CISO PLAYBOOK SERIES

CYBER LEADERSHIP INSTITUTE
KNOW YOU'RE READY

CISO PLAYBOOK:
FIRST 100 DAYS

Setting the CISO up for success

CISO PLAYBOOK:

FIRST 100 DAYS

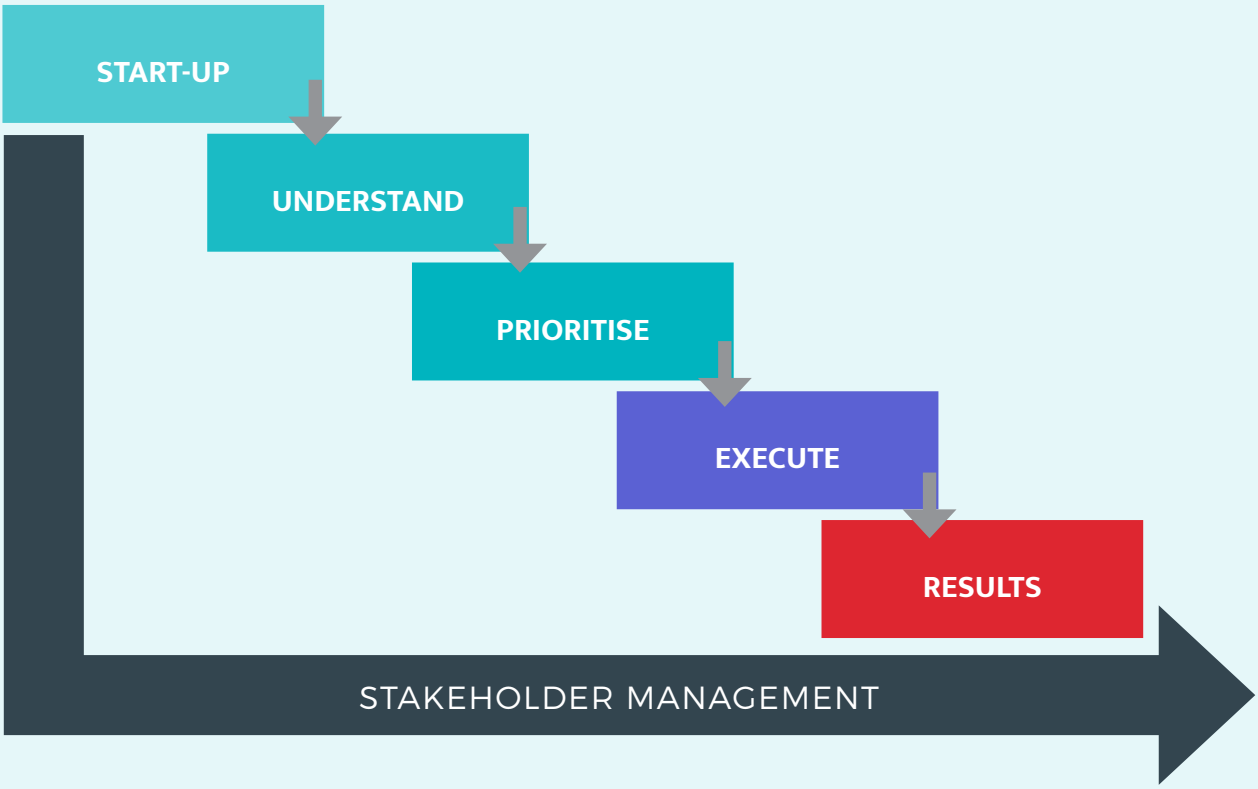
Setting the CISO up for success

EXECUTIVE SUMMARY

We propose a series of recommendations from hard lessons learned and a best practice approach to:

- Build and deliver a CISO first 100-day plan, to organise the key activities and initiatives that should be undertaken at the start-up phase, through to delivery of the final results at the end of 100 days; and
- Increase the chances of success, reduce the risk of failure and provide a platform for a new CISO to thrive in the role.

According to a study from the Enterprise Strategy Group and the Information Systems Security Association, a lack of alignment between the CISO role and the business, the C-suite and the Board of Directors can contribute to high CISO turnover. Therefore, it's essential for a new CISO to have a plan and be able to communicate it consistently to all the key stakeholders.



The **SUPER** acronym provides a framework for each of the phases:

S

START-UP: before starting the role; conduct thorough research into the company, read the company annual report, what headline breaches the company has had, who's who in the executive team etc. If possible, meet with key stakeholders before starting. Engage with your EA/PA (if you have one), start setting up meetings. Refine your plan.

U

UNDERSTAND: meet the important stakeholders first, map them and learn about the business, what are the issues and opportunities to improve the situation. Gather reports, assessments, audit findings, existing strategy documents, policies, metrics, Board reports etc.

P

PRIORITISE: know the quick wins, understand which issues will take longer to resolve, what current processes are working well and should continue to be executed on. Develop vision and share it with your line manager, your team and your key stakeholders, get feedback and refine.

E

EXECUTE: deliver on quick wins, put agreed plans in place to address some of the longer-term issues. Organise your team, set up your management system and ensure governance structures are established and effective.

R

RESULTS: re-engage with all your key stakeholders, re-confirm the key actions you're taking, any progress you have made, where you might need their help and feedback on your first 100 days. An executive assessment report of key risks and issues.

Below are the key SUPER phases and recommended initiative headings for the 100 days.

PHASE	INITIATIVE HEADINGS
STARTUP Days 10 to 15	› Common agreement on CISO role and scope › Personal management system, acccess to relevant reports, shared spaces, support systems, tools, etc. › Key stakeholder meetings scheduled, invites to existing security related regular meetings/calls and general lines of communication established › Establish external associations; Industry memberships, industry research/ best practice, information sharing forums, etc.
UNDERSTAND Days 0 to 45	› Gather together combined insights into the overall current state maturity, the security program, critical control deployment and top risks › Early indications of what's working and what isn't, and identification of 'good practice' that could be replicated (find Centres of Excellence) › Identify business unit priorities and alignment to overall organisation corporate objectives › Identified urgent issues and longer terms strategic issues to be addressed
PRIORITISE Days 15 to 60	› Identified and agreed the top five strategicchallenges to be prioritized for the next 12 months › Planned operational security budget for the next two months, including early indication of personnel organisation › Agreed at least three key issues (quick wins) to close out over the next two months › Awareness and education information on resources confirmed, online/off-line
EXECUTE Days 30 to 80	› Gain approval for the nformation security charter, interim strategy and vision - socialise with key stakeholders › Leading security related governance forums and committees › Cyber education delivered to the business and executive team, take feedback on assumed crown jewels › Actively making progress towards closing out quick wins - top three urgen issues
RESULTS Days 45 to 100	› An initial status report for the executive management (including maturity assessment, SWOT analysis, critical control deployment) › Evidence of early progress, achievements and measurable plans for next 6 to 12 months › Deliver effective executive monthly information security scorecard / dashboard › Demonstrate progress against top five outcomes for 100 day plan

STAKEHOLDER MANAGEMENT

PURPOSE

This playbook is intended as a complete set of end-to-end strategic initiatives and a framework to build a first 100-day plan for a new CISO.

ABOUT

The Chief Information Security Officer, or CISO, oversees all aspects of securing the integrity and safety of a company's information assets. From establishing the standards, to maintaining them, the CISO is required to uncover any potential risks to company-held information and IT systems. The CISO also defines and often leads the program of work to implement and maintain the necessary capabilities to control those risks within the Board's appetite; ensuring the organisation remains on a trajectory of meeting compliance with polices and regulatory demands.

SETTLING INTO THE ROLE OF CISO

There are many different routes to becoming a CISO: the majority will have worked their way up through the broad range of information security disciplines, many have an engineering and network security background, but others enter the profession via an alternative route, such as audit, legal, or recommendation from corporate colleagues. Wherever they come from, it's rare to reach the role of CISO without some preconceptions built up during the course of a career.

People are most comfortable with what they know, but a more helpful approach can be to focus primarily on those areas that are least familiar. A good starting point is to drill down into your weakest areas and seek to make the necessary improvements, before applying the same process to the CISO team members. Leadership skills in this executive position is a much more important aspect in ensuring that you the new CISO can fulfil the role and be successful.

A new CISO finding their feet should take time to understand the cyber risks and issues, but just as important is the time required to learn about the business: who are its customers, how does it make money, what is the culture of the employees etc. It's impossible to underestimate the importance of knowing the value of the company's assets, in terms of confidentiality, integrity and availability and ranking them accordingly to understand what the business cares about most, the critical assets, also known as the 'Crown Jewels'. (For a more detailed analysis of this area refer to our separate **CISO Playbook: Protecting the Crown Jewels**.) The CISO will need a deep understanding of the cyber capabilities in place to protect those assets to be able to discuss strategy and plans confidently with a wide number of stakeholders, including the Board.

KEY CONSIDERATIONS

BEFORE "DAY ZERO" – PREPARE THOROUGHLY

- Before a new leader embarks on a role as a CISO there are some essential knowledge and skills to acquire. It's no good having a great 100-day plan, if you can't communicate it effectively. Unlike a couple of years ago, CISOs now need to demonstrate that they possess the necessary soft skills as well as sound technical knowledge to perform well, such as establishing and maintaining effective lines of communication with a myriad of stakeholders and departments. According to Deloitte, the majority of CISOs "have to invest a lot of time to get buy-in and support for security initiatives". In other words, communication and credibility have become critical success factors for CISOs. The more effective a CISO's communication skills, the easier it is to secure the top job during an interview, and once in the role gain executive cooperation to support a new strategy and program of work. Here at the Cyber Leadership Institute, we help emerging CISOs and new cyber executives develop the necessary skills, providing training packages, mentorship and ongoing support. Click the link here 'Cyber Leadership Program' for more details.

- Learning about the company is essential, both during the interview stage and once in the role. Begin with the organizational mission statement, it highlights the core values and what is to be achieved. Learn about organizational core activities, its products, services, research and development, intellectual properties, mergers and acquisitions. Research through other publicly available information, such as the company annual report, financial statements, press releases, news, audit statements, data breaches, patents, executive leadership team, Board of Directors etc.

STAKEHOLDER MANAGEMENT

- Once in the role, it is important to take time to get to know everyone in the team. It's only by getting to grips with their personalities, concerns, pain points, and their goals that the new CISO will come to understand the way in which they work. But it's not just the people in the team - fostering good relationships with everyone with whom the CISO has regular contact with is just as important: the business, IT teams, C-suite, external partners/agencies, sales/marketing, auditors, Board members, members of the public etc.

- Probably the most crucial step is to gain top-down support, making sure that there is buy-in from the Board of Directors. CISOs are no longer just technology leaders but are a strategic and integral part of the business management team. According to Forbes, "the Board has a fiduciary obligation to protect shareholder value, so the Board needs to take security seriously".

- The CISO should develop a general narrative that says "Cybersecurity is no longer just a cost of doing business, it's an investment in the brand. It becomes an asset that contributes to — or the lack of damage — the company bottom line." Consumers care about their security, their personal data and their privacy more than ever before — customers, or potential customers, will change their behaviour if the company is the subject of a successful cyber-attack. Recent research — which was run in the US, UK, France, and Germany — suggests that 78% of the total participants said that they would stop shopping online with a brand if it gets breached — and 36% would stop engaging with a brand both on and offline. This is not just about missing sales; it is also about losing the brand support and promotion that comes from a positive customer/brand interaction and engagement on social media.

ASSESSING RISK, KNOWING THE ISSUES AND MEASURING CAPABILITIES

- During the first 100 days, it's unlikely there will be an opportunity to conduct a full threat scenario based cyber risk assessment, but it will be important for the CISO to demonstrate why this activity will be important after the 100 days and how it will be conducted as part of the overall strategy. The CISO should instead focus on performing a high-level maturity capability self-assessment during the first 100 days and define the likely threats the organisation faces. This initial executive report will also demonstrate the need for a more thorough independent third-party assessment, to look at maturity against industry standards, such NIST Cybersecurity Framework, and benchmark against similar peer organisations.

- At minimum, the end of 100 days report should be able to provide answers to the following questions:
  - How well protected is the organization, what is our capability maturity?
  - Who and what is our biggest threat?
  - What areas have the greatest negative impact on the organization's security posture?
  - What will it take to improve the organization's security posture?
  - How can effectiveness of investments be measured?
  - What will the ROI of the security-related initiatives be?
  - What will the organization risk if nothing changes?
  - What is required from the Board to be successful?
  - What is being done well, how can this be preserved during change?

NO ONE SIZE FITS ALL CISO

- An effective CISO will be able to assess the ways in which people contribute to the company. It is essential that a new CISO immediately assesses the organisation's commitment to Information Security. One indication, which is also a question for the interview stage, is who will the CISO be reporting to - directly to the CEO, the CIO, the COO or the CRO? It can depend on the type of organisation, but the direction of execution, and potential effectiveness will depend on the level of empowerment, and who the role reports to. Regardless to whom the CISO reports, it's crucial that a charter with clear principles be drawn up and be approved by the CEO and shared with the Board during the first 100 days.

BE READY TO RESPOND TO MAJOR CYBER INCIDENT AND/OR CRISIS

- Cyber incidents are inevitable, and although less frequent, a major cyber breach of some kind will happen - it's possible that a significant breach could happen during the first 100 days. Cyber-simulation exercises are recommended as a means of testing plans to manage a cyber security incident, this provides an opportunity to test the team's incident management capability. The role of the CISO might not be directly be involved in managing the incident, but definitely will be a major stakeholder, and the person the Executive Team and Board will look to for assurance that everything is under control. A simulation exercise will help the CISO understand how the organisation responds, and at the same time provide an opportunity for increased level of awareness about the impact a major breach of security can have on the business.

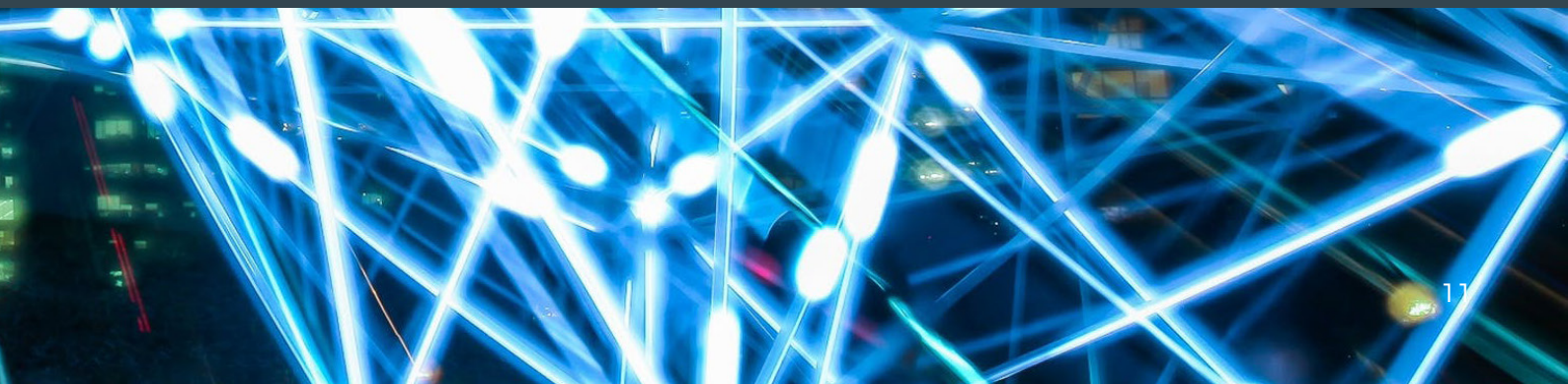
LEADERSHIP AND TEAM

- It's essential in the very early days that a new leader meet with all of the team, start with the direct reports (ideally 1-to-1 face-to-face) and then a team meeting. Depending on the size of the team, it will be good to try and meet as many as possible, this will give a sense of any unrest, and things that are going well.

- Any new leader will need to evaluate the team. In any team there may be some excellent, some average and some unsatisfactory people in place. The team will have its own dynamics and habitual ways of working. Go in and shake the tree, but always evaluate thoroughly before acting. Hasty action compromises trust and credibility, which may inadvertently lose valuable team members. A checklist below can help structure decision making

  - Competence – Does this person have the technical skills and experience to do the job well?
  - Judgment – Does this person exercise good judgment under pressure or when faced with sacrifice for the greater good?
  - Energy – Does this team member bring the right kind of energy to the job, or is he/she disengaged, burned out or unfulfilled?
  - Focus – Does this person stick to priorities, or is he/she easily distracted and scattered?
  - Relationships – Does this person get along well with other team members, supporting team decisions?
  - Trust – Can this person be trusted to be honest, consistent and reliable?

- Quickly establish a team management system, what regular meetings do they attend, reports they produce, projects and deliverables each person is accountable for. Pull this together into a consolidated tracker, even if you're using just a spreadsheet. Add to this the CISO commitments, and this will provide transparency into the current workload, and visibility into the heartbeat of the team, which will serve as another decision-making tool.

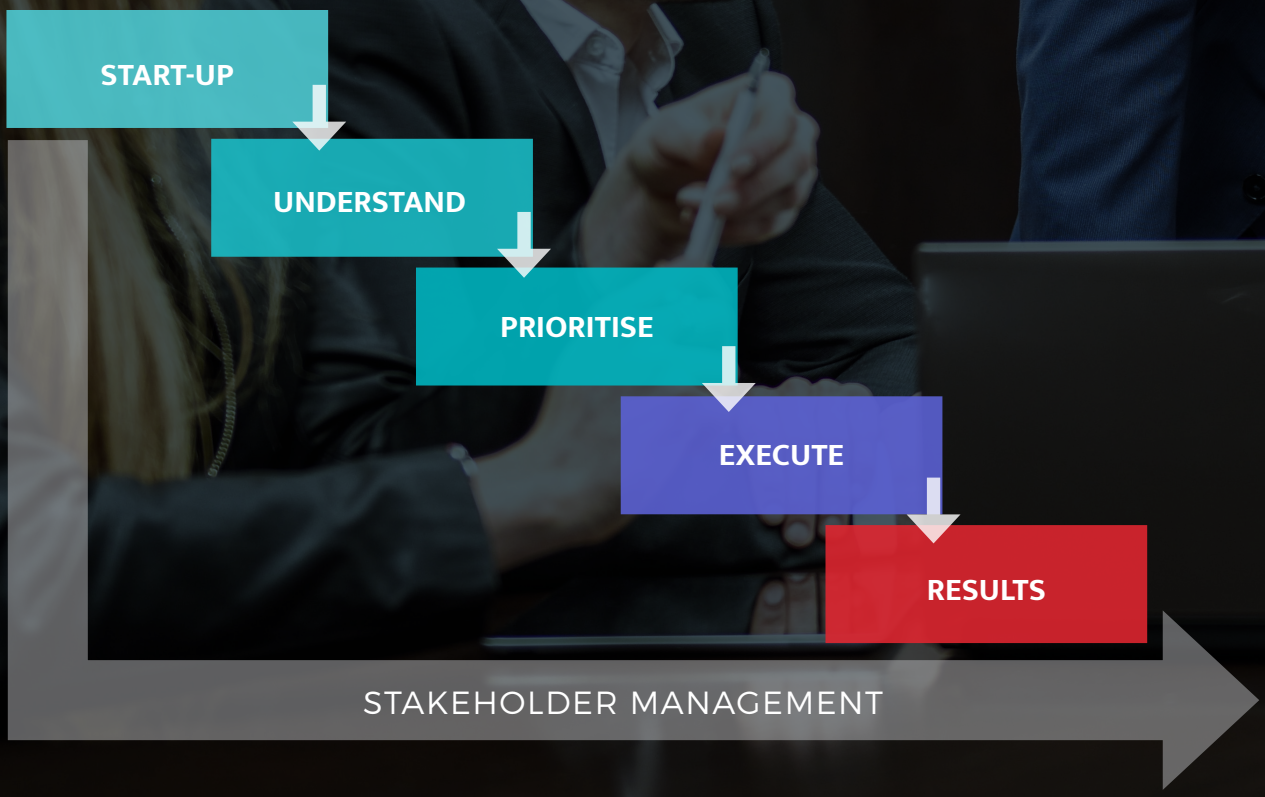


CYBER LEADERSHIP INSTITUTE
KNOW YOU'RE READY

ACTION PLAN

This five-phase approach helps provide structure to the 100-day plan, providing a checklist of the key activities to undertake. The **S.U.P.E.R** acronym provides a framework for each of the phases.

NOTE : a complete 100 days spreadsheet tracking template, plus additional tools and templates to support this first 100 days are available for free as part of the **Cyber Leadership Program** https://cyberleadershipinstitute.com/cyber-leadership-program/ and for members of the Cyber Resilience Hub https://cyberleadershipinstitute.com/cyber-resilience-hub/



PHASE 1: S - START-UP

Before starting the role, conduct thorough research into the company, read the company annual report, what headline breaches has the company had, who's who in the executive team etc. Engage with your EA/PA (if you have one), start setting up meetings. Refine your plan and begin.

TIMING	ACTIVITIES
Before day 1	Reinforce new connections with people already talked to in the company during the interview process
Before day 1	Gather and consolidate external industry analyst research reports, identify key industry security conferences, memberships/associations (cyber leadership hub) - document and pull together costs
Before day 1	Set logistics with manager, HR, EA etc. and readiness for day one (who will meet me, technology set up, access, badges, The company induction etc.)
Before day 1	Identify key templates for documentation, frameworks, presentations, reporting etc. and align to each row in the reference section of the 100 days plan.
Before day 1	Begin discovery conversations with external security consultants for the independent maturity assessment - references, pricing, availability etc.
Before day 1	Ideally using admin support, gather a list of key stakeholders and agree with manager which should be the priority to meet in the first two weeks. Admin support to schedule these in before arrival
Before day 1	Prepare introductory communication about me, including thoughts on joining the company and key priorities in life/work etc.
Before day 1	Prepare stakeholder and staff discussion guides that can be used in 1-1s and meetings (questions, open and specific)
On day 1	Meet and greet with named person responsible, ensure technology assigned, access, badges etc. also any enrolment with formal on-boarding process that the company operates
On day 1	Communications - meeting/call with manager, send introductory emails to key stakeholders, and to wider organisation e.g. company intranet posting

On day 1	Regroup with manager - from managers perspective, understand what are the key challenges/opportunities/known issues. Schedule regular communications schedule between us
On day 1	Regroup with manager - discuss introductory vision for information security in the company and document the key asks/requests to support the new role
Week 1	Set up calendar invites for 1-1 meetings with key stakeholders and teams responsible for delivering information security. Request invites from current repeating calls/ meetings required for the role, including company communications
Week 1	Request organisation structure, reporting lines and in particular those in legal, security, risk and compliance. Review and begin aligning to a structure that might work, virtually and direct reporting. Meetings with your manger to confirm security teams.
Week 1	Send your manager costs cases for CISO required subscription for executive insights and further templates e.g. Cyber Leadership Hub
Week 1	Access to general working practices - access to corporate systems, team shared areas, administration tools etc.
Week 2	Establish name/links with third party information sharing forums specific for the industry, including law national enforcement, government agencies etc.
Week 2	Request access to security and risk related data - current security strategy/programme, pen test, vulnerability assessments, polices/standards, audit findings, current risk management tools etc.
Week 2	Confirm with manager key memberships/associations and provide business case and costs
Week 2	Understand pricing and scope for independent security assessment activity and external benchmarking
Week 2	Establish personal management systems and communications. Hook into internal and external communications, added to intranet pages, blogs, news articles and publications

PHASE 2: U - UNDERSTAND

Meet the important stakeholders first, map them and learn about the business, what are the issues and opportunities to improve the situation. Gather reports, assessments, audit findings, existing strategy documents, policies, metrics, Board reports etc.

Key Activities include:

TIMING	ACTIVITIES
Week 1/2/3	Gain business insight - Meet with key stakeholders that were prioritised by manager, business leaders (CxO) and operational teams (security, risk, compliance etc.), establish opinions on current security program and what they believe are the priorities. Capture output into a report
Week 2	Send your manager costs cases for CISO required subscription for executive insights and further template e.g. Cyber Leadership Hub
Week 2	Assess how many resources are in place globally to manage the security organisation, including financial parameters (including operational security budgets)
Week 2/3	Using a high-level maturity model/assessment tool (Cyber Resilience Hub): Review existing security governance, strategy, policy, standards and overall framework architecture and where is this stored, central or distributed. Look for good practice and document findings
Week 4	Review recent high-level executive summaries of audit findings, vulnerability assessments, penetration tests reports, recent security incidents
Week 4	Seek at least one executive mentor internally, one external and formally join the priority industry information sharing forum
Week 5	Review cross business projects and initiatives; what are currently underway across the business, what is security's involvement? E.g. M&A activity
Week 5	Assess scope of the CISO role and overall remit following previous meetings and company discovery (information security, IT, risk, compliance, privacy, fraud, physical, business continuity etc.)
Week 6	Review security and compliance specific projects and initiatives; which are seen by the business as being a priority currently underway across the business, what is security's involvement
Week 6	Understand at macro level what is functioning well and which require some effort to be brought up to the next level of maturity.

PHASE 3: P - PRIORITISE

Know the quick wins, understand which issues will take longer to resolve, what current processes are working well and should continue to be executed on. Develop vision and share it with your manager, your team and your key stakeholders, get feedback and refine

TIMING	ACTIVITIES
Week 3	Build requirements for security education packages, identify external specialist security companies (perhaps hosted)
Week 3	Identify an appropriate tool for measuring ongoing information security, risk and compliance globally for company (may already have a tool internally?) - this should be an information security governance model
Week 3	Tightly scope an information security assessment to measure general maturity and provide a benchmark measure.
Week 4	Plan global site visits, arrange to meet security, risk, compliance personal and any key stakeholders face-to-face
Week 5	Design a draft of the information security organisation that could operate within company, consider both IT and business security roles, and identify headcount for security role gaps. Align to budgets (Opex/capex)
Week 5	Plan operational security budget for the next three months - work with assigned financial analyst and consider ROI metrics and specific head count shifts/new hire
Week 5	Schedule monthly calls with current identified security related personal, amend as required as the team shapes up during the next six months. Share executive communications, review individual activities, allocate actions and track etc.
Week 6	Establish blueprint for office of the CISO online information source
Week 6	Review existing/prepare the draft information security charter and prepare materials for information security steering committee
Week 7	From the assessment of major issues, select prioritised two key issues to focus on over the next two months to close out
Week 8	Draft and socialise an interim information security strategy and vision - where we want to be, where we're currently, and the gap showing current/proposed projects to close the gap (two focus areas highlighted)

PHASE 4: E - EXECUTE

Deliver on some of the quick wins, put agreed plans in place to address some of the longer-term issues. Organise your team, set up your management system and ensure governance effectiveness is established

TIMING	ACTIVITIES
Week 5	Refine new global information security organisation, operating model and raise any headcount requests. Create info security team roles and responsibilities (leaders, analysts, engineers, PM's etc.)
Week 5	Visit key sites globally, meet security, risk, compliance personal and any key stakeholders face-to-face. Review high level physical security of data centres/server rooms
Week 6	Begin a tightly scoped information security assessment to measure general maturity and provide a benchmark measure
Week 7	Appoint security champions globally, clarify R&Rs, arrange a kick off call and publish
Week 7	Get directly involved in projects and as appropriate, question 'why?'.....ensure the teams are focused on the business value, executing in line to agreed milestones and project RAID is clearly documented/maintained
Week 8	For new projects, validate and have identified security leaders assigned, ensure status reported back into the info security programme office
Week 8	Draft and socialize information security charter with executive leadership team. Obtain approval from key stakeholders
Week 9	Establish (or re-establish) the information security governance process and forums based on previous maturity assessments (instituting effective decision making linked to accountability, responsibility and authority, also budgeting and reporting)
Week 9	Conduct a senior executive management cyber education meeting and develop a quarterly schedule with a repeatable format
Week 9	Deliver basic security awareness/education in areas of the business identified as being a priority
Week 10	Engage in planning activities for next 6 to 12 months and assign resources/funding
Week 11	Establish office of the CISO online information source

PHASE 5: R - RESULTS

Re-engage with all your key stakeholders, re-confirm the key actions you're taking, any progress you have made, where you might need their help and feedback on your first 100 days. An executive assessment report of key risks and issues.

TIMING	ACTIVITIES
Week 7 onwards	Monitor status and measure success of existing security related programmes, and build into regular reporting, include planned projects as initiated
Week 10	Deliver effective executive monthly information security scorecard / dashboard. Important to take feedback and amend as required
Week 11	Measure performance of current security personnel, using a 360-degree feedback process. Ensure low performers have a plan to improve and high performers recognised for their contribution (objectives set)
Week 13	Highlight any early wins, successes, challenges and schedule a meeting with meeting with manager, team leaders and key stakeholders and refine reporting based on feedback
Week 13	Complete an executive report, that includes - maturity assessment, SWOT analysis, critical controls deployment rate etc.
Week 14	Conduct a senior executive management status meeting, includes early wins and plans for 6 to 12 months, use presentation format from earlier meeting and develop a quarterly schedule with a repeatable format

STRONGER TOGETHER

CONTRIBUTE AND HELP US IMPROVE

Any Playbook such as this can never be completely comprehensive, so we encourage you to contribute any additional considerations, thoughts or questions through the Cyber Leadership Hub. We will use your contributions and feedback to update the content and continuously improve the Playbook, for the benefit of the whole community.

Together as a Cyber Resilience community we can continue to improve our resilience against cybercrime and jointly manage and reduce cyber risk.

APPENDIX 1 – CAREER RESILIENCE FOR A CISO

The CISO is a challenging role and constantly under pressure to demonstrate business value in their strategy. Perhaps the most challenging time is during the first 100 days. The need to demonstrate value early is a key component of the CISO role – new CISOs need to quickly establish the key issues and risks facing the organisation and demonstrate their ability to address them. There may be no formal or public record of CISOs being given the boot but it is clear that this happens on a fairly regular basis. CISOs could depart for their organization suffering a damaging breach, but could leave too in the event of failing to spot or report a bug, poor purchasing decisions or because of disagreements with senior management. One head of information governance, previously working in the US media sector, saw her CISO asked to leave. The dismissal, she said, "mostly centred about [an] inability to address risk to a satisfactory state and in an economical manner." There are many things a CISO can do to reduce the risk of career failure and protect themselves, but let's first hear what some sacked CISOs had to say.

CISOS TELL ALL

Two CISOs who were dismissed described the experience of being fired, and the lessons they learned. One CISO, who previously worked in the UK financial services sector, says that his dismissal ultimately came down to "a difference of opinion" between him and the CIO. "The information security budget was part of the overall IT budget, and the CIO had to make cost reductions. While information security still had to show savings in the budget, this increased risk in certain areas." He continued that, having explained the potential damages to senior management, the CIO took a nasty turn. "The CIO did not like this, although agreed that the business should be responsible, which was a case of do as I say not as I do." He says that he felt he handled the departure well, but believes he learned a lot from the experience. "It is best not to report directly into Technology, and have your budget controlled by the CIO, who is under pressure to show aggressive costs savings. Also, businesses leaders do not like to hear the truth or have transparency, even if they publicly state that."

Unfortunately, this tale is similar elsewhere. A Head of InfoSec at a managed service provider also cites difficulties with the IT team, with this eventually paving the way for his own exit. "The IT director constantly ignored the advice of information security, thought that he knew better, and while telling the Board that we should improve, undermined my position by telling my peers to let me fail, as he just did not like what I did.

This resulted in a complaint to HR against my director, for conduct unbecoming a director and also a breach of our corporate ethics policy. HR brushed it under the carpet. A month before my two-year employment period, where employment law would have protected me with unfair dismissal, I was dismissed."

Another CISO, working in the US pharmaceutical industry, explained why he resigned after blowing the whistle on insider fraud following an M&A. "There was a merger and acquisition with another bigger US company with a global reach, as this was a publicly traded business we had Sarbanes Oxley and SEC compliance which fell under my remit, as the parent organization's information security function was less mature than ours. "There were a number of financial irregularities throughout the year, and while carrying out some analysis on data loss prevention, came across what looked like fraud and insider trading. One of these was a regional CFO, who I got on well with. "The information was not conclusive, and after debating with myself for a week what to do, I passed on the information in confidence to the new CEO in accordance with our own policies (ethics, and whistleblowing). The CEO then forwarded on my confidential email to the person I reported asking what was going on, in which I straightaway received retaliatory action against me.

He resigned the day after, but four months later the company filed for bankruptcy, and later last year the old CEO and CFO were investigated by the SEC.

SO WHAT CAN A CISO DO TO PROTECT THEMSELVES?

Here are five top tips:

1. Firstly, it's important to get off on the right foot, develop a 100-day plan like the one suggested in this playbook, it provides structure and a communications tool for all your key stakeholders.
2. Definitely know your scope, and your boundaries, plus where you can break [the business] and where you can add value
3. Take time to get to know of the key stakeholders, and understand the business, how does it make money, who are its customers and be clear what the priorities of the business
4. Try and make it real for executives, use benchmarks and maturity assessments to show how the company stacks up to competitors and best practice. What assets do they really care about (the Crown Jewels), what are the most likely threat actors, what are the critical few things they must accelerate (cyber hygiene factors). If they understand it and it challenges them, they can tell you their risk appetite.
5. And finally, register with the Cyber Leadership Program, gain valuable insights from mentors and gain free access to tools, templates and much more.

APPENDIX 2 – REFERENCES

CREDIT GIVEN TO ONLINE REFERENCES FOR THIS DOCUMENT

https://www.linkedin.com/pulse/new-ciso-part-1-first-90-days-pope-sccp-sira-sccp-arch-cissp-/

https://cybersymbiosis.com/2018/03/22/the-first-100-days-of-the-next-generation-ciso/

https://www.forbes.com/sites/tonybradley/2015/01/22/7-ceos-share-why-cisos-need-to-be-involved-in-the-boardroom/#5e450c77e0ad

https://www.cio.com/article/3058726/these-cisos-explain-why-they-got-fired.html

THE CYBER LEADERSHIP INSTITUTE

Develop and grow your cyber skills

We provide capability development and training programs to accelerate the development of cyber strategy, leadership and risk management skills.

https://cyberleadershipinstitute.com/what-we-do/

ABOUT THE CYBER LEADERSHIP INSTITUTE

Our mission is to empower cyber leaders to embrace the technological revolution and improve the way we all live, work and interact.

Our purpose is to give business leaders the skills to confidently lead their organizations in the digital economy.

We strive to:

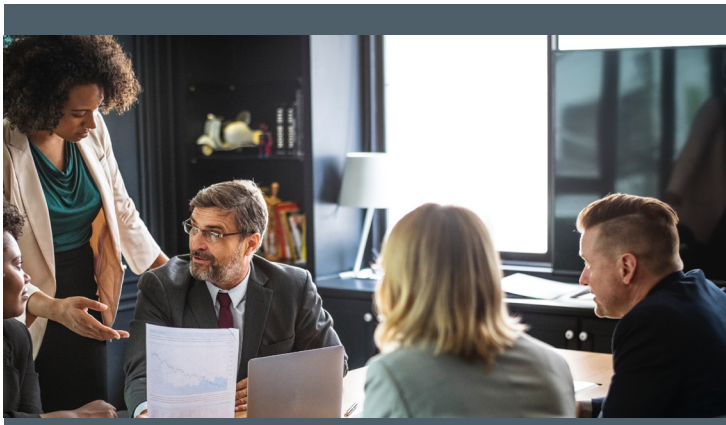
- Develop cyber leaders who build resilience into business strategy
- Empower business leaders to develop sustainable cyber strategies
- Inspire leaders to work together to secure our digital world

JOIN THE CYBER LEADERSHIP HUB

Stronger together – co-create cyber resilience solutions

There is strength in collaboration. Join a community of business, technology and cyber leaders who co-create solutions to cyber challenges, and develop and share business ready templates, methodologies and tools via a digital platform – the Cyber Leadership Hub.

https://cyberleadershipinstitute.com/cyber-leadership-hub/



CONTACT US

CYBER LEADERSHIP INSTITUTE
Level 17 Angel Place
123 Pitt Street
Sydney NSW 2000 Australia
contact@cyberleadershipinstitute.com

CYBER LEADERSHIP INSTITUTE

KNOW YOU'RE READY