What we learned from...

6th CSO/CISO Roundtable

SASIG was honoured to be hosted by Barclays at their London headquarters for the latest in our CISO Roundtable series on Thursday 23 March 2023. Senior cybersecurity and data protection professionals were in attendance and contributed to the forward-thinking and industry-specific conversations that yielded valuable insights. The main themes of the day focused on:

- the evolving threat landscape in cybersecurity;
- the importance of CISOs and their teams;
- the challenges faced by businesses in maintaining cyber resilience;
- the need for sophisticated strategies to mitigate threats;
- the retention of skilled CISOs and the technical teams; and
- the threat posed by a conscious and unconscious insider in the context of hybrid working.

These topics were all identified as the key challenges for our CISOs in the current cybersecurity landscape.

Operation Stronghold: How one CISO made cybersecurity their company's number one priority

The changing threat landscape in cybersecurity requires organisations to prioritise their readiness for an attack. Our case study looked at how a geopolitical threat affected one company, emphasising the importance of continuous risk assessment and decision-making within the cybersecurity function. CISOs should know their **critical services**, **gaps**, and **control failures** and be able to take proactive, reactive, and predictive measures to control their environments.

It is imperative for CISOs to build a good relationship with their board: In our case study, it allowed the CISO to convince their board to prioritise cybersecurity and implement an **IT-change freeze**, dedicating all IT staff globally to cybersecurity remediation for three days. This exercise led to the board instructing the cybersecurity team to run a similar exercise every six months ("Operation Stronghold"). This consists of reviewing access control, DevSecOps, and vulnerability management, to control the company's environment proactively and predictively.

Continuing the security momentum gained during the pandemic

The Covid pandemic saw a revolution in how we work, through remote working and communication. This posed numerous challenges for the technology sector and security community, which sometimes resulted in **relaxed security practices to enable the speed of change** that was required at that time. There is a need to maintain a **balance** of tight security measures against reasonable working practices for the workforce. In pursuit of this, we considered independent oversight in a company's technological development and its expanding change control.

The panel also discussed challenges in incorporating and keeping up with the pace of digitalisation and the need for leadership to adapt to an ever-changing landscape and give people the **freedom to work in ways that suit them best**. Finally, there was also a discussion about how to look after people who are not in the office, a problem faced not just by security, but by industry at large.

Other challenges the security profession needs to address include its reputation within the company, understanding the organisation's data flows and vulnerabilities, as well as ensuring that it is sufficiently funded so that it can invest in new technologies to protect the wider organisation.

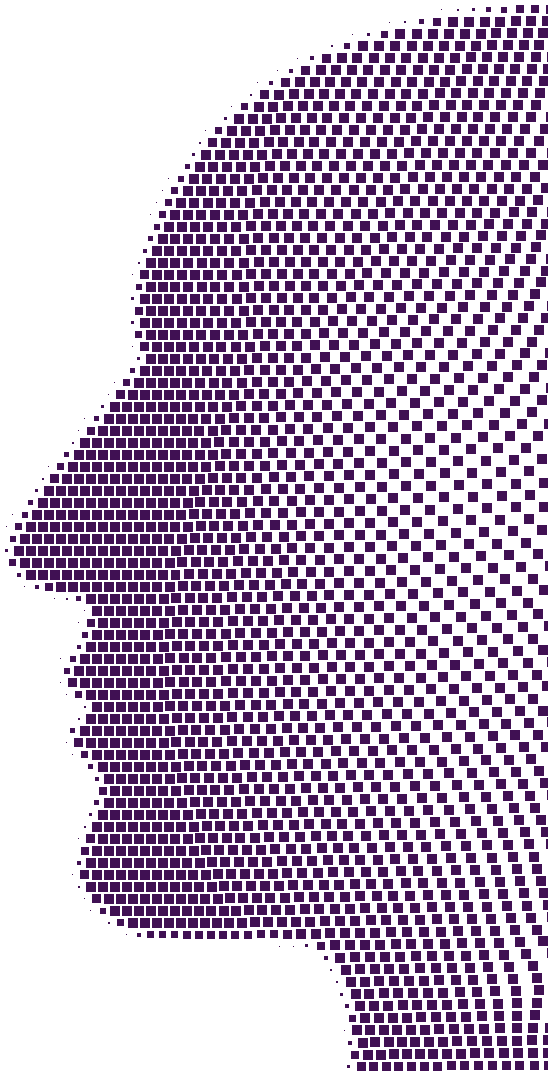
How do organisations adopt converged security? An evidence-based roadmap

We looked at PhD research that focused on how organisations **adopt convergence** and make decisions to move towards it. Convergence integrates different security resources within an organisation to provide a more holistic view of security, which is important due to the increasing threat of cyber-physical systems being targeted by **hostile actors**. The studies identified several interconnected factors that support convergence within an organisation. These included challenges and considerations such as **timing** and ensuring that **security goals** align with **broader business objectives**.

A roadmap was proposed to help organisations navigate the decision-making process when moving towards convergence. A converged approach requires more than just reorganising personnel; it also needs **effective collaboration** between different security resources.

Mental health, stress and burnout

We looked at the mental health of the overburdened cybersecurity industry, and the importance of paying attention to one's well-being and observing the signs of burnout. There was consensus by the panellists that going through their respective journeys of mental health allowed them to appreciate their mental health - and that of others - more. The pandemic has brought about an **increased awareness** of mental health and allowed general discussion around this to open up. It has also highlighted how the **pressure to be seen as a leader** is a significant factor in burnout, increasingly so, the more senior within an organisation you are.



There was discussion on the importance of **checking in on colleagues** and creating a **culture** where staff feel comfortable speaking up and asking for help. Sleep deprivation through stress can cause further serious issues that need to be addressed, and it's crucial to pay attention to physical and mental well-being. The panel also touched on the importance of leadership training and that people management may not be within everybody's skill set. It is important to test out **support systems** for employees to ensure they are easily accessible.

Perspectives on the insider threat

It is important for managers to **understand human behaviour** and take on the responsibility of securing corporate information within the workplace environment, commencing right from the recruitment of a new member of staff.

Leaders should look to create **supportive environments** that promote open **communication**, being mindful of the pressure employees face in their work roles. **Toxic leadership** can discourage staff to speak up when they identify insider risks and threats through incorrect or unsafe working practices.

It is invaluable for organisations to conduct **incident reviews** and be able to learn from past experiences. The board has a crucial role in setting the culture of their organisation and understanding why an event has occurred, and what can be learnt from it. However, overly complicated rules and processes can burden a workforce, so a relaxed approach that uses tools to identify high-risk behaviours is recommended.

A wider view on industry approaches to phishing simulations

The final presentation covered the importance of educating employees about phishing and cyber threats. **Technical defences are not enough** to prevent cyber-attacks alone, with 80-90% of attacks starting off with a phishing incident. Phishing simulations can be a useful tool for improving education and awareness, although there is no clear evidence of their effectiveness. Nonetheless, there is a need for **continuous staff learning** and improvement to stay ahead of the ever-evolving cyber threats that present themselves.

It is important that the whole workforce, including top-level executives, participate in any simulation exercises, and **know how to report** any phishing emails that they receive. The session concluded with tips on encouraging reporting, such as using **incentives** and **awards** for employees to report suspicious activity.

Data from these exercises can be used to identify areas for improvement and target education campaigns, but a 'click rate' from such an exercise is not a meaningful metric in itself.

Register for our upcoming events at thesasig.com/events

With thanks to our Supporters