NETTITUDE

AN LRQA COMPANY

Effective Cyber Security Strategy

How to establish a cyber resilient organization by adopting the right strategy and approach

Contents

1.0 Defining the purpose. 2
1.1 Defining what 'good' looks like 2

2.0 Building blocks: Key considerations. 3
2.1 Nettitude's approach 3
2.2 Stage 1: Mission and objectives (Define what good looks like) . . . 4
2.3 Stage 2: Frameworks (What are we going to do?): 5
2.4 Stage 3: Risk assessments (Why are we going to do it?) 6
2.5 Stage 4: Controls (How are we going to do it?). 7
2.6 Stage 5: Assurance/maturity assessments (Are we doing it?) 7

3.0 Summary. 8

01 Defining the purpose

Cyber attacks and the impact they have on organizations are becoming much better understood. However, in facing increasingly sophisticated, targeted and untargeted attacks, the complexity and scale of the threat means that avoiding a cyber attack will become harder for organizations. Therefore, if a cyber attack is going to happen at some point it's essential that organizations plan for, and prepare to respond to, the inevitable.

> If a cyber attack is going to happen at some point it's essential that organizations plan for, and prepare to respond to, the inevitable.

Building the right approach to an effective cyber security strategy sounds simple, but is often much harder in practice. Nettitude has helped countless organizations (large and small) develop their cyber security posture, defense and response as well as their governance and assessments of their assurance levels.

This experience has shown that it is fundamentally critical to ensure that time is taken to develop a longer term vision of what 'good' looks like for your organization, especially in relation to cyber threats. It's vital that this vision is clearly articulated, has board level engagement and is appropriate and relevant to the threats faced.

> Delivering exhaustive defense alone is an illusion. With shadow IT, cloud, 3rd parties, the human element, IoT and evolving threats, defending against infinity is impossible.

Many organizations have had, and in some cases many, historic cyber security assessments and gap analyses performed on their controls. They have studied relevant cyber security standards and regulations. They have implemented technology and written policies. But they don't have a clear idea of why they are doing what they are doing, or are able to determine when they have done enough.

- What is the end game?
- What does a successful cyber security posture look like?
- What level of effort, resource and approach is relevant and needed for your organization?

Nettitude can help you develop an overarching cyber security strategy, which is pragmatic, relevant and measurable. Defining the roles and responsibilities, the governance and objectives, methods of assurance and continuous measurement – as well as the appropriate controls/standards – will ensure you can articulate and achieve the right level of cyber security assurance needed for your organization.

1.1 Defining what 'good' looks like

At the outset, Nettitude will sit down with your senior team to establish the end goal, what 'good' looks like for your organization. Determining the scope, scale and expected goals will enable the right questions to be asked and the right approach to be taken.

This may lead to a staged approach to good based on developing maturity. It should be understood that this cannot be 'learned' in a training session, or completed by updating a policy document alone. It is a way of operating, thinking and behaving with the ability to have effective business functions operating and reporting in a timely manner as required.

The ability to respond effectively to a future cyber event will only come through cultural changes, education and mind-sets that adopt the objectives and purpose of your cyber strategy.

02 Building Blocks: Key Considerations

Before you build a cyber security strategy, the following key thoughts should be considered:

1. **Define your strategic approach and leadership:** Ensure you have identified and resourced the people, teams and focus that is appropriate for your organizations
2. **Become threat-centric:**
   a. Know what assets are important to your organization
   b. Understand how cyber threat actors are likely to strike
   c. Gain a true picture of your organization's threat environment and threat surface
3. **Consider it now:** If you wait to think about cyber security after a breach, you're already in trouble
4. **Expect the worst:** Shift mind-sets and attitudes from 'it'll never happen to us', to 'when it happens to us'
5. **Look at the most likely attack paths first:** Work on common attack vectors/paths (e.g. phishing) – consider the risk of issues that come from human error
6. **Privacy by design:** Build security thinking into each part of your business eco system
7. **Gain assurance:** Ensure awareness of your current ability to detect and respond effectively - Conduct Threat-Led Red Teaming simulation exercises and verify the response capability
8. **Test, train and prepare:** Continuously emulate adversaries to measure and assure how your detect and response capability works
9. **Learn, evolve and mature:** Recognize that your business is living. Scope, operations, threats, processes, innovation, technology, people - all of these change therefore your cyber strategy must be constantly reviewed, dynamic and adaptable.

2.1 Nettitude's Approach

The diagram below shows the approach that Nettitude has developed in order to create an effective approach to developing a cyber security strategy. This can be applied across all sectors, geographies and business models:

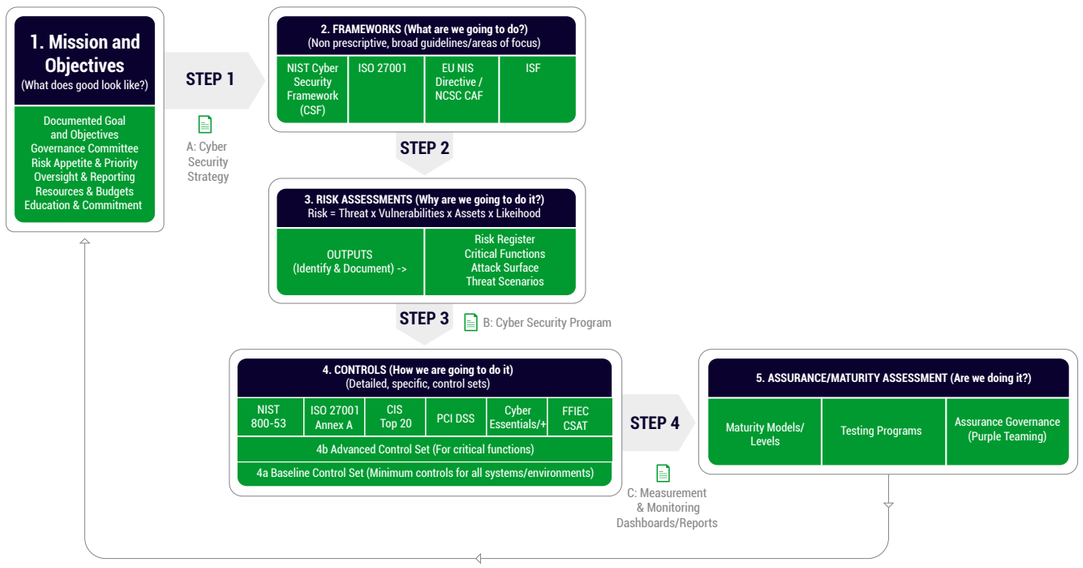

Figure 1: Cyber Security Strategy Lifecycle

2.2 Stage 1: Mission and Objectives (Define what good looks like)

Many organizations fail to define the overall objective for a cyber strategy or program of work. How do you know when you have got what you need? What is a good cyber security posture for your organization and how do you know when you have got there?

This description of what good looks like should be defined by business outcomes but include enough clarity to be measured and assessed.

There are 6 key elements:

1. **Documented Goals and Objectives:** Have you set out to the whole business what the end game looks like? What are you protecting, from what threats and how important is this to the organization? Define the services, assets and things you need to protect and in what way. Describe the objectives from a business impact perspective.
2. **Governance Committee:** Who will oversee and measure the progress and current state of security posture? Your governance committee needs to be able to challenge and question, provide the checks and balances to the operational state and have the power to test and verify outcomes.
3. **Risk Appetite & Priority:** Define a clear risk preference or appetite for the organization. What level of risk is tolerable and what is unacceptable?
4. **Oversight & Reporting:** Define the dashboards, the metrics/KPIs and the measurements that test the goals and objectives. Defining the right things to measure can be one of the hardest tasks to get right. Ensure the technical output can be translated into business outcomes.
5. **Resources & Budgets:** Make budget and resource decisions based on the goals and objectives required.
6. **Education & Commitments:** Ensure buy in by the business (managers and team members), ensure ownership, accountability and belief.

Sector Specific Requirements

Within any given cyber security strategy, sector specific requirements will need to be addressed. For some industries, regulation and oversight around cyber resiliency is mature and focused, for example within Financial Services. However, many other sectors are maturing or even just starting to look at the threats faced. Many areas of critical national infrastructure, for example, contain challenges around the integration and operation of IT vs OT environments, and the opportunities presented by connectivity, cloud and automation (e.g. Industry 4.0) mean the attack surface for many industries is rapidly changing.

The EU NIS Directive is focusing attention on critical national functions within a wide range of sectors including transport, energy and utilities. Marine and Offshore is developing and Nettitude have a specific framework and vessel class standard to look at the safety related threats facing the industry.

Your strategy and approach to the threats faced should take into account the specific needs presented by the sectors, geographies and business model you have adopted.

2.3 Stage 2: Frameworks (What are we going to do?):

Once stage 1 has been set, and often in parallel to its development, the selection and choice of a cyber security framework is essential. There is often a need to use different frameworks for different needs but a main standard should be selected from which the others should be linked or cross referenced. The choice is wide and will vary depending on sector, geography, business model and your own internal skill sets.

A framework is not the same as a control set. The framework gives an organizational and operational model to hang your overall approach to security from.

Examples include:

- NIST Cyber Security Framework (CSF)
- ISO27001
- ISF Standard of Good Practice (SoGP)

Equally, you may define your own approach. This should be done to provide the structure from which the objectives and goals for the business can be met.

In addition, Nettitude has worked extensively to create operating models for security functions within organizations. A critical example is within the detect and response capability, often run as an in house or 3rd party security operations center (SOC). Delivering a mature, capable and relevant service that meets the needs of the cyber security strategy objectives is a particular challenge faced by many organizations, as this is not yet well defined within the industry.

24 Stage 3: Risk Assessments (Why are we going to do it?)

Before any work is done on developing controls (people, technology or process) a risk assessment should be conducted. Without a fundamental idea of what you're protecting, where it is, and how it could be impacted by a cyber threat, it will be impossible to define the relevant or appropriate level of controls or mitigations required.

The risk assessment process should result in a risk register that defines the critical functions, their dependencies, their operation and use, the threats faced and the vulnerabilities within the environment. The likelihood of these threats impacting the assets can then be defined and the overall risk level determined.

Unless this is defined at the business level, it will be hard for the engineering teams, development teams and the SOC (detect and respond capability) to be aligned in their purpose and objectives – let alone being able to prioritize work effectively.

An organization's appetite for risk and their maturity towards it will influence the starting point for this work. However, Nettitude will seek to educate and migrate the risk management process and policy towards the upper end of the scale.

In reality, differences are often seen in the approach taken as shown on the scale below. This is often seen between the governance committee and the operational or tactical departments implementing controls.

Figure 2 – Risk Scales

Nettitude aims to operate at the strategic, operational and technical levels and will seek to accommodate any existing risk frameworks in use already.

2.5 Stage 4: Controls (How are we going to do it?)

Controls should be selected to reduce risk. They should be deployed in a way that is measurable and impacts the risk appetite of the business in a positive manner. There are many security control sets that can be used and leveraged to assist with this and an appropriate set(s) should be used to support the delivery of the strategy.

In most cases, a baseline level (minimum standard) should be defined for all systems alongside an enhanced control set of high security areas and systems. The approach to security architecture, the business model and the nature of services being delivered will affect the choice and application of these controls.

2.6 Stage 5: Assurance/Maturity Assessments (Are we doing it?)

In order to effectively measure success and progress, it's essential to develop appropriate assurance methods and assessments. The use of vulnerability scanning, penetration testing and red team testing will provide levels of assurance for different purposes.

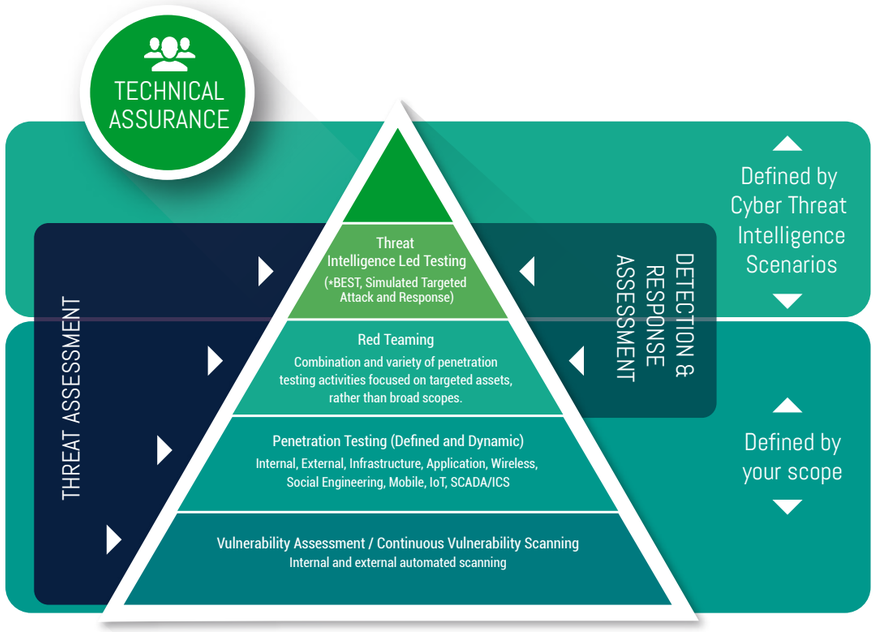

Figure 3: Technical Assurance Sophistication Levels

By applying a maturity model to your security strategy, a staged approach and prioritized task list can be developed. Signing off, maintenance and continuous assurance needs to be considered and planned/reported effectively. A mature organization will adopt a continuous level of assurance at the lower level (vulnerability assessments and identification) with penetration testing built into BAU service, platform, software and component testing and red team/threat led simulations to test the business level threats being addressed.

Nettitude can help develop the right levels of assurance, for each part of your business, strategy and environment.

03 Summary

Developing, implementing and running a cyber security strategy is a long term activity. Getting feedback, and maturing and evolving a strategy is key as it's not a linear process. Cyber security threats evolve faster than many other threats to our organizations, so ensuring adaptability and current awareness of these threats and your current security posture is key.

Nettitude can help establish the right approach to developing a cyber security strategy for your organization.

Getting this right will allow all the other elements shown in the diagram below to flow down from this and be delivered to meet a common goal and clear need.

CYBER SECURITY STRATEGY, FRAMEWORKS, STANDARDS AND CONTROLS

NOTE: It is fully recognized that there are many frameworks and standards in use, all relevant to regulators, data held and business needs. A mapping tool has been created that shows the common areas across the following: NIST Cyber Framework, NIST 800-53, ISF Standard of Good Practice, Cyber Essentials, PCI DSS, ISO27002, COBIT 5, Cloud Security Alliance, UK ICO Protecting Data, FFIEC Examiners Handbook and others.

Please contact us for a further conversation.

Please speak to us further for more information on how we can support you

NETTITUDE
AN LRQA COMPANY

NETTITUDE

AN LRQA COMPANY

UK Head Office
Jephson Court, Tancred Close, Leamington Spa, CV31 3RZ

Americas
50 Broad Street, Suite 403, New York, NY 10004

Asia Pacific
1 Fusionopolis Place, #09-01, Singapore, 138522

Europe
Leof. Siggrou 348 Kallithea, Athens, 176 74 +30 210 300 4935

Follow Us

solutions@nettitude.com
www.nettitude.com