protelligent®

How Do I Assess My Cybersecurity Risk Footprint?

Checklist

Every single business operating today has some level of connectivity and IT infrastructure; even a single-person firm. Which means that we are all at risk for a cybersecurity attack. We're not ones to fear-monger but given that cyberattacks are not simply a part of doing business and living in our connected world, we do encourage businesses to stay realistically apprised of the risks. These days, the best modus operandi is to expect an attack to happen to you.

The Critical Risks of a Cybersecurity Breach

- **Cybersecurity breaches can make a major financial impact:** 95% of breaches are financially driven, with the average cost of a data breach reaching $9.48 million in 2023.
- **Breaches deliver a long-lasting "ripple" effect:** the costs of getting hit by a cybersecurity breach are multifaceted. They can not only include any ransom your business might pay, but also lost revenue from extended downtime, customer loss—and associated revenue loss—following a breach, legal fees, increased insurance costs, and audit fees—which can be up to 13.5% higher for companies following a data breach than for those without one.
- **Loss of customer trust + impact on business reputation cannot be understated:** indeed, the lingering ripple impact of a breach can follow your business for years to come, resulting not only in an immediate loss of customer trust and business but also in damages to your reputation that can hurt potential business down the road. Depending on your business, your customers are entrusting various forms of data with you.
    - One Centrify study found that 65% of data breach victims lost trust in an organization as a direct result of the breach.
    - Another study found that 85% of breach victims tell others in their network about their experience.
    - After all, how would you handle it if your business or personal data was impacted by a breach?

The Compliance + Insurance Factor

Regulatory compliance and cybersecurity insurance are getting more stringent, which means you'll soon be required to take these steps, with a hefty financial impact in the form of non-compliance fees and increased insurance costs (if not insurance denials) if you don't. Why not get ahead and into the habit? You can even turn your proactivity into positive communication with your clients, letting them know you're prepared to protect their data in the case of a breach, and building trust ahead of an incident—so that when you're hit with one, not if, they're aware you've been doing everything you can, making them far more likely to keep their business with you.

How to Perform a Cybersecurity Risk Assessment

Performing a cybersecurity risk assessment is a systematic process you can perform regularly to understand the size of your business's risk, as well as what endpoints and assets are most vulnerable. It will help you understand and assess the likelihood of security events, determine their potential impact, and then map out recommendations for additional security controls. As they say, you can't manage what you don't know: these risk assessments give you an actionable plan to manage your business's cybersecurity.

- **Determine the scope:** Depending on the size of your business, you could regularly perform a risk assessment on your entire business, but if this is too large, it's helpful to break up your scope and move through the business in phases. This could be by business unit, location, or a specific part or function of your business.
- **Determine which compliance standards you need to follow:** Most industries these days must adhere to compliance standards, whether HIPPA for health fields, NIST, ISO, or the FTC's rules and standards. It's not only crucial for compliance and customer data protection that you understand which ones you fall under the governance of, but these standards also provide helpful guidelines for each step your business needs to take to establish and maintain a resilient security posture.

- **Get buy-in:** No matter where you start, it's vital to have the buy-in and participation of all stakeholders within your current scope. Cybersecurity has as much to do with employee awareness, education, and participation as it does with security controls. A third-party assessment partner can help you gain buy-in and ensure success by bringing in expertise, change management, and project management.
- **Identify your assets:** The next main task is to create an inventory of all your business's assets—within your scope—that would be at risk. What has the potential to be targeted by attackers? You should think about the types of assets that are critical to your business as well as any systems that attackers might want to take control over. You should also create an inventory of every type of customer data you hold, where it's kept, and who has access to it. This goes for any other types of sensitive data too.
- **Visualize access with a network architecture diagram:** From your asset inventory, you can create a network architecture diagram that maps out and helps you visualize all the potential interconnections and pathways to access your assets—as well as potential entry points to your network. This will help you bridge to the next major part of your risk assessment: identifying your business's potential threats.
- **Identify threats:** Threats are any of the tactics, techniques, and types of attacks that "bad actors" might use to attack your business. New threats are constantly emerging—especially with the onset of AI—and it's best practice to stay abreast of what they are. Good resources for news and updates on the latest, emerging, and consistent threats include government agencies like the Cybersecurity and Infrastructure Security Agency (CISA) and resource libraries like Mitre's ATT&CK® Knowledge Base. A good third-party cybersecurity partner can also provide helpful insights and expertise based on what they see "on the ground" every day and can also help break threats down into layman's terms so they're simple to educate employees on.
- **Determine consequences:** As you identify the threats, identify their potential consequences as well. For example, a common vulnerability is not running software updates. Because software updates commonly include patches to fix known vulnerabilities, not running these gives attackers an easy, common knowledge entry point to look for. This vulnerability could give a threat actor the opening to make an SQL injection—a common threat type where they inject a bit of code that enables them to either view or modify a database. The consequence? They're then able to further burrow their way into your network systems and extract sensitive information such as financial details, private customer data, and proprietary information. The consequence doesn't stop there though: this would result in regulatory fees, insurance increases, loss of customer trust, and damage to your reputation.
- **Assign risk levels:** A strong security posture addresses the highest threat levels first, then moves down through your priorities. You can create a straightforward risk matrix by ranking threats according to how likely they are to happen, beginning with Risk Level 1 (Rare) and moving up to Risk Level 5 (Very Likely). You can also rank their consequences from Level 1 (Negligible) to Level 5 (Very Severe).
- **Develop response plans:** With your assets, threats, consequences, and risks identified, now you can determine your responses. These will include updating or adding new security controls but should also include backup and disaster recovery plans.

  As we said in the beginning, you should expect an attack. Even the most solid defense may not be impenetrable though. This is why the most resilient defense strategy includes a plan for what to do with the inevitable happens. How quickly would you be able to recover your data and your systems? How will you address a breach with your employees and customers?

  Having a plan of action means at the first sign of a breach, you can jump in and stop it faster, minimizing the damage. It also means you'll be able to communicate with your customers so they know you were prepared ahead of time and did everything you were supposed to do—which will help maintain their sense of trust and help prevent the loss of their business.

Make Governance a Priority:

Verizon's 2023 Data Breach report found that "74% of all breaches include the human element, with people being involved either via Error, Privilege Misuse, Use of stolen credentials or Social Engineering."

While we're all familiar with social engineering attacks like phishing, which trick employees into transferring money or data, employees are also used so threat actors can gain access to applications without their knowledge. Either way, employee training and awareness are critical when it comes to protecting your business from cyberattacks. And it's just one piece of the pie when it comes to governance:

- **Establish effective password management:** Support your organization in the use of password management applications and remind employees to change their passwords on a regular schedule. Train them on what makes for a strong password.
- **Maintain software updates:** As we mentioned earlier, one of the most common vulnerabilities is software updates that haven't been installed. This gives attackers an easy entry. You can introduce automation to ensure these software updates get run, but also make sure to educate employees on why they're important—and the consequences of not running them—so they understand they're not just a nuisance, they're critical for the business.
- **Go beyond making a security checklist for compliance:** You're likely required by a variety of compliance standards and/or cyber insurance to create this type of checklist. And while it's true that those standards can be used as a helpful guide to establish a strong security defense, it's important to actually use them. If you're simply checking off a box to say you have something, you're not really preparing or protecting your business for the very real case scenario when you're hit by a breach.
- **Establish a project lead and committee:** This step may be required by different compliance standards, but it's also simply an effective way to ensure security is being managed actively. Name someone in your IT or Operations department as the project lead for cybersecurity, with a committee made up of department heads. This person should also be responsible for making reports to your board as to your cybersecurity defense; an external cybersecurity partner can also help you prepare these reports.
- **Manage risk with vendors up and down your supply chain:** Not only are small- and mid-sized businesses (SMBs) increasingly the main targets for attacks themselves, but businesses up and down the supply chain are breached so attackers can then gain access to their ultimate target. We're all connected, so your business is only as secure as your vendors. Create a security checklist to go through with each of your vendors to ensure their security standards are up to yours, and your data and your customers' data are being protected at every potential endpoint.
- **Conduct internal and external penetration testing:** Another step that is now often required by compliance and cyber insurance, you should regularly perform internal penetration testing and then validate those tests through a third-party external penetration test. These tests launch "mock attacks" into your systems to search out each potential vulnerability, enabling you to identify these and then take steps to fix your security weaknesses and prevent actual damage. These steps take your threat and vulnerability assessments a step further and exploit the weaknesses in your system, so you understand what they are and how to fix them. Again, these are now commonly required for you to perform on an annual basis at a minimum.

protelligent®

Get an Expert, Third-Party Assessment of Your Security Posture

Cybersecurity is mission-critical for your business, but you don't have to go it alone. We didn't build Protelligent on tiers and transactions but on a duty to be better than the rest. Engineering-minded and purpose-driven, we traded the traditional MSP model for something more personal, proactive, and intelligent. We believe that you deserve access to enterprise tools and talent, always-on services, business insights, and reliable support because innovation should always be within reach.

We can help you reap the benefits of an enterprise IT team, with deep security expertise and capabilities, without the hurdles of hiring a full-time employee. Starting with helping you understand and assess where your risk levels are at.

Schedule a no-cost meeting with a seasoned security professional to discuss your current security posture and risks. Together we can gain a clear understanding of your vulnerabilities, how to fix them, and create a plan to protect your business from financial and reputational damage. Post-call you will receive an actionable recommendations document to help you better secure your environment and protect your business.

Contact the Pros