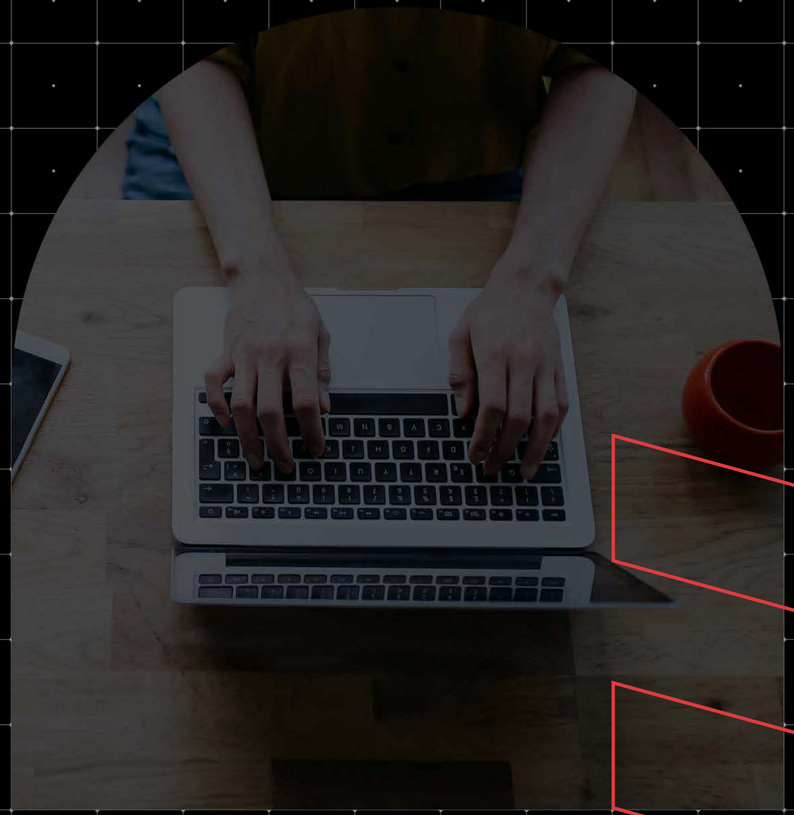
NEXON

Expert Strategies for Tackling Cyber Security Norms



Daniel Weiss
Garth Sperring

Index

Letter from the author 3
A note from Garth Sperring

Introduction 4

Strategy 1 5
Preemptively safeguarding your cyber security

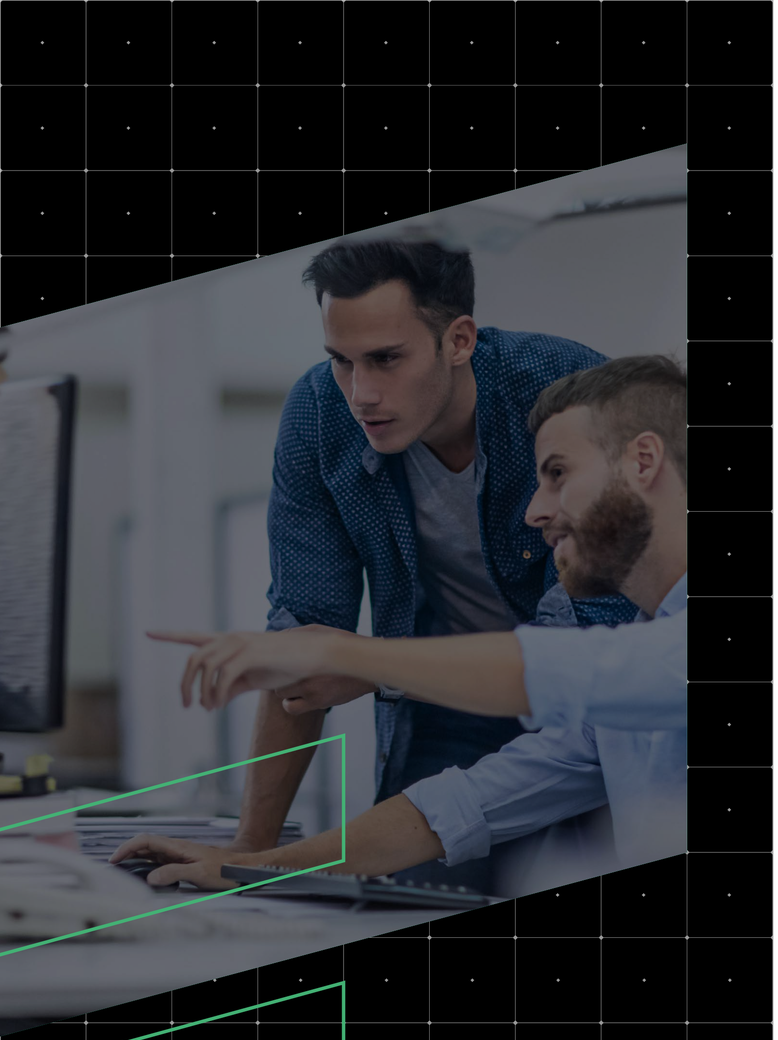
Strategy 2 8
Producing an agile prevention approach

Strategy 3 10
Defining a detection strategy

Strategy 4 12
Creating a robust reaction strategy

Conclusion 14
Safeguarding your future through cyber protection

Meet the authors 15
Authors' biographies



Letter from the author

Dan Weis and I created this eBook to share our knowledge, and give business leaders and decision makers like you the insight to tackle the world of Cyber Security. In doing so, we hope to demystify Cyber risks, and help you learn how to highlight risks that may affect your business by seeing them for what they really are.

As Nexon's Network & Security Business Lead, I am proud to head a team of experienced and passionate security professionals who, combined with our managed security services, help our clients understand and defend against the Cyber risks associated with running a business in today's ever-changing environment.

We are a hyper-connected society. We enjoy the freedom and convenience that easy-to-consume mobile and connected services offer at work, in our home and at play. However, this also means that everyone, anytime, anywhere is exposed to Cyber risks. This poses a larger problem: not everyone who uses an app understands the associated risks—let alone how to defend themselves.

As a result, Cyber Security is often shrouded in mystery. It's difficult to discern between the benign and the reality of the risks associated with something that is not well understood. When we fly, we don't need to understand aeronautical engineering and design, or the job of the pilot and crew. We trust in the historical reputation of the airline.

In the same vein at Nexon, we choose to partner with our clients so that they can go about their business in the same way — knowing that they're working with a team that holds a proven history — with confidence that we'll always have their Cyber Security in hand.

We hope this eBook will enable you to make informed decisions to secure your business operations, especially as we move as a world to adopt new business models, new connected applications and most importantly, learn to adapt to new ways of working.

Garth Sperring
Nexon's Network and Security Practice Lead
Product Services

Introduction

Whether you're an experienced practitioner or new to security practices, this eBook will provide you with comprehensive and clear-cut insight into modern Cyber Security.

We'll dissect exactly what your business needs to understand about Cyber Security, how implementing a strong Cyber Security strategy is essential to protecting your business, and how to go about developing a strategy that will benefit your operations now, and into the future.

This discussion will be broken down into the following sections:

1. **Preemptively safeguarding your cyber security**

   How your business can establish a foundation at the outset that is able to anticipate cyber security threats before they emerge.

2. **Producing an agile prevention approach**

   How to prevent a cyber security attack by devising a strong prevention strategy.

3. **Defining a detection strategy**

   How to build processes into your business operations in order to quickly detect potential cyber security breaches.

4. **Creating a robust reaction strategy**

   The specific steps your company should take when responding to a cyber security threat.

By evidencing the immense and complex cyber security threats posed to a modern-day business, we explain how the right cyber security strategy can help your business continue to operate safely today, while building its next security chapter for tomorrow with complete confidence.

Strategy 1

Pre-emptively safeguarding your cyber security

Understanding the threat

Businesses today are facing immense and agile threats to their Cyber Security. From the general risks of privacy breaches and compromised data, to the more sophisticated penetration of Cyber Security systems by cyber criminals — businesses must act against those who are determined and dangerous. Now more than ever, state-based actors essentially guarantee a greater threat to your Cyber Security, given their endless resources. The consequences of a Cyber Security breach can cause immense harm to the finances, reputation, and operations of any business.

Though these dynamics have existed in the Cyber Security space for many years, the onset of the coronavirus pandemic has further deepened the challenge. Many businesses and industries were already becoming more digital in their operations before the pandemic. The rapid onset of the virus has sped-up this process, and increased the pace of digital transformation—causing a heightened need for preventative Cyber Security measures.

This transformation has unquestionably exposed more businesses to a far greater risk of Cyber Security breaches. Even businesses that have not substantially changed their operations due to the pandemic have found themselves more vulnerable, with more people than ever before relying predominantly on digital technology to continue ongoing business operations.

Garth Sperring, Nexon's Network & Security Practice Lead Product Services, has seen the effect of this transition first-hand.

> Everybody is a target, and as much as you may want to not believe it, you will be hacked at some point.
>
> What this means is that you should have incident response processes in place, invest in cyber security technology, and have a roadmap setup for improvements, training programs in place and regular testing of your incident response capabilities to ensure that you are prepared and can quickly and effectively respond to a cyber attack or data breach.
>
> Garth Sperring
> Nexon's Network and Security Practice Lead
> Product Services

Strategy 1

Pre-emptively safeguarding your cyber security

Crafting a cyber security plan

Cyber security threats are real and confronting. However, businesses can take proactive steps to enhance their cyber security in response to emerging threats. The key focus for any business operating digitally is to minimise the risk of a breach and maximise the capacity to respond to it swiftly if one occurs. Contemporary threats in cyber security are highly sophisticated and continue to evolve daily. Your preparation and response to the potential of a cyber security attack must be as equally sophisticated.

Developing a strong, proactive cyber security strategy requires ongoing education, and can be furthered by increasing cyber security awareness activities amongst staff. Businesses that wish to address cyber security preemptively could run security event simulations so that, in the event of a cyber security attack, they have a plan in place to be able to mount an effective response quickly. These businesses could also partake in penetration and vulnerability testing regularly, to identify and address any potential weak points in their cyber security strategy.

Education and awareness training

Your staff's awareness of Cyber Security concerns can be your strongest asset or weakest link in safeguarding your organisation. Staff who undergo regular education and are vigilant in maintaining best practices in online activities and the management of data offer a strong line of defence against the risk of a breach.

Security event simulations

In order to guard against a Cyber Security attack, it is necessary to understand how attackers operate. This is where security event simulations —controlled processes through which your existing systems are 'pressure tested'—are invaluable for understanding how they would perform in the event of an attack. Among the best ways to pre-emptively prepare for a cyber security attack is to undertake a penetration test.

Penetration testing

A penetration test is where a reputable security provider will perform an assessment of your systems, users, processes, defensive and detection systems and overall security posture of your organisation. Your organisation will then be provided with a detailed report; detailing all of the risks, threats, vulnerabilities and overall security posture of the organisation, as well as recommended remediations to apply—thus increasing your company's overall security posture.

Strategy 1

Pre-emptively safeguarding your cyber security

A penetration test typically commences with a precise goal on the part of the simulator(s) that tests a specific aspect of your cyber security defence. This style of testing provides immense insight into which existing systems are working well, and which flaws within the existing system architecture could be exposed through an attack.

Vulnerability testing

Often incorrectly conflated with penetration testing, vulnerability testing ultimately seeks a complementary, but different, goal. Vulnerability testing is used to identify the potential exploitation avenues that can be leveraged by an attacker. It also identifies common vulnerabilities, such as missing patches or the misconfiguration of systems.

The key aim of this process is to identify where loopholes exist within your cyber security infrastructure and to assess their associated risk accordingly. This process is always invaluable. Even if a system stands up well to a simulated attack, every attack can ultimately differ in its goals and methodology. Vulnerability testing offers an avenue to cover all bases and to close all known loopholes.

Anticipate and deter attacks using a strong pre-emption strategy

Businesses that implement a strong and agile cyber security strategy gain greater peace of mind. Threats are sizable and diverse, but the right strategy can offer a very high level of protection against them. Having the right resources—such as cyber insurance cover—in place to help combat and neutralise any attack that does occur is imperative for any business.

Daniel Weis, Nexon's Senior Cyber Security Specialist, has seen the benefit first-hand of having a strong pre-emption strategy in place.

> Ensuring you have cyber insurance coverage in place allows you to call on a network of professionals in the event of a data breach.
>
> Daniel Weiss
> Nexon's Senior Cyber Security Specialist

Why prevention is better than a cure

Today's world is more complex and uncertain than at any other time in human history. Our daily work relies heavily on the digital economy, leaving our businesses vulnerable to online threats. In addition, widespread economic crises, natural disasters, and global pandemics have made it essential for businesses to learn how to bounce back and recover quickly in adverse situations.

The ability for a business to rebound does not happen overnight. Building up resilience and ensuring that you can stay in control when times get tough requires the careful creation of prevention systems, as well as ongoing vigilance in their application and maintenance by a team of professionals who understand the ins and outs of cyber security prevention.

Threats are inevitable: how can you navigate them?

Businesses will always face uncertainty, just as they will always face cyber security threats. There is no use ignoring them or trying to remove all unknowns. The best way for an organisation to do business in this environment is to acknowledge the potential for threats and to be proactive about their prevention strategy.

The key to dealing with cyber security threats is identifying them before situations escalate and preparing accordingly. Cyber criminals use a variety of sophisticated methods to gain entry to your systems, including threats such as password sprays. In order to respond to threats like these, businesses need to be technically proficient in their systems and aware of where breaches may be likely to occur.

The specific threats a business may face can vary considerably from one business and industry to the next. However, businesses that are proactive in preventing cyber attacks have a common component: a planning life cycle for prevention that is continuous, circular, and able to be utilised in a variety of situations.

Developing a prevention strategy to mitigate the risk of cyber security attacks

Developing a strong prevention strategy for your business requires real skill and precision. The strategy must also incorporate the various stages of prevention: reduce, response, recover, resume, restore, and return. Collectively, these stages form a digital wall of defence that helps safeguard your business's cyber security. According to Weis:

> Arguably, most data breaches happen through phishing and a lack of awareness.
>
> It's important that you ensure you have a regular phishing and awareness training platform to keep staff on the lookout for phishing emails. Along with user education, you should be undertaking regular penetration testing to make sure your systems and technologies are as secure as they can possibly be and have the necessary security controls in place.
>
> Daniel Weiss
> Nexon's Senior Cyber Security Specialist

Strategy 2

Producing an agile prevention approach

He adds that, “this testing can also include Blue/Red/Purple teaming exercises to ensure that you can detect and respond effectively to a malicious adversary. You should also ensure you are utilising cloud services such as Office 365 and cloud security controls such as MFA, Conditional Access, Data Classification policies and secure score.

All Internet facing services must have MFA configured to prevent data breaches through password attacks such as sprays. Internally, you should be leveraging an Endpoint Detection and Response (EDR) product that incorporates cyber threat containment controls and application controls/whitelisting such as Carbon Black”.

By being aware of potential threats, your business can successfully set up systems to manage different risk scenarios. In turn, this approach can help adapt and refine your processes in response to the wider world of security threats.

Specific solutions organisations may want to adopt include:


Analysis of current systems and risks


Design of potential solutions


Implementation measures


Testing and acceptance


Maintenance of systems


Further analysis

Investing in the resources of a security partner like Nexon can assist with the identification and implementation of an appropriate solution for your business—based on your company’s individual needs.

Is your business vulnerable?
Organise a Cyber Security Assessment with a Nexon expert today.

Book your assessment

Strategy 2
Producing an agile prevention approach

Strategy 3

Defining a detection strategy

Why Cloud is critical to preventing cyber security attacks

The use of cloud technology within the business environment has rapidly advanced during the past decade. Cloud tech offers an easy and efficient way for organisations to store, share, and collaborate on data. Although the opportunities that cloud offers are tremendous, the same storage and methods that make the technology so useful can also result in a greater vulnerability to cyber attacks. In fact, it's not uncommon for adversaries to be operating within a network for days or weeks before an attack actually occurs.

It is critical for organisations to understand how they can use cloud management and monitoring capabilities to their advantage. Today, we're seeing more effective Security Incident and Event Management (SIEM), as well as stronger Managed Detection Response (MDR) and SIEM collaboration. Ongoing advances in the integration of AI and data are particularly promising, as these technologies can work together with impressive precision to quickly detect a cyber attack as it begins.

The importance of cutting-edge Cloud technology

In the current environment, businesses can no longer accept cloud services that remain a step behind contemporary technology and its capabilities. This includes cloud services that lack the capacity to deliver in-depth analysis of data. These services are often unable to provide credible risk assessment of infrastructure and personnel resources (including the analysis of security threats that can be posed by both employees and computers alike). Sperring notes:

> These days, everyone knows they will be hacked at some point, but it's now all about how quickly you can detect, respond and contain the threat
>
> Garth Sperring
> Nexon's Network and Security Practice Lead
> Product Services

Strategy 3

Defining a detection strategy

The line of defence: artificial intelligence, data and Cloud

Implementing proper detection measures help cyber security experts prevent security breaches. It also allows for the quick identification of threats which operate behind the scenes that would otherwise go undetected. According to Sperring:

> A critical component of an in-depth defence strategy is having systems in place to detect Indicators of Compromise or IOCs.
>
> Garth Sperring
> Nexon's Network and Security Practice Lead
> Product Services

An IoC is a forensic term that refers to a device's evidence which identifies a security breach. The IoC gathers data after a suspicious security incident or event that is flagged by an organisation's network. Businesses should check IoC data regularly to detect strange activity or system vulnerabilities. Sperring continues,

"This can be achieved through the use of a SIEM solution (Security Information & Event Monitoring) which combines data from various sources e.g firewalls, active directory, server logs, EDR software etc and combines them in one central system and applies behavioural analytics and reputational analysis and threat feeds across the data to look for suspicious anomalies and IoCs and alerts accordingly."

"Most SIEM's also encompass SOAR (Security Orchestration and Response) capabilities which allows them to automatically take controls to reduce the severity of an attack, for example if an account has been detected as compromised, the system will automatically lock and change the password." The power of Artificial Intelligence (AI) in this arena is also important. AI assists in SIEM by analysing huge volumes of data in a fraction of the time compared to older methods. It can also help identify any hidden relationships that exist within the data.

As a self-curing system, it can identify and correct its own faults without human intervention, making it more effective each time. As a result, AI empowers IT teams to anticipate future cyber security threats and mitigate them before a breach occurs.

Why slow reactions are detrimental to your business

There is no room in today's business landscape for stagnation. With more pitfalls than ever before on the path to building a dynamic and agile business, it's understandable that organisations can face substantial setbacks in the process.

Businesses that thrive in this dynamic understand that there is immense opportunity amidst these challenges. With the right approach to scalability and flexibility, your business can achieve organisational agility and leverage it to your advantage — empowering your staff to pursue new avenues for growth and survive the turbulence that comes with operating in a globalised economy.

A case for a strong reaction response to a cyber security attack

To be able to effectively scale and pivot your operations, you must not only navigate changing economic conditions but hedge against direct threats to your survival.

This is where a comprehensive cyber security strategy is critical to combating threats like phishing and ransomware attacks. A comprehensive strategy helps ensure that — should an attack occur — your organisation has the capacity to recognise it, respond to it, and neutralise it. This is especially important as attacks often originate from unassuming sources, such as phishing emails.

A framework like this requires your business being ready to deploy both people and processes when the need arises. It outlines with precise detail the appropriate response to a threat, including what steps should be taken to secure your data and infrastructure as quickly and comprehensively as possible, so that your business and staff can keep operating while the threat is handled.

Are you on top of potential threats?
Reduce the risk of cyber security attacks with a cyber security assessment.

Book your assessment

Strategy 4

Creating a robust reaction strategy

Two reaction strategy options for your business

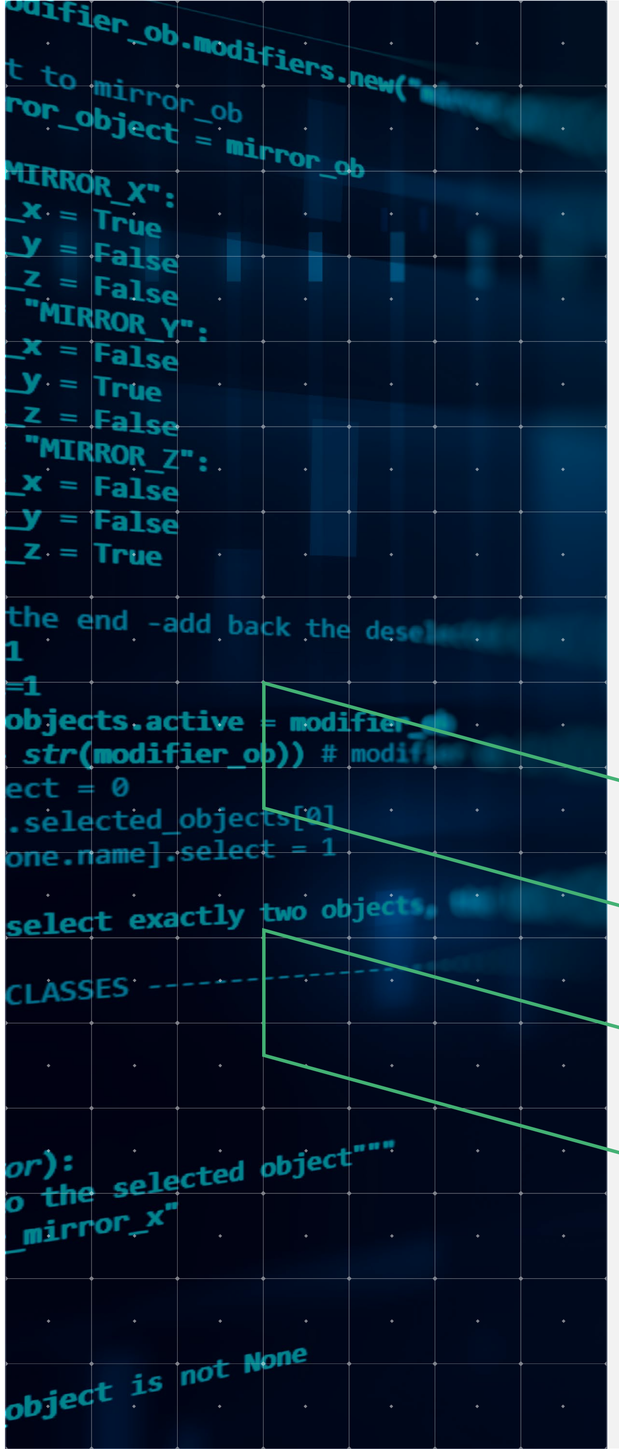
There are two possible approaches for businesses seeking to implement this strategy. Both are strong and capable, but one may be preferable for your business over the other depending on your team's unique needs and processes.

The first involves a centralised system that aggregates and analyses events from multiple sources, providing visibility across your business's digital environment.

The second involves ensuring access to people and processes that facilitate the examination of data entering into the SIEM via your business's digital environment.

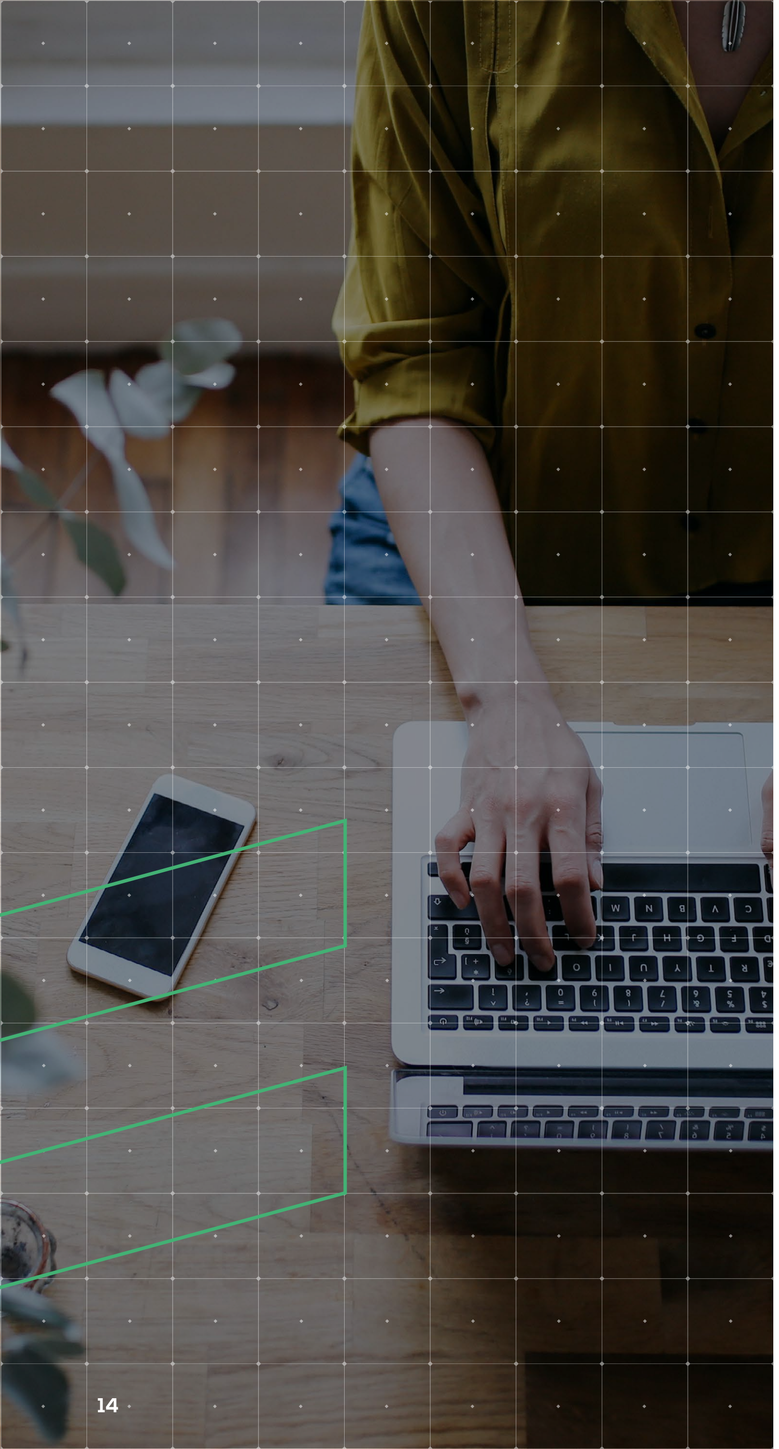
Sperring explains the importance of implementing a reaction strategy, stating, "Once an attack has been detected, this is where your Incident Response plans and processes come into play. The SIRT team will be kicked into action, containment measures are introduced/actioned (such as endpoint isolations and account changes) and investigative actions are performed."

> Remember, the longer an adversary is in a network or has access to a system, the more data they could potentially be exfiltrating from the network and the bigger the risk.
>
> How quickly you can detect and respond is key. Once the Incident is wrapped up, it's important that everything is documented, lessons learnt and ensure you have submitted any notifications to the OAIC.
>
> Garth Sperring
> Nexon's Network and Security Practice Lead
> Product Services



Strategy 4

Creating a robust reaction strategy



Safeguarding your future through cyber protection

Pre-empt, prevent, detect, and react

In order to craft a strong cyber security strategy, businesses must possess the ability to pre-empt, prevent, detect, and react. This is not a task that can be taken on alone, but should instead be addressed with expert insight and support.

Not only is it crucial for your business to understand the key foundations of cyber security that must be present within your organisation, you must also be able to identify partners like Nexon who can assist in ensuring the ongoing security and stability of your operations.

A solid pre-emptive strategy is informed by the understanding that it's impossible to contain all threats, but that it is possible to anticipate them. Similarly, a good prevention strategy requires the recognition that there is not simply one step to preventing cyber security attacks. Rather, a multifaceted approach is required. When it comes to detection, the need for cutting-edge Cloud technology is essential. Finally, the proper reaction to a cyber security attack requires a framework that can deploy the appropriate people and processes to contain it.

The challenges of defending against future cyber security attacks are substantial, but they are not insurmountable. At every stage of your business's growth, the opportunity exists to optimise cyber security processes to defend its infrastructure and future operations.

To learn more, or to gain a better understanding of your organisation's existing cyber security capabilities—reach out to Nexon and schedule a cyber security assessment today.

Doing nothing is not an option.
Organise a cyber security assessment with a Nexon expert today.

Book your assessment

Meet the authors

Daniel Weis

Senior Cyber Security Specialist, Nexon's leading Australian cyber security expert

Daniel Weis is a Licensed Penetration Tester, and one of the first 10 people globally to become a v7 Certified Ethical Hacker. As an active participant in renowned security and IT industry programs and development strategies, Weis has worked in multiple high stake security environments across law enforcement, government security and private businesses. Daniel now works as Nexon's Senior Cyber Security Specialist. He recently released his book, Hack Proof Yourself! The essential guide to securing your digital world.

Garth Sperring

Network and Security Business Lead, Nexon's leading Australian cyber security expert

Garth Sperring has worked with Nexon to demystify cyber security and provide customers with end-to-end visibility of their activity and surrounding environment. Sperring has helped secure multiple environments before an attack was successful. He has worked to collate data across security infrastructure services such as O365, Proofpoint and API enabled SaaS applications to give insight to user activity. Sperring enjoys the success of Nexon's implementations, which involve the full suite of cyber security services, integrated into the network, infrastructure, cloud UC and Cloud services for client environments.

About Nexon

Nexon Asia Pacific (Nexon) is an award-winning digital consulting and managed services partner for mid-market, and government organisations across Australia. We have a uniquely broad suite of solutions to service clients who require end-to-end capabilities coupled with specialist expertise in security, cloud and digital solutions.

Our end-to-end solutions help clients to solve problems, address frictions and accelerate growth. Committed to the highest standards of responsiveness, competency and transparency, Nexon is built on a unique client care model that is fuelled by continuous feedback. With over 400 staff, we employ some of the country's most experienced consultants and empowers teams to make decisions that accelerate change for client organisations.

As a certified and accredited local and state government provider, CREST and ISO-certified, Nexon partners with world-class technology vendors to deliver innovative solutions and service excellence.

We help our clients move from a position of overwhelm to empowerment, looking forward to a more agile and digital future.

Look to the future, with Nexon

Take the next step.
Get in touch with the Nexon team.

1300 800 000
enquiries@nexon.com.au
nexon.com.au

Follow **nexonap**