RNI No.35850/80; Reg. No. MCS-123/2018-20; Published on: Every alternate Monday

₹100

# Business India

THE MAGAZINE OF THE CORPORATE WORLD

April 17-30, 2023

- INDIA'S ELECTRONICS EDGE
- MILK WARS
- LIGHTHOUSE LEARNING
- IKIO LIGHTING


# Digital scores over Television

# Realities of our cyber society

**Robust security cultures are just as crucial as technical measures**

The pandemic has made us realise that we cannot undervalue the unpredictable and transformative nature of the rapid changes in digital initiatives that forced organisations to control and manage disruptions of their businesses. Nearly every industry is now affected by the issue of cyber-security -- from SMEs to numerous organisations in charge of managing critical infrastructure. Cyber-crime is a growth industry which was estimated at about $6.9 billion last year and continues to expand and diversify.

With the rapidly evolving landscape, organisations must acquaint themselves with the overall threat environment by implementing strategic cyber security solutions when allocating resources and selecting products. Below are some of the key 2023 cyber-security predictions, which offer complete insights.

Insider risks will rise as attackers try to extort and compel otherwise reliable insiders into doing bad things. Meanwhile, attacks on federated identity and authentication manufacturers will intensify to hit additional software-as-a-service (SaaS) providers. Targeted Phishing or Whaling Attacks are also expected to increase significantly in the coming years, where senior executives are more often aimed for getting out sensitive company information through legitimate e-mails.

Last year, we witnessed various cyber-security developments ranging from cyber-attacks on nations like Ukraine and Costa Rica to alerts about state-sponsored threat actors endangering critical industries. The tech sector took a sharp blow from the looming recession, which will continue this year, increasing the risk of security breaches as the cyber-security sector is not immune to these changes.

It is a persistent tug of war for security professionals, who constantly put up a fight against cyber threats to protect increasingly expansive digital assets. These have grave repercussions, leading to the evolving risk of cyber security burnout. According to the latest Forrester survey, about 51 per cent of cyber security professionals have experienced extreme stress or burnout, with 65 per cent thinking of putting their papers because of excessive mental, physical and emotional exhaustion.

Critical infrastructure industries like manufacturing, healthcare, education and energy, to name a few, will be among the sectors under high attack in 2023. With the ongoing global geo-political conflicts such as the Ukraine/ Russia war, cyber-criminals are intensifying their activities targeting these industries. The most vulnerable sectors are healthcare and education, where the latter saw a 328 per cent increase in ransomware attacks last year. And, as both these sectors are expanding their IoT footprint, this has made them more susceptible to digital attacks.

PRIYA KANDURI

Perceived as one of the most prevalent and damaging tools for cybercriminals at their disposal, ransomware has roughly extorted $100 million from companies since June 2021. It is a growing threat through double extortion tactics, ransomware as a service, and massive DDOS attacks, forcing governments and companies to work together to eliminate ransomware forever. Experts believe one way to eradicate ransomware and ensure a robust cyber security solution framework is to stop paying for any such malicious activity entirely.

Attackers are leveraging technologies like AI & ML for social engineering attacks and impersonation, referred to as 'deep fakes'. They use them to create fake images and videos of real people to infiltrate organisations that can be 'difficult to prevent'. Biometric authentication methods can prove less useful in security, with deep fakes becoming more sophisticated. On the other hand, everyday individuals should routinely check their accounts, particularly for banking, loans, and other financial services.

It has become a 'cat-and-mouse' game with attackers trying to slice out ways to exploit weakness and 'MFA fatigue' as more organisations are adding MFA as a security layer. Experts fear that the attackers may use the technology and human weaknesses like 'notification fatigue' to bombard customers with requests until they finally relent.

Not everything will go wrong in 2023. Employee views towards cyber security solutions have improved due to the shift to remote and hybrid work. Firms that have regular security awareness training have developed a positive security culture.

Organisations are learning that 95 per cent of cyber-security breaches are caused by human factors, underscoring the significance of having a strong security culture. Attack risk is decreased through a robust security culture, while personnel is operationalised as the last line of defence. Many tech CEOs (87 per cent) think robust security cultures are just as crucial as technical measures. ◆

*The author is senior vice president & CTO, IMSS and head, cyber security, Happiest Minds Technologies*