eBook

The Importance of Cyber Resilience

According to the National Cyber Security Alliance study, 60% of businesses that are hacked go out of business within six months.

The vast majority of damage done in cyber attacks is due to the inability of the company to respond because they have not developed a cyber prevention and response strategy.

Think about it. We practice fire drills and earthquake duck and cover drills. Shouldn't we do the same to prepare for risk with similar catastrophic consequences? If your e-commerce system, website, email, or customer data was suddenly inaccessible because of an attack, would you be able to get back up and running within minutes, hours, days, or at all? That depends on your business's level of cyber resilience.

Unfortunately, most businesses fail to develop a plan.

What is Cyber Resilience?

The most common definition of cyber resilience is the ability of an enterprise to limit the impact of security incidents. It's a broad approach that encompasses cybersecurity and business continuity management, which aims to defend against cyber attacks and ensure that the business is able to survive.

Cyber resilience includes two primary components. Step 1 includes prevention measures, such as the ability to continuously discover and monitor all points in your attack surface and analyze this information to predict likely breach scenarios. Step 2 is to develop a plan to take appropriate action if and when an attack occurs. Unfortunately, most businesses fail at this critical second step.

Before you implement an incident response plan, you'll first need to assess the risks.

Step 1: Assess the Risks

Before you implement an incident response plan, you'll first need to assess the risks to which your company is exposed. Risks may include:

- **Strategic** - the failure to implement business decisions that align with the organization's strategic goals;
- **Reputational** - negative public opinion;
- **Operational** - loss resulting from failed internal processes, people, systems, etc.;
- **Transactional** - problems with service or product delivery; and
- **Compliance** - violations of laws, rules, or regulations.

To conduct a risk assessment, you'll need to:

1. Characterize Your Business

Some questions to ask are: What kind of data do you use? Who uses it? What is the data flow? Where does the information go?

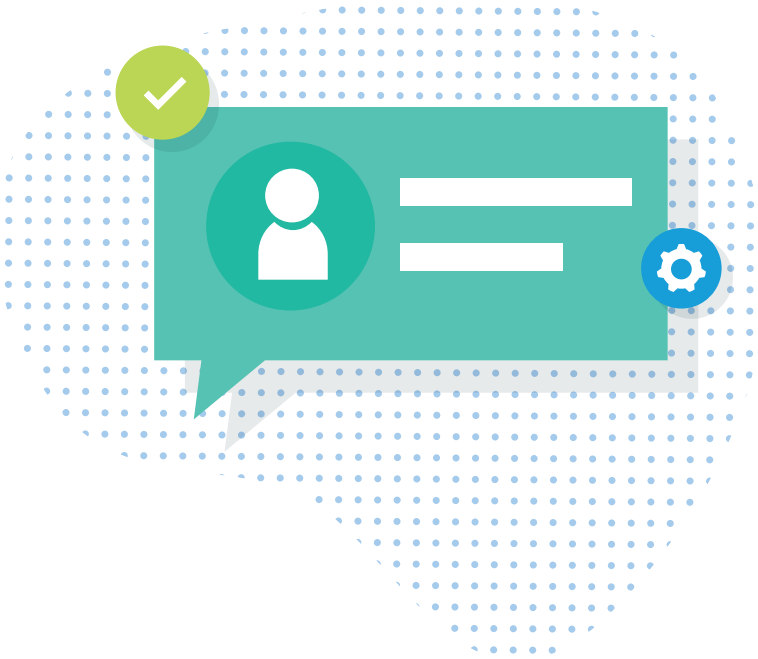
2. Identify Threats

Common threat types include unauthorized access, misuse of information, data leakage or unintentional exposure of information, loss of data, or disruption of service or productivity.

3. Determine Inherent Risk and Impact

What would be the impact on your organization if the threat was exercised? Would the impact be high, medium, or low?

Regular risk assessments are a fundamental part of your business and they should be reviewed regularly.



4. Analyze the Control Environment

You typically need to look at several categories of information to adequately assess your business's vulnerabilities. Are your controls satisfactory or do they need improvement? A few examples of controls you might want to look at include:

- Organizational Risk Management Controls
- User Provisioning Controls
- Administration Controls
- User Authentication Controls
- Infrastructure Data Protection Controls
- Data Center Physical & Environmental Security Controls
- Continuity of Operations Controls

5. Determine Your Organizational Risk

To do this, you'll need to consider how high the threats are and how vulnerable the controls are. From there, you can decide if the risk is severe, elevated, or low.

Regular risk assessments are a fundamental part of your business and they should be reviewed regularly. Once you've completed your first risk assessment, you can implement an incident response plan.[1]

1 https://www.sagedatasecurity.com/blog/6-steps-to-a-cybersecurity-risk-assessment

Once your team isolates a security incident, the aim is to mitigate the damage.

Step 2: Develop the Incident Response Plan

An incident response plan will identify the actions that should be taken when a data incident occurs. The aim of it is to identify the attack, contain the damage, and eradicate the root cause. When your organization responds to an incident quickly, it can reduce losses, restore processes and services, and mitigate exploited vulnerabilities.

The SANS Institutes's Incident Handlers Handbook defines a six-step incident response plan:

1. Preparation

This step involves creating an incident response team and outlining their roles and responsibilities. You'll also need to develop policies to implement in the event of a cyber attack, as well as a communication plan.

2. Identification

Decide what criteria calls the team into action, such as a phishing attack. Start to assess the incident and gather evidence.

3. Containment

Once your team isolates a security incident, the aim is to mitigate the damage. This includes an instant response, such as taking down production servers, a system backup, and long term containment, such as installing security patches on affected systems.

Following these steps can prepare your organization for a security incident and ensure that you're taking the appropriate measures.

4. Eradication

Contain the threat and restore systems to their initial state. This step also includes seeing if the attacker reacted to your actions and anticipating a different type of attack.

5. Recovery

Ensure that affected systems are not in danger and can be restored to working condition. Monitor the network system to ensure that another incident doesn't occur.

6. Lessons Learned

Review the steps you took and see if there are areas for improvement. This report can be used as a benchmark for comparison or as training information for new incident response team members.

Following these steps can prepare your organization for a security incident and ensure that you're taking appropriate measures.

Benefits

Cyber resilience can reduce the economic impact on your business after a cyber attack and instill confidence in your customers who know that you are able to protect their data. Consequently, a significant amount of underwriting now takes into account business resiliency.

Cybersecurity practices such as password management, risk assessments, employee training, and incident response plans can prove your organization's resiliency and thus lower insurance costs. With premiums ranging from $10,000 for small organizations to over $100,000 for million-dollar businesses, these cost savings can be valuable.

Ideally, you should implement an incident response plan before you purchase cyber insurance to better understand what your needs are and how you can enjoy lower rates.

By documenting prevention, detection, and mitigation best practices, you can negotiate better insurance terms and conditions, which may include:

- Reduced premiums
- Broader coverage
- Higher amounts of coverage

In the case of cybersecurity, offense wins and the defense loses. Interested in learning more about cyber resilience or risk assessment? Give me a call.