EMBRACING CHANGE

Next-generation CISOs who grasp the changes required are starting to transform how information security operates and is viewed inside and outside their organisation. Leading by example and sharing their knowledge, experience and passion for security, these CISOs are often high profile, technically adept and focused on endowing their organisation with a secure culture.

The next-generation CISO is becoming a skilled communicator who is gaining a unique insight into how the enterprise operates and proves pivotal to its improvement and advancement.

ABOUT THIS BRIEFING PAPER

This briefing paper sets out the range of disciplines a next-generation CISO can be expected to master. It draws on desktop research, testimony from 40 CISOs at Member organisations, a dedicated survey and interviews with subject matter experts. These have highlighted how those leading the information security function can react, grow and ultimately prosper when confronted with uncertain times.

It will help CISOs (and those that aspire to the role) to:
- understand the forces shaping the role of the CISO
- identify and recognise where CISOs are being stretched
- explore ways CISOs can improve and future-proof their skills and value.

As digital transformation drives organisations to become more agile and responsive, the Chief Information Security Officer (CISO) faces demands to quickly prove their worth as an enabling force, while protecting the business in an increasingly turbulent risk environment. Becoming a next-generation CISO requires an individual to embrace and master new skills and disciplines, making themselves indispensable, future-proof and highly sought after.

Figure 1: How CISO skill sets have changed

The briefing paper continues the ISF’s focus on the role of the CISO — a research effort that has charted 15 years of change and adaptation. Figure 1 shows the steady accumulation of skills and qualities that CISOs are now expected to embody. Since the last ISF report on the subject in 2013, the demands placed on CISOs have reached extraordinary levels, encompassing almost all previous responsibilities. They also face novel high-level threats such as state-sponsored attacks and global pandemics. All require the CISO to respond quickly and demonstrate their worth.
1 Forces shaping the CISO

The Chief Information Security Officer is coming under pressure from many different directions. Whether this is external, internal or personal, these forces have combined to create a situation that demands a new approach – one that the next-generation CISO is pioneering.

The role of the CISO has always been in flux, largely because there has never been a succinct and exacting definition of what the CISO is expected to do. Instead, the CISO often acquires tasks and responsibilities that have traditionally had no clear business owner. It is a position that has become defined by personality, history, practice and the demands of individual organisations, rather than through clearly defined policies and procedures. Next-generation CISOs will need to respond to these forces and take a keen interest in a wide variety of topics to stay at the top of their game.

EXTERNAL FORCES

Many of the forces shaping the role of the CISO derive from the wider environment in which organisations operate. Such forces include a rush to digital technology, an overwhelming regulatory burden and the occurrence of disruptive events.

The rush to digital technology

While CISOs are having less direct involvement in technical operations, they increasingly need to understand and react to successive waves of technological innovation. Each wave (shown in Figure 2) has brought about significant changes in how organisations operate, enabled novel working practices and reshaped interactions with customers and suppliers, requiring the CISO to adapt to handle these constant changes.

Figure 2: Successive waves of innovation

Over the last seven years society and business have changed significantly, with technology at the fore. They have seen the rise of the gig economy, numerous disruptor start-ups, big data and challenger banks – all of which are forcing organisations to respond. This has, in turn, added to the pressures on the CISO and the information security function to ensure the risks are appropriately managed.
In 2020, change is again being borne on the back of a technological shift, but it is one with a different quality. Instead of technological improvements forcing businesses to change, organisations are now using technology to disrupt themselves, helping them to keep pace in a crowded marketplace. These technological changes will always form part of the CISO’s remit, so CISOs need to remain focused on understanding how these changes impact their organisation. Above all, given findings which suggest that less than 25% of business executives see information security as a “proactive enabler of digital transformation”,\(^1\) they need to be vocal advocates of good security practice.

---

### The overwhelming regulatory burden

Regulation has been an intrinsic part of the CISO’s journey over the last 20 years. The burden of regulatory compliance has steadily increased and, thanks to the material fines associated with directives such as the EU General Data Protection Regulation (GDPR), it has now become a regular item of debate in board rooms and among senior executives – heightening the onus on the CISO to ensure that the organisation achieves compliance.

The CISO is often seen as the face of regulatory compliance and can represent their enterprise in dealings with regulators and other oversight bodies. For organisations that operate across the globe this can be a considerable overhead, with multiple regulators in different jurisdictions to contend with.

Recent regulation has highlighted the importance of ethical walls and avoiding conflicts of interest, reigniting the debate over separating information into its own autonomous function and which line of defence it should occupy.

For a long time, and particularly in financial organisations, information security resided in the first line. Increasingly, regulation has made its position more uncertain and now it straddles two or more lines of defence, often uneasily. This undermines the separation it is intended to enshrine.

The survey conducted alongside this research revealed that 53% of CISOs were in the second line of defence but a minority, 25%, were across two or more lines.

Next-generation CISOs believe it does not matter where the information security function sits. The important step is establishing its mandate and governance framework. This clarity helps define the mission and reduce the ambiguity around the roles and responsibilities of the security function and who they report to.

### Disruptive events

Non-security incidents can have a substantial knock-on effect within the information security spectrum. In 2020 the striking example has been the global COVID-19 pandemic. This forced digital change on organisations at high speed and certainly faster than many had dealt with before. It meant that senior security managers have been called on to refocus efforts and help their organisation reorientate around secure remote working practices. They also had to ensure supply chains remain secure and roll out tailored security awareness campaigns and training, for example to combat the sudden flood of phishing scams related to COVID-19.

COVID-19 represents both a crisis and an opportunity. It has accelerated and concentrated forces, such as the move to remote working and adoption of cloud services, that were already in motion. CISOs must be willing to respond to non-information security-related threats if they have a significant impact on the way an organisation operates or threaten its technical infrastructure.

---

INTERNAL FORCES

Organisations strive to change constantly, and that continuous improvement mantra will inevitably shape the role of a CISO. It subjects the CISO to pressures that include evolving methodologies and changing approaches to security measurement.

Evolving methodologies

Digital transformation changes the way organisations operate and how they develop software. It can often mean the adoption of agile methodologies, DevOps and SecDevOps and other techniques to help speed up the pace at which organisations produce, test and deploy code – typically to service a broader organisational change. CISOs should become familiar with these techniques and how they demand quick responses – far faster than was previously required to check and sign-off development work. It can also force changes in infrastructure that put more demands on the security function to secure the extra resources, such as cloud-based software repositories, which development teams start to require. CISOs need to amend thinking, procedures and practices to account for this significant change in speed and culture.

The shift to faster software development represents an opportunity for next-generation CISOs to be involved with the fast-moving operational end of the business and to demonstrate their value by including security in these evolving practices. Early and continuous involvement can also reduce the technical debt that these projects can accrue if they are left to proceed without security oversight.

Next-generation CISOs join, or embed, their staff in accelerated projects and agile teams because they know that being present during the early discussions will help security receive the attention it requires. This allows them to demonstrate their value to the business, win allies and help them gain a better sense of technology use across the enterprise. They are also aware that no matter what approach an organisation takes to development, it is the outcome that is important.

Changing approaches to measuring security

Information security departments, as well as their individual functions, often make use of a maturity curve to demonstrate the steadily growing sophistication of their activity. CISOs are familiar with these models and use them to locate themselves, and other departments, on this curve and to guide their strategy.

However, many recognise shortcomings in maturity models – for example, they need to be tailored to the subtleties of each organisation, often lag behind technical innovation, do not account for external events and can distract information security staff from more pressing needs.

Increasingly, maturity models are being combined with risk management as a means of refining approaches to information security and helping it become more relevant to the organisation’s way of doing business.2

Moving from a maturity model-based approach can put pressure on the CISO to resolve and justify the adoption of a more risk-based approach. The shift involves discovering and cataloguing organisational assets, determining the current level of control implementation and accurately profiling threats to assets, which enables controls to be implemented or improved.

---

PERSONAL FORCES

The high-profile nature of the role and a skills shortage have resulted in human and personal factors becoming prominent. These factors relate to issues around shaping the role, improving personal brands and managing careers.

Shaping the role

Information security as a profession has never been static. It is always evolving in line with innovations in technology and the threats to infrastructure and data. Leaving aside the constant innovation that challenges CISOs to gauge the effectiveness of new tools and technologies, there are continuous debates within the industry about novel approaches such as using quantitative techniques for information risk assessment. In addition, many CISOs are keen to stand out in their organisation by shaking up the internally held view of information security and surprising their colleagues with innovative approaches.

Improving the personal brand

The global impact of cyber attacks and the role of information security in combatting them has put a spotlight on the role of the CISO, the individual themselves, and their ability to corral teams to mitigate risks. Increasingly, CISOs are expected to be public figures happy to share their views on breaches, attacks, and what counts as good practice when responding. The debate around information security has become louder thanks to a wealth of industry groups, social media platforms, conferences and media opportunities keen to hear about all aspects of the industry. Participation in these gatherings gives CISOs the chance to showcase their good work, celebrate success and help raise their own profile. Increasingly employers expect a CISO to be recognised in the industry for their views and to have the connections that can help them succeed.

Managing careers

CISOs are also facing pressure to take a more hands-on approach to their career and worth. As recently as 2017 the average tenure of a CISO was about 36 months, yet a survey released in 2020 suggested this had now shrunk to about 18 months. Many CISOs will move regularly from organisation to organisation throughout their career. Given their short tenures, it makes sense for CISOs to gain a better insight into the qualities that will help them secure their next position and how to cultivate those qualities.

As the profile of the CISO role has increased, other senior leaders have recognised that their own success can be closely linked to the success of their CISO. This creates personal alignments and an arriving Chief Information Officer (CIO) at an organisation is very likely to bring their own choice of CISO, i.e. someone they feel they can trust, but then also take that same person with them on their departure.

All of these factors create dynamism in the role and can mean that CISOs have to keep one eye on the exit at the same time as they help an organisation navigate significant change.

Maintaining good mental health

Being a CISO is not easy. Many organisations suffer from a “blame culture” that can mean the CISO takes the blame when an organisation is exposed by a serious breach or cyber attack. This can impose significant stress and a mental burden that can be hard to handle. One survey of senior industry figures suggests almost 20% are either medicating or using alcohol to cope with the burden of their responsibilities. Many CISOs are pushing back and finding ways to help manage their mental well-being. Organisational changes, that require the functions which incur risk to own it, can help diffuse the blame culture and lighten the load on the CISO. Another approach has seen some CISOs seek outside help to manage stress or seek to set up a working culture that makes it easier to strike a work-life balance so that they, and their employees, can leave their job behind when they go home.

The next-generation CISO acknowledges the operational demands of the role, but protects their well-being by appointing a strong deputy and empowering them through delegation.

The forces that are acting on the information security function will inevitably shape the form of the next-generation CISO. Whilst there is not an exact one-to-one mapping, the effect of those forces is illustrated in Figure 3 and explored in the next section.
2 How next-generation CISOs react

All these external, internal and personal forces have combined to put a tremendous amount of pressure on CISOs, raising expectations about the wide range of responsibilities they should take on and the fields of knowledge in which they are presumed to be an expert. Inevitably this has harmed many CISOs – up to 27% experience so much pressure that it affects their ability to do their job.6

While CISOs collectively exert command over a vast array of technical and managerial disciplines, individual CISOs are adept in some areas and novices in others. This is largely because of the different routes through which they have joined the industry and gained their experience. Figure 4 shows the range of CISO backgrounds – with technical origins predominating.

Figure 4: CISO backgrounds (Source: ISF Member survey)

This section provides more detail about what next-generation CISOs are doing that will help to reshape the role in the future. It identifies six differentiating characteristics:

1. BALANCING OPPORTUNITY WITH RISK
2. DEMONSTRATING LEADERSHIP
3. MANAGING INCIDENTS AND CRISSES
4. FINDING THEIR OWN VOICE
5. DEALING WITH REGULATORY VOLUME
6. HANDLING TECHNOLOGY

These six do not stand alone – there are many other factors in the make-up of the next-generation CISO, but these six characteristics stand out as key differentiators of forward-looking professionals.

---

### 1. BALANCING OPPORTUNITY WITH RISK

“Never say you can’t do this – you have to phrase the message in a different way and offer an alternative route through.” – ISF Member

Next-generation CISOs are adept at helping the organisation make the most of its commercial opportunities without straying beyond its risk appetite. This characteristic underlines the privileged position that next-generation CISOs fashion for themselves. Advice is expected and welcomed because next-generation CISOs are diplomats who have done the work to ensure they are visible to many other parts of the organisation and are seen as an enabler rather than a blocker. They have secured the strong support of senior staff, audit committees and other stakeholders. This can be a powerful and influential position.

Next-generation CISOs work to create the reporting structure around themselves and their role. Figure 5 shows that the largest proportion of CISOs report to the CIO. Next-generation CISOs set up reporting lines outside IT to emphasise their independence and keep in contact with more senior executives while still maintaining a link with the IT chief.

The importance of balancing opportunity with risk is emphasised by ISF survey results that looked at the focus of current CISOs. At the top of the list of activities that occupy most of a CISO’s time is “helping projects in other parts of the business consider security early on”. There are many ways to accomplish this with some Members using information about like-for-like initiatives adopted by industry peers to illustrate risks and solutions.

Many CISOs, or their team members, set the security backdrop to every project by defining the policies and practices that developers and others are expected to work to. They have established intranet-based repositories of building blocks or catalogues of controls that development teams can use to initiate projects. Setting these standards is especially important when organisations adopt agile and other fast-moving development methodologies. Next-generation CISOs go further by actively consulting on bigger projects and giving advice on useful approaches.

Next-generation CISOs also ensure that the risks associated with launching new services or products are owned by the department, unit or function that proposed and manages them. Next-generation CISOs provide advice about the risks they are taking on, and whether they cross boundaries set by the organisation’s risk appetite.
Assurance requirements for effective security controls provide the next-generation CISO with an opportunity. By creating mutually beneficial relationships with related functions, such as audit, they can ensure that consistent security messages are generated from multiple stakeholders.

Some next-generation CISOs have gone as far as to embed security staff in other departments so advice is given on the ground as it is needed. These federated models can be part of a broader digital transformation and help the organisation accelerate the speed at which it adapts.

Wide departmental involvement provides next-generation CISOs with the necessary expertise to concentrate on the elements of information security that are essential to maintain business operations. For instance, a mining conglomerate will place much more emphasis on securing the operational systems on site than they would their corporate website. By contrast, a gambling firm would care most about the uptime and response speed of its customer-facing website and the integrity of its payment systems.

**NEXT-GENERATION CISOS FUTURE-PROOF THEMSELVES BY:**

**HOW CISOS CAN DEVELOP THIS**

| Talking about risks to business goals: turn statistics into measures of how well risks are being mitigated. | Stop talking about vulnerability statistics and learn to express such metrics in broader business terms. |
| Informing the business: take time to explain the potential benefits of security innovations and new technologies and how they can create business opportunities. | Seek out novel security technologies. |
| Fixing problems and keeping projects moving: find out about the issues other departments suffer and help to remove the blocks. | Know that there is a time to say “No”. Use this veto sparingly for the things that really matter. |

For practical guidance around producing reports to inform decision making, see the ISF report *Engaged Reporting: Fact and fortitude.*

For more information about setting up a comprehensive assurance programme, see the ISF report *Establishing a Business-Focused Security Assurance Programme: Confidence in controls.*
2. DEMONSTRATING LEADERSHIP

“If you’re a CISO who only has two hands on the keyboard, no, you’re not going to be successful as the CISO of the future.” – ISF Member

Next-generation CISOs are distinguished by their visibility and confidence. They are great communicators and have a view of the world that they seek to convey to senior managers, the board and non-executives. They are regarded as a model of good practice by others in the information security industry and seek to share their experiences via involvement in industry initiatives, as well as networking at professional events, on social media and across broadcast and print media.

Visibility is key because many information security functions, especially those that operate independently of the IT function, can be formed of a very small team – despite the requirement to manage many external parties and vendors providing security services essential to keep the organisation running. Small departments can be overlooked if their leader does not make themselves heard and seen. A strong leader and figurehead is a good start and the next-generation CISO should fill this role. This visibility also helps to foster a secure culture within an organisation – it can remind other departments how seriously the enterprise as a whole responds to security and cement the messages about working securely.

A significant part of this role involves looking after information security staff, but this is complicated by a global lack of experienced staff, resulting in both retention and hiring being time-consuming, expensive and sometimes fruitless processes. Next-generation CISOs therefore seek to reward those already working for them by fostering a working environment that treats them well. Next-generation CISOs know that good leadership promotes loyalty. The visibility of the next-generation CISO, combined with corporate and industry chatter about the strong culture they have embedded, can ease recruitment problems as information security professionals are more likely to apply for roles at organisations where they feel they will be valued.

Some next-generation CISOs assemble a team of experts that they seek to take with them when they move to a new position as they know their success and reputation is bound up with the competencies and skills of the whole group.

Effective leaders attract and retain good people and understand that there is more to a positive working environment than a high salary. They challenge and stretch employees as well as reward success. Next-generation CISOs also recognise that leadership requires them to monitor and manage stress levels among their teams, especially given the high-pressure nature of information security roles, as well as the long hours sometimes associated with them.

NEXT-GENERATION CISOS FUTURE-PROOF THEMSELVES BY:

<table>
<thead>
<tr>
<th>HOW CISOS CAN DEVELOP THIS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Managing visibility:</strong> become known inside and outside their organisation for their views and for their direct contribution to significant and cutting-edge projects.</td>
</tr>
<tr>
<td><strong>Setting their own mission:</strong> establish a clear mission, be comfortable with multiple reporting lines and ambiguity.</td>
</tr>
<tr>
<td><strong>Preparing their successors:</strong> be conscious of their legacy and pass on their view of the world, making sure staff know how to run an information security department in their absence.</td>
</tr>
<tr>
<td><strong>Employing key experts:</strong> find the people within the organisation, or recruit them, who can help the next-generation CISO reach their goals.</td>
</tr>
</tbody>
</table>

For help mentoring staff and creating effective teams see the ISF briefing paper *Building Tomorrow’s Security Workforce*. For more information about helping staff and building culture, see the ISF briefing paper *Human-Centred Security: Addressing psychological vulnerabilities.*
3. MANAGING INCIDENTS AND CRISSES

“CISOs are fired for two reasons; either they had too few incidents, or they had too many.”

– ISF Member

Every CISO will experience major security incidents during their career – a next-generation CISO does not waste the opportunity to demonstrate the value of information security in handling and recovering from incidents. Good incident management also helps to address ongoing queries about the resources an organisation spends on security and controls. Next-generation CISOs work hard to change the security ethos of an organisation and this will involve putting an end to the blame culture still operating in many enterprises.

Interviewees suggest that organisations are dealing with dozens of minor incidents every day. Bigger incidents, requiring the involvement of the CISO and other senior staff, occur on a weekly basis. Next-generation CISOs should position themselves to help with a significant breach as it unfolds, as it is investigated and ultimately dealt with.

Security incidents should not be treated in isolation – instead they should be used as a chance to learn and to improve the organisation’s resilience. Next-generation CISOs use high-level committees, such as audit teams and the risk function, to ensure the lessons learned are fed back to the relevant department, are acted upon, and subsequently assessed to determine their ongoing effectiveness.

While security professionals may become familiar with data breaches and security incidents due to their regular occurrence, the plans put in place to handle them may fall short of what is needed when responding to the most serious, catastrophic attacks. Acknowledging this, next-generation CISOs work to increase their organisation’s resilience to less damaging incidents so the preparations can carry over in the event of a business-critical event.

<table>
<thead>
<tr>
<th>NEXT-GENERATION CISOs FUTURE-PROOF THEMSELVES BY:</th>
<th>HOW CISOs CAN DEVELOP THIS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowing when incidents occur: develop networks, such as access to SOC analysts, to receive notifications of when data breaches and other security incidents occur.</td>
<td>Build strong relationships with key personnel involved in incident handling.</td>
</tr>
<tr>
<td>Being prepared: help to draw up and rehearse response plans and seek out the weak points of their organisation.</td>
<td>Experience security incidents and identify good and bad practice in handling them.</td>
</tr>
<tr>
<td>Adding value to crisis recovery: demonstrate their value by mitigating an incident’s effects and using the information to adjust strategies, by liaising with regulators and law enforcement and ensuring customers are impacted as little as possible.</td>
<td>Study breaches and outcomes in other organisations to understand how these could be handled differently. Share experiences with peers and learn about best practices.</td>
</tr>
</tbody>
</table>

For more information about protecting key assets, see the ISF report *Protecting the Crown Jewels: How to secure mission-critical information assets.*

For help with spotting and reacting to potential security incidents, see the ISF report *Building a Successful SOC: Detect earlier, respond faster.*
4. FINDING THEIR OWN VOICE

“Simplify messages so they resonate with boards – that makes it easier for you.” – ISF Member

Next-generation CISOs are always ready to evangelise their craft to senior executives, board members and non-executive directors. They rehearse key appearances, such as when addressing the board, knowing that it could be one of only a few times during the year when they have the attention of an organisation’s most senior executives. The next-generation CISO also knows that they must map out who their stakeholders are, visit them and identify the risks they worry about the most.

Next-generation CISOs seek out those departments and managers with whom they have had little or no contact or are known to be critical of information security. The forward-looking CISO is happy to find out about problems and do the work to shift attitudes and raise expectations as part of a larger programme of culture change. This work can take many months of diplomacy in order to change views or ensure other functions are onside.

When preparing to present, next-generation CISOs ensure that their language fits the knowledge level of those in the room they are addressing – they should be aware that few board members will share the technical background or understanding CISOs possess.

While many CISOs view presenting to the board as a mark of respect and success, the next-generation CISO knows it is not an easy path. Boards are often very demanding in terms of the information they want, and any report must be backed up by rigorous statistics and metrics.

The easiest time to start being noticed is when a CISO takes up a new post. At this point they are expected to make contact with executives in similar positions, which will help to map out influencers and stakeholders. It is also a good time to ask about the problems that other leaders face and identify straightforward solutions to quickly build trust. Next-generation CISOs also look for activities to set themselves apart from the actions of their predecessor to convey their unique voice in the organisation.

As well as communicating upwards, CISOs should also ensure that their voice is heard across the entire organisation. They need to understand the different views and interests of other functions and maintain links across the enterprise. By being visible and collaborating with others, next-generation CISOs can create a secure culture that consistently embeds good behaviour across the organisation.

Next-generation CISOs use analogies, storytelling and other techniques to bring home to staff the risks they take if they do not follow good practice around security, and the negative impact this can have on family, friends and their employer. Encouraging staff to think about how risks affect them directly can make them more diligent while at work. Above all, the next-generation CISO is an exemplar for good security practice.

<table>
<thead>
<tr>
<th>NEXT-G generation CISOs future-proof themselves by:</th>
<th>HOW CISOs CAN DEVELOP THIS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowing senior executives and board members: know about spheres of influence, key advisors and interest groups. Visit board members in advance to rehearse what they will say and explain their approach.</td>
<td>Study senior executives, visit managers at a similar level in the organisation and learn more about how the organisation operates at an executive level.</td>
</tr>
<tr>
<td>Being very effective communicators: use stories and express points in non-technical language to ensure the audience understands the point being made. Become part of everyone’s success.</td>
<td>Undergo training and practise presentations. Seek feedback after key meetings to see if messages were received or if they need to be refined.</td>
</tr>
<tr>
<td>Being context aware: understand the organisation and reframe information so it is tailored to the perspective of different managers. Quickly move from discussing specific details to general points when communicating.</td>
<td>Become more familiar with the broad range of functions in an organisation. Spend time with other departments to find out how they operate.</td>
</tr>
</tbody>
</table>

For guidance around communicating with senior executives, see the ISF report Engaging with the Board: Balancing cyber risk and reward.
5. DEALING WITH REGULATORY VOLUME

“If you treat regulation as a risk, you’ll manage it well.” – ISF Member

CISOs have become familiar with the demands of regulators and the ever increasing need to be compliant. There is no doubt that compliance is a significant burden, with one survey suggesting that 40% of IT budgets are now being spent on compliance.7

Part of the reason compliance is so time-consuming and expensive is because there is some disparity among regulations, resulting in conflicting requirements. At the same time, boards are expressing more interest in understanding whether the organisation is compliant with the range of regulations covering their own specific market sector and those that are more generally applicable. The material fines that can be levied for non-compliance have concentrated minds and mean that next-generation CISOs must recognise which regulations apply and whether their organisation operates in line with their requirements.

Next-generation CISOs should recruit allies in the shape of senior executives, audit committees or oversight bodies in their organisation to put pressure on any business unit that is falling short of its regulatory responsibilities and to police the steps taken to correct any shortfall.

The next-generation CISO knows to do more than just chase compliance, not least because blindly following regulations does not necessarily reduce information risk. Next-generation CISOs also appreciate the value of documenting their journey to compliance as it will demonstrate to regulators why the organisation took a decision that may result in a deviation from regulation. This may be because the regulation as applied would leave the organisation less secure than it currently stands, or it may be that one regulation clashes with another.

In addition, next-generation CISOs get their team to map requirements across regulations to look for commonalities. Addressing the most stringent requirements first will help meet less rigorous obligations. This mapping exercise involves creating a pool of responses to limit the amount of research required to produce relevant evidence requested by regulators.

Next-generation CISOs are often a key part of the interaction their organisation has with the regulators. This interaction and visibility can be used to lend weight to the CISO’s recommendations for achieving compliance.

<table>
<thead>
<tr>
<th>NEXT-GENERATION CISOS FUTURE-PROOF THEMSELVES BY</th>
<th>HOW CISOS CAN DEVELOP THIS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating a dialogue with regulators: inform regulators about how the CISO’s industry is changing and give feedback on the parts of the regulation that are too prescriptive.</td>
<td>Establish regular contact with regulators to inform them about relevant industry developments. Contribute to industry forums.</td>
</tr>
<tr>
<td>Recruiting allies: work with other functions to help them meet their regulatory requirements. Establish committees and governance structures that control mitigation.</td>
<td>Become known as the regulator’s representative. Either become an expert on compliance, or employ staff who are highly knowledgeable on applicable regulations.</td>
</tr>
<tr>
<td>Focusing on risk rather than compliance: take a more risk-based approach to compliance rather than just ticking boxes.</td>
<td>Learn what departments do to meet compliance demands. Encourage better behaviour that focuses on reducing risk.</td>
</tr>
<tr>
<td>Fostering change: strive to change the nature of regulation across the industry and the world by establishing global baselines.</td>
<td>Reach out to CISOs at peer organisations to discuss the common problems relating to compliance.</td>
</tr>
</tbody>
</table>

For more information about understanding key regulations and laws, see the ISF interactive guide Legal and Regulatory Implications for Information Security.

---

6. HANDLING TECHNOLOGY

“CISOs need proven technical knowledge of security, and how the tools and everything else works.”

– ISF Member

Next-generation CISOs are more strategically focused and have less hands-on contact than their predecessors with the technical systems underpinning security controls. Regardless of this softening of the technical nature of the day-to-day role, it is crucial that the next-generation CISO develops a voracious appetite for understanding technology and an appropriately sceptical approach to its application.

The next-generation CISO should be familiar with how to arrange people and processes around technology so it is configured, monitored and updated correctly. They know that an investment in a technology should not be made unless it can be supported and secured correctly.

Next-generation CISOs know that simply buying a security tool is no guarantee that it will help an organisation combat risks to the extent a vendor claims it does – either by rigorous testing or via their own network of peers. A 2020 report by cybersecurity consultancy Mandiant suggested only 9% of attacks generated alerts in security event analysis platforms. Relying solely on these attack-spotting tools can make organisations complacent and leave them open to compromise.

However, next-generation CISOs are well aware that they need monitoring and metrics in place so they can be assured, as much as possible, that the activity on their organisation’s IT assets and estate are being scrutinised effectively. This enables them to do a better job of understanding the risks faced by different parts of the organisation because they know the technology underpinning that business unit’s functions.

The familiarity with an organisation’s technological anatomy built up by the next-generation CISO helps establish a level of comfort around how well the enterprise is handling its risks. This way, next-generation CISOs can develop a “nose” for problems and spot areas that otherwise might be missed.

![Next-generation CISOs know that simply buying a security tool is no guarantee that it will help an organisation combat risks to the extent a vendor claims it does – either by rigorous testing or via their own network of peers.](image)

### NEXT-GENERATION CISOS FUTURE-PROOF THEMSELVES BY:

<table>
<thead>
<tr>
<th>HOW CISOS CAN DEVELOP THIS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Keeping close to the IT function:</strong> know about an organisation’s infrastructure and have a good sense of how it is operating.</td>
</tr>
<tr>
<td><strong>Testing technology:</strong> use rigorous testing regimes and expert staff to ensure that tools and services, including those already in use, are fit for purpose.</td>
</tr>
<tr>
<td><strong>Looking ahead:</strong> take a hands-off approach but be aware of future innovations (e.g. AI, edge computing and blockchain) and consider their potential to mitigate risks.</td>
</tr>
<tr>
<td><strong>Knowing about legacy IT:</strong> take time to understand the older technology the organisation runs and the risks surrounding its continued use.</td>
</tr>
<tr>
<td><strong>Managing suppliers:</strong> employ staff that can evaluate how suppliers perform and manage the relationship with them.</td>
</tr>
</tbody>
</table>

For more information about managing cloud services, see the ISF report *Using Cloud Services Securely: Harnessing core controls.*

For guidance on securing the Internet of Things, see the ISF briefing paper *Securing the IoT: Taming the connected world.*

CISOs keen to gain a clear understanding of emerging technologies should consult the ISF Library on *ISF Live* for information on AI, blockchain, agile development, open source software and other relevant topics.

---

Beyond the next-generation

Next-generation CISOs embrace the logic of transformation and adapt themselves, their function and their organisation to new ways of working. Being a next-generation CISO is an extremely rewarding position that allows an individual to become a pivotal member of their organisation, involved in and advising on almost every level. Next-generation CISOs help steer their organisation to a footing that helps it manage risk so deftly that it surpasses its rivals. There are few executive positions in organisations with so much potential freedom and influence.

However, this is not an easy role. Time and again during interviews supporting this research, ISF Members discussed the challenges they face, their wrangles over budgets and the sheer doggedness they need to get the job done – stress and pressure are common features of the position. The next-generation CISO needs to be self-aware and generate strategies to cope with these types of challenge.

Looking further ahead, next-generation CISOs will carve out their own path. They will mark where the future of the role lies, adjusting and amending their own skills and knowledge to cope with the ever-changing demands placed on the CISO. The next-generation CISO will be a master of change and familiar with the need to continuously learn – stretching themselves and their teams so they keep up with the restless pace of 21st century business.

Above all, the next-generation CISO has a bright future ahead of them and will be welcomed almost anywhere as more and more organisations turn their focus to the risks and opportunities of the evolving digital world.

---

**Figure 6: The future is unwritten for next-generation CISOs**

<table>
<thead>
<tr>
<th>TRADITIONAL</th>
<th>MODERN</th>
<th>NEXT-GENERATION</th>
<th>FUTURE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is a decision maker</td>
<td>Has C-level type skills</td>
<td>Balances opportunity with risk</td>
<td>Balances opportunity with risk</td>
</tr>
<tr>
<td>Has a good understanding of business principles</td>
<td>Engages with the board(s)</td>
<td>Demonstrates leadership</td>
<td>Demonstrates leadership</td>
</tr>
<tr>
<td>Has a good understanding of the organisation</td>
<td>Recruits from the business</td>
<td>Manages incidents and crises</td>
<td>Manages incidents and crises</td>
</tr>
<tr>
<td>Talks business language</td>
<td>Leads operational risk activities</td>
<td>Finds their own voice</td>
<td>Finds their own voice</td>
</tr>
<tr>
<td>Aligns security strategy with business strategy</td>
<td>Enhances the value of the company and brand</td>
<td>Deals with regulatory volume</td>
<td>Deals with regulatory volume</td>
</tr>
<tr>
<td>Is sensitive to the organisation’s risk appetite</td>
<td>Takes greater responsibility for risk and governance</td>
<td>Handles technology</td>
<td>Handles technology</td>
</tr>
<tr>
<td>Is willing to take responsibility</td>
<td>Talks business risk</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gets fundamentals dealt with first</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Talks information risk</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2006 2013 2020 BEYOND