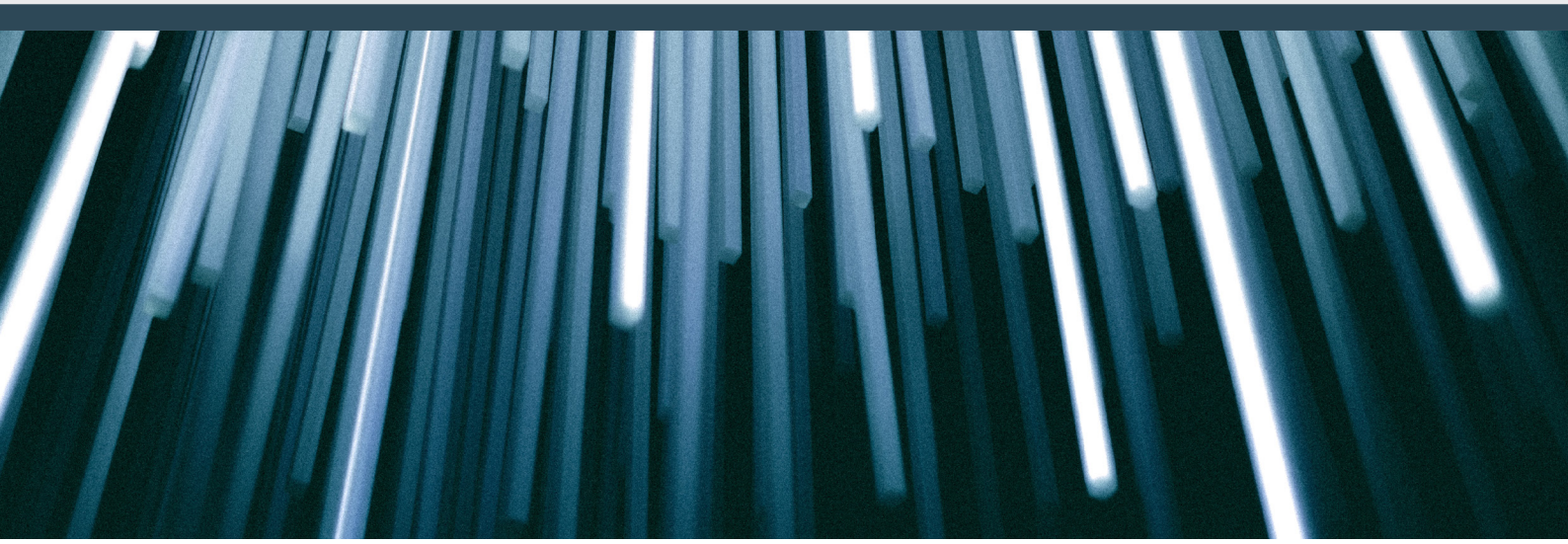
onelaw

CYBER SECURITY



As the frequency of cyber attacks rise, New Zealand law firms are increasingly concerned about the security of their data. Read on for a crash course on the cyber threat landscape, and what you can do to protect your law firm.

By OneLaw Technical Services Specialist, Caio Souza

Cyber security is a critical concern for law firms in today's technology-driven world.

Cyber criminals are constantly evolving their tactics to exploit vulnerabilities in online systems. As we hear more often about the havoc wreaked by these bad actors, we must armour up to protect valuable law firm data.

This paper covers:

+ Understanding the cyber threat landscape
+ Common attack vectors
+ Cloud security
+ Top tips to protect your law firm

CYBER THREAT LANDSCAPE

Understanding the evolving cyber threat landscape is crucial to help employ appropriate security measures and stay vigilant against emerging threats.

Several types of threat actors exist in the cyber threat landscape, each with distinct motivations and capabilities:

1. **Cyber criminals** are motivated by financial gain. They target organisations to steal sensitive data, then leverage it through financial fraud, sale on the black market or ransomware attacks.

2. **State-sponsored** cyber attacks are carried out by governments or intelligence agencies, to gain access to classified information or intellectual property of other countries or organisations. These attacks can support political, economic or military objectives.

3. **Hacktivists** launch attacks to promote a specific ideology or raise awareness about social or political issues. They target organisations or individuals associated with their cause.

4. **Insider threats** involve individuals within an organisation who misuse their authorised access to compromise systems, steal data or disrupt operations. Insiders can be disgruntled employees, contractors or business partners with malicious intent or unintentional negligence.

5. **Hackers** ranging from skilled individuals to inexperienced "script kiddies" exploit vulnerabilities for personal satisfaction, to prove their skills or to gain unauthorised access to systems.

COMMON ATTACK VECTORS

Cyber attackers employ various techniques to compromise systems, steal data or disrupt operations. Understanding these common attack vectors is essential for implementing effective cyber security measures:

1. **Malware**, short for malicious software, is a broad category of software designed to harm or exploit computer systems. It includes viruses, worms, Trojans, spyware and ransomware. Malware is typically delivered through infected email attachments, malicious websites or software downloads. Once executed, malware can perform various malicious activities such as stealing data, hijacking systems or encrypting files for ransom.

2. **Ransomware,** a specific type of malware, encrypts a victim's files or locks their system, demanding a ransom payment in exchange for restoring access. Ransomware attacks have become increasingly prevalent, targeting individuals, businesses and even critical infrastructure.

OneLaw Cloud mitigates ransomware risks through 24/7 threat detection and alerting, a small attack surface, and industry-standard authentication with mandatory MFA (Multi Factor Authentication). Our team conducts regular backups that are retained for a year, as well as an annual independent security review. All access to backend systems is strictly controlled by staff with security training.

3. **Phishing** attacks involve deceiving individuals into divulging sensitive information, such as usernames, passwords or financial details by masquerading as a trustworthy entity. Attackers often use email, text messages or fraudulent websites that appear legitimate to trick users into providing their information. Social engineering techniques are frequently employed to enhance the effectiveness of phishing attacks.

While OneLaw Cloud is designed to be resilient against phishing attempts, it is crucial for users to remain vigilant. While end users may be vulnerable to phishing, any malware that could potentially be introduced into their local area network (LAN) should not be able to spread to OneLaw Cloud due to our secure and obscure binary Transmission Control Protocol (TCP) connection.

4. **Insiders** may be disgruntled employees, contractors or business partners with malicious intent or unintentional negligence. Insider threats can result in data breaches, unauthorised access to systems or the introduction of malware.

5. **Zero-day exploits** target vulnerabilities in software that are unknown to the software vendor and have no available patches or fixes. Cyber attackers discover and exploit these vulnerabilities before they are patched, gaining unauthorised access to systems or deploying malware.

Zero-day exploits pose a significant risk as organisations have no advance warning or protective measures against them.

Our development partners have a security committee that assess any possible vulnerabilities to prevent such an attack.

6. **Advanced Persistent Threats (APTs)** are sophisticated, long-term cyber attacks that involve a stealthy presence within a system or network. APTs employ a range of techniques to extract valuable information, and are usually carried out by well-funded, highly skilled threat actors.

7. **Exposing Remote Desktop Protocol (RDP)** hosts to the internet without proper security measures can result in businesses being vulnerable to various hacking methods and attacks.

   OneLaw mitigates this risk by configuring our Virtual Machines (VMs) to be private, or, if public, they are IP whitelisted with strong passwords. This prevents unauthorised access through RDP.

8. **Network infrastructure vulnerability exploitation** occurs when attackers identify and take advantage of weaknesses or vulnerabilities in a networks' infrastructure components, such as routers, switches, firewalls and other networking devices.

   OneLaw proactively maintains the security of our network by keeping the many components of our cloud infrastructure up to date. We continuously improve this security and perform regular upgrades for firms using our software.

CLOUD SECURITY

Cloud computing has revolutionised the way organisations store, process and access data. It also introduces unique security challenges. Key tenets of cloud security include:

1. **Cloud Service Providers (CSPs)** and customers share responsibilities for security. The CSP is responsible for securing the underlying infrastructure, such as physical servers and networks. Customers are responsible for securing their data, applications, user access and configurations within the cloud environment.

2. **Data Protection** is crucial. CSPs often provide encryption at rest and in transit, but customers should also implement additional encryption measures to ensure data privacy. Proper access controls, strong authentication mechanisms and secure key management are essential components of data protection in the cloud.

3. **Identity and Access Management (IAM)** ensures that only authorised individuals or systems can access cloud resources. It involves managing user roles and permissions, implementing strong authentication mechanisms (e.g., MFA) and enforcing appropriate information barriers.

4. **Proper configuration of cloud services** is vital to mitigate risks. Firms should follow security best practices provided by CSPs, such as configuring firewalls, network segmentation and access controls. Continuous monitoring of cloud resources, event logging and real-time threat detection help identify and respond to security incidents promptly.

5. **Developing an incident response plan** specific to cloud environments helps organisations respond effectively to security incidents. This includes steps to isolate affected resources, collect evidence, notify appropriate parties and restore services. Regular backup and disaster recovery strategies are critical for minimising data loss and ensuring business continuity, and should be worked through with your IT team.

6. **Choosing a reputable and reliable CSP** is vital for maintaining strong cloud security. Organisations should assess the provider's security controls, certifications, data privacy policies, incident response capabilities and contractual obligations. Regular audits and assessments help ensure ongoing security and compliance.

7. **Security awareness and training programs** should educate employees about cloud security risks, best practice and their responsibilities. Topics may include secure data handling, phishing prevention, secure use of cloud services and adherence to organisational security policies.

At OneLaw we take the security of our systems seriously. Our commitment to maintaining a secure environment includes regularly reviewing and implementing Microsoft Azure (cloud computing platform) security recommendations, including regulatory compliance measures.

"The [OneLaw] Cloud platform has allowed me to work from overseas a couple months every year. It's way better than some of the experiences I've had previously"

Gerard Molloy, Partner, Molloy Hucker
(Read the case study here)

We are in the process of formally adopting an industry-standard cyber security framework to further enhance our security practices.

To safeguard our services, requests sent between the OneLaw client software and our Cloud service are sent using an obscure network protocol. This is more secure than a standard web application. Our system also undergoes regular independent security reviews and penetration testing to identify and address potential vulnerabilities.

We utilise Microsoft Azure backup technology to ensure data resiliency. We are exploring additional security practices, such as air gapping (isolating a private network from all external networks) to provide additional protection.

Learn more about our Cloud offering here and the migration process here.

TOP TIPS TO PROTECT YOUR FIRM

By incorporating cutting-edge technologies and best practice in your firm, you can establish a strong defence against cyber threats.

1. **Make cyber security a top priority** within your organisation. Allocate appropriate resources to this area and recognise that cyber security requires continuous investment and attention.

2. **Adhere to cyber security best practices** such as conducting regular risk assessments, practising strong access management, encrypting sensitive data and establishing an incident response plan. Regularly update and patch software and systems to address known vulnerabilities.

3. **Promote cyber security awareness**. Conduct regular training sessions and encourage a culture of security consciousness throughout your organisation.

4. **Foster collaboration among industry peers.** Share threat intelligence, lessons learned from security incidents and best practice. By collaborating, we can collectively strengthen our defences and respond more effectively to emerging threats.

5. **Stay updated** on the latest cyber security trends, emerging threats and industry-specific regulations. Regularly monitor reputable cyber security sources and participate in relevant communities to stay ahead of evolving threats.

6. **Consider engaging third-party cyber security experts** to assess your organisation's security posture, conduct penetration testing and provide guidance on security improvements. Leverage their expertise to enhance your overall cyber security capabilities.

7. **Develop and test an incident response plan** for your organisation. Define roles, establish communication channels and outline your response in the event of a security incident. Regularly review this plan in line with the changing threat landscape.

For further information, read our paper on Account Security here.

Caio Souza
OneLaw Technical Services Specialist

Caio joined the OneLaw team in 2023, with a strong customer service background and love for technical problem solving. Alongside working for OneLaw, Caio is pursuing a Bachelor of Commerce with a double Major in Information Systems and Human Resources.

onelaw.co.nz
Find us on LinkedIn

If you would like more information on OneLaw and our services, get in touch at enquiries@onelaw.co.nz