SLAUGHTER AND MAY/

CYBERSECURITY IN 2024

CRISIS MANAGEMENT
Part of the Horizon Scanning series

Rob Sumroy
Partner

Rebecca Cousin
Partner

Richard Jeens
Partner

The global cyber threat landscape will continue to evolve in 2024 alongside rapid technological and geopolitical developments. Potential risks from AI, a renewed focus from ransomware gangs and the difficulties in mitigating supply chain risk are issues that organisations need to manage. We've also seen the emergence of state-aligned actors as a new threat to critical infrastructure. As the risks continue to evolve, so too does the legal and regulatory landscape, with new rules expected to take effect in 2024.

Cyber risk can be mitigated with a well-considered preparedness strategy. While this may not prevent all attacks, it will flag issues to fix and provides a clear guide on how to manage an attack effectively. It is vital that organisations regularly update, and practice, their cyber incident response plans, stress-testing them in simulations, ensuring key stakeholders understand their roles and responsibilities and evolving plans to take into account current risks.

RANSOMWARE

In its latest annual review, the UK's National Cyber Security Centre warns that "Ransomware remains one of the most acute cyber threats facing the UK, and all domestic organisations should take action to protect themselves from this pervasive threat." It is important that your organisation understands how it would respond to a ransomware attack. While governments and regulators warn against payment, there are a range of issues an organisation will need to weigh up before making that decision. The first is, whether it is lawful to pay (and there are circumstances where it is not).

The key to a successful ransom response is therefore having the ability to assess, in real time, the threat facing your organisation. For example, who are the threat actors? Can you do reasonable diligence on their track record, behaviours and the seriousness of their threats? Are they inside your systems and have they copied your data? Are your backups sufficient? How long would it take to recover (whether or not you pay the ransom)? Will they release confidential/sensitive information? And are you covered by insurance?

In the coming year, it will be important for organisation to monitor the changing ransomware landscape as new threat actors, tactics and regulatory requirements emerge.

SUPPLY CHAIN

The recent Capita, MOVEit and Zellis cyber attacks are a reminder of the importance of considering supply chain risk. As companies increase their cyber security, threat actors are increasingly targeting their suppliers, who may be less secure and therefore offer a "weak link" into that organisation's systems. Alternatively, ransomware gangs may target high value (e.g. outsourcing or IT) suppliers who offer access to multiple organisations once breached.

Traditionally supply chain risk has been a blind spot for many organisations. However, recent government research suggests this is starting to change – at least in larger organisations where over half are now reviewing supply chain risk.

That said, effective supply chain management, particularly beyond first tier suppliers, is difficult. It must include new suppliers acquired into your supply chain through M&A, and legacy suppliers who still hold your data, as well as current service providers (and their suppliers).

Legislators and regulators are alive to supply chain risk, and there are plans to bring material IT service providers under both the critical infrastructure (NIS), and financial regulatory, regimes.

FINES

Fines are a reality for cyber breaches and draft guidance from the UK's data regulator suggests high penalties could be more common in future. Duplicate fines are also a risk for cross-border breaches or where different laws apply to the same incident. For example, Equifax was recently fined by the UK financial regulator despite previously receiving a fine for the same incident from the data regulator (the ICO). ICO fines will also be calculated without prejudice to any compensation claims, which again could lead to a double payout.

We are, however, increasingly seeing that proactive remediation and investigation can help reduce the size of fines.

CONCLUSION

Cyber continues to be a board level risk. Throughout 2024, organisations should regularly update and rehearse their cyber incident response plans, and keep pace with the evolving threat, and legal, landscape.

CONTACT US TO FIND OUT MORE

Rob Sumroy
Partner
T +44 (0)20 7090 4032
E rob.sumroy@slaughterandmay.com

Rebecca Cousin
Partner
T +44 (0)20 7090 3049
E rebecca.cousin@slaughterandmay.com

Richard Jeens
Partner
T +44 (0)20 7090 5281
E richard.jeens@slaughterandmay.com

To view the full Horizon Scanning 2024 programme, including our podcast series, please scan the QR code or visit www.slaughterandmay.com/horizonscanning