SECURE IMPACT

7 strategies to effectively communicate cyber risk to the board.

> "Communicating cyber risk is hard to do well and it's really easy to burn credibility with the board. The skills required to manage and communicate risk, to work with stakeholders and have that seat at the table, are different to traditional technical leadership skills. It is however one of the crucial practices that defines today's security leadership, and the stakes have never been higher, so it's critical that we get it right."
> **James Lyne**

1 Have a 'board muse'.

- A common mistake in reporting cyber risk is either chronic oversharing or under sharing. You need to prioritise aggressively to what really matters when communicating with stakeholders.
- Identify someone else in your organisation who also has to regularly share with the board (finance is often good!) and ask them to be your sounding board to validate messaging and to ensure clarity.

2 Consider using a cyber risk model.

- Translating cyber risk is 50% art, 50% science, but using a cyber risk model can be a helpful place to start (and to ensure you aren't being too creative!) Models & frameworks can often come with overheads and extra paperwork, but the benefit is that it does let you standardise your practice.
- We've included several examples below, although this is certainly not an exhaustive list. If there are any that you've found useful, please do let us know!

3 Context is critical.

- Putting cyber risk into context for the board is key. Risk needs to be framed as a constantly evolving, moving beast, with the landscape changing from one month to the next.
- The role of the security team is to be cognisant of how the landscape is moving, generally and specifically within your sector, as attackers are always trying to counteract what you have in place. It's important that the board understands the need for flexibility, and that priorities and plans might need to be changed.

www.secure-impact.com

4 Build buy-in and keep it simple.

- With a non-technical audience, there should be a process of ongoing education, helping stakeholders to really understand the threat landscape. For example, you could walk the board through what a basic ransomware attack looks like, or run an executive tabletop or cyber drill exercise.
- Demonstrating in a clear, practical way can help the board to understand how security affects the business, building buy-in and giving a more holistic view around brand and revenue protection.

5 Speak the language of the board.

In order to tailor your messaging effectively, get to know each individual stakeholder. How do they talk about risk? Do all of the board understand cyber risk? How can you as a CISO help them to achieve their strategic goals and objectives? This will help you to report on cyber risk in a targeted way, using language that resonates.

> "There's a huge challenge because different businesses talk about risk in different ways. From industry to industry, the board will have different levels of understanding when it comes to risk, so as a CISO your aim has to be to understand the business and to build strong relationships with the board so that you can talk in their language." **Lee Whatford**

6 You can't measure risk if you don't know your scope.

To truly understand risk within the context of your organisation you need to know the lay of the land, the wider scope of the business as well as asset discovery. This exercise should be done regularly so that you can continue to re-evaluate as part of the risk management process, and to allow the board to effectively prioritise.

7 Practice!

A simple but effective top tip! Choose one stakeholder and organise a practice run so that you can test and validate before presenting to the whole board. Although this may seem obvious, security leaders often send risk reports straight to stakeholders, without testing that it makes sense to the audience first.

A selection of cyber risk models & frameworks

- NIST SP 800-30 framework
- Factor Analysis of Information Risk (FAIR) Model for Cyber Risk Quantification
- ISO 27005
- COSO ERM
- ISF methods for risk assessment /management

If you have any comments on this webinar, or resources to add to our list, please let us know.

If you need an external sounding board to help with implementing any of these strategies, please do get in touch. We regularly hold tabletops and executive leadership workshops to help security teams to build stronger stakeholder relationships and to improve organisational cyber maturity.

> "We all know that you can never be 100% secure because the risk landscape is constantly changing. You therefore need to understand where your crown jewels are and how they could be targeted, as well as focusing on your overall security posture, so that you can keep evolving and moving forward."
> **Sarah Armstrong-Smith**

THE PANEL

James Lyne
Founder
at Secure Impact

Sarah Armstrong-Smith
Chief Security Advisor
at Microsoft

Lee Whatford
Previously CISO at Domino's
& Director of Cyber Security
at Royal Mail

Giorgia Cacace
General Manager
at Secure Impact