TOP 5

CYBERSECURITY TRENDS
FOR 2022 (AND BEYOND...)

The years 2020 and 2021 have been revolutionary in every sense, in the way they have made humanity evolve, from new ways to work to newer ways of communication, from pathbreaking discoveries in the medical field to innovative technological developments. The possibilities & the probabilities are aplenty, especially when we talk about the cybersecurity space. From the malicious phishing attacks to the paralyzing data breaches businesses worldwide have seen it all in the past couple of years. And while we have kept some of those calamitous attacks at bay, we still have a long way to go, as the complexity and sophistication of cyber-attacks keep on evolving.

So, here are 5 Cybersecurity trends that we feel will emerge (or continue to emerge) in 2022 (and beyond)

SUPPLY CHAIN / RANSOMWARE ATTACKS

Supply Chain / Ransomware attacks are the most popular attacks among cybercriminals. It certainly is a trend that will evolve in the year 2022. All the operating systems (Windows, Linux, macOS, Etc.) are vulnerable to ransomware attacks. The most common and potent infection is imitating a renowned application, as seen in the infamous Fantom ransomware operators' MO.

CHALLENGES OF REMOTE WORKING

With the culture of remote working to continue in the year 2022, the IT admins will be presented with a plethora of new challenges as they prepare to deal with remote working aspects like IoT (Internet-of-Things), BYOD (Bring-your-own-Device), and Cloud security. Even the age-old threats like email phishing, PAM, and Zero-Trust issues will continue to soar. So, the organizations need to set up a Zero-Trust framework as a mandate in the year 2022.

HEALTHCARE SECTOR - THE PRIMARY TARGET FOR CYBERCRIMINALS

The Healthcare sector has been the primary victim of catastrophic data violations. With many health care organizations relaxing their firewall rules to help their employees work remotely, it has allowed Cybercriminals to exploit those relaxations to compromise sensitive information associated with their businesses, employees, and patients. According to our study, the **Global Cybersecurity Market is expected to grow up to USD 216.0 billion by 2025 at a CAGR of 11% from 2020 to 2025.** All the health care organizations need to strengthen their security requirements like HIPAA compliance to safeguard critical health information.

THE EVOLUTION OF AUTHENTICATION

Authentication is the first step towards keeping data safe. In the year 2022, organizations will move beyond the standard "complex" password that requires changing after a certain period. There is bound to be an influx of additional authentication methods such as three-factor authentication, smart cards, and biometrics to bolster security and enhance the user experience.

AI AND ML - MAINSTREAM PREVENTION OF CYBERATTACKS

It's 2022 almost; yet, the world is far from having accepted AI & ML as the primary "cure" against the cyberattacks. But all this is set to change as the world steps into 2022. AI and ML will play a crucial role in anticipating and responding to cyber threats in real-time, making the existing cybersecurity solutions even more powerful and, simultaneously, convenient.

CLOSING WORDS

Cybersecurity has been a crucial part of the modern world for long now, on a personal to an organizational level. While the onus of data security on a personal level lies with the individuals, while at an organizational level, it's the CTOs and the leaders who need to take the initiatives to strike a balance between customer experience, data security, and data privacy. Businesses have been prone to cyberattacks for a long time now. However, with the outbreak of the COVID-19 pandemic forced everyone behind personal walls, it's time for businesses to take extraordinary measures to strengthen their firewalls and IT Security.

For a more detailed assessment please reach out to marketing@datamaticsbpm.com.