Whitepaper

Best Practices For Developing A Cybersecurity Roadmap

VIRTUELLE
GROUP

Best Practices For Developing A Cybersecurity Roadmap

WHEN IT COMES TO CYBERSECURITY, IT'S SAFE TO SAY THAT FEW COMPANIES ARE ON THE FRONT FOOT. OVER HALF A MILLION AUSTRALIAN BUSINESSES FELL VICTIM TO CYBERCRIME IN 2017,[1] WHILE 70 PERCENT OF RESPONDENTS IN A RECENT SURVEY ADMITTED THEIR ORGANISATIONS ARE UNPREPARED TO DEAL WITH A CYBERATTACK.[2]

From hacking, ransomware attacks and phishing through to data breaches and distributed denial of service attacks, poor cybersecurity affects businesses across all industries, with significant consequences.

Medium-sized Australian businesses, for example, can expect to be left **$1.9 mil** out of pocket in the event of a cyberattack.[3]

They may also suffer from reputational damage, a loss of customer trust, and - particularly for those in the finance industry - increased audit exposure and regulatory scrutiny.

That is not to say that businesses aren't taking steps to thwart cyberattacks. Most have some security protocols and protection in place, but often focus on 'putting out fires' rather than proactively planning to prevent and mitigate threats. This approach is risky at best, as underinvestment in active cybersecurity defence leaves organisations exposed and vulnerable to threats.

The good news is that there's one step every CIO/CISO can take to transform their organisation's approach to cybersecurity: develop a cybersecurity roadmap.

A cybersecurity roadmap is a powerful, strategic and actionable tool that:

- **Articulates the current state of an organisation's IT security landscape,** including identifying potential vulnerabilities
- **Outlines future goals** for ensuring that information and data security is upheld in the face of changing cyber threats
- **Sets out a pathway** – linked to tangible projects and activities – for the organisation to achieve identified future goals within an agreed timeframe

This whitepaper will explain why every business needs a cybersecurity roadmap. It will focus on defining effective cybersecurity, and provide guidance on developing a cybersecurity roadmap for your own organisation.

[1] SMB Cyber Security Survey Australia 2017, Norton.
[2] Cyber Readiness Report 2018, Hiscox.
[3] Cyber Threats in Small to Medium Australian Businesses 2017, Webroot.

Effective Cybersecurity In Action

Before developing a cybersecurity roadmap, it is critical to have a strong understanding of how effective cybersecurity benefits the organisation and what good cybersecurity practices look like for the firm. This serves as a starting point when assessing how well the current IT environment protects against cybersecurity threats, and in determining the next steps to achieve cybersecurity goals.

An organisation with effective cybersecurity typically ensures that:

DECISION MAKERS ARE AWARE OF HOW THE CYBERSECURITY LANDSCAPE IS CHANGING

As cybercriminals get smarter, cybersecurity measures that worked in the past will not be as effective today. It is also important to understand that the infrastructure we need to protect today is different than it was in the past. Historically, we needed to protect computers and desktops in our offices. Now, with more organisations storing data in the cloud, allowing employees to work on mobile devices and offering remote work options, bedrock IT security methods such as firewalls and anti-virus software are no longer enough to defeat attackers. Organisations also face new security challenges, such as those identified by the Australian Signals Directorate:

- **Cyber incidents are happening more frequently,** on a larger scale and with greater severity
- **Attempts to compromise networks** are becoming more diverse and innovative
- **Distributed denial of service (DDoS) incidents** are increasing in frequency and scale
- **Cybercriminals are becoming more sophisticated** and using deliberate targeting[4]

Organisations that excel at cybersecurity have IT teams that stay up-to-date with relevant trends and proactively educate employees across the business.

SECURITY AUDITS ARE REGULAR AND COMPREHENSIVE

It is almost impossible to truly understand the effectiveness of an organisation's cybersecurity capabilities without assessing its:

- **IT assets**
- **Security practices and policies**
- **Levels of user compliance**

Organisations with effective cybersecurity understand their IT landscape and have mechanisms in place to encourage and/or enforce compliance.

SOFTWARE AND SYSTEMS ARE KEPT UP TO DATE

With the speed at which vulnerabilities can be detected and exploited, keeping software and systems up-to-date with the latest security updates is a non-negotiable. Organisations with effective cybersecurity plan these updates ahead of time and 'push' changes to users, rather than allowing individuals to delay changes to when it suits them.

DATA IS BACKED UP AND SECURED

To minimise the impact of a potential cybersecurity attack, organisations with effective cybersecurity conduct daily data back-ups. They have physical barriers in place to limit access to information assets (e.g. restricted access, locked server rooms).

SECURITY PROCESSES ARE MATURE

Information security processes are documented, accessible to IT staff, applied consistently and simple enough to be repeatable. Effective security should not rely on the knowledge or expertise of a single individual, nor should there be excessive effort involved in problem-solving known issues.

IT SECURITY ENABLES BUSINESS TEAMS – AND DOESN'T OBSTRUCT THEM

Organisations can go too far in enforcing cybersecurity practices that prevent teams from working in an efficient and timely manner. Effective cybersecurity strikes a balance between preventing information security risks, and giving teams the freedom to achieve their goals.

ORGANISATIONAL LEADERSHIP IS ALIGNED ON CYBERSECURITY

Organisations with the most effective cybersecurity capabilities have IT teams that communicate about cybersecurity technologies, risks and mitigations in plain language. As a result, their executives and board members can proactively engage in discussions and make informed decisions on matters with significant cybersecurity implications.

As these principles demonstrate, effective cybersecurity requires a whole-of-organisation effort. Although cybersecurity is often seen as the domain of the IT team, a broader view is needed to deliver the right balance between cybersecurity and user choice across the organisation. The CIO/CISO must, therefore, understand and engage with the competing goals of IT services, security administration, security architecture, risk management, compliance/legal and core business teams.

[4] Threat Report 2017, Australian Signals Directorate.

Measuring Cybersecurity Effectiveness

A cybersecurity roadmap documents an organisation's current IT landscape and articulates the necessary improvements that will strengthen cybersecurity capabilities in the future. A robust plan to measure cybersecurity at two key points is critical to the success of a cybersecurity roadmap:

- **Understanding the effectiveness of the current IT security programme** is an ideal starting point for most organisations. This helps to determine whether an organisation needs to focus on the cybersecurity basics or if it is sufficiently mature to undertake the deployment of more sophisticated tools and technologies. This assessment should include gathering data from a diverse set of sources (such as interviews with IT staff and organisational leaders, conducting an IT audit and reviewing data relating to information security activities and breaches).

- **Assessing the effectiveness of IT security efforts after cybersecurity initiatives have been implemented** provides valuable feedback on the impact that the projects, activities and initiatives in the roadmap had on improving the organisation's overall cybersecurity posture. This measurement activity should be completed at timeframes defined in the cybersecurity roadmap (typically annually, starting from one year after implementation).

There are many approaches to measuring the effectiveness of an organisation's cybersecurity capabilities. Existing models, such as the National Institute of Standards and Technology's (NIST) cybersecurity framework, provide useful guidance to assess cybersecurity effectiveness. This framework has four tiers that describe the level of rigour and sophistication in an organisation's cybersecurity risk management practices. While these tiers do not officially function as a maturity model, many organisations use them to benchmark their security practices.

Virtuelle's Cybersecurity Framework I-P-D-R-R

I **Identify**
high-value assets

P **Protect**
against known and unknown threats

D **Detect**
attacks

R **Respond**
to suspicious activities

R **Recover**
from breach

How To Develop A Cybersecurity Roadmap

With an understanding of the components of effective cybersecurity and how to measure cybersecurity performance, it's time to start developing a cybersecurity roadmap.

A cybersecurity roadmap is a comprehensive document that communicates:

- The current state of an organisation's IT landscape
- The future cybersecurity capability that will be developed
- The actions that the organisation will take to get there

Above all, a cybersecurity roadmap tells a compelling story to senior executives and decision-makers about risk, compliance and innovation in the information security domain. It provides a basis for IT staff to align their day-to-day work to agreed organisational priorities, and includes a realistic and actionable implementation plan to ensure the future vision can be realised.

There are three key steps to crafting a comprehensive and effective cybersecurity roadmap:

⚠ **Identify key assets**
What are the assets that your organisation owns, uses or manages that most require protection from cyber threats? For example, you may consider software, systems, datasets, sensitive information and critical services/processes.

Prioritise vulnerabilities and threats
What are the internal vulnerabilities and/or external threats that could have an impact on your organisation's cybersecurity? Which are most likely to materialise or would have the greatest impact on your organisation?

◎ **Define actionable goals**
Describe the outcomes you want to achieve to address vulnerabilities and threats, and link them to tangible and time-bound projects, activities or initiatives.

1. IDENTIFY KEY ASSETS

Identifying the assets that are most important to an organisation is essential for ensuring that cybersecurity strategy is focused on protecting the right things. Getting it right requires a solid technical understanding of the organisation's IT landscape, and an excellent understanding of its broader business context and goals. Engaging senior leadership and business teams from a range of business areas to shape this exercise is strongly recommended.

2. PRIORITISE VULNERABILITIES AND THREATS

Drawing on principles of risk management and compliance, this exercise is focused on defining the risks and threats that an organisation faces and determining the level of risk that it is willing to accept.

Consider internal vulnerabilities (e.g. areas where there is underinvestment in cybersecurity or where loopholes could be exploited) and external threats (e.g. cybersecurity risks that are growing among, or most impacting, the industry/sector). Then, assess each vulnerability and threat to judge the likelihood that it will materialise and the associated impact.

Having defined the risk and threat landscape, prioritise those which will be targeted in the cybersecurity roadmap. Identify where 'quick wins' (e.g. easy to implement activities that will realise a benefit quickly) are feasible and prioritise changes that will significantly improve the organisation's maturity and/or cybersecurity effectiveness in line with the future vision. Once again, this step will benefit from engaging organisational leaders and key stakeholders who deeply understand business risk.

3. SET ACHIEVABLE GOALS

Develop an action plan to implement tangible activities that will address the priority vulnerabilities and identified risks within an achievable timeframe. In this exercise, be realistic and focus on activities to improve cybersecurity that are genuinely achievable.

What Next?

Every CIO/CISO needs to understand their organization's information risks and cybersecurity capabilities. With that understanding, it lays the foundation to enhance the effectiveness of their cybersecurity efforts against potential attacks. It is no longer viable to rely on reacting to issues after the fact – there is too much at stake for cybersecurity to be a secondary consideration. A cybersecurity roadmap is an ideal starting point for guiding your organisation towards proactive cyber defence.

Executives would do well to remember that cybersecurity is a rapidly evolving domain. It must be continuously discussed and enhanced to ensure that organisations keep pace with advances in technological threats.

About the Author

Robert Kirtley is an internationally recognised leader in cybersecurity. Robert has 25 years of experience in both technical and leadership positions in IT management, cybersecurity consulting and investigations. Robert speaks on a regular basis at international conferences on three continents regarding cybersecurity. Robert has been involved in dozens of global investigations and has worked as a consultant for leading corporations, government organisations and law enforcement agencies. Robert has testified numerous times as a consultant for clients in jurisdictions in 5 countries and worked as expert for the US Department of Justice.

Share this white paper with your networks to start the conversation, or contact Virtuelle Group for more information:

VISIT	virtuellegroup.com.au
CALL	1300 653 059
EMAIL	info@virtuellegroup.com.au