Cyber Security for Law Firms

14 September 2021

ADLS | CPD

About us

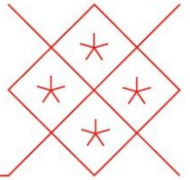
Campbell McKenzie
Director

INCIDENT RESPONSE SOLUTIONS

ADLS CPD

Cyber is Contextual – Law Firms

Law Firm Cyber Security 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 Firm)*
- 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)*
- 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)*

Legal Technology

In 2017, the New Zealand Law Society issued a Practice Brief titled “Cloud Computing”. In summary, law firms are increasingly using cloud computing as an alternative to in-house systems. Advantages such as flexibility and cost must be balanced against risks to privacy and control. It recommends that where third-party IT is involved, 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.

Cyber Tip: Cloud Computing

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

Cyber Security in the NZ Legal Context

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.

Rules of Conduct and Client Care

- Chapter 7 (Disclosure and communication of information to clients)
- Chapter 8 (Confidential information)
- Chapter 11 (Proper professional practice)

A Global Perspective

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

- Cyber security threats are increasing

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

- Over a quarter of firms report that they have experienced some sort of security breach
- Less than a third of law firms have an incident response plan.

2019 PwC Law Firms' Survey *(Global)*

- The insider threat is prevalent in all sizes of firms, with the majority having experienced incidents due to insiders over the last year

Cyber Tip: Websites

Beware of suspicious websites sent to you by email.

https://fakewebshop.nz

Cyber Tip: Social Media

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

Cybercrime - The Key Threats We Know

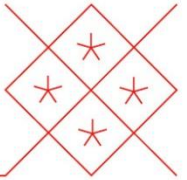
- Business Email Compromise
- Ransomware
- Supply Chain Compromise
- Crypto jacking
- Malicious Insider Attacks
- Remote Desktop Protocol (RDP)
- Social Engineering

Cyber Risk Management - Framework

The NIST cyber security framework enables law firms to assess maturity across five functions: **identify, protect, detect, respond** and **recover** 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.

Cyber Risk Management - Controls



The CIS Controls are a set of 18 prioritised, well-vetted, and supported security actions that organisations can take to assess and improve their current security state.

The controls are designed using knowledge of actual attacks to help an organisation prioritise their investment in controls that will provide the greatest risk reduction and protection against the most dangerous threat actors, and that can be feasibly implemented.

Cyber Tip: 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?*

Cyber Tip: 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

Cyber Tip: 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.

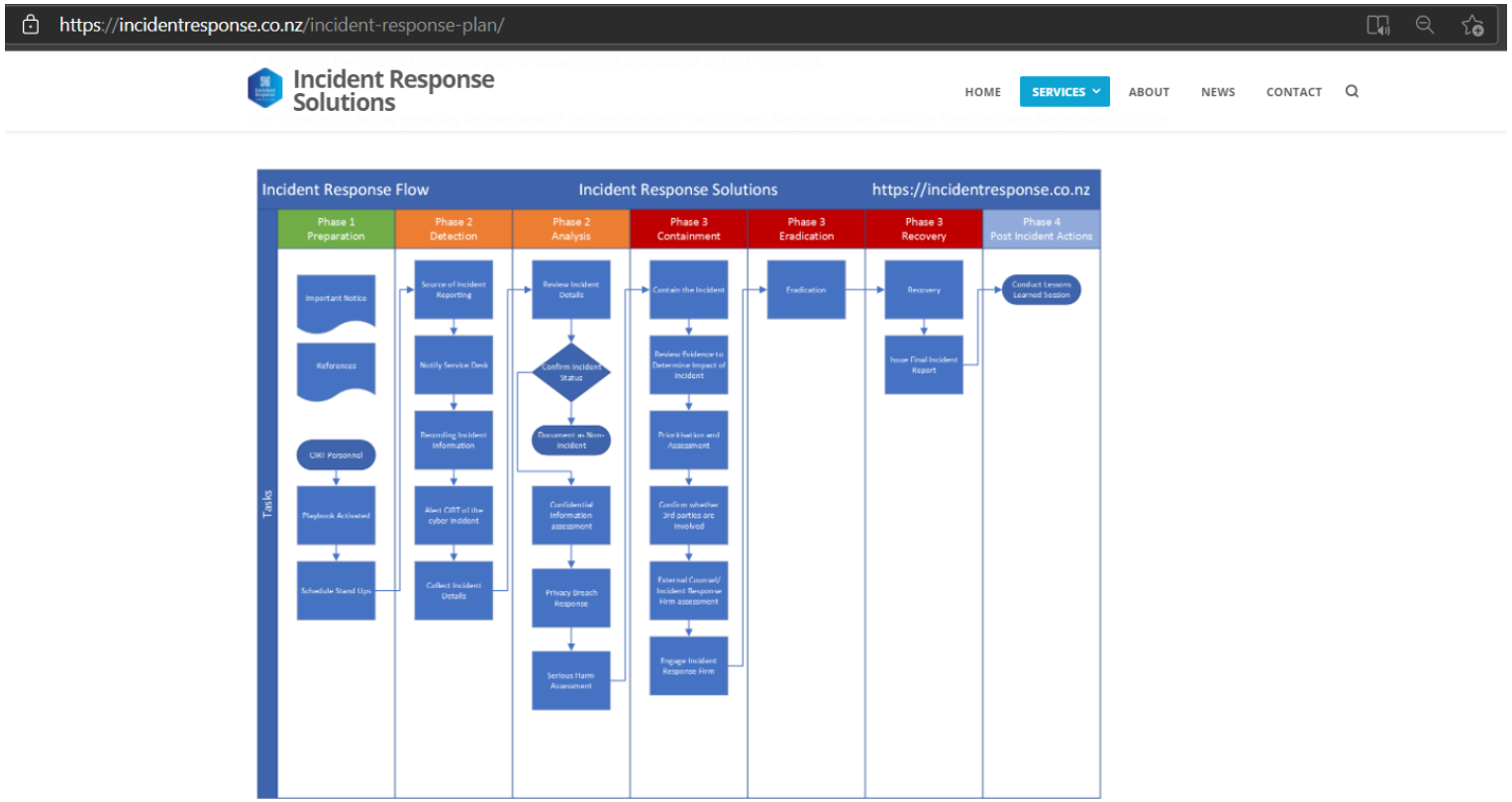
Cyber Tip: Password Management

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).

Our work in NZ

- Cyber Framework and Controls
- Incident response plans and playbooks
- Tabletop simulations
- Responding to incidents including forensics
- Incident Response Retainer

Incident Response Plan



Our Incident Response Plan and full set of associated Cyber Playbooks are hosted in an electronic control room which is hosted in a cloud solution. Read more on our Control Room offering here.

Click here to obtain the remainder of the Incident Response Plan.

Questions and Answers

ADLS | CPD