THE WEAKEST LINK

Paul Ponzeka *outlines the cyber threats and trends that lie ahead in the alternative investment industry*

Cybersecurity is an ever-moving treadmill of change, constantly bringing new trends, threats, technologies and solutions into our daily digital lives. As such, organisations must continually adapt to new threats and changing attack strategies, especially as remote and hybrid working models push businesses beyond the traditional security perimeter. Critical data and applications have moved far beyond the protection of a company's four walls, leaving organisations increasingly vulnerable to potential security breaches.

The expanded attack surface, combined with a rapidly evolving threat landscape, is causing cybersecurity to soar rapidly up the boardroom agenda. This spotlight will shine brightly throughout 2023 and well beyond – in fact, Gartner predicts that at least 50 percent of C-level executives will have performance requirements related to cybersecurity built into their employment contracts as soon as 2026, an imperative that puts further pressure on business leaders to strengthen their organisations' cyber defences.

All the while, today's distributed workforce continues to be both the strongest – and weakest – link in a company's cybersecurity posture. Statistics from the Cybersecurity & Infrastructure Security Agency in the United States reveals that almost half (47 percent) of American adults have had their personal information exposed by cybercriminals. Moreover, as many as one-in-three homes with computers are believed to currently be infected with malicious software, representing a growing threat as the boundaries between home and work life continue to blur, and the sharing of devices becomes more commonplace.

Almost half of American adults have had their personal information exposed by a cybercriminal

For alternative investment firms, it's a warning that any employee could fall victim to a sophisticated cyber-attack. The proposed rules by the Securities and Exchange Commission states firms must consider frequent updates to their cybersecurity tools to address potential threats. It will also demand timely and accurate disclosures of policies, procedures, and any breaches of regulated firms to meet investor requests. The SEC is also continuing to update its regulatory framework to keep pace with technology changes, meaning that non-compliant businesses are rapidly running out of places to hide.

As the landscape continues to evolve, which threats will cause the greatest concern among decision-makers and their teams in 2023? Just as importantly, what steps can they take to mitigate these risks?

As technology evolves, the number of attack targets grow exponentially. So, too, do the number of methods cybercriminals will use to launch attacks on an organisation. While cyber-attacks against large global companies tend to make the headlines, businesses of all sizes are vulnerable to sophisticated cybersecurity threats. In fact, Verizon found that one-in-five breach victims in 2021 were small and medium-sized enterprises (SMEs), with losses averaging $21,659. These attacks on businesses are set to become more frequent, targeted and complex.

Once a small-time malware-based threat, ransomware scams have grown to become a lucrative criminal enterprise and an international concern. The attack on Colonial Pipeline, one of the largest and most vital oil pipelines in the US, is a prime example of the damage that can be inflicted by ransomware. Not only were 100GB of sensitive data stolen in the initial breach, but Colonial Pipeline was forced to pay the hackers to access the decryption key and regain control of its systems. The attack resulted in the pipeline being shut down for several days, affecting consumers and airlines across the East Coast and incurring heavy financial and reputational loss.

2023 won't see the last of ransomware attacks, and targets will range from SMEs to entire countries. Ransomware groups are likely to evolve their tactics and techniques further, making increased use of zero-day vulnerabilities to get initial access to targeted networks.

Social engineering, where cyber attackers manipulate humans into performing actions or divulging confidential information, will also see continued prevalence in 2023. As workforces become more physically disparate, face-to-face interactions between employees have significantly decreased in frequency, creating a heavy reliance on electronic communication. This distance provides criminals with opportunities to socially engineer, preying on employees' cognitive biases and 'benefit of the doubt' to persuade them to hand over sensitive data.

Email is far from the only vector that a bad actor can use to instigate a social engineering attack. Phishing continues to evolve as a sophisticated and ruthless means of attacking a business – and criminals are increasingly leveraging popular cloud-based file-sharing and collaboration services as an initial point of penetration into a network. Spear phishing, which targets a specific person or organisation, and smishing ('SMS phishing) are similarly likely to gain prominence throughout 2023 as attacks become more personalised and human-centric to help convince targets that they're legitimate.

Concerningly, the APWG's Phishing Activity Trends Report found that the financial industry was the sector most likely to be targeted by phishing attacks, with 23.6 percent of all incidents involving such institutions . These social engineering tactics, including phishing, are particularly dangerous because they rely on human error. It, therefore, says a lot that social engineering is one of the most significant security threats facing alternative investment firms today. A single victim can provide enough critical information to trigger a large-scale cyberattack on the wider organisation. And as attacks grow increasingly sophisticated, there is more than ever at stake. It's proof that humans, in many cases, will continue to remain the weak link in the cybersecurity chain.

BUSINESSES OF ALL SIZES ARE VULNERABLE TO SOPHISTICATED CYBERSECURITY THREATS

The tendency for humans to be both the strongest and weakest links in the cybersecurity chain highlights the importance of education in 2023. Despite the increasing sophistication of software and solutions to protect systems, people act as the first line of defence from security threats. Organisations have a responsibility to ensure that their employees know how best to protect themselves and each other. After all, cybercriminals are finding increased success in personalising their tactics – organisations should now do the same by ensuring the human element is woven into their security strategy at every level.

To manage evolving threats in an ever more complex environment, businesses must adopt a proactive approach to cybersecurity. Therefore, continual and multi-layered education programmes incorporating training, phishing tests, tabletop exercises and compliance reporting will grow in importance in the months and years ahead. These programmes will help individuals to mitigate the risk of a cyber-attack by empowering them to make smarter security decisions. It will also prove critical in demonstrating due diligence, thereby reducing liability and giving businesses the best chance of avoiding any additional collateral damage in the event of a breach.

Educational programmes should also be continuous and updated as cyber threats evolve and new employees join the workforce. The right policies and controls also need to be implemented, and a firm's chief information security officer (CISO) can play a key role in enabling this.

Previously, an organisation's CISO largely managed from the shadows, leaning on their technical expertise to provide value. However, as cybersecurity continues to rise up the list of C-suite priorities, 2023 will see more CISOs becoming business enablers and promoting an outcome-driven approach to security. Rather than completing tasks on the ground, they'll take a seat at the boardroom

▶

table to advise on strategic direction. Adapting to the business-critical nature of their role will prove pivotal to the success of the modern CISO.

With cybersecurity now playing a central role in organisations' wider strategic outcomes, cyber policies are being elevated to the status of business policies – not just technology ones. This change is putting the CISO in uncharted territory, as they move from the purely technical and instead begin to master a broader range of skills and knowledge, including business risk management.

> **NON-COMPLIANT BUSINESSES ARE RAPIDLY RUNNING OUT OF PLACES TO HIDE**

As a result, a variety of new and exciting opportunities and challenges await the CISO in 2023. In a number of organisations, CISOs have already evolved into business information security officers (BISOs). The CISO/BISO hybrid has leadership and executive traits, focusing on structuring, delegating, and enabling the digital transformation from the top down.

CISOs must proactively look beyond their technical capabilities and adopt broader skills and knowledge, including relationship-building and business risk management. This will also include the education of employees. CISOs are ideally placed to take on a new position at the forefront of employee awareness and adopt responsibility for upskilling others in the business on the importance of cybersecurity. This education needs to extend all the way up to the C-suite and the executive board, as those at the top must be continually upskilled and incentivised to take an outcome-driven approach to cybersecurity.

The cybersecurity landscape continues to take on new forms. Alternative investment firms must meet evolving financial regulations and ensure compliance with data privacy governance requirements such as GDPR. In addition to protection against threats, there are now regulatory requirements to ensure best practices are in place. Plus, investors will perform sophisticated due diligence checks to ascertain that the cyber strategies of firms are up to scratch.

Organisations are likely to shore up their security posture by following a zero-trust policy and adding endpoint management, which allows IT teams to identify, monitor and control employee access to corporate networks and systems. Artificial intelligence and machine learning can also automate decision-making processes.

The urgency to empower cybersecurity strategies in 2023 is clear. The key is supporting humans where possible by incorporating solutions to assist them in their roles and educating them with multi-layered programmes. Leaders must take the lead in tuition of employees and help protect their organisation from evolving threats ●

Paul Ponzeka is CTO at Abacus Group.

Critical data and applications have moved far beyond the protection of a company's four walls, leaving organisations increasingly vulnerable to security breaches

Picture credit: Andrew Neel