Five Key Cyber Security Trends for 2023 Predicted by CyberQ Group

Five Key Cyber Security Trends for 2023 Predicted by CyberQ Group

CyberQ Group - Predictions

WEST MIDLANDS, ENGLAND, UNITED KINGDOM, January 9, 2023 /EINPresswire.com/ -- Five Key Cyber Security Trends for 2023 Predicted by CyberQ Group

1. Further outsourcing of security operations. This is being driven by several factors including: increasing complexity and sophistication of attacks; further legislation and hence penalties relating to data breaches; internal security operations already over-stretched given budget constraints; and a severe skills shortage of security trained professionals. Companies will desire to focus their internal security skills into more business-critical activities such as DevSecOps, while outsourcing SOC and other routine cybersecurity tasks to dedicated security service providers.

CyberQ Groups position: As a MSSP with a multi-tenanted SOC, we fully embrace this trend. The key benefits are economies of scale enabling competitively priced services, and the application of best practices to ensure clients are compliant while leveraging multiple best of breed technologies.

2. Greater focus on resilience. As many companies are now finding, while prevention is the main objective of security operations, it is best to assume that an attack is “not if, but when”. Therefor, damage limitation, business continuity, and recovery are scoped into all aspects of a companies’ security posture. This encompasses technology, but also people, policies, and processes.

CyberQ Groups position: We find many clients are competently focused on prevention technologies, but do need help with other aspects of the “3P’s” of resilience. MSSP’s need to assist with these ‘softer’ aspects of policy definition, training and cyber essentials.

3. Buying cybersecurity insurance – and will this continue to be an option. Insuring against cyber attacks is tenuous at best. Many Insurers will only insure against professional services' fees following an attack (such as incidence response, forensics, legal fees, and possible fines). Furthermore, these service costs are typically capped in the event of a claim. Insurees are increasingly asking to insure against business continuity – this is a service Insurers are reluctant to offer given the difficulty in quantifying the risk. As cyber insurance is a relatively nascent business, many Insurers are now considering if this business is viable, and how to price the risk. Insurers have for years struggled to qualify if a company has a good or bad risk posture. This will certainly increase premiums and possibly make it harder for companies to obtain insurance.

CyberQ Groups position: Clearly businesses will demand the ability to insure all elements of risk, and hopefully Insurers will recognise and profitably deliver the appropriate products. We do believe it's likely Insurers' will start to demand of their clients' 3rd party professionals audit security to validate risk and help mitigate claims. Think automobile MOT's as a condition of car insurance.

4. Increase in ransomware attacks – but with a difference. The gift that keeps giving. As we saw in 2022, it's so much easier for a bad actor to create a "build once infect many" ransomware. The beauty of this model is efficiency over a targeted brute force attack. It's also possible to 'milk' the victim several times: Firstly, sell a decryptor (even if it doesn't exist). Secondly, extort the victim to prevent leaking/selling extrapolated data (if extracted). Thirdly, further extort the victim to prevent publicising the attack and so creating bad press and external investigations. However, given best practice of multiple back-ups, ransomware with data-destruction capabilities are in vogue so rendering (or at least threatening) to render back-ups useless.

CyberQ Groups position: This is business as usual for MSSP's like us. Prevention is better than cure, and constant vigilance of company assets including back-ups should all be part of an MSSP's service. Assisting with recovery is all part of protection.

5. Blurring cyber and physical security. As cyber resilience focuses so much on people and processes, so cybersecurity increasingly looks at human behaviour (multi-factor authentication as an attack vector for example) and training staff to be security smart. Therefor security now extends to looking at contractors entering buildings, supply chains sharing data (and malware), and OT and IoT devices attached to corporate networks. The war in the Ukraine has exemplified this with Microsoft publicly stating "…more than 40% of the destructive (cyber) attacks were aimed at organizations in critical infrastructure sectors that could have negative second-order effects on the government, military, economy and people…".

CyberQ Groups position: We already offer a Buildings Assurance service which takes into account securing OT and IoT technology. We also partner with companies specialising in providing physical security to assist in exposing vulnerabilities such as MITM attacks and exploits relating to physical access to building and other assets.

About CyberQ Group : Established in 2016, CyberQ Group’s global team of cyber and business professionals have decades of combined experience within the cyber and technology sectors. We are CREST, ISO27001 and GCloud accredited. We believe even the most daunting challenges can be overcome through collaboration, innovative technology and great people.

CyberQ Group - We Make Your Business Cyber Resilience.

The Team
CyberQ Group
email us here
Visit us on social media:
Twitter
LinkedIn
