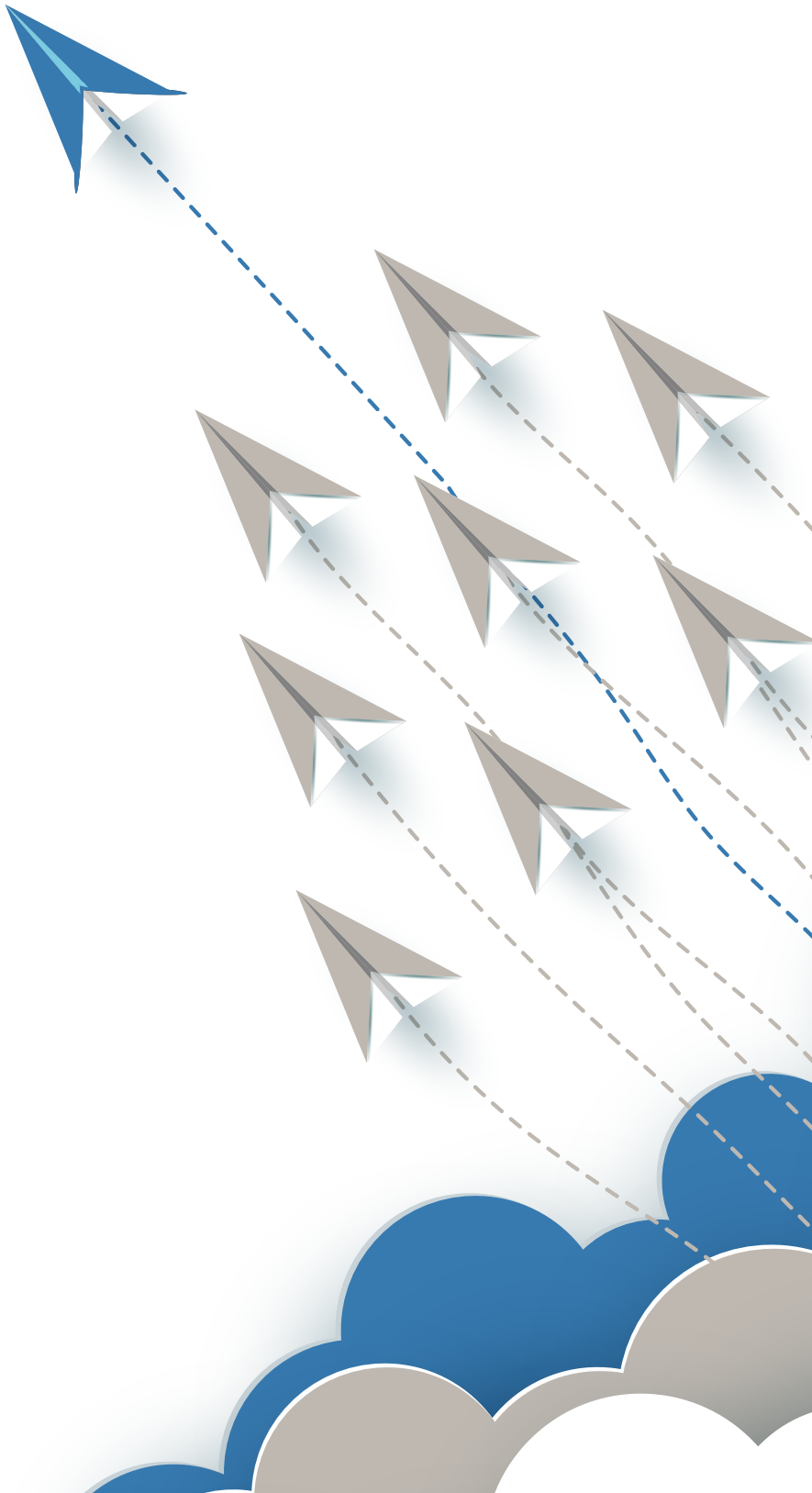
THE FUTURE OF CYBER SECURITY LEADERSHIP SERIES – Part 1

CYBER SECURITY LEADERSHIP IS BROKEN

Here's how to fix it

Richard Brinson and Rachel Briggs OBE



savanti
PART OF FSP.

INTRODUCTION

We are in the middle of a cyber security perfect storm. The threat of cyber-attack has never been higher, from criminals, terrorists and rogue states, with digital transformation and the post-pandemic shift to working from home further increasing vulnerability to cyber-attack.

While cyber budgets are increasing, the function has historically suffered from chronic underinvestment and the people who need to make decisions – boards – almost universally don't understand the risk and often don't want to own it. This means they make poor hiring decisions and don't govern cyber security effectively. Many boards are by-standers on cyber security – unable to challenge or assess value for money.

At a time when we need clear direction the most, cyber security leadership is broken. The majority of Chief Information Security Officers (CISOs), the people responsible for managing cyber risks, are operating at a relatively junior level for the importance of their role, and the majority of boards still see cyber as a technical problem. Cyber leadership is currently based on individual best effort, with no agreement on what good looks like, with CISOs typically blinkered on the implementation of controls rather than understanding the risks to the business and driving cultural change accordingly.

We are in the middle of a cyber security perfect storm

There is very little topflight talent in the market, which has led to spiraling salaries and boards are unable to assess whether they are getting value for money. Replacing a CISO is time-consuming, expensive and disruptive, and many CISOs have a 'tear it up' mentality as they prioritise being heroes rather than steady builders. We estimate the cost of a bad CISO hire to be at least £7.6 million for a typical large corporation, which encompasses average remuneration for the average CISO tenure of 2.3 years, associated hiring costs and an estimated budget wastage on unfinished cyber projects.[1] **In the race against cybercriminals, it's only a matter of time before the shortcomings in cyber leadership will be laid bare** – with potentially substantial consequences.

As a first step to addressing this issue, **we need a new generation of business-aligned CISOs** who are excellent communicators and business leaders first, focused on risks rather than technologies, who work through the whole organisation, are more interested in evolution than revolution, and enable the business as well as protect it. **Done well, cyber security can be one of the greatest sources of competitive advantage for businesses,** and increasingly so. Both boards and cyber security leaders need to understand and embrace this.

In this paper, we outline the characteristics of the business-aligned CISO and put forward a number of recommendations to improve the probability of success for both boards and cyber leaders:

- **Boards should prioritise communications skills** as non-negotiable when appointing a CISO
- **CISOs should be hired, managed and measured as business leaders** rather than technical experts
- **Cyber risk should be owned by the board,** overseen by the audit committee with individual decisions about risk sitting with business leaders. Cyber risk management should be embedded in organisational processes and led by the CISO with sufficient budget and staffing to drive organisation-wide change
- Cyber leaders need to achieve **change through influence rather than control**
- **Boards need independent trusted cyber advisors,** including ex-CISOs, to help them effectively interrogate all aspects of cyber leadership and strategy
- **CISOs should be integrated into all forward-looking aspects of business growth**

In subsequent papers, we will outline the other essential pillars of a business-aligned cyber security capability: effective board governance, creative approaches to closing the talent gap, nimble and pragmatic cyber risk management frameworks, and a practical toolkit for business-aligned CISOs.

This is the first time such a broad study of topflight CISOs, Chief Information Officers (CIOs), Chief Technology Officers (CTOs), Non Executive Directors (NEDs) and Chief Executive Officers (CEOs) has been conducted, giving a comprehensive view of the problem. It has involved scores of interviews, drawn on over 500 years' collective cyber security experience within the Savanti team and benefited from industry-leading research from the sector.

> We estimate the **cost of a bad CISO** hire to be **at least £7.6 million**

[1] Calculation is based on a median salary package of £525,000 over 2.3 years according to Heidrick and Struggles data, recruitment fees of 10 percent for both the original and new hire, and an assumed 25 percent budget wastage on unfinished cyber projects on an average annual cyber budget for an enterprise firm of £10.8 million per year over 2.3 years according to data from Hiscox. We based 25 percent wastage on Savanti's experience of working with companies who have come to us for help following a bad hire.

Cyber threats are higher than ever

Cyber security threats are growing exponentially. According to Cybersecurity Ventures, it's predicted that cybercrime globally will increase by 15 percent per year, reaching $10.5 trillion USD annually by 2025. As Steve Morgan, Editor-in-Chief of Cyber Crime Magazine and CEO of Cybersecurity Ventures put it, "This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, is exponentially larger than the damage inflicted from natural disasters in a year, and will be more profitable than the global trade of all major illegal drugs combined." If it were measured as a country, cybercrime would be the world's third-largest economy after the US and China.

Organisations are in the firing line for cyber criminals. The top five sectors facing cyber-attack are tech, media and telecoms, financial services, energy, construction, and transport and distribution. **Given the current conflict in Ukraine and the knock-on impact on energy supply, it is especially worrying to note that attacks on energy companies have increased by one third in recent years; 40 percent of energy companies had been attacked in 2020, rising to 54 percent in 2021.** This is likely to increase as utility companies become increasingly attractive targets for cyber-attack.

It's predicted that cybercrime globally will increase by 15% per year, reaching $10.5 trillion USD annually by 2025

Almost two-thirds (61 percent) of enterprise firms were targeted in 2021, up from 51 percent in 2020. Almost half of those that were attacked fended off hackers six or more times. One in six of all companies that had been attacked in the past year said they almost went under as a result. More than half of those hit with a ransom paid up, with some ransoms running to hundreds of thousands of pounds, or even millions, such as the cyber-attacks on JBS which paid out $11 million, and the Colonial pipeline, where a ransom of $4.4 million was paid. The average total cost of a ransomware incident for multinational companies, excluding ransom, is $4.54 million, due to the impact on operations and reputation.

If it were measured as a country, cybercrime would be the world's third-largest economy after the US and China

The threat of cyber-attacks perpetrated by nation states is also growing. A recent study reported a 100 percent increase in nation-state incidents from 2017 to 2021. These attackers are now more interested in the private sector (35 percent of attacks) than government cyber defence agencies (25 percent) and other government bodies (12 percent).

The average **total cost of a ransomware incident** for multinational companies, excluding ransom, is **$4.54 million**

One in six of all **companies attacked** in the past year said they **almost went under as a result**

Another study found that 90 percent of organisations believe they have been targeted by a nation state threat actor, with 39 per cent of them citing Russia and 44 percent China. The heads of the FBI and MI5 took the unprecedented step of speaking out publicly about China; MI5 has seen a sevenfold increase in China-related investigations since 2018, and the FBI opens a China-related investigation every 12 hours.

90% of organisations believe they have been **targeted by a nation state threat actor**

There has been a **100% increase** in **nation state incidents** from 2017 to 2021

THE CYBER SECURITY PERFECT STORM

Huge reliance on technology is making organisations increasingly vulnerable to cyber-attacks. Technology underpins most organisational processes, business growth is powered by tech-centric intellectual property, and most productivity gains are made through technological innovations. What's more, many organisations are nursing highly vulnerable legacy IT estates.

The pandemic hastened this reliance – and created more risks. Hiscox reports that almost two thirds (61 percent) of ransomware claims in 2020 were due to open remote desktop protocol ports, increasingly in use as staff work from home, and 70 percent of companies considered cyber 'experts' said they saw the move to remote working as increasing their vulnerability. A recent IBM study found that, when remote working was a factor in the breach, costs were an average of nearly $1 million greater than in breaches where remote working wasn't a factor.

For many organisations, cyber security represents a potentially existential threat. Danny Attias, Chief Digital and Information Officer for the London Business School told us, "We rely on the generosity of our donors to supplement the income we generate from student fees, which is predicated on their confidence in us running an effective business. If we have a cyber breach when we haven't done the work and we cannot function as a business, donors would rightly ask tough questions about why they should support us."

Organisations are investing in cyber security

Investment in cyber security is growing: 69 percent of organisations said they expected to boost cyber security spending in 2022, with 26 percent envisioning their security budget increasing by 10 percent or more. The average spend by enterprise firms increased from $8 million in 2020 to $13 million in 2021, and energy firms were the biggest spenders, averaging $13.4 million. For most companies, overall IT spend remains constant, but the proportion devoted to cyber has increased dramatically.

For those who get it right, the benefits are significant. Companies ranked as 'cyber experts' on the Hiscox maturity scale had fewer attacks, were less likely to pay a ransom or fall victim to phishing emails and tended to recover faster. Despite the growing threat and evidence of the benefits of cyber maturity, only one-fifth qualify as expert, including only 23 percent of energy companies.

69% of organisations said they expected to **boost cyber security spending in 2022.**

The **average spend** by enterprise firms increased from **$8 million in 2020 to $13 million in 2021**

83% of board directors identify cyber security as a **top priority**, but **less than half have taken any dedicated action**

Cyber security is a top boardroom priority – but most boards don't understand the risk

Cyber security is now one of the top concerns for boards. In one survey, corporate board members ranked cyber security as their third concern, behind corporate strategy and leadership succession.

Yet those responsible for owning cyber security risks – boards – have low levels of understanding. In one study, a majority of board directors said they "only somewhat" understand their company's cyber security vulnerabilities. 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.

> **"Clients come to us and say they are so nervous about going out to market because they don't know if they can find what they need. In fact, they're not even sure what they need"**
>
> Harriet Wood, Russell Reynolds Associates

> **70% of companies** considered cyber 'experts' said they saw **the move to remote working as increasing their vulnerability**

As a result, boards and executives don't understand what cyber capacity they need and their default position is to hire a CISO and let them deal with it. Those who have been burned with a bad hire have no idea what to put in place instead. Harriet Wood of Russell Reynolds Associates told us "Clients come to us and say they are so nervous about going out to market because they don't know if they can find what they need. In fact, they're not even sure what they need." In many ways, this is history repeating itself; many hired the wrong people to drive digital transformation in the dot.com era or more recently to create data functions because they didn't understand what they were looking for.

In these scenarios, progress is difficult unless someone at the top of the organisation is willing to take it on. As Mike Altendorf, a seasoned entrepreneur and investor put it, "There is often a strange willingness for people in senior roles to push this kind of problem away when they know it's not being represented properly. Ultimately, it's a C-Suite responsibility, but no-one wants to own it because they don't understand it. You end up with a merry-go-round within the company. Companies haven't learned the lessons from the dot.com era."

> **"Ultimately, it's a C-Suite responsibility, but no-one wants to own it because they don't understand it."**
>
> Mike Altendorf, Entrepreneur and Investor

We have a cyber security leadership problem

There is a very limited supply of CISOs at the top end of the market; executive recruitment consultants **Russell Reynolds Associates estimate around 60 percent of CISOs are operating at a junior level.** Most are not developing the skills and expertise needed for this increasingly important and demanding job. One CIO we interviewed described CISO recruitment challenges, "It was close to impossible. Finding the right quality of CISO is difficult because you need somebody that can engage at board level on one side, and on the other side understands a lot of the technicalities behind it."

When topflight CISOs find themselves in organisations where they can't influence – whether due to lack of board mandate, budget or support to drive cultural change – they leave; nearly all the CISOs we interviewed cited this as their main reason for changing roles.

CISOs move more frequently than any other corporate leader; the CISOs we interviewed are approached at least once per month with a serious job offer.

Their average tenure is 2.3 years,[2] compared to 6.9 years for a CEO, 4.7 years for a CFO, 4.6 years for a CIO, 3.5 years for a CMO and 3.7 years for a CHRO. This means that the average CIO (to whom a majority of CISOs report) will cycle through two CISOs during their tenure, and the average CEO will cycle through three. If cyber security really is a top three board priority, that's a worrying amount of churn.

Replacing a CISO is time-consuming, on average seven months, plus 3-6 months' notice period. For one of our clients, the search lasted three years. The cost of getting it wrong is considerable; **we estimate the direct cost of making the wrong hire is at least £7.6 million.**[3] It also brings disruption, a negative impact on team morale, and the cyber programme stalls. Harriet Wood of Russell Reynolds Associates told us, "We've been working with a client that has cycled through four CISOs in 18 months, two years. It's really challenging because they're so nervous about making another mis-hire. The team is incredibly unsettled. The function, the agenda, the security transformation programme is now probably five years behind."

There is a tendency for CISOs towards a 'tear it up' mentality, rather than building on the work of their predecessor. Harriet Wood told us, "A lot of the CISOs we interview have this need to transform, a 'tear everything up' mentality." The frontier mindset is helpful in a new organisation, but in established functions it creates vulnerabilities. One CIO told us, "I think of cyber security as being like a pyramid with all the exotic things at the top, and all the more basic stuff at the bottom. Technology teams tend to focus on the things at the top because it's more interesting. That's fine if you've nailed all the stuff at the bottom, but if you're not paying attention to the basics, you leave yourself wide open."

[2] Based on interview with representative from an executive search firm
[3] Calculation is based on a median salary package of £525,000 over 2.3 years according to Heidrick and Struggles data, recruitment fees of 10 percent for both the original and new hire, and an assumed 25 percent budget wastage on unfinished cyber projects on an average annual cyber budget for an enterprise firm of £10.8 million per year over 2.3 years according to data from Hiscox. We based 25 percent wastage on Savanti's experience of working with companies who have come to us for help following a bad hire.

THE CYBER SECURITY PERFECT STORM

With low supply and high demand, CISO salaries are spiraling. According to Heidrick and Struggles, median packages for CISOs in the US, including cash, bonuses and equity, rose from $784,000 in 2020 to $936,000 in 2021, with some reporting total packages of $2.5 million, and reports that Equifax paid Jamil Farshchi $3.89 million in 2018. In the UK, the median package in 2021 was £523,000, with some as high as £1.1 million.

> **“We’ve been working with a client that has cycled through four CISOs in 18 months, two years. It’s really challenging because they’re so nervous about making another mis-hire ”**

Harriet Wood, Russell Reynolds Associates

Around 60% of CISOs are operating at a junior level

The average CISO tenure is **2.3 years,compared to**

6.9 years for a CEO

4.7 years for a CFO

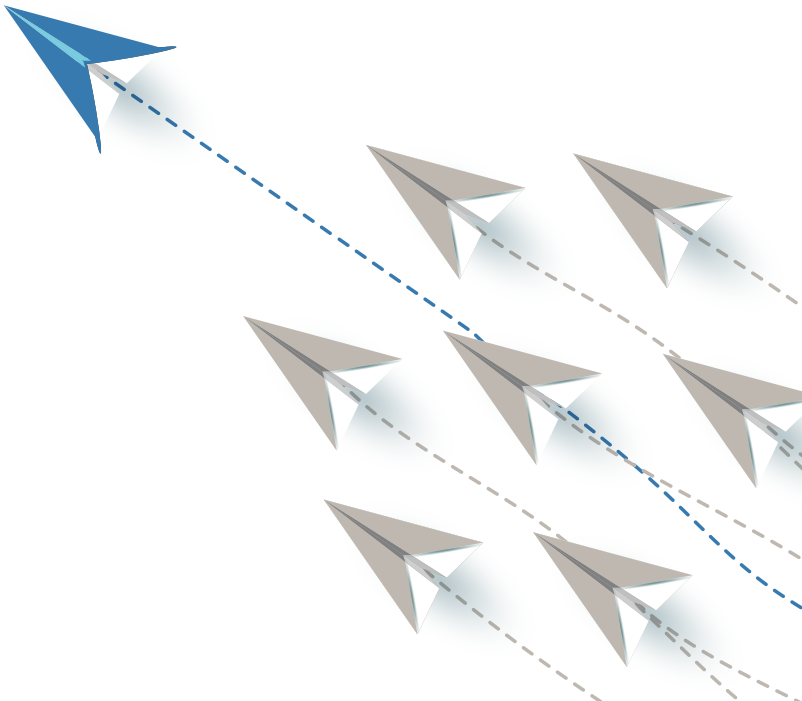
4.6 years for a CIO

3.5 years for a CMO

3.7 years for a CHRO

> **“It was close to impossible. Finding the right quality of CISO is difficult because you need somebody that can engage at board level on one side, and on the other side understands a lot of the technicalities behind it. ”**

CIO, Multinational Corporation



A NEW MODEL OF CYBER SECURITY LEADERSHIP

We need a new model of cyber security leadership; business-aligned CISOs who can bridge the gap between the technical and the business, help their boards to understand cyber risk, make themselves heard across the business, and drive organisation-wide change through influence rather than control. Our vision for a mature business-aligned cyber security function is ambitious and aspirational. It calls for transformational change because we don't have time for iterative adjustments.

The business -aligned CISO exhibits six characteristics.

1 Business-aligned CISOs are accomplished communicators

The CISOs, CIOs, CTOs, and NEDs we interviewed told us that **effective communication is the most important skill for a business-aligned CISO.** In one **major study**, the vast majority of CISOs said they were "spending time with business leaders who think cyber security risk is a technical problem or a compliance exercise." Business-aligned CISOs explain in terms that the board and senior leaders understand in order to shift this perception. "You can turn up at the board level and if no one understands what you're saying, you can't influence any change, you can't get the budget you need, what's the point? You might be able to personally stop 27 hackers with a blindfold on, but if you can't influence the organisation, what good is that?" Danny Attias, Chief Digital and Information Officer for the London Business School.

> **"You can turn up at the board level and if no one understands what you're saying, you can't influence any change, you can't get the budget you need, what's the point? You might be able to personally stop 27 hackers with a blindfold on, but if you can't influence the organisation, what good is that?"**

Danny Attias, Chief Digital and Information Officer, London Business School

> **"They need to be very good communicators, not just submerge themselves in jargon… Often, I suspect it's done because they don't know how to be relevant."**

NED, FTSE 100 Corporation

Many of those we interviewed expressed frustration with the communications skills of CISOs they had worked with. One CIO told us, "In a commercial organisation, the first skill is being able to understand the business and communicate to the business the importance of cyber security. So many CISOs fail because they're unable to bridge that gap." A NED of a FTSE 100 company commented, "They need to be very good communicators, not just submerge themselves in jargon… Often, I suspect it's done because they don't know how to be relevant." Business-aligned CISOs speak in plain English and relate what they are saying to the business. This is the most basic non-negotiable skill they require to influence and educate their organisations.

Recommendations

Boards should prioritise communications skills as a non-negotiable when appointing a CISO:

- **When recruiting** CISOs, interview panels should include non-technical colleagues and **test for communications skills as well as technical knowledge**
- **Executive teams** should **invest in communications training for CISOs**
- **Boards should insist that cyber strategies are jargon-free** presentations focused on risks and organisational change

2 Business-aligned CISOs are strong business leaders

There was universal agreement among the CISOs, CIOs, CTOs and NEDs we interviewed that CISOs need to be strong business leaders, encompassing a range of skills: leadership, people skills, influencing, stakeholder management, navigating complex matrix structures, and financial literacy.

They understand that their role is to make cyber security relevant in their organisation's setting. Charlie Timblin, Group CISO at Kantar, described the challenge, "In my current organisation, one of the key drivers is to delight the client. With the organisation hardwired that way, if

I were to come in and talk about cyber-attacks and threats, it wouldn't play to that intent, to their ethos, and it would drive a lot of fear and uncertainty. I have to think of a different way to influence the outcomes that I need to generate in a way that is oriented with the thinking, the context, the values of the organisation."

> **"When assessing risk, a lot of practitioners immediately ask, 'what does this mean for me? What is the impact from a pure infosec perspective?' What they should be asking is, 'what does this mean for the business?'"**

Joe Da Silva, CISO, RS Group

CISOs who see themselves as business leaders are in the minority. One CIO told us, "I don't think there's enough CISOs that truly understand how business operates; what drives the P&L, how to define the cyber security strategy in a way that's truly linked to your technology and business strategy." Joe Da Silva, CISO at RS Group commented, "When assessing risk, a lot of practitioners immediately ask, 'what does this mean for me? What is the impact from a pure infosec perspective?' What they should be asking is, 'what does this mean for the business?'."

There is a balance to be struck between business and technical skills, "The best CISOs are the people who can balance that technical knowledge with commercial reality," a CTO told us. It would be difficult to perform the role effectively without any technical experience, especially when ill-informed boards lurch from strategic to tactical, and so many cyber functions are still getting established.

One CISO described the challenge faced by a colleague, "One of my regional CISOs often feels exposed because he doesn't have the technical experience and expertise. Put him in front of a risk committee, absolutely awesome. But put him on the spot with a technical question, and then he looks nervous and starts to lose credibility."

In mature, large organisations, the CISO should be operating exclusively at the strategic level. A tactical CISO trying to operate at a strategic level, in the absence of informed oversight, can be destabilising and take an organisation backwards on cyber security. One of our clients came to us after experiencing this kind of CISO, who caused them huge disruption and set back their cyber programme after spending a lot of money and delivering no return on investment.

In small to medium-sized organisations, CISOs often need more technical expertise as they are inevitably hands on, especially as they set up the function. One CISO told us, "For an organisation like mine with 1500 employees, you do need technical skills, you need to dive into the detail, help steer the ship and recruit the right people from a technical perspective and check that they can do their job." These organisations often benefit from external help as they cannot retain the full range of talent within a very small team. A recent Hiscox study found that one third of the companies considered 'expert' on their cyber maturity scale are planning to increase cyber security outsourcing and 38 per cent plan to increase their use of third-party services.

In mature, large organisations, the CISO should be operating exclusively at the strategic level

Recommendations

CISOs should be hired, managed and measured as business leaders rather than technical experts:

- **Interview panels should ask a range of questions about the business** to ensure candidates understand as much about net present value, return on investment and how to make a business case, as they do about architecture, systems and the latest cyber security technologies.
- **The cyber strategy should be clearly aligned with the business strategy**
- **CISO performance** should include a **measure on the quality of business stakeholder relationships**
- Boards should invest in **business training for CISOs**

3 Business-aligned CISOs talk about risks rather than controls

There was one common theme among the CISOs we interviewed; cyber security management is risk management. Joe Da Silva, CISO at RS Group told us, "It's not about what I think is right, it's about what's right for the business and how it effectively manages that risk." Too many CISOs seek gold-plated solutions without considering the impact, such as higher costs, drag on technological innovation, or poorer customer interfaces. They are focused on controls rather than risks. For businesses with finite resources, a control-based approach to cyber security without a clear return on investment case is simply unacceptable.

Business-aligned CISOs highlight risks, explain the potential impact, offer a sliding scale of solutions, and ask the business to make informed risk-based decisions. This relies on the organisation having a mature approach to risk appetite. CISOs are critical to maturing this approach, but can't do it alone.

> **"The business risk should sit with the business because the business knows best."**

CISO, Multinational Corporation

A mature cyber risk management model is one where cyber risk appetite is owned by the board, overseen by the audit committee in consultation with the CISO, and individual decisions about risk sit with business leaders. This approach aligns cyber with the business and drives awareness of cyber security among business leaders who are forced to grapple with the tradeoff between risk and opportunity. Business-aligned CISOs see this as an opportunity rather than a threat to their status; they recognise that their power lies in their ability to influence, not dictate. As one CISO said, "The business risk should sit with the business because the business knows best."

> **"It's not about what I think is right, it's about what's right for the business and how it effectively manages that risk"**

Joe Da Silva, CISO, RS Group

Recommendations

Cyber risk should be owned by the board, overseen by the audit committee, embedded in organisational processes and led by the CISO with sufficient budget and staffing to drive organisation-wide change:

- **CISOs should attend and present quarterly at the audit committee**
- **CISOs should be integrated into the organisation's enterprise risk management structure**
- **CISOs should model a pragmatic approach to risk management**

4 Business-aligned CISOs deliver cyber security through the whole organisation

Business-aligned CISOs recognise that cyber security is not a discrete function they deliver for and on behalf of the organisation; it relies on the everyday actions of employees across the business. Individual behaviours matter; 28 percent of the first ports of entry for cyber-attacks are employees through, for example, phishing, and 23 percent are via employee -owned mobile phones. As Charlie Timblin, Group CISO at Kantar, put it, "It's less me and more we. Many CISOs talk about cyber security as if they own it all and the responsibility rests with them. In most organisations, cyber security is an influencer and the people responsible for cyber controls are across the rest of the business."

> **"It's less me and more we. Many CISOs talk about cyber security as if they own it all and the responsibility rests with them. In most organisations, cyber security is an influencer and the people responsible for cyber controls are across the rest of the business."**

Charlie Timblin, Group CISO, Kantar

Business-aligned CISOs are influencers who understand how to get things done by working through others. One CIO told us, "The cyber security team might be 5-6 percent of your technology headcount, so they are very limited in what they can do themselves. They need to have a multiplier effect, galvanising the rest of the organisation to what they need to do." Research shows that most CISOs underinvest in stakeholder relationships and over invest in operational activities.

Most of the business-aligned CISOs we interviewed spend at least 75 percent of their time on stakeholder engagement. The strongest relationships are with technology, data and operations, but their sphere of influence is growing beyond this. As CISOs mature in their stakeholder management, their visibility and relationships develop up and out of the function, with the highest performing CISOs also managing relationships outside the organisation, including investors.

Leading change through influence is challenging. It's delivered through clear goals that align with the business, structures and processes for assessing and managing risks, policies that are matched to the business, clear and transparent mechanisms of accountability, measurement of return on investment, and significant education and outreach efforts to make partners of your colleagues. It cannot be delivered without a team and an appropriate budget, as this leaves the CISO sidelined and leadership unwilling to own the risk.

Devolved delivery is not an excuse for the CISO to position themselves as a 'trusted advisor' to the board. Most organisations need to deliver a significant programme of cyber security transformation, and CISOs need to drive that change. In our experience, many CISOs position themselves as advisors rather than business transformation leaders because they are more concerned about being liked than banging heads together. Boards do need advisors, but they should be independent.

This relies on the organisation having a mature approach to risk appetite. CISOs are critical to maturing this approach, but can't do it alone.

Recommendations

Cyber leaders need to achieve change through influence rather than control:

- **CISOs should have an appropriate team and budget** to deliver the cyber security programme
- **CISOs need a budget for communication,** awareness raising and training
- **CISO performance should include a measure of cyber security awareness** across the business based on staff understanding of their role in delivering cyber security

> Most of the business-aligned CISOs we interviewed spend **at least 75% of their time on stakeholder engagement**

5 Business-aligned CISOs are more interested in evolution than revolution

Revolution in cyber security is only appropriate when a function is newly established or in need of remedial action. In any other situation, a business-aligned CISO looks for continuity rather than radical change and seeks to build upon what their predecessor has done, rather than rip it up and start again. With the average CISO term just 2.3 years, there isn't the bandwidth for radical change. In interviews, boards and leadership need to be wary of CISOs predisposed to change unless the function is new or failing. Stable growth is almost always the best approach. As one CEO said about cyber security, "What organisations need most is consistency and to keep moving forward."

Recommendations

Boards need independent trusted cyber advisors, including ex-CISOs, to help them effectively interrogate all aspects of cyber leadership and strategy:

- **Boards should consult their external board advisors on all proposed new cyber projects**
- **Boards should seek a detailed business case from their CISO** when seeking sign off on new cyber projects

> **"What organisations need most is consistency and to keep moving forward."**
>
> CEO, Multinational Corporation

6 Business-aligned CISOs enable the business as well as protect it

Business-aligned CISOs are involved in activities that enable the business as well as protect it. As technology drives ever more business processes, a cyber security function that focuses on 'no' rather than 'go' will be a drag on innovation, productivity and profitability; instead CISOs need to identify opportunities to enhance the business. As one CISO, Sarb Sembhi from Virtually Informed, told us, "We need to look for ways to facilitate new tools and encourage and foster those ideas and principles that get the business innovation moving faster because that's what the business is there for. It's not there to support security."

There are six ways the CISO and cyber security function can act as business enablers:

- **Data insights:** advice on how to produce meaningful and usable insights from their data on employees, customers, supply chain and environment, offering a more creative approach than sometimes risk-averse in-house lawyers.
- **Cyber security service spin-offs:** services their organisation can market for sale to others
- **Cyber security as a value-add:** in some sectors, notably banking and defence, being seen as a cyber leader offers a marketing edge
- **Competitive edge in procurement:** some customers insist on minimum cyber security standards to be eligible to bid for their contracts, such as ISO27001 or Cyber Essentials Plus
- **Mergers and acquisitions:** ensuring sufficient security due diligence is conducted
- **Investor confidence:** investors are increasingly looking for assurance about cyber security as they recognise poor management can negatively impact valuation due to reputational damage and regulatory fines

Recommendations

CISOs should be integrated into all forward-looking aspects of business growth:

- **CISOs should be included in groups and committees leading change projects**
- **CISOs should be consulted on new business and market development activities**
- **Cyber strategies should include customer, stakeholder and investor relations plans**
- **CISOs should play a role in investor relations events**

> **"We need to look for ways to facilitate new tools and encourage and foster those ideas and principles that get the business innovation moving faster because thats's what the business is there for. It's not there to support security."**

Sarb Sembhi, CISO Virtually Informed

Get involved

Send us your feedback on our new model for cyber security leadership, email: insight@savanti.co.uk

Follow Savanti on LinkedIn and continue the conversation.

Savanti cyber leadership services

Virtual CISO
CISO Hiring Support
Governance, Risk and Compliance Services
Board Advisory Services

Methodology

We conducted interviews with CISOs, CIOs, CTOs, NEDs and CEOs from leading organisations in industrial and electronics, consultancies, transport, higher education, financial services, luxury goods, medical research, non-profit, tech, entertainment, and marketing. We also interviewed executive headhunters working on senior cyber security roles. Additionally, we drew on over 500 years' collective cyber security experience within the Savanti team, and benefited from industry-leading research from the sector.

Authors

Richard Brinson is CEO of Savanti. He is an experienced FTSE 100 Executive and Board Advisor and has been CISO at several large companies, including Unilever, Sainsbury's, RS Components and Verisure. He was named one of the top 100 CISOs in the world and has over 20 years' experience in the field.

Rachel Briggs OBE is Executive Advisor to Savanti. She is a leading expert on security and regularly advises large multinationals and governments. She is an Associate Fellow at Chatham House and Co-Founder and CEO of The Clarity Factory and was awarded an OBE in 2014.

Practitioner-led Cyber Security Services

We remove the fear, uncertainty and doubt associated with cyber risk allowing you to get on with what you do best.

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