Guide: Top Cyber Threats

How to address and combat the top cyber threats.

new era. TECHNOLOGY

Preparing and building robust defenses against cyber threats.

The dawn of the digital age promised enterprises unmatched growth and connectivity, a modern gold rush of opportunities. Yet, with these prospects came the specter of cyber threats, silently lurking and constantly evolving.

Every enterprise, regardless of its size, has a unique digital footprint. This footprint, composed of your online interactions, stored data, and the software tools you use, is what makes you both valuable and vulnerable.

Let's explore the top threats, and how your organization can build a 'cyber fort' to create robust defenses against cyber threats.

USD $4.45 Million

The average cost of a data breach reached an all-time high in 2023 of USD 4.45 million. This represents a 2.3% increase from the 2022 cost of USD 4.35 million. Taking a long-term view, the average cost has increased 15.3% from USD 3.86 million in the 2020 report.

– IBM 'Cost of a Data Breach' Report 2023

Top Cyber Threats

Cyber threats to your organization are occurring every day and are always changing and evolving as bad actors develop new tactics. Here are some of the cyber-attacks that should be top of mind.

Phishing Attacks

Attempts by cybercriminals to dupe people into disclosing personal information, such as passwords and credit card details, by posing as a reliable organization.

Ransomware

Attacks using ransomware encrypt the victim's data and demand payment (often in cryptocurrency) to decrypt it.

Insider Threats

Include malevolent (workers who leak information on purpose) and non-malicious (employees who unintentionally compromise security, like by clicking on a phishing email).

Supply Chain Attacks

When a reputable vendor or supplier is compromised to get access to their clients' computer systems.

DDoS Attacks

A Distributed Denial of Service (DDoS) attack overloads a network, system, or website with traffic, rendering it unusable for users.

Advanced Persistent Threats (APTs)

Targeted long-term attacks in which a hacker acquires access to a network and uses that access while going unnoticed for a long time.

Be Prepared Against Breaches

According to IBM's 'Cost of a Data Breach' 2023 report, the following stats were provided.

1.76 Million

USD

The average savings for organizations that use security AI and automation extensively is USD 1.76 million compared to organizations that don't.

51%

of Organizations

Are planning to increase security investments as a result of a breach, including incident response (IR) planning and testing, employee training, and threat detection and response tools.

4.45 Million

USD

The global average cost of a data breach in 2023 was USD 4.45 million, a 15% increase over three years.

newera. TECHNOLOGY

Prevent, Detect & Contain Threats

In several ways, managed detection, and response (MDR) services can aid in reducing these threats and provide the visibility and peace of mind your organization requires such as:

» **Proactive Monitoring:** MDR services offer round-the-clock surveillance of a business's networks and systems, enabling it to identify and counter threats as soon as they emerge.

» **Threat Detection and Response**: Find anomalies that could be signs of a security threat, MDR use advanced analytics, threat intelligence, machine learning, automation, and SOAR.

» **Enhance Security Posture:** MDR providers can provide insight and advice on enhancing a company's security posture such as on proper security procedures and current cyber threats and how to defend against them.

» **Incident Response (IR):** In the event of a security event, an MDR service can aid with the investigation, damage control, and recovery processes.

» **Compliance:** Meeting compliance and regulatory regulations for log monitoring and by ensuring your security procedures are current and effective.

Additionally, businesses must establish and continue to foster a culture of security awareness and implement fundamental and 'best' security practices like using strong passwords and MFA and providing employee security training to minimize the likelihood of compromise from cyber-attacks.

Take the Next Step

MDR services can greatly enhance a business' security posture and reduce risk. New Era Technology's Managed Detection and Response (MDR) service maintains optimal security posture by continuously minimizing the attack surface and improving visibility via enhanced monitoring and response. Leveraging defense-in-depth and best-of-breed security technologies, MDR integrates with a multitude of environments.

Deployable at any scale, it provides complete and layered end-toend security. The transparent subscription model provides predictability of expenditure. The ability to integrate with your existing digital assets offers an added boost to the return on previous investments.

Through New Era's SecureBlu Security services, we can assist you with ransomware preparedness, prevention, monitoring, and response.

Talk to Us Today

To find out more information about New Era's SecureBlu MDR services and how your business can begin to protect against cyber threats, please **contact us** today.

www.neweratech.com/us/security-services/

877.696.7720