555 Waters Edge Lane, Lombard, Illinois 60148,
https://www.greggtechnologies.com
630-706-8222

DBIR 2024: RELEVANT STATS AND TAKEAWAYS

Verizon recently released this year's Verizon Data Breach Investigations Report ("DBIR"), which analyzed over 30,000 security incidents. Of these, more than 10,000 were confirmed data breaches across more than 90 countries. Here are some of the most relevant stats and takeaways, and how you can reframe them into questions to identify the proper solutions for your customers.

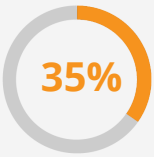
RANSOMWARE

The average Ransomware loss to a company was 1.34% of the corporate revenue. Some ransomware attacks took up to 24% of the annual corporate revenue.

ONE THIRD

of all breaches involved Ransomware or other extortion. Pure extortion attacks account for 9% of all breaches.

How is your Ransomware response and preparation program?



of all breaches involved The Insider Threat. Most (73%) are due to errors rather than malicious intent.

Do you have an insider threat program?

THREAT ACTORS

will use email to target users and built-in desktop sharing apps to gain access to systems.

How are you protecting yourself from built-in software attacks?

VULNERABILITY EXPLOITATION

- Vulnerability exploitation as the critical path to initiate a breach **tripled** last year.
  Do you have a vulnerability management program?
- VPNs vulnerability exploitation is likely to **increase in 2025.**
  How do you secure your remote workforce? Is a traditional VPN enough?
- The exploitation of subcontractors increased from **9% to 15%** in 2023.
  How are you vetting anyone allowed to access your environment?
  How safe is your supply chain?
- Patching vulnerabilities takes the average user between **30 and 55 days.**
  How long does it take you to patch a vulnerability?
- Once a vulnerability is disclosed to CISA, it will start being exploited **within 5 days.**
  How long does it take your vendors to patch your products?

PRETEXTING/PHISHING

The median time for a user to fall for a phishing attack is less than

60 SECONDS

Do you train your employees on phishing awareness?

Pretexting is more likely a

SOCIAL ENGINEERING ATTACK

than phishing. The threat actor will stay engaged longer and often use impersonation to gain trust in an environment.

How do you verify that someone contacting you is, in fact, who they say they are?

Do you test for pretexting as well as phishing?

Servers are targeted in more than

80%

of all events yet we spend a lot of time focused on end-point products such as EDR/XDR.

How are you protecting your servers from threats?

WHAT DO YOU DO IF YOU HAVE A DATA BREACH?

- Stolen credentials are often sold on the Dark Web **less than a day after they are collected.**

  Do you have any Dark Web scanning tools to let you know when a credential has been sold?

- In a Business E-mail Compromise (BEC), companies that worked with the FBI recovered **79% of their losses.**

  Do you have "Contacting the FBI" built into your Incident Response Plan?

IMPORTANT TAKEAWAYS

The MoveIT breach had the largest effect on education.

Generative AI has not been used significantly in attacks in 2023. That could change in 2024.