Why SMBs Can't Ignore These Ransomware Statistics

Cybercriminals attack organizations of all sizes across the globe. Here's what you need to know about these growing ransomware threats and the steps you can take to protect your business.

1 Risks of Cyberattacks

13% Verizon Data Breach Investigation Report (DBIR) found that ransomware attacks have increased by 13% between 2020 and 2021 – a bigger jump than the past FIVE years combined.

$265 billion Ransomware will cost its victims around $265 billion (USD) annually by 2031.

EVERY 02 SECONDS Cybersecurity Ventures predicts, a new attack on businesses every TWO seconds by 2031.

2 Cyber risks top worldwide business concerns in 2022

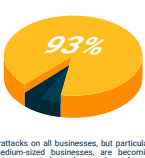
44% Cyber Incidents

42% Business Interruption

25% Natural Disasters

Cyber incidents top the Allianz Risk Barometer for only the second time in the survey's history (44% of responses). Business interruption drops to a close second (42%) and Natural catastrophes ranks third (25%), up from sixth in 2021.

Cybercriminals can penetrate 93 percent of company networks



Among the findings of a new study of pentesting projects from Positive Technologies, conducted among financial organizations, fuel, and energy organizations, government bodies, industrial businesses, IT companies, and other sectors. In 93 percent of cases, an external attacker can breach an organization's network perimeter and gain access to local network resources.

43% Cyberattacks are aimed at SMB's

Cyberattacks on all businesses, but particularly small to medium-sized businesses, are becoming more frequent, targeted, and complex. According to Accenture's Cost of Cybercrime Study, 43% of cyberattacks are aimed at small businesses, but only 14% are prepared to defend themselves.

14% SMB's are prepared to defend themselves

According to Ponemon Institute's State of Cybersecurity Report, small to medium businesses around the globe report recent experiences with cyberattacks:

- **45% say that their processes are ineffective at mitigating attacks.**
- **66% have experienced a cyberattack in the past 12 months.**
- **69% say that cyberattacks are becoming more targeted.**

57% Phishing / Social Engineering

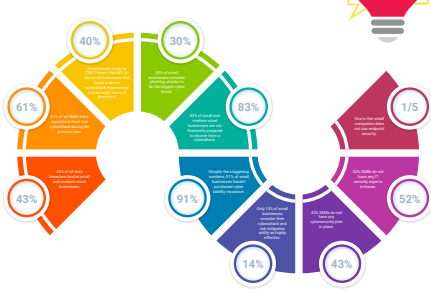
33% Stolen Devices

30% Credential Theft

3 Ransomware Key Findings

Keeping up with the latest cyberattack statistics is pertinent for understanding the state of cyber threats, commonly leveraged vulnerabilities, implications of successful cyberattacks, and effective strategies for mitigating prevalent threats. So, here are 10 important cybersecurity statistics to open your eyes towards the insufficiency of preventative and combative measures in smaller companies despite the inevitability of modern cyberattacks:

10 Important STATISTICS



4 Costs of Cybercrime

Cybercrime will cost companies worldwide an estimated $10.5 trillion annually by 2025, up from $3 trillion in 2015. At a growth rate of 15 percent, year over year — Cybersecurity Ventures also reports that cybercrime represents the greatest transfer of economic wealth in history.

2015 - 2021

Between 2015 - 2021, global spending on cybersecurity products & services is predicted to exceed $1 trillion cumulatively over the five-year period.

2021 - 2022

From 2021 to 2022, security budgets as a share of overall revenue jumped by 51%.

This year's budgets will comprise 12% to 15% of overall enterprise IT spending, which is 2X from the recent past.

5 Ransomware Trends in 2023

6 Who's behind ransomware attacks?

REvil (Sodinokibi):
Group operated by the Russian-speaking REvil since 2019, has been responsible for breaches such as Kaseya & JBS.

Lockbit:
Data encryption malware in operation since 2019.

DearCry:
Ransomware variant designed to take advantage of four disclosed vulnerabilities in Microsoft Exchange.

Lapsus$:
A South American ransomware gang that has been linked to cyberattacks on some high-profile targets, like Nvidia, Samsung, and Ubisoft, Okta, Vodafone, T-Mobile, Microsoft.

7 How to protect from ransomware attack

Patch regularly.
Ransomware code often targets known vulnerabilities. Keep your software and firmware updated.

Use antivirus and anti-spam solutions.
Enable regular system and network scans and automatically update signatures. Implement an anti-spam solution to stop phishing emails from reaching the network.

Perform frequent data backups.
By having reliable backups, the risk of losing data can be minimized.

Provide social engineering and phishing training.
Urge not to open suspicious emails, click on links, or open attachments, and be cautious before visiting an unknown website.

Check out this short webinar on "Why Companies Need a New BDR Strategy for 2023"

LEARN MORE

For more information

CONTACT

Source Link :

1. https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf
2. https://www.allianz.com/content/dam/onemarketing/azcom/Allianz_com/press/document/Allianz_Risk_Barometer_2022_FINAL.pdf
3. https://www.verizon.com/business/en-gb/resources/reports/dbir/
4. https://www.globenewswire.com/news-release/2020/11/18/2129432/0/en/Cybercrime-To-Cost-The-World-10-5-Trillion-Annually-By-2025.html
5. https://www.infrascale.com/blog/preparing-for-a-ransomware-attack/