What is Cyber Resilience, and Why is it Important for Your Business?

Contents

Introduction

Cyberattacks have gone up by 600% due to the global pandemic. Cybercrime troubles the public and private sector alike and continues to grow with each passing day. IoT (Internet of Things) attacks are expected to double by 2025, and cybercrime may cost companies worldwide nearly $10.5 trillion by 2025. Going by these numbers, every organization needs to take measures to tackle cybercrime.

Our society has become increasingly reliant on interconnected cyber systems from managing personal finance to controlling air traffic. Digitalization and technology have, without a doubt, has empowered people and change the way the world lives and works. However, that has also increased the risk of cybercrime. Attack targets have also become a lot more diver see than before. From individuals to multinational companies, anyone can become the target of cybercrime. A technology evolves, so does cybercrime. Cyberattacks have cost organizations millions of dollars worldwide, so cyber resilience is of prime importance in today's day and age.

Chapter 1 - What is cyber resilience?

The ability to prepare for, respond to, and recover from cyberattacks is called cyber resilience. The cyber resilience of an organization refers to how well the organization manages a cyberattack while continuing to run its business operations efficiently.

Cyber resilience has the following key features:

- **Adapt**

This involves adjusting response strategies or changing the management approach beforehand to tackle future threats. Learning from previous disruptions can help create effective strategies to mitigate the effects of cybercrime.

- **Prepare**

Organizations should dedicate time to predict, anticipate, and plan for stressors or potential threats. They should identify and monitor critical functions of the systems that may be at the greatest risk.

- **Withstand**

It helps businesses maintain business operations without impairing performance or stopping business functions, even under a cyberattack.

- **Recover**

Cyber resilience helps businesses rebound from an adverse incident to full business operations, functionalities, and performance.

The concept of cyber resilience first came into the limelight in 2012 after Presidential Decision Directive 21 was issued. Although cyber resilience became more visible, the fact remains that many organizations had already been working on cyber resilience. For instance, in 2010, the MITRE Corporation published its Cyber Resilience Engineering Framework. Similarly, the Carnegie Mellon Computer Emergency Response Team published the CERT Resilience Management Model in October 2011.

Chapter 2 - How does cyber resilience work?

Cyber resilience is a preventive step to counteract unsafe software and hardware or human error. It takes into consideration all the insecure components in the infrastructure of an organization to meet its aim of protecting the entire enterprise.

There are four main components of cyber resilience:

Threat protection

Cybercriminals are extremely innovative. As new technologies come about, they come up with newer ways to orchestrate cyberattacks. Having just basic security when technology is evolving so rapidly puts your organization at great risk. So, what should organizations do to safeguard themselves if a threat arises?

To start with, organizations need to take strong measures for data protection. Email attacks are among the preferred ways of cybercriminals. Installing anti-virus and anti-spam is not enough to protect your emails. Organizations should incorporate DNS Authentication mechanisms for enhanced security. Investing in a versatile solution that adapts to evolving cyberattacks is a great solution to protect your data and emails.

Another solution worth considering is the endpoint detection and response tool. These tools work by monitoring network events and endpoints and recording the information at a centralized location. Organizations can then analyze, detect, investigate, report, and set alerts to mitigate cyber-attacks. Analytical tools can facilitate threat detection, deflect common threats, facilitate early detection of ongoing threats to improve the overall security of the organization.

Recoverability

An organization's ability to resume normal functions after a cyberattack is called recoverability. Ransomware attacks are quite prevalent, and the number of attacks doubled in the first half of 2021. A ransomware attack could encrypt all your data, causing you to either lose the data or pay the attackers a hefty ransom. To protect your organization against ransomware attacks, organizations must back up their data on separate networks so that data can be recovered after an attack.

Organizations should also consider running a data breach scenario every once in a while. During such a drill, organizations should walk through all the steps that they would have taken in the event of a real cyberattack. This will help strengthen cyber resilience.

Adaptability

Cybercriminals are constantly creating new ways to avoid detection and launch new attacks. It is crucial for organizations to adapt quickly so that they can defend themselves against future attacks. For preventing attacks in the first place, security teams should be able to detect attacks quickly and respond to them. There should also be in-built administrator tracking so that organizations can identify at-risk and infected users.

Adaptability is crucial for cyber resilience. When security teams are well-trained on cyber threats, they can recognize real threats and use automation to mitigate such threats. The more adaptable an organization is, the stronger the cyber resilience.

Durability

The durability of cyber resilience is not dictated by the IT environment but by your organization's ability to function properly after a cyberattack. Regular updates and system enhancements can improve the cyber resilience of an organization.

The aim of cyber resilience is to secure the organization. A data breach could result in financial, legal, social, or technical repercussions. Therefore, it is important that all organizations prioritize cyber resilience by integrating IT with business operations.

Chapter 3 - How is cyber resilience different from cybersecurity?

Cybersecurity refers to steps or measures that an individual or an organization takes to protect their data or device from threats or potential cyberattacks. Implementing cybersecurity best practices can help many cyberattacks. However, cybercriminals may still be able to find holes in your defense system when the landscape changes. 100% prevention may not be possible when it comes to cyberattacks. That is why organizations need cyber resilience.

Cyber resilience is a comprehensive set of cybersecurity measures combined with other strategies to protect an organization. Important organizational strategies, such as cyberattack management plans and strategies to regain customer trust, all form a part of cyber resilience. A serious cyberattack could hamper the delivery of services and business operations. If your organization works in the field of national security or public safety, the impact of a security breach could be enormous. The same applies to other organizations as well, such as banks, online retailers, or streaming providers.

Cyber resilience is important because relying on cybersecurity measures alone may not be enough to prevent the consequences after an attack. Being able to detect and respond to a cyberattack is a much more effective measure than assuming that your cybersecurity measures will hold. Your cybersecurity measures may be able to stave off a cyberattack, but they may also fail. If they fail, then your organization needs cyber resilience to be able to bounce back.

Chapter 4 - What are the benefits of cyber resilience?

A well-developed cyber resilience strategy offers numerous benefits for an organization.

Reduces financial losses

According to the report, The Hidden Costs of CyberCrime, financial losses due to cybercrime may reach $1 trillion. When an organization is cyber resilient, it is well-prepared to mitigate or handle cyberattacks. Such organizations also recover from such attacks a lot faster to resume normal business operations. This prevents significant financial losses that occur from cyberattacks or security breaches.

Helps businesses remain compliant

Data is an important asset for most businesses nowadays. Businesses worldwide gather and handle incredible amounts of data. A large part of this data consists of critical business data and sensitive customer information. Therefore, it is important for businesses to comply with data privacy laws such as the GDPR (General Data Protection Regulation), the FIPA (Florida Information Protection Act), the CCPA (California Consumer Privacy Act), and more. Violation of these regulations could lead to penalties, fines, and lawsuits. Having an effective cyber resilience framework helps businesses assess the security status of the organization. It also helps them identify loopholes in their security infrastructure that could lead to possible non-compliance. A cyber resilience framework ensures that legal and regulatory requirements are met.

Enhances brand reputation

A data or security breach not only exposes your business to financial risks but also reputational risks. When clients feel that their data is not safe with you, it could negatively impact their trust in you. Cyber resilience strengthens information security and establishes your business as a secure entity that customers can rely on.

Ensures business continuity

Cyber resilience improves business security and eliminates threats before they can cause damage to your business. It also reduces the occurrence of cyberattacks. A well-designed cyber resilience plan includes an incident response plan that helps mitigate risks and minimizes the impact of cyberattacks on your business. Cyber resilience ensures business continuity with none or minimum downtime during and after a cyberattack.

Chapter 5 - Why is cyber resilience important for businesses?

As the frequency and vigor of cyberattacks increase, businesses have come to realize that traditional security measures are not enough. That is why cyber resilience has grown in popularity in the recent years. Organizations realize that preventing cyberattacks 100% of the time may not be possible. So, it is important to implement strategies to resist and handle cyberattacks.

Cyber resilience offers numerous advantages for businesses, both during and after a cyberattack.

- **It helps maintain the integrity of your organization.**

Without cyber resilience, organizations are unable to monitor the damage caused by cybercriminals. A strong cyber resilience plan safeguards an organization from public criticism, sudden revenue loss, administrative penalties, or business losses.

- **It enhances safety and security.**

Cyber resilience helps to respond and withstand cyberattacks. It also enhances the safety and security of sensitive assets, helps organizations build IT governance strategies, and strengthens data protection efforts. It also minimizes the impact of human error and natural disasters on the safety and security of an organization.

- **It creates more trust in the vendor and customer ecosystem.**

In the last few years, organizations are paying a lot of emphasis on third-party risk management and vendor risk management frameworks. However, just like it is important for organizations to assess their vendors, it is important for vendors to trust your organization too. A lack of cyber resilience could impact the credibility of your vendors and clients.

- **It helps to improve organizational work culture.**

It is not only the responsibility of the IT team, but that of every employee in an organization to ensure data protection. They should all play an active role in ensuring the safety of all IT infrastructure. When people are motivated to take security seriously, you can rest assured that physical properties as well as confidential information are in safe hands. The organization would be able to focus on the right security measures within the departments and minimize human error that could potentially leak confidential data.

Chapter 6 - How can you improve cyber resilience?

In today's day and age, when a cyberattack could happen at any time, organizations must prioritize cyber resilience.

Here's how your organization can improve cyber resilience:

- **Automation**

Cyberattacks are becoming increasingly innovative and complex. Relying on manual systems to thwart cyberattacks is no longer an option. Progressive organizations are embracing Artificial Intelligence and Machine Learning to automate critical functions that help assess risks and identify vulnerabilities faster. Automation reduces the occurrence of errors and also enables faster decision-making through accuracy and efficiency.

- **Strict security protocols**

No one should be trusted when it comes to data security. In fact, insider threats have risen by 47% in the past couple of years. Strict security protocols, such as multi-factor authentication, encryption of valuable digital assets, and identity and access management are a must to reduce the risk of unlawful access and data theft.

- **Back up your data**

When a cyberattack happens, your last resort is your backed up data. When you ensure that your data is backed up securely, recovery from any cyberattack is much faster. By having a copy of your valuable data at a secure location, you can ensure business continuity and prevent any data loss or corruption due to IT failure or cyberattacks.

- **Include cyber resilience as part of your organizational culture**

The entire organization is responsible for security, and not just a handful of IT professionals. Organizations should conduct security awareness and training programs regularly to keep everyone up-to-date on the latest cybersecurity trends. Measures should be taken to encourage all employees to adhere to the security guidelines and policies set by the organization.

Conclusion

Organizations today cannot undermine the importance of investing in cybersecurity as part of their cyber resilience plan. Regardless of the technologies in place, organizations should always plan for the worst so that they can mitigate an attack, if it occurs. Using security software and tools is as important as training the staff on how to ensure security and data protection. By being cyber resilient organizations can minimize financial losses and ensure recovery happens a lot faster if they do face an attack.