Dec 14, 2020 17:06 GMT

Looking back to look forward: predictions for 2021

With the new year just around the corner, experts from across the cyber security sector are making their predictions for 2021.

This year, following a well-publicised hack on the coronavirus vaccine supply chain, a ransomware attack on a German hospital that was initially linked to a patient's death, and research into security flaws in connected devices that are fast becoming a critical part of our personal and professional lives, cyber security is part of the everyday news agenda and conversation.

With this in mind, we decided to stop and take stock of how legislative

measures and cyber security research have advanced to keep pace with this rapidly evolving landscape.

To start this process, we're looking back at some of our most recent predictions to see how they've progressed, whether our own research is contributing to making the world safer and more secure and how those predictions might develop over the next 12 months.

Prediction 1: Vendors and third-parties prove their worth
Verdict: Accurate

In 2019, we expected that organisations would seek more assurances and risk assessments from their partners and suppliers, driven by continued reports of hackers infiltrating companies through their supply chains. We also predicted that some organisations would try to shift responsibility for post-breach remediation to a third-party.

With nearly 300 cybersecurity incidents impacting supply chain entities last year, the scrutiny on vendors and third parties has only increased in 2020. And, while no organisation has publicly blamed a supplier for a data breach in the last 12 months, heightened regulatory pressure could soon mean that they no longer have the option to.

Last year, lawmakers in New York State mandated that regulated financial institutions must ensure that their third-party providers have appropriate cyber security protections in place. It is likely that other countries, industries and sectors will follow their example in 2021, making it even more crucial for security vendors and other suppliers to evidence their real-world efficacy and value.

Prediction 2: Post-breach fallout causes financial peril
Verdict: To be confirmed

When GDPR was implemented in May 2018, we predicted that the financial consequences of a data breach would be more ruinous than ever before. We even suggested that at least one organisation could be bankrupted due to reputational damage, claims for compensation and a subsequent loss of

earnings associated with an unprecedented fine.

In October 2020, three of the largest fines for breaches of GDPR were imposed by data protection authorities in the EU. The UK's Information Commissioner's Office (ICO) fined British Airways and Marriott International €22m and €20.45m respectively, while H&M received a fine of €35.3m from Germany's Data Protection Authority of Hamburg.

The impact of these fines remains to be seen, but it has not been as ruinous as we predicted. To date, the authorities have been relatively lenient, with the ICO taking an approach that was not entirely revenue-centric: it reduced British Airways and Marriott's fines from £189m and £99m to £20m and £18m, noting the impact of COVID-19 and both companies' reactions to their breaches as mitigating factors.

However, with data protection authorities in the EU increasing their personnel and budgets by 42% and 49% to make use of their stronger regulatory powers, it's likely that organisations will continue to fall victim to large GDPR fines in 2021.

Prediction 3: State-sponsored attacks have public impact
Verdict: Accurate

Following the USA's announcement that it had granted its Defence Department greater authority to penetrate foreign networks in September 2018, we predicted that state-sponsored attacks would become increasingly prominent as other countries scaled up their offensive cyber capabilities.

With Australia's government being targeted by a state hack in June 2020 and the UK and its international allies attributing cyber attacks against organisations conducting research into a vaccine for COVID-19 to Russia in July, offensive nation-state cyber activity is showing no signs of slowing down in 2021.

We also predicted that at least one attack would have a clear, publicly visible impact and could even result in the first loss of life directly attributable to a cyber attack. In September this year, it initially appeared that this prediction

was becoming accurate as German police launched a homicide investigation after a woman died during a ransomware attack on a hospital.

Although the resulting investigation suggested that the attack was not to blame for the death, the attack was not attributed to nation state actors and the risk of a deadly cyber attack remains low, we predict that offensive cyber activity will continue to physically affect us in 2021.

Prediction 4: Hackers get in the driving seat of connected vehicles
Verdict: To be confirmed

Recently, we claimed that the automotive supply chain was not geared up to effectively respond to the modern cyber security threat. We predicted that hackers would expose vulnerabilities in this chain, prompting manufacturers to implement more robust cyber security processes before, during and after a vehicle is rolled out to the public.

Although hackers do not appear to have successfully breached an automotive manufacturer through its supply chain, the transport sector has remained a hot target with attacks on connected cars up 99% since 2018 and Gedia Automotive Group suffering a cyber attack which saw 50GB-worth of sensitive information being advertised for sale. In November, academic researchers were able to hack into a keyfob via Bluetooth and ultimately compromise a vehicle.

Encouragingly, the second part of our prediction is becoming increasingly accurate: in June this year, the UN Economic Commission for Europe (UNECE) adopted new regulations for approving car manufacturers and their vehicle types to ensure that they are protected against cyber attacks, including due diligence on their suppliers. Similarly, maritime industry bodies have published IT security guidelines to help shipping groups to tackle cyber security more effectively.

The new automotive cyber regulations will be mandatory for all new vehicle types from July 2022 and for all new vehicles produced from July 2024, but these measures, combined with the work that manufacturers are already

doing to make connected transport safer and more secure, will see cyber investment increase significantly in transport in 2021.

Prediction 5: IoT security legislation tightens in the public interest
Verdict: Accurate

With more and more people bringing connected devices into their homes and workplaces, we predicted that the security of IoT devices would be more closely regulated than ever before, driven by public pressure for watertight IoT security to be written into legislation.

This year, we have worked with independent UK consumer body, Which?, to identify safety and security issues in popular smart devices including smart doorbells and smart plugs. This research has driven market change in the UK, prompting vendors to rollout fixes and marketplaces to remove affected products.

In the UK, the Department for Digital, Culture, Media and Sport (DCMS) announced new legislation making manufacturers accountable for building robust security standards in from the design stage this year. Meanwhile, the European ETSI Technical Committee on Cybersecurity released a new, globally applicable standard for IoT security in June 2020, while Australia and California and Oregon have also recently brought IoT security laws and frameworks into effect. In March, Singapore announced that it would introduce a Cybersecurity Labelling Scheme for IoT devices.

Meanwhile, The United States of America Senate passed the IoT Cyber Security bill by unanimous consent. The IoT Cybersecurity Improvement Act directs the National Institute of Standards and Technology (NIST) to develop standards and guidelines on how federal government agencies should appropriately use and manage IoT devices connected to information systems. In doing so, the bill directs NIST to develop “minimum information security requirements for managing cybersecurity risks associated with such devices” and further requires NIST to take into account current standards and best practices in the marketplace.

However, as the consumer IoT market continues to grow in complexity and

the attack surface for hackers increases in size, it will be increasingly important for lawmakers to share best practices and collaborate towards a globally recognized standard in 2021 and beyond.

With this in mind, the role of the ioXt Alliance will become even more prominent and important than it already is. The Alliance, of which NCC Group is a member company, aims to build confidence in IoT products through international, harmonised, and standardised security and privacy requirements, product compliance programs, and public transparency of those requirements and programs.

Looking back, it's clear that cyber security standards and legislation have advanced since we last made our predictions. However, as our society continues to become ever more connected, we all need to continue looking forward, to anticipate adversaries' next move and ultimately to make our world safer and more secure.

ENDS

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 15,000 clients worldwide to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience and global footprint, it is best placed to help businesses identify, assess, mitigate and respond to the evolving cyber risks they face.

To support its mission, NCC Group continually invests in research and innovation, and is passionate about developing the next generation of cyber scientists.

With over 1,800 colleagues in 12 countries, NCC Group has a significant market presence in North America, continental Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia and

Singapore.

Contacts

NCC Group Press Office
Press Contact
All media enquires relating to NCC Group plc
press@nccgroup.com
+44 7824 412 405
+44 7976 234 970

NCC Group - Financial Media Enquiries
Press Contact
Maitland AMO
Financial Results Media Enquiries
+44 (0)20 7379 5151

Regional Press Office - North America
Press Contact
NCCGroup@cdc.agency
+1 408 776 1400
+1 408 893 8750