SECURE IMPACT

THE CISO ROUNDTABLE REPORT

Bridging the gap between security and business

www.secure-impact.com

Bridging the gap between security and business

We were delighted to host our first CISO roundtable event this month, where we welcomed a group of some of the UK's leading cyber security executives to discuss the most pressing challenges they face today.

Chaired by James Lyne, the discussion itself was open, honest and rich, and replaying all of the insights would be impossible. However, this report serves as a prompt on a few of the themes the room considered important, with additional key actions for CISOs to not only address similar challenges but drive toward real business improvement.

"As security leaders, engagement with the business, communication, and a relentless approach to self-reflection on our measurements, investments and team capabilities is key to success. I was delighted to see sharing between the leaders in the room, and the potential for cross functional legal, technical, security and leadership teams to better manage security is vast. My biggest take away is there are parts of the industry where security has become a race to the bottom, not a strategic partner or roadmap to improvement, and that is something I want to focus on in 2022." James Lyne

James Lyne
Founder

Giorgia Cacace
General Manager

If you would like to discuss these takeaway actions in more detail, or are interested in attending a future roundtable event, please contact Giorgia Cacace directly at gcacace@secure-impact.com

CISO Roundtable themes

1 **Theme 1:** How to win friends and influence people

2 **Theme 2:** Speak the C-suite language with metrics that matter

3 **Theme 3:** The inconsequential endeavour of penetration testing

4 **Theme 4:** The best version of an ICO investigation

Theme 1: How to win friends and influence people

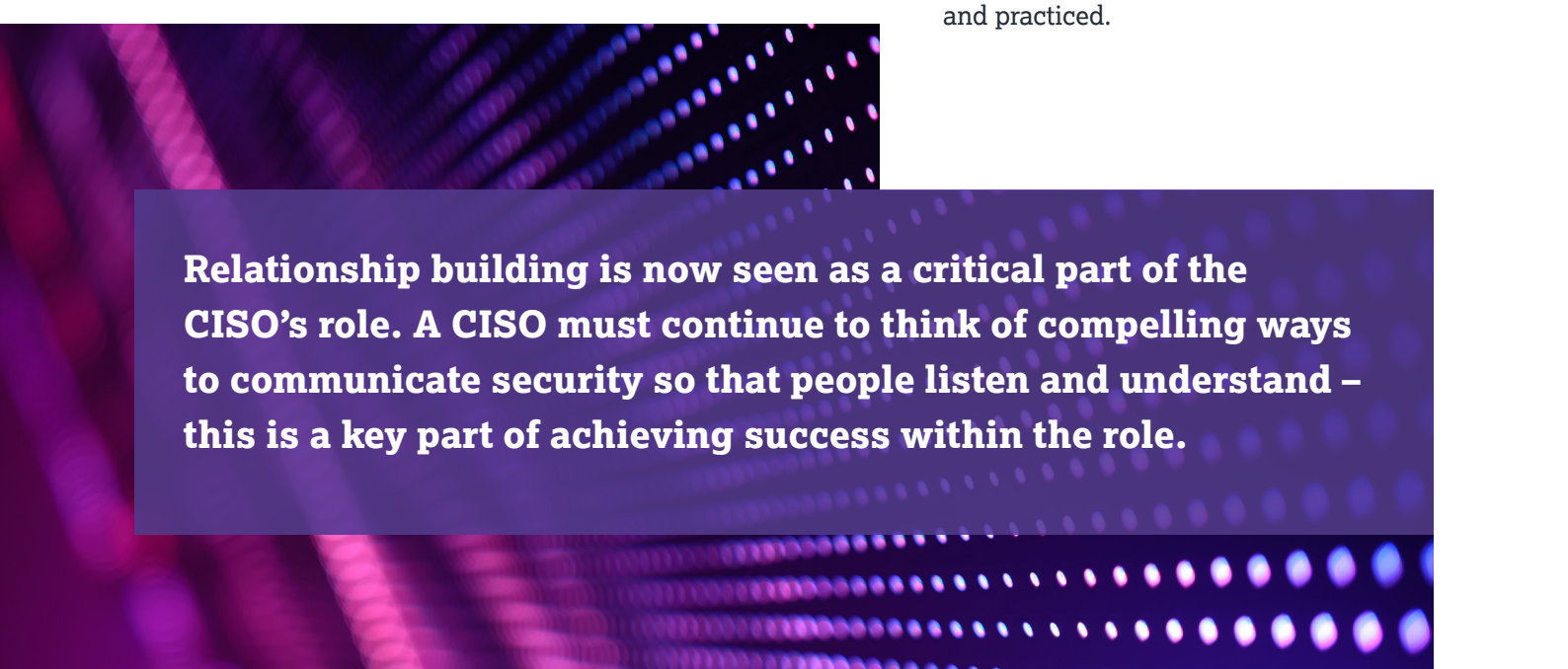
A recurring challenge for the group, regardless of sector, is how to build buy-in internally.

At its most basic level, CISOs report that their function and team are seen to 'stop bad things happening', resulting in the common misconception that CISOs say 'no', rather than adding any positive value.

Contributing factors to this misconception include organisational structure and behaviour, such as the prevalence of silos, which inhibit effective communication, in turn limiting awareness of the purpose of and indeed achievements of the security function. As suggested by a CISO from a well-known financial services company, it is therefore now a critical part of the CISO role to re-frame this perception and promote security as a business enabler.

This is easier said than done, however, as culture change is a continual war of attrition. It cannot be achieved through one internal marketing campaign, and instead must take a multi-pronged approach:

- **Align the security function with other departments and create internal allies** – use similar goals and issues these other internal teams face to build alignment and cohesion between security and the rest of the company, for example meeting regulatory requirements or improving efficiencies. By building up strong relationships across legal, IT, operations, and senior leadership, your company's internal security practices will improve, and these relationships will also prove invaluable if an incident does occur. Businesses that respond best to an incident already have a clear plan in place, with key responsibilities and processes identified, communicated, and practiced.



Relationship building is now seen as a critical part of the CISO's role. A CISO must continue to think of compelling ways to communicate security so that people listen and understand – this is a key part of achieving success within the role.

- **Sharing good news stories** – security teams do great work, however often they fail to share their success stories with leadership or the wider business. It is important to communicate during the good, not just during the bad, and highlight the positive achievements of your team.
- **Security awareness and education** – to meaningfully improve a company's security posture, a CISO needs to champion education to create buy-in to the value security practices bring, as well as the consequences of not doing it. Taking this further, security can be positioned as an enabler: an app that is created to enable business growth would not exist without security. Hybrid working is only enabled as a result of security processes. It is important to push the message relentlessly – security does not just mean saying no to things.

Relationship building is now seen as a critical part of the CISO's role. A CISO must continue to think of compelling ways to communicate security so that people listen and understand – this is a key part of achieving success within the role.

Key takeaway actions

1 To build up good news stories and advocate your team, create your version of a 'Security Newsletter' to market your excellent work. Have a 'good things' pack ready – both an internal and external version.

2 Organise tabletop exercises to build up allies, create alignment between functions, and raise awareness with departmental decision makers.

3 Continually reframe the message. Sell security as a positive business enabler and be relentless with this messaging.

Theme 2: Speak the C-suite language with metrics that matter

How do you report to your board, and are you focusing on the right metrics?

The CISO discussion surfaced certain reporting strategies which can pivot focus to metrics which show genuine insight to the company's security posture, demonstrating what the function is achieving, the value they are adding to the business, as well as drilling down to areas requiring significant improvement and likely budget.

Selecting the correct metrics is key to portraying this effectively and capturing attention and buy-in. Some KPIs can be lost in the noise to a board and become just another risk rating. A metric displaying vulnerability month by month for example, can become an arbitrary measurement, as it is not a true indicator of why or how this will affect the business. Several examples of metrics that have proved to be successful in achieving this goal are:

- Penetration test findings across server and desktop, benchmarked against industry standards and highlighting the business's relative position against competitors.
- Percentage of estate that has been penetration tested to express the continuous efforts to risk assess the surface area – and this is a metric itself, not just an outcome.

At Secure Impact we have done extensive review projects with CISOs to help them objectively reflect on the metrics and their comparison to other companies, which can strengthen their executive reporting. It is common for security teams to pick 'unwinnable' metrics, such as patch deployment, which will always, even when great, hover at a high but not complete percentage. It is easy to focus solely on the areas of failure, as security teams are trained to always be thinking about gaps or vulnerabilities, however it is equally important to be vocal about your successes and what has worked well.

Speaking the C-suite language can help bypass a CISO's innate frustration of lacking security understanding, and home in on positioning requirement and achievement in metrics that resonate. Furthermore, these metrics and other data have multiple benefits, including a trail to be shared with insurers and regulators, particularly if an incident does occur, as well as KPIs for your internal team and informing goals or expectations with other departments.

Key takeaway actions

1. Assess your current reporting framework and be honest with yourself about whether your metrics are truly driving business improvement. Consider implementing alternative metrics that may help your board to understand in clearer terms the impact that the security function is having within the business. It can also help to measure against market standards in this respect too.

2. Consider the use of the MITRE ATT&CK framework. It maps out adversary tactics and approaches, and can be used as a standard to roadmap security changes based on your threat model. Both blue and red teams can coordinate around attacker scenarios.

Speaking the C-suite language can help bypass a CISO's innate frustration of lacking security understanding, and home in on positioning requirement and achievement in metrics that resonate.

Theme 3: The inconsequential endeavour of penetration testing

A clear theme that emerged was CISOs' demand for security services that actually drive commercial value and business improvements, and there is a clear level of frustration within the industry at the lack of commercial advice that many penetration testing suppliers provide.

Endemic to the cyber security industry is the positioning of tick box exercises in place of services which genuinely improve a business's security longevity, with the CISOs reporting the near redundancy of today's generic penetration test service. For the attendees, the penetration test has become the same report year on year without clear road mapping for practical change nor tailoring of outcomes and priorities to make it a truly valuable exercise.

Penetration tests are not intended to be a complete analysis of a business, but more a sample or a snapshot in time. And aligning near perfectly to Secure Impact's own value proposition and raison d'etre, penetration testing should be aligned with your business goals and provide clear commercial value.

Additionally, when reporting a breach to a regulator, your previous penetration report can be used as due diligence, framing you as a victim of a breach rather than negligent, and proving that you have been taking steps to improve your security posture. A regulator will consider reasonability in each case – what more could you have reasonably done to prevent a breach from happening?

Key takeaway actions

1. Use purple team approaches that make each engagement a training opportunity for the team. Let them adapt and learn each time and make each other better. Initial purple teamwork can be hard for teams without a spirit guide, so consider a practiced outsider to assist.

2. Testing should be an ongoing continuous process, rather than simply one test conducted a year.

Theme 4: The best version of an ICO investigation

As part of the conversation, questions were raised around best practice when interacting with the Information Commissioner's Office (ICO).

It is common to be uncertain as to how to manage your relationship with the ICO, and it is important to remember that they are a regulator and can take enforcement action. Think strategically ahead of your conversations, and whilst you should acknowledge and take full ownership of your issues, it is not necessary to provide a full incident report. Demonstrate the lessons you have learnt and the steps you are taking to develop your security maturity.

Security assessments don't have to be 'terrifying paperwork in the drawer'. An engagement report will never be able to provide a business with a perfect score of 100%, and instead should focus on a list of items they are doing well, and a further list of items that could be improved to manage risk even further. Language in engagement reports are often built around catching companies out, instead of focusing on opportunities to improve and validation of the good.

In addition, businesses can deliver reports under privilege if a more careful approach is taken. The right legal setup and engagement style is crucial to success on discoverability and legal utility of such documents.

During the COVID-19 pandemic there was a grace period, where the regulator would be more lenient on companies who had an incident as a result of remote working. This period is now over, and companies are expected to have policies in place to look at issues such as privacy, confidential data, and other challenges associated with remote working.

Key takeaway actions

1. As part of your incident response plan, have a clear process in place for contacting the relevant regulatory bodies.
2. As well as practicing your incident response plan internally, consider sending your security playbook to be reviewed by your legal team.

Think strategically ahead of your conversations, and whilst you should acknowledge and take full ownership of your issues, it is not necessary to provide a full incident report.

Final comments

It was a pleasure to discuss these themes with experts in the industry, and we hope that the key takeaways provide you with some valuable practical steps. If you are interested to learn more about our approach to purple teaming, you can download our 'CISO's guide to purple teaming' e-book, for information about strategy, process and top tips.

If you would like to discuss these takeaway actions in more detail, or are interested in attending a future roundtable event, please contact Giorgia Cacace directly at gcacace@secure-impact.com.

SECURE IMPACT

Your security team.

Your security team.

With superior technical expertise and a business-oriented approach, we offer cyber security services which drive positive commercial impact for organisations, and shared learning outcomes for your team. Our experts are GIAC certified with specialist risk modelling expertise. We can help you develop the right level of cyber security capability to meaningfully improve your posture, and enable business objectives.

We offer offensive services such as penetration testing and purple teaming, and defensive such as digital forensics, and incident response.

Secure Impact Ltd.
The Old Bull Pens, Sezincote, Moreton-In-Marsh, Gloucestershire, GL56 9AW

Want to discuss how we can help your business? Contact us to learn more.

hello@secure-impact.com | +44 (0)20 45514730

www.secure-impact.com

SM22-647