LATERAL CONNECT

Lessons Learnt from 2022 Data Breaches

Protect your Organisation from Cyberattacks

www.lateral-connect.com

Cyberattacks and data breaches are still a big business, despite substantial increases in cybersecurity defences around the globe. Data breaches continue to affect companies and organisations of all shapes, sizes, and sectors, and they're costing US businesses millions in damages. This puts more onerous in organisations investing in a cybersecurity framework and an organisational resilience, to avoid regulatory fines, other technical issues, litigations or class action lawsuits.

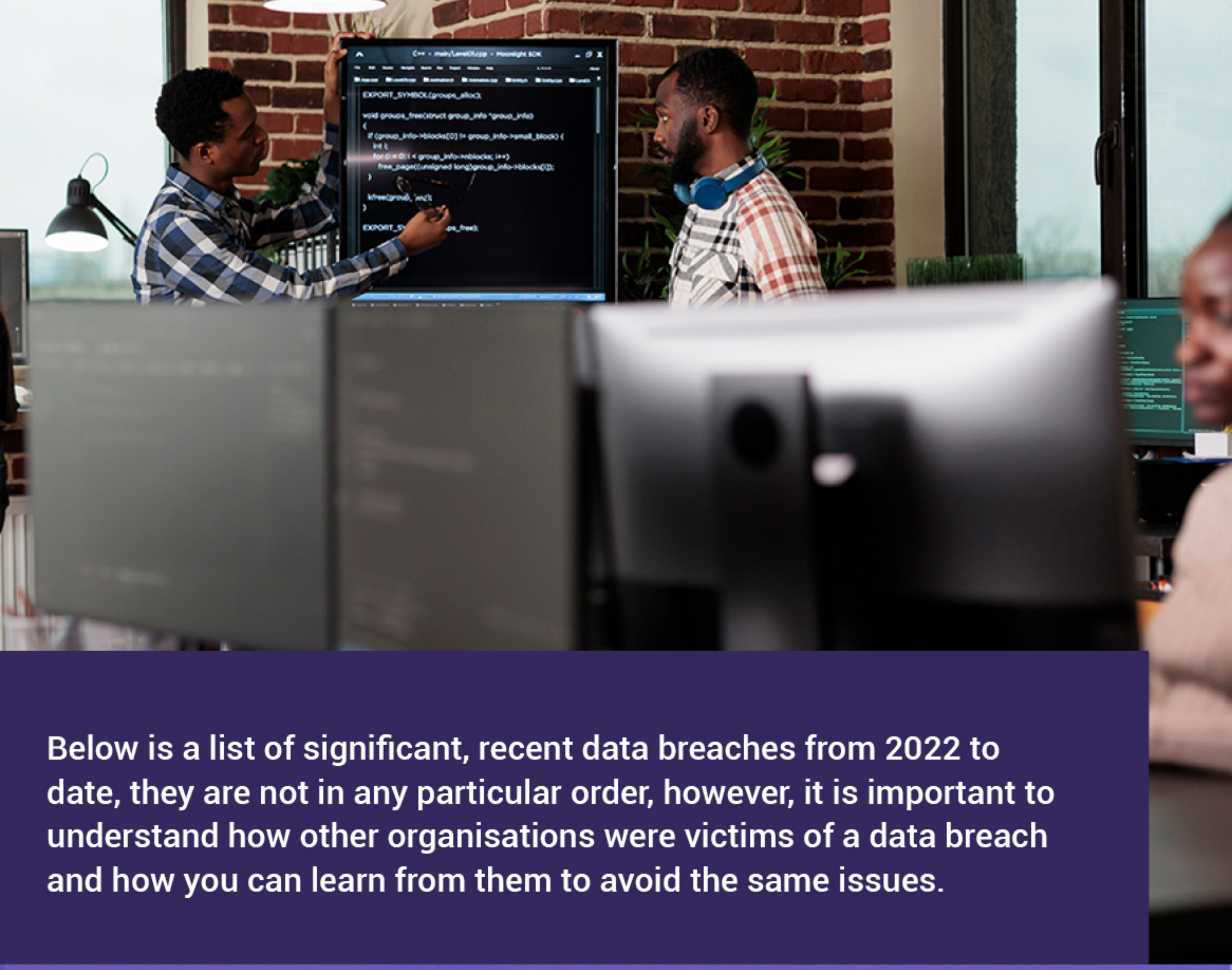
Cyber resilience vs. Cybersecurity

Cybersecurity

Having a cyber defence strategy which consists of technologies, people and processes that are designed to enforce policies and protect systems, networks, data, and IT infrastructure from cyber threats (e.g., malware, ransomware, hacktivism, malicious insiders)

Organisational Resilience

Is the ability to anticipate, prepare for, respond and adapt to incremental change and sudden disruptions in order to survive and prosper.



Below is a list of significant, recent data breaches from 2022 to date, they are not in any particular order, however, it is important to understand how other organisations were victims of a data breach and how you can learn from them to avoid the same issues.

1. Rackspace - managed hosting, cloud storage, databases and analytics company

In Dec. 2022, Rackspace suffered one of the most high-profile ransomware attacks, which caused significant outages and disruptions for its Hosted Exchange services. Customers were unable to access their mail services, four days later, Rackspace confirmed the outages were caused by ransomware and began migrating its Hosted Exchange customers to Microsoft 365. Rackspace had not yet determined if any data was affected, however, Cole & Van Note have filed a class action over this incident and how Rackspce handled the protection of their personal data.

2. T-Mobile - mobile communications and telecommunications company

In Dec. 2022, Rackspace suffered one of the most high-profile ransomware attacks, which caused significant outages and disruptions for its Hosted Exchange services. Customers were unable to access their mail services, four days later, Rackspace confirmed the outages were caused by ransomware and began migrating its Hosted Exchange customers to Microsoft 365. Rackspace had not yet determined if any data was affected, however, Cole & Van Note have filed a class action over this incident and how Rackspce handled the protection of their personal data.

3. Royal Mail - a british multinational postal service and courier company

On Tuesday of this week Royal Mail services Royal Mail were unable to dispatch export items, including letters and parcels to overseas destinations due to a cyberattack. The share price of International Distributions Services, the name of Royal Mail's London-listed parent group, fell on Wednesday afternoon after the announcement, finishing the day down by 0.8%. The National Cyber Security Centre (NCSC) are aware of the incident and working with them to "understand the impact

4. LassPass - online password manager and form

On Tuesday of this week Royal Mail services Royal Mail were unable to dispatch export items, including letters and parcels to overseas destinations due to a cyberattack. The share price of International Distributions Services, the name of Royal Mail's London-listed parent group, fell on Wednesday afternoon after the announcement, finishing the day down by 0.8%. The National Cyber Security Centre (NCSC) are aware of the incident and working with them to "understand the impact

5. OKTA - an identity and access management company

OKTA suffered its fourth cyber attack this year when it was informed by GitHub about "suspicious access" to its code repositories earlier in Dec. 2022. They have since concluded that hackers used malicious access from a current employee, to copy code repositories associated with Workforce Identity Cloud (WIC), the organisation's enterprise-facing security solution. Okta said it has also notified law enforcement.

All data breaches are different and will have compromised all organisations in different ways, however, its affected customers suffer most from either identity theft, potential social engineering, or potential phishing campaigns.

How To Help Prevent a Data Breach

Patch your vulnerabilities

- Ensure these are managed adequately, as it is a common way a hacker can use to access a company's systems again after a successful first attempt

- Failing to patch vulnerabilities from the first attack can lead to a second one take extra care with on-premises tools

Human error

- Train your work workforce, especially admin and super admin users to use a strong password, as these may expose a company's systems to subsequent attacks

- Train your work workforce, especially admin and super admin users to use a strong password, as these may expose a company's systems to subsequent attacks

Malware

- Hackers use malicious software such as viruses, ransomware, Trojans, spyware, adware, etc., to steal confidential information from an organisation's network system. If a company fails to step up monitoring protocols after its first breach, there is nothing to stop repeat attacks from occurring.

LATERAL CONNECT

Written by a Security Trainer @lateral-connect.com