Do You Know the Risks of In-House Security Risk Assessments?

Written by
CompliancePro Solutions

Posted on
Oct 25, 2022 9:56:38 AM

Who doesn't like a little DIY? You save a little money. You get bragging rights. You may even learn a thing or two. But there's always that chance something could wrong, costing you more in the long run. Sometimes it's better to let a professional handle a project and get it done right the first time—especially for complicated projects far outside your skill set.

Security assessments are often one of those tasks best left to an expert. If you don't get it right, your data, your business, and your reputation could bear the consequences.

Are Security Risk Assessments Necessary, Really?

For organizations within certain industries, such as healthcare and government third-party contractors, risk assessments are mandatory for compliance or certification. But for organizations outside those decrees, some question whether a security assessment is even necessary. They might feel they're too small to be of interest to hackers—a missed software update or a few weak passwords won't matter. Others may think they have a strong cybersecurity program in place, they've done it right, they're not at risk—security assessments are just overkill. In truth, every organization is at risk. Cybercriminals aren't concerned with an organization's size, industry, etc. They want easy ingress. They seek vulnerabilities: unpatched software updates, network security holes, weak firewalls—any frailty that gains them access.

Real-Life Testaments

The Equifax data breach speaks as an object lesson to the necessity of security assessments. In 2017, bad actors discovered a weakness in the company's web application framework and pirated sensitive data of 143 million customers. The last reported cost of the breach totaled $1.5 billion.

Another example is brought to us by a public research university for diagnostic, preventive, and rehabilitative care. A cybercriminal was able to infect the facility's system with malware, which exposed the electronic protected health information (EPHI) of 279,865 patients. The Office for Civil Rights (OCR) investigated and determined the university violated several HIPAA rules. One of the many infractions was ***the failure to conduct a thorough and accurate risk analysis***. The OCR hit the facility with a $875,000 fine.

In 2022, the average cost of a data breach is estimated around $4.35 million.

Data breaches and security are more than just about money, though. Reputation, customer data, and customer retention are always at stake. Customers and clients want assurance that their data or networks are secure. Proactive measures, such as risks assessments are cornerstones of that assertion and trust.

Outsourced or In-house Assessments?

This is where many organizations get stuck—to outsource assessments or conduct them internally. Sometimes organizations jump into an in-house assessment thinking it saves money and bypasses the hassle of finding a reputable assessment partner. But upfront costs shouldn't be the deciding factor. An insufficient self-assessment that to fails detect vulnerabilities will most likely cost more down the road when a hacker uncovers a weakness.

Let's take a look at three common risks of internal security assessments and why outsourcing may be the better way to ensure your organization is thoroughly secure.

Top 3 Dangers of In-House Security Assessments

#1 - Insufficient Expertise

Many organizations, particularly small-to-medium businesses (SMBs), lack the expertise to perform comprehensive risk assessments. Data and network security are vital to an organization. Someone possessing full-spectrum expertise should manage the intricacies of analyzing security vulnerabilities. Just one missed defect could be the "broken window" access point for a cyber saboteur.

> **Outsourced Assessment Benefit:** Third-party auditors possess the expertise to perform comprehensive assessments—it's what they do every day. They know what hazards to look for, the degree of risks associated with those hazards, and what is critical for formidable security.

#2 - Limited Internal Resources

Even if a business possesses staff with abundant expertise, do they have the time? Many IT departments are overworked and overwhelmed already. Piling on additional duties can endanger not only the integrity of their standing responsibilities but also that of the assessment.

> **Outsourced Assessment Benefit:** External assessors are focused on your assessment only. They can perform it in a timely manner without distractions—unlike your staff, who could be pulled to other duties during the course of the assessment.

#3 - Unreliable Objectivity

Who better to perform a security assessment than those who know and manage the organization's networks and security day in and day out? But self-evaluation is often tricky, even for an organization. Objectivity can be hard to come by when internal workers are so accustomed to the organization and its systems—they may overlook elements that are too familiar—even ones that are deficiencies.

> **Outsourced Assessment Benefit:** Third parties aren't afflicted with familiarity and routine that can breed complacency; they carry a fresh perspective of your networks and security measures and may notice vulnerabilities that onsite staff could overlook.

Looking Out to Strengthen Within

When organizations perform risk assessments internally, they often base the decision on cost, trying to save a little money. But lack of onsite expertise, limited resources, and questionable objectivity can taint security self-assessments—leading to a security incident and even more expense. Furthermore, a quality, third-party assessment might not be as expensive as you think. Outsourced assessors can ensure the experience, dedication, and clarity that will deliver an exhaustive security risk assessment, imparting peace-of-mind for your organization's security status.

Read more on how CompliancePro Solutions can help your organization with security risk assessments and security automation.