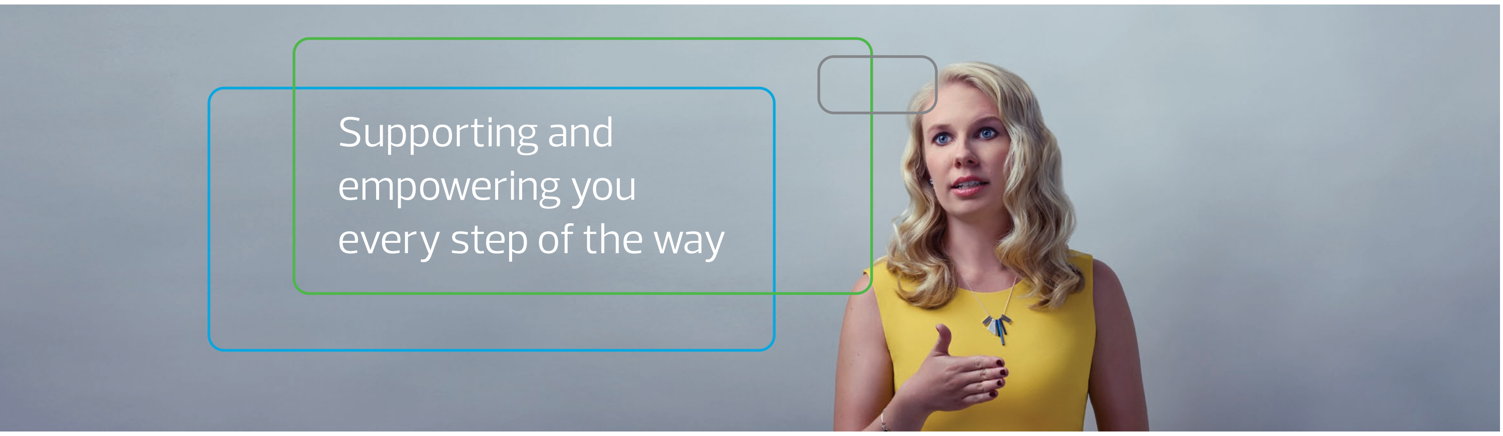
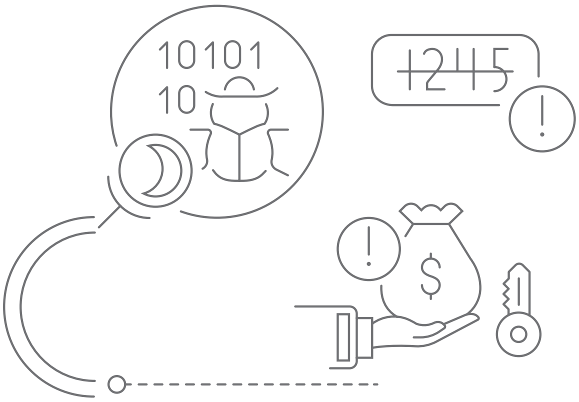


Supporting and empowering you every step of the way

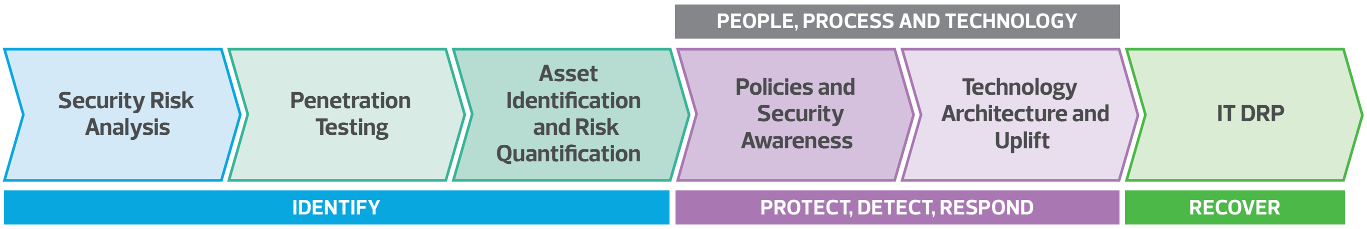
CYBER SECURITY – A PRACTICAL APPROACH

As the threat landscape worsens and we see new attacks emerging daily, organisations are left asking the question "what needs to change" to stop this? Having worked with multiple organisations to develop their cyber security strategy and to uplift their cyber security posture, our advice has stayed the same over the last two decades – **focus on the basics**.

> What this practically means is to approach cyber security in a methodical and thought out way so that we can understand our key risks and then start treating these risks in a prioritised manner.



Depicted below is the **NIST-CSF framework** which has successfully helped organisations understand their key cyber security risks and then bolster their defences to help mitigate these risks to within tolerance levels.



PEOPLE, PROCESS AND TECHNOLOGY

Security Risk Analysis

Penetration Testing

Asset Identification and Risk Quantification

Policies and Security Awareness

Technology Architecture and Uplift

IT DRP

IDENTIFY

PROTECT, DETECT, RESPOND

RECOVER

IDENTIFY

Stage 1: Security Risk Analysis

This step involves understanding where your control gaps may lie (vulnerabilities) as well as active threats that are looking to exploit these gaps. It is also important to understand the potential losses (impact) if these risks were to eventuate.

The last two components (threat and impact) are important, as without these, you will not be able to prioritise your risks adequately and may end up focusing on the wrong vulnerabilities. Vulnerabilities that are being actively exploited by threat actors are more important than those that are not. Equally, threats and vulnerabilities that lead to the greatest potential loss is more important that ones that cause less harm. The end result of this stage will be a security roadmap/strategy that will provide a path to uplifting your cyber security in line with risk tolerance.

The security strategy and risk analysis should be updated at least annually.

Stage 2: Penetration Testing

We often get asked, "why penetration testing?". The answer is simple – the risk analysis will often give a controls-based view of risks within an organisation. Performing a penetration test to augment this will give the organisation the proof needed to bring reality to the risk analysis and encourage the right actions in terms of risk mitigation.

As an example, the risk analysis may find that patching procedures are not up to standard. Exploiting missing patches and demonstrating the impact these could have on the organisation as part of a penetration test can bring reality to the issue and motivate the organisation to take the right actions to address the issue.

Penetration testing should be performed every six months.

Stage 3: Asset Identification and Risk Quantification

This is where the rubber hits the road! This process will identify the assets you have (both IT and OT) and provide a point in time picture of the threats and vulnerabilities they are susceptible to. This is important as without this asset inventory, it is difficult to protect what you don't know exists. Further, the risk quantification allows you to understand risks at an asset level so that you can mitigate them in a granular fashion, effectively augmenting Stage 1 above.

This stage should be performed at least quarterly.

PROTECT, DETECT AND RESPOND

Stage 4: Policies and Security Awareness

Within this stage, we implement the foundational elements of cyber security. Policies and associated responsibilities will start to document and define what security to implement within the organisation. The user awareness component will start to educate users so that they can detect cyber risks and defend their organisation better.

These two elements are critical to lay the foundations on which a cyber secure organisation will be built. We will also look to deliver incident response plans, incident response playbooks as well as incident response training as part of this stage.

Stage 5: Technology Architecture and Uplift

We will create an organisational security architecture that will enable the organisation to implement the technology controls necessary to mitigate cyber risk to an acceptable level. Please note that it is critical to ensure technology investments are aligned to a cyber security strategy and the subsequent organisational security architecture so that:

1. Technology investments are made according to a plan / strategy and will deliver to a defined business need and risk mitigation outcome.
2. All technology investments adhere to a documented architecture to ensure everything fits within requirements and there is no wastage in terms of duplication or gaps.

Typical investments here will include technology controls such as firewall, web and email filtering, etc., Security Information and Event Management (SIEM), Security Orchestration, Automation and Response (SOAR), etc.

Stages 4 and 5 will also deliver the necessary People, Process and Technology controls required to uplift the security posture of the organisation.

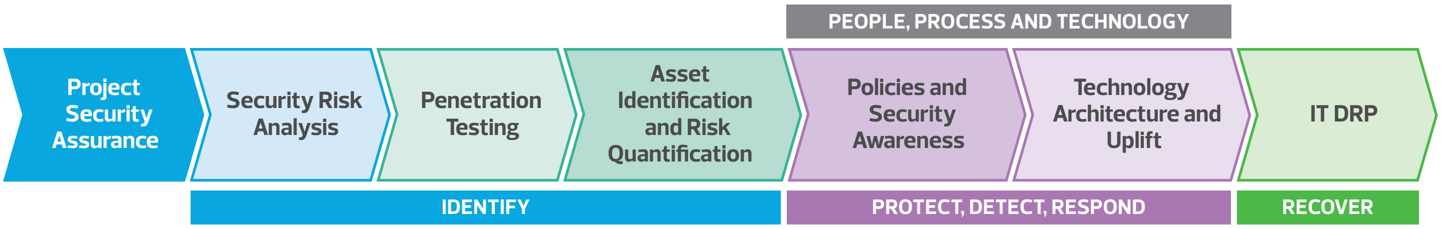
RECOVER

Stage 6: IT Disaster Recovery Planning (IT DRP)

Despite our best efforts, cyber security incidents are possible. When this occurs, you want to ensure that you can recover from an incident quickly in order to minimise damage. This is where an IT DRP is crucial. A well developed, tested and up to date plan will ensure you can recover quickly from an interruption and resume operations so that the damage is minimal.

PROJECT SECURITY ASSURANCE

The above approach will work well for a new organisation or one that is about to embark on a complete technology refresh. However, most organisations will already have cyber security projects inflight. For these organisations, an alternate, but similar approach is outlined below.



PEOPLE, PROCESS AND TECHNOLOGY

Project Security Assurance

Security Risk Analysis

Penetration Testing

Asset Identification and Risk Quantification

Policies and Security Awareness

Technology Architecture and Uplift

IT DRP

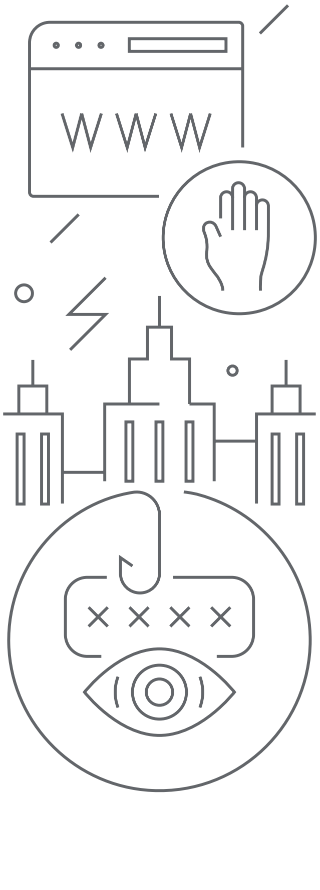
IDENTIFY

PROTECT, DETECT, RESPOND

RECOVER

With projects inflight, it is important to ensure that the cyber security projects are delivered securely and that they are addressing a business need. The other stages described earlier are still important, but securely delivering inflight cyber security projects will ensure that these investments are not wasted and can be retrofitted within the strategy when the Security Risk Analysis is performed and can be added into the overall organisational security architecture when this is created in the Technology Architecture and Uplift stage.

> Approaching cyber security in a methodical fashion is critical to ensuring that any effort extended will protect the organisation and is aligned its risk appetite and threat profile. The approach outlined above will help achieve this in a simple and effective manner.



For more information about the Cyber Security and Resilience Services at RSM, please visit rsm.com.au/cyber-security-resilience-services

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

rsm.com.au
Liability limited by a scheme approved under professional standards legislation