THE FUTURE OF CYBER SECURITY SERIES – Part 2

EFFECTIVE BOARD GOVERNANCE OF CYBER SECURITY
– A source of competitive advantage

Richard Brinson and Rachel Briggs OBE

savanti
PART OF FSP.

EXECUTIVE SUMMARY

Cyber security is no longer just a necessary hygiene factor – it is a key differentiator for the increasingly digital organisation. Doing it well starts at the top, but the majority of Boards still don't get it.

Boards are increasingly concerned about cyber security, ranking it as one of their top priorities, and for good reason. The cyber security risk is growing, more companies are being targeted, and while multi-million dollar ransoms attract the headlines, the impacts of a cyber incident are felt right across the business: higher insurance premiums, business disruption, lower production, delays, reputational damage, intellectual property theft, litigation, and regulatory actions, to name a few. Board interest is also being piqued as a result of growing media reporting of cyber incidents, a heightened board focus on operational resilience post-pandemic, investor pressure and a tightening regulatory environment.

While there has undoubtedly been progress in recent years on board governance of cyber security, many boards struggle to dispense their responsibilities. Many don't understand their unique role on cyber security, lack the right level of cyber awareness and can't turn to CISOs or other executives to bridge this gap, and as a result fail to challenge what they hear in the boardroom.

> **Getting cyber security governance right is not just a win for the security of individual companies; evidence shows that large enterprises with digitally savvy executive teams have significantly higher revenue growth, valuations and net margins.**

This vacuum in cyber security board governance leads to three common problematic postures: passive, in the weeds, and deferential. Directors on these boards, respectively, have a tendency to disengage from the conversation, get distracted by the technical details at the expense of a risk-based approach, or wave through the recommendations of a trusted and well-presented CISO.

Cyber-engaged boards operate differently. Exactly what cyber-engaged looks like will differ according to a company's cyber risk profile, but these boards share the following six characteristics: a) they have a clear understanding of the unique role of the board, b) they recruit directors with specialist knowledge of technology, digital, data or cyber, c) they invest in education to raise their individual and collective knowledge of cyber security, d) they make cyber security a regular topic of discussion in board meetings, e) they ensure cyber security has a home within a designated board committee, and f) they seek out advice from the CISO and independent cyber advisors.

Getting cyber security governance right is not just a win for the security of individual companies; evidence shows that large enterprises with digitally savvy executive teams have significantly higher revenue growth, valuations and net margins. Effective cyber security also brings many top line benefits, including greater success rates when tendering for new clients, improved data insights, investor confidence and maintenance of share-holder value during mergers and acquisitions

What's more, effective cyber security contributes to the trust and integrity our societies and economies rely on to survive.

There is a growing urgency to act, and it requires companies, regulators, investors and public bodies to play their respective roles.

We set out a **5-point plan for effective cyber security board governance** which includes recommendations for all these bodies:

Boards should:

1. **Understand their unique role as a board,** in setting the company's risk appetite, focusing on resilience and recovery, ensuring they remain informed and up-to-date, and being prepared to respond as a board in the event of a cyber incident

2. **Be appropriately informed about technology, data and cyber security:**
   - Boards should have at least one NED with experience in, and capable of speaking at board level to, technology, digital, data, cyber security or other forms of security, such as physical or supply chain.
   - Chairs should encourage directors to educate themselves, invite experts in to brief the board, allow and encourage NEDs (Non-executive directors) to be in contact with CISOs between board meetings, and ensure directors have access to independent board advisors.

3. **Put cyber security on the board's agenda**
   - Cyber security should feature at least quarterly and more frequently when there is something critical ongoing.
   - The board report should be delivered by the CISO.
   - Companies with elevated technology, data and cyber risks should consider establishing a technology committee of the board.

4. Ensure they have access to independent cyber security advisors

- CEO and CFO: to help them challenge and arbitrate between the CISO, CIO and CTO in prioritising between security, reliability and uptime. Often security needs to be prioritised against features and functions of business systems or customer facing apps, for example. They can also help them to interpret reports from the CISO before or after board meetings, helping them to understand what questions to ask and which lines of enquiry to probe.
- Non-executive directors: to offer 1-2-1 coaching and mentoring for NEDs, help them to prepare for board meetings, understand cyber strategy, formulate the right questions to ask, and help them to identify red flags.
- CISO: to coach CISOs on how to communicate and engage appropriately at board level.

5. Actions for regulators, investors and public bodies:

- Regulators: While regulation should be the last resort in many situations, it is time to act on cyber security with smart and focused regulation. This means requirements for boards to: report on relevant expertise at board and senior management level on cyber security; report on risk management arrangements for cyber security; and disclose breaches to the relevant public authority to build a more comprehensive shared picture of the emerging threat. We welcome the July 2023 SEC ruling on cyber security disclosure.
- Investors: investors should continue to ask questions of their portfolio companies to help drive action on cyber security and more effective governance.
- Public-private partnerships on cyber security:
  - They can deliver three vital outcomes for cyber security: a) shared and improved knowledge about incidents and trends, b) shared best practice on cyber security management and governance, and c) joint activities to strengthen the cyber security capability of organisations and the general public.
  - The National Cyber Security Centre (NCSC) does sterling work in the UK and should be further resourced and supported to extend this work to ensure all organisations have somewhere to turn for information, mentorship, best practice, and joint working.

> **“When you think the things that keep them up at night, it’s cyber because the impact can be unquantifiable. When it comes to data breaches, cyber hacks, the impact on your business can expotential and potentially existential”**
>
> Leading recruitment consultant working on non-executive board recruitment

WE HAVE AN OPPORTUNITY – BOARD GOVERNANCE OF CYBER SECURITY IS A SOURCE OF COMPETITIVE ADVANTAGE

The cyber security risk for companies is growing. Almost two-thirds (61 percent) of enterprise firms were targeted in 2021, up from 51 percent in 2020. One in six of all companies that were attacked in the past year said they almost went under as a result. Ransomware attacks increased in frequency by 200% between 2019 and 2021 and multi-million dollar ransom payments grab the headlines, such as JBS who paid out $11 million, and the Colonial pipeline, where a ransom of $4.4 million was paid. The impact of cyber events extend well beyond ransom payments; remediation efforts, higher insurance premiums, business disruption, lower production, delays, reputational damage, intellectual property theft, litigation, and regulatory actions, to name a few.

It’s therefore not surprising that cyber security is a boardroom priority; almost three-quarters of board directors rank it as a top priority. As a leading recruitment consultant working on non-executive board recruitment commented, “When you think about the things that keep them up at night, it’s cyber, because the impact can be unquantifiable. When it comes to data breaches, cyber hacks, the impact on your business can be exponential and potentially existential.”

There are five trends driving board prioritisation of cyber security:

- **Increasing frequency of cyber events:** board directors are rarely more than two or three degrees of separation from a cyber security event. As Ian Haslegrave, a General Counsel commented, “I think there’s been more transparency on the types of cases coming out and the impacts. The more of those events, the more likely that they’re getting closer to somebody that they know.”
- **Increased media reporting:** most cyber incidents are not reported publicly, but a growing number are making the headlines. As one CIO and cyber board advisor reflected, “No-one wants to be the next Dido Harding,” referring to the former CEO of TalkTalk, who resigned following a major breach. This translates into discussions in the boardroom. CISO, Dr. Joe Da Silva, told us, “Media is obviously a factor; whenever there is something in the media, there are questions that come through to you, there’s interest, there’s curiosity about what’s happened and whether it can happen here.”

There are five trends driving board prioritisation of cyber security:

- **Pandemic focus on operational resilience:** a heightened focus on operational resilience during the pandemic shone a spotlight on technology, digital and data systems. Steven McCord, a board recruitment consultant with Russell Reynolds Associates commented, "There has been a sea change in attitudes to technology leadership on boards over the last five years. It was certainly happening pre-pandemic, but what the pandemic did was accelerate this because it forced boards to think really hard about resilience, about cyber, about data, and also about basic operational technology."

- **Investor pressure:** many investors see cyber as the canary in the coal mine for organisational health; if a company can demonstrate effective cyber preparedness, it is a sign of the strength of their overall leadership, operations and governance. Investor concerns form part of the SEC's rationale for proposed regulation of cyber governance.

- **Regulation:** a growing number of regulators have acted on cyber, including most recently the SEC, which has implemented new requirements around disclosure and board and management oversight. It follows the EU's NIS2 Directive, Australia's Critical Infrastructure Act and Norway's Security Act, amongst others. It seems likely more cyber regulation will emerge in the coming years.

> **Investors see cyber as the canary in the coal mine for organisational health.**

Board directors often struggle to define their unique role on cyber security governance. In one study, there was no consensus on what the role should be: 41% of directors felt they were there to provide guidance to operating managers or C-Level leaders, 14% to participate in tabletop exercises, and 23% thought their role was in "standing by to respond should the board be needed." In our experience working with boards as part of our board advisory service, we see that the most effective are those who focus on setting the company's risk appetite, satisfy themselves of the company's cyber resilience and ability to recover in the event of an incident, remain informed of latest cyber trends and put in place preparations that enable them to act swiftly should the worst happen.

> **"There has been a sea change in attitudes to technology leadership on boards over the last five years. It was certainly happening pre-pandemic, but what the pandemic did was accelerate this because it forced boards to think really hard about resilience, about cyber, about data, and also about basic operational technology"**
>
> Steven McCord, board recruitment consultant,
> Russell Reynolds Associates

Board directors often lack the right level of cyber awareness. A majority (59%) of directors say their board is not very effective in understanding the drivers and impacts of cyber risks for their organisation, and in another study, a majority said they "only somewhat" understand their company's cyber security vulnerabilities. One of the main reasons for this knowledge gap is the small number of directors with cyber or related expertise, such as technology, information or corporate security. While some boards are actively targeting NED recruitment towards directors with these profiles, research on board succession suggests change will be slow; very few boards have explicit board term limits and mandatory retirement ages are increasing. Half (51%) of boards with a mandatory retirement age set it at 75 or older, compared with 20% a decade ago. As one CTO we interviewed said, "I've been an advocate for many years of boards needing to have more technology capability. There's a lot of people there who have deep financial understanding and competence, but as more and more organisations are driven by a technology landscape, not having good technology experience there for governance and oversight is a real weakness."

The benefits of enhanced digital and technology knowledge at board and executive level extend beyond a tech or cyber dividend. Large enterprises with digitally savvy executive teams where more than half of members are digitally savvy have 48% higher revenue growth and higher valuations (share price to sales ratio) and 15% higher net margins.

Most CISOs can't bridge the gap in board awareness of cyber security. As we outlined in our paper, *Cyber security leadership is broken*, many CISOs struggle to communicate at board level, focusing on tactical and technical briefings, rather than strategic risk-based discussions. As one NED told us, "One of the things that's wrong with the cyber industry is it's very technically focused and dominated by people who speak technobabble and obsess about the minutiae of some interesting engineering element as opposed to the big picture around risk and the controls that make the biggest difference." This is felt across boards; as Peter R Gleason, President and CEO of the National Association of Corporate Directors (NACD), is quoted in the *Harvard Business Review*, "We have heard from many directors the need to understand the financial exposure resulting from cyber risk, going beyond the threat-focused, technical cyber presentations most boards receive." Perhaps unsurprisingly, board members tend to have little interaction with CISOs outside board meetings, one-third only interact with the CISO when he/she is presenting to the board.

> **“We have heard from many directors the need to understand the financial exposure resulting from cyber risk, going beyond the threat-focused, technical cyber presentations most boards receive.”**
>
> Peter R Gleason, President and CEO,
> National Association of Corporate Directors (NACD)

Boards are increasingly turning to independent board advisors to help them make sense of what they hear and ask the right questions of CISOs. This function is well-known on information and technology, but newer for cyber security. Ian Cohen, Chief Product & Information Officer at Acacium Group and board advisor commented, "The CISO community is suffering in the same way that the CIO and the technology community suffered with about ten years ago. They are not speaking a language that is 'board or investor accessible'. Hence boards are often hiring advisors, in part to translate the cyber-tech speak of the CISO and to help demystify the data and digital narrative they receive because they don't receive the context. Much like the early digital and data conversations, they may not think what their leadership's telling them is correct (or simply do not understand). In many cases the internal people who are reporting to these boards are often very, very good on the cyber technology and types of threat, but don't come with the business context."

Boards often can't look to executive teams for technology and associated knowledge. A 2019 study looked at the level of 'digital savvy' among boards and executive teams in 3228 large US-listed companies with annual revenues over $1 billion. Only 24% of the boards and 7% of the executive teams were digitally savvy. Among these companies, the average top management team had nine members and overall, only 17% of individual team members were digitally savvy, including slightly less than 1 in 4 CEOs, and only about 1 in 8 CFOs. The level was higher among CTOs (47%) and CIOs (45%).

The benefits of enhanced digital and technology knowledge at board and executive level extend beyond a tech or cyber dividend. Large enterprises with digitally savvy executive teams where more than half of members are digitally savvy have 48% higher revenue growth and higher valuations (share price to sales ratio) and 15% higher net margins. As the percentage of digital savviness on top teams increases, so does net margin and revenue growth. For every 10% increase in top team digital savviness, there is a 0.4 percentage point increase in profitability and a 0.7 percentage point increase in revenue growth, compared with the industry average. **Effectiveness in the cyber security domain is a source of competitive advantage.**

COMMON CYBER SECURITY BOARD POSTURES

> **“The CISO community is suffering in the same way that the CIO and the technology community suffered with about ten years ago. They are not speaking a language that is ‘board or investor accessible’. Hence boards are often hiring advisors.”**

Ian Cohen, Chief Product & Information Officer, Acacium Group

As a result of insufficient cyber knowledge and the lack of clarity about their role, many boards struggle to challenge what they hear about cyber security. Some take it as read, others remain silent for fear of betraying their ignorance, and others still hone in on tiny details because they are not sure how to tackle the bigger picture. Research shows this creates the risk of ‘cyber sophistry’; as one PhD-qualified CISO, Dr. Joe Da Silva, told us, “There's an opportunity for CISOs to pull the wool over board's eyes. I've been at plenty of organisations where if you tell them it's all fine, nobody's going to question you. Boards need to be able to assure themselves that they can verify what they are being told. The concept I used in my research on cyber security in organisations is ‘Cyber Sophistry’, which is the opportunity for CISOs to manipulate or spin things in such a way that means that boards don't look too closely.”

> **“Most boards don't know what questions to ask to be able to challenge it, so they move on because they don't want to look stupid.”**

Anne Woodley, NED; Senior Security Specialist, Microsoft

It can lead boards into a holding pattern on cyber security. In a survey of 800 global board directors, 83 percent identified cyber security as a top priority, but less than half had taken any dedicated action, such as requesting cyber security updates, conducting third party audits, or involving themselves in their organisation's cyber security threat response simulations. Only one-third of IT and security executives believe their interactions with the board reduce organisational risk. Around half of board directors believe their organisation is unprepared for a cyber attack.

In a survey of 800 global board directors, 83 percent identified cyber security as a top priority, but less than half had taken any dedicated action, such as requesting cyber security updates, conducting third party audits, or involving themselves in their organisation's cyber security threat response simulations.

We identified four common cyber security board postures: passive, in the weeds, deferential and cyber-engaged. Boards are rarely just one; they alternate between these approaches within and between meetings and over time, and there are different levels of maturity within individual boards.

Passive: this is driven by a number of factors. Some are passive because they don't think cyber is important. One CISO commented, “I've been at board meetings talking about security and half the non-execs are looking out the window or playing with their phones.” Others prefer not to speak first for fear of exposing their lack of understanding. Anne Woodley, a NED and Senior Security Specialist at Microsoft, told us, “Most boards don't know what questions to ask to be able to challenge it, so they move on because they don't want to look stupid.” When passive boards recruit a technology or cyber NED, they often defer to them, something we call ‘board room cyber rubber necking’. As one NED told us, “Whenever the topic comes up, you see the heads swivel towards that person.”

> **“There's an opportunity for CISOs to pull the wool over board's eyes. I've been at plenty of organisations where if you tell them it's all fine, nobody's going to question you. Boards need to be able to assure themselves that they can verify what they are being told.”**

Dr. Joe Da Silva, CISO, RS Components

In the weeds: this happens for two main reasons. First, when CISOs focus on threats and controls, it leads boards into a tactical rather than strategic and risk-based discussion. As experienced NED, Paul Cutter, told us, "I don't think most frameworks are very helpful for boards. The board conversation has to be at the right level and it has to be about the stuff they understand and care about and then track that to where the organisation should respond." Second, boards that tend to micromanage on all areas, also micromanage on cyber security. As experienced NED and CEO, Nicola Horlick told us, "I'd rather spend time making sure we've got the right person being the CTO or CDIO, rather than have the board hanging over their shoulder, breathing down their neck, trying to make sure that they've chosen the right system."

Deferential: even boards with relevant experience can tend towards being deferential to the CISO, especially when that individual is trusted and communicates well and appropriately at board level. This is the cyber board trust paradox. As one CISO told us, "The more trusted you are and the better the content that you write for them, the fewer questions they ask you because they trust you. That is obviously a good thing in one regard, but actually it's potentially open to abuse." Deferential boards are often cyber aware enough to ask the right questions, but not enough to understand the answers, and their deference to the CISO means they reduce the opportunity for conversations that would mature their posture.

> **"I don't think most frameworks are very helpful for boards. The board conversation has to be at the right level and it has to be about the stuff they understand and care about and then track that to where the organisation should respond."**

Paul Cutter, NED

Cyber-engaged: boards that are effectively disbursing their responsibilities for cyber security understand that they are responsible for ensuring the executive is effectively managing cyber risk for their company. As such, they are engaged, informed, constantly learning and are in an ongoing dialogue with their CISO and amongst themselves about cyber risk for their organisation. Exactly what cyber-engaged looks like will differ according to a company's cyber risk profile. These boards exhibit six behaviours:

- They have a clear understanding of the unique role of the board
- They recruit directors with specialist knowledge of technology, digital, data or cyber
- They invest in education to raise their individual and collective knowledge of cyber security
- They make cyber security a regular topic of discussion in board meetings
- They ensure cyber security has a home within a designated board committee
- They seek out advice from the CISO and independent cyber advisors

> **"I'd rather spend time making sure we've got the right person being the CTO or CDIO, rather than have the board hanging over their shoulder, breathing down their neck, trying to make sure that they've chosen the right system."**

Nicola Horlick, Founder and CEO, Money & Co.

SAVANTI'S 5-POINT PLAN FOR EFFECTIVE CYBER SECURITY BOARD GOVERNANCE

Effective cyber security governance is an increasingly critical responsibility for boards of directors. There has been steady improvement of board performance in recent years; as Ian Haslegrave, a General Counsel commented, "We've got a maturity curve for board members and it's gone up quite significantly." Getting this right is not only a win for an individual company; it contributes to the trust and integrity our societies and economies rely on to survive. As such, our 5-point plan for effective cyber security board governance covers actions not just of boards and their companies, but also regulators, investors and public bodies.

Actions for boards

1. Understand your unique role as a board

Boards have four roles in relation to cyber security:

- **Set your company's risk appetite for cyber security:** boards should understand their risks and articulate the ones they are willing and unwilling to take. As the global CISO with a financial institution told us, "What a lot of boards don't yet do, but they should be doing, is setting the risk appetite. To set the right risk appetite, you have to understand what threat is particular to your business and what your vulnerability is." It is especially important they acknowledge the risks they accept and the areas where they agree action should not be taken. NED, Paul Cutter, told us, "Part of the responsibility of the board is to define the risk appetite for the business and to hold management to account for managing within that risk appetite."

- **Resilience and recovery:** boards should satisfy themselves that they understand how the organisation would recover from a breach, how long this would take, and the impacts it would have. Too many boards accept what they are told and make assumptions about recovery times that are unrealistic.
- **Informed:** boards have a responsibility to ensure they have a board-appropriate level of knowledge of cyber security that enables them to interrogate what they are told, ask the right questions and understand the responses they get from CISOs.
- **Be prepared:** boards need to ensure they are ready for their role during a crisis incident, have established policy positions on key issues such as ransomware payments, and have pre-approvals in place to streamline the response.

> **"We've got a maturity curve for board members and it's gone up quite significantly."**

Ian Haslegrave, General Counsel, OFI

2. Be appropriately informed about technology, data and cyber security

As technology, digital transformation, data-led decision-making and effective cyber security become ever more critical to business, this should be reflected at board level. Calls for CISOs to be elevated to board level are too broad; board skills should be needs-driven. There are also currently few CISOs with the breadth of skills, experience and business acumen necessary for board positions, although this is growing over time. As one CISO commented, "I can only count on two hands the sort of person that we're talking about." Boards need well-rounded directors – capable of contributing across all board discussions. As one board recruiter told us, "The challenge for boards and chairs is you have finite number of seats. Boards are like orchestras, and everybody plays a slightly different instrument and they all play harmoniously. You need people who can speak to their area of expertise, but they need also to lean into other conversations; otherwise, it's less of a holistic discussion." **Boards should have at least one NED with experience in and capable of speaking at board level to, technology, digital, data, cyber security or other forms of security, such as physical or supply chain.**

As well as recruiting board members with specific expert knowledge, all board members should have sufficient knowledge to play an active role in cyber security discussions to avoid 'board room cyber rubber necking'. As one global CISO put it, "I think they need to be GCSE French level fluent in cyber security." **Chairs should encourage directors to educate themselves, invite experts in to brief the board, allow and encourage NEDs to be in contact with CISOs between board meetings and ensure directors have access to independent board advisors.**

3. Put cyber security on the board's agenda

Boards should make cyber security a regular discussion at their meetings, **featuring at least quarterly and more frequently when there is something critical ongoing.** As a global CISO with a financial institution commented, "The beginning of good looks like boards at least showing an appetite to get this, to ask the right questions, to make sure that cyber is a regular board level topic and not just discussed when there's a problem." **The board report should be delivered by the CISO** to ensure cyber security discussions are not filtered through the lens of competing concerns, such as reliability and uptime, and also to ensure all questions can be addressed head on, rather than deferred and forgotten.

> **"The normal audit is all about the figures, it's not necessarily about processes and making sure that you've got the best things in place for things like cyber security. So, I think it's important for boards to get someone to perform that independent assessment and advisory role."**

Nicola Horlick, Founder and CEO, Money & Co.

Companies with elevated technology, data and cyber risks should consider establishing a technology committee of the board, something that a small but growing number of companies are doing. Less formal than the audit committee, they bring focus and oversight and allow for open discussions that will help mature cyber security governance.

> **"I'm not a fan of overregulation, but smart regulations and targeted regulations, would help to raise everyone's standards up a little bit and make it easy to understand how you're measured against it."**

Anne Woodley, NED; Senior Security Specialist, Microsoft

4. Board and executive access to independent cyber security advisors

Boards can accelerate their cyber knowledge and enhance cyber governance through the use of independent cyber security advisors. A number of interviewees commented on their value. One NED told us, "Independent board advisors are invaluable. Any time I have served on the board that has had one, it's been fantastic because you can also have those conversations offline with them, call them up to ask them the question you didn't want to ask in front of everybody." Nicola Horlick reflected, "The normal audit is all about the figures, it's not necessarily about processes and making sure that you've got the best things in place for things like cyber security. So I think it's important for boards to get someone to perform that independent assessment and advisory role."

Independent board advisors can contribute to three aspects of cyber security governance:

- **CEO and CFO:** to help them challenge and arbitrate between the CISO, CIO and CTO in prioritising between security, reliability and uptime. Often security needs to be prioritised against features and functions of business systems or customer facing apps, for example. They can also help them to interpret reports from the CISO before or after board meetings, helping them to understand what questions to ask and which lines of enquiry to probe.
- **Non-executive directors:** independent cyber security advisors can offer 1-2-1 coaching and mentoring for NEDs, help them to prepare for board meetings, understand cyber strategy, formulate the right questions to ask, and help them to identify red flags. They can also help NEDs to benchmark the company's stance on cyber.
- **CISO:** independent cyber security advisors are increasingly being hired to coach CISOs on how to communicate and engage appropriately at board level.

5. Actions for regulators, investors and public bodies

Effective cyber security board governance is vital – not just for individual companies, but to create the trust and integrity that societies and economies rely upon. There is, therefore, an important role for regulators, investors and the public sector.

- **Regulators:** While regulation should be the last resort in many situations, it is time to act on cyber security with smart and focused regulation. This means requirements for boards to: report on relevant expertise at board and senior management level on cyber security; report on risk management arrangements for cyber security; and disclose breaches to the relevant public authority to build a more comprehensive shared picture of the emerging threat. Many of our interviewees agreed; Anne Woodley, a NED and Senior Security Specialist at Microsoft reflected, "I'm not a fan of overregulation, but smart regulations and targeted regulations, would help to raise everyone's standards up a little bit and make it easy to understand how you're measured against it." This chimes with wider research, with 80% of senior executives agreeing that mandatory disclosure of cyber incidents, with comparable and consistent formats, is necessary for building confidence and trust. We welcome the July 2023 SEC regulations on cyber security disclosure on incidents and board and management oversight.
- **Investors:** investors should continue to ask questions of their portfolio companies to help drive action on cyber security and more effective governance.
- **Public-private partnerships on cyber security:** they can deliver three vital outcomes for cyber security: a) shared and improved knowledge about incidents and trends, b) shared best practice on cyber security management and governance, and c) joint activities to strengthen the cyber security capability of organisations and the general public. The National Cyber Security Centre (NCSC) does sterling work in the UK and should be further resourced and supported to extend this work to ensure all organisations have somewhere to turn for information, mentorship, best practice, and joint working. As a former senior law enforcement leader told us, "The policing world is intelligence heavy but resource poor, and business is the reverse. Potentially it's a match made in heaven, bringing the two much more closely together."

SAVANTI SERVICES

Board advisory service
Outsourced vCISO service

FURTHER READING

Cyber security leadership is broken: Here's how to fix it, Richard Brinson and Rachel Briggs OBE

Cyber Security Toolkit for Boards, National Cyber Security Centre

Global Cybersecurity Outlook 2023, World Economic Forum

'Cyber security is a dark art': The CISO as soothsayer, J. Da Silva and R. B. Jensen, ACM Conference On Computer-Supported Cooperative Work And Social Computing (CSCW), Feb. 2022.

Practitioner-led Cyber Security Services

Fortify your resilience with best-in-class cyber security expertise from Savanti.
Effectively manage security risks, safeguard your data
and protect your organisation

savanti
PART OF FSP.

ISO 27001
INFORMATION SECURITY MANAGEMENT

TECHTALENT CHARTER
SIGNATORY

Crown
Commercial
Service
Supplier

FOLLOW US ON:

E: insight@savanti.co.uk T: +44 (0) 207 608 5632

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisers. Image usage vecteezy.com