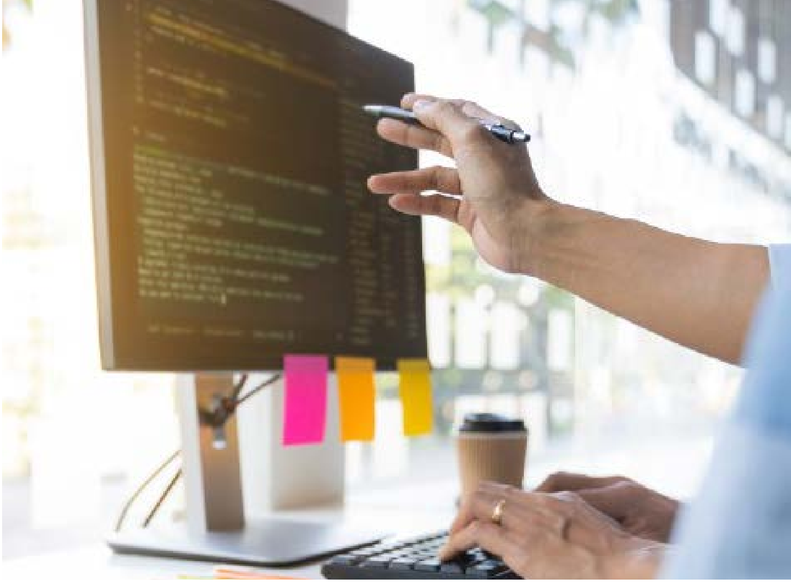
Insurance and the evolving cyber landscape



Cyber insurance is still very much an emerging area for the industry since its first appearance in the 1990s but recent socio-political events are shaping the types of attack being perpetrated and, as a result, companies' cybersecurity requirements.

In this article we consider some key factors shaping the future of cyber insurance; the most prevalent types of attack being deployed by criminals; and guidance for businesses in combatting cyber threats.

External influences

Covid

The COVID lockdown in March 2020 forced the large-scale move towards working from home, presenting new opportunities for cyber criminals. The rapid geographical spread of employees resulted in the wide distribution of office IT equipment, thereby introducing thousands of new routers, networks and personal WiFi connections. This, coupled with remote workers using their own (noncorporate) devices, led to increased exposure across companies' IT ecosystems. According to government data, 2020 saw a peak in cyber incidents, with 46% of businesses identifying an attack. [1]

Ransomware

Incidence of ransomware also accelerated during the pandemic, with criminals operating phishing scams involving information about vaccines or government financial assistance. [2] Perhaps unsurprisingly, ransomware ranked as the top cyber exposure of concern in the 2022 Allianz Risk Barometer.

Additionally, the various lockdowns prompted an increased reliance on video conferencing apps both for individuals and businesses. One which gained major prominence was Zoom – at the time a relatively underdeveloped and cost-free application. Companies started using the app en masse for business purposes and Zoom became a household name almost overnight, increasing from 10 million daily participants in 2019 to 300 million by October 2020. [3]

Security concerns

However, since Zoom was never designed specifically for corporate use, concerns soon surfaced around security vulnerabilities, such as the potential for any individual being able to gain access to meetings (known as 'Zoombombing'). Larger organisations with more mature security postures were less at risk, having processes in place for testing software or preventing the unauthorised installation of software.

Cyber incidents can have huge repercussions for organisations, from financial loss to business disruption, reputational damage and fines. Given predictions that flexible working is set to continue, it's concerning that more than half of firms believe their exposure to attack has increased due to working from home arrangements. [4]

With many households retaining their dual function as both home and office at least some of the time, businesses will need to consider ways to improve their cyber security posture and minimise the risk of attack.

[1] Cyber Security Breaches Survey 2022. Cyber Security Breaches Survey 2022 - GOV.UK (www.gov.uk). Published March 2022.
[2] KPMG. The rise of ransomware during Covid-19. 2022.
[3] Forbes. In the Post Covid-19 world, Zoom is here to stay. In The Post COVID-19 World, Zoom Is Here To Stay. (forbes.com). February 2021.
[4] Survey of 1,000 UK firms from British Chambers of Commerce and Cisco. BCC FINDS RISING CYBER-ATTACK FEARS IN HYBRID WORKING WORLD (britishchambers.org.uk) January 2022.

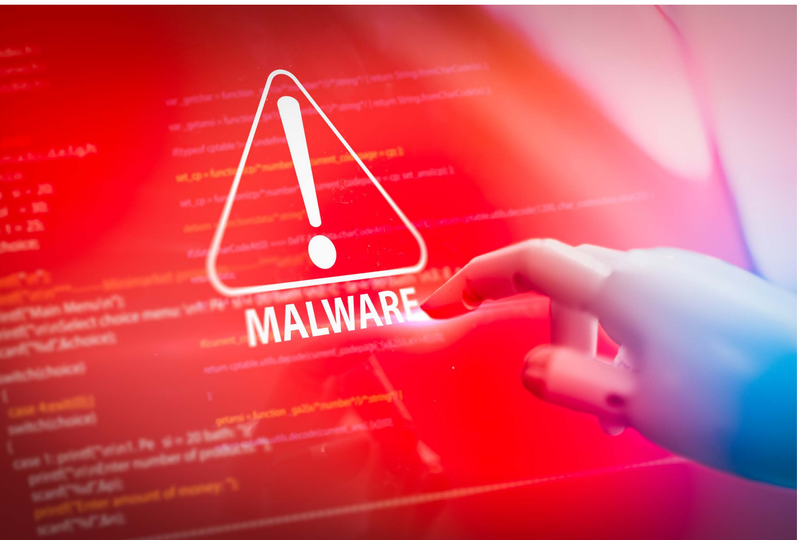
Allianz

Unsupported systems can be open to security threats and provide easy access to computer systems.

Artificial Intelligence (AI)

Cyber criminals are exploiting AI for cyber-attack purposes, leveraging its ability to identify patterns in behaviour. For example, hackers can use machine learning (ML) – a form of AI - to support password guessing. By using ML, including something known as generative adversarial networks (GANs), it's possible to analyse a vast dataset of passwords and generate likely password variations. So-called 'bad actors' can use AI to create personalised 'spear phishing' messages which target C-suite executives (CEOs, CCOs, etc) and either seek to obtain confidential information, or install malware on a device.

But AI can actually be used positively to thwart cyber criminals. Whereas monitoring cyber threats used to be an involved and time-consuming manual task, sophisticated AI systems are able to expedite the process without experiencing human fatigue and susceptibility to error. They achieve this by processing huge amounts of data to detect malware, run pattern recognition and automate defence responses.



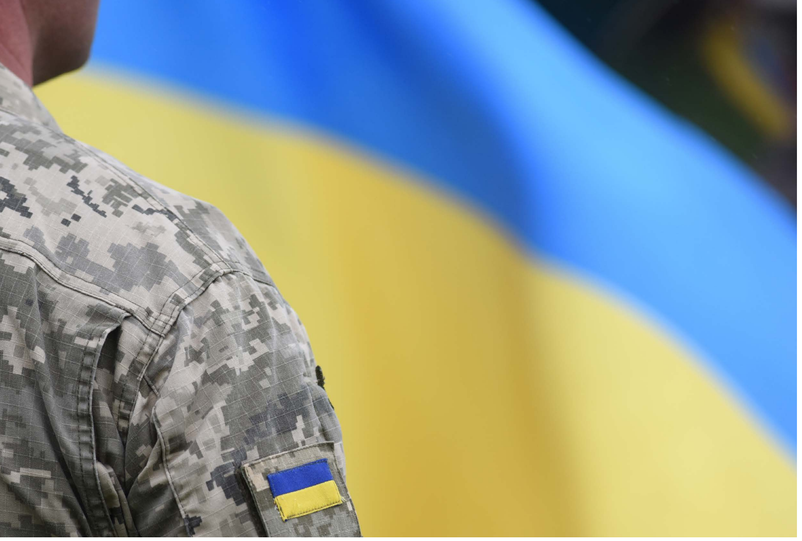
Internet of Things (IoT)

It's estimated that by 2030, there may be as many as 50 billion IoT connected devices globally.[5] As more smart devices become connected in the Internet of Things, it will heighten exposure to cyber risk, especially where connected devices might have lower levels of security.

For instance, criminals may be able to gain access to an organisation's IT systems through employees' mobile devices or the company's connected kettle. Computerised controls, including alarms, environmental controls and CCTV can provide a back door for cyber criminals because they often utilise cost-effective but non-supported operating systems.

Unsupported systems can be open to security threats and provide easy access to computer systems, bypassing firewalls and enabling hackers to gain access to a business's privateor confidential data.

[5] Statista. https://www.statista.com/statistics/802690/worldwide-connected-devices-by-access-technology/



Russia-Ukraine war

At time of writing, there have been no confirmed Ukraine-Russia related attacks on the UK. However, there are fears that any heightened cyberactivity against Ukraine could signal an elevated threat for allies. Previously, in June 2017, the NotPetya attack on Ukraine spread beyond its borders and impacted upon some UK operations.

It's thought to be the most costly cyber-attack in history. More recently, a series of distributed denial of service (DDoS) attacks in February, which attacked Ukrainian banking and defence websites, was attributed to the Russian military intelligence agency GRU.[6] Such attacks have led the UK's National Cyber Security Centre (NCSC) to issue guidance for organisations on how to improve their cybersecurity resilience.

Outsourcing of IT/security

Another worrying trend is the amount of attacks on managed service providers (MSPs). Many companies outsource their IT services to an MSP, not considering that even MSPs themselves are not immune to cyber threats. In fact, since MSPs may support hundreds of customers, criminals see this as a way of attacking multiple companies via a single vector.

The SolarWinds attack in 2020 was one such example, when hackers broke into the company's systems and ended up impacting around 20,000 of its customers. The attack was described as 'the largest and most sophisticated attack the world has ever seen'. [7] It's important for organisations to undertake due diligence when selecting an MSP, such as understanding what security mechanisms they deploy, how they back up customer data and whether they have ransomware insurance, to name just a few.

SolarWinds attack in 2020 was one such example, when hackers broke into the company's systems and ended up impacting around 20,000 of its customers.

How can a business best mitigate against cyber security threats?

In addition to the measures mentioned above, organisations can strengthen their security posture in a number of ways, including:

- training employees on how to recognise and report a potential breach
- implementing robust password security and considering the use of password manager tools
- using data encryption methods and ensuring data is backed up
- use of network segmentation; ensuring users only have access to relevant systems. Also using methods such as firewalls or airwalls (which securely connect anything, everywhere) to prevent an attack from spreading
- having a documented process for patching, including factoring in how quickly these can be implemented following a critical update
- maintaining a list of trusted applications and software, ensuring that anything not on the list cannot be used or installed
- allocating budget for IT security and infrastructure spend; the cost of this would be dwarfed by the repercussions of any cyber security breach
- having a current, robust business continuity in place.

ACOM9860 03.23

[6] https://www.gov.uk/government/news/uk-assess-russian-involvement-in-cyber-attacks-on-ukraine. 18 February 2022
[7] Reuters. SolarWinds hack was 'largest and most sophisticated attack' ever: Microsoft president. February 2021.