Incident Response
FORENSIC & CYBER

INCIDENT RESPONSE SOLUTIONS

Cyber Security Guide for NZ Law Firms

2020 Edition

https://incidentresponse.co.nz/cyber-security-for-law-firms

Welcome to the Cyber Security Guide for NZ Law Firms

The storage of sensitive client information and management of large funds make law firms an attractive target for cybercriminals. It is therefore critical for law firms to understand and mitigate the cyber risks they face.

The *'Cyber Security Guide for NZ Law Firms'* is a contextual resource to assist lawyers and law firms manage their cyber security risk.

With recent advances in cloud and legal technologies, law firms are transforming their information systems. While these new technologies present business opportunities, they also create new risks.

Law firms store large quantities of sensitive client information and process significant financial transactions on behalf of their clients. To quote the New Zealand Law Society, *"the storage of personal and sensitive information on clients is an integral part of the work of a lawyer".*

A cyber attack or data breach has the potential to cause major disruption, reputational damage and financial loss. According to research, the most common types of attacks on law firms include business email or supply chain compromises, data breaches and the ever-present threat of ransomware.

In the event of a breach, a law firm is obliged to comply with several Acts including the Privacy Act 1993 and the Lawyers and Conveyancers Act 2008.

Cyber risk should be managed using a recognised cyber security framework. Such frameworks involve a risk assessment, the selection of applicable security controls and an achievable roadmap of improvement. Legal professionals should also undergo cyber security training and awareness programmes to ensure they have more than a basic understanding of cyber risks.

Having worked on numerous cyber-related matters for New Zealand law firms, we are pleased to present you with this guide and accompanying collection of practical cyber security resources.

I trust that you and your firm will benefit from the guide and we would be happy to discuss any relevant aspects with you.

CBMckenzie

Campbell McKenzie

Incident Response Solutions

At a Glance

- More than a quarter of law firms experienced a data breach.
  The American Bar Association's 2019 Legal Technology Survey Report

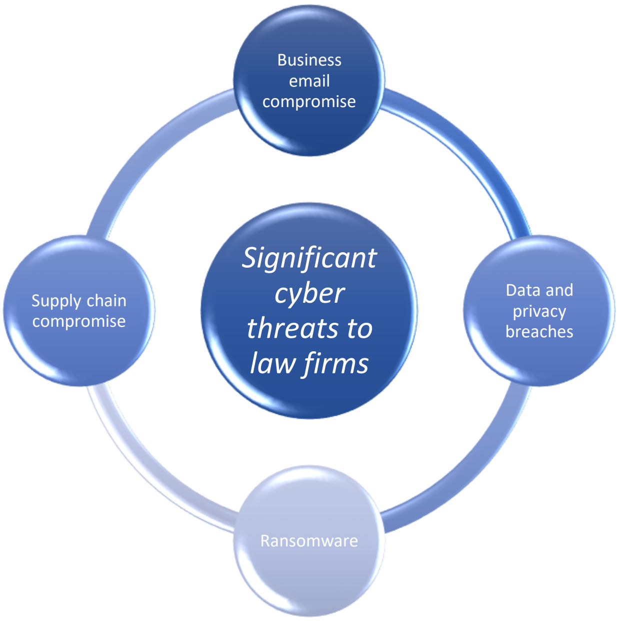
- Every respondent suffered a security incident, with the most common attack being phishing.
  2019 Survey of Global Law Firms

- The most significant cyber threats to a law firm are phishing, data breaches, ransomware and supply chain compromise.
  The UK's National Cyber Security Centre 2018 Report

- In quarter three 2019, there were 1,354 incident reports with phishing and credential harvesting activity 27% higher than in the previous quarter.
  CERT NZ's Third Quarter 2019 Report

- Companies with an incident response team that also extensively tested their incident response plan incurred significantly less costs on average compared to those that had neither measure in place.
  Cost of a Data Breach Report 2019

- Total or partial outsourcing of services and the use of automation and robotics to assist with repeatable activities using third-party services are both increasing.
  The Cyber Threat to UK Legal Sector 2018


Business email compromise
Significant cyber threats to law firms
Supply chain compromise
Data and privacy breaches
Ransomware

Cyber Tip #1: Cloud Computing

When sharing documents on a cloud platform, ensure that the correct permissions are set.

Legal Technology

Legal technology (commonly known as Legal Tech), refers to the use of technology and software to provide legal services. A vast number of vendors offer solutions, many of which are hosted in the 'Cloud'.

Cloud computing enables convenient, on-demand access to a shared pool of computing resources that can be rapidly provisioned with minimal management effort or service provider interaction[1].

In 2017, the New Zealand Law Society issued a Practice Brief titled "Cloud Computing"[2]. In summary, the Law Society reported that law firms are increasingly using cloud computing as an alternative to in-house systems. It stated that advantages such as flexibility and cost must be balanced against risks to privacy and control. It goes on to recommend that if the outsourcing arrangement could result in a third party accessing clients' data, then contractual terms should be sought to ensure that:

- clients' information is protected, and the cloud service will not compromise client confidentiality.
- the law firm makes all reasonable efforts to ensure attackers cannot access this client data.

According to the 2018 report 'The cyber threat to UK legal sector[3]', a number of emerging trends are influencing the use of technology within law firms. These include:

- A continuing need to connect and collaborate with clients, placing requirements on technical capabilities
- Flexibility of the workforce requiring remote access to data
- An expansion of outsourcing services, using automation and robotics to assist with repeatable activities.

Another recent survey report 'Will 2020 be the turning point in legal operations?[4]' focuses on eDiscovery solutions. The authors found that data security is a top concern amongst law firms, with 94% concerned about distributing electronically-stored information to multiple discovery vendors and law firms.

Consider the types of data that your law firm stores which cybercriminals may target, such as:

- Contract management
- Conveyancing
- Deals data
- eDiscovery data
- Intellectual property
- Legal research
- Personally identifiable information (PII)

Cyber Tip #2: Websites

Beware of suspicious websites sent to you by email. Familiarise yourself with the following training resource from the New Zealand Domain Name Commission: https://fakewebshop.nz

A complete set of references is listed on the following webpage

https://incidentresponse.co.nz/cyber-security-guide-for-nz-law-firms

[1] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[2] https://www.lawsociety.org.nz/practice-resources/practice-briefings/Cloud-Computing.pdf

[3] https://www.ncsc.gov.uk/report/-the-cyber-threat-to-uk-legal-sector--2018-report

[4] https://www.opentext.com/info/ediscovery/corporate-legal-ops-survey

Cyber Security in the NZ Legal Context

This guide considers the cyber security implications of the Privacy Act 1993 (The Privacy Act) and The Lawyers and Conveyancers Act (Lawyers: Conduct and Client Care) Rules 2008 (Rules of Conduct and Client Care).

This guide does not attempt to, nor should it be used to determine whether the Privacy Act or the Rules of Conduct and Client Care prevail. If in doubt, seek formal advice.

In 2014, the New Zealand Law Society issued a Practice Brief titled "Protecting Clients' Personal Information"[5]. A summary follows, we recommend that the brief also be read in full.

The Privacy Act

Any law firm or lawyer in sole practice has obligations as an agency under the Privacy Act, including the mandatory designation of a privacy officer.

Principle 5 of the Privacy Act requires that an agency holding personal information shall ensure that the information is reasonably protected by security safeguards against loss and misuse. If it is necessary to give the information to a person in connection with the provision of a service, then all reasonable steps must be taken to prevent unauthorised use or unauthorised disclosure of the information.

A cyber incident response plan will assist in dealing with a privacy breach and should include a determination of what constitutes a 'serious' privacy breach requiring notification of the Office of the Privacy Commissioner. For further guidance, visit the website[6] and the 'Data Safety Toolkit'[7].

Rules of Conduct and Client Care

Under the Rules of Conduct and Client Care, lawyers are required to protect and hold in strict confidence all information concerning a client acquired in the course of the professional relationship. In the event of a privacy breach, a lawyer may also have the obligation to ensure clients are fully informed of any potential compromise of privacy and confidentiality.

A summary of the key chapters relating to cyber security follows.

Chapter 7 (Disclosure and communication of information to clients)

Subject to limited exceptions, a lawyer must promptly disclose to a client all information that he/she already has or acquires that is relevant to the matter in respect of which he/she is engaged by the client.

Chapter 8 (Confidential information)

A lawyer has a duty to protect and to hold in strict confidence all information concerning a client, the retainer, and the client's business and affairs which he/she acquires in the course of the professional relationship. The obligation of confidentiality continues indefinitely after the person has ceased to be the lawyer's client.

Chapter 11 (Proper professional practice)

A lawyer must take all reasonable steps to prevent any person perpetrating a crime or fraud through the lawyer's practice. This includes taking reasonable steps to ensure the security of and access to electronic systems and passwords.

Cyber Tip #3: Social Media

Be careful about what you share, particularly sensitive information. The more you post the easier it is to have your identity stolen.

[5] https://www.lawsociety.org.nz/practice-resources/practice-briefings/Protecting-clients-personal-information-2014-06-19-v1.pdf

[6] https://privacy.org.nz/privacy-for-agencies/data-breaches

[7] https://privacy.org.nz/assets/Files/Data-Safety-Toolkit/Data-Safety-Toolkit-May-2014.pdf

A Global Perspective

For a wider view on law firm cyber security, we have drawn on a number of recently published legal reports from around the globe.

2017 Key Roundtable Takeaways - Cyber Security and Legal Practice[8] *(Australia)*

- Cyber security threats are increasing
- Cyber security in the nation's legal firms is inadequate and most professionals with responsibility for cyber defence are aware of the vulnerabilities
- The fight against cyber threats is hampered by a lack of resources, especially in smaller law firms without dedicated internal IT capabilities
- Employees are the weakest link
- Investment in awareness and training of cyber security issues is increasing.

2019 Cyber Security Report - American Bar Association (ABA)[9] *(United States)*

- Over a quarter of firms report that they have experienced some sort of security breach
- Consequences of security incidents:
  - consulting fees for repair (37%)
  - downtime/loss of billable hours (35%)
  - expense of replacing hardware or software (20%)
  - destruction or loss of files (15%)
  - notification of law enforcement and clients of the breach (9% each)
- More than a third report they were aware that their systems had been infected with malware
- Less than a third of law firms have an incident response plan.

PwC Law Firms' Survey 2019[10] *(Global)*

- Every respondent suffered a security incident
- Common attack types included phishing, malware, network intrusion, denial of service and confidential information loss or leakage
- Network intrusion was the least commonly known cyber security attack and this, perhaps, implies poor detection capabilities across the legal sector
- The insider threat is prevalent in all sizes of firms, with the majority having experienced incidents due to insiders over the last year
- Participation in annual crisis management exercises is low.

Cyber Tip #4: Emails

When receiving emails, be careful with links and attachments. Ask yourself:

- ***Do I know this person and is this their usual email address?***
- ***Does this email subject look unusual?***
- ***Is there an attached document?***
- ***Does the email ask me to visit a website, send personal information or reply immediately?***

[8] https://www.cli.collaw.com/-/media/col/cli_files/cybersecurity-and-legal-practice-rt-2017---key-takeaways.pdf?la=en

[9] https://www.americanbar.org/groups/law_practice/publications/techreport/abatechreport2019/cybersecurity2019

[10] https://www.pwc.co.uk/industries/law-firms/pwc-law-firms-survey-report-2019.pdf

Cybercrime - The Threats We Know

A cybercriminal may attempt to compromise your law firm using any number of attack types. Based on our experience of responding to actual incidents in New Zealand, we consider that the first four are the most prevalent attack types that would carry the largest potential impact for a law firm.

In this section, we first describe each threat and then provide some recommendations (in blue).

1. Business Email Compromise

Email compromises have become so common that the New Zealand Law Society have a dedicated Practice Resource on their website[11].

A business email compromise is typically launched via a phishing attack by changing (or 'spoofing') an email address to make email messages appear convincing. A phishing email contains a link to a fake website encouraging the victim to enter their login credentials (to their email account). The cybercriminals scan the emails for payment instructions and then send an email requesting that the victim make the payment to a different bank account. In some cases, cybercriminals may forge the bank account details on the invoice to circumvent traditional fraud controls. To hide their tracks, cybercriminals set up auto-forwarding and deletion rules in the compromised email account.

- *Use stronger passwords and enable two-factor authentication (2FA or MFA)*
- *Conduct cyber security user awareness training*
- *Implement processes to verify invoices and account details for money transfers*
- *Use 'cooling off' periods for changing account details for high-value transactions*
- *Educate your clients about your firm's finance processes to help them avoid falling victim to email fraud.*

The following events occurred in a New Zealand law firm recently during a property settlement.

- *The lawyer emails the client requesting deposit of several hundred thousand dollars in the firm's trust account. The client was expecting the email.*
- *The client's IT system has been hacked. The hackers intercept the email and draw up a new trust account deposit slip and create an email address very similar to the lawyer's (replacing one letter with a numeral). They forward the email to the client.*
- *The client is confused by the numbers on the deposit slip. She decides to test it by sending a small amount, and then emails the hackers' fabricated email address requesting confirmation that the funds have been received.*
- *The hackers respond in the name of the lawyer, saying he has received the test amount.*
- *The client transfers the remainder of the money into the fraudulent account.*
- *Two days later, on the day before settlement, the lawyer notices that the funds have not arrived. He rings the client, who tells him of the confirmation email – which the lawyer knows he has not sent.*
- *Realising that hackers are at work, the lawyer asks the client to send him all the emails (to a trusted email address). The lawyer detects the fake email address and deposit slip and immediately advises the client to contact her bank.*
- *Shortly afterwards the lawyer receives an email from the 'client', saying she had tried transferring funds but that there has been a problem, and could the firm cover for her over the weekend. It is clear this is not the client – in the language used and, of course, in the knowledge that she has been hacked - but it shows the hackers are still tracking the client.*
- *The bank confirms that the money is still in the country. The funds are later recovered.*

Source – NZ Law Society[12]

Cyber Tip #5: Invoice hijacking

Warn your clients never to send funds to a new account without speaking to your firm first; remind clients to check the addresses of any emails purportedly sent by your firm, particularly if they relate to payment of funds.

[11] https://www.lawsociety.org.nz/practice-resources/email-scam-information

[12] http://www.lawsociety.org.nz/practice-resources/email-scam-information/how-fraudsters-interfere-in-money-transfers

2. Data or Privacy Breach

Lawyers who breach their clients' privacy may have breached their professional obligations under the Lawyers and Conveyancers Act 2006. A breach can also have a devastating impact on a firm's reputation.

In 2016, Panama-based law firm Mossack Fonseca suffered a major data breach (the Panama Papers). It is estimated that over two Terabytes (TB) of data were compromised. This is roughly equivalent to the amount of information contained in an average library. According to Action Fraud, in the two years to March 2018, eighteen law firms reported hacking attempts[13]. Data and privacy breaches can also be caused by an accidental act by an employee.

- *Conduct a security audit of both physical and technical security, including the NIST cyber security framework phases of identify, protect and detect*
- *Review supply chain providers*
- *Ensure your cyber incident response plan is operational and understood by all relevant staff.*

3. Ransomware

Ransomware is a type of malicious software (or Malware) that locks files, preventing victims from accessing electronic data until a ransom has been paid[14].

High-profile incidents such as WannaCry and NotPetya[15] both in 2017, highlight the nature and severity of such attacks. Global law firms are known to have been impacted by such attacks.

- *Regularly back up your data and test the restore process*
- *Ensure systems are regularly patched*
- *Implement an anti-malware solution that includes ransomware mitigation.*

4. Supply Chain Compromise

The cyber risk profile of law firms will continue to increase as they adopt more legal tech and cloud services. The supply chain can be compromised in various ways. For example, the NotPetya ransomware attack is understood to have been spread by infecting the cloud providers' system used to deploy software updates to its clients, otherwise known as a watering-hole attack.

Managed service providers (MSPs) delivering technology services to clients are an attractive target as they host data for multiple organisations. If a system is not properly secured, once entry is gained, an attacker can traverse it in search of valuable information. According to a US Justice Department indictment in 2018, a hacking group targeted managed service providers to steal intellectual property (Advanced Persistent Threat 10, or 'APT10'[16]).

- *Maintain a register of suppliers with access to sensitive information*
- *Separate or protect critical devices from networks that are accessed by third parties*
- *Ensure your suppliers, and their suppliers, adhere to the same or better security protocols as your firm.*

Cyber Tip #6: Working Remotely

Avoid transferring confidential information over public Wi-Fi networks as this can easily be compromised. Use a Virtual Private Network (VPN) wherever possible and ensure that your remote software is up to date.

[13] https://www.ncsc.gov.uk/report/-the-cyber-threat-to-uk-legal-sector--2018-report

[14] https://incidentresponse.co.nz/protecting-against-ransomware

[15] https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world

[16] https://www.wired.com/story/doj-indictment-chinese-hackers-apt10

5. *Cryptojacking*

Cryptojacking involves stealing victims' physical or cloud computing services to use their processing power and electricity supply to 'mine' crypto currencies such as Bitcoin and Monero.

- *Set payment thresholds and regularly review invoices from cloud providers.*

6. *Malicious Insider Attacks*

A disgruntled employee, who has physical and electronic access to your information systems, can cause significant damage such as stealing intellectual property or destroying data.

- *Restrict what data employees' can either copy or delete.*

7. *Remote Desktop Protocol (RDP)*

RDP is designed to provide access to a computer system for support purposes. Cybercriminals take advantage of vulnerabilities in this software to copy data and launch ransomware attacks.

- *Ensure that your RDP software is regularly updated to minimise this risk.*

8. *Social Engineering*

Social engineering involves human interaction that relies on trust to trick people. Phishing and whaling are common formats; the latter involves an email being sent purportedly from the CEO to the CFO requesting urgent payment of funds.

- *Insurance companies now offer optional policy extensions to cover this threat*
- *Provide staff with suitable cyber security awareness and training.*

9. *Social Media*

The more you post online, the easier it is to have your identity stolen. According to the NZ Law Society[17], lawyers also need to be aware of the potential consequences of their use of both personal and professional social media accounts. Such content has the potential to reach unintended audiences, including the Lawyers Complaints Service.

- *Be careful about what you share on social media, particularly sensitive information.*

10. *Website Hacking*

Websites are hacked to obtain login credentials and personally identifiable information, which can later be used to commit further crimes, or sell the compromised information on the dark web. The dark web is an area of the internet which is frequented by cybercriminals.

- *Dark web monitoring of your information may identify cyber risks*
- *In the event of a cyber attack, ensure all affected login credentials are changed.*

Cyber Tip #7: The Crimes Act

Under the Crimes Act, it is illegal to:

- ***Access a computer system for dishonest purposes***
- ***Damage or interfere with a computer system***
- ***Make, sell, distribute or possess software for committing crime***
- ***Access a computer system without authorisation***

[17] https://www.lawsociety.org.nz/practice-resources/the-business-of-law/legal-practice/lawyers-and-social-media

Cyber Risk Management

Since a law firm's information systems are an attractive target, cybercriminals will go to great lengths to compromise them. All legal professionals must therefore understand and actively participate in managing their firms' cyber risk. Ultimately however, it is senior management who should take ownership of this risk and monitor it at the firm's partnership meetings. A senior member of staff should be appointed to oversee data privacy and cyber security, who will ask and act on the following questions relating to cyber attacks:

- Does the board understand its exposure?
- What are the vulnerabilities of the organisation?
- What are the likely business impacts?
- What is the planned response?
- How often does the organisation undergo testing of its preparedness?

One of the first steps in a cyber risk programme is to decide on and then use a suitable framework, comprising a risk assessment and selection of relevant security controls.

Cyber Security Framework

The New Zealand Government encourages the use of the National Institute of Standards and Technology (NIST) cyber security framework which was first published in 2014[18]. The framework enables firms to assess maturity across five functions: identify, protect, detect, respond and recover. Law firms can use the NIST cyber security framework to:

- Describe their current cyber security posture;
- Describe their target profile for cyber security;
- Identify and prioritise opportunities for improvement within the context of a continuous and repeatable process;
- Assess progress towards the target profile; and
- Communicate the cyber security risk to internal and external stakeholders.

Privacy Framework

In 2020, NIST also released a Privacy Framework[19], which has an overarching structure modelled on that of the cyber security framework. The two frameworks are designed to be complementary, given that privacy and security are related, but distinct concepts. Law firms can use the NIST privacy framework to:

- Take privacy into account as they design and deploy systems, products, and services that affect individuals;
- Communicate about their privacy practices; and
- Encourage cross-organisational workforce collaboration through the development of profiles, the selection of tiers and the achievement of outcomes.

We also recommend referring to The Institute of Directors 'Cyber Risk Practice Guide[20]'.

Cyber Tip #8: Password and Access Management

Use a password management system that is robustly protected with a secure and strong password. Add extra protection by applying multi-factor authentication (MFA or 2FA).

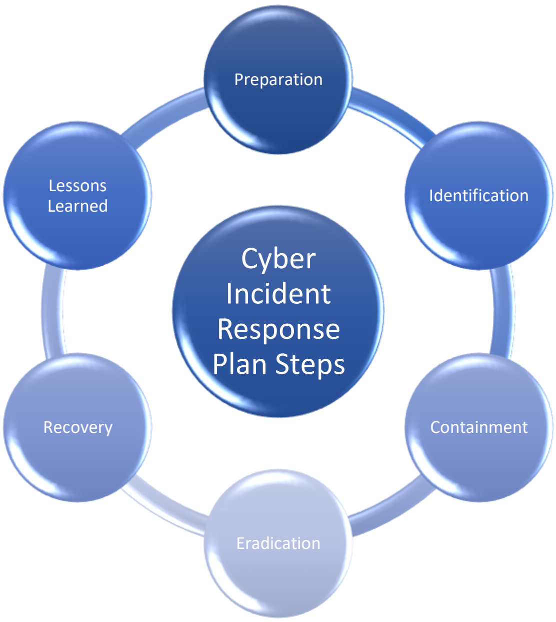
[18] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[19] https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf

[20] https://www.iod.org.nz/resources-and-insights/guides-and-resources/cyber-risk-practice-guide/#

Incident Response Recommendations

Your law firm needs to be ready to act in the event of a cyber incident. With robust incident response procedures in place, you will be better prepared to respond and recover.



Refer to the checklist below in the event of a data or privacy breach:

- Follow your cyber incident response plan
- Activate your response team
- Conduct a forensic examination
- Contact issuing banks
- Alert your insurance company if applicable
- Notify affected individuals
- Notify the New Zealand Law Society
- Notify the Office of the Privacy Commissioner and any other relevant jurisdictions
- File a complaint with the New Zealand Police and CERT NZ
- Confirm contractual obligations with suppliers and other third parties
- Have a public relations strategy in place

Contact us for a free cyber incident response template that is configured for NZ Law Firms.

Cyber Tip #9: User Training and Awareness

Ensure that your staff have read this guide and received appropriate training so that everyone is aware of their role in keeping the firm secure. As well as explaining procedures, the training should include advice on the potential cyber risks and their consequences.

All appropriate staff should be aware of the firm's cyber incident response plan and take part in regular cyber simulations.

We also recommend staff complete the following training resources

- ***ConnectSmart NZ - How Cyber Smart are you?***
- ***Domain Name Commission – Detecting Fake Websites***
- ***eLearning Site of The Office of the Privacy Commissioner, Privacy 101***
- ***Google Phishing Quiz***

How we can help you

We can help you at any stage of the development of your incident response process which we've summarised into the guide below.

Strategy and plans

We develop and improve incident response plans; we can also help with your security strategy, framework and roadmap of improvements.

Testing through simulations

Using forensic and cyber experts, we facilitate robust tabletop exercises to test and improve your incident response plan.

Panel of experts

We establish a suitable panel of experts including a breach coach and forensic, security, legal and public relations specialists who are ready to assist.

Forensic technology expert witness

We have significant experience in providing expert witness reports and in delivering expert witness testimony at trial.

Electronic investigations and eDiscovery

We love finding needles in haystacks, using our analytical and investigative techniques to a Forensic standard. Our eDiscovery expertise is also recognised by the Courts.

Risk mitigation

We help you to identify, contain and eradicate risks from your business, e.g. if a staff member has stolen your IP, we can wipe it from their electronic devices and cloud storage.

Return to business as usual

You may require data breach notification services, assistance with your cyber insurance requirements, or general security recommendations.

Post-incident review and improvement plans

Following an incident, we evaluate your response to correct any weaknesses and build on your strengths.

Resources

Incident Response Solutions has developed the following resources, tailored to the needs of New Zealand Law Firms.

- Cyber Incident Response Plan
- Cyber Incident Simulation Exercises
- NIST Cyber Security Framework Assessments
- NIST Privacy Framework Assessments
- Incident Response Retainer

Contact us if you would like to discuss any of these resources further.

Incident Response Retainer

With our Incident Response Retainer, you can take comfort knowing that when you need us, you will quickly have access to Incident Response experts, along with a comprehensive network of associated professionals. We can tailor a plan to meet your requirements, including the following:

- A welcome pack and initial consultation to explain how to maximise the service
- Access to a panel of experts who are ready to help
- Support desk for ad-hoc queries
- Our monthly forensic and cyber bulletin
- Yearly forensic readiness assessments
- Yearly assistance in drafting or revising your cyber incident response plan
- Board briefing packs and deep dive presentations
- Access to our incident response service desk tool for managing incidents
- Facilitation of a yearly cyber incident tabletop simulation
- Discounted rates on our forensic technology expert services

To find out more, please give us a call, send us an email, or visit our website.

Incident Response Solutions
Plaza Level
41 Shortland Street
Auckland 1010
New Zealand

Phone	0800 WITNESS or 021 779 310 (24 Hour Support)
Email	support@incidentresponse.co.nz
Website	https://incidentresponse.co.nz

Incident Response
FORENSIC & CYBER

INCIDENT RESPONSE SOLUTIONS

This document is prepared for general guidance and does not constitute formal advice. This information should not be relied on without obtaining specific formal advice. We do not make any representation as to the accuracy or completeness of the information contained in this document. Incident Response Solutions Limited does not accept any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining from acting, when relying on the information contained in this document or for any decision based on it.

https://incidentresponse.co.nz/cyber-security-guide-for-nz-law-firms