Cybersecurity: Its Significance And Top Trends

Description

Cybersecurity: Its Significance And Top Trends

- ATMECS â?? Content Team

Cybercrime had cost the world $6 trillion in 2021. The costs are expected to increase up to $10.5 trillion by 2025. Investing in cybersecurity is the best course of action to protect against or deter criminal activities like hacking, unauthorized access, and attacks on data centers or computerized systems. It helps safeguard connected systems like software, hardware, and data from multiple threats and defends computers, mobile devices, servers, networks, and other electronic devices from malicious attacks.

The best cybersecurity strategies provide an efficient security posture against cyber threats and malicious attacks that aim to access, change, destroy, delete, or extort systems and sensitive data.

Why is cybersecurity critical?

Cybersecurity is vital to minimize the risk of cyberattacks, and secure data and systems. The proliferation of digital technology, increased dependence on the internet and smart devices, complex global supply chains, and critical digital economy data have led to an increased probability of cyberattacks. Individuals, organizations, governments, educational institutions, etc., are all at risk of data breaches and cyberattacks. No one is immune to the cyber threats of today.

Studies suggest that global cybercrime costs will reportedly rise by almost 15% annually over the next four years. If you are not convinced about the importance of cybersecurity in curbing these threats, the following points will help you understand its significance.

- **Increased exposure of organizations to attacks**

Cybercriminals try to access organizational data through employees, and the increased use of internet services and IoT devices worsens the problem. The criminals hack into the system by sending fraudulent messages and emails. Organizations with minimal or less than optimal security protocols cannot tackle such security threats. Organizations have to beat such threats 100% of the time while cybercriminals need to win only once to do irreparable damage. This is the reason why cybersecurity is critical in proactively preventing theft, hacking, fraudulent emails, viruses etc., before it happens.

- **Increased cybersecurity threats to individuals**

Hackers may steal an individualâ??s personal information and sell it in unlegislated or unregulated markets like the dark web for profit. All data on personal mobile phones, computers, or other digital platforms is no longer safe. Individuals with high-profile identities or at-risk segments like senior citizens are the most vulnerable. Phishing, where the attacker sends fraudulent messages that appear to come from a recognized source, is one of the most frequent types of cyberthreats. Phishing algorithms run behind the scenes stealing login information and sensitive data and in many cases, installing malware on the devices. If you see a lot of emails in your inboxâ??s spam folder, chances are you received a phishing email.

- **Expensive data breach costs**

Organizations cannot afford data breaches. Even the smallest data breach can amount to exponential losses due to litigation costs. Data breaches on average cost $3.62 million, leading many small organizations to go out of business. According to recent research, the cost of breaches has increased quite a bit, and new vulnerabilities have prompted hackers to launch automated attacks on systems.

- **Modern day hacking**

Hacking and data breaches threaten network systems and make them vulnerable. Present-day cybercriminals range from privately funded individuals to activist outfits, from anarchists to well trained state sponsored actors. The scope of cyberattacks have also widened to include:

1. Information systems and network infiltration
2. Password sniffing
3. Website defacement
4. Breach of access
5. Instant messaging abuse
6. Web browser exploitation
7. Intellectual Property (IP) theft
8. Unauthorized access to systems

- **Increasing vulnerabilities**

Malicious actors take advantage of everyone â?? from business organizations and professionals to educational and health institutions. Vulnerabilities are prevalent everywhere, and every system is facing a new security threat. Cybersecurity professionals are constantly playing catch-up to mitigate the risks related to data and system security.

Which are the top cybersecurity trends?

The year 2022 is all about digital business processes and hybrid work, making it difficult for cybersecurity teams to ensure secured individual or organizational networks. The hybrid working environment has highlighted the need for security monitoring to prevent attacks on cyber-physical systems. Identity threat detection and response will be on top of the list for security leaders across organizations that engage multiple vendors for their IT needs.

Data suggests 45% of organizations will experience attacks on software supply chains by 2025, three times as much as 2021. Vendor consolidation leading to a single platform for multiple security needs will cause disruption in the cybersecurity market but offer respite to consumers through innovative pricing and licensing models. One of the most talked about trends is the emergence of the cybersecurity mesh. A cybersecurity mesh is a conceptual approach to a security architecture that helps distributed enterprises integrate security into their assets. It is expected to reduce the financial impact of security incidents by 90% by 2024. Many organizations still donâ??t have a dedicated Chief Information Security Officer. It is expected that the CISO role will gain significant traction and the office of CISO will emulate both a decentralized and centralized model for greater agility and responsiveness.

It is time to pay close attention to the aforementioned trends and understand the risks/benefits associated with cybersecurity. Organizations and individuals investing in development of best practices with respect to data and information security will not only insulate themselves from todayâ??s cyber threats but also lay the foundation for sustainable growth in the future.

How can ATMECS help?

ATMECS Cybersecurity Practice helps our clients protect themselves against todayâ??s cyberthreats with both tactical and strategic solution offerings. Our practice follows a metrics-driven approach to providing resilient and reliable security services and preventing cyber threats. We understand business risks, evolve mitigation measures for data threats and attacks, and enable security posturing to ensure an efficient working system. We provide scalable services that handle all our clientsâ?? cybersecurity needs.

References

8 Huge Cybersecurity Trends (2022) â?? Link

Alarming Cyber Statistics For Mid-Year 2022 That You Need To Know â?? Link

7 Top Trends in Cybersecurity for 2022 â?? Link

TOP TRENDS IN CYBERSECURITY 2022 â?? **Link**

DEFENDING THE EXPANDING ATTACK SURFACE â?? **Link**

Category

1. Atmecs-Blog
2. Cybersecurity

Tags

1. Cyberattack
2. Cybercrime
3. Cybersecurity
4. Data Breach
5. Malware

Date Created
November 9, 2022
Author
admin