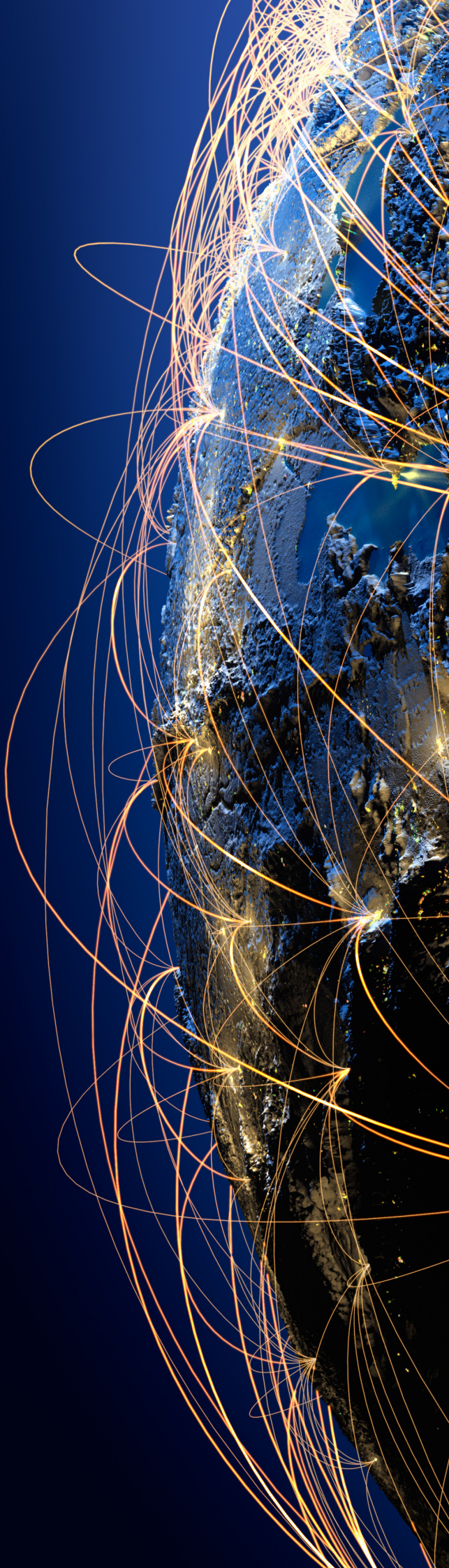
KPMG

Cyber security guide for SMEs



KPMG New Zealand

kpmg.com/nz/cyber

Contents

"Cyber security is becoming a risk that needs to be considered by all businesses."

New Zealand SMEs are often underestimating the impact a cyber-attack could have on their reputation and must take steps to protect it.

Traditionally cyber security has been a risk associated with big business, however, as the global digital landscape has become more accessible, the range of threats has extended and protection cannot be taken for granted.

Furthermore, increasingly clients and business partners are asking questions about the cyber security controls implemented within an organisation, to ensure that their information is protected. Demonstrating that you have effective cyber security controls in place builds upon the trust you have already established, and may also provide you a competitive advantage.

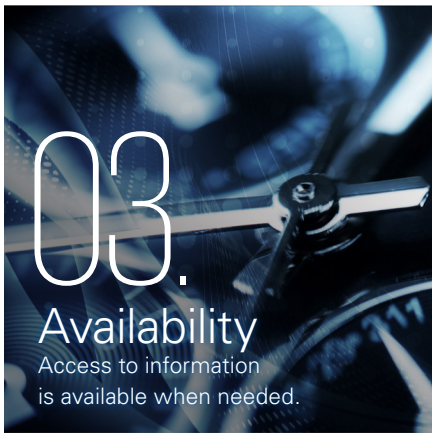
Cyber security is by no means an all or nothing approach but should be something that scales as the business grows. Over the next few pages, we aim to demystify some of the key elements of cyber security that are relevant for SMEs, to help you ensure that you are starting to take the necessary steps to improve your cyber security environment.

What is cyber security?

Put simply, cyber security is about an organisation's ability to protect its information assets and its preparedness against IT security threats.

This takes into account a rounded view of people, process and technology to reduce vulnerability and the long term impacts of any breach.

CYBER SECURITY CONSIDERS THREE ASPECTS:



The cyber security threat landscape in New Zealand and globally has rapidly changed, particularly over the last five years.

Tactics and tools developed by crime syndicates are sold or freely shared – as a consequence the average level of attack sophistication is increasing.

Money, or information that can be sold for money, is not always the target, with organisations increasingly being attacked for actions perceived as unethical, or because of political desire to gain economic advantage.

The threat landscape is now made up of many players, including organised criminals, opportunists, insiders (such as disgruntled staff), political activists, terrorists and foreign nations.

Why is cyber security important to your business?

In the digital economy, the valuation of a business is based heavily on its intangible assets, whether this is transactional data or intellectual property (IP), customer information or other similar data assets.

A breach of your data could lead to competitors gaining access to valuable IP, loss of customer trust, or potential legal and financial implications. For this reason, SMEs can't afford to ignore cyber security.

According to the Institute of Director's 2016 Directors' Risk Survey, cyber security is in the top three business risks faced by most New Zealand organisations, including SMEs.

Business is built upon trust, and while it takes many years to build a brand and an organisation's reputation, if cyber security controls are not effective, this can be destroyed in a nano-second.

At the same time, ensuring New Zealand is secure and resilient online is essential to building a more competitive and productive economy. This is why cyber security is a priority of the New Zealand Government. The Government's Cyber Security Strategy recognises that the threat to New Zealanders and the New Zealand economy from cyber intrusions is real and growing.

'A breach of your data could lead to competitors gaining access to valuable IP, loss of customer trust, or potential legal and financial implications.'

Penetration testing

What is it?

Penetration testing (also known as pen testing) is the process by which a computer system, network infrastructure or application (including those that are web based) is tested to find vulnerabilities that a hacker could exploit.

The goal of penetration testing is to identify any vulnerabilities, ascertain what they are, where they are and provide recommendations to fix them.

Penetration testing provides insights and recommendations through simulating what someone seeking to gain unauthorised access would do – whether from the Internet, against your wireless network or within an organisation. It provides the insight and feedback necessary to protect the IT environment against an external or internal attack.

As well as aiming to identify technical weaknesses, penetration tests can look to identify weaknesses in an organisation's security policies, behaviour and culture.

Why would I need it?

The goal of penetration testing is to identify any vulnerabilities, ascertain what they are, where they are and provide recommendations to fix them.

Penetration testing provides insights and recommendations through simulating what someone seeking to gain unauthorised access would do – whether from the Internet, against your wireless network or within an organisation. It provides the insight and feedback necessary to protect the IT environment against an external or internal attack.

As well as aiming to identify technical weaknesses, penetration tests can look to identify weaknesses in an organisation's security policies, behaviour and culture.

How do I go about getting it?

Is the organisation reputable?

In some cases you are giving them quite sensitive access to your systems; do you trust them with this?

What is the technical expertise of the testers?

Your penetration test is only as good as the technical expertise of those carrying it out. An organisation with highly skilled penetration testers is likely to find vulnerabilities that may be harder to spot.

Do they just use automated techniques, or is there also a high degree of manual testing?

Penetration testing involves the use of both automated and manual testing techniques. Some penetration testers will however just use automated tools to find vulnerabilities. This is likely to result in a lower quality test, and may miss 8 Cyber

Phishing, spear phishing and whaling

What is it?

Phishing is a deceptive process by which a cyber-criminal attempts to make you divulge sensitive or confidential information (such as passwords or credit card information), or attempts to make you undertake specific actions (such as downloading malware or making a payment to them).

Typically carried out via email, phishing attacks may also come via other technologies such as instant messaging, text messages or phone calls. The phishing correspondence commonly appears to come from a legitimate party with who you may a relationship with.

Phishing represents the most common method used by cyber-criminals to gain unauthorised access to systems, or to distribute malware such as ransomware, which extorts money by encrypting all of your data until you pay a fee.

Spear phishing is a targeted and more sophisticated form of phishing. Unlike standard phishing schemes that use mass emails, spear phishing targets individuals that fit a certain profile. For example, it may only target senior staff of a specific organisation, or users of a specific website.

Whaling is phishing for the bigger fish. Phishing attacks targeted at senior members of staff, such as C-level executives. This can include, for example, a phishing email to the Chief Financial Officer appearing to come from the Chief Executive, in an attempt to get fraudulent payments made.

How do I combat phishing attacks?

There are several proactive steps an organisation can take to minimise the likelihood of a successful phishing attack. These cover people, process and technology, as no one element is sufficient.

Educate and train all staff – It is critical to provide ongoing training and education for all staff, including C-level executives, in order to increase security awareness. Remember it only takes one staff member opening an attachment in a targeted email to open the door for cyber criminals and potentially compromise an organisation's network.

Perform simulated phishing attacks – Organisations should perform simulated phishing attacks to measure the effectiveness of their end-user education and incident response processes. These simulations can help an organisation identify individuals and groups that require additional training and help to identify gaps in security controls and policies.

Develop an incident response process – By developing an incident response process that defines key roles and responsibilities as well as internal and external coordination steps throughout the incident life cycle, an organisation can prepare itself for a potential phishing attack, as well as other cyber-attacks. In addition, the organisation should test its plan periodically to help ensure that staff are prepared to respond to an incident and that the planned steps are effective.

Update patching and antivirus programs – Effective patch management and up-to-date applications, including web browser add-ons such as Java and Adobe Flash, are critical components of an effective defence. An organisation should confirm that its antivirus programs, operating system patches, and application patches are up-to-date in order to increase its overall security posture and protect against cyber-attacks.

Limit who has administrative access of their workstation – Most staff do not have a need to have administrative access of their laptop or desktop computer. By limiting administrative access to those staff that absolutely need it to undertake their jobs, limits the ability for any malware delivered by a phishing attack to run.

Implement two factor authentication – Organisations should implement two factor authentication for remote access. Two factor authentication requires both something you know (such as a password) and something you have (such as a cellphone that a text message is sent to) to gain remote access. If someone inadvertently discloses their password as part of a phishing attack, unauthorised access will not be able to be gained as the attacker will not have the second factor.

Ensure that financial controls over payment processes are robust – Individuals are often tricked through phishing to make bogus payments. The payment processes in place should not be bypassed in the rush to make a payment because of an unexpected email.

PCI DSS compliance

What is it?

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organisations that handle credit and debit cards from the major providers such as Visa, MasterCard and American Express. The PCI Standard is mandated by the card brands and administered by the Payment Card Industry Security Standards Council.

The standard represents a common set of requirements to help ensure the safe handling of sensitive payment card information. Compliance with PCI DSS is reported to the merchant's acquiring bank.

Why would I need it?

PCI DSS applies to any organisation, regardless of size or number of transactions, that accepts, transmits or stores cardholder data. The number of annual transactions being processed will define the "Merchant Level", which range from 1–4.

Organisations that are not compliant may be liable for non-compliance fines if they do not work towards compliance with their merchant bank (known under PCI DSS as the acquirer). Ultimately, the acquirer may be forced to terminate the relationship, which will prevent the organisation from accepting card payments.

How do I go about getting it?

The first thing an organisation needs to do is fully understand how they process card payments. In particular, if the e-commerce environment is capturing, storing, processing or transmitting card data then they should think very carefully whether this is really necessary.

The most secure approach to processing e-commerce transactions is to outsource your card data to a Payment Service Provider (PSP). When the card data is outsourced, it is totally segregated from your environment and consequently the capturing, processing, storage and transmission of card data is totally removed from your e-commerce environment. This is commonly known as a 'fully hosted solution'. Often when a PSP is used, the merchant only needs to complete a shortened version of the Self-Assessment Questionnaire (SAQ).

If a PSP is not an appropriate solution, the organisation needs to consider the twelve high level requirements of PCI DSS, which fall into six categories. These cover: building and maintaining a secure network, protecting card holder data, maintaining a vulnerability management program, implementing strong access control measures, regularly monitoring and testing networks, and maintaining an information security policy.

"PCI DSS applies to any organisation, regardless of size or number of transactions, that accepts, transmits or stores cardholder data."

'Often when a Payment Service Provider (PSP) is used, the merchant only needs to complete a shortened version of the Self-Assessment Questionnaire (SAQ).'

Third party controls assurance

What is it?

Organisations are increasingly outsourcing activities to third party service providers. It is often difficult for an organisation to monitor the actions of the third party and this can introduce risk.

A third party assurance report, also known as a Service Organisation Assurance Report (SOAR), demonstrates an appreciation of clients' risks through obtaining third party assurance on effective processes and controls under an established international framework.

Why would I need it?

If you have outsourced certain aspects of your business to a service organisation, it may be important to you and your customers to know that the service organisation is following formal processes and policies when handling your data. In this scenario, you would want to obtain a SOAR report from your suppliers covering their processes.

On the other hand, if you are acting as a service organisation to your clients, they may require you to be covered by a SOAR report.

In both scenarios, the requirement may be the result of regulation that is specific to your industry, or may otherwise be a requirement of the procurement frameworks implemented by your clients.

How do I go about getting it?

The main international reporting standard for third party controls assurance is ISAE 3402, which is known as ISAE (NZ) 3402 in New Zealand. Another common reporting standard in New Zealand is SAE 3150. There is also an American standard, which is similar to ISAE 3402, known as SSAE 16 (which superseded SAS 70).

Unlike ISO 27001, there is no standard set of processes or controls that are covered by a SOAR report. The service organisation will work with the auditors providing assurance to draw up a relevant set of controls that will be adhered to and audited.

Under both reporting standards, there are two types of report:

Type 1: This is a snapshot, single point in time, view. It assesses the design of the controls and whether they are suitable to cover the control objectives set out in the agreed framework. An independent report will be issued for that agreed date.

Type 2: This will cover a consecutive period of typically 12 months, and will assess the design and effectiveness of the controls, set out by the agreed framework, during that period. This includes the steps involved in the Type 1 assessment plus the additional evaluation of the operating effectiveness of the controls.

'If you have outsourced certain aspects of your business to a service organisation, it may be important to you and your customers to know that the service organisation is following formal processes and policies when handling your data.'

ISO 27001

What is it?

ISO 27000 is a global family of standards relating to Information Security Management. Using this family of standards will help your organisation manage the security of assets such as financial information, intellectual property, employee details and information entrusted to you by third parties. ISO 27001 is the best known standard in this family, providing requirements for an Information Security Management System (ISMS).

The standard covers a variety of areas including physical and environmental security, information security policies, access control and operations security. Once a company has been certified as ISO 27001 accredited, they will undergo recurring audits to ensure compliance is maintained.

Why would I need it?

ISO 27001 is a widely recognised accreditation that many large organisations (particularly those offshore) will require from their suppliers. This is often because they are certified themselves and will want assurances that any sensitive data processed externally is done in a controlled environment.

In an environment where accreditation is not required, ISO 27001 compliance will often provide a market edge and demonstrate that you take customer data security seriously. It will also lower the risk of data breaches from accidental or malicious incidents and ensure that appropriate processes are in place for managing these incidents.

How do I go about getting it?

It is rare that a company will be ready for an ISO 27001 audit immediately.

A number of external organisations can therefore come in to assess your ISMS and conduct a gap analysis against the ISO 27001 controls. They will then work with you to produce a remediation plan to help you get up to the required standard.

When ready, you can undergo a formal audit, where the implementation of the ISMS will be assessed to ensure it is operating effectively, as required by ISO 27001.

When you have passed the formal assessment you will receive an ISO 27001 certificate, along with a statement of applicability which denotes the controls you have been audited against. This is valid for three years, within which you will receive regular visits to ensure you remain compliant and continually improve your ISMS.

When choosing your ISO27001 auditor, it is important to choose an auditor who is reputable in the market – you may find that many large corporates will only recognise audits that have been conducted by specific auditors.

'ISO 27001 is the best known standard, providing requirements for an Information Security Management System (ISMS).'

Business Continuity and Disaster Recovery (BCDR) Planning

What is it?

Business continuity and disaster recovery (BCDR) planning are the set of terms that cover the preparation and testing of measures that protect your business operations in the event of a disruptive incident.

Planning will cover the governance and processes related to an incident, such as who would contact and inform staff, where staff would work and how clients would be notified, as well as the technology in place, such as automated backups and fall-back systems.

Why would I need it?

Would your business incur significant costs during a period of downtime? Is the availability of timely information essential to your processes and those that rely on them? Do your staff and/or clients expect uninterrupted services from you?

Unexpected incidents, natural disasters, and malicious intent may disrupt information availability and negatively impact key business processes, causing lost revenue and adverse reputational damage.

BCDR planning helps you to ensure that the appropriate procedures are followed in the event of a service- disrupting incident, minimising risk, time offline and financial losses.

How do I go about getting it?

Organisations will usually have their own BCDR plans which they will work towards. However, if a more formal approach is desired, Business Continuity is covered by the ISO 22301 framework and Disaster Recovery by the ISO 27031 framework, which organisations can be accredited against. Aspects of BCDR can also be included in a service organisation assurance report.

You do not need to have reached a particular company size before you start thinking about business continuity and disaster recovery. Drawing up plans that define responsibilities and processes during an incident, as well as testing how your business would react to a real incident, are all good ways to start planning.

"Drawing up policies that define responsibilities and processes during an incident, as well as testing how your business would react to a real incident, are all good ways to start planning."

Cloud Computing

What is it?

In its simplest terms, cloud computing is an IT delivery model where computing resources can be delivered on a pay-as-you-use basis over the Internet – essentially you are leasing someone else's IT systems. It allows cloud providers to benefit from economies of scale, while giving smaller organisations access to high performance IT equipment and services.

Large and small organisations now have the confidence that the cloud offers the cost-effectiveness, agility and security necessary. However, not all cloud solutions are the same when it comes to security. Many will have robust security controls implemented, while others may not be as robust as they appear.

What are the different cloud models?

Private cloud – With a private cloud, organisations build their own dedicated cloud infrastructure. This dedicated infrastructure could be procured, built and managed by the organisation or it could be provided to the organisation by a third party. The advantage of private cloud infrastructures is that they can be more straightforward to secure as no other customers of the cloud provider have access to the dedicated equipment.

Public cloud – A public cloud service provider makes applications, data storage capacity and other resources available to organisations or the general public using its own servers. Public clouds offer the advantages of rapid service deployment and utility pricing.

Hybrid cloud – Hybrid cloud balances the use of different cloud deployment models and can offer organisations the advantage of flexibility and scalability. Hybrid cloud allows organisations to balance isolation, cost and scaling requirements.

Infrastructure as a Service (IaaS) – IaaS generally allows users to provision a virtual infrastructure for the processing and storage of data. Organisations can deploy a variety of virtualised servers in a flexible and easily changeable configuration.

Platform as a Service (PaaS) – PaaS provides users with the ability to develop and deploy applications of their own choosing on to a pre-configured "platform". In essence this means that the providers are responsible for the security and maintenance of the underlying virtualised infrastructures that provide the platform.

Software as a Service (SaaS) – SaaS delivers business applications for a usage or subscription-based cost at an agreed service level. In other words, organisations can make use of a shared service, such as a finance application or e-mail service, which removes any requirement for the organisation to develop and secure its own application and infrastructure (although a level of configuration effort will likely be required).

What are the security risks associated with cloud computing?

Inherently the security risks associated with cloud computing are similar to those when using your own systems and applications, but may be larger due to the shared nature of the solutions offered. Typically however, the scale of a cloud provider allows them to heavily invest in security, meaning that the security is likely to be better than what you could achieve yourself.

Not all cloud providers are the same however, so it is important that you do due diligence to ensure that robust security is implemented by the cloud provider. Often you won't have a direct relationship with the cloud providers, making it difficult to gain comfort over their security. Recognising this, most reputable cloud providers will have a Service Organisation Assurance Report (SOAR) available, detailing the results of an independent security assessment.

What are the key questions I should keep in mind?

- How sensitive is the data, and what are the necessary minimum security controls?
- How critical is the service to our organisation, partners and customers?
- Is the data subject to regulation? Do privacy restrictions apply?
- How is the confidentiality, integrity and availability of data maintained?
- Where is the data stored?
- If the data is stored off-shore, are the additional legal implications and risks assessed and understood?
- Can the data be encrypted in transit and/or at rest?
- Who generates, holds and distributes the encryption keys?
- Where is the data encrypted?
- How can you make your users' access to cloud services seamless yet secure?
- Can the data and service be easily moved to another provider?
- Does the provider preclude us from conducting our own penetration testing of our services?
- Is the provider and service compliant with applicable regulation?
- Is the cloud contract fit for purpose and compliant with all applicable regulation?

Philip Whitmore
Partner – Cyber Security
T 09 367 5931
M 021 654 846
E pwhitmore@kpmg.co.nz

KPMG Cyber Security

KPMGNZ_Cyber

kpmg.com/nz/cyber

connect SMART
Protect yourself online
GOLD PARTNER 2016/17