Assessing Your Cybersecurity Risk: Why, What, How?

A risk assessment can reveal unique vulnerabilities that could impact your company. Here are the basics you need to know.

Business today is inseparable from digital tools and data. Although this widespread digitization has many advantages, it also comes with the rising threat of cybercrime. Many organizations understand the need for reliable cybersecurity, but more must be able to achieve it. Assessing a business›s unique cyber risks is the first step.

Why Perform a Cybersecurity Risk Assessment?

Cybersecurity incidents are costly and getting costlier. In ٢٠٢١, the average data breach cost reached ٢,٩٨$ million for small businesses, a nearly ٢٧ percent increase over ٢٠٢٠. These smaller companies also make ideal victims because they often don't have robust protections and may falsely assume, they're not valuable targets.

If businesses don't want to suffer those losses, they must address any possible vulnerabilities a cybercriminal could exploit. Because every system in every organization differs, those specific weak points will vary. A risk assessment can reveal those unique vulnerabilities, providing the basis for the most effective mitigation measures.

What the Assessment Should Cover

When planning a cybersecurity risk assessment, it is vital that it covers all vulnerabilities. Although the organization's network is the most obvious place to start, it's just one of many areas that deserve attention.

Other potentially vulnerable areas to assess include:

- Data storage, both on premises and in the cloud
- User behavior and security knowledge
- Web-based applications
- Internet of Things (IoT) endpoints
- Disaster recovery systems
- Third-party vulnerabilities

Risk assessments should also look at more than just what's at risk. For these audits to be helpful, they also need to weigh each vulnerability's likelihood of being exploited and the potential impact. This will help rank their urgency, revealing which need the most attention and investment.

Depending on an organization's industry and location, they may face also regulatory guidelines over what these assessments should include. For example, the Health Insurance Portability and Accountability Act requires physical and administrative safeguards for protected health information, not just technical ones. Companies should review any applicable regulations for guidance on what assessments should cover.

How to Assess Your Cybersecurity Risk

Once businesses know what to include in their risk assessment, they can begin the actual audit process. Many third-party specialists offer assessment services, which may be the best option for companies with minimal cybersecurity experience. However, other organizations may prefer to perform these assessments in-house to minimize costs.

The first step is to gain complete visibility across the network, including devices, third-party dependencies, and other risk factors. That includes mapping data flows, auditing access privileges, and reviewing past incidents. Once teams have a map of how information and access flow throughout the company, they can see where vulnerabilities may arise.

As auditors find risks, they should classify them by likelihood and severity. This is possible by looking at what has affected them in the past and reviewing industry-specific cybercrime trends. For example, although just ١ percent of attacks in the energy sector involve ransomware, it's one of the most common attack types in manufacturing, so manufacturers should consider ransomware protection more heavily. Some organizations may want to perform penetration tests. This involves hiring a cybersecurity expert to attempt to breach its security to reveal weak points, so it's an excellent way to learn of overlooked company-specific vulnerabilities. It's also a good way to measure human issues such as susceptibility to phishing, which can be challenging to quantify otherwise.

Throughout the whole process, keep thorough records. The more hard data your business has, the easier it will be to communicate risks to stakeholders and implement necessary changes.

Cybersecurity Risk Assessments Are Crucial for Businesses Today

Cybercrime is a pressing and continually evolving threat for any company today. Consequently, regular cybersecurity risk assessments are increasingly crucial to ensuring a business's success. Performing these audits at least once a year can help guide security decisions and keep businesses safe from emerging threats.