Cyber Jargon Buster

AI (Artificial Intelligence)

A broad term for technologies that allow computers to analyse information, learn or identify patterns, and generate responses, recommendations or content. This includes systems that can work with language, images, audio and large amounts of data.

What brokers need to know

AI is helping businesses become more productive. It's also helping cybercriminals create more convincing phishing emails, scams and impersonation attacks.

Breach Counsel

Specialist lawyers who help organisations respond to cyber incidents.

What brokers need to know

They often coordinate the incident response, advise on legal obligations and help businesses understand what they need to do next.

---

24 hour Breach Response Hotline

A dedicated incident reporting service available to insureds following a cyber event.

What brokers need to know

Early notification allows breach counsel and other specialists to be engaged quickly, often reducing disruption and improving outcomes. It’s important to refer to the policy wording for how to notify claims to insurers.

Business email compromise

A type of fraud where criminals gain access to, impersonate or spoof a legitimate email account to trick individuals into transferring funds or disclosing information.

What brokers need to know
Many cybercrime claims involve BEC rather than a traditional "hack". A convincing email can result in significant financial loss without any systems being encrypted.

Business Interruption Losses

The financial impact of a business being unable to operate normally.

What brokers need to know

The biggest cost of a cyber incident is often the disruption caused to trading, production or service delivery rather than the attack itself.

Data Breach

Unauthorised access to sensitive or confidential information.

What brokers need to know

A data breach can trigger legal, regulatory, operational and reputational consequences, even when no money is stolen.

Data Mining

The process of reviewing compromised data to identify what information has been affected and who may need to be notified.

What brokers need to know

Data mining can significantly reduce notification costs by identifying exactly which individuals are impacted.

Deepfake

An AI-generated image, video or voice designed to appear genuine.

What brokers need to know

Deepfakes are increasingly being used to impersonate trusted individuals and support fraud or social engineering attacks.

Digital Forensics

The process of investigating how a cyber incident happened.

What brokers need to know

Think of digital forensic specialists as cyber detectives. Their role is to understand what happened, how it happened and what needs to happen next.

Funds Transfer Fraud

The fraudulent transfer of money following deception, impersonation or compromised communications.

What brokers need to know

Often linked to BEC incidents and can lead to substantial losses before the fraud is detected.

Incident Response

The coordinated process of investigating, containing, managing and recovering from a cyber incident.

What brokers need to know

Early incident response can significantly reduce costs and business disruption

MFA (Multi-Factor Authentication)

An additional security check used alongside a password.

What brokers need to know

One of the simplest and most effective cyber security controls available. It's often a key topic in cyber insurance conversations.

OSINT (Open-Source Intelligence)

Information gathered from publicly available sources such as websites, social media and public records.

What brokers need to know

Cybercriminals often use publicly available information to make phishing and impersonation attacks more convincing.

Phishing

A fraudulent email, text or message designed to trick someone into clicking a link, sharing information or taking an action.

What brokers need to know

Phishing remains one of the most common causes of cyber incidents.

Ransomware

Malicious software that prevents access to systems or data until demands are met.

What brokers need to know

The real cost often comes from operational disruption, recovery costs and lost revenue rather than any ransom demand.

Ransomware-as-a-Service (RaaS)

A criminal business model where ransomware developers provide tools and infrastructure to affiliates in return for a share of the proceeds.

What brokers need to know

This has made ransomware more frequent and accessible, allowing criminals with limited technical skills to conduct sophisticated attacks.

Social Engineering

The use of manipulation, trust and persuasion to influence people into taking actions they normally wouldn't.

What brokers need to know

Many cyberattacks target people before they target technology. Social engineering is often at the heart of phishing, fraud and impersonation attacks.

Threat Actor

A person or group responsible for carrying out a cyberattack.

What brokers need to know

Not all threat actors are the same. Some are financially motivated criminals, others are organised groups, insiders or activists.

Vishing

Short for "voice phishing".

A scam carried out by telephone where an attacker pretends to be somebody trusted.

What brokers need to know

If you've ever heard of somebody receiving a convincing call from "IT Support" or their bank, that's often a vishing attack.

Zero-Day Vulnerability

A software flaw that is unknown to the software provider when attackers first begin exploiting it.

What brokers need to know

These vulnerabilities can be particularly valuable to attackers because organisations may not yet have a fix available.

This document provides examples of incidents and does not constitute an expression of coverage under any insurance product. This is not a solicitation or offer for insurance. Coverage is only available from licensed brokers. Coverage is subject to the full terms and conditions of the policy

Cyber risk isn't really about technology.

It's about people, businesses and resilience.

The technology changes.

The jargon changes.

The threats evolve.

But the broker's role remains the same:

Helping clients understand and mitigate risk.

Get in touch with our cyber team via our website

britinsurance.com/insurance/cyber

Continue your learning

For more cyber insights, emerging threats, broker resources and client-friendly content, visit the Brit Cyber Knowledge Hub. The guide is designed to start the conversation; the Knowledge Hub helps you continue it.