STOTTANDMAY

The CISO Survival Guide

Practical advice for Security Leaders

Contents

5 questions to ask before taking a CISO role

The evolution of the CISO role

The most common mistakes CISO's make

The first 100 day plan

5 questions to ask before taking a CISO role

Author: Stephen Singam
Chief Information Security Officer
& Venture Capital Advisory

Stephen is a senior professional in the cyber security industry with extensive experience in Financial Services, Start-ups, Media & Entertainment and Consulting. He has held senior cyber security positions across a range of geographies at Hewlett Packard, Bank of Australia, 20th Century Fox/News Corporation, Salesforce.com, IBM and Nokia.

He is a regular speaker at industry events such as Tech ROI, New York Times Business-Innovation, RSA Conference, B-Sides, UK's KTN and PwC's Data Privacy & Big Data and Silicon Valley's ISACA Annual Meetings. In addition, he is on the Advisory Board at numerous cyber security start-up ventures and was a reviewing member of the 9th working draft of the United States Government NIST Cloud Computing Standards.

1. Who will I be reporting into?

It's important to understand straight from the outset what your reporting line will look like. Organisational design and stakeholder engagement will have a significant bearing on your ability to build a security function that moves the needle for the business. The size and sector of the company you are potentially coming into will obviously also have a bearing on who you end up reporting into. For example, in smaller organisations it's more likely you'll have a direct line into the CEO and certainly, in industries such as online banking, where security is core to the proposition, there's a higher chance you'll have board level influence. But this reporting line question is important to note because as a CISO it is essential to be empowered politically within the organisation. Getting to the root of this will help provide an indicator as to whether the board see security as a strategic differentiator or a compliance box-ticking exercise.

Historically it's been common for CISO's to report directly into the CIO. There are two challenges that come to mind here. Firstly, security has become more complicated and pervasive than ever before. There are so many 'unknown unknowns' that the CIO reporting line perhaps isn't as natural as fit as it used to be. There comes a point where you should ask the question: how can the CIO advise, council and be accountable for a department that they might not fundamentally understand? We should then also factor in the fact that the risk is becoming much bigger than the CIO. This is now an issue that impacts the entire boardroom. Cybersecurity has evolved to become a business risk rather than just a technology risk. CISO's reporting directly into the CIO will need to be mindful of these issues and develop a clear strategy to avoid becoming just another 'technology problem' for the organisation.

Another 'option' in terms of reporting lines is into the Chief Risk Officer. This is often deployed in organisations that operate across a range of different geographies as regulatory compliance demands become more complex and nuanced by territory. Whoever you do end up reporting into it's essential that as a CISO you have discretions and accountability in your own right and aren't reliant on Chinese whispers from the boardroom.

2. What cyber risks are keeping the board awake at night?

The average shelf life of a CISO is around 18 months. To ensure longevity in the role you need to be mindful of the headline issues that you will be tackling from day one. This question will help to uncover some of those high-level themes. One of the key challenges of our roles as CISO's is to translate cyber risk into a language that the board not only understands but buys into. Your first step on this journey is to assess the board's appreciation, maturity and understanding of the current threats facing the business. This will put you in a position to articulate risk appropriately and ensure it's understood to avoid the challenges associated with misalignment between board expectations and operational expectations. How often have we seen situations where the board say they 'were not informed' in the aftermath of a breach? It's prudent to get a solid understanding from the outset of the risks that the board are aware of and their potential impact on the business. In effect, your goal is to simply ask the question 'where are we complying and where are we not'?

3. Has the company completed a business impact assessment?

Identifying risks with the board is one thing but it's all for nothing if those risks cannot be prioritised effectively. One way of achieving this would be to ascertain whether a Business Impact Assessment (BIA) has been conducted. The goal of such a project is to identify and evaluate the potential knock-on effect of risks to actual business operations. For example, the maximum amount of time a business process can be obstructed before the organisation's financial objectives or legal commitments are compromised. The net outcome is the ability to understand the financial, legal and reputational impact of a given scenario. This can be a powerful tool to win investment in the cybersecurity function as a clear association can be made between risk and the financial implications of that risk. It will inform recovery plans. It will impact incident response procedures. Perhaps more importantly, it will help you understand what will actually impact the bottom line. It comes back to knowing the environment you are walking into as a CISO. If you don't know the situation at hand it's hard to know where you are going and how you will add value.

4. How do you measure success?

Continuing the same theme of establishing a clear frame of reference make sure you find out right from the initial conversations what success looks like. How do they want to measure success? Let's not just be busy for the sake of being busy. It can't just be a case of doing 'things'. What are the goals? What is your department going to stand for? Get a deeper appreciation of what really matters to the customer. How can you make a measurable impact on the value proposition? It's much easier to justify investment when you are passing on value to the customer. These questions are important because they take you to a more strategic place rather than merely focusing in on the operational. That's not to say that the operational side isn't important. There are a few measures you might want to focus in on here:

- **Mean-Time-to-Detect & Mean-Time-to-Respond**
- **Number of systems with known vulnerabilities**
- **The number of users with "superuser" access level**
- **Number of days to deactivate former employee credentials**

5. How will we collectively gather intelligence?

You may also want to get a better understanding of what type of stakeholders the leadership team are likely to be. How much participation will you get from them? How keen are they to proactively work with you to move the security agenda forward? This question around collectively gathering intelligence effectively asks these direct questions in a more indirect way. CISO's need to be able to align with the strategy of the business. To do that they need to have insight into the risks that ultimately exist within the organisation. As a CISO you are not going to be effective unless you can collaborate effectively with the board in the identification and prioritisation of risk. It's no good finding out after the fact.

> "CISO's need to be able to align to the strategy of the business. To do that they need to have insight into the risks that ultimately exist within the organisation."

The evolution of the CISO role

Author: CISO incognito

Our mystery CISO covers the key topics surrounding the evolution of the role from boardroom engagement through to the build or buy debate. We tackle some of the key questions facing CISO's today in this rapidly changing market where risk is seemingly everywhere and prioritisation is essential.

There's a lot of talk about cyber security moving up the board's whiteboard of priorities. How much of that is hype vs reality?

I would certainly agree that cyber is genuinely moving up the board's agenda – particularly in enterprise level organisations. I put this more down to customer demand than anything else. The customer is becoming far more knowledgeable about security. They know what they want from a partner or supplier and know how to validate what they are getting.

In more and more sectors, security is a pre-requisite to the offering and is a feature customers won't take lightly. At a macro level regulation is also driving a focus at board level, coupled with a desire to protect against the reputational and financial damage of becoming front page news. The net result has been risk and audit committees getting more face time and attention at board level over the last 12 months.

How have the demands placed on the CISO evolved over the last 18 months?

Growing expectation and demand is something that needs to be managed by the CISO. Security is all too often seen as a firefighting capability and that's not good enough in a corporate world. It's become essential to operate in a more controlled fashion. The CISO needs to be accountable for formally documenting the services the security function offers to both the business and its customers. We are talking about 'demands' here but there is an association between demand and the capabilities of the team. If the security team are ineffective then the business will go off and do things themselves, which exacerbates the challenge.

We talk a lot about risk in our line of work but the opposite to risk is opportunity. Every business is looking to grow and deliver their service more effectively. There is, quite rightly, a growing expectation for the CISO to define what we do as a function to help the organisation grow, whether that's delivering services better with more control or simply stopping things from failing so frequently. I'd also say that our remit is about more than just the information security side of things. The CISO needs to understand business continuity, commercial management, supplier management, program management and service delivery management. Everything we do should be targeted at driving the business objectives and as a community we need to get far better at expressing that.

How would you go about making the business case for further investment in cyber security initiatives?

Building a business case for investment in cyber security is pretty much the same as any other business case. You need to understand who your supporters are and what motivates them. You need to be clear about what the benefits are actually going to be. You need to be clear about how the initiative will be funded, is it a capital project for example? Could you sell the benefit on to the customer? None of this is likely to be new information but bringing your sponsor along the journey with you is key.

Sometimes it's about benchmarking and ensuring everyone understands where you are today. There are plenty of reference points to utilise from internal audit reports through to external maturity assessments. To get that investment you need to paint a very clear picture of what the organisation looks like today and where you want to be.

Would you say that motivation to invest in cyber security initiatives is all about 'sticks' or is there a lot more 'carrot' in there too?

I am going to swerve the question slightly and say it's all about good financial planning. Investment in cyber security is about understanding who you are, who your customers are and assessing each other's maturity levels. Then it's a case of working out what the delta is and how you bridge that gap. There's always going to be carrots and there's always going to be sticks and the two aren't mutually exclusive.

What advice would you give to a CISO who is literally overwhelmed with potential projects? When risk is everywhere how do you prioritise?

My advice would be to agree a clearly defined program of work with the business as quickly as possible. There's a few steps you should look at taking to achieve this, some you can do yourself and others will rely on your internal and external stakeholders.

Firstly, on the more technical side, you need to understand where the vulnerabilities are. You need to actively review events as they happen on the network. You also need to look at how you are managing incidents. For me solid preparation is 90% of the battle here. At some point something will happen and everybody needs to know what their roles and responsibilities are. How are you going to run that incident? Which 3rd parties will you be calling upon? Then rehearse, rehearse, rehearse.

Finally, on the technical side you need to do an impact analysis on those scenarios and that will undoubtedly help you with the challenge of prioritisation.

It's important to hear lots of voices. Don't just plough on with your own agenda without considering the issues of the stakeholders that make money for the business. In defining your program of work make sure you don't include too many white elephants. Look for quick and meaningful wins like a repeatable, continuous vulnerability management capability for example.

How good a job are security teams are doing in terms of understanding the business and translating risk issues effectively?

As a community we absolutely have to get better. I think there is still an element of doing security for the sake of security; risk assessment for the sake of risk assessment. But that counts for nothing if it's not adding value to the businesses proposition. I always want to be in a place where we target everything we do against the strategy of the business or the customer.

To make that step change we need to inspire our teams to think outside the 'security 101' textbook. I am also a big believer that we should be placing a heavy emphasis on development. All roles should have a clear terms of reference that include a level of stakeholder management. Skills are important but given the shortage that exists it's rare that you will find a candidate that has every attribute you are looking for. In such cases it's often a good idea to develop from within where you'll find people that know the business and know the stakeholders – that's a great starting point.

Do you think there is a difference in terms of perception and reality when it comes to who really owns the risk between the CISO and the business?

I think 10 years ago the perception might have been that security owned a lot more of the risk. That has probably changed somewhat as security functions get better at defining and revising their risk management processes. This is important as unless people in the business understand their roles and responsibilities we ultimately can't manage that risk for them. I like to think of it that you will have risk owners who ultimately sit within the business and risk managers that sit in security.

The issue of MSSP's and whether to insource or outsource is a really hot topic. What's your take on it?

Whenever you look at the question of whether to build or buy you need to think about what's right for the organisation. I often find it helpful to look at external options first and move forward from there. The key to the build vs buy debate to my mind is understanding which requirements are a commodity and which are truly bespoke to your organisation. 1st line security services might be a relevant example. You might not be trying to reinvent the wheel here. It's like when you go to buy a car do you look at the proven manufacturers first before you build a custom one from scratch? I'd be tempted to.

> “Unless people in the business understand their roles and responsibilities we ultimately can’t manage that risk for them. I like to think of it that you will have risk owners who ultimately sit within the business and risk managers that sit in security.”

The most common mistakes CISO's make

We canvassed the views of our CISO network to pull together a helpful list of things to avoid if you want to create successful outcomes in role. If you want to learn from the past mistakes of others then read on.

Avoid 'the sky is falling approach'.

As a CISO role your role is to solve problems not to create them (or make them seem worse than they actually are). The board are ultimately not interested in constant reactive fixes (it makes it hard for them to separate the small stuff from the big stuff) and want to hear about how they can help in a proactive way. If you are seen as the creator of FUD (Fear, Uncertainty and Doubt) on every single risk issue then it will become harder for you to win investment in a genuine crisis.

Don't become an island.

It's critical that security doesn't become a siloed department. If people don't have visibility of the function they will just go off and do things by themselves. Have a vision and make sure the business understands that vision. If you don't have a mentor then get yourself one. It's important (certainly in the early years) to have a genuine peer to bounce ideas off. After all, that's what security is about, leveraging different views to make us safer. You also may want to consider how you are engaging with the vendor and IT analyst communities. Are they adding value to your strategy or taking too much time out of your diary?

Don't just rip and replace.

Nobody likes to admit that their child is ugly and a change in leadership within the cyber security function is a great opportunity to move the strategy in a different direction. But do your due diligence. Don't just burn the house down and start again to make a political point or because you have a preconceived notion of how the world should look. It won't endear you to your new team or your incumbent suppliers. Understand what's working and what's not and define a clear programme of work based on priorities.

Never accept the status quo.

The company will constantly evolve and change. Security needs to grow organically with the organisation, so there's never going to be an opportunity to rest on your laurels no matter how good your track record has been previously. Challenge your teams to understand the business. Challenge the business to move outside of their comfort zone. You need to lay down these challenges (in the right way) in order to find new ways to succeed.

Avoid becoming the department that says no.

Every business process carries an element of risk. We have to remind ourselves sometimes as CISO's that our role is to enable the business rather than restrict it. It's your job to be visible, walk the halls, press the flesh and be seen as a champion of the business in the quest for competitive advantage. You can't build that relationship and trust with business owners if they think you're here to hinder rather than help. It's your responsibility to manage the balance between business risk and technology risk to really move the corporate needle.

The first 100 day plan

The four key pillars to focus on.

Security Strategy and Corporate Governance

Revise or create security strategy, governance and operational model.

Identify key critical corporate data by locations, functions, ownership and risk value.

Revise or create corporate security policy, standards & operating procedures.

Security Transformation

Review and adjust security human, intellectual and corporate fit and capital.

Review and define security operations and of the business and corporate partners.

Data Protection

Review all privacy and regulatory compliance efforts to date.

Review and re-define governance, regulatory and compliance (GRC) reporting.

Incident Response and Digital Resiliency

Review and test the current incident response plan (IRP) and DRS plans.

Incorporate threat intelligence and information from fellow CISO peers.

Here are some important initiatives to work towards in the early part of your tenure as a CISO that should form part of your objectives:

1. Facilitate better stakeholder management between security and business & data Owners, which can be addressed by focusing on the corporation's business risks foremost rather than via common Security Policy/Audit/Technology hard-hammer approaches.

2. Deploy a Defensive Security Architecture such as zero trust model rather than using "whack a mole" reactive approaches.

3. Perform an enterprise threat and vulnerability management assessment on one of the most critical applications, or infrastructure and concurrently prepare a practical and cost-effective cybersecurity program as part of the first 100 days.

4. Embed security personnel, processes, awareness, and technologies within the business stakeholders, technical architects and application developers organizations from a ground-up level rather than top-down - an organic ecosystem approach.

STOTTANDMAY

About Stott and May

Founded in 2009 Stott and May are a professional search firm with a passion for helping leaders achieve complete confidence that they have hired the right talent, first time in fiercely competitive markets. We believe you should never have to make the choice between quality of candidate and time to hire.

As a result, our business has been founded on the principle of offering a premier standard of search service delivered in vastly accelerated timescales, that our competition simply cannot match. Because after all this is about more than just recruitment, it's about turning your business vision into reality.