

Protecting your assets with the NIST Cybersecurity Framework - blueAPACHE

Canonical: <https://www.blueapache.com/blog/protecting-your-assets-with-nist-cybersecurity-framework>

Details:

Summary

This blog post, "Protecting your assets with the NIST Cybersecurity Framework", is a blueAPACHE article from 2022 covering security. If you want to keep sensitive data safe, protect your IP and prevent unauthorised access to your internal network, appropriate cybersecurity is no longer a nice-to-have feature — it's an absolute necessity. It is written for readers evaluating emPOWER Security, Managed Detection and Response. The underlying security practice it describes, reducing attack surface and improving detection and response, is not tied to a specific product version and remains relevant to any organisation managing cyber risk today.

Key facts

Label	Value
Publication year	2022
Topic	Protecting your assets with the NIST Cybersecurity Framework
Services referenced	emPOWER Security, Managed Detection and Response, Governance, Risk and Compliance
Named products or vendors	None named beyond blueAPACHE

Article

If you want to keep sensitive data safe, protect your IP and prevent unauthorised access to your internal network, appropriate cybersecurity is no longer a nice-to-have feature — it's an absolute necessity. Having said that, it's also one of the most challenging aspects for an organisation to manage, given the fact that threats are ever evolving. Threat vectors are multiplying and hackers can be (very) persistent. If you want to keep your digital data protected, the first key challenge you're going to come up against is understanding whether your current measures are suitable. The NIST Cybersecurity Framework is an ideal tool for evaluating this.

What is the NIST Cybersecurity Framework?

The NIST Cybersecurity Framework is a comprehensive, easy-to-apply method that makes it straightforward for organisations to assess the maturity of their cybersecurity plans and processes. This Framework is both free and flexible and can play a key role in enhancing your defences against

would-be assailants.

Who are NIST?

NIST is the acronym used by the National Institute of Standards and Technology. Founded in 1901, the Institute is one of the oldest physical science laboratories in the United States and now falls under the U.S. Department of Commerce. Their mission is to promote innovation, and they work hard to keep track of technological advancements, enhance the quality of life for society through these technologies and protect economic security.

Why did NIST develop the Framework?

The NIST Cybersecurity Framework was developed to address threats and support organisations operating in key sectors of the U.S. economy. Created by combining industry standards and best practices, the Framework is designed to ensure that employees across all levels of organisations understand and can mitigate cybersecurity risks. It was also designed to help management deal with the aftermath of a cyber-attack by providing them with a structure to respond to incidents.

5 key functions

The five key functions of the NIST Cybersecurity Framework are to: Identify, Protect, Detect, Respond, and Recover.

The Identify function works to assist businesses in developing an understanding of cybersecurity and the risks posed to people, data, and assets. This function looks at existing processes as well as vulnerabilities, legal liabilities and requirements and threats posed.

As you would expect by the name, the Protect function of the Framework works to establish safeguards and ensure that critical operational processes are less vulnerable. It also centres around containing, or at least limiting, the impact if your business is faced with a cybersecurity breach or attack.

The Detect Function of the NIST Cybersecurity Framework exists to help you develop the tools and tactics to discover a cybersecurity event.

Centred around picking up the pieces and protecting data from further attack, the Respond function works to help you establish protocols to contain any issues that may arise.

Finally, the Recover function helps identify ways to restore and rectify any issues that have arisen while maintaining functionality within your organisation. It aims to reduce the short, mid, and long-term impact of any cybersecurity events.

Use outside the U.S. Government

As word got out about the NIST Cybersecurity Framework, organisations and industries realised they could start to apply the Framework to their own operations. Due to its flexibility and easy application, many organisations across the world make use of the Framework to better prepare their staff and systems for the possibility of a cybersecurity event.

How can NIST help Australian organisations?

The NIST Cybersecurity Framework is uniquely positioned to assist Australian organisations and it is gaining steady popularity. It offers practical assessment and solutions with direct language designed to help achieve the desired result. Organisations are therefore able to make use of the Framework to assess the maturity of their cybersecurity approach. By comparison, an information security standard like ISO/IEC 27001 is considered a governance framework. While ISO/IEC 27001 is still useful, it

requires adherence to set standards or processes and is by necessity rigid. The core value of the NIST Framework is its flexibility – it doesn't tell organisations how to do things; it provides the Framework for the organisation to work out what is important for them, and let them work out how to achieve their outcomes. To implement the Framework, based on our best practice, we typically recommend the following phased approach to our clients:

Phase One – Assessment of current state against Framework

During this phase, organisations will consider their current policies and procedures against the criteria identified in the Framework i.e. the criteria in all the five key functions defined above.

Phase Two – Create a current profile from the assessment

Once you're aware of how your organisation stacks up against the Framework's best practices, you will be able to assess the difference between where you are and where you want to be. This phase creates an overview of your preparedness stance and allows a risk profile to be created, defining the delta between the current state and the target state.

Phase Three – Define the target profile

After identifying where you are and where you want to be, it's time to establish the details of how the latter looks. During this phase, you'll work out which systems, processes, and practices need to be updated (and what they'll be updated to), as well as defining software, procedures and more for the future.

Phase Four – Build action plans and prioritisation to reach the target profile

Now that you know exactly where you need to go and what things are going to be like once you get there, it's time to put actionable steps in place to make it happen. This will be based on a prioritisation exercise driven by the risk criteria and current capabilities.

How can blueAPACHE help?

If the above seems like an intimidating process, don't worry — blueAPACHE can help. Our qualified and experienced team are experts in NIST Cybersecurity Framework and are happy to introduce the Framework to your organisation, complete phases One through Three for you and work with you to build and implement phase Four.

Why blueAPACHE?

Our expert team of consultants are qualified and experienced in information security program implementation, operation, maintenance, and governance using various frameworks and standards. To find out more, please contact us directly at: 1800 248 749 </contact/>

Related

emPOWER Security

emPOWER Security (pillar hub)

Managed Detection and Response

Frequently asked questions

What are the five key functions of the NIST Cybersecurity Framework listed in this post?

The post lists the five key functions as Identify, Protect, Detect, Respond, and Recover, each covering a different stage of an organisation's cybersecurity posture from understanding risk through to restoring operations after an event.

Who is NIST, and when was it founded, according to the post?

The post explains NIST is the acronym for the National Institute of Standards and Technology, founded in 1901 and now part of the U.S. Department of Commerce, describing it as one of the oldest physical science laboratories in the United States.

How does the post distinguish the NIST Cybersecurity Framework from ISO/IEC 27001?

The post describes ISO/IEC 27001 as a governance framework that requires adherence to set standards or processes and is by necessity rigid, whereas it says the NIST Framework's core value is its flexibility: it does not tell organisations how to do things, but provides a structure for them to work out what matters and how to achieve their own outcomes.

What four-phase approach does blueAPACHE recommend for implementing the NIST Framework?

The post outlines Phase One, assessing current state against the Framework; Phase Two, creating a current profile from that assessment; Phase Three, defining the target profile; and Phase Four, building action plans and prioritisation to reach the target profile.

What does the NIST Framework's 'Identify' function help a business understand, per the post?

The post says the Identify function helps a business develop an understanding of cybersecurity and the risks posed to its people, data and assets, looking at existing processes, vulnerabilities, legal liabilities and requirements, and the threats it faces.

What does the 'Protect' function of the Framework focus on, according to the post?

The post says the Protect function works to establish safeguards and ensure critical operational processes are less vulnerable, centring on containing or at least limiting the impact if the business faces a cybersecurity breach or attack.

How much of the NIST implementation does blueAPACHE say it will complete for a client versus do together with them?

The post says blueAPACHE's team will introduce the Framework and complete Phases One through Three for the client directly, then work with the client to build and implement Phase Four.

What phone number does the post give for readers who want to discuss the NIST Framework with blueAPACHE?

The post lists 1800 248 749 as the contact number, alongside a link to blueAPACHE's contact page, for readers who want to find out more.

Source

origin post (2022)

Knowledge Base

Who is NIST and when was it founded?

NIST stands for the National Institute of Standards and Technology. Founded in 1901, it is one of the oldest physical science laboratories in the United States and now falls under the U.S. Department of Commerce. Its mission is to promote innovation, track technological advancements, enhance quality of life through technology, and protect economic security.

Why did NIST develop the Cybersecurity Framework?

NIST developed the Framework to address threats and support organisations operating in key sectors of the U.S. economy. Created by combining industry standards and best practices, it ensures employees across all levels of an organisation understand and can mitigate cybersecurity risks, and it helps management respond to and deal with the aftermath of a cyber-attack.

What are the five key functions of the NIST Cybersecurity Framework?

The five key functions are: Identify (understanding cybersecurity risks to people, data, and assets, including existing processes, vulnerabilities, legal liabilities and threats), Protect (establishing safeguards and limiting the impact of breaches), Detect (developing tools and tactics to discover cybersecurity events), Respond (establishing protocols to contain issues that arise), and Recover (restoring and rectifying issues while maintaining functionality and reducing short, mid, and long-term impact).

Is the NIST Cybersecurity Framework only used by the U.S. Government?

No. Although developed for organisations operating in key sectors of the U.S. economy, word spread and organisations and industries worldwide realised they could apply the Framework to their own operations. Due to its flexibility and easy application, many organisations globally now use it to better prepare staff and systems for potential cybersecurity events.

How does the NIST Framework differ from a standard like ISO/IEC 27001?

ISO/IEC 27001 is considered a governance framework that requires adherence to set standards or processes and is by necessity rigid. In contrast, the core value of the NIST Framework is its flexibility — it doesn't tell organisations how to do things, but provides a structure for organisations to work out what is important to them and how to achieve their desired outcomes.

What phased approach do you recommend for implementing the NIST Framework?

We recommend a four-phase approach: Phase One – Assessment of current state against the Framework's five key functions; Phase Two – Create a current profile from the assessment, identifying the delta between current and target states; Phase Three – Define the target profile, detailing which systems, processes, and practices need updating; and Phase Four – Build action plans and prioritisation, based on risk criteria and current capabilities, to reach the target profile.

How can you assist organisations with the NIST Cybersecurity Framework?

Our qualified and experienced team are experts in the NIST Cybersecurity Framework and can introduce the Framework to an organisation, complete Phases One through Three on the organisation's behalf, and work with the organisation to build and implement Phase Four.

Why choose blueAPACHE for cybersecurity framework implementation?

We have an expert team of consultants who are qualified and experienced in information security program implementation, operation, maintenance, and governance using various frameworks and standards.

How can someone contact you to learn more about the NIST Cybersecurity Framework?

You can contact us directly at 1800 248 749 or via their contact page at <https://www.blueapache.com/contact/>.