Guide to Developing a CYBERSECURITY ROADMAP

How to plan for success

SHEARWATER™
securing your information

Introduction

If you're like most IT managers and security managers, chances are you can recall a pointed – and challenging – conversation with a senior executive about your organisation's cybersecurity. And that's no surprise. Whether you're working for a small business, an established company or a government department, executives tend to ask the same difficult questions about cybersecurity:

1 Are we compliant?

What they're really asking is...

What standards do we need to meet or exceed?

Have we met them, and will we continue to meet them?

What do we have in place to ensure that we maintain our compliance?

2 Are we secure?

What they're really asking is...

Do we understand our risks and threats?

Do we know our key assets?

Are we protecting them?

3 Are we more secure than last year?

What they're really asking is...

What's changed in the security landscape or within our organisation in the last 12 months?

How are we meeting those new challenges?

Where did we improve?

4 What do we do in case of a breach or attack?

What they're really asking is...

What incidents have occurred in our organisation and/or comparable ones?

How were they handled?

What did we learn?

How did we adapt?

Asked individually, these questions can be confusing and difficult to answer. However, when asked together, they paint a useful strategic picture of the state of an organisation's cybersecurity. They also establish the foundations for developing a cybersecurity roadmap.

This Ebook draws on Shearwater's extensive experience in cybersecurity to help you successfully plan your cybersecurity roadmap. It provides an overview of:

- *What good cybersecurity looks like*
- *How to assess your cybersecurity practices*
- *Where to begin developing your cybersecurity roadmap.*

A cybersecurity roadmap is an essential tool for any organisation that seeks to protect its customers, employees and corporate information.

What does good security look like?

The first step in developing a cybersecurity roadmap is understanding where your organisation is at present, and where you'd like it to be in the future. To do this, you need to define the characteristics of your cybersecurity approach as well as its specific *enabling functions*.

Good cybersecurity has the following characteristics:

Security is proactive, not reactive.

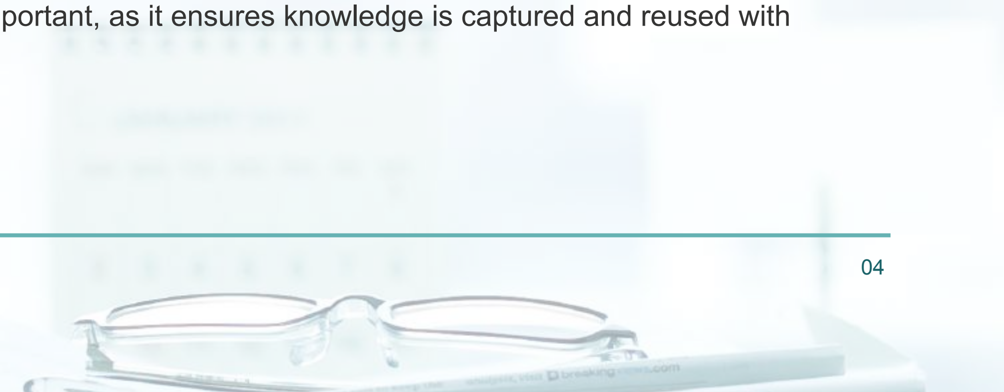
In many organisations, IT and security teams are purely reactive. They have limited ability to plan ahead, and they're constantly responding to requests along the lines of: "Hey, I know it's 4pm on a Friday, but this project needs to go live in a few hours. Can you please approve it?" An effective cybersecurity roadmap avoids these last-minute requests because it proactively identifies upgrades and changes. IT and security teams have more time to focus on strategic activities that support the detection and mitigation of potential threats, instead of putting out fires.

Security is unobtrusive.

Cybersecurity teams exist to enable the operations of the broader organisation and allow business objectives to be achieved in a secure manner. Security that is in-your-face or over-the-top can generate obstacles, especially if it gets in the way of employees as they try to do their jobs. At the same time, nobody ever thanked an IT team for rejecting every request that is put forward. There's a balance between stifling bad ideas and allowing organisations to deliver, but it's difficult to achieve without identifying which objectives are the most important.

Security processes are repeatable and documented.

Whatever steps an organisation takes to achieve cybersecurity, they need to be repeatable – solve the problem once and then move along. This approach allows IT teams to focus on high-value work rather than fixing the same issue over and over. Documentation of key processes is equally important, as it ensures knowledge is captured and reused with minimal effort.



There is a risk management mindset.

Good security is premised on having a strong understanding of what the risks or threats are, how they will be addressed and how they can be avoided. Every organisation can benefit from a solid grasp of what's happening in cybersecurity, both internally and elsewhere, to make informed decisions that support business objectives.

So, what does it take to embed better practice security practices in an organisation?

We've identified four key functions, although their specific operations may vary depending on the maturity of your organisation.

01

Risk and compliance:

An effective risk and compliance or governance function will help your organisation to identify what needs to be protected and how best to go about it. To do this well you need to identify your assets, know your risks, choose your controls, agree your metrics and have the right policies in place.

02

Security administration:

This is a fairly standard function, but nonetheless an important one. Security administration covers tasks such as adding and deleting users, managing access and conducting reviews.

03

Security architecture and design:

This function liaises closely with the business to better understand their requirements, identify products that are needed and manage the impacts. In other words, it identifies what needs to be protected and how you will be sure it's protected well. Early engagement with the business is key to success here.

04

Security operations:

This function detects, identifies and responds to the workloads that come your way. The main objectives are to achieve visibility on networks, servers and endpoints, and ensure that all tools are working to deliver their intended purpose.

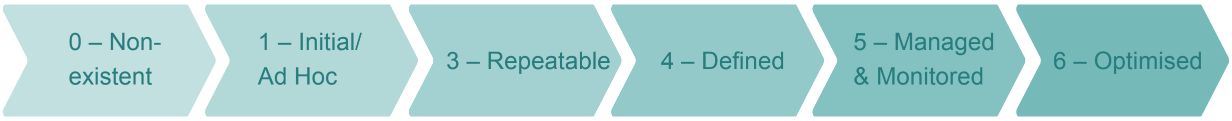
Assessing your cybersecurity practices

Before developing your roadmap it's sensible to assess your organisation's cybersecurity maturity. This simple activity is valuable because it helps to determine where to start strengthening cybersecurity in your organisation.

There are many models to assess maturity. These include:

Cobit
Open-ISMs
ISO 27001
NIST
Australian Government Information Security Manual (ISM)

We have used a simple five-point scale, shown in the table on page 7, which broadly aligns to the Cobit 4 model below.


0 – Non-existent

1 – Initial/ Ad Hoc

3 – Repeatable

4 – Defined

5 – Managed & Monitored

6 – Optimised

To assess your organisation's maturity, read through the characteristics on page 7 and identify the level that best resonates with your current cybersecurity environment. If you need more guidance, you can review our list of questions for assessing cybersecurity maturity – see Appendix A.

You may find it valuable to discuss this table with others in your organisation. In organisations with lower maturity, it's often the case that a document or process does exist, but only a single individual or a small pool of staff is aware of it.

Maturity Level	Characteristics
0 – Non-existent	• Limited beyond firewall and AV
1 – Immature	• Security administration function may be occurring • No policies – people ‘know’ what to do • Some technical controls implemented • There are no real plans to move forward or improve security
2 – Doing our best	• Security administration function is working • There is a policy, or policies are being developed • Developing risk and compliance and/or security operations • Technical controls are basic with some customisation
3 – Getting there	• Security administration is working • Policies and processes are defined, communicated and known • Security operations have visibility of critical assets • Risk and compliance is being performed • Technical controls have full coverage and are configured correctly • Starting to get involved in projects
4 – Mature	• Risk and compliance function exists • Security architecture and design is established • Security administration has regular reviews • Security operations has visibility of the environment and responds to issues • Policies and processes are in place and reviewed regularly • Technological controls are in place and reviewed regularly
5 – Very mature	• Risk and compliance function is established and working • Metrics are in place and used to inform activities • Security architecture and design engages early with business • Documented security architecture exists • Security administration is automated • Security operations has visibility and is reducing response times • Policies and processes are in place and reviewed regularly • Technological controls are in place, reviewed and automated • Advanced tools are deployed if required

Your organisation may have different maturity levels for each security function. Overlaying maturity scores with security components functions in a structured framework, such as the NIST cybersecurity framework, will help to clearly identify areas for improvement.

NIST cybersecurity framework

Domain	Subdomain	Risk & Compliance	Security Architecture & Design	Security Adminstration	Security Operations
Identify	Business Context	1			
	Asset Management	0		3	2
	Governance	2			
	Risk Assessment & Risk Management	3			
Protect	Access Control		2	3	
	Awareness Training	3			
	Information Protection processes & procedures		1		3
	Protective Technology		1		3
Detect	Anomalies and Events				2
	Monitoring				3
	Detection Processes				4
	Detection Technologies				3
Response	Response Planning				2
	Communications	2			
	Analysis				3
	Mitigation		2	1	3
	Improvements		2	1	2
Recover		4	2		3

Overlaying maturity scores with security components functions in a structured framework, such as the NIST cybersecurity framework, will help to clearly identify areas for improvement.

Developing your cybersecurity roadmap

Once you understand best practices in cybersecurity and have assessed your organisation's maturity, you're ready to start building your cybersecurity roadmap.

Identify key assets and threats

The first step in developing a cybersecurity roadmap is to identify the assets you're protecting. What are your crown jewels? Where are they located? From what do they need protection? This step involves active consideration of the business context, combined with straightforward asset management, risk assessment and threat management processes.

Prioritise risks and threats

There are many ways to prioritise risks and threats, with the right approach depending on the context of your organisation. In any case, there are three questions that will help you to identify top priority risks and threats:

01 What are the active and current risks or threats that are relevant to your organisation?

02 From a security perspective, what are the main concerns of senior executives?

03 Which risks and threats would hurt your organisation the most?

Next, identify the treatments for each risk or threat. Classify them as 'easy wins', 'high cost', 'biggest impact' and 'hardest to achieve.'

Think about changes that will have the most impact on improving your maturity scores. For example, there may be more benefit investing in moving from a 0 to a 2 than from a 3 to a 5.

Set achievable goals

While a cybersecurity roadmap should identify all activities that you'd like to undertake, you need to identify those goals that will be truly achievable. Few people have said, "We'll finish this identity and access management program in less than six months," and still believed it was possible half a year later.

- *Start with the basics.* If you don't have policies, focus on publishing key documents – acceptable use and cybersecurity policies are a strong foundation that will drive the rest of your efforts.

- *Focus on high-risk areas first.* This one speaks for itself, but it's worth reiterating that you should address exposed high-risk areas as a matter of priority.

- *Leverage what you have.* Review the tools you already have in place and identify opportunities to improve or extend their capability. Many people are surprised when you remind them that, for example, their antivirus tool can also perform intrusion detection.

- *Link goals to business objectives.* Identify the business reason for each goal or activity. For example, management is unlikely to be convinced by "We need a new firewall." It's far more compelling to argue that "We need a new firewall so that staff can easily access the data they need to do their jobs." Your communication approach is essential to securing the endorsement of senior executives.

Conclusion

A cybersecurity roadmap is an essential tool for any organisation that seeks to protect its customers, employees and corporate information. By defining the current and future state of a cybersecurity landscape, it provides the clarity and assurance about cybersecurity that senior executives crave. A cybersecurity roadmap also enables IT to communicate effectively about how cybersecurity capability is positioned within an organisation.

Building a cybersecurity roadmap doesn't have to be laborious or overly theoretical. By beginning with high-level objectives and adding details as you progress and mature, you'll be well on your way to success.

Next steps

To get started developing a cybersecurity roadmap for your organisation, contact Shearwater Solutions today:

🌐 www.shearwater.com.au

☎ 1300 228 872

About the author

Mark Hofman is Shearwater Solutions' Chief Technology Officer. He has over 25 years' experience in information security. He has worked for both private industry and government and has provided a wide range of cybersecurity consulting services to organisations in the financial, private and government sectors.

Mark is a certified instructor for the SANS Institute and he has trained and lectured internationally. Mark holds professional certifications including CISSP, GIAC GCFW, CompTIA Security+ and BSI lead auditor accreditations.

Appendix A – Evaluating your organisation's cybersecurity maturity

For all questions ask: *"Is it documented, and do the right people know it exists?"*

Do you have the following policies?

- Acceptable use policy
- Cybersecurity policy
- Others?

Is there a risk assessment process?

- How long ago was the last risk assessment?
- What happened with the findings?
- What percentage of treatments were implemented?
- Were high risks retested?

Do you have an asset register?

- How up to date is it?
- Does it include information assets?

If your crown jewels left the organisation would you know?

- Would you recognise them?
- Do you know where they are now?

How many dormant accounts exist?

How accessible is your data?

- When was it last reviewed?

When was the last security awareness training course you attended?

Who approves access to data?

How are accounts created?

Who has responsibility for:

- Creating, deleting changing users?
- Conducting user reviews? When was the last one?

How frequently do you look at your logs?

- When something breaks
- When you are notified of a breach
- Every day, all day

What do you look for when reviewing logs?

Do you have tools in place to help?

Do you collect the right information?

Do you have an incident response plan?

- When was it last used?
- Did you identify the root cause?
- Did you fix it?

Were the recommendations accepted and implemented?

How soon was the machine compromised again?

How was security improved?

About Shearwater

Shearwater is a specialist information security service provider with an unwavering focus on providing service excellence across our portfolio of services. Since 2003, we have enabled millions of secure interactions across government and private sectors.

Shearwater's expertise include security education, security operations management, security consulting, and application security including penetration testing. Our highly developed methodologies enable organisations to implement best security practices and help them achieve, maintain and prove compliance against a range of security standards.

Shearwater focuses on helping you manage the security risks associated with running your business whilst providing actionable recommendations to the internal security team. We pride ourselves on client communication, customer service, fast response, and on-time delivery. Learn more at www.shearwater.com.au.

Whatever your Information Security challenge, we're here to help you find the right solution.

Sydney I Melbourne I Canberra I Brisbane I Perth