Skillmine
Technology • Consulting • Services

Measures to Avoid Cyber-attacks

info@skill-mine.com www.skill-mine.com

In 2021, on an average, a data breach cost an astounding $4.24 million compared to $3.86 million in 2020. With cyberattacks on the rise, cybersecurity is crucial for businesses of all sizes. Companies should invest in effective attack and defensive strategies. While knowing how to respond to a cyber threat once it has already occurred is essential, taking proactive steps to thwart cybersecurity threats should be prioritised.

What is a cyberattack?

A cyberattack is an intentional exploitation of your systems and network. By introducing malicious code, attackers might infiltrate your computer and steal, leak, or hostage your data.

Cybercriminals, threat actors, or hackers are common terms for the people who conduct cyberattacks. They may operate independently, in tandem with other attackers, or as a unit of a gang of organised criminals. They look for flaws in computer systems and attempt to take advantage of them to further their objectives.

Cyberattacks may be launched for a variety of reasons. Some attackers target monetary or personal benefits. Others are "hacktivists" who commit crimes for political or social reasons.

Here are a few examples of some **common cyberattacks and data breaches:**

- Viruses, malware, spyware, trojans, phishing, spam, and spoofing
- Attacks involving denial-of-service and distributed denial-of-service
- Unauthorised access, Password sniffing
- Extortion, fraud, and identity theft
- Theft of or illegal access to intellectual property
- Network intrusion, Website vandalism
- Public and private web browser exploits
- Abuse of instant messaging

A growing EduTech company has a small IT department and no specific security specialists. They had to deal with the possibility of numerous undetected attacks invading the network. A fully equipped Security Operations Centre (SOC) was set up to reflect the most recent threats and vulnerabilities.

An advanced Sense Analytics engine was also used to normalize and correlate data and identify the security offences requiring investigation. Threat Intelligence was used to supply a list of potentially malicious IP addresses, including malware hosts and spam sources. By undertaking these steps, the company saw continuous improvement, increased efficiencies and reduced number of risks.

Although it is impossible to defend a company against cyberattacks completely, many physical and technical measures may be taken to increase network data security.

Train your employees

It's through your employees that most cybercriminals get access to your data. Hackers may send fraudulent emails asking for personal information or access to specific files while posing as a member of your company. These links can be frequently mistaken for trustworthy sources, and it's easy to fall for the trick. Employee awareness is essential due to this reason.

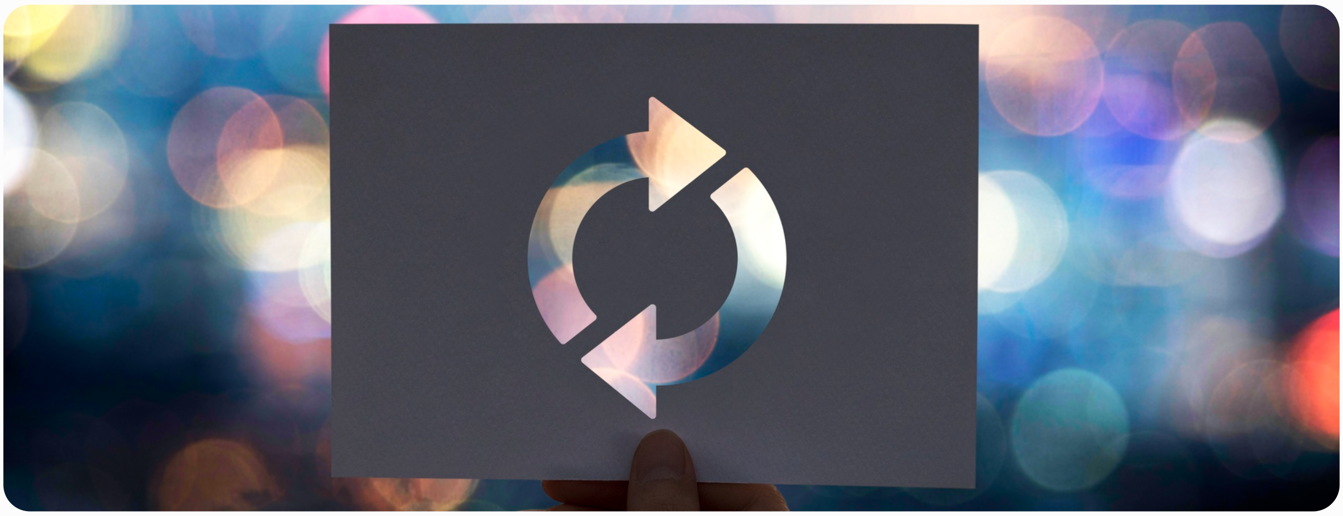
Training your staff on cyber-attack prevention and educating them on current cyber-attacks is one of the most effective strategies to protect your organization against cyber-attacks and all forms of data breaches.
Employees should:

Check links before they click them

Verify email addresses in the email they get.

Before sending out sensitive info, be cautious and sensible.

Before carrying out the "request," call the person to confirm.



Keep your systems fully updated

Cyber-attacks frequently occur due to vulnerabilities due to out-of-date software or systems. Hackers use these flaws to break into your network.

A patch management solution, which will oversee all software and system updates and keep your system resilient and current, is a wise investment to combat this.

Incorporate zero trust and SSL inspection

The most accessible and essential component of cybersecurity operations is zero trust, the methods and tools underpinning the maxim "trust no one and verify everything." Zero trust is not a feature, product, or service. Instead, it's a target to aim at. It's a method of thinking. It encompasses identifying the greatest dangers and utilising a risk-based strategy to map a certain event's frequency, likelihood, and impact.

Intercepting and examining SSL-encrypted internet traffic between a client and a server is known as SSL inspection. Since most internet traffic, including dangerous material is SSL encrypted, inspecting SSL traffic is crucial. Data is scrambled via SSL encryption, rendering it unreadable until decoded.
Adding SSL inspection to zero trust completes the architecture and guarantees that our cybersecurity and cyberattack prevention underpinnings are future-proof.

Examine components of frequently used apps

The most popular apps in your company are quite likely to still have traces of users, permissions, and out-of-date security measures that leave those tools open to attack. It's crucial to examine how each of those programmes is set up and keep track of who has access, when they use it, and how.

Ensuring all aspects of Active Directory that can be compromised are adequately secured is the first step in keeping it secure. This includes users, attributes, groups, group members, permissions, trusts, settings linked to Group Policy, user rights, and more. Mandating multi-factor authentication for users is a good step. To prevent lateral movement, enforce the principle of least privilege across all end-points by disabling default administration, denying access from a built-in local administrator account, and avoiding many built-in groups with excessive permissions.

Invest in e-mail specific security tools

Many successfully launched cyber-attacks infiltrate company networks due to an authorised user's ignorance, most often due to a phishing email. Enterprises can add extra security measures to email and other applications that convert users into a gateway for outsiders.

In order to safeguard your users and their network activity, robust tools must be used to inspect the link, and any payloads are essential. A reliable next-generation firewall, secure email service, and endpoint technology can be effective tools in protecting against cyberattacks.

Create a mobile and data management plan

Most business personnel use personal mobile devices in addition to company equipment for tasks like checking email, opening collaborative projects, and other tasks that could disclose confidential company information.

Establishing and enforcing a mobile device and data management plan is the best approach to ensure that personal mobile devices do not expose the network to unwanted hazards.

Effective inspection of the guest network can also help prevent the spread of threats from device to device and protect the organization from potential harm.

Go passwordless and use UEBA

Employees frequently struggle to remember their user access credentials. Therefore, in an effort to make things simpler, they use easy-to-remember passwords and keep their data in unprotected locations. Wrong password practices put company networks at significant risk, allowing criminals to acquire credentials from any number of users.

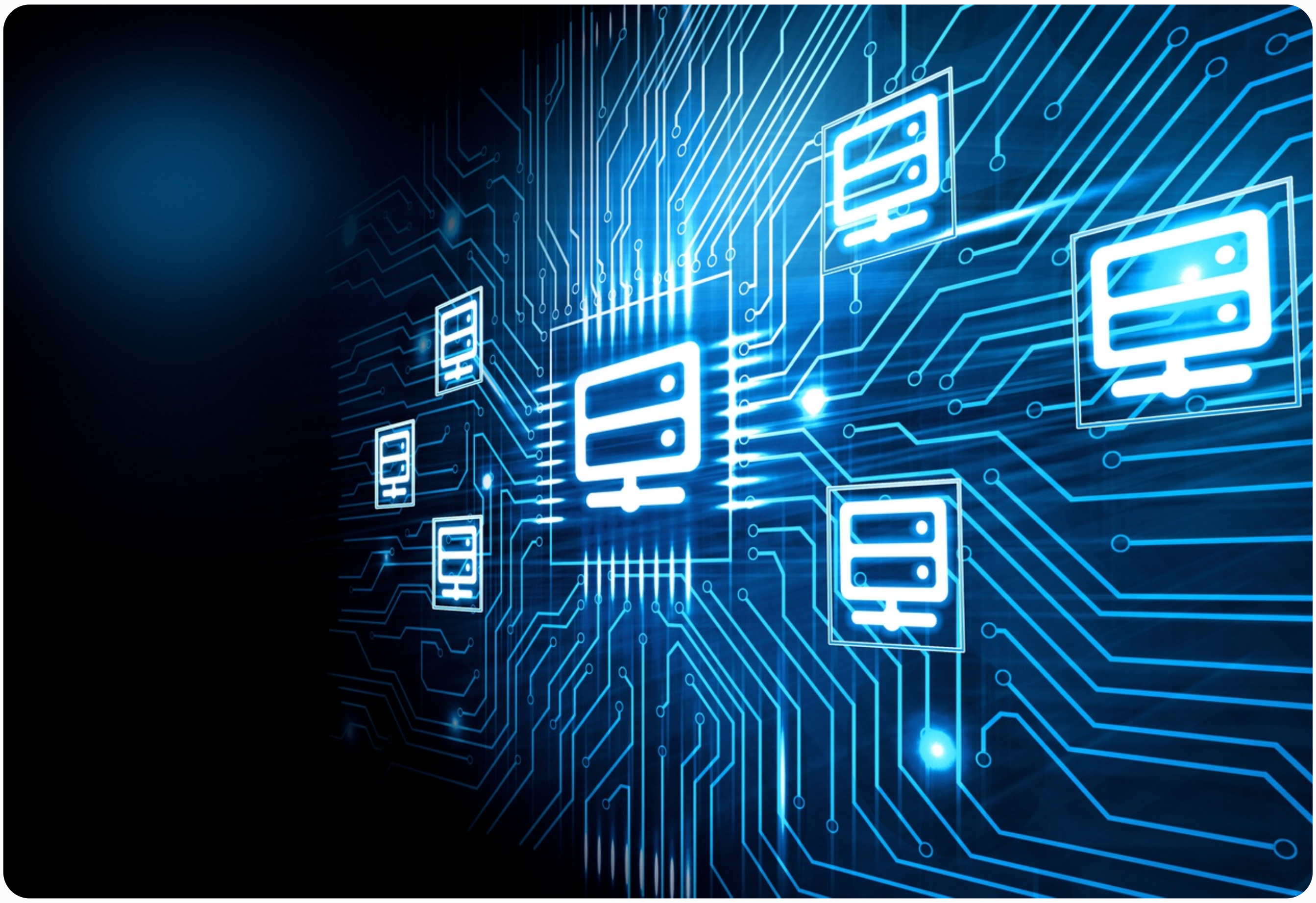
It is a good idea to encourage businesses to find passwordless and User and Entity Behaviour Analytics (UEBA) techniques for user account security due to the numerous cyber-attacks focused on credential theft. These modern methods and tools boost security while enhancing user experience.

Users can take a far easier and more safe cybersecurity stance than having to remember a complicated password. Skillmine has developed an indigenous solution in this direction- Auth. Skillmine Auth is an authentication and authorization solution that helps businesses centralize access management. It supports classical login, passwordless login, social logins and enterprise providers.

Update your incident response plan

The majority of businesses make the error of responding to cyber attacks reactively, taking care of the security issue as it arises without undertaking any additional effort, training, or policy formulation to shield themselves against future attacks.

When breaches occur, your SecOps team, IT employees, and security partners need to be aware of their roles, responsibilities, and tasks. A prompt response can help you reduce the impact caused by a minor attack or catastrophe- whatever the episode's scale.

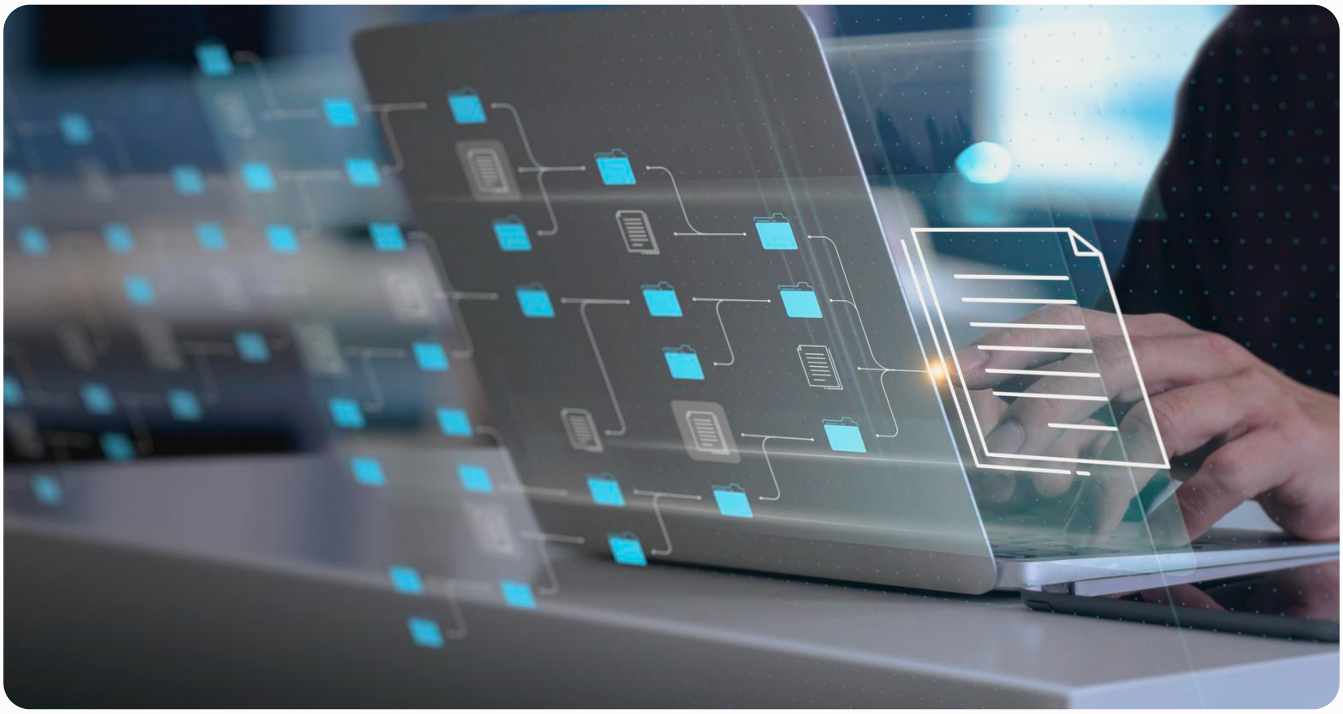


✓ Regularly monitor and audit your network

In addition to the policy formulation and training, building an incident response plan is essential to spot minor concerns before they evolve into large ones.

While preventive security solutions like firewalls, antivirus, proxies, multi-factor authentication, and others are essential, they are insufficient. The threat actor landscape has changed from just creating malicious software to now incorporating sophisticated weaponization of that malware with reliable delivery techniques to hide unwanted behaviour.

Security specialists must continuously monitor all potential attack surfaces using best practices and repeatable procedures to detect and address threats. This will ensure your organization’s preventive layer is adequate. Since many firms choose a "set-it-and-forget-it" strategy for the preventative layer, continuous monitoring has become crucial to reduce risk by offering a crucial feedback loop.



Develop strong data governance principles

Data security is a critical component of cybersecurity. Data governance ensures that the right data obtains the necessary protection.

Strong data governance entails analysing data at the source and continuously shielding users from unauthorised data access.

Sensitive information is a target for criminals, which raises corporate risk. Suitable data governance measures, such as removing any data that is not necessary for them to perform their services or to meet a regulatory need, are essential to reduce this hazard. By shrinking the infrastructure footprint and decreasing the potential for privacy and other regulatory requirements, deleting unnecessary sensitive data in the environment lowers the danger of a hack, and IT costs.

The effects of data overload on cybersecurity are also increasing as data volume increases. Businesses should consider data classification, tagging, and creating clear guidelines and regulations on data retention to assist in alleviating data overload.

Automate security management practices

Automation is not the solution for all cybersecurity issues. Still, solutions that are Artificial Intelligence (AI) and Machine Learning (ML) greatly simplify the process of implementing security monitoring and other quality controls in the cloud.

One of the most time- and cost-efficient methods to safeguard distributed networks is cloud security automation.

In order to cut down on the amount of time, resources, and money needed to comprehend an event's cause, extent, and effect, automation must be incorporated into the cloud investigation route. Organizations need the capacity to automatically acquire and analyse data at cloud speed and scale, given the volume of data now stored in the cloud.

Conclusion

According to a report by McAfee, “The Hidden Costs of Cybercrime”, 56% of organizations do not have a cyber incident response plan.

When it comes to defending your business against cyberattacks, it can be challenging to know where to begin. The amount of information available might be daunting, especially when it contains contradictions.

You need a solution appropriate for your company and its employees. For an evaluation of your cyber security, get in touch with Skillmine right away. Accelerate your path to security with our assistance.

Is your business at a Risk of Data Breach

Know more

Skillmine
Technology • Consulting • Services

sales@skill-mine.com

www.skill-mine.com