Marsh Commercial

Cyber Security Glossary

Accidental disclosure

This refers to the accidental disclosure of sensitive data resulting in data breach.

Business email compromise (BEC)

Business email compromise (BEC) is a form of phishing attack where a cyber-criminal impersonates a senior executive and attempts to coerce an employee, customer, or vendor to transfer funds or sensitive information to the phisher. BEC scams are a serious threat to organisations of all sizes and across all sectors, including non-profit organisations and government. It represents one of the fastest growing cyber-crime operations due to the low cost and high return.[1]

Cost per compromised record

This works out the cost or loss per customer or client record impacted by a data breach. Sometimes, if a criminal accesses one customer – they can access them all. However in some cases the breach may involve just one or a handful of records. Records can also be segmented based on type, with different costs attached depending on how sensitive the information is.[2]

Cyber-crime

Cyber-crime is criminal activity that either targets or uses a computer, a computer network or a networked device. Most cyber-crime is committed by cyber-criminals or hackers who want to make money. Cyber-crime is carried out by individuals or organisations.

Some cyber-criminals are organised, use advanced techniques and are highly technically skilled. Others are novice hackers. Rarely, cyber-crime aims to damage computers for reasons other than profit. These could be political or personal.[3]

Cyber liability insurance policies

A cyber liability insurance policy can cover your initial liabilities on media, data security, viruses and hacking. A policy can then cover costs associated with customer notifications, credit monitoring and legal fees. If required, forensics will be appointed to identify the root cause and PR consultants can mitigate damage to your brand, often at an additional cost.[4]

Data breach

A data breach is the intentional or unintentional release of secure or private/confidential information to an untrusted environment. Other terms for this phenomenon include unintentional information disclosure, data leak, information leakage and also data spill.[5]

Fraudulent instruction

Fraudulent instruction is a social engineering attack in which compromised email credentials or spoofing are used to induce an employee to make a wire transfer or other electronic payment to a bank account controlled by a cyber-criminal.[6]

Human error

Human error enables attackers to access encrypted channels and sensitive information. Staff can make a variety of mistakes that put their company's data or systems at risk, often because they lack the knowledge or motivation to act securely, or simply because they accidentally slip up.[7]

The most common types of human error leading to data breach are:

- Sending valuable data to incorrect recipients via email
- Accidentally emailing documents with sensitive data
- Publishing confidential data on websites by mistake
- Outdated software allowing unwanted access
- Phishing scams

Phishing

Phishing is when cyber-criminals create an email to look like it comes from a trusted source. The email is designed to induce a recipient into sharing sensitive information, download malware or visit an infected website.

Social engineering

Social engineering involves techniques such as email phishing used to manipulate someone into providing confidential information, e.g. log-in credentials, or taking other actions that bypass normal security to help the attacker commit theft or fraud.

[1] National Crime Agency
[2] Capita.com
[3] Kaspersky
[4] Marsh Commercial Cyber Liability for Healthcare
[5] Wikipedia
[6] Beazley Breach Briefing 2019
[7] Oz Alashe, CEO of Cybsafe