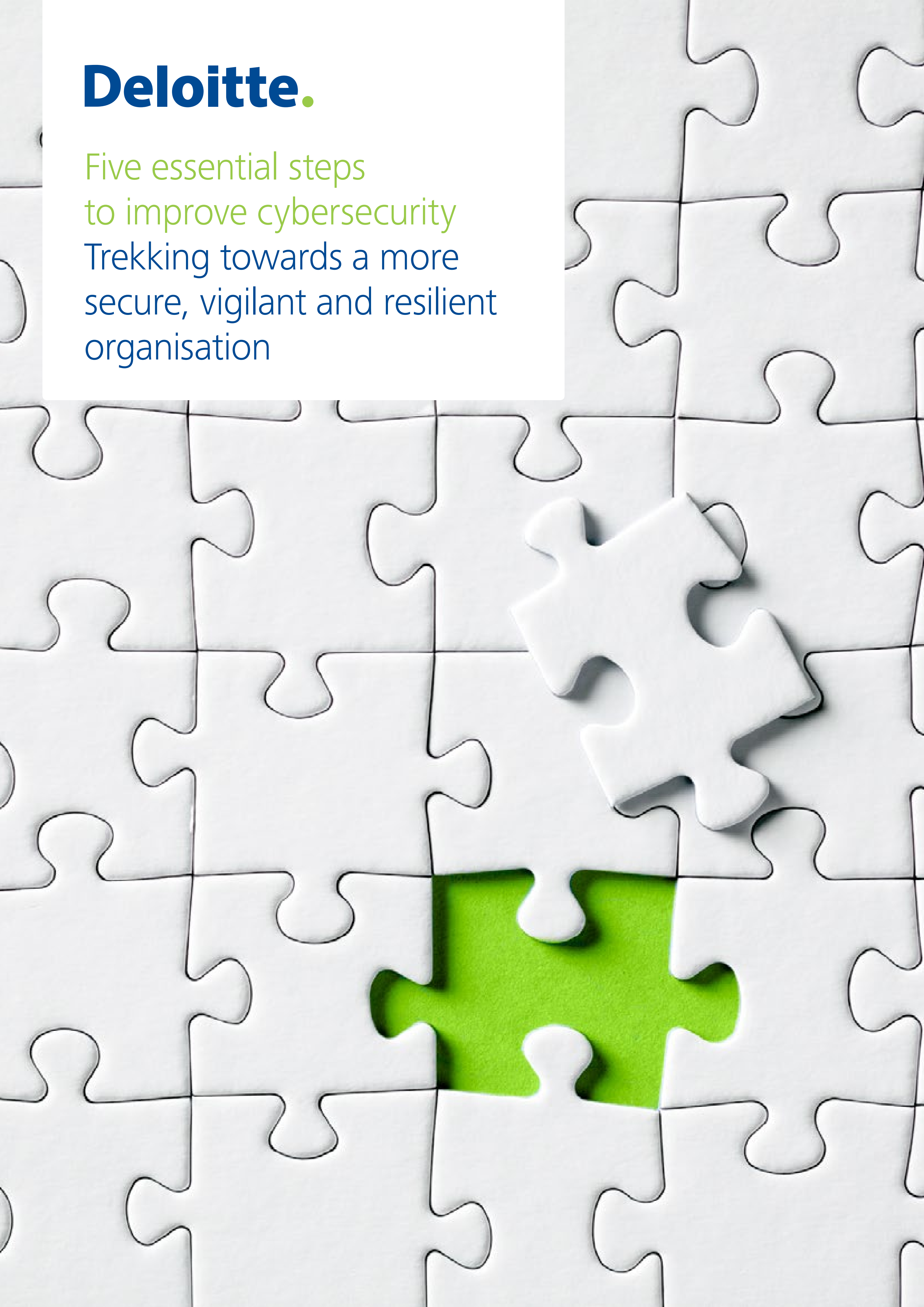
Five essential steps to improve cybersecurity

Trekking towards a more secure, vigilant and resilient organisation



New Zealand organisations continue to experience cyber threats that hold the potential to disrupt business operations and service to customers. A vast majority of those threats can go undetected, or they are detected too late for an organisation to avoid exposure and the associated risk.

To address the threats, preparation is paramount, but many New Zealand organisations have struggled to know how to take essential steps to prepare their operations for the evolving cybersecurity landscape.

In developing a cybersecurity strategy, it's not enough to prepare for the threats you believe you know. You should also endeavor to prepare for unknown threats.

Understanding the risk

When it comes to addressing cybersecurity, the ramifications extend to the entirety of your organisation — from the smallest processes to your organisation's overall ability to function effectively. An attack that results in the leak of proprietary data can destroy your competitive edge. An attack that steals private customer data can result in lost public trust and lost revenue. An attack that paralyses even seemingly innocuous information systems can destroy your ability to operate and communicate effectively.

And these days, organisations can get attacked on more fronts than ever before. Each application of cloud-based technology or mobile technology presents a new opening through which attackers may seek to gain access to your organisation's valuable information. Tools for social media also present windows through which hackers may attempt to gain insights into your organisation and the type of information and systems you possess — insights they can leverage to launch an attack.

Beginning the journey

Defending your organisation against a sophisticated adversary involves a multifaceted approach that ranges from executive/board member awareness to the implementation of a viable but pragmatic cybersecurity framework.

Cybersecurity involves more than understanding the capabilities and exposure of existing and emerging information technologies. It involves understanding that you are in an arms race with hackers. It involves understanding business needs, business processes, and the players involved in your business operations. It involves understanding where your greatest assets and your biggest risks are so you can focus and manage your investments to address relevant cyber threats. Improving cybersecurity is not a one-time solution. It's a journey for business decision makers and IT leaders alike. And like any journey, it starts with a single step, followed by a few more steps.

Figuring out which steps to take and which direction to move in can sometimes prove a challenging decision for organisations. But there are essential steps that all organisations must take to improve their cybersecurity.

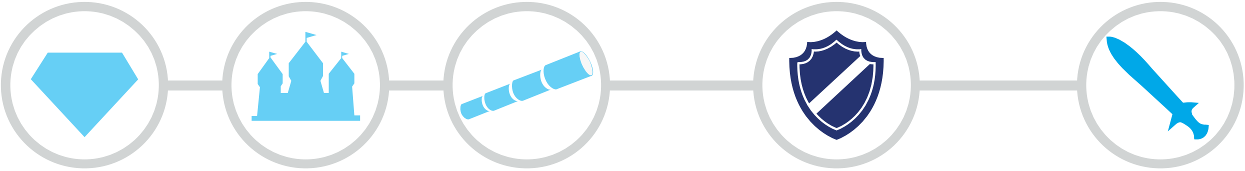
The five steps

Experiencing a cyber-attack is not a matter of *if* for your organisation. It’s a matter of *when.* And the time to prepare is *now*.

The following five steps can help you create an organisation that operates securely, that remains vigilant in the face of cyber threats, and that can show resiliency when attacked. The approach emphasises pragmatic solutions — solutions that are industry specific and that deploy the right people, processes and tools to address known and emerging cyber threats.

Businesses that take these five critical steps can transform themselves to become more secure, vigilant and resilient.

Vigilant



Know your crown jewels and understand friends’ roles

Understand critical assets and interactions.

Proactively assess your cyber risk

Know what to look for and how to detect threats — whether conventional or emerging.

Make awareness a priority

Help employees and partners understand the roles they play.

Secure

Fortify your organisation

Have a plan to patch holes, manage patches, develop software securely, and address physical security.

Resilient

Prepare for the inevitable

Focus on incident management and simulation to “test your gates” and your response.

1 Know your crown jewels and understand friends’ roles

Cyber hackers continue to show an abundance of motivation. They need to be successful only once to see a payoff for their efforts. But your organisation must be successful in managing an attack each and every time. Your success depends largely on knowing the value of your information assets and knowing the risks to those assets. Know your “crown jewels” and understand your friends’ role in protecting them.

Crown jewels

As the level of sophistication in hacker goals and hacker tools continues to rise, your organisation might continue to face the traditional budget pressures. You have no blank check to spend on security. You have to think strategically. You have to know and protect your information crown jewels. What is worth protecting? What investments can you make to protect those information assets?

Fending off an attack begins with knowing what you need to protect, not just what you want to protect. You need to understand what your crown jewels are and where they are located. Many hackers are looking aggressively for your crown jewels — your critical assets and sensitive data.

Identifying your crown jewels will help you prioritise security investments and the security requirements for third parties that might host your data off premises. As you begin to discover and identify your crown jewels — and as you begin to determine what investments you can make to protect them — resist the urge to prioritise them based solely on standard business continuity plans.

You might be overlooking the value of some of your information assets. For example, what you consider routine administrative systems can matter a great deal during a cyber-attack. If an e-mail server or authentication server gets hacked, your organisation could be out of commission for longer than you can imagine and possibly out of commission for good.

Remember that your crown jewels can reside virtually anywhere as your workers and partners turn to mobile and cloud-based technologies to access and share information to do business. As you seek to identify your crown jewels, think outside the walls of your organisation.

Key points

- The level of sophistication in hacker goals and hacker tools continues to rise.
- Determining your crown jewels and the investments required to protect them will vary from industry to industry.
- Don’t prioritise your crown jewels based solely on business-continuity plans. Consider risk.
- Remember that your crown jewels can reside virtually anywhere — in the cloud, on mobile devices or with partners.

Friends

Thinking outside the walls of your organisation means thinking primarily about contractors, vendors, and suppliers whether they're cloud providers, outsourcing partners, or other business allies.

Whether you are a business leader or IT manager within your organisation, you need to know who your organisation is sharing information with and where your crown jewels reside because the hackers do know. Attack patterns show that they're increasingly targeting third parties to get to their true target organisation.

Addressing the threat means taking a risk-based approach to security. You'll need to know your risk exposure — which friends host or have access to your critical information and systems, and how vulnerable they are to cyber-attacks.

Don't rely too heavily on a vendor questionnaire to determine how at risk a partner is. That's not enough. Ask your partners and potential partners for security audit reports — and consider conducting site visits, based on criticality of assets being accessed or hosted by the third party.

Know also that your third party business partners' technology and information-sharing patterns might change. Don't rely on initial security/risk assessments. Keep checking in with them. They might be turning increasingly to new technologies such as cloud computing and mobile applications without thinking about how that could affect risk or policies for your organisation. Partners won't necessarily assess what the loss of your data will mean for them, so it's up to your organisation to do that. You need to make sure your partners are keeping your data as secure as possible because if your third party partner is hacked, the party you're now dealing with can serve as the jump point for a hacker.

Key points

- Know who your organisation is sharing information with.
- Know which friends have access to your critical information and systems.
- Don't rely heavily on questionnaires. Ask your partners and potential partners for security audit reports.
- Keep checking in with partners to understand how their IT and service landscape is changing.

2 Proactively assess your cyber risk

To address cyber threats effectively, organisations should have a cyber threat intelligence (CTI) capability that will help them rapidly identify, detect, and respond to threats.

Cyber threat intelligence involves using technology, processes, and people to proactively acquire, analyse, and disseminate intelligence internally and externally as a way to improve security. The CTI approach emphasises situational awareness and tactical/strategic responses that can help reduce the likelihood of harm or risk for your organisation.

A CTI approach depends on an organisation's ability to synthesise external and internal intelligence in a timely manner to develop a constant "situational awareness" that will become part of the organisation's overall security posture. CTI is critical to maintaining the confidentiality, integrity and availability of information assets.

In addition to a host of technology products and services that can help an organisation develop its CTI capabilities, human interaction also comes into play. Participating in industry groups can help your organisation become aware of security trends and tactics at peer organisations and also offer you an avenue for sharing your own experiences with your neighbours to help create a common picture and a heightened awareness on cybersecurity issues.

Internal intelligence

Don't forget to dive deeper within your own data to uncover useful intelligence. Maintaining a trail of data access activity — a trail that you can follow and investigate — can help improve your overall security posture. Actively monitoring and analysing your data trails is essential. Do you really know what's happening in your organisation? Do you know what's happening with your data as it flows through mobile and cloud applications and as your partners handle it?

Many organisations keep activity logs merely for compliance purposes. But logs can offer powerful clues for detecting not-so-obvious threats to your business. Logs can help you identify patterns or incidents that suggest a more subtle intrusion or a potential data hole that needs to be plugged. Don't just review your log data and related data. Use it for insight. Doing so can help you detect a threat in a timely fashion. You might require new tools to develop an advanced detection capability.

More mature organisations are increasingly putting in place comprehensive security analytics solutions to effectively manage large volumes of security data and hunt for suspicious patterns to find that threatening needle in the haystack.

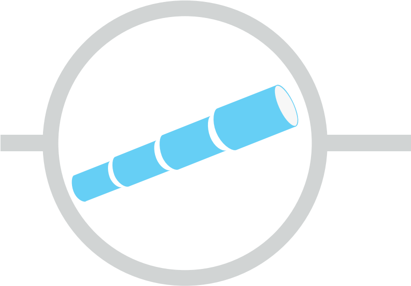
External intelligence

Get smart about where cyber-attacks are happening within your industry and what they look like. Seek new sources of information. Then share that knowledge within your industry, with partners and especially with other organisations with which you exchange data for business purposes.

Key points

- Work towards a comprehensive plan for cyber threat intelligence.
- Be proactive. Seek new sources of information and new ways to interact with peers to identify trends and tactics.
- Monitor your data access trails and data logs to gain insight and detect threats early.
- Review log data to gain insight into potentially suspicious patterns or activities.

3 Make awareness a priority



Improving security relies heavily on awareness — an awareness of threats, risks, challenges and solutions within every department inside your organisation and within every partner organisation.

Security awareness should be more than a compliance exercise. Your aim should be to change your organisation's security culture and the behaviour of employees. Building awareness is about building a culture.

The more people you have thinking about cybersecurity, the more vigilant your organisation. To do that, continue to encourage workers beyond the IT staff to think about cybersecurity — to ponder not only the technical challenges but the business and process challenges too. Each set of participants needs to know what the organisation expects of them, what's at risk, and what they need to be doing.

It's also important to make workers in your organisation aware that cyber threats are not just an IT problem. They're a people problem — a business problem — and internal and external system users ultimately are accountable for overall security. Communicating that point might pose a challenge, especially if employees view new security measures as a hindrance or an inconvenience. So organisation leaders should develop training/awareness programs and make a sincere effort to explain security challenges and rules in language that users can understand.

Moreover, they should build confidence that the various components of leadership — IT leadership or other business leadership areas — are aware of the cybersecurity activities and messages for which they're responsible. Leadership must set a "tone at the top" when it comes to security awareness.

Workers also need to be made aware of specific threats and their potential consequences. For example, workers should be on guard for "spear-phishing" campaigns, in which a hacker leverages personal or customised information to target an individual user (via an e-mail message with bogus corporate links, for example) and then ultimately infiltrates or infects the larger organisation.

For example, a fake "internal revenue report" e-mail attachment sent to members of a sales team can harbor malware that could infect an organisation's network. Thinking about awareness in a more interactive, ongoing manner can help organisations engage workers and partners. It can make the threats seem more imminent and make each employee's role seem more vital for securing the organisation.

Key points

- Make sure employees and partners know that security measures are instrumental for your entire organisation.
- Explain security challenges and rules in language that users can understand.
- Think about awareness in a more interactive, on-going manner to engage workers and partners and to make threats seem more concrete.

4 Fortify your organisation

Even though you know what your organisation's critical assets are, that doesn't make you secure. While the news is filled with accounts of cyber-attacks that target *unknown* system weaknesses, most attacks exploit *well-known* system weaknesses.

The issue is straightforward: known vulnerabilities — vulnerabilities that are known to hackers and known to the organisations they target. The ultimate solution also can be straightforward: a targeted patch-management programme that focuses on crown jewels and critical assets.

Organisations should seek to move from a compliance based approach to a risk-based approach. They should resist the urge to follow the easy route of performing ad-hoc patching and leaning too heavily on "Super Tuesday patching," in which they rely on a regular weekly patching update from a single major software vendor and just assume they've done a good job of patching their holes. When it comes to attacks, hackers are expanding their scope. Organisations should expand their scope too.

Fix known weaknesses

Solving the "known vulnerability" problem involves simple due diligence. This due diligence will take time and can be tedious. And it should be undertaken using a risk-based approach, with IT departments working in co-ordination with other internal decision makers to help determine priorities based on your organisation's "crown jewels," your constraints, and your existing controls. Work to understand what's possible given your organisation's manpower and technical know-how. Value your risk in a real terms to the business — in the form of customer impacts, service disruption and the loss of sensitive data.

Security by design

Software development also can pose a security risk. Security procedures often can be perceived as a hindrance or a factor that can delay the timely development of new systems. But development activities are ripe with opportunities to overlook security needs or to create new security holes. Organisations should strive to add security protocols and a security mindset to the development process.

Physical security still counts

It's not enough to address the software side of security. You must also spot physical security holes and weaknesses that could allow an unauthorised individual, a disgruntled worker, or an unwitting employee to leak or steal critical information. Addressing potential weaknesses in physical security and access rights can sometimes prove more challenging. Defining roles, responsibilities and procedures for accessing data and for accessing physical areas within your organisation can help move your organisation in a more secure direction.

Key points

- Patch holes, focusing on critical holes as well as holes that might not seem critical but that are known.
- Resist the urge to lean too heavily on regular patches from a single major software provider.
- Work to spot physical security holes and weaknesses in data-access procedures.

5 Prepare for the inevitable

Most organisations have a security incident management process in place. But few have tested it. When, not *if* your organisation is attacked, how will you respond? How will the operational side of your organisation — and the communication arm of your organisation — react? How will the IT department react? How will they work together to understand the problem, remediate the problem, and let partners and customers know what's going on? How will you contain the damage you may experience?

To prepare for the inevitable attack, your organisation should be asking the following questions now:

- Who should be contacted during and after an incident?
- Which groups and individuals should be engaged?
- Which third parties will you need to notify or engage?
- Which customers or external users will you need to alert? What will you tell them? How will you tell them?
- What about regulators and the role of privacy and legal groups in your organisation? How will you engage them?
- Ultimately, how quickly can you contain a security breach and restore your organisation to normal or better operation?

Having answers to the key questions and many more organisation specific questions can help you bounce back quickly after an attack. But answering the questions is just part of the equation. Testing your answers is critical.

To do that, many organisations are carrying out cyber simulations to test their true cybersecurity preparedness and to determine the usefulness of existing crisis management and security incident management processes. Cyber simulations are interactive techniques that immerse participants in a simulated attack scenario to help organisations evaluate their response and preparedness. It gives organisations a much needed and valuable reality check to improve your resilience.

Traditional cyber threat preparedness assessments focus on evaluating technology controls and incident-response plans, where as cyber simulations involve not only technology, but also the people involved in responding to incidents. Organisations should include not only their IT staff, but also their operational staff and senior business leadership and boards when simulating cybersecurity incidents.

Key points

- Know how departments will work together during a cyber-attack.
- Know how you will engage regulators as well as observers, such as privacy groups.
- Know how you will engage partners and customers.
- Simulate incident management, bringing in leadership, the board, operations and IT to test your preparedness.

Staying on your toes

Becoming a secure, vigilant, and resilient organisation doesn't happen quickly. But it's something that has to happen if your organisation intends to survive, and even better, thrive amid the emerging technology landscape and the evolving terrain of cyber threats. Becoming a secure, vigilant and resilient organisation requires not only these five important steps; it requires constant assessment of how well you are carrying out those steps — constant assessment of whether you're taking the steps effectively, and whether those steps are taking you where you want to go.

Despite the challenges, improving cybersecurity doesn't have to be a grueling journey. Deloitte can help. We know cybersecurity. We have deep experience addressing issues in a variety of industries, from financial services and retail to the public sector and energy/resources. We're up to date on the challenges that face organisations as they embrace cloud, mobile, social and analytics technologies. From stategy to implementation, we stand ready to assist you with the steps you need to take to get on your way.

For more information, please contact our Cyber, Privacy and Resilience leaders:

Wellington

Anu Nayar
Partner – National Leader
(021) 207 9573
anayar@deloitte.co.nz

Joanne Lu
Associate Director
(04) 470 3651
joannelu@deloitte.co.nz

Auckland

Faris Azimullah
Partner
(09) 303 0842
fazimullah@deloitte.co.nz

Kevin Kanji
Associate Director
(09) 306 4424
kkanji@deloitte.co.nz

Raj Pradhan
Associate Director
(09) 303 0938
rpradhan@deloitte.co.nz

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte network") is, by means of this communication, rendering professional advice or services. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

Auckland
Deloitte Centre
80 Queen Street, Auckland 1010
Private Bag 115033
Shortland Street, Auckland 1140
New Zealand
Tel: +64 (0) 9 303 0700
Fax: +64 (0) 9 303 0701

Hamilton
Deloitte House
24 Bridge Street, Hamilton East
Hamilton, 3216
PO Box 17, Hamilton, 3240
New Zealand
Tel +64 (0) 7 838 4800
Fax +64 (0) 7 838 4810

Rotorua
Level 2, Pukeroa Oruawhata House
2/1176 Amohau Street,
Rotorua 3010
PO Box 12003, Rotorua 3045
New Zealand
Tel +64 (0) 7 343 1050
Fax +64 (0) 7 343 1051

Wellington
Deloitte House
10 Brandon Street
Wellington, 6011
PO Box 1990, Wellington, 6140
New Zealand
Tel +64 (0) 4 470 3500
Fax +64 (0) 4 470 3501

Christchurch
Level 4, 151 Cambridge Terrace
Christchurch 8013
PO Box 248
Christchurch, 8140
New Zealand
Tel +64 (0) 3 363 3800
Fax +64 (0) 3 363 3801

Dunedin
Otago House
481 Moray Place
Dunedin, 9016
PO Box 1245, Dunedin, 9054
New Zealand
Tel +64 (0) 3 474 8630
Fax +64 (0) 3 474 8650