Cyber Insurance Assessments

As cyber incidents continue to increase, it is becoming abundantly clear that cybersecurity is one of the most critical business services available. In order to ensure robust and comprehensive protection, companies must regularly audit their existing digital security infrastructure and pursue protective measures like purchasing cyber insurance.

According to a recent report from Statista, nearly 15 million data records were exposed worldwide through data breaches during the third quarter of 2022. Statista also reported that the average cost of a data breach in the United States amounted to $9.44 million in 2022, which is a significant increase from 2021. Additionally, the global average cost per data breach rose to $4.35 million in 2022.

IN THIS ARTICLE, WE WILL DISCUSS THE FOLLOWING POINTS:

- The fundamentals of conducting an internal risk assessment in cybersecurity
- What cyber insurance is and how coverage works
- Why cyber insurance is vital in today's increasingly digital world of work
- What the cyber insurance assessment process looks like
- How Moser can help you navigate and qualify for cyber insurance

What is Risk Assessment in Cybersecurity?

Conducting a cybersecurity assessment is the first step in determining your ability to protect sensitive data and information systems from various attacks. Different from a threat assessment in cybersecurity — which reviews threats as they are detected — risk assessments are meant to analyze a wide range of potential nefarious incidents, predict how much damage each incident will cause, and recommend prevention methods.

Some common questions asked during a cybersecurity risk assessment include:

- Does our workforce know how to identify and respond to ransomware attacks and other types of potential security incidents?
- What security regulations is our organization required to adhere to?
- Do we already have an established cybersecurity program in place?
- Are we building on our existing cybersecurity program?
- How is our sensitive data currently protected?
- What authentication protocols do we have in place, if any?

Cybersecurity Risk Examples

There are many factors that can contribute to increased risk of a cyber breach, including:

- Outdated technology
- Security vulnerabilities with your remote employees
- Weak cybersecurity protocols and overall strategy
- Poor cybersecurity education for your employees
- Lacking defenses on mobile devices

Additionally, some of the most common threats to cybersecurity are:

- Phishing attacks
- Ransomware and malware
- Lone hackers and cyber criminal organizations
- Data leakages
- Insider Threats

How Often Should You Perform Risk Assessments in Cybersecurity?

According to the Information Systems Audit and Control Association (ISACA), cybersecurity risk assessments are not a one-time affair. As a best practice, ISACA recommends that comprehensive enterprise security risk assessments be completed once every two years at minimum. Each assessment should conduct a deep dive into your organization's information systems in order to unearth all possible risks.

Additional resources explaining how to do a cybersecurity risk assessment can be found on the ISACA website. For US specific standards, you should review NIST's guidelines for conducting risk assessments. To learn more about cybersecurity risks and how to combat them, review this comprehensive guide from the National Institute of Standards and Technology (NIST).

What is Cyber Insurance?

Like any form of insurance, cyber insurance is intended to provide support after an attack. This support can ease the financial burden that comes along with digital security incidents or problems with IT infrastructure that are out of your control. Some notable cyber insurance benefits include:

- Legal guidance and support
- Support for digital forensic investigations
- Assistance in recovering stolen data
- Support for restoring identities for compromised customers
- Direct access to a breach hotline

What is Covered in a Cyber Insurance Policy?

In today's market, there are two types of cyber insurance available; third-party and first-party. Each type offers different coverage and unique cyber insurance terms. Depending on the needs of your business, and your available budget, you may select one or both types of insurance.

THIRD-PARTY CYBER COVERAGE

Third-party cyber coverage generally shields your business from liability if a third-party raises claims against you. This type of plan will typically cover the following items:

- Payments to impacted customers
- Claims and settlement costs
- Defamation losses
- Litigation expenses
- Cost of responding to regulatory investigations
- Settlement expenses
- Accounting fees

FIRST-PARTY CYBER COVERAGE

First-party cyber coverage is used to protect your business from the financial consequences of cyberattacks and data breaches. The following costs are often covered with this type of policy:

- Fees and fines incurred after a breach
- Legal counsel
- Sourcing and replacing lost data
- Replacing lost profits due to business interruption
- PR and crisis management
- Extortion costs

Is Cyber Insurance Worth It?

In short, yes, purchasing cyber insurance is entirely worth the investment. Like risk assessments and other cybersecurity practices, cyber insurance has become a basic requirement for many business engagements across various industries.

Inevitably, assaults on your information systems will occur. Although adhering to cybersecurity best practices significantly reduces the risk of a breach, these measures cannot ensure fool-proof protection against all threats. It's a grievous error to assume that cybercriminals are easily outsmarted. The modern cybercrime landscape consists of highly organized international operations that often involve the collaboration of several bad actors. Considering how powerful many of these groups are, businesses would do well to pursue all preventative and protective measures available, including cyber insurance.

What are Cyber Insurance Assessments? And How Do They Differ From Cybersecurity Risk Assessments?

A cyber insurance assessment is quite similar to a risk assessment in that they both are designed to identify cybersecurity gaps and areas of concern within your company's IT infrastructure. Additionally, both evaluate your company's protocols, employee procedures, and technology to pinpoint any potential risks. However, there are three key differences that set these assessments apart.

A cyber insurance assessment is conducted by your insurance provider before you purchase cyber insurance, whereas cybersecurity risk assessments are conducted internally on a repeated basis.

The goal of cyber insurance assessment is different from cybersecurity risk assessments. Cybersecurity risk assessments are meant to provide insight into the overall health of an organization's digital security infrastructure. Cyber insurance assessments are only used to help insurers determine if organizations have taken necessary steps to strengthen their security framework before a policy is issued.

The results of a cyber risk assessment are intended to be purely informational. Cyber insurance assessments function to help the insurer decide if coverage should be denied or approved.

In today's climate, many organizations are finding it difficult to obtain cyber insurance. According to a report from CNBC, the significant rise in cyber crimes has caused cyber insurance companies to limit coverage and increase premiums exponentially. In short, insurers have become more wary, while the demand for cyber insurance surges — shoving many companies between a rock and a hard place.

Moser Can Help You Navigate Cyber Insurance and Achieve Enhanced Protection

Because of the current state of cyber insurance, many businesses do not possess the technology or cybersecurity know-how to qualify for complete coverage from any cyber insurance provider. Although any company can purchase cyber insurance, coverage for specific areas could be denied if the insurer determines that the company is not using the correct tools or following the insurance company's recommended security best practices. Much of this can be easily overlooked by business leaders since cyber insurance policies are often dense and difficult to understand.

To help companies qualify for full coverage, Moser offers a cyber insurance readiness review to ensure that all policy requirements are understood and met. Additionally, Moser will facilitate discussions related to required coverage and appropriate limits.

Our assessment allows organizations to:

Fully understand their cyber insurance policy

Review gaps or overages that exist in a current policy (if the company already has a cyber insurance policy)

Ensure that all requirements are properly deployed to meet the cyber insurance provider's specifications

Our assessment process can apply to companies looking to acquire cyber insurance coverage for the first time, and to those with existing policies. If your company is not currently insured, Moser will conduct a pre-application assessment to verify what you need to put in place to successfully apply and receive the full benefits of your policy.

If your company has already purchased a cyber insurance policy, and that policy is up for review, then Moser can also be of assistance. We will read your policy, pull the requirements and document them and determine if your business remains compliant or if adjustments need to be made in order for you to retain coverage. Finally, the insights gleaned from our cyber insurance readiness review can help you determine if it would benefit your company to pursue a new cyber insurance policy all together.

THE CYBERSECURITY ASSESSMENT TEMPLATE FOR INSURANCE BELOW EXPLAINS HOW MOSER WILL ASSESS YOUR READINESS OR EVALUATE YOUR EXISTING POLICY.

Entry Interview: Meet with client to discuss current issues and concerns to obtain scope of engagement.

Document Review: Review existing cyber insurance policies, related client documents, and systems or configurations. Review existing documents and systems/configurations in preparation of obtaining Cyber Insurance.

Client Interview after initial document review: Discuss potential findings or issues related to new or existing cyber insurance. Document any open concerns or outstanding questions prior to report generation.

Detailed Cyber Insurance Report: Within two weeks of the second client review, the client will receive a comprehensive report on their readiness to meet existing policy requirements or their readiness to begin looking for a new/different cyber insurance plan.

Exit Interview: A final meeting is scheduled with the client to discuss our detailed cyber insurance report and determine if additional work is needed.

Moser's expert Business Services teams possess the knowledge, experience, and certifications needed to provide guidance on the most complex IT processes and security measures across multiple industries. Discover how we can help you protect your business here.

INTERESTED IN LEARNING MORE?

DEEP DIVE INTO OUR OTHER CONTENT:

Security Assessments and Disaster Recovery for Businesses

SECURITY ASSESSMENTS

Disaster recovery is an important part of the preparedness process in any organization, and it is especially critical when it comes to technology and cybersecurity. A proper disaster recovery plan should be put in place to ensure that data can be quickly and effectively recovered in case of a disaster or system failure.

MOSERIT.COM/SECURITY-ASSESSMENTS

DISASTER RECOVERY FOR BUSINESSES

As just about anyone in the business world can tell you, having a plan is an absolute necessity to succeed. But, what some people might not realize is that a business continuity/disaster recovery (BCDR) plan is important too. That's why we're taking a look at some of the basics of disaster recovery strategies and what we at Moser Consulting offer in the way of assistance as part of our IT infrastructure services!

MOSERIT.COM/ DISASTER-RECOVERY-FOR-BUSINESSES