HISCOX
CYBERCLEAR®

Top cyber risk trends for 2022

Supply chain vulnerabilities

1

Next year we expect the supply chain attack trend will continue, and we see there being at least three distinct varieties:

i. a 'visible' supplier of yours (e.g. SolarWinds/Exchange) – a malicious actor exploits a known vendor/partner;
ii. an 'invisible' supplier of yours (e.g. Log4j/Eternal blue) – a third-party vendor/open source library that a vendor or you rely on uses. This dependency may be abstracted many layers away from your or your supplier's code;
iii. you are targeted as part of a larger vendor's supply chain. We have seen a number of incidents whereby smaller (and less well funded) companies have been targeted as an easier method of entry into large and generally better funded larger organisations.

2

Hybrid working is here to stay

We reported in our 2021 Hiscox Cyber Readiness Report that 41% of respondents had increased numbers of staff working remotely, and with coronavirus strains continuing to rear their heads, this likely won't revert back drastically anytime soon. Businesses are adapting and evolving to deal with these new ways of working and trading. Nearly one fifth (18%) said they had added new e-commerce channels. However, these changes were forced on businesses at very short notice, meaning they were not always planned, tested and secured with the rigour that they might have been under more normal times.

The Log4j vulnerability at the end of 2021 is a good example. If a company has had to invest in a new VPN solution it may not have sufficient in-house skills or experience to ensure that service is checked for the vulnerability and remediated in a timely fashion.

Ransomware evolves, regulation applies pressure

3

2022 will see the continued cat and mouse fight between the ransomware gangs and defenders/law enforcement. Expect ransomware groups to morph and rebrand as well as keep affiliates closer to minimise their chance of infiltration or compromise by competitors/disgruntled affiliates. Ransomware techniques will no doubt evolve, perhaps with better tools to exfiltrate sensitive data for 'double extortion' attacks.

Law enforcement will continue offensive cyber operations against ransomware gangs, and companies will be forced to do a better job at segmenting networks, securing back-ups and improving their resiliency.

Regulators will continue to focus on crypto exchanges, putting pressure on them to make it more difficult for criminals to 'cash out' their illegal gains.

4

Activism moves online

2021 has been another year in which a number of protest groups (notably Extinction Rebellion and Insulate Britain in the UK, but there are many other groups in other territories) have taken direct action is response to the climate challenge and other social-political issues the world is facing. The majority of this direct action has been physical events, ranging from protests to more intrusive action such as motorway blockades.

2022 could be the year we start to see protestors move online in a meaningful way. Perhaps technically-savvy disenfranchised activists will use online means to protest a company or government's stance on certain topics through a botnet or a DDoS-for-hire (distributed denial of service).

Quantum computing a possibility

5

Quantum is gaining momentum with some analysts predicting that a quantum computing breakthrough is around the corner. We're not convinced that this will necessarily come true in 2022, but what is undeniable true is that headway is being made and quantum's time is definitely coming. The world needs to consider the implications of ubiquitous quantum computing soon, and plan for its arrival.

Previously intractable problems will gain new approaches, as well as having a significant impact on cyber security. Software developers will need to keep one eye on these advances and start developing systems that are quantum-aware. This will no doubt lead to better and more sophisticated encryption algorithms and we may even get accurate weather predictions!

6

Cyber war and cyber operations

As we continue to deal with the global pandemic, and the impact this is having on the geopolitical and socioeconomic status quo, the use of overt cyberwarfare could very well emerge as the preferred method of force projection. Certainly Lloyd's of London seem concerned this could be the case, with the introduction this year of four new exclusions for cyber war and cyber operations. Though offensive cyber operations appear to be largely used by a government's intelligence agencies, it's not unusual for Lloyd's to have an advanced understanding of emerging risk.