nccgroup

Cyber Security Predictions & Trends:

2024 and Beyond

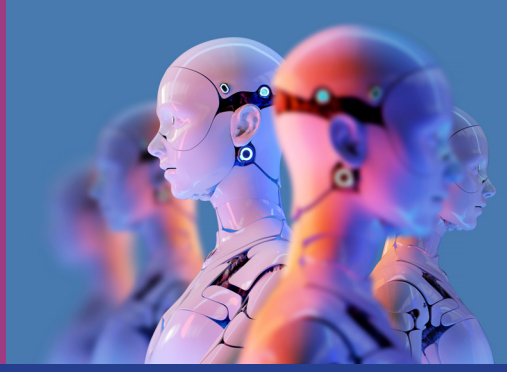
NCC Group's Cyber Security Predictions and Trends for 2024 and Beyond

We asked our experts for their thoughts on key areas of technology developments and advancements that are challenging the way in which we must approach cyber security and resilience in 2024 and beyond.

We're covering the ever-present AI conversation, preparing for Post Quantum Cryptography, the increasing threat to operational technology, what's next for blockchain, election year challenges and the converging landscape of net zero and cyber security.

Commercialisation of AI

1



2023 has seen the staggering increase in the use of Large Language Models; with ChatGPT, Bard and Bing chat fast becoming household names. Organisations have faced the challenge of managing the tricky balance between enabling staff to use these systems, while keeping their sensitive information secure.

Commercial offerings like ChatGPT Enterprise, Github CoPilot Enterprise, and Amazon Q, are specifically targeted at enabling enterprises to safely leverage this sensitive information via, while retaining security controls. In 2024 we can expect to see more businesses take advantage of these enterprise-oriented LLMs to improve productivity, drive efficiency and provide new business capabilities and applications.

Businesses are now seeing that there are real financial benefits to be gained - perhaps not the science fiction style capabilities predicted by some, but - certainly - practical, measurable improvements in productivity.

Now that these benefits are becoming clearer - in financial terms - investment by companies in these systems will increase. We are likely to see a steady increase in the use of LLMs and AI assistants in business; by the end of 2024, using AI assistants to help draft documentation, summarise documents, or reformat data, will be as natural as using a spelling or grammar checker today.

You can't have commerce without trust, and you can't have trust without security. Making sensitive data more available and useful, also exposes it. The business benefits of AI come with risks. Integrating sensitive information with Large Language Models will expose it to attackers in new ways; security controls that previously applied to (say) databases don't apply in the same way to free-text training corpuses, or Retrieval Augmented Generation systems.

The growing use of AI as a security control also presents a huge challenge – the efficacy of such solutions demands robust testing, evaluation, and assurance, lest we become too trusting of automated decision making in security governance that we believe to be optimal but renders our systems more vulnerable.

Recognising these risks, we'll see governments moving forward with their approaches to regulating AI security, with the EU edging ever closer to enacting the AI Act and other governments globally developing their plans to embed these safety and security principles in domestic regulation.

Operational Technology (OT)

2

Traditionally, attacks and malware specifically developed for Industrial Automation and Control Systems (IACS)/Operational Technology (OT) have been predominantly orchestrated at the nation-state level. Stuxnet, the first publicly known example, followed by others like Triton in 2017, highlights this trend.

In the past, financially motivated cybercriminals typically did not target these systems, mainly due to their air-gapped nature and the relatively low return on investment (ROI) compared to IT systems rich in monetizable data. However, the landscape is shifting. Ransomware, notably the most financially lucrative attack vector on traditional office IT systems, has seen an exponential rise. As OT/IT convergence accelerates for business benefits, ransomware attacks have begun to impact safety-critical and industrial systems. The Colonial Pipeline incident in May 2021 marked a significant turning point, demonstrating the potential to disrupt critical infrastructure through ransomware, even if unintentionally.

This shift is leading to a broader spectrum of attackers developing targeted attacks on critical infrastructure and IACS. What was once the exclusive domain of nation states is now expanding to include a wider range of cybercriminals.

Looking ahead, we anticipate a continued increase in malware targeting not only IACS but also SCADA systems, manufacturing, and robotics as businesses increasingly integrate and internet-enable their operations and facilities. The potential to take a manufacturing production line offline presents a lucrative ransom opportunity, with the equation of days of halted production multiplied by daily output translating into substantial lost revenue. This type of disruption extends to supply chain vulnerabilities. An effective attack on a key supplier in an interconnected industry, such as the Taiwanese semiconductor manufacturing sector, could have profound impacts across the global tech hardware landscape.

Preparing for Post Quantum Cryptography

4

It is possible we will see Quantum Supremacy in our lifetime, meaning there is a burgeoning challenge in preparing businesses for Post-Quantum Cryptography (PQC). While the requirements and PQC algorithms are broadly understood, ensuring a worldwide migration to robust PQC presents a challenging undertaking.

Existing trends are only accelerating – we are seeing more frequent and more sophisticated attacks that result in deprecating old algorithms, stimulate further improvements to existing algorithms and provide the potential for drastic changes to future algorithms. Nothing is standing still. Hence, the importance of crypto agility is rapidly increasing. Currently deployed solutions need to address this change, and near-future deployments should have plans in place to address issues with thought being given to the post-quantum landscape.

NIST will continue work on post quantum-cryptography standardization on FIPS 203, FIPS 204 and FIPS 205 and we'll see further post-quantum cryptography development in libraries and protocols (example).

Blockchain

5

Blockchain technology is the culmination of ideas from and built by thousands of individuals as a collective striving towards a unified goal; transparency and openness. The result is a paradigm shift where there is no middleman; everything is open and visible. While this provides efficiency benefits, it also shifts the general threat landscape contours to the end-user and smart contracts. Any transaction sent cannot easily be undone due to the finality and immutability of the chain. The finality of blockchain based systems, coupled with the absence of intermediaries and middlemen, provides excellent opportunities for hackers. The primary focus of these hackers is smart contracts, with over $3.8 billion lost to hacks in 2022 alone, providing a very tempting target at present. However, this area is starting to mature.

Both governmental, community standards, and regulations are starting to emerge, addressing the need for security and standardisation. Examples of which being the EU's Markets in Crypto-Assets (MiCA) Regulation, and Enterprise Ethereum Alliance (EEA) EthTrust Security Levels Specification. This will result in an eventual maturing of the smart contract space, with less opportunity for exploitation.

The focus will eventually shift to end-users. At present, the Web3 experience and underlying user knowledge is still very poor. This opens users to attacks such as phishing and malware, where we are observing an ever-increasing number of occurrences. To ensure a secure Web3 future, the Web3 experience and user education would need to mature, this will require the collaboration of both blockchain and security professionals to identify risks and educate on a massive scale.

A bumper election year

6

Dubbed as the biggest election year in history, 2024 will see voters in countries representing 41% of the world's population flexing their right to elect leaders next year.

With major elections across the world expected to shape the global order, unease is spreading around the ability to control election dis- and misinformation.

Technological advancements, least of all AI, are effectively 'democratising' the ability to create false content at scale. So, what digital and cyber advancements - and risks - can we anticipate in the year of the election?

As the political campaign trails intensify, could we see a hostile cyber attack on election infrastructure or a successful deepfake on a prominent politician that could move polls or put people in jeopardy – will it ultimately take a hostile cyber attack or a widely disruptive political deepfake to reinvigorate the push for proper safeguarding against dis- and misinformation?

In the case of deepfakes and misinformation, a lot of it goes back to fundamental themes - how are we educating and empowering the public to understand politics and spot disinformation? While we have seen the acceleration of online literacy, online safety has become the poor relation. Will we pay the price for neglecting it?

Criminal gangs continue to evolve

7

The pervasive threat from organised crime groups should still be at the forefront of minds in 2024. We have seen a gradual increase in the activities of Initial Access Brokers, the deployment of info-stealer malware, and of course extortion in the form of Ransomware.

In terms of the latter, we have seen record numbers of victims in 2023, but most notably, we have seen yet again new and novel techniques used by ransomware operators to maximise their gains.

As global government and law enforcements implement new regimes to tackle the threat from ransomware, criminals will continue to evolve and diversify their services. Even if an organisation doesn't perceive a direct threat to ransomware as plausible, they should really be thinking about the potential impact to their supply chain.

Net zero and cyber security

8

The drive towards NetZero is increasingly urgent as countries deal with the impact of climate change and we fall behind targets set for reducing emissions. An important element of this is the move towards creating renewable energy, if we are to continue to support our current lifestyle but still meet these targets. Energy and critical infrastructure have also been a target in recent geo-political conflicts such as Ukraine, with both physical and cyber attacks being used against them. This makes the cyber-physical resilience of infrastructure essential.

To achieve NetZero goals, we need to increase the amount of renewable energy that we use by at least double by 2050. Renewable energy relies on technology and smart grids to match demand to generation. This means connecting physical infrastructure that often has an expected lifespan of 30-40 years to digital industrial control systems. This brings with it modern connectively technology with a shorter lifespan and a larger attack surface.

As we build towards NetZero we need to ensure that cyber security is built in and that the systems are resilient against digital as well as physical interruption.

Finally, yet crucially, there is a fundamental research challenge around energy use in the face of an energy crisis and climate change. There are estimates that 21% of the world's overall energy usage by 2030 will be computing power alone, yet technologies in AI, Cloud and Quantum are inherently power-hungry. We therefore need to be incredibly mindful of, and proactive in the development of secure, power-efficient and sustainable technical solutions for the technologies and systems that we will create and use over the coming decade. This includes considering how the way we use technology for cyber security including threat hunting and generative AI use energy and considering how to do this sustainably.

Closing thoughts

The big cyber security challenges for the next year and beyond relate to ever-evolving technology and threat landscapes, and the need for agility to keep pace in line with these evolutions against the backdrop of a volatile geopolitical landscape. Research has never been more important to help us in our endeavor to achieve security and resilience in these times.

There is also a broader research challenge relating to horizon scanning and knowing how and where to prioritize security advice and guidance on technologies in terms of their likely adoption. Examples we can expect to see in the next 10 years include Brain Computer Interfaces (BCIs), the Metaverse and its associated VR/AR technologies, increased space-based telecoms, neuromorphic computing and synthetic biology to name but a few – understanding the security capabilities and issues with these technologies will require vast amounts of research.

& beyond...