Engaging with Boards to improve the management of cyber security risk

How to communicate more effectively with board members to improve cyber security decision making.

Cyber security is a critical risk for boards and executive teams. Cyber security leaders (such as CISOs) play a crucial role in describing and mitigating the risks. This guidance helps those leaders to communicate effectively with Boards, and to better engage with their members.

Introduction: why engaging with Boards matters

Communicating with Boards and senior executives about cyber security can feel daunting, with the scrutiny this entails.

It's important to remember that Boards ultimately want you to be successful in defending the organisation against cyber security threats. When the Board is behind your efforts, cyber security can be recognised as a positive thing that helps your organisation's digital activity to flourish, and not just seen as a necessary evil or cost-centre.

Most Board members do **not** have in-depth cyber security knowledge. That's not their role. Cyber security leaders, on the other hand, **do** have detailed knowledge of the domain, but maybe less experience in communicating with Board or senior executive teams. As a cyber professional, it is part of your job to bridge this gap to provide better cyber security outcomes.

Cyber security is a *strategic* issue, which means you must engage with Boards on *their* terms and in *their* language to ensure the cyber risk is understood, managed and mitigated. This guidance describes how to communicate and engage more effectively with board members, to improve cyber security decision making within your organisation. It will also help you to communicate with senior executives, who make recommendations to the Board and are responsible for executing the strategy. Executives will take most of the decisions

relating to cyber security and will be answerable to the Board for those decisions. Your CEO and CFO will likely be board members too.

> **Note:**
> This guidance does not aim to increase cyber security *understanding* amongst board members. The NCSC has produced separate guidance designed to help Boards 'get a grip on cyber', and includes briefings, guidance and training material directed at non-technical decision makers.

Understanding your audience

As an enthusiastic and knowledgeable subject matter expert, you will probably have a tendency to want to tell, share and provide substantial updates on all your activities. In doing so, it's easy to forget to calibrate your output for your audience. 'Cyber' is 99% your day job. For Boards, this topic will be competing for space on an agenda already packed with dozens of other topics. It is therefore essential that you understand this broader Board agenda, the corporate strategy and goals, and the challenges the business faces.

You won't have (and don't need) access to **all** the details; just reminding yourself of the top-down position, and asking questions if you need to, will help you talk about cyber in a relevant way that is connected to the strategic agenda. As with any audience, investing time in understanding what is important to the Board, their context and how they work will make you a more effective communicator.

Understand how ALL Boards work

This guidance focuses on engagement with **Boards**, the formal corporate group who are responsible for:

- the long-term strategy of the organisation in the interests of stakeholders-at-large
- the governance of the execution of that strategy and management of risks associated with it

It is a common misconception that Boards make all the decisions; most will be made by the executive management team, with the Board concerning itself with the governance and oversight of those decisions and recommendations. The NCSC has produced a useful summary of cyber security regulations and directors duties in the UK, which you should familiarise yourself with so you can better understand the Board's obligations.

The role of cyber security professionals here is:

1. To ensure the cyber security implications of strategic decisions are understood by decision makers.
2. To ensure that risks to delivering the organisation's strategy are identified, evaluated, and mitigated in line with the business risk appetite. This includes ensuring that the business has adequate cyber resilience to prevent, detect and respond to cyber attacks.

The latter is most naturally where the conversation will start. To contribute to the former you will need to build trust in your knowledge and ability to deliver, and have demonstrated that you can contribute positively to the strategic discussions.

Boards are responsible for overseeing a broad range of issues in their governance roles. Time allocated to even the most important subjects can often look very limited and dismissive of the importance of the subject. Respecting the preciousness of Board time is key to 'operating at Board level'.

> **Note:**
> The Financial Reporting Council - UK Corporate Governance Code gives a more detailed view of the role of a Board (and its members).

Understand how YOUR Board works (and who is on it)

We tend to think of 'The Board' as a single entity, but it is of course made up of individual humans just like any other group, each with their own knowledge, skills, styles and preferences.

As well as **who** is on the Board, it's important to understand the mechanisms and practicalities of **how** your Board operates. How often do they meet? What format

do the meetings take? What committees are there? Find out who manages the Board in your organisation. Larger companies will have a Company Secretary team who will be able to support you. Responsibility sometimes falls to a Chief of Staff role. In particular, seek advice on their 'ways of working', such as how they like sessions to work, and what style of papers and presentations work best. Read what Board output might be available to you.

Cyber is a risk - talk about it as such

Boards understand risk. Many Boards will have a Risk Committee possibly combined with other functions such as Audit, Governance or Compliance.

Whilst cyber risks may be notably different from other risks (the adversarial nature, the potential for catastrophic impact, their often very technical nature - and more generally how 'new' cyber risk is), it is helpful to align it with the framework and language of risk the Board are already familiar with. It allows you to locate 'cyber' in what should be familiar territory for board members. Your role is to help them understand how the cyber risks manifest as business risks, their potential impact and what you (with their support) will do to avoid or mitigate them.

In practice this means decomposing the threat landscape into clearly stated risks, in natural language, then grading the likelihood and impact of those risks.

Where possible, quantify and make the risks tangible, using precise language. You should reserve 'doomsday scenario' language and hyperbole for risks that really really warrant it. Equally Boards expect honest, matter-of-fact assessments of risks and your current position. Trying to gloss-over the risk (or overstate the mitigation) is not helpful.

Recent research commissioned by the NCSC revealed that 80% of Boards do not realise that the accountability for cyber risk rests with them, even when cyber aspects are outsourced. Remember, it's your job to advise; you can't set the appetite for risk. That has to be done by the Board.

Engage outside of Board meetings

Board meetings aren't the best place for you to ask questions, or to have in-depth discussions. 'Cyber' is more likely to be allocated a 15-minute session,

rather than a two-hour workshop. It is much easier to have longer discussions between individuals and smaller groups. You may also find Board members are more comfortable asking questions about things they are unsure about in these smaller groups, something that's hard for anyone to do in a formal setting.

You'll soon be able to identify the individuals on the Board who have a particular interest or knowledge of your area, so try and develop regular communication with them outside the regular Board agenda. Work with your executive management to achieve this.

High-profile incidents present an opportunity to inform, update and advise. When cyber hits the news, which it frequently does, use the story to put a short briefing together for executive teams and Boards. This should cover the potential impact on your organisation, the steps you're taking to protect against similar incidents, and anything within your organisation that might heighten the risk or block progress in mitigating it. It may not be appropriate for you to send this *directly* to the Board, but share these thoughts with executives for them to share, if they see fit.

Answer the most important questions first

Make sure that you understand what is most important from the Board's perspective. This might include:

- What are the key risks and mitigation plans that you need to show progress against?
- What are the KPIs and metrics that are most relevant to your organisation?
- What impacts are your Board most worried about? Downtime? Client impact? Regulation?
- What are the critical questions the Board wants answering?
- What operational data can you surface to show activity and the benefits being achieved by investments made?

A 'one-page' summary dashboard maybe called for here. Your organisation or Board meetings may have a preferred format and approach to routine reporting which you should work with.

Expect to be asked about the big picture

Part of Board's role in governance and oversight is to make sure experts don't get lost in the weeds at the expense of the bigger picture. One way Board members will do this is by 'stepping back' and asking broad questions. Questions you can expect to be asked may include:

- *Do we understand the cyber security threat, and how it might impact our business strategy and plans?*
- *How do we benchmark against other organisations? Our peers? Our sector?*
- *How do we consider cyber security implications when we take decisions?*
- *Have the critical assets for protecting our key business objectives been identified?*
- *Are we managing the risks in an effective way?*
- *Are we executing against the mitigation actions?*
- *Are responsibilities clear?*
- *Are we working with our supply chains and customers on this?*
- *Do we have incident and contingency plans in place? Have they been tested?*

The NCSC's 'Cyber security 101' for board members (PDF) gives insights into the types of questions Boards should and might reasonably be asking. Note that these aren't **technical questions**; these are **governance & assurance questions** that Board members will feel comfortable asking, and to test the answers to.

Engaging strategically

As the authority for cyber security in your organisation, you must elevate your conversations with board members and other senior decision makers so that they connect 'cyber' with the overall business challenges and context. You need to connect what you want to tell the Board with what is most important to them (and therefore what they are interested in hearing about).

Presenting to senior business leaders – with all their necessary challenges and push-back – can feel daunting. By taking the time to elevate the discussion to the strategic level, to understand your Board audience and to communicate clearly, you have a greater chance of winning their confidence and support.

Being able to engage Board members and executives is a fundamental aspect of your role which grows the cyber capability within your organisation, and develops your own skills as a communicator. More pressingly, if you fail to engage *strategically*, then you are less likely to receive the investment and resources needed to mitigate the increasingly complex and sophisticated threat landscape.

Own the problem

If you find yourself thinking '*I've explained it three times and they still don't get it!*', then ask yourself how you can change your approach so that:

- the executive and governance of your organisation are engaged
- you feel confident that the risks you've outlined are understood
- your work plan is summarised well and it is clear that progress is being made

The crucial first step is to recognise that - rightly or wrongly - this is **your** problem to solve. You will need to work with the audience as you find them, which may not be the audience you'd perhaps wish you had.

Provide a holistic view

Cyber security. IT Infrastructure. Infosec. Online fraud. A specialist might understand why fraud, data theft and malicious attacks are treated as discrete topics, but from a Board's perspective, these distinctions will often seem academic.

It's not the Board's problem to understand the minutiae, or how the different facets of cyber security, which maybe 'owned' by different parts of the organisation, fit together. They need to be confident that everything is being addressed through a cohesive approach, and there are no gaps in your mitigation plan.

Be clear on the definition and components of what cyber security means in your organisation, and be clear about who owns which parts. Work with your colleagues to provide the holistic view a Board needs.

Advise rather than educate

Board members rely on advice from experts - like you - to discharge their governance responsibilities. It's **not** your role to train them to do your job, but instead to put them in a position where they can make informed decisions about corporate strategy and cyber risks. Boards do this all the time with different type of risk, such as financial risk, and one of the Boards functions is to approve statutory financial accounts. They can do this without understanding the intricacies of the local accounting and tax rules their organisations operate in. Instead Boards rely on their financial teams, and take advice from accountants and specialists to do so.

Ultimately it is Boards and executives who are accountable for risk decisions about cyber security. In some industry sectors they may have specific regulatory obligations. It is your responsibility to put them in a position so the Board - with advice from you - can make those decisions.

Be open to external scrutiny

Finance teams expect to be audited.

Health and Safety teams expect to be inspected.

Cyber security functions should expect the same, especially over critical matters or significant investments. It can feel uncomfortable when people question our work, but Boards will naturally seek independent assurance from external specialists on critical matters. Back up your assertions and facts from trusted and approved third parties (such as the NCSC website and the Cyber Security Toolkit for Boards).

Communicating clearly

Whether you're presenting or writing, the Board may well be interested in what you have to say, but the *way in which you convey* it will either encourage them to take note, or to stop listening. This section contains some tips that can help you refine your messaging.

To get busy boards to engage with cyber, you'll need to communicate in a language that resonates with their business mindset, and share updates concisely, using a business-focused approach (with minimal technical detail) for maximum impact.

Pick a model and stick with it

Using a consistent structure across your communications (which you can use over and over again) is very helpful when dealing with an audience who engages with the topic infrequently. It's helpful to give your audience a way of thinking about something; it's less helpful to be given two ways to think about it. It's even more unhelpful if you get a new one every time you address the Board.

If you are new to the organisation, take time to understand how they work, and their existing content and practices. Obviously, this will vary with each organisation. Some organisations will have standardised reporting structures for risks and investment programmes, others may have a suite of dashboards and KPIs in place, or a mixture of these. Whatever is used, make it work for you, don't work against it.

You'll also need a simple way to report what you have been doing. If you are using a formal cyber framework, then the headings from there might be useful (taking care to avoid the complexities of the frameworks), or use the NCSC's 10 Steps to Cyber Security. Or make your own.

Keep it simple

Perhaps the most frequent complaint from Boards is that cyber experts use technical language and jargon when describing unfamiliar topics. Given this, it's no surprise that many board members struggle to unpick and engage with cyber security. Whilst the appropriate level and language to communicate will depend on the organisation, **natural language that's free from jargon and acronyms is the order of the day**. Simple descriptions will always work better.

This challenge is heightened by Boards who are required to switch context between multiple subjects while reading Board papers and in meetings.

For example, the following definition '*The firewall controls network traffic entering and leaving our organisation*' is neither over-simplified nor patronising. Don't be frightened to explain things at (what you consider to be) an absurdly high-level. You can always add detail if required, which is much easier than starting with the details and then having to work back up.

Technical teams tend to talk about the names of systems or the vendor that provides those systems (or both at once). This is not helpful. Don't talk about '*CyberPro18.2 as our End Point Protection*'. Instead talk about '*protecting PC and servers from viruses and other types of malware*'.

Use diagrams and images to aid comprehension if that is what your Board prefers. The NCSC Cyber Security Toolkit for Boards is a great resource for board-ready communication collateral covering the cyber domain.

Less is more

Brevity is good. Use fewer words. Use more headings and fewer blocks of text than you would when addressing technical teams. Favour 'executive summaries' (that is, a *summary of your whole argument*) over 'introductions' (which oblige your audience to read more). This isn't about dumbing down or leaving out important parts of the story. You must give a complete and balanced view. This is not easy. It sometimes feels rude or terse. Work at it if you want to get heard.

It's important to remember that the more complex the subject matter (and cyber security can be complex), the simpler the language needs to be. There's lots of evidence and usability studies that support this. *Everyone* likes clear language, and this includes highly educated Board members who are experts in their own fields and don't have time to read pages of dry technical prose.

Prepare and rehearse

You may know your stuff technically, but do you know it so well you can explain it effortlessly without drifting into too much technical detail and language? We expect Board-level communication to be at the very highest level of quality, so it's worth sweating over, and getting it right.

If you are uncomfortable presenting to a senior business audience, or perhaps just daunted a little by the Board, find someone you can partner with when presenting. This will ideally be a 'cyber champion' on the Board or Exec team who can help you with content and also help you field questions.

Make sure you check and test your content with your manager and/or the executive responsible for cyber security. Executives have managers too; they don't want to be surprised or embarrassed by content that the Board will see.

Communications around cyber - especially in the media - are often fear inducing. You can counter that when presenting with non-alarmist, measured communications that shows how this very real threat can be managed and mitigated. Tone and body language are important here too. You should be upbeat and positive about the work you have done and the challenges in front of you.

To sum up...

Following this advice will help improve your engagement with Board members on this important strategic topic. By doing so you are more likely to receive the investment and resources you need, ultimately reducing the cyber security risk and enabling the business to focus on its value-creating work.

PUBLISHED

7 October 2024

REVIEWED

7 October 2024

VERSION

1.0

WRITTEN FOR

Small & medium sized organisations

Large organisations

Cyber security professionals