INDUSFACE™

5 Top Cyber Threats That Will Ruin Your Business

As our digital activities increase, so does cyber criminals' opportunity to take advantage of it, which leads to new innovations in cyber threats against businesses.

Global cyberattack costs are on the rise, it is predicted that by **2025,** cybercrime will cost global businesses **$10.5 trillion** annually. (Cybersecurity Ventures)

Cyber threats are everywhere, and they are not going anywhere. However, knowing which attack vectors are highly prone to be exploited can help in designing proactive cyber defense. Here are the top cyber threats that will continue to turn the enterprises around the world into hackers' gold mines.

VULNERABILITIES

Did you know? If you enter the unusual command, your devices can begin to react unexpectedly.

Attackers exploit such errors, enter unexpected instructions, and disable security bypass logins and firewalls. Extra layers of security with regular updates can guard you against such attacks when they're due to vulnerabilities.

PHISHING ATTEMPTS THAT MOVE BEYOND EMAILS

How much do you think a phishing attack will cost your business?
A successful phishing attack is a **$3.7 million** annual cost for a company. (csoonline)

Phishing is a kind of threat where a hacker attempts to obtain sensitive details by pretending to be a legitimate person through email.

In 2020, phishing was the most common type of cyberattack 2020 and the frequency of phishing incidents doubled. (FBI)

114, 702 incidents in 2019
241, 324 incidents in 2020

FOCUSED RANSOMWARE ATTACKS

This cybercrime threatens businesses with harm by denying access to their data. A successful ransomware attack can cause businesses to lose millions of dollars as ransom payments. It is estimated that by 2021 ransomware attacks can cost companies **$20 billion** annually (Cybersecurity Ventures).

Ransomware grows easier to spread, tougher to stop – paying ransom encouraging hackers to keep refining these kinds of attacks. This is not just a security problem; it is a business and cultural problem.

INSIDER THREAT

As more employees shift to work from home that opens them to more risks, enterprises should consider extra precautions to limit insider threats. Careless or disgruntled employees and attackers who access credentials can cause massive damage to enterprises.

Negligent employees were found to have triggered **62%** of cyber threats, making the highest financial burden costing an average of **$4.58 million** per year. (Observeit)

Further, security teams are forced to balance the business and budgetary concerns with the requirement for data protection.

"A stitch in time saves nine" – the longer an insider threat stays the costlier it's to rectify.

POOR PATCH MANAGEMENT

57% of data breaches are due to poor patch management (Ponemon).

Software patches are a vital component of IT security. Through unpatched software, attackers learn the software vulnerabilities and exploit them to launch an attack.

Having a solid vulnerability assessment methodology can reduce the risk of poor patch management threats.

PROTECT YOUR BUSINESS WITH INDUSFACE

Start with the cybersecurity service at Indusface to learn how you can prepare for the ever-increasing cyber threat landscape. The security solutions we offer are sophisticated as the security threats facing businesses. Web application firewall, web application scanning, patch management, bot mitigation, DDoS protection, SSL encryption are few samples of our services.

REFERENCE

https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/
https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf
https://www.csoonline.com/article/2975807/phishing-is-a-37-million-annual-cost-for-average-large-company.html
https://www.observeit.com/cost-of-insider-threats/
https://www/indusface.com