the latest security technologies, tools, and tactics

Ongoing security awareness training for all employees is critical to preventing a cyberattack.

Key benefits of working with a managed security services partner

- Continuous monitoring
- Anti-virus and anti-malware tools
- Network firewalls and VPNs
- Intrusion prevention and detection
- Event logging and content filtering
- Vulnerability and patch management
- Remediation
- Centralized reporting

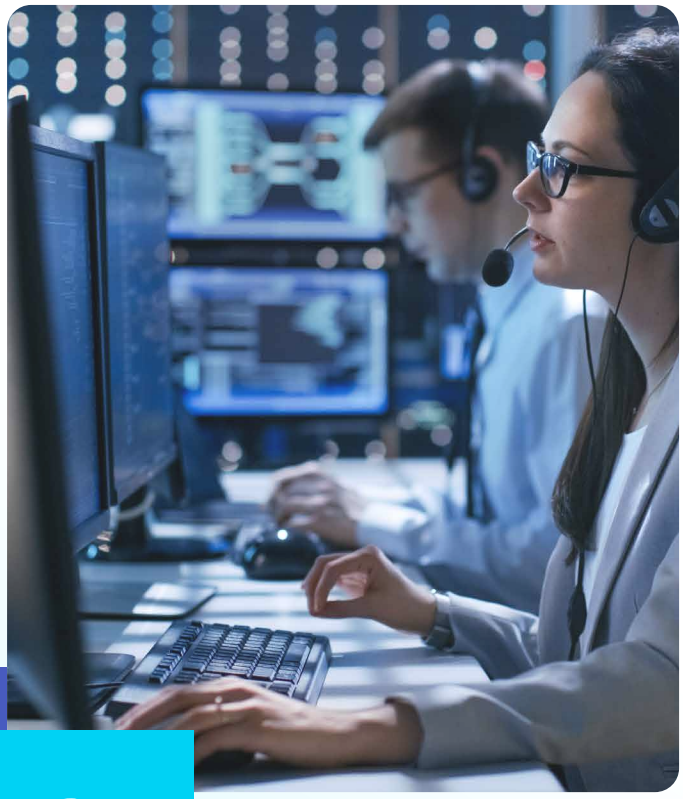
Elevate Your Cybersecurity Posture

If you have the expertise and budget to enact cybersecurity best practices across your business, make sure your tools and technologies are as sophisticated as the cyberattacks you're trying to prevent. If you're looking for ways to supplement your cybersecurity strategy, seek out a reputable vendor that can cover everything you can't.

Note that the actual scope of capabilities can vary from vendor to vendor, so make sure they're aligned with your unique business goals. And with the comfort of knowing your digital footprint is secure, you can concentrate on:

- Adapting faster to the latest market trends and disruptions
- Improving operational efficiency
- Growing revenue and increasing profitability

To learn more about smart ways to enhance cybersecurity, visit **www.pditechnologies.com/pdi-security-solutions/** or contact PDI for a deeper discussion about how we can support your business.



About PDI

Professional Datasolutions, Inc. (PDI) software helps businesses and brands increase sales, operate more efficiently and securely, and improve critical decision-making. Since 1983, PDI has proudly served the convenience retail and petroleum wholesale industries. Over 1,500 companies, representing more than 200,000 locations worldwide, count on PDI's solutions and expertise to deliver convenience and energy to the world.

For more information about PDI, visit us at **www.pditechnologies.com**.