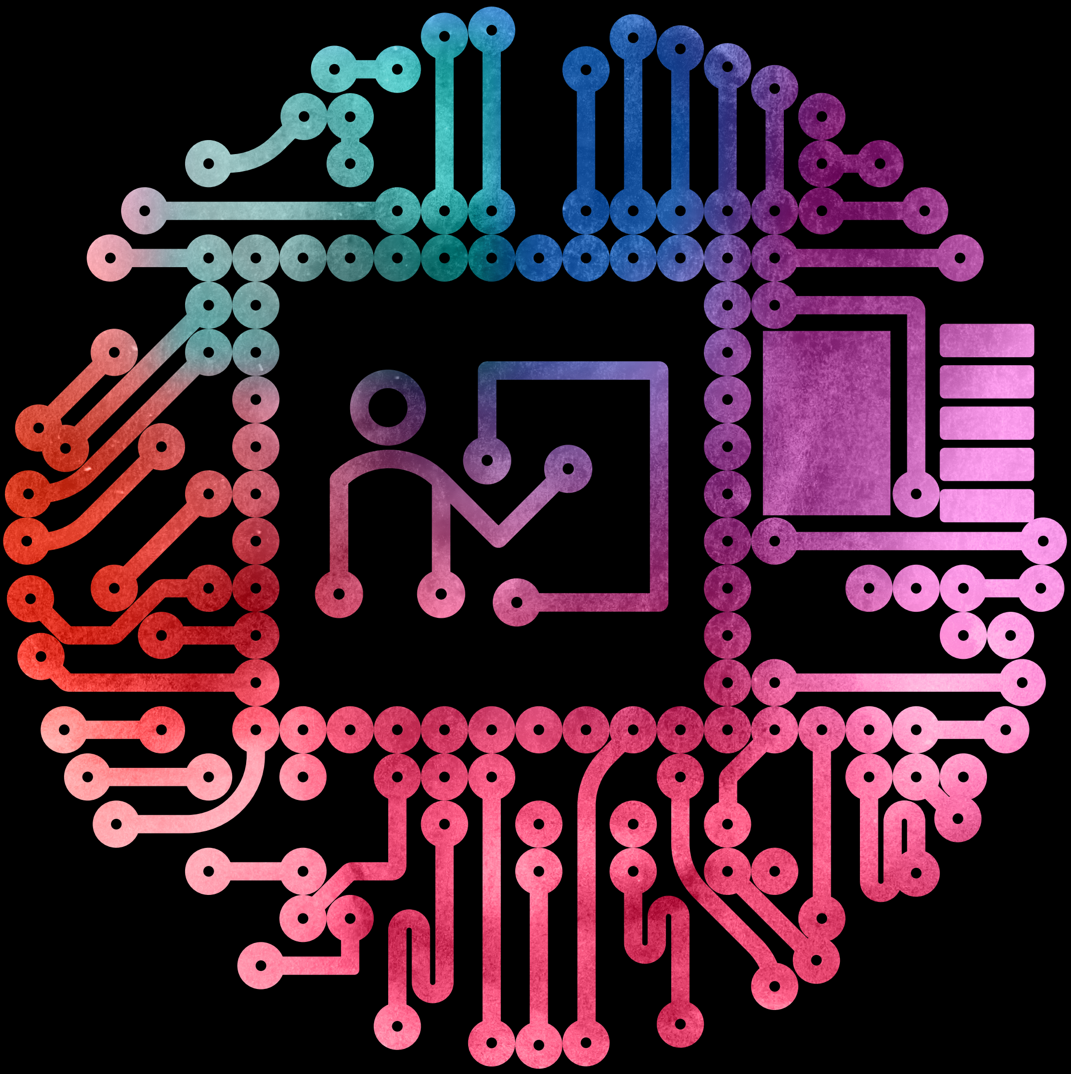
Deloitte.



Be the beacon

Leadership to build and manage as a CISO

May 2021

MAKING AN IMPACT THAT MATTERS since 1845

Contents

Introduction

Distinctive leadership is ambitious in any context. But when considered in the context of being a CISO, your authority may be relatively new to you or your company, and a firm seat at the C-suite table is not guaranteed.

The perception of your role varies, as does the power assigned to it. And then there's our ever-shifting business world; even before COVID-19 hit, unprecedented challenges were manifesting in markets, customers, ideas and talent,[1] driven largely by the sheer speed of technological, social and economic change.[2] As a CISO, there's no question you're a leader, but you may sometimes be acutely aware of the challenges.

Today's context brings tests of all descriptions, and we should all be taking a moment to recognise that new leadership competencies are needed to succeed across the business world.[3] This paper offers first-hand insights and research into what it means to excel as an **inclusive leader** while you build and maintain a cyber-security capability, and highlights key qualities for your immediate attention. You may think all a CISO needs is to show resilience: someone who can be trusted to hold up the beacon when a storm hits. But tapping into other competencies can elevate your role and unlock opportunities to extend your reach.

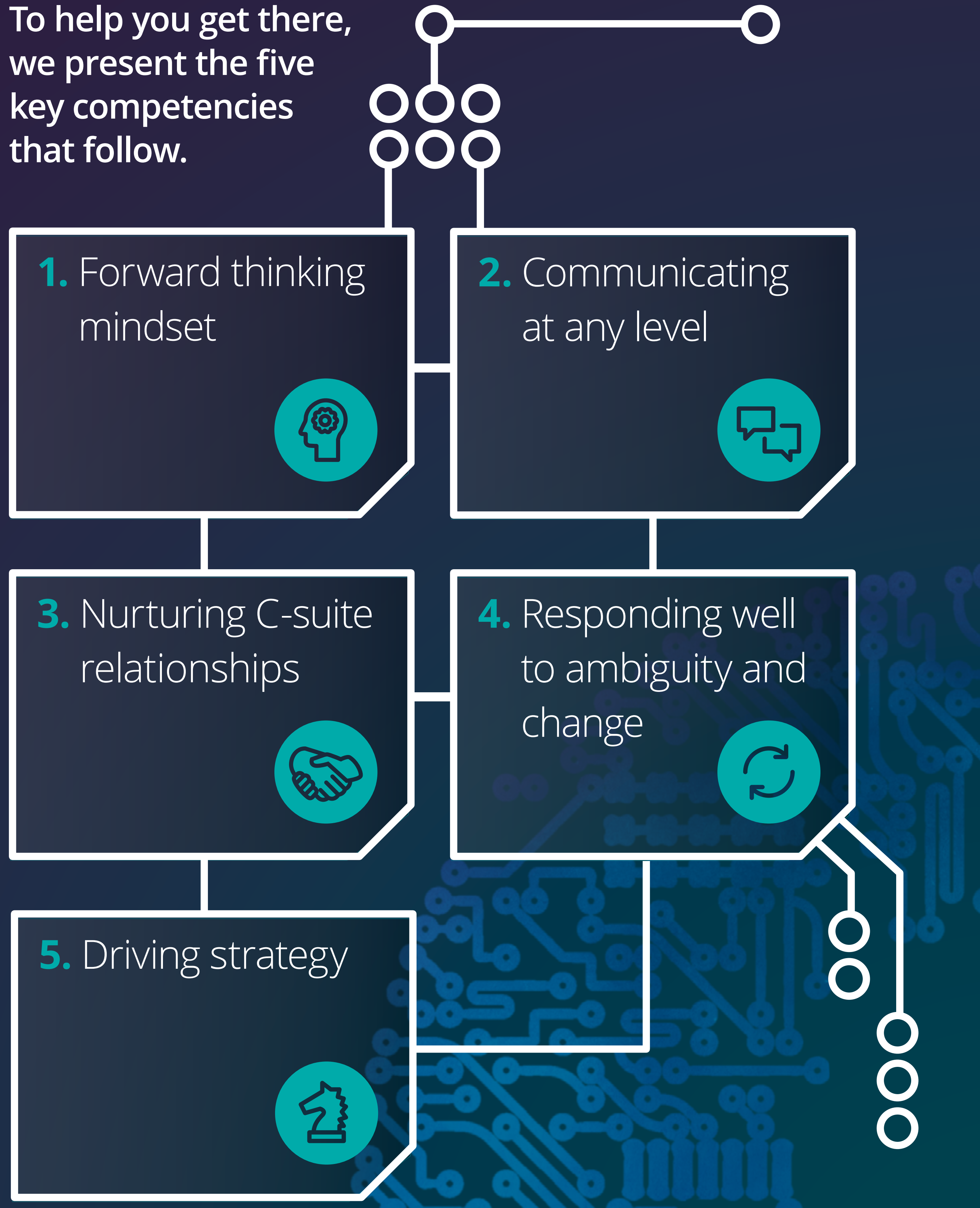
We'll explore the perception of the CISO role, and how you can best fit with your organisation's culture and structure to exceed expectations. This will take some work – in developing relationships and strengthening your leadership abilities – but the payoff will be worth it. As an inclusive leader, you'll no longer be someone just holding up the beacon in a stormy world, but someone who is that beacon.

As an inclusive leader, you'll no longer be someone just holding up the beacon in a stormy world, but someone who is that beacon.

Inclusive leadership 101

Inclusive leaders are well placed to succeed in our increasingly diverse and evolving environment.[4] They've achieved a symbiotic mix of traditional and new leadership skills, with a style comprising: cognisance of bias, curiosity, cultural intelligence, collaboration, commitment and courage.[5] The inclusive leader focuses on recognising talent and capabilities in unusual places, understanding other cultures and showing empathy toward them, and championing diverse ideas and people.

To help you get there, we present the five key competencies that follow.



1. Forward thinking mindset

2. Communicating at any level

3. Nurturing C-suite relationships

4. Responding well to ambiguity and change

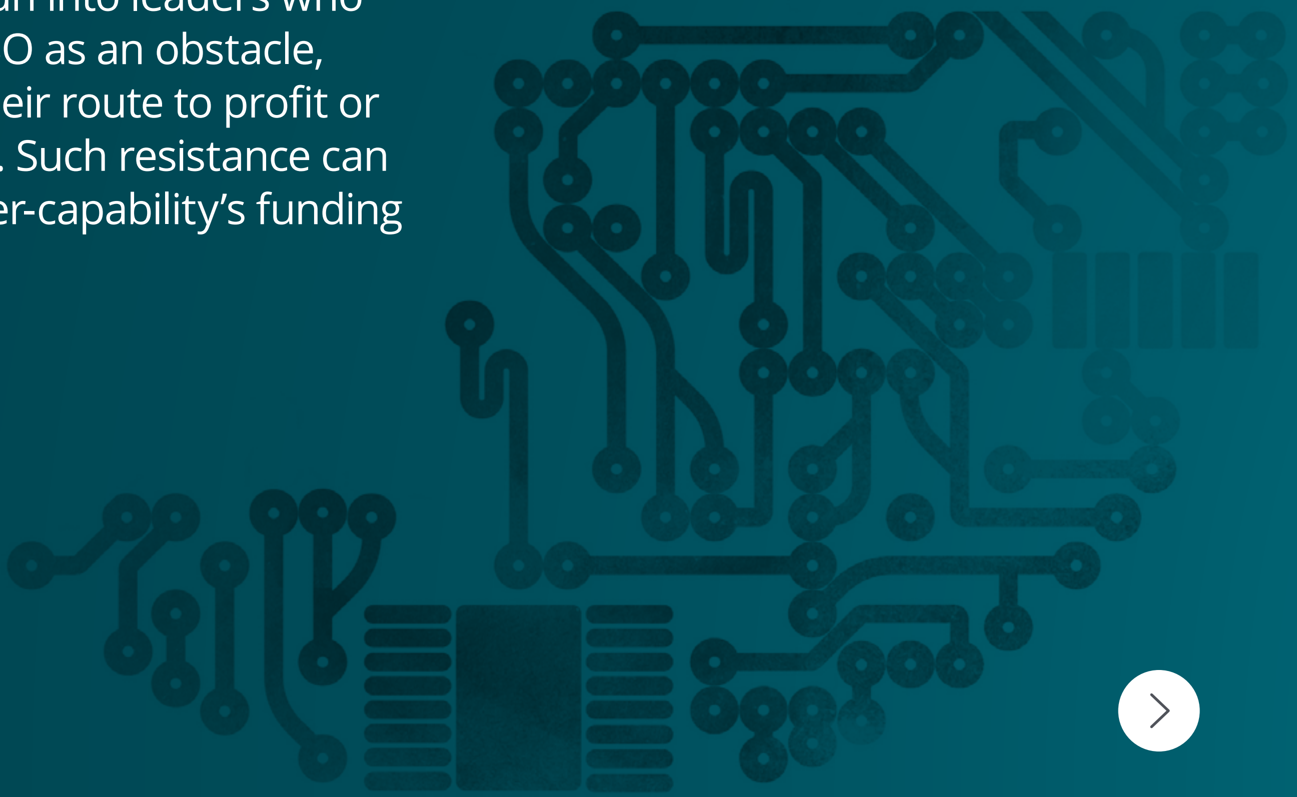
5. Driving strategy

1. Forward-thinking mindset

Building a cyber-security capability

The CISO tasked with building or evolving a cyber-security capability and team has their work cut out for them. Even though the business world has largely acknowledged how critical cyber-security is, your organisation may still be adjusting to its sustained elevation at the top table and the investment required. They may not be aware of its holistic, intrinsic value, let alone its financial value. You may even still run into leaders who see the CISO as an obstacle, blocking their route to profit or innovation. Such resistance can limit a cyber-capability's funding and reach.

Your key to hitting the ground running will be finding a reliable source of information about your organisation. According to former Edmond de Rothschild CISO Cedric Nabe, who is now Head of Risk Advisory for the Romandie Region in Deloitte Switzerland, "What you need to do is be a strategist, and understand the business: where we are today, but also where we're going." With a full, detailed picture, you can identify the organisation's cyber-risk position and determine how to work within it; but if you develop capabilities based on legacy skills and environments, you're failing. Look beyond the existing situation to what will – or should – unfold tomorrow, to stay a step ahead of security needs.



click to return to **Inclusive Leadership 101**

Developing a cyber-security team

Make sure there's a member of your team who is designated to support you in building your organisation. Both of you will need to accept the reality that there will be budget constraints, requiring a balance of operational expenditure with capital expenditure. In securing the right people for your internal team; you may decide that outsourcing will be a better match for certain aspects of your operation, and the IT environment. Again, know your organisation, and learn to work within its limits.

A diverse business world demands diverse thinking and experience. When recruiting for your cyber-security team, look beyond the traditional career path to find people who will bring unconventional ideas and solutions. Good talent is often overlooked if a candidate is not seen to fit a conventional mould, but here's where your inclusive leadership mentality can open up doors. Is a technical degree really necessary for your go-to responder? And couldn't a business analyst be just as valuable as a technical guru – especially when you need support as a C-level strategist?

The typical cyber-security team is a tight-knit bunch. This might be because they can be seen as outsiders, on the periphery of mainstream business acceptance, even if those outsiders are helping their organisation dodge risks on a daily basis. This breeds a certain degree of loyalty, but it doesn't guarantee they'll retain loyalty for their CISO; as with any professional group, they want to be led by someone who empowers them, believes in them and invests in their career. If you're spending all your time as a CISO worrying about handling relationships outside your team (e.g., other executives, your peers), you're ignoring your most important asset and you stand to lose it.

Prioritise developing your team's skills and ensure a formal training plan is in place, focusing on any weaknesses you've spotted and key competencies needing development. Give them the tools to stay relevant, and a dynamic environment with sufficient time to grow. Above all, seek to build autonomy and trust within your team. If you can equip them with the right tools and skills, you can count on them to support you in a multitude of ways.

Developing talent also means demonstrating empathy, and encouraging it of others; allow your team to ask bold questions and look at a problem through a new lens. As discussed in the next section, you need to speak several 'languages' as you communicate with the business, and you should advocate that your team members learn the same skill. Inclusive leadership means seeing a different perspective, and adapting to/around it.

2. Communicating at any level

Communication is a key competency to develop alongside your other leadership skills, and this doesn't just extend to directing your team or delivering presentations. You should be pitching each discussion, from the board room to the casual run-in, at a level appropriate to your conversational partner. Recognise when their knowledge of technical terms and concepts is limited, and speak the language that will resonate with them. Also, don't waste their time with insights that aren't directly relevant to them. If your listener is concerned with regulatory compliance, talk about your data privacy efforts. If you've got the CFO's ear, talk about what a breach could cost.

> "You should be pitching each discussion, from the board room to the casual run-in, at a level appropriate to your conversational partner."

click to return to **Inclusive Leadership 101**

Of course, communicating with the C-suite or the board is paramount, and so is being able to effectively convey cyber-risk to them. According to Steve Knight, former Technology Risk Managing Director, "Being able to offer high-level advice is key," and good CISOs can articulate risk in ways others can both make sense of, and can meaningfully respond to.

Telling an executive that a cloud service is not secure won't prevent them from buying it, because cost and efficiency will win. Instead, "you have to have a message that's a bit more nuanced," says Steve, who is now Senior Manager in Cyber Risk, Information Security and Privacy in Deloitte UK. "The CISOs who will flourish and lead in this environment of persistent and pervasive change are the ones who will know the relevant principles to lay out, without being proscriptive."

Again, this is a question of knowing your audience – and the company's situation. To garner understanding and support, you should be framing risk within a specific reality. How will your efforts aid particular aspects of the business? How will you actually cut costs by investing in cyber-security? And how do your initiatives align with the overall business strategy?

A final consideration about communication is the setting. If you have a new initiative, executives shouldn't be hearing about it for the first time in the board room. That's a better environment for the final green light, so find another setting to engage C-suite executives in advance. Use private discussions to float ideas and feel out any opposition they might have, then talk through their concerns.

> "The CISOs who will flourish and lead in this environment of persistent and pervasive change are the ones who will know the relevant principles to lay out, without being proscriptive."

3. Nurturing C-suite relationships

Engaging the C-suite is not just beneficial, it's necessary as C-suite roles and work become more complex and integrated.[6] You'll be expected to work more closely together, especially as offerings are becoming commoditised with the move toward service-centre business models.[7]

This interaction may not come naturally to all C-suite incumbents, owing to their perception of the CISO role. Some CISOs are not seen as equals to their peers, and find their voice is not always heard. Short-sightedness is partly to blame; even if a cyber capability is in place, there will remain individuals – or even organisations – unable to discern its direct value. What's worse, as a CISO you may even be seen as stymying innovative ideas or technologies. Or you might find yourself in the uncomfortable role of a bad-news courier: someone inevitably linked to the very problems they seek to mitigate.

It's not a lost cause. Kjersti Stathopoulou, Cyber Partner in Deloitte Norway, points out that cyber-security sits where IT once did: as a bolt-on, not fully integrated into organisations; but as we've seen with IT, that can change. Kjersti believes the CISO's role will evolve, and rise in prominence, as cyber-security becomes "something that you can't opt out of". Kjersti also forecasts that with a continued increase in regulations – in the context of a global economy, growing threats and digitalisation – the evolution may even occur at a faster pace. The path to technological transformation and even greater data consumption offers no U-turns, meaning that as security awareness grows, the CISO's influence will probably grow.

click to return to **Inclusive Leadership 101**

Until then, it's up to you as a CISO to present yourself as an advisor to the entire C-suite, brimming with relevant expertise aligned directly with the business strategy. Striving for direct access to the CEO is a smart move in this regard, as it will enable you to nurture their trust, but it's also important to recognise the importance of the CIO; over time there's a chance that succession opportunities for the CIO role may open up for a CISO, and you could be laying the groundwork now to step into that role. Start supporting your CIO and coaching them on security issues, to help you both understand how security is a piece of the bigger puzzle and how to best convey that piece to other executives.

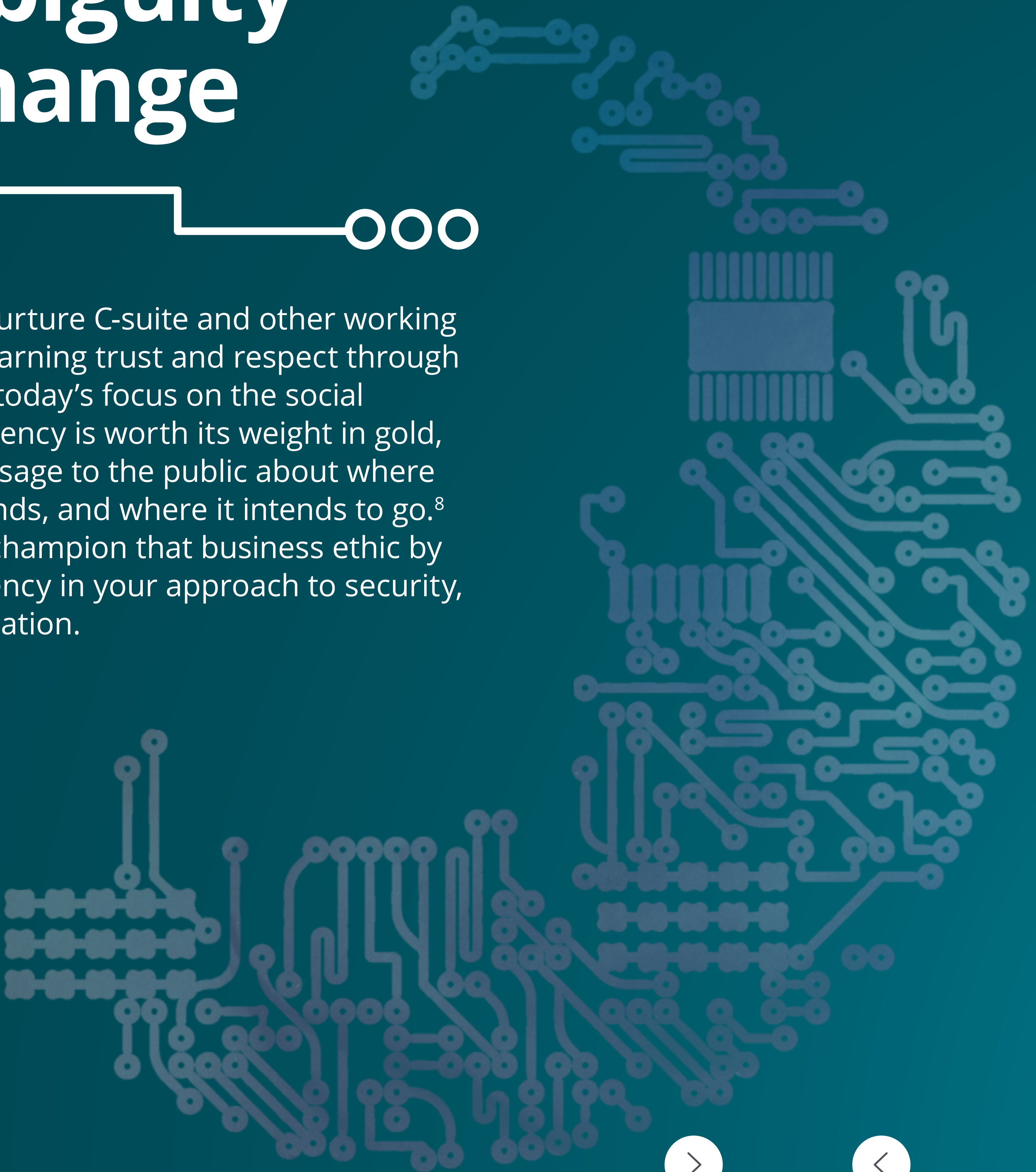
Another relationship you'll want to manage carefully is with the ubiquitous 'armchair' cyber-security expert: that colleague from another department who's read about the latest threat and is convinced they know the right action to take. The best space to indulge these individuals is behind closed doors, where you can win their approval before you enter a formal meeting.

A final word of advice on relationships: Practice being flexible and adaptable to any person and any situation – key skills for any leader, and certainly one in a C-suite role. Respond to whatever issues come up by getting involved early on; this will help get you into the right meetings with the right people.

> Cyber-security sits where IT once did: as a bolt-on, not fully integrated into organisations; but as we've seen with IT, that can change.

4. Responding well to ambiguity and change

Part of the way to nurture C-suite and other working relationships is by earning trust and respect through transparency. With today's focus on the social enterprise, transparency is worth its weight in gold, sending a clear message to the public about where an organisation stands, and where it intends to go.[8] As a CISO, you can champion that business ethic by practising transparency in your approach to security, and your communication.



click to return to **Inclusive Leadership 101**

It wouldn't be far off the mark to describe cyber-security as being on an up escalator that never reaches the top. Because the threats are constantly evolving, change and ambiguity are constants you must not just accept, but promote. Managing risk means challenging the status quo, but every action should be made fully transparent: A CISO must clearly convey the scale of the concern, the likelihood of falling victim to a threat and how your actions will help. It's also your responsibility to remind leaders that you can never really have everything under control; the threats will keep coming, the hackers will always be two steps ahead, and the sooner you come clean about that, the sooner they'll learn to trust you.

You may be perfectly comfortable working in a volatile environment, sizing up a future that presents enormous uncertainty. But your organisation might have a different comfort level, so strategize carefully before you explain a situation. A CISO is often the bearer of bad news, but you'll serve no one well by dancing around the dangers. Aim to strike a balance between reassurance and caution, being clear about what is at risk, but also projecting confidence about what can mitigate the risks. By accompanying warnings with specific, actionable suggestions, you can show that you're at ease with ambiguity and change, because you respond to it quickly and effectively.

Managing risk means challenging the status quo, but every action should be made fully transparent.

5.
Driving strategy[6]

The final competency to add to your CISO arsenal is learning to drive strategy. Leaders who fail to look beyond their own unit, to sync up with the overall business strategy, risk being viewed as not fully engaged with the challenges of the broader business and social environment.[10] In Deloitte's CISO Transition Labs, we describe CISOs as having four faces (see Figure 1), dividing their time among the roles of guardian, technologist, strategist and advisor. But for most, there is an imbalance – often tipping in the direction of technologist/guardian of the business.

With more than a handful of CISOS having risen through the ranks of a technology career, it isn't surprising to find out many still spend most of their time fighting cyber-security 'fires'. But the business expects you to show all four faces, even if the harsh truth is that you're spreading yourself too thin.

If you're a technologist, work on becoming a strategist. How can you shift your approach and working style to accommodate this new angle? This goes back to knowing the business and how your work fits into it – in terms of not just protection, but enablement. The cyber-security capability should enable the wider organisation to fully embrace a customer-centric approach, to innovate confidently and to invest smartly.

> Speak the language, and be ready to address all questions.

click to return to **Inclusive Leadership 101**

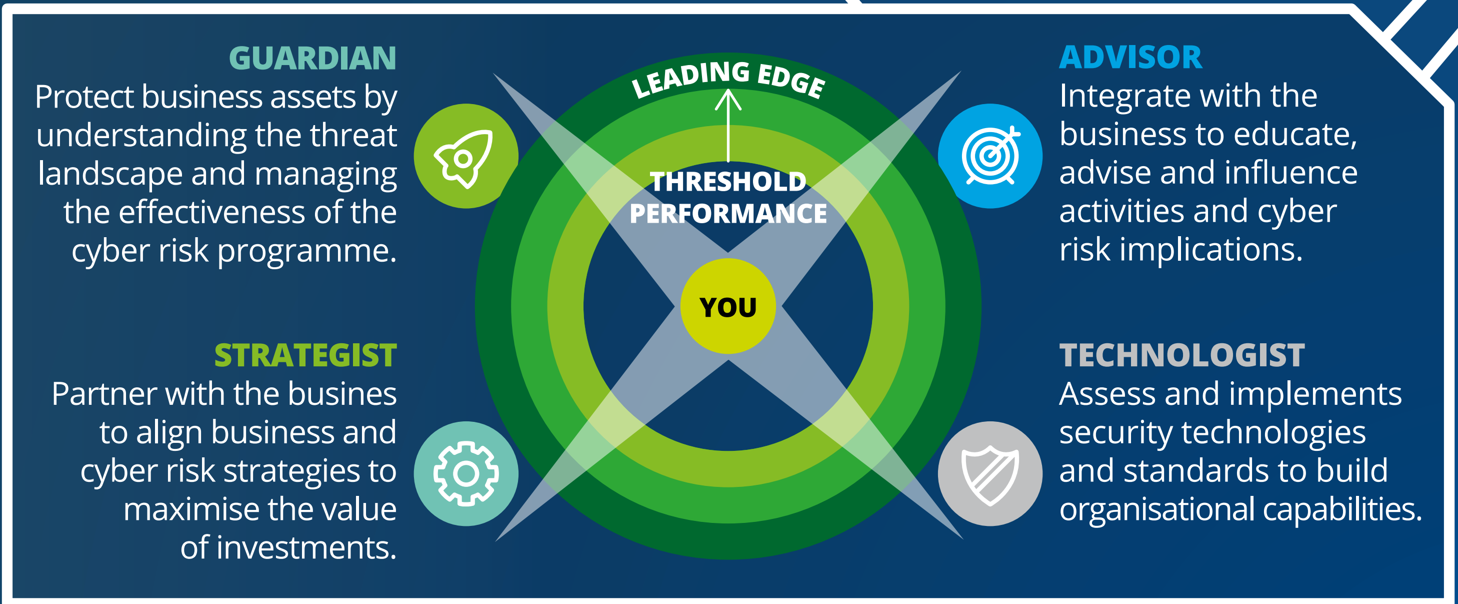
To beef up your knowledge of the business, start with determining how each department drives growth and sales, gaining a better understanding of non-IT business functions, and improving your business and commercial acumen. Your ultimate objective should be staying abreast of the business's values and plans for innovation, so you can align your team's initiatives with the overall strategy.

Becoming more strategy oriented also demands that you become more risk driven. You should be linking cyber initiatives to a risk, quantifying and qualifying the impact if that risk is not managed. Beyond knowing what the threats are, figure out what the business stands to lose. The C-suite wants to know exactly what's at stake, in language they will related to, and your intimate familiarity with the business's exposure and vulnerabilities will give them a clear picture and a pathway to making decisions.

Fundamental to driving strategy is being able to articulate cyber-security's financial value. If you understand the business and how it earns a profit, and are interested in its performance, you can better position your capability within that profit-making model. Rather than just dangling threats in front of the C-suite, point out opportunities to save and make money. Remind them that, in a world of cloud technologies, market share can actually increase if customers see that your company is taking security seriously.

By the same token, if you're a strategist – a savvy business analyst who can slide confidently into a seat at the executive table – get to know the technical guru inside you. Speak the language, and be ready to address all questions.

Figure 1. Four Faces of the CISO



GUARDIAN
Protect business assets by understanding the threat landscape and managing the effectiveness of the cyber risk programme.

ADVISOR
Integrate with the business to educate, advise and influence activities and cyber risk implications.

STRATEGIST
Partner with the busines to align business and cyber risk strategies to maximise the value of investments.

TECHNOLOGIST
Assess and implements security technologies and standards to build organisational capabilities.

Beyond competencies

Find support to lead
Leading as a CISO is demanding; don't shy away from seeking informal feedback from others about whether you're hitting the mark.[11] More importantly, support yourself by finding people among your stakeholders who can support you.

According to Wim Boonstra, a Deloitte Netherlands Cyber Security Programme Leader, the structure you oversee "is not a democracy, but it's also not a dictatorship". Wim explains: "You need relationships to bring your security vision to your organization. Your few direct reports won't be enough. As a CISO you cannot mandate your ideas as a CEO sometimes can." As you make efforts to engage with stakeholders, think about who could act as your unofficial sponsor at the C-suite level – the CIO, ideally, and one or two other people who have an interest in your efforts.

Working toward the end goal
Inclusive leadership isn't easily won. It means putting aside paradigms, looking beyond yourself to observe and react, and breaking through resistance. It also means investing time and effort in developing the key attributes discussed above: a forward-thinking mindset, communicating at any level, nurturing C-suite relationships, responding well to ambiguity and change, and driving strategy.

Yes, you'll somehow have to find extra time, but as a CISO in an ever-shifting context, you can't afford not to work on these competencies. Invest in yourself, and your reward will be confidence to lead through the next big change. And when the going gets tough, remember that by wearing the CISO leadership badge you've opened yourself up to new career opportunities in security – ones that may never otherwise have surfaced. This is an exceptional time for growth: to learn and shape your abilities, and your image. And at the end of the day, your visibility as a C-suite leader gives you influence that enables you to make a real difference, shining a light even beyond the boundaries of your organisation.

Endnotes

1. Bernadette Dillon and Juliet Bourke, "The six signature traits of inclusive leadership: Thriving in a diverse new world," Deloitte University Press, https://www2.deloitte.com/content/dam/Deloitte/au/Documents/human-capital/deloitte-au-hc-six-signature-traits-inclusive-leadership-020516.pdf
2. Erica Volini, Jeff Schwartz and Indranil Roy, "Leadership for the 21st century: The intersection of the traditional and the new," Deloitte Insights, 11 April 2019, https://www2.deloitte.com/global/en/insights/focus/human-capital-trends/2019/21st-century-leadership-challenges-and-development.html
3. Bernadette Dillon and Juliet Bourke, "The six signature traits of inclusive leadership: Thriving in a diverse new world," Deloitte University Press, https://www2.deloitte.com/content/dam/Deloitte/au/Documents/human-capital/deloitte-au-hc-six-signature-traits-inclusive-leadership-020516.pdf
4. Bernadette Dillon and Juliet Bourke, "The six signature traits of inclusive leadership: Thriving in a diverse new world," Deloitte University Press, https://www2.deloitte.com/content/dam/Deloitte/au/Documents/human-capital/deloitte-au-hc-six-signature-traits-inclusive-leadership-020516.pdf
5. Bernadette Dillon and Juliet Bourke, "The six signature traits of inclusive leadership: Thriving in a diverse new world," Deloitte University Press, https://www2.deloitte.com/content/dam/Deloitte/au/Documents/human-capital/deloitte-au-hc-six-signature-traits-inclusive-leadership-020516.pdf
6. Erica Volini, Jeff Schwartz and Indranil Roy, "Leadership for the 21st century: The intersection of the traditional and the new," Deloitte Insights, 11 April 2019, https://www2.deloitte.com/global/en/insights/focus/human-capital-trends/2019/21st-century-leadership-challenges-and-development.html
7. Erica Volini, Jeff Schwartz and Indranil Roy, "Leadership for the 21st century: The intersection of the traditional and the new," Deloitte Insights, 11 April 2019, https://www2.deloitte.com/global/en/insights/focus/human-capital-trends/2019/21st-century-leadership-challenges-and-development.html
8. Erica Volini, Jeff Schwartz and Indranil Roy, "Leadership for the 21st century: The intersection of the traditional and the new," Deloitte Insights, 11 April 2019, https://www2.deloitte.com/global/en/insights/focus/human-capital-trends/2019/21st-century-leadership-challenges-and-development.html
9. Erica Volini, Jeff Schwartz and Indranil Roy, "Leadership for the 21st century: The intersection of the traditional and the new," Deloitte Insights, 11 April 2019, https://www2.deloitte.com/global/en/insights/focus/human-capital-trends/2019/21st-century-leadership-challenges-and-development.html
10. Erica Volini, Jeff Schwartz and Indranil Roy, "Leadership for the 21st century: The intersection of the traditional and the new," Deloitte Insights, 11 April 2019, https://www2.deloitte.com/global/en/insights/focus/human-capital-trends/2019/21st-century-leadership-challenges-and-development.html
11. Bernadette Dillon and Juliet Bourke, "The six signature traits of inclusive leadership: Thriving in a diverse new world," Deloitte University Press, https://www2.deloitte.com/content/dam/Deloitte/au/Documents/human-capital/deloitte-au-hc-six-signature-traits-inclusive-leadership-020516.pdf

Acknowledgements

If you would like to discuss any topics discussed or if you have any feedback regarding this paper, please contact us NSEDeloitteCISOprog@deloitte.co.uk

Peter Gooch
Cyber Partner, UK
UK CISO Programme Lead
pgooch@deloitte.co.uk

Kjersti Stathopoulou
Cyber Partner, Norway
kstathopoulou@deloitte.no

Cedric Nabe
Head of Risk Advisory for the Romandie Region, Switzerland
cnabe@deloitte.ch

Steve Knight
Cyber Risk Senior Manager, UK
srknight@deloitte.co.uk

Wim Boonstra
Cyber Security Programme Leader, Netherlands
wboonstra@deloitte.nl

Rosie Shepherd
Cyber Marketing Lead, UK
rshepherd@deloitte.co.uk

Deloitte.

This publication has been written in general terms and we recommend that you obtain professional advice before acting or refraining from action on any of the contents of this publication. Deloitte LLP accepts no liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 1 New Street Square, London EC4A 3HQ, United Kingdom.

Designed and produced by 368 at Deloitte, London. J20952