Cybersecurity

The 5 Critical Elements of Risk Assessment

You do a number of things to maintain your business: update insurance policies, upgrade equipment, and conduct personnel reviews, just to name a few. Given the challenging cybersecurity environment, adding a cybersecurity risk assessment to the list makes sense. Learn about the five critical elements of a cybersecurity assessment.

XANTRION
CYBERSECURITY • IT SUPPORT

Introduction

Cyber risk involves any potential threat to your electronic data, usually in these three main areas:

- Data integrity - data that is accurate and that has not been tampered with.
- Data security - data that can only be accessed by authorized users.
- Data availability - data that your authorized users can access reliably, whenever and wherever they need it.

Why Perform a Risk Assessment?

Lost or compromised data could potentially bankrupt your company. A risk assessment gives you the information you need to create a risk management plan. A risk management plan, in turn, ensures that the measures you put in place to protect your data are both appropriate and cost-effective.

An effective risk assessment addresses all of these questions:

- What threats are most likely to occur?
- Which of these threats are likely to have a significant impact on your company if they do occur?
- What strategies should you use to prevent and mitigate threats?
- Which strategies offer the best combination of cost and effectiveness–neither leaving you exposed to risks you aren't aware of, nor wasting money on solutions that guard against risks that you may not actually face?

Which strategies offer the best combination of cost effectiveness–neither leaving you exposed to risks that you aren't aware of, nor wasting money on solutions that guard against risks you don't actually face?

In addition to protecting your business, performing a cyber risk assessment makes you a more desirable business partner. Just as your partners and customers want to see proof that your company is insured or has audited financial controls, being able to show them that your cyber risk management plan is in order will reassure them that working with you doesn't endanger their own data. In highly regulated industries, a risk assessment and risk management plan may even be required by law.

Step 1. Make Risk Assessment a Team Effort

Many companies assume that managing cyber risk is only the IT department's responsibility. However, this is the equivalent of triple-locking every door while leaving a side window wide open. For example, the IT department recommends logging and reviewing all employee activity on the corporate network as a way to combat insider abuse of data. However, the company may not realize the potential legal ramifications and the negative ramifications for employee morale. But with input from both the human resources and legal departments, the company can come up with a satisfactory alternative. For example, companies can come up with programs that improve employee satisfaction and thus reduce the risk of a disgruntled employee tampering with or leaking sensitive information.

Include the Right Team Members

For an in-depth understanding of the risks you face, consider building a risk assessment team that includes IT, legal and compliance personnel, HR, finance, and operations. If you face particular regulatory demands, you should also consider including a relevant external auditor, such as a CPA familiar with SSAE 16 SOC attestation, a HIPAA compliance expert, or a PCI compliance specialist.

Step 2. Identify Your Digital Assets

Your risk assessment team's first project should be to list all your systems and data, ranking them by the importance of each one to your business. After all, you can't determine how best to protect your assets if you don't know what they are, or how badly your business would be impacted if they were compromised.

Digital Asset Categories

Your digital assets include, but are not limited to the following categories and systems:

Communications	Email, telephone, and video conferencing
Storage	Server and storage infrastructure
Software	Billing, CRM, order entry, service delivery, manufacturing, general accounting, digital marketing, and human resources
Networking	Firewalls, switches, routers, and internet connections
Data warehouses	Customer, sales, inventory management, accounting, marketing, and HR
Repositories	Contracts, forms, marketing brochures, and sales presentations
Public	Website, customer service forums, and content placed on the Web

Step 3. Identify the Risks to Your Assets

Once you have a list of assets ranked in order of importance to the business, your team needs to consider what would happen if any of the following events occured:

The asset fails or is lost	The asset is stolen or controlled by an unauthorized entity	The system or data is no longer trustworthy or accurate

How might each of these failures happen? What would be the consequences in each case? How often might each of these failures occur?

The definition of risk is the probable frequency of a failure multiplied by the consequences of that failure. Since it's impossible to predict precisely how often these events might occur, educated estimates are in order. An expert will be able to tell you how often a particular failure occurs in the average day, week, month, quarter, or year.

The definition of risk is the probable frequency of a failure multiplied by the consequences of that failure.

Risk Examples

Threat	Consequence	Frequency	Annual Cost
Internet connection fails, resulting in a one-day outage	Loss of productivity for entire office, loss of reputation	Triennial	$20,000
Unencrypted laptop, containing one million HIPAA-sensitive records, is lost	Fines and, identity protection costs totaling $200 per lost record	Annual	$200M
Server room destroyed by earthquake, resulting in 24 hours of lost data and three weeks of downtime	Loss of productivity; $5M in lost revenues and rebuilding costs; time incurred to restore data from backups	Once a century	$50,000

The virtual desktop approach makes it easy to enforce specific access policies for individuals.

Step 4. Identify Ways to Mitigate Risk for Your Assets

For each potential threat, list ways to avoid the risk, or mitigate it if it happens, and the cost of each prevention and mitigation strategy. For the events in the previous example, that might look like this:

Threat	Annual Cost	Mitigation	Annual Cost
Internet connection fails, resulting in a one-day outage	$20,000	Install failover Internet connection	$2,400
Unencrypted laptop, containing one million HIPAA-sensitive records, is lost	$200M	Encrpt all laptops	$2,000
Server room destroyed by earthquake, resulting in 24 hours of lost data and three weeks of downtime	$50,000	Relocate servers to colocation facility; educate employees on data protection practices.	$25,000

Innovative Risk Mitigation Measures

Cyberattacks are becoming more creative, so your countermeasures should be, too. Below are examples of innovative risk mitigation measures that we've seen:

Threat	Original Best Practice	New Best Practice
Compromise of credit card data	Harden servers, install intrusion detection systems, encrypt stored data	Embed the website of a specialty payment processing firm, skinned with your look, as your payment page; no credit card data resides on your systems
Insider theft of information	Install electronic systems to monitor and audit employee activity	Focus on employee satisfaction to reduce the motivation for bad behavior
Environmental destruction of server systems	Replicate information to offsite standby systems	Move all systems to secure co-location facilities in areas not subject to environmental risk and access them remotely

Step 5. Implementation and Maintenance

In the early years of the Internet era, every online transaction was experimental and problems were only to be expected—but those days are long gone. CIOs are held accountable when their companies are hacked, and the government is ramping up its prosecution of regulatory violations. Insurance companies are carving cyber risk coverage out of general liability and selling it as a separately priced policy. Consumers and law enforcement expect companies to comply with security and risk management best practices.

Yet those best practices must keep evolving in order to keep pace with changing technology. That's why companies must review their risk management practices regularly. This is the only way they can be sure that they are on top of new threats and that they are implementing protections that hit the "sweet spot" between affordability and effectiveness.

Summary

As persuasive as some sales presentations might be, companies must be careful not to invest in expensive data protection solutions that don't align with their actual risks. They should also avoid preventive measures that cost more than the risk they're designed to protect against.

For small and midsize businesses, this particularly applies to intrusion detection and employee activity logging systems, which are so costly and complex that the company is unlikely to realize a full return on investment. For example, a typical intrusion detection system can easily cost $200,000 to install plus more than $100,000 in annual operations and maintenance costs. Because it is often unlikely that companies will face the sophisticated targeted attacks that these systems are meant to thwart, it is best to deal with the more common and obvious types of attacks first. The result is a prioritized and more cost-effective alternative to mitigate the risk of intrusion.

Although unforeseen disasters are, by definition, impossible to predict, the point of cyber risk assessment is not to spot every possible risk and guard against it. Cyber risk assessment determines which of all possible risks are both most likely to happen and most likely to do significant business damage. That allows your company to invest in solutions that do not, in themselves, threaten your company's fiscal stability.

Schedule your free assessment or let us know if you need more information

Xantrion provides the expertise and the skilled people necessary to assist you with risk assessment and to help you put sound risk management practices in place. We can do everything from recommending legal, insurance, and accounting cybersecurity experts to consulting with you on appropriate technology approaches. Since we have successfully implemented best practices for ourselves and for multiple clients, we know the pros and cons of various approaches as well as the implementation pitfalls.

Give us a call at (510) 272-4701 or visit https://www.xantrion.com/it-roadmap.html and let us know how we can help.

XANTRION
CYBERSECURITY • IT SUPPORT

Xantrion
651 20th Street
Oakland, CA 94612

xantrion.com

(510) 272-4701