White Paper

Are You At Risk?

9 Common Security Mistakes Your Organization Might Be Making

Abstract

- Gartner reports that the cybersecurity market is projected to grow to $175.5 billion by 2022.
- The average cost to deploy security automation is $2.88 million, according to the study. Without cybersecurity solutions, a company could risk up to $4.43 million in breach costs, according to the Ponemon/IBM 2018 Cost of a Data Breach Study.
- International Data Corporation (IDC) Worldwide Business Resilience Readiness Thought Leadership Survey says three out of ten organizations have no plans in place for a security disaster.
- IDC also says three quarters of companies surveyed believe their cloud data is insufficiently secured.

Based on statistics like this, and our experiences providing IT security services and consulting to companies of all sizes, we're comfortable saying that most companies should be very concerned about their security practices.

There are nine security mistakes that are commonly made over and over again. Companies that are making any of these should consider themselves extremely vulnerable to compromise and possibly breach. Continue reading to find out what these common security mistakes are and what you can do to avoid these mistakes. Before it's too late.

9 Common Security Mistakes

Security Mistake #1:

Overlooking social engineering.

Does your organization specifically train employees on social engineering? How to recognize it and how to handle it? Social engineering is a commonly exploited threat vector, especially now that Twitter, LinkedIn, Facebook and other social networks make it trivial for an attacker to piece together internal details about your company. Phishing via email is the most common social engineering vector we see. It's dangerous because so much information can be gleaned – and stealthy malware can be transmitted – in emails that appear legitimate to end users.

Security Mistake #2:

Assuming you haven't been compromised.

Many people assume that if they haven't been personally alerted of suspicious activity – a financial institution flagging an unusual transaction or an IT department noticing something odd – then they're in the clear. But the truth of the matter is that in the past two years, whether you know it or not, you have likely done business with a company that has been compromised. Sophisticated attackers can penetrate a poorly secured network while barely causing a ripple.

If you don't have active credit and fraud monitoring mechanisms in place and your accounts do get compromised, untangling the mess could take months, and the financial and reputational impacts could persist for years. In 2018, IBM Security and the Ponemon Institute Cost of Data Breach Study suggested a single breach costs an average of $3.86 million to a company, up 6.4% from the prior year.

Security Mistake #3:

Assuming you're too small to be a target.

Small businesses, you're not off the hook here. People ask us what industries and business sizes are at risk. Our answer? Everyone is at risk. Regardless of how mature an organization may be on its IT journey, many are finding it impossible to manage data transactions happening both externally and internally. Many are also finding it too expensive to maintain the proper headcount to support a quality security solution. This combination of valuable assets and immature cybersecurity makes them a very attractive target: "low-hanging fruit" for attackers. It explains why 70% of cyberattacks target small businesses, according to the National Cyber Security Alliance.

Security Mistake #4:

Neglecting organization-wide password security.

Recently, an enterprise business engaged Involta to perform a security assessment. As part of that assessment, one of our security specialists went into the company's headquarters. In under an hour, with no special equipment, the specialist had a list of 86% of the employees' passwords, including the CEO's.

The good news: the company recognized the need for stronger security and engaged Involta as a partner. Since then, that company aced a third-party security audit. The reason we were able to grab so many passwords with such ease? The company hadn't properly configured its active directory environment. In a company's active directory, there are hundreds of parameters that can be configured in terms of policies and privileges, but many are not set by default. Meaning that if you don't set up some of the foundational settings in the active directory, you might as well slap a "Welcome Hackers" sign on it. Using weak passwords, saving passwords in browsers, writing them down on a notepad under your keyboard and using the same password for multiple accounts are some of the top mistakes that will most certainly get an organization hacked.

Security Mistake #5:

Trusting antivirus programs to protect you.

Now, regularly updated antivirus protection from a leading company is a solid defense strategy against malware. But those programs don't protect you from zero-day exploits – malicious intrusions taking advantage of just-discovered vulnerabilities in programs or protocols. Also, most malware these days goes undetected. Security should be a layered approach, using a number of harmonious tools to secure your data.

Security Mistake #6:

No one "owns" security.

When there's a critical lack of focus on security in an organization, often it is because no one "owns" security. If you're an enterprise business, you should have someone identified as your security leader. In most organizations, that's a CSO or CISO, or sometimes a Director of Security. Who that person reports to is really important. Your security leader should not report to the same people that the implementers report to, because it creates an inherent conflict of interest at the top of that chain. When we consult, we advise organizations to have the CSO/CISO report to the CEO.

Security Mistake #7:

You don't have a breach response plan.

You need to have a security breach response plan. You have to know that a reputation-impacting breach could happen to your company and have a plan for what you'll do if it does. International Data Corporation (IDC) found that 78% of consumers would take their business elsewhere if directly affected by a data breach. If a security breach is not properly handled quickly, the company risks losing some or all of its customer base. A data breach doesn't instill confidence in your customers. You probably know by now that it can literally be a public relations nightmare for organizations.

The faster your organization can detect and respond to a data breach or even security incidents, the less likely it will be to have a significant impact on your data, customer trust, reputation and a potential loss in revenue. Ultimately, you have to know how you will alert your customers. What media outlets will you contact? What law enforcement agencies need to be notified?

Security Mistake #8:

Assuming that a "security" firm knows what they're doing.

Anyone can call themselves a security organization. But it's one thing to brand yourself as experts in an area; it's another thing entirely to be able to execute.

If you have a low level of IT security knowledge and you're looking for a security partner, talk to references. Do your homework. In particular, ask about third-party audits. For example, every year Involta gets audited by a third party for our managed services, finances and data center operations so our customers can be confident we meet the same requirements we preach. Involta has assisted customers in achieving successful results for a variety of review standards (PCI-DSS, NIST, COBIT, GLBA, ISO/IEC 27000-series, HIPAA/HITECH/Omnibus, SOX, J-SOX and internal assessments).

Security Mistake #9:

Not understanding the true importance of security.

The biggest mistake you can make with regard to security is not taking it seriously. Risk doesn't feel real until you have had a loss. Many organizations either haven't suffered a loss or haven't suffered a large enough or recent enough loss to make a lasting impression. As a result, their security programs are starved for people and resources. Until something forces them to act. Don't wait.

How Involta Can Help

All companies are at risk for a security breach. Organizations today are beginning to understand that it is no longer a matter of if they will experience a security breach, but rather when it will happen and how they will respond to it.

Involta Secure delivers security consulting and a suite of SOC Services, which include both host and parameter defense layers to clients large and small. Involta goes beyond traditional security to provide an advanced solution that protects your business. Monitoring and analyzing your business's security posture on an ongoing basis through a combination of supported security toolsets, incident response and operational process is the key to securing your most critical assets. We'll monitor your systems around the clock and manage predictive toolsets so we can stop attacks before they happen.

About Involta

Involta is an award winning national IT service provider and consulting firm. Involta helps organizations plan, manage and execute hybrid IT strategies using a broad range of services including colocation, cloud computing, managed IT, cybersecurity, fiber and network connectivity. Involta has industry-specific services for healthcare, manufacturing, finance, and technology that enable compliance and IT transformation initiatives.

Involta maintains partnerships with top tier technology vendors and major public cloud providers such as Cisco, Veeam and Pure Storage and employs a large number of highly certified technical engineers dedicated to building reliable and secure solutions. Through innovative consulting engagements, Involta is able to utilize its unique resources and partnerships to deliver advanced hybrid IT solutions that meet the ever-changing needs of organizations while maintaining the Involta brand promise of Superior Infrastructure, Operational Excellence and People Who Deliver.