LOOKING FORWARD

Matt Middleton-Leal *looks to the future as he predicts some of the cyber security challenges for the year ahead*

At this time, it's useful to think ahead about what the coming year may be like. This can get you ahead in reducing risk for the business and communicating around security to executive stakeholders like the CEO and your board of directors. To make this easier, 2024 will be about measuring cyber risk in terms of financial risk to the business, communicating that risk effectively to the C-suite and boardroom, and eliminating the most significant risks expediently.

The past year has been dominated by conversations around artificial intelligence (AI) and automation. Teams of all sizes are struggling to cope with the volume of attacks, as well as the dearth of people with the right skills. According to ISC2, more than 5.5-million people are now employed in cyber security roles, but there are more than 4-million open roles that have to be filled.

On top of this, operational security has come to the forefront of risk management. The US Cybersecurity and Infrastructure Security Agency (CISA) has announced new pilot initiatives to help scale up security around critical infrastructure providers against attacks, while the National Cyber Security Centre (NCSC) has warned of serious and sustained threats to these organisations in the UK too. These services are essential to how society as a whole functions and they are at risk from nation-state threat actors and affiliated groups.

Attacks associated with the Russian state could theoretically be denied coverage by insurance

At the same time, managing risk is more complex than before. Cyber insurance providers have adopted new guidelines around cyber attacks linked to acts of war, which limit pay-outs on attacks that are connected to nation-states. The conflict in Ukraine qualifies as a war, so any attacks associated with the Russian state could theoretically be denied coverage. What is the impact here for security professionals? Planning ahead around risk is more essential than ever, while working with your legal teams on cyber insurance policies will be critical too.

AI AND AUTOMATION IN SECURITY

AI has been the subject of huge amounts of hype during 2023. However, the vast majority of AI projects have not gone beyond initial pilot stages. With so much noise in the market, teams will want to concentrate on specific results that can be achieved, rather than the dizzying heights that were promised. This will help lower expectations around AI and keep the focus on what can be delivered in reality. Over time, AI will move into security operations procedures – for more junior roles, which will help them be productive faster, while more senior roles will be able to handle the volume of potential issues that are thrown at them. However, it will not replace existing staff.

Gartner makes a prediction that lack of talent will be responsible for more than half of significant cyber incidents by 2025. Getting ahead of this and helping teams to be more effective will be a significant goal in 2024, so that prediction by Gartner does not come true. AI will take some of that low-hanging fruit around process improvement and efficiency that teams have not been able to achieve, and help teams to concentrate on where they can have the most impact.

For CISOs, AI and automation projects link into another long-term trend that they want to take advantage of – consolidation. According to research by Gartner, 75 percent of security leaders want to reduce the number of separate tools that their teams have to use as part of their workflows and processes. Currently, companies have a huge number of tools implemented - anywhere from 70 to 90 is the average – and CISOs want to make their operations work more effectively.

While this might provide a benefit around reducing costs, the main goal that security teams want to achieve is greater efficiency. Following on from initial discussions in 2023, 2024 will be the year when more consolidated security projects will move into production. The overall goal for this is how to make security simpler to achieve and to reduce potential risk. Implementing 'one click to rule them all' approaches that consolidate processes into automatic workflows will improve efficiency and reduce the potential window for IT security issues. Areas like remediation will get more automated, freeing up skilled people and allowing them to focus their efforts where they can make the most difference.

JOINING UP OPERATIONAL SECURITY AND IT SECURITY PROCESSES

This consolidation will extend to more than just specific IT issues – companies will take their disparate teams and bring them together. Rather than looking at security challenges as individual issues, companies want to improve their approach to risk and prioritise their work to get the most return on any effort. This involves looking at risk across the whole organisation.

Hackers don't look at IT, cloud or operational technology assets alone. They are looking for initial routes into target organisations, and will take those routes where they exist. Internet-facing applications like remote management software or file sharing tools have been popular with attackers in 2023, and they will remain one of the most high-profile targets in 2024. This will include using specific stolen credentials bought on the black market or taken from other credential thefts, as well as software vulnerabilities that are found in the software products used.

> **THE AVERAGE AMOUNT OF SLEEP THAT IT SECURITY PROFESSIONALS GET IS JUST 5.7 HOURS A NIGHT**

On the operational technology side, more issues are being found in this group of technology assets. These applications and hardware items are often critical to the business, yet may be behind on updates for that very reason. Getting the time to implement updates can be difficult when businesses have to maintain their operations and revenue generating activities, but the risk profile around technology is very different compared with previous years. Today, business leaders are more likely to understand technology risk and accept those changes with appropriate planning.

Operational technology teams and IT security departments will have to collaborate more around risk management. With more hardware assets getting connected to internet-based services and more reliance on data than ever before, both teams will have to understand the risks that they each face and how to respond appropriately. By considering security issues from an overall risk perspective, regardless of where those issues exist within the organisation's operations, teams can ensure that they are all pulling in the same direction.

SECURITY WILL HAVE TO GET OUT INTO THE BUSINESS

The role that security has to play within the organisation will have to evolve as part of these changes around risk management. However, this is not the only reason why this change will take place over the next year. With the rest of the business looking at how to get the most value out of AI as well, data will become more and more essential to delivering for customers.

According to Accenture, AI will support or augment around 40 percent of all working hours. Goldman Sachs has estimated it will add around seven percent to global gross domestic product. This level of value will attract interest from businesses, and that in turn will draw interest from threat actors. Those sets of data will be increasingly valuable assets that hacker groups may try to steal and sell on to the highest bidder, alongside the current approach of using ransomware to extract cash.

Alongside the threat to that data, businesses will create more data and more IT and business operations around that data. In 2024, security teams will be asked to take on more responsibility for these data management tasks. This will make the business more reliant on the security team for how that data gets used.

As an example, our team worked with a manufacturer where the security department had taken on responsibility for the operational technology assets on the network as well. The security department took data from ten robots to check that they were secure. At the same time, the data could be used for operational performance monitoring.

WITH BUSINESSES LOOKING TO GET THE MOST FROM AI, DATA WILL BECOME MORE VITAL

What did the security data show? All ten robots were secure. However, when the department looked a little closer, they could see that one of the robots was suffering from some abnormalities that affected its operational performance. The issue was traced back to some faulty programming in that particular robot. The security and software development departments then collaborated to fix the problem, and it led to an overall improvement in efficiency across the whole manufacturing process. Working with us, the security department had a direct impact on business performance through its responsibility for data.

Every company and each industry will be different around data. Some will make changes quickly, while others may take longer to get there due to regulations. However, this is an opportunity to stop security being perceived as a cost centre. To make this happen in practice, CISOs and their GRC counterparts should get involved in the conversations taking place around data and AI early.

LOOK AFTER YOUR TEAM

It is also important to look after your team. According to Rubrik Zero Labs, more than half of IT security professionals have reported increased stress around their work, while Censornet found that the average amount of sleep IT security professionals get is 5.7 hours rather than the recommended seven to eight.

Your team's health and well-being will be the biggest human issue to take care of. Understanding personal motivations and workloads helps prevent burnout and ensure that each member of the team can fulfil their work effectively. This helps retain staff and keep them focused, rather than looking for new roles. AI and automation can help by keeping the manual and drudgery work to a minimum. By keeping your staff concentrating on where they can deliver the most value, you can improve your retention rates and increase efficiency too.

Whatever your position in the security industry, new technologies like AI will affect the work that you do and how you judge your results. However, it will also improve the overall position of the industry as a whole and ensure that your team can deliver effectively. By consolidating your security strategy across tools, and areas of the business, you can concentrate on providing the best risk management approach for your organisation ●

Matt Middleton-Leal is Managing Director EMEA at Qualys.

More than 5.5-million people are employed in cyber security roles, but there are more than 4-million open roles that have to be filled