INTERACTIVE SECURITY

JUSTIFYING REGULAR RISK ASSESSMENTS: *A CYBERATTACK COULD MEAN A SIGNIFICANT LOSS OF BUSINESS, LAWSUITS OR MUCH WORSE*

Performing regular risk assessments help generate a greater sense of trust with clients and investors and as a result, better position companies to win business and strengthen their reputation

Author: Emory Vandiver
VP Business Operations/Partner
Interactive Security
www.intactsec.com
267.824.2500

Is it ever "OK" for a company to be willing to risk losing its data and/or the data of its customers or partners? *Obviously not*. Even though technology continues to advance in terms of cybersecurity, nobody is immune to the threat of data loss or hacking. Depending on the industry of an organization, a cyberattack could mean a significant loss of business, lawsuits or much worse. A first step toward preventing such incidents from happening is to opt for regular risk assessments – it's prudent for several reasons:

- **THE CHANCE TO EITHER AVOID OR MITIGATE THE RISK**

After performing a risk assessment, a business becomes empowered to better identify the probability of various risk(s) and their associated potential impact(s). If there's a higher probability of a certain risk occurring, and a severe impact would result, then preparations can be made proactively to begin eliminating risk. Or, if there's a higher probability but the impact isn't serious, less urgent risk mitigation can happen instead. Knowing how to differentiate between these two scenarios can help prevent operational inefficiency such as dedicating unnecessary amounts of time, money and resource toward a non-urgent task.

- **REDUCING THE RISK OF DATA LOSS ALSO REDUCES THE RISK OF PAYING FINES**

In 2009, TJMaxx faced a hefty $9 million fine due to data loss following security breaches. Government agencies found that the retail outlet hadn't provided an adequate level of protection when safeguarding its customers' data. Although most companies are unlikely to face fines at this scale, it's still worth taking proactive measures to avoid them altogether. When organizations engage in regular risk assessments and follow the advice of the experts performing them, they can then easily illustrate they've taken the right steps toward protecting client information.

- **REGULAR RISK ASSESSMENTS AVOID DISRUPTIVE NETWORK OUTAGES**

If you cast your mind back to 2017, you may remember the Ransomware attacks that resulted in significant digital network breaches. After successfully infiltrating networks around the world, hackers demanded ransoms amounting to millions of dollars. One of the most severe and public examples was such a breach was the case of the United Kingdom's National Health Service which was forced to cancel a significant number of their operations. Although such outages are rare, they tend to occur in networks where the owner hasn't mitigated risks against current threats. Again, engaging in regular risk assessments, provides visibility into potential threats and reduces the chance of a similar business disruption.

- **INSPIRE GREATER CONFIDENCE WITH CUSTOMERS AND CLIENTS**

Depending on the nature of an organization's business and their industry, their clients may be quite concerned to know how their data is protected. In fact, many companies now require detailed information from their vendors so they can verify that their data is being handled and secured properly. Organizations that submit to regular risk assessments have found them to be a competitive advantage in the eyes of clients - they promote a greater sense of trust and accountability resulting in more business won and a strengthened reputation.

Regular risk assessments bring many operational benefits and thus should be scheduled routinely in advance. By maintaining a regular schedule, no room is left for failure when it comes to maintaining the safety of your data and network.

About Interactive Security

Since 2007 Interactive Security, Inc. has been at the forefront of providing industry leading expert information technology security services to clients across the globe - focused on IT Security Auditing & Compliance.

Our team is comprised of highly skilled industry certified professionals with diverse experience serving technology consulting firms and enterprise security departments. We serve a broad base of clients and industries including the payment card industry, finance, legal, healthcare, education, government, restaurant and hospitality.

Our clients and partners choose Interactive Security because of our uncommon ability to provide expert custom IT security services that exceed both technical and business expectations.

We pride ourselves on Making ***IT COMPLIANCE OBTAINABLE, SIMPLE AND AFFORDABLE.***

*Vulnerability / Penetration Assessments * Application Security * BCP/DR Planning * PCI DSS * HIPAA * HiTRUST * ISO 27001-27002 * ISO 31000 * NACHA ACH * FEDRAMP * FISMA/NIST * GDPR * Privacy Shield*