National Cyber Security Centre

CYBER SECURITY INVESTMENT.

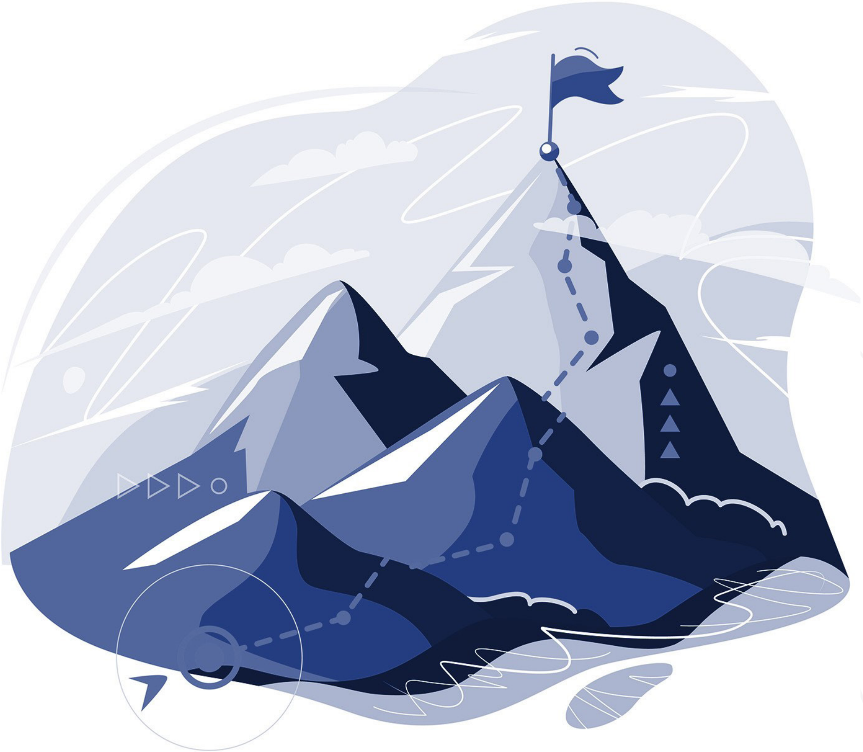
A STRUCTURED APPROACH.

Te Tira Tiaki
Government Communications
Security Bureau

Who is this guidance for?

New Zealand's National Cyber Security Centre (NCSC), a part of the Government Communications Security Bureau (GCSB), has produced this guidance to help business leaders and cyber security professionals better understand and manage their investments in cyber security. This guidance is designed for both government and non-government organisations of varying sizes and capabilities. Investment in cyber security is a complex area, and is highly specific to each organisation's requirements. This document is therefore not an exhaustive guide to the subject, but it can be used as a useful starting point.

This guide accompanies the NCSC's Charting Your Course series of publications on **Cyber Security Governance,**[1] **Incident Management**[2] and **Supply Chain Cyber Security.**[3]



[1] https://www.ncsc.govt.nz/resources/cyber-resilience-guidance/charting/

[2] https://www.ncsc.govt.nz/resources/cyber-resilience-guidance/incident-management/

[3] https://www.ncsc.govt.nz/resources/cyber-resilience-guidance/supply-chain/

Contents

Executive summary

As organisations expand their digital footprints, there are increasing risks to their information assets and their ability to operate and maintain services. These risks prompt expenditure on cyber security and introduce the challenge of rationalising this spending with the organisation's wider investment approach.

Cyber security should be considered as a critical business function. Cyber security investments must be justified and validated in alignment with the organisation's overall business strategy. One vital component of a well-defined cyber security strategy is an investment plan.

This plan ensures that any investments in the deployment, maintenance or improvement of controls are aligned to the organisational cyber security strategy and will deliver outcomes in accordance with an agreed roadmap and alignment with the overall business strategy.

Adopting a flexible investment plan helps the organisation to scale and adjust to meet changing needs in a constantly shifting landscape. By using metrics, it is possible to link the investment plan's outputs to the delivery of organisational improvements. This, in turn, enhances cyber resilience and ultimately assists the organisation in achieving its strategic objectives.

This guide provides practical advice on how organisations can structure their approach to cyber security investments and manage a delivery programme that is aligned to their strategic and financial governance.

Conversation starters appear throughout this document. These are designed to enable senior leaders to initiate useful conversations about cyber security investment with specialists or managers.

Investing in cyber security: where do you start?

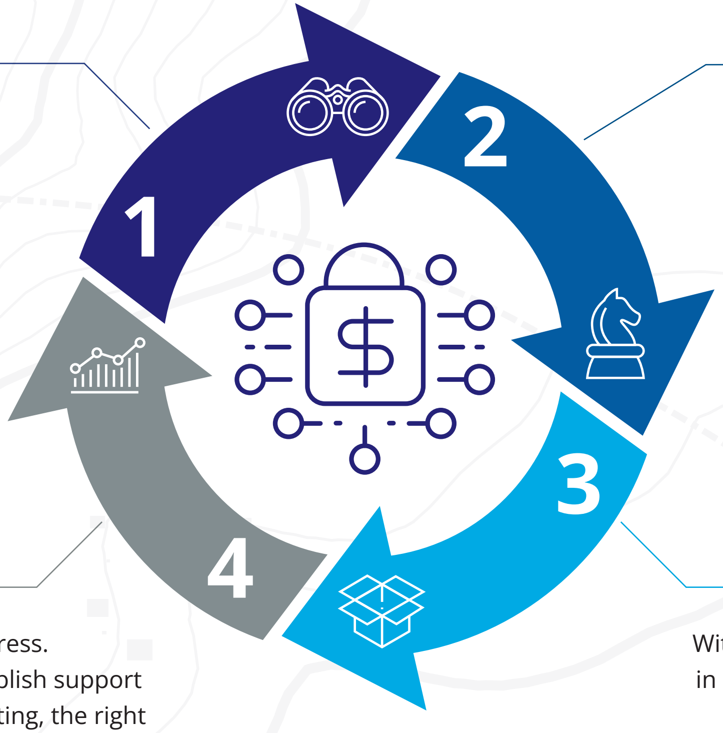
Traditionally, cyber security was often treated separately to other business areas, from an investment and governance perspective. This was due to its relative infancy as a distinct field, and to a lack of definition around the measures that guided this type of investment.

As cyber security has become an accepted part of every major organisation's operational capability, and in many cases the responsibility for it has been designated to senior positions within the organisation, the perception of cyber investment has also changed. The need for increased cyber security funding is leading organisations to ask some increasingly common questions such as, "Are we investing the right amount of money in the right areas to improve our cyber resilience?" and, "Are we tracking the return on that investment?" The response that "risks will be reduced" is no longer enough detail to justify the ongoing investment.

It is important that investment in cyber security is considered in the context of both the threat landscape and the organisation's desired outcomes. It's critical to ask, "What increase in cyber resilience and management of risk can we afford and sustain?" For some organisations, it may be a change in approach to think about investing in cyber security initiatives by presenting them in a clear business context. However, taking the time to align these investments to the organisation's strategy, direction and financial governance is vital to ensuring good-quality investment decisions are made and the best outcomes are achieved. We recommend a cyclical approach to investment consisting of four key phases, shown on the next page.

Cyber security investment cycle

Four key phases



1. Know the landscape

Senior leadership within the organisation must have a consistent outlook on cyber security.

2. Define the strategy

Every cyber security investment must be supported by a strategic plan and a balanced analysis across the breadth of the organisation.

3. Deliver results

With a cyber security strategy and investment plan in place, the next step is to implement an effective method to deliver the desired outcomes.

4. Measure success

Stakeholders should have good visibility of progress. Reporting from the outset is a great way to establish support and share successes. To support effective reporting, the right metrics must be used.

PHASE ONE:

KNOW THE LANDSCAPE

Your organisation should have a consistent view of the cyber security threat landscape and the risks presented. This view must be communicated and shared at both a senior and operational level. This visibility helps to set the right objectives and ensure that cyber security investments are successful.

CONVERSATION STARTERS

- Does your organisation have shared visibility of the threats you face?
- Have your key business assets been identified and prioritised in the context of those threats?
- Have you identified your tangible and intangible business assets?
- Does your cyber security programme have a dedicated budget?

Aligning investments to the threat landscape

Cyber security as a business area has matured in recent years, as evidenced by an increased use of formal structures and frameworks to guide governance and operational activity. However, it remains a challenge to consider an extensive list of potential threats, impacts and consequences, as well as managing change within an organisation.

It is imperative that all investments are evaluated within the context of the threat landscape, the risks to the organisation's assets, the projected outcomes the investments will provide, and the increase in cyber resilience the investments will afford. Any prospective investment plan must be presented in a clear business context aligned to the organisation's strategic and financial governance.

The first step in this process is to identify the key threats and the risks facing the organisation's assets. This task often is performed as part of creating the cyber security strategy, and the information is already available. If the organisation is beginning the process, they will require input from an executive and leadership perspective, as well as from technology teams.

It's not possible to prioritise funding without an understanding of which assets (including business services and technical capabilities) are critical to the business, and the potential impacts of the threats they are exposed to. Some organisations' most significant assets may be their intangible goodwill or their reputation with customers. With limited funds, it will always be necessary to prioritise investments.

Every investment must clearly identify the risks being addressed, the threats being considered, and the controls being deployed, improved or maintained. Achieving this in practice may require focusing on a set of critical or key controls that relate directly to the threat scenarios identified. Even a well-resourced organisation may not be able to focus on all controls at once.

Organisations should give appropriate consideration to the effectiveness and the desired maturity level of investment proposals. While it's tempting to commit funding to advanced capabilities, stakeholders should utilise a risk-informed approach to investments and reduce risk to a level that aligns with the organisation's risk appetite. Doing so ensures the best use of resources while maintaining the flexibility to respond to a rapidly evolving threat landscape.

Focussing on the *how*

Even the best cyber security investment plan can be undermined by focusing too much on *what* the investment represents, and not *how* it will be approached.

To set the right environment for investing, remember these key points:

- **Fear tactics don't work.** Cyber security investments are often proposed using pressure and fear tactics: *invest now or bad things will happen!* This message quickly becomes ineffective with repetition. Investing in cyber security is about making a change to effect a positive outcome, and should be messaged this way.
- **Cyber security is an enabler.** Effective cyber security enables an organisation to be more resilient while still accomplishing its business objectives. Cyber security can help an organisation to achieve its business goals faster by enabling a secure journey. This can be achieved by embedding cyber security across the business and building secure services from the outset to avoid needing rework and validation later.
- **Business alignment.** Any investment plan for cyber security must align with the wider business and clearly demonstrate how that investment will support the organisation's strategic objectives.
- **Diminishing returns.** Each successive level of cyber maturity is generally much more difficult to achieve than the level before. As investment increases over time in a specific area, the rate of return will likely decrease. Organisations should understand that improvements cannot always be achieved at a linear rate, year on year.
- **Lifecycle management.** Every investment that creates a new capability or service will also need lifecycle maintenance and support, which increases funding pressure. This means that even the most focused areas of cyber security investment can rapidly deplete funds.

CAN YOU BENCHMARK YOUR CYBER SECURITY INVESTMENTS?

Benchmarking is complex due to a large number of contributing factors, including the size of the organisation and its subsidiaries, the business sector, the operating environment, the technology landscape, relative technical complexity, and technology age. Tracking and assessing all these variables is extremely challenging, and benchmarks are often inadequate to measure this level of detail. It is also common for elements of cyber security investment to be shared with other budgets. For these reasons, any benchmark based on a simple percentage investment relative to IT investment or even organisation size or industry will only provide a rough indication at best, and may confuse stakeholders at worst.

PHASE TWO:

DEFINE THE STRATEGY

A compelling event like an incident or a security audit can prompt an organisation to invest in cyber security and improve their defences. However, effective cyber security investments must be supported by a cyber security strategy and aligned to the organisation's overall business strategy and financial governance. Cyber resilience is built through proactive planning and understanding. Reactive spending may completely miss the underlying root causes of the issues that need to be remedied.

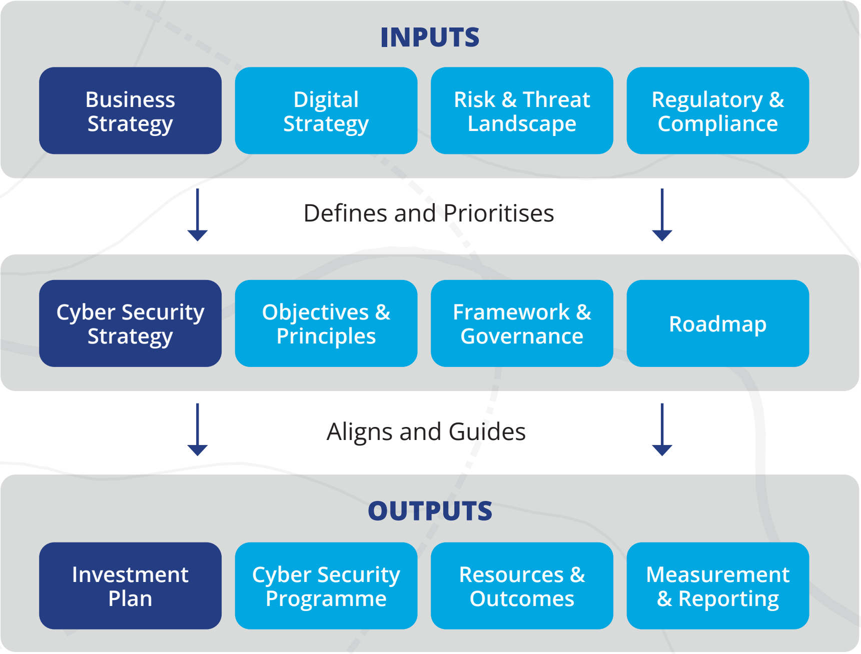
CONVERSATION STARTERS

- Is your cyber security investment aligned to a strategic plan, or is it an unplanned investment? If it's unplanned, why is that?
- Is your cyber security spending consistent or sporadic?
- Is there a clear line of sight between your cyber security spending and the organisational benefits it produces?
- Do you have a cyber security investment roadmap?

Many organisations will already have developed a cyber security strategy, and this can be used to align their investment plan with the wider business. However, making investments without a cyber security strategy can result in targeting the wrong threats and risks, or lacking the governance and support required to deliver the right outcomes.

There are several considerations that should guide any investment plan to maximise its chance of success.

Key elements of an investment plan lifecycle.



INPUTS

Business Strategy | Digital Strategy | Risk & Threat Landscape | Regulatory & Compliance

Defines and Prioritises

Cyber Security Strategy | Objectives & Principles | Framework & Governance | Roadmap

Aligns and Guides

OUTPUTS

Investment Plan | Cyber Security Programme | Resources & Outcomes | Measurement & Reporting

Governance is key

A key to successful investment planning is to ensure that that any cyber security strategy is aligned with the governance of the organisation. Endorsement by the board of directors should be achieved to ensure that a culture of cyber security is embedded from the top, and the right level of sponsorship and authority is established. It is also vital to ensure that there is a clear line-of-sight through governance forums, working groups and senior leaders from the approval of the strategy to its implementation through the investment plan.

Every investment in cyber security should be linked to the strategic outcome it is helping enable.

The NCSC's **Charting Your Course: Cyber Security Governance**[4] documents provide further guidance on establishing effective governance for cyber security within an organisation.

SEPARATING INFORMATION TECHNOLOGY AND CYBER SECURITY BUDGETS

Many organisations still treat their cyber security budget as a subset of their information technology budget. Even if the cyber security function and leadership reside within the information technology area, the funding allocation should be separated or, at a minimum, clearly ringfenced. The business outcomes achieved through investing in information technology are quite different to those achieved through investing in cyber security, and don't necessarily align. Organisations should not expose themselves to the risk that cyber security investment might be reduced or withdrawn due to overspending or insufficient funding across information technology.

Business financial alignment

A cyber security investment plan must align with the organisation's approach to financial planning. Most organisations delineate capital investment (CapEx) and operational investment (OpEx) and distinguish how these two expense categories are allocated. CapEx is generally focussed on acquiring and upgrading assets and building long-term value for the organisation, while OpEx is intended for the ongoing maintenance of existing resources and day-to-day expenses such as salaries.

Any capital investment will also require ongoing operational investment, and so the investment plan must consider both OpEx and CapEx in balance, and how they will change and grow over time.

For example, cloud services generally consume OpEx funding, and as security services move to the cloud, OpEx requirements might outstrip CapEx needs.

Ideally, the organisation should allocate a base amount of CapEx and OpEx to cyber security on an ongoing basis. Effective cyber security improvements require continual and committed investment. Sporadic or ad-hoc investments can make planning incredibly difficult and often result in skilled people being redeployed or leaving the organisation. Cyber security assets, like other assets, need lifecycle investment and maintenance. Even a significant budget can rapidly be exhausted if too much money is invested in technologies that have large deployment or maintenance costs. Many organisations also track budgets and headcount allocations separately, and these need to be considered not just in the security team but also the wider business.

Smaller organisations may not have a high level of definition around their cyber security investment plan. Even so, it's still important to ensure that there is a set amount of funds allocated every year to ensure continuous improvement.

[4] https://www.ncsc.govt.nz/resources/cyber-resilience-guidance/charting/

Investment outcomes

Investing in cyber security should always be linked to strategic outcomes, even if tactical investments are needed along the way. Without a plan to anchor investments, it is very likely that incidents, assessments, audits, or other external factors will redirect or derail current programmes of work. Establishing agreed outcomes from the beginning ensures that a balanced focus remains on those outcomes, even as flexibility to adjust to landscape changes is maintained.

Desired outcomes and goals will differ for every organisation, but these should be carefully selected as they can significantly alter the direction of any investment. Investment needs to consider a balance between **cyber security compliance**, **risk management** and **cyber resilience**. These outcomes can be in tension with each other, so consciously balancing the focus between them is critical. For example, a heavy focus on one particular risk may result in capable defences against that threat scenario but could leave areas of potential vulnerability against other threats.

Balance is key.

To simplify investment outcomes, create clarity and improve business understanding, it may make sense to group initiatives or controls changes into specific areas. These could be aligned around protective, reactive or preventive controls outcomes. Alternatively, they could focus on controls changes like maintenance, enhancement or even evolution for initiatives focussed on new or emerging threats.

Selecting inputs

When establishing an investment plan, one of the most important actions is deciding which inputs will be used to determine the investment's delivery and direction. The correct inputs can be difficult to identify in cyber security. Where an investment plan is based predominantly on one type of input (for example, the results of a stand-alone penetration test, an isolated incident, or an external report), bias can creep into planning and execution. This bias has the potential to lead an organisation down a specific investment path without first considering the entire landscape. The investment plan should be guided by the cyber security strategy but informed using accurate findings and assessments. The goal should be to ensure that breadth across the entire organisation is established before depth in a specific business area or technology domain.

STRATEGIC OUTCOMES VERSUS TACTICAL INVESTMENTS

Cyber security is a fast-moving environment and it's not always possible to ensure investments are linked to strategic plans. When a vulnerability has been identified or an incident has occurred, an organisation may need to make tactical investments while the strategic plan is still being formulated. In these situations, it is important to support timely decision-making but also consider the longer-term impacts of these decisions.

Consider whether it's possible to reverse an investment decision in the future if a better option is determined by the strategy. Consider the impact of long-term contracts or agreements and focus on the minimum investment needed to address the immediate risk or issue.

Even small tactical decisions can quickly build up a significant lifecycle maintenance cost and technical debt.

Agreeing on the return on investment

A challenge with any investment plan is reaching agreement on what the return on investment (ROI) measurement will be. This is a crucial step, since committing to any activity without a definition of success is risky. If there's no clear ROI definition, the delivery team and the wider business will need to define success in their own terms, which may lead to friction or misalignment as the programme progresses.

There are a range of risk management methodologies available:
ISO 31000[5] and NIST SP 800-30 Revision 1[6] are two of the most frequently applied. If risk reduction is used as a measure of return on investment, it does require considerable effort up-front to establish the framework and agree on the measures. It requires the board and executive leadership to agree on what an acceptable level of risk is. Additionally, the planning inputs may not be sufficiently well-developed to have captured the breadth of cyber security risks across the organisation, which could direct investment too deeply into a specific area.

A range of calculations and formulas exist to determine the probabilities of risks occurring. The selection of these is often determined by the organisation's preferred outcomes and overall enterprise approach. Security investment calculations are often based around the reduction of the likelihood and impact of risk. Advice and resources detailing risk management processes and frameworks for government organisations can be found on the New Zealand Digital Government website.[7]

Establishing an investment plan often requires finding a balance between the time spent on planning versus focussing on delivering the actual improvements. It may therefore be more effective to agree on ROI measures that are based on improvements in the effectiveness of controls, or on the maturity of the organisation's cyber security capabilities, rather than a purely risk-based approach. This should consider the operational and systems maturity of the organisation, as well as processes linked to controls. Having a framework with agreed controls and definitions of effectiveness will make this easier.

In **Measure Success,** later in this guide, there is an overview of how to present progress and returns to the organisation. Before this can be done, it is necessary to agree on what success looks like.

[5] - https://www.iso.org/iso-31000-risk-management.html

[6] - https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

[7] - https://www.digital.govt.nz/standards-and-guidance/privacy-security-and-risk/risk-management/

Establishing a roadmap

Roadmaps are vital tools for coordinating delivery, setting milestones and visualising the phasing of activities. Roadmaps help to bring people together and develop a consensus across organisational and contractual boundaries.

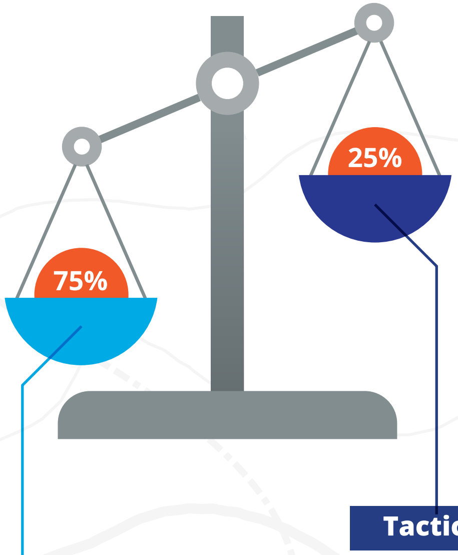
With governance established and business alignment in place, it's possible to build a roadmap to guide the investment plan and begin the process of steering delivery. This process takes the planning inputs and the agreed return on investment and outlines a path for the future. The roadmap should be presented at a **strategic** level, should be aligned to **outcomes**, and should identify **core delivery areas**. In some organisations the roadmap may be produced as part of the cyber security strategy, or it may be necessary to establish this as part of the investment plan.

The strategic roadmap should project at least three years into the future, but with a proviso that it's subject to change. As delivery progresses, internal developments may require reprioritisation, changes in direction, or additional funding. Changes in the threat landscape will also alter the roadmap. Within a three-year period, it is also quite likely that the organisational landscape will change, which will require the cyber security strategy and investment plan to be adapted accordingly.

The process of developing a roadmap may be as valuable to the outcome as the product itself.

Strategic and tactical priorities

An investment should weigh tactical improvements against longer-term strategic transformation.



Strategic

Plan out strategic investments for long-term benefit.

Tactical

While neccessary, tactical improvements may yield quick wins but rarely bring lasting resiliency.

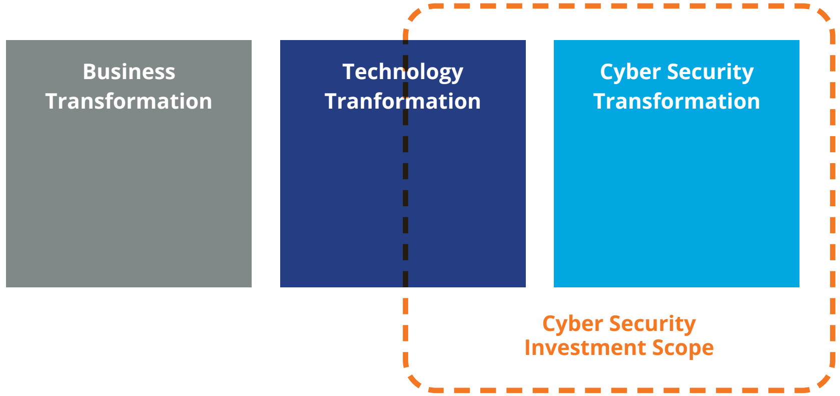
PHASE THREE:

DELIVER RESULTS

With an investment plan and a roadmap in place, the next step is to ensure effective and efficient delivery.

At a high level, it's possible to separate transformation initiatives into three areas: business transformation, technology transformation and cyber security transformation. Any investment in cyber security needs a clearly defined scope. While the cyber security strategy may guide business and technology transformation, the investment plan may be limited to only directly funding cyber security transformation.

The scope of cyber security investment is not necessarily the same as the cyber security transformation required across the organisation.



Business Transformation

Technology Tranformation

Cyber Security Transformation

Cyber Security Investment Scope

CONVERSATION STARTERS

- Do your cyber security investments consider the impact of change to the organisation?
- Do you have sufficient people available to support your cyber security transformation?
- Do your cyber security investments consider the entire business landscape and any other changes or activities that might be happening?
- Does your cyber security team have the skills and support to run and deliver an effective transformation programme?
- Have you considered your indirect costs as well as your direct costs?

Defining scope

Many organisations already have transformation programmes in place (for more information, see **Charting Your Course: Step 5**[8]) and the investment plan will serve to provide additional context.

The scope of the cyber security programme may already be established, and it is important to consider this from an investment plan perspective. Considerations may include whether the cyber security programme should be funding and delivering the transformation in other business areas such as the digital or information technology teams.

There are no right or wrong answers but, in general, organisations should adopt a *secure services by default* approach. This means that foremost accountability lies with the lines of business and information technology to deliver and maintain the security of their services.

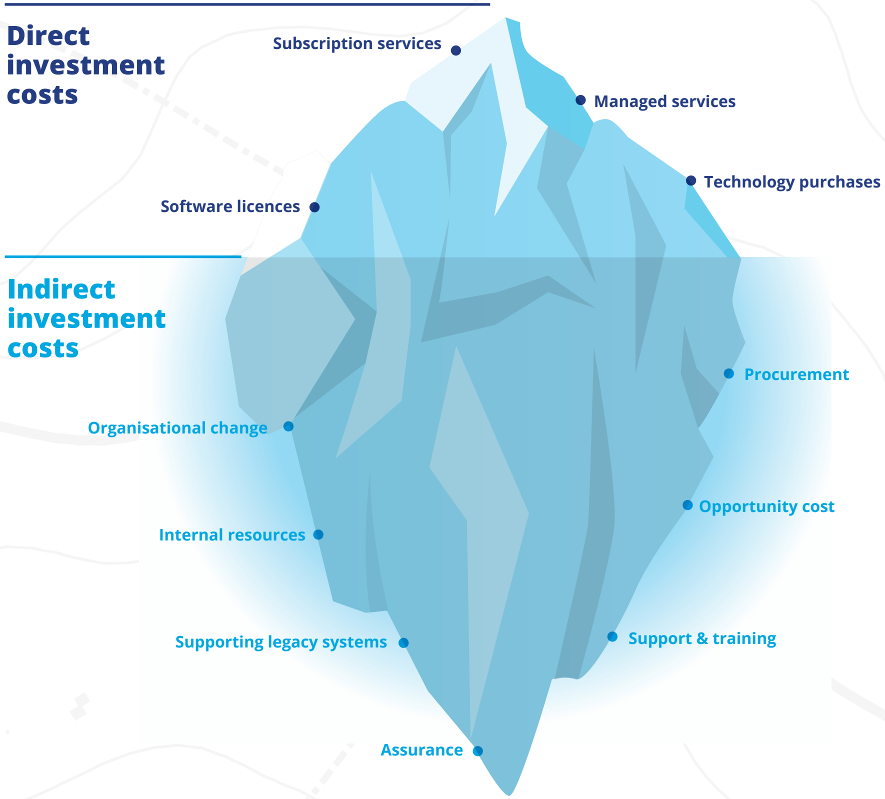
CONTINUOUS VERSUS AD-HOC INVESTMENT

Lasting improvement in cyber resilience is achieved through continuous investment and commitment. Ad-hoc investments often don't provide support for long-term improvement initiatives or the lifecycle maintenance of existing investments.

Estimating costs

While an investment plan provides a high-level budget, the accurate allocation and spending of this budget can be challenging in cyber security. One reason is that no matter how much up-front assessment and audit work has been done, there will almost always be unexpected events during delivery. A cyber security programme must consider these surprises and expand the scope to resolve them.

The true costs of an investment can be deceptive.



[8] - https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Charting-Your-Course-Governance-Step-5-Nov-2019.pdf

Common areas of overlooked cost

Cost of organisational change	Cyber security's breadth of impact means that any initiative has the potential to affect the entire organisation and its people. Introducing security products and processes (such as improving identity and access management) can have significant hidden costs (such as the costs of change planning and user training) when the entire organisation is affected, and the changes must be communicated and managed.
Cost of procurement	A market exercise is often required when pursuing large investments, in order to ensure value for money. These exercises can be significant undertakings in themselves and require additional resources to be allocated. The cyber security strategy should define the approach to technology selection and partnering to ensure the right cyber resilience outcomes.
Cost of technology change	Changing to new technologies can involve additional costs beyond the initial purchase. Organisations often overlook the costs of decommissioning existing technologies or systems, which may be a complex and manual activity. In critical environments, change-control processes must be carefully planned, driving costs up. The cost of defining end-to-end operational processes should not be underestimated either. All new services and technologies must have fully defined operational processes that include day-to-day operations and maintenance. These processes may include end users, service desk personnel and engineers.
Cost of legacy systems	While it may be desirable to deploy modern and sophisticated cyber security technologies, there is the risk that these may not support all environments or systems in use. Often this can lead to unforeseen and additional costs to deploy point solutions or assist in the migration to more modern environments.
Cost of internal resources	Cyber security programmes should allow for the cost of internal staffing or the backfill of internal resources, but often neglect these. Cyber security processes often span many organisational teams and will fall outside the information technology area. Changes can involve large parts of the organisation that may need to be allowed for, from a cost perspective.
Opportunity cost	Consider the pros and cons of utilising internal resources to deliver change, or engaging external contractors. The opportunity cost of internal resources can be high, especially when internal recharging or cost centre structures put high value on those resources, as would an external contractor. Exploring the opportunity cost of various options versus others is another way of properly weighing up and estimating costs for delivering investment outcomes.
Cost of licensing	Many organisations underestimate the ongoing costs to maintain licences on an annual basis, as well as potential increases in costs arising from greater consumption. A rapid move to cloud or online services can result in additional licences or storage costs that should be factored in. Most licences have annual maintenance costs or monthly subscription charges that need to be considered during any deployment as part of ongoing maintenance.
Cost of operational support and training	New technologies and systems need to be supported by trained and qualified staff. Teams should not be expected to operate and maintain new services or systems without adequate training and defined operational processes.
Cost of assurance	Costs associated with external assurance and insurance providers are increasingly commonplace and often are not factored into programmes focused on a technical capability or a change in information technology infrastructure.

Defining a resourcing model

It is common for organisations to engage external service providers and specialists to assist in the establishment and running of their cyber security programme. External support can be advantageous at times when recruiting and retaining in-house staff is challenging. While the resourcing model may be defined at a programme level, it does have significant bearing on the investment plan from a cost perspective. Any external engagements should have clear milestones and success criteria aligned to defined controls being deployed, improved, or maintained. Any external delivery should also make provision for training and handover to internal operational teams. While external resources can be more expensive, they can bring skills and expertise that improve the speed and quality of the outputs required by the organisation.

IT DOESN'T ALWAYS NEED TO BE AGILE

Agile provides a great mechanism for continuously improving and readily adapting when the need arises. It is, however, important to consider that larger security investments can be highly complex and span a broad range of people, processes and technologies. Therefore, maintaining a formal design process with clear traceability of control requirements and delivery is still sometimes necessary. What matters is that the delivery methodology in use is appropriate for the cost of failure. Where that cost is likely to be low, approaches that are adaptive, iterative, and fail-fast (such as Agile) are extremely powerful. Where that cost is high (financially or, for example, in safety terms), a formal design methodology may be more appropriate.

Choosing the right delivery methodology

Many cyber security programmes now utilise Agile delivery methodologies. Overall, cyber security lends itself well to Agile practices as it allows for a layered approach of improving and embedding capabilities over time. This also enables the organisation to respond quickly to internal or external changes. Complex, multi-year initiatives risk delivering a product or service to an organisation that has already changed its requirements, or the initiative may address a threat landscape that has significantly evolved. It is crucial that clear measures of success are established and tracked, particularly in Agile programmes. At a practical level, this means demonstrating success against the following measures:

- **Cyber resilience:** every initiative is mapped to the controls being deployed, improved, or maintained, with a clear definition of the current and target states.
- **Risk management:** every initiative must clearly identify the associated risks and scenarios that it will address. This includes clearly describing what success looks like in terms of risk reduction.
- **Compliance:** every initiative clearly defines compliance requirements and how they will be achieved.
- **Strategic outcomes:** initiatives should be clearly linked to the outcomes they are supporting and enabling in the organisation.

Shaping the cyber security operating model

Cyber security investments combine people, processes, and technology. Effective investments must consider the organisation’s cyber security operating model and must be integrated into the organisation. It is no longer sufficient for cyber security to focus on traditional operational capabilities; the secure operation and delivery of every business service must be factored in. Traditional security processes must be considered as well as wider lines of business operations. The 15 indicative capabilities below are derived from ISO 27002:2022 and should be considered by the cyber security programme in an organisation-wide context.

CYBER SECURITY OPERATING MODEL: KEY CAPABILITIES

Governance	Asset Management
Information Protection	Human Resource Security
Physical Security	System and Network Security
Application Security	Secure Configuration
Identity and Access Management	Threat and Vulnerability Management
Continuity	Supplier Relationships Security
Legal and Compliance	Information Security Event Management
Information Security Assurance	

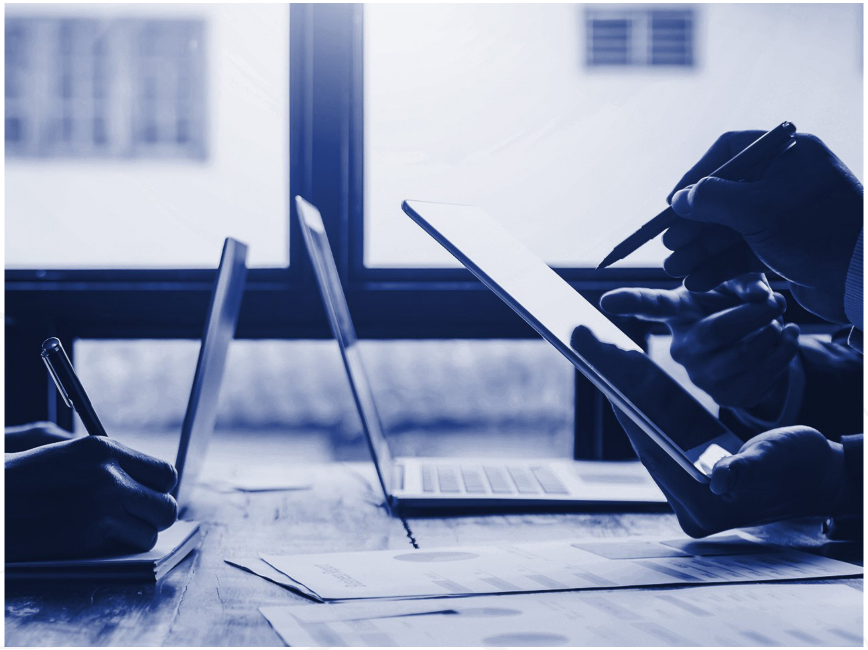
ASSIGNING OWNERSHIP

Establishing accountabilities is foundational to embedding cyber security improvements into the organisation. The ownership of key systems, services and processes must be determined. Organisations use a range of definitions including ‘service owner’, ‘business owner’, ‘technical owner’, ‘operational owner’, or ‘process owner’. In some cases, business owners may not have a deep technical understanding of the capabilities assigned to them, and having additional technical owners can be useful.

PHASE FOUR:

MEASURE SUCCESS

It is important that the investment plan is supported through effective governance, measurement and reporting to provide continual feedback to the organisation. This ensures that stakeholders have good visibility of progress. Reporting from the outset is a great way to establish support and share successes. To support effective reporting, the right metrics must be used.



CONVERSATION STARTERS

- Are the business benefits of each of your investments clearly defined?
- Is it clear how your investments will reduce risk to the organisation?
- Have you clearly identified the improvements that an investment will make, and defined the target state?
- Do you receive regular reporting and updates on the progress of your cyber security investments?

Metrics, dashboards and reporting

While the drivers and outcomes detailed in the cyber security strategy (see: **Phase 2: Define the strategy** on page 10) are vital to ensuring alignment and direction at a strategic level, they will not necessarily provide enough detail to be interpreted at a delivery level. Delivery-related metrics should be specific, measurable, assignable, realistic, and time-bound (often referred to as SMART metrics).

Consider how each metric links to the investment drivers and outcomes. Metrics should be aligned with long-term improvements and, where possible, should indicate the causes of performance issues. Metrics should be refined as the organisation matures and develops their capabilities.

A useful mechanism to report progress is a cyber security dashboard (see: **Charting Your Course: Step 6 – Measuring Resilience**[9]). Dashboards present a range of information in an accessible visual style. An example dashboard can be seen on the next page.

EFFECTIVENESS OF CONTROLS

Reporting should provide clear assurance on the operational effectiveness of controls that have been deployed, maintained or enhanced. This assurance is needed to inform the business on the overall risk position, threat exposure and return on investment. It's important to remember that controls can only be as good as they are designed to be. Poorly designed controls will not deliver operational effectiveness.

Leading and lagging indicators

When reporting metrics, it is useful to consider a balance between leading and lagging indicators. Leading indicators suggest potential events that might occur, while lagging indicators measure events that have already happened. Leading indicators can provide opportunities to make course corrections and prevent undesirable events from taking place. An example of a leading indicator is staff turnover rate as a gauge of the risk to confidentiality of information. Another example is the potential for the adoption of a significant new technology to introduce new cyber security risks. Leading indicators can be helpful tools for exploring where investment should be directed.

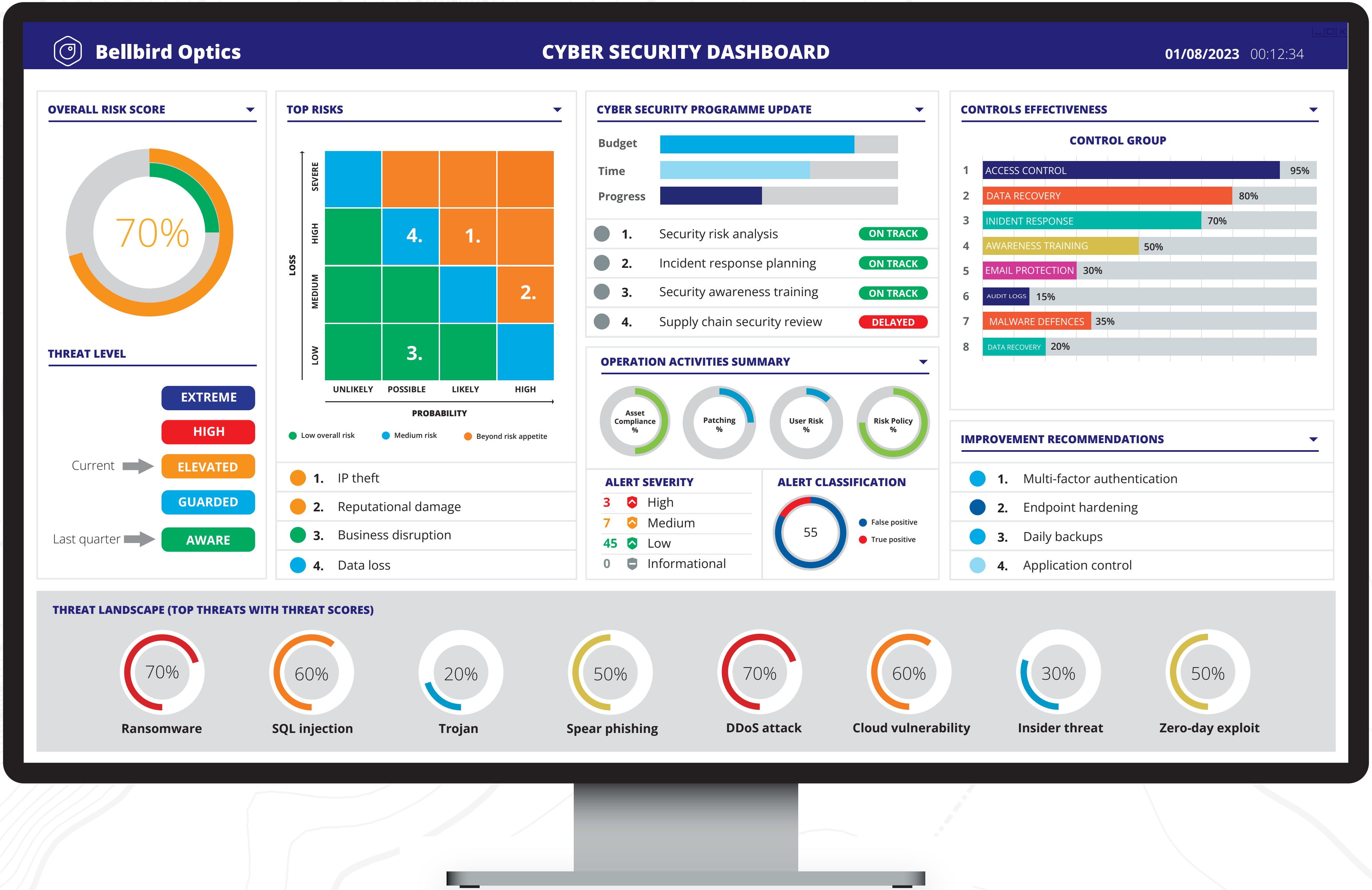
As organisational maturity develops, it may be possible to add additional indicators to dashboards and reporting. Good examples of lagging indicators are improvements in compliance or maturity levels, decreased incidents and events, decreased vulnerabilities, as well as results of awareness training and other improvement initiatives.

Outsourcing and third-party metrics

Many organisations choose to outsource part or all of their cyber security programme. For any externally delivered initiatives, the desired business outcomes should be clearly detailed along with the required metrics. Any delivery should be managed to achieve these metrics and embedded within the operating model.

[9] https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Charting-Your-Course-Governance-Step-6-Nov-2019.pdf

A simplified cyber security dashboard.



Bellbird Optics | **CYBER SECURITY DASHBOARD** | **01/08/2023** 00:12:34

OVERALL RISK SCORE

70%

THREAT LEVEL

- EXTREME
- HIGH
- Current → ELEVATED
- GUARDED
- Last quarter → AWARE

TOP RISKS

LOSS / PROBABILITY	UNLIKELY	POSSIBLE	LIKELY	HIGH
SEVERE	🟦	🟧	🟧	🟧
HIGH	🟩	🟦 4.	🟧 1.	🟧
MEDIUM	🟩	🟩	🟦	🟧 2.
LOW	🟩	🟩 3.	🟩	🟦

● Low overall risk ● Medium risk ● Beyond risk appetite

1. IP theft
2. Reputational damage
3. Business disruption
4. Data loss

CYBER SECURITY PROGRAMME UPDATE

Budget

Time

Progress

1.	Security risk analysis	ON TRACK
2.	Incident response planning	ON TRACK
3.	Security awareness training	ON TRACK
4.	Supply chain security review	DELAYED

OPERATION ACTIVITIES SUMMARY

ALERT SEVERITY

3	High
7	Medium
45	Low
0	Informational

ALERT CLASSIFICATION

55

● False positive
● True positive

CONTROLS EFFECTIVENESS

CONTROL GROUP

1	ACCESS CONTROL	95%
2	DATA RECOVERY	80%
3	INIDENT RESPONSE	70%
4	AWARENESS TRAINING	50%
5	EMAIL PROTECTION	30%
6	AUDIT LOGS	15%
7	MALWARE DEFENCES	35%
8	DATA RECOVERY	20%

IMPROVEMENT RECOMMENDATIONS

1. Multi-factor authentication
2. Endpoint hardening
3. Daily backups
4. Application control

THREAT LANDSCAPE (TOP THREATS WITH THREAT SCORES)

Ransomware	SQL injection	Trojan	Spear phishing	DDoS attack	Cloud vulnerability	Insider threat	Zero-day exploit
70%	60%	20%	50%	70%	60%	30%	50%

Challenges, pitfalls and opportunities

The processes of implementing an effective cyber security strategy and delivering an investment plan are complex undertakings for any organisation. These common challenges and pitfalls are useful to consider and prepare for.

Over-optimistic planning. When there's an opportunity to invest in improving cyber security, it can be tempting to add as many deliverables into the roadmap as possible and commence many initiatives at the same time. This can quickly stretch allocated resources and slow down overall progress.

Underestimating project complexity. Even small organisations can harbour a significant amount of technical complexity and reliance on legacy systems. Cyber security initiatives are likely to be complicated by unforeseen technical details. At a strategic level, those details may not be evident and it is important to allow for time to address them. When new issues are uncovered, they cannot be ignored or descoped without risking the outcomes of the overall project.

People and multi-threading. No matter how large an organisation is, there will always be dependencies on a few key staff, and they may become impediments to progressing initiatives. The more initiatives people are tasked to work on simultaneously, the less effective they become overall. Sometimes it is necessary to focus on fewer initiatives but deliver them well.

Technology and domain-aligned initiatives. Technologies require processes to run and maintain them, and these often extend well beyond the technology or security domain. For example, deploying a new security information and event management (SIEM) platform may require changing incident management processes (see the **NCSC's Incident Management guidance**[10]) that involve a range of other tools and systems. Consider any initiative in the wider context of the operational processes and people being impacted. Employing use-cases to define scope can be an effective way of supporting this.

Information overload. The wide range of available tools, approaches, reports, and assessments can result in excessive information being captured or reported and may impede the determination of a clear path of action. Link the details back to the investment drivers and outcomes aligned to the risks facing the organisation to provide priority and context.

Complexity of metrics and reporting. Many organisations create significant extra effort by adding too much complexity and detail into their reporting from the outset. It should be expected that sophistication of reporting and metrics will mature over time. It is more important to focus on maintaining cadence of delivery rather than generating overly complex reports. Ideally, metrics should provide a mechanism to report on the effectiveness of investments, and illustrate the value contributed to the organisation's strategic goals.

Quick wins versus fundamental exposures. Decision-makers should ensure that their investments prioritise mitigation of the most significant threats to achieving their organisation's strategic objectives. When producing an investment plan for cyber security improvements, the concept of quick wins (which can be implemented in a short time frame) may be attractive. However, rapid delivery of new capabilities is not necessarily synonymous with value. In contrast, ensuring that fundamental cyber security hygiene measures are in place may take a longer time, but will provide the best broad coverage to mitigate the majority of threats faced. It is recommended that known risks are prioritised to determine which of these will most likely disrupt the organisation's success.

[10] https://www.ncsc.govt.nz/guidance/incident-management/

Risk of underspending. Cyber security investment can have significant cost impacts as the threat landscape becomes more complex and the pressure builds to protect the organisation. When cyber security budgets are allocated, funding may be at the expense of other initiatives or investments that are part of the organisation's core business. It is therefore important that any cyber security investment is fully utilised and wisely allocated. The allocated funds should be used in the agreed timeframe but should not generate an end-of-year urgency to rapidly use up any remaining budget. This urgency may result in poorly planned investments that add unforeseen operational and lifecycle costs in the future.

Strategic and delivery disconnect. When a cyber security programme is underway it can easily take its own direction in the absence of continual checking and alignment with the strategic drivers and outcomes. Particularly in large organisations, effective governance is vital to maintaining direction. This is particularly important if prioritisation is needed, or circumstances require a change in focus.

Shared journeys. To ensure the ongoing effectiveness of cyber security initiatives, stakeholders must ensure that decisions are not made in isolation from other parts of the organisation. Sharing in this process allows an opportunity to tailor solutions that can be embedded within business processes and are therefore most likely to succeed.

Transformation takes time. Any cyber security programme has considerable impact on people, processes, and technologies within an organisation. Embedding the programme into the organisation is a gradual process that often requires delivery in stages to ensure effective operationalisation. Even if there is significant pressure to improve cyber resilience, it will take time to make the transformation happen. This must be clearly communicated from the outset.

CELEBRATE WINS!

The value delivered by cyber security initiatives should be shared and communicated. Successes should be visible to everyone in the organisation, not just the leadership or technical teams.

Conclusions

Approaching cyber security investment as a continuous process is key to ensuring positive outcomes. Planning strategically and setting a structured course of investment underpinned by a visible set of measures will ensure the best chance of successfully managing risk and achieving an increase in the organisation's resilience to cyber threats.

Consider these key points throughout the process of understanding the threat landscape, defining the investment strategy, delivering the agreed outcomes, and measuring the results:

1. Investment in cyber security should be set in the context of the threat landscape the organisation is operating in. It is crucial to consider how any cyber security investment addresses risk.
2. Establishing the right environment for investments will enable success. Investment decision-makers within an organisation must have an aligned outlook on cyber security. Making hasty decisions to invest in technology without considering wider organisational change may limit value.
3. A strategic approach to cyber security investment means deciding how any subsequent programme or activity will be governed, and how resources will be deployed to achieve improvements in cyber resilience.
4. Consideration must be given to how cyber security investments will be measured and reported. These metrics will help to reveal whether the organisation is focusing on the right areas, and when is it time to change focus and divert resources into other areas.

It is challenging to ensure that every cyber security investment is made in the right area, delivers effective outcomes, and provides a measurable return. This assurance requires a clear understanding of the organisation's strategic goals and how cyber security enables them. It requires a cyber security roadmap that is aligned to the organisation and its financial governance. It also requires a programme of continuous improvement delivering measurable results that can be evaluated at an executive and an operational level.

The organisation may need to change its approach as its capabilities mature or the threat landscape evolves. It is important to continually monitor the alignment of investments to the organisation, and amend methodologies or approaches as required.

Effective investment in cyber security will ensure that cyber resilience improvements are embedded into the organisational culture. This changes cyber security from being a problem faced by the security team to an enabler for the entire organisation.

Cyber security terminology guide

Cyber resilience: an organisation's ability to prepare for an adverse cyber security event, maintain essential functions during a disruption, and recover quickly.

Cyber security compliance: an organisation's adherence to regulations and industry standards to protect networks and data from cyber threats.

Dashboard: a graphical display of key metrics aligned to the strategic and investment outcomes of the organisation.

Framework: a structure that supports the key elements and relationships existing within a system or concept. A shared framework promotes interoperability and alignment.

Investment plan: a sequence of activities needed to enable an investment.

Operating model: a conceptual array of processes, roles, activities, capabilities, and interfaces that explain how an organisation achieves its goals.

Programme: a detailed plan of work that has clear resource requirements, delivery estimates and defined outcomes.

RASCI: a conceptual tool used to define who is: Responsible, Accountable, Supporting, Consulted, and Informed in the context of a process or activity.

Roadmap: a representation of the high-level milestones required to progress organisational cyber security goals.

Strategy: the overarching approach to achieving the agreed cyber security and resilience goals of the organisation.

Threat Level: a defined evaluation of readiness that may be adjusted in accordance with internal and external threats faced by the organisation.

Resources

Essential Eight Maturity Model (ACSC)
https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model

Ten Critical Controls 2023 (CERT NZ)
https://www.cert.govt.nz/assets/Uploads/documents/cert-nz-critical-controls-2023.pdf

The 18 CIS Critical Security Controls (CIS)
https://www.cisecurity.org/controls/cis-controls-list

The Business Case for Security (CISA)
https://www.cisa.gov/sites/default/files/publications/The-Business-Case-for-Security.pdf

Charting Your Course: Cyber Security Governance (NCSC NZ)
https://www.ncsc.govt.nz/resources/cyber-resilience-guidance/charting/

Supply Chain Cyber Security: In Safe Hands (NCSC NZ)
https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Supply-Chain-Cyber-Security.pdf

Incident Management: Be Resilient, Be Prepared (NCSC NZ)
https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Incident-Management-Be-Resilient-Be-Prepared.pdf

Cyber Security Board Toolkit (NCSC UK)
https://www.ncsc.gov.uk/collection/board-toolkit

ISO/IEC 27002:22: Information security, cybersecurity and privacy protection — Information security controls
https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-3:v2:en

NIST SP 800-30 Rev. 1: Guide for Conducting Risk Assessments (NIST)
https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

Cyber Security Framework (NCSC NZ)
https://www.ncsc.govt.nz/resources/ncsc-cyber-security-framework/

NIST SP 800-55 Rev. 1: Performance Measurement Guide for Information Security (NIST)
https://csrc.nist.gov/publications/detail/sp/800-55/rev-1/final

Te Tira Tiaki
Government Communications
Security Bureau

For futher information visit: www.ncsc.govt.nz
or email: info@ncsc.govt.nz