sentients

Cybersecurity Executive Search

The First 100 Days.

F100 Planning for Cybersecurity Leaders

info@sentients.io

Introduction

Many excellent publications, both in short and long form, can be found on the design and execution of plans for the first ninety or one hundred days in a new leadership role. This guide seeks to bring together these methodologies, contextualized for information security and risk management leadership.

Given the rate of evolution seen in these roles, and the organisations who hire for them, we believe that Sentients' viewpoint through the eyes of our network of security professionals across the UK economy may help to identify potential pitfalls and set conditions for success before, during and after a new security leader arrives in post.

The role of a CISO

The definition of the Chief Information Security role, it's reporting lines and stakeholder interactions, both internally and externally, has changed significantly over the last few years. This has been driven in part by regulatory change and GDPR, more engagement with the board and enhanced fiscal responsibility, and also the expectations of the IT and information security team members.

Most of us have seen statistics on LinkedIn and from various studies, stating that security leaders' tenures last just 18-26 months, with nearly a quarter of Fortune 500 CISOs moving on within a year of taking on a new role. We've seen much speculation and hand-wringing over whether this is the fault of organisations or individuals, though we can see a distinct trend towards emphasis on 'soft' or 'core' skills, change management language and stakeholder management expertise come to the fore in job descriptions.

In truth, very few of the 'CISO' roles you will be approached about meet the criteria for that title. Rarely do we see a perfect amalgam of executive status, budgetary responsibility, autonomy and delineation from IT or the CIO office. These roles still offer great opportunity for security leaders who are willing to educate and evolve the organisational perception of information security. Under these circumstances, you can make rapid strides and improvements, broadening your influence over time.

Where you might be replacing another CISO, the gains will be marginal, at least for the first period, as the organisation and team are already at an advanced state of competence. Under these circumstances, your technical competencies become less important than your ability to motivate and retain team stability, and expand the reach of the security function across the business.

Key alignments for sucess

Fiscal responsibility, especially in organisations where a breach or regulatory change has prompted improvement, can be vexing for CEOs and CFOs who struggle to measure return on investment for security tooling using the same metrics used for business systems upgrades. The key here is to align your team objectives to the wider business objectives, bringing meaning, purpose and connection between your team members, and how they interact with the business. How your team conducts their business with other departments will reflect on you, and their mindset should be to facilitate, not block, the day to day operations.

It's normal to be the smartest guy in the room and demonstrate your higher level technical expertise, but adapting to the board room and presenting business cases from investment is a skill in its own right. For smaller organisations where your role may be both strategic and tactical, generating buy in from the team to embrace new methods and systems of, and feeding and watering these systems for sustained success, require immense agility to translate messages up, down and across the business.

Psychological alliance

One element of the role often overlooked by both organisations and new leaders coming into post has been the psychological condition of the wider team. Given the high turnover of leadership, this 'change fatigue' is more prevalent within the security industry than many others. Each time a new leader arrives, there's a period of uncertainty as the new strategy comes together, the team target operating model is defined, hiring and firing begins, then, just as the dust starts to settle and improvements begin to manifest, the leadership changes and the process begins again.

Most senior leaders of any discipline would agree that building alliances inside and outside the organisation is critical, both to support and inform your decisions, and to keep an eye on competitor activity. Historically, many industries have been compliance-led, with little focus on the wider threat landscape. If you are entering into a new industry or organisation where there is no prevailing best practice, guidance or market leaders to aim for, you'll need to define success and reporting metrics based on incremental improvements, budgets and organisational readiness.

Finally, balancing your own needs with that of the organisation can certainly improve the chances of your long term success. Few of us enter into a new role with the attitude that it will only last for a couple of years. We like to believe that we'll grow with the organisation, whilst simultaneously depleting our internal resources by absorbing more stress and neglecting our personal relationships and wellbeing. Research suggests that stress levels for security leaders are increasing steadily year on year, significantly impacting mental health, physical health and home lives.

We urge you to build and maintain a support network of peers, mentors and people outside of the security industry to maintain perspective and find new ways to approach challenges and prevent burnout. Your team and the information security industry needs your leadership, and it's your responsibility to find ways to stay resilient, especially early in your tenure.

sentients
Cybersecurity Executive Search

The First 100 Days

During your notice period

Notice period

The trend towards longer notice periods offer both the opportunity to plan your landing well ahead of time, and also the challenge of managing a transition of power from your current role. Under these circumstances, there are many opportunities to gain insights from your successors arrival and the effect on your existing team, taking that forward into the new engagement.

Connect

The uncertainty of a new arrival, the pain of breaking long-standing, reliable relationships, and the sudden availability of time in your schedule can result in a roller coaster ride of emotions for all parties. We recommend that you look forward, and manufacture time in your calendar, especially in the final four weeks of your notice, to reconnect with industry peers and progress the relationship with your new line manager and HR.

Good Terms

It's also useful to leave on good terms with your current team, integrating your successor and making a clean break. If you are able to execute an effective handover and communicate your choices and milestones to the new leader, your systems and methods are more likely to continue, rather than be erased and remodelled. This benefits the team who are already unsettled by a change in management. Acknowledging and thanking your team members at the end of your tenure has its benefits; you might also need to hire into your new team, and your previous employer might prove a useful hunting ground for skills.

sentients
Cybersecurity Executive Search

The First 100 Days

During your notice period

Build your foundation

At this point, you have the opportunity to reflect on your experience to date, celebrate past successes, coming to terms with any unfinished business and redefine your leadership style moving forwards. This is also the time to be seeking out other security leaders and networking groups within your new vertical, building a foundation of regulatory and best practice knowledge. Understanding the expectations from the regulator and evaluating the security capability or maturity of competitors can be very helpful in benchmarking performance levels and progress for your own organisations.

Schedule

Once your mindset has moved from handover to new beginnings, this is the time for you to create a schedule and plan for your first 100 days. Not only will your document bring structure and a focal point to your activities during inductions and the initial flurry of stakeholder meetings, it's something tangible you can share with people in your new organisation, demonstrating that you have a plan and building trust in your methodology.

sentients
Cybersecurity Executive Search

Zero to Thirty Days

Connecting to the Team & Organisation

You will carry a tremendous amount of goodwill as you start your new role. HR, the directors and data owners all have a stake in your success. The information security team may well be worried about any forthcoming changes you want to make, and you may already have a target operating model in mind.

Clear communication and a willingness to engage with every individual who reports to you shows fairness and pragmatism.

1. Acknowledge the work of your predecessor and the team
2. Share something of yourself and your life outside of work, make it easy for others to relate to you
3. Agree that there will be a period of uncertainty, and that changes to the team structure and size may change
4. Confirm that any changes that do take place will be communicated within your first 100 days
5. State that any changes will serve to realign the security function with the business objectives, removing your own biases from the decision making
6. Set regular team meetings and schedule meet and greets with everyone, inviting them to present on their role, attributes and aspirations

This last point is essential. It is never too early to review and practice how the organisation responds to an incident. Many of us have heard horror stories about major incidents occurring within the first few weeks of a new leaders' tenure, and often it takes years to remedy the event and rework processes for future breaches.

sentients
Cybersecurity Executive Search

Zero to Thirty Days
Evaluating Capability

Now is the time to meet, ideally face to face, with the most influential members of the organisation, specifically those involved in budget sign off, incident management, data ownership and compliance.

Items for your agenda could include:

1. Review security metrics and incidents to date
2. Meet separately with the Incident Response team and review the play books. If there aren't any, create some.
3. Review documentation and change control with IT operations, architecture teams and security engineering
4. Test the understanding of risk and the threat landscape, both within your team and across senior leadership in finance, IT, HR and operations
5. Review recruitment and retention strategy, and any historic performance management issues, with HR leadership
6. Meet with your external partners, vendors and regulatory bodies, get a feel for their perception of your capability and any obvious issues
7. Review commercial agreements and contract scope with vendors

We would recommend that you engage with an external consultancy to assess your current state of maturity. You will already have an idea of how the organisation and the team measures up, and a third party consultancy will help to validate or challenge your perceptions, facilitate team meetings about any concerns or areas requiring immediate focus, and also provide a body of evidence that you can use to justify additional investment and reorganisation.

sentients
Cybersecurity Executive Search

Days Thirty One to Sixty

Harnessing Influencers

After one month in your role, it is likely that you'll have encountered everyone in your team and many of the wider business, and can now gauge the atmosphere in the office, who the informal leaders are and who really influences or hinders progress. Aside from the management team underneath you, now is a good time to make informal appointments for policy implementation.

You can foster a greater ownership amongst the team by using their personalities in some roles; minuting or chairing team meetings, monitoring data quality for reporting, or organising the quarterly team off-site are all opportunities for you to leverage those leaders, quieter types, or cynics in your team and help to drive through new initiatives.

Similarly, it can be useful to invite leaders from the wider business to participate in the infosec team meetings. Transparency and acknowledging the importance of other departments in the security strategy can quickly turn cynicism and misunderstanding into championing of your work. Follow up their attendance by sharing reports and asking for feedback, and a request to attend one of their own team stand-ups can help to cement that relationship.

sentients
Cybersecurity Executive Search

Days Thirty One to Sixty

Measuring & Sharing

Create universal dashboards with metrics that can be understood by anyone in the organisation. A straightforward RAG status for the risk register, improvement project progress, security event management and training completion for team members should suffice. Drawing attention to these four areas demonstrates that you are taking a holistic approach; risk management aligns to the wider business, security project and event ticketing status shows that the team is coherent and takes responsibility as a unit, and training completion shows everyone that you're investing in your people, and that you're all trying to continuously improve skills and knowledge.

This dashboard is a neat visual representation of your leadership approach, willingness to be transparent and accept accountability. It can be easily shared and understood by anyone who takes an interest, or who wishes to scrutinise where investment and activity happens within the information security function and how that benefits their own agenda. It's also a mirror that you can hold up to the team, to reward or rally efforts during your weekly team meetings and one to ones, a data-driven tool that everyone shares responsibility for maintaining and improving.

Application	Priority	Status	Completion
Risk Register	High	In Progress	75%
Improvement Project Progress	Amber	Done	100%
Security Event Management	Low	Not Started	0%
Training	High	Done	100%

Template plan for a universal RAG dashabord.

Now you are able to track the progress of each department, now is the ideal time to engage with your HR team and recruitment partners to discuss skills gaps, salary benchmarking and training needs analysis. Look at your team holistically, not just in terms of the hiring needs; bringing in new people without knowing industry standard pay rates, the availability of niche skills, succession planning and training needs can set your recruitment campaigns up to fail, damaging your reputation in the process.

sentients
Cybersecurity Executive Search

Days Sixty One to One Hundred

Redefining the Stratgey

By now you will know what is working, what isn't and who is really driving the performance of the team. Your new strategy, plans and target operating model need to be clearly documented and communicated, including the following elements;

1. Highlight any early wins or obvious shortcomings, and how these will be celebrated or addressed in the future
2. Define a new team structure, job titles and hierarchy
3. Lay out your policies for selecting and integrating third party vendors and advisors into the organisation
4. Priorities and initiatives, based on maturity assessments and gap analysis
5. Create a long term vision and objectives, aligned to the business
6. Define your role as the leader and how that serves the organisation and your own aspirations
7. Set out an annual schedule for individual and team performance reviews

Draft this and share it with a trusted peer or colleague, taking on board any constructive feedback before refining the plans and discussing them with your line manager or executive sponsor. Where your vision relies, or impacts, on another department, it would make sense to pitch your plans to the head of that department. It would not be appropriate for you to discuss personnel or budgetary changes, and the earlier you can create security champions in influential roles, the better chance you have of the overall organisation adopting your proposed changes and new controls.

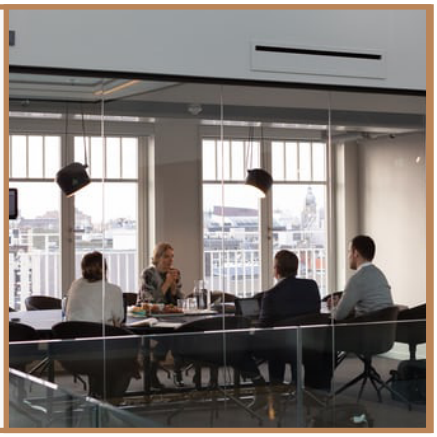
Days Sixty One to One Hundred

Resetting Direction

This is the time to share your vision for the new structure and priorities, and to deliver on your initial promise of making necessary changes within 100 days. Bring the team together to share your findings from the first two months, identifying successes and opportunities to improve. Share a visual representation of how you see the new team structure and objectives for the next 12 months (longer if you can), aligned to both the business and compliance requirements you've identified. Ask for feedback on your leadership and the proposed new direction, and reiterate your intention to assign new job roles, training needs, and any hiring or downsizing, within the next 30-40 days.

Keep in mind that any rumour or speculation about leavers during this period will be unhelpful to the remaining staff. Once you have informed those who are exiting, get the remaining team together to explain (not justify) your decisions and invite questions. Close this meeting by reiterating that the new mission and model begins from that point onward.

Following this, meet with the team individually, accompanied by their line manager and, where appropriate, a HR representative. State how you see their role moving forward, the resources available to help support them, their new career path and address any performance issues with a clear action plan. Where you have decided to remove a member from the team, be clear and concise about the reasons why, and offer support for their transition out of the business. It may be appropriate for them to work their notice from home, though we would not recommend that you isolate them from the team entirely.



sentients
Cybersecurity Executive Search

Days Sixty One to One Hundred

The First Board Meeting

There's no question that reporting to the board for the first time can be a daunting experience. This skill has become an essential part of security leadership role profiles and search briefs, often for businesses with little understanding of risk and security outside of regulatory compliance.

Setting expectations, both for yourself and the board members, well ahead of the first quarterly presentation, can be helpful. The first step to achieving this is through interviews with stakeholders across the business to assess their understanding of risk and internal vocabulary; can they differentiate and define the differences between information risk, technology risk and business risk? This helps prevent any misunderstanding and informs your choice of language.

Straightforward risk management KPIs, directly linked to business objectives and key departments, should form the basis of your presentation and discussion. In the early days of your tenure, demonstrating a reduction in events, response times to events and any other quick wins you've managed to achieve, will reassure and disarm audiences expecting a more damning appraisal of capability and demands for increased budget.

When speaking with non-technical CxOs, it would seem obvious that we avoid using technical jargon, but this is the default language of many technical leaders, especially when put under pressure. Do also remember that your definition of 'technical' may be different to the board's. Don't assume that they understand basic infosec terms such as 'malware', otherwise you risk making senior leaders feel uneducated and disengaged. For your first presentation, we suggest that you adopt some of these commonly-used metrics and define their meaning and relevance;

1. **Cyber Risk Level vs Risk Tolerance**
2. **Top Five Risks, Prioritised**
3. **Intrusion Attempts**
4. **Volume of Internal vs External Security Events**
5. **Capability Maturity Scorecard vs Competitors**

On the other hand, some senior leaders may have a sophisticated understanding of information security and the threat landscape for your business, so do ensure that your metrics stand up to scrutiny and that you are have more detailed analyses ready at hand.

sentients
Cybersecurity Executive Search

Summary

Navigating through these first days in a new organisation can be taxing, and a coherent plan can be helpful in maintaining a calm, pragmatic approach that balances your engagement with people, strategy and evaluation of the existing capability. Rarely do we get to see and experience the difficulties of the business until we sit within it for a period, though our tendency is to try to make a meaningful impact from Day One.

This guide assumes that you already have a level of technical and managerial competence, and does not include detail on how to audit systems, conduct tooling reviews and get under the hood of your security environment. Rather, we highlight the areas of neglect, and the new areas of focus we have seen creep into security leadership searches which we execute on behalf of a diverse portfolio of clients.

These sometimes appear in the 'soft skills' area of job descriptions, low down on the bullet pointed shopping list. And yet, these are frequently the areas of failure that lead to short tenures; lack of engagement from teams and senior stakeholders which erodes that initial goodwill, isolation and burnout in leaders who do not connect with their peers and external partners, and, most frequently, a lack of visibility into the business culture and true risk appetite.

We do hope that you've found this guide to be a useful supplement to your other trusted resources. In order to produce these recommendations, we referred to Niamh O'Keefe's excellent 'Lead Your Team in Your First 100 Days', 'The First 90 Days' by Michael D. Watkins, and several shorter works from cyber security vendors, leadership institutions and industry publications. These works offer a great deal of support and reassurance as you transition, though we would also encourage you to connect and talk openly with others who've been through this process of personal change, both inside and outside of the information security community.

sentients

Cybersecurity Executive Search

About Sentients

Sentients is a leading international executive search firm, specializing in finding cyber and technology leaders. We help companies ranging from iconic tech giants to exciting VC-backed cyber and tech scale-ups.

With over a decade in building the most comprehensive talent network of CISOs, CSOs, and security leaders across industries, Sentients actively contributes to the cybersecurity landscape whilst making impactful placements to enable secure technology growth.

Our business is founded on treating people differently; building genuine, long-term trusted relationships with our clients and candidates alike. Our Partners and Associates share the vision of working with honesty, integrity, and transparency at our core.

info@sentients.io

https://sentients.io/