How to proactively manage cyber security threats

stickman
CYBER SECURITY BY DESIGN

Introduction

Hackers are not going anywhere, anytime soon.

The burgeoning new wave of hackers are tech-savvy and hell-bent on causing maximum damage. Virtually all organisations face constant threat from cyber-attack; unfortunately, it's a matter of when, not if, someone tries to hack your data. Times have changed, and responding to attacks as they happen is simply not enough. There is only one way to achieve complete cyber security: by planning ahead for digital defence that covers all aspects of your business.

Traditionally, organisations have taken a reactive approach to cyber security - responding to threats as they occur, rather than pro-actively protecting and managing cyber risk. Today's sophisticated hackers are always finding new opportunities for attack, which makes it mission critical to stay on the offence with cyber security. Managing compliance for multiple security standards has also proven challenging, with cyber security not visible at board level or even considered to be a business priority. That is, of course, until a data breach occurs and it becomes everybody's problem.

This fragmented approach is ineffective – and dangerous. The consequences of a cyber-attack can be devastating, such as loss of customer confidence, ruined reputation and costly legal ramifications. Not to mention the potential destruction of your entire business.

To be fully effective, cyber security must be proactively managed and owned at board level. Not not just by the IT department. It needs to be broad in scope, and senior management needs to recognise that it's a whole of business challenge.

> "You can't keep going out and giving clients 50,000-line excel spreadsheets and 1000-page gap analyses that never get acted upon. We need actionable frameworks to help companies navigate their security requirements." **Ajay Unni, CEO, Stickman**

What is Cyber Security By Design?

Stickman's 'Cyber Security By Design', is a company-wide, proactive approach to managing cyber security as a function within an organisation.

It's a methodology that adopts the gold standard **NIST Cyber Security Framework** and brings a broad-scale, customised approach to managing cyber risk. Some of it's benefits include:

Tailored risk based cyber security

Instead of one-size fits all, the cyber security program is tailord to meet your specific needs, risk tolerance and resources available, with the focus firmly on risk minimisation.

Collaboration for best results

The lack of visibility of cyber security at board level and senior management is a common problem for security professionals within large organisations. This methodology promotes external and internal collaboration and buy-in. Cyber security is quickly integrated into more business functions, such as new product development and infrastructure design, meaning your business is more protected.

Keeping you on the front foot

Cyber security is constantly changing. With new technology and smarter cyber criminals, this dynamic approach enables rapid evolution to keep security steps ahead of hackers. Our methodology is designed to be flexible, always keeping you on the front foot.

Customised cyber security

Our methodology adopts the industry gold standard **NIST Cyber Security Framework** to bring you a proactive, broad-scale and customised approach to managing cyber risk.

NIST Cyber Security Framework

The **NIST Cyber Security Framework** is the framework used to implement this approach.

Developed in the United States by the **National Insitute of Standards and Technology (NIST)**, the framework helps organisations shift the balance from reactive compliance, to proactive cyber risk management.

> “”The Frameworks is risk based and requires organisations to assess and treat risk without the guidance of a compliance check list. This creates a foundation for the future of cyber security regulations. **Ajay Unni, CEO, Stickman**

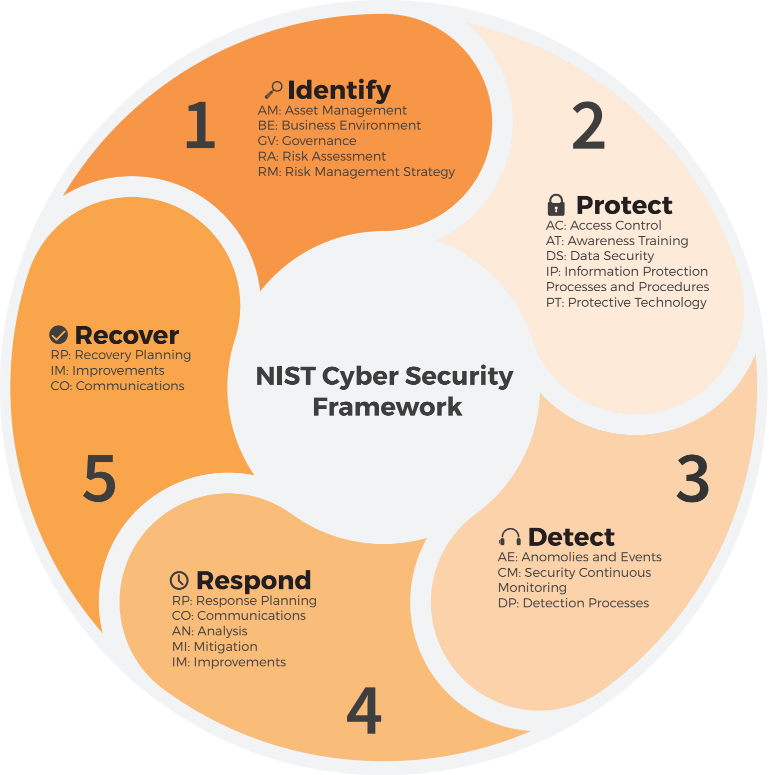
It was developed as a result of an Executive Order in 2013 titled “Improving Critical Infrastructure Cyber Security” with input from more than 3,000 security professionals from the US and overseas.

It’s objective, is to help identify, implement and improve cyber security practises. It places organisations in the best position to comply with current and future regulatory standards and improve collaboration on cyber security issues across divisional, management and board levels.

The key components of the NIST Framework are: Identify, Protect, Detect, Respond and Recover.

NIST Cyber Security Framework

The five key components represent the key continuous functions of a well structured Cyber Security management system.



1. **Identify:** Review capability of managing cyber security risk by reviewing systems,assets, policies and capabilities.

2. **Protect:** The controls, technologies, and safeguards required to deter cyber security threats.

3. **Detect:** Proactive and real-time monitoriing to detect cyber security events.

4. **Respond:** Co-ordinated response planning including communications and mitigation.

5. **Recover:** Continuity plans to ensure resiliance and recover from a cyber security breach.

Benefits of adopting the NIST framework

Whilst the NIST Cyber Security Framework is a voluntary model in the United States, it's structure and the intent driving it's development bring some potential benefits to Australian organisations.

The framework supports a continuous process of improvement

Cyber Security within any organisation is a process of continuous improvement. From new vulnerabilities, changing IT infrastructure to technological advances, what is sufficient one year will be redundant the next. The NIST framework supports the evolving nature of cyber security by providing the structure to manage this change via its five core functions.

Insurance underwriting and legal evidence of a structured cyber security program

Legal responsibility to protect customer data is a factor in any cyber security program. But how does an organisation provide evidence of due care? As it evolves, the NIST framework has the potential to be identified as the minimum standard for a cyber security program with those not adopting it, potentially considered negligent when tested in a court of law and assessing cyber insurance underwriting.

Supplier opportunities with others that adopt the framework

As the framework develops and adoption increases, there is potential for suppliers to use it as a basis for selecting partners. In particular, in instances where data is to be shared across organisations and security risk is a factor in decision making, the use of the NIST framework and evidence of it's implementation could become an importance criteria for selection.

> "Businesses are working to different security standards, and their security programs are fragmented to the extent many of them become messy and difficult to navigate"
> **Ajay Unni, CEO, Stickman**

How can Stickman help?

In April 2016, Ajay Unni, Stickman's CEO attended the latest NIST Cyber Security Framework workshop in Maryland, US. As the only participant from the Asia-Pacific region, Ajay developed a deep understanding of the frameworks benefits, and how it can benefit Australian and Asia-Pacific based organisations.

This greatly assisted in the ongoing development of Stickman's Cyber Security By Design methodology which builds security systems customised for each organisation, transforming their approach to cyber security and ensuring their environment is secure - both now and into the future.

If you need help building your Cyber Security resiliance, contact us today.

Stickman Consulting
Contact: Gergana Kiryakova
Level 11, Suite 2
210 George Street,
Sydney, 2000
Ph: 1800 785 626
e: gergana.kiryakova@stickman.com.au
w: www.stickman.com.au

stickman
CYBER SECURITY BY DESIGN

Level 11, Suite 2,
210 George Street,
Sydney, NSW, 2000

P: 1800 785 626
E: sales@stickman.com.au

www.stickman.com.au