SPOOKY *CYBERSECURITY* STATISTICS

TO HELP YOU PREPARE FOR THE WORST

A cyberattack is a scary event. It can shut down businesses, cripple governments and incapacitate entire countries if the right measures are not taken against it.

This Halloween, we bring you eight cybersecurity statistics that emphasize the dangers of cyberthreats and impel you to prepare for the worst.

8 Scary Cybersecurity Statistics

1

SMBs FACE CONSIDERABLY HIGHER DATA BREACH COSTS THAN LARGE ORGANIZATIONS

Cyberattacks on SMBs have spiked considerably in the last few years since they often have fewer resources and lack security expertise. In 2023, data breach cost increases range from 13.4% for companies with less than 500 employees to almost 20% for those with 1,001-5,000 employees.

Source: *Cost of a Data Breach Report 2023, IBM*

2

17% OF SMBs FEEL THEY FACED CYBERSECURITY ISSUES DUE TO LOST/STOLEN CRENDENTIALS

Compromised passwords are a threat to businesses. Tighten your password security protocols and implement authentication methods like two-factor authentication (2FA) and single sign-on (SSO) for maximized security.

Source: *SMB Cybersecurity for MSPs Report, Datto*

3

3.5 MILLION UNFILLED CYBERSECURITY JOBS PREDICTED TILL 2025

The number of unfilled cybersecurity jobs globally remains at 3.5 million in 2023, and the disparity between demand and supply is expected to remain the same until at least 2025. Address the skill gap by implementing cybersecurity training or partner with academic institutions to nurture cybersecurity talent.

Source: *Cybersecurity Jobs Report, Cybersecurity Ventures*

4

37% OF COMPANIES FACED $10,000–$50,000 IN RANSOM COSTS

Most SMBs believe that a successful ransomware attack can be detrimental to their business. The potential costs of ransomware attacks go well beyond the price of the ransom. Many attacked businesses experience significant downtime, which could also lead to customer and revenue losses.

Source: *SMB Cybersecurity for MSPs Report, Datto*

5

PHISHING IS THE BIGGEST SECURITY WOE THAT SMBs FACE

32% of SMBs experienced a phishing attack in the past 12 months (July 2021 to July 2022), with 72% expecting a phishing attack in the next year. Since phishing messages are a precursor to severe cyberattacks like ransomware, business email compromise (BEC) and account takeover (ATO), organizations must fine-tune their phishing mitigation strategies and train their employees to identify and report any phishing activities.

Source: *SMB Cybersecurity for MSPs Report, Datto*

6

NEGLIGENCE-BASED INSIDER THREAT INCIDENTS COST ORGANIZATIONS AN AVERAGE OF $6.6 MILLION PER YEAR

56% of security incidents experienced by organizations were due to a negligent employee or contractor, and the average annual cost to remediate the incident was $6.6 million. The average number of days to contain an insider incident was 85 days.

Source: *2022 Cost of Insider Threats Global Report, Ponemon Institute*

7

INSIDER THREATS HAVE RISEN 44% IN THE LAST TWO YEARS

Malicious, negligent and compromised users are a serious and growing risk for organizations across sectors. In the last two years, insider threat incidents have risen 44%, with costs per incident up more than a third to $15.38 million.

Source: *2022 Cost of Insider Threats Global Report, Ponemon Institute*

8

GLOBAL CYBERCRIME DAMAGE COSTS PROJECTED TO HIT $10.5 TRILLION BY 2025

Cybercrime damage costs include theft of personal and financial data, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems and reputational harm. This statistic reinforces the fact that a large number of organizations still remain unprepared for a cyberattack.

Source: *2022 Official Cybercrime Report, Cybersecurity Ventures*

The above statistics show that cyberattacks and data breaches can be a huge threat to you. It is critical for your organization to establish a proper strategy to mitigate security risks. Even if you are a small business with limited budget, you can achieve enterprise-level security with Kaseya VSA.

Kaseya VSA is a unified endpoint management solution that manages your entire IT environment and ensures that your systems and data are always protected. To learn more about Kaseya VSA

REQUEST A DEMO HERE

Kaseya