In the Boxing Ring
MAR 2025

Network Box Technical News
from Mark Webb-Johnson
Chief Technology Officer, Network Box

Welcome to the February 2025 edition of In the **Boxing Ring**

This month, Network Box's Managing Director, Michael Gazeley, discusses **Cybersecurity Imperatives for the Legal Profession**. Modern law firms are no longer just targets for traditional crimes; they have become prime targets for cybercriminals, who are attracted by the vast amounts of confidential client information contained within each firm's digital infrastructure. Unfortunately, many firms fail to implement comprehensive cybersecurity measures to safeguard this sensitive data. On pages 2 to 4, we highlight the threats facing law firms and suggest strategies to protect both their practices and their clients.

In other news, Network Box Hong Kong held a cybersecurity workshop in partnership with **Tradelink Electronic Commerce Limited**. Additionally, we are thrilled to announce the launch of our **Box Mail** app for Android and iOS. Tailored for users who have subscribed to our email scanning services, Box Mail allows users to manage their email security on the go, anytime and anywhere. Please use the links to download the FREE app today.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
February 2025

Stay Connected

You can contact us here at Network Box HQ by email: **nbhq@network-box.com**, or drop by our office next time you are in town. You can also keep in touch with several social networks:

https://x.com/networkbox
https://www.facebook.com/networkbox
https://www.facebook.com/networkboxresponse
https://www.linkedin.com/company/network-box-corporation-limited/
https://www.youtube.com/user/NetworkBox

In this month's issue:

Page 2 to 4
Cybersecurity Imperatives for the Legal Profession

Technology has revolutionized law practice, providing unparalleled efficiency and reach. However, it has also introduced a new set of threats that are silent, invisible, and potentially devastating. Modern legal professionals now face challenges from malware, phishing attacks, and ransomware, rather than traditional crimes. In our featured article, we discuss these cyber risks and present our top 10 cybersecurity essentials for law firms.

Page 5
Network Box Highlights:

- **Box Mail - Network Box Mail Portal App**
- **Network Box Hong Kong**
  - Cybersecurity Workshop

CYBERSECURITY IMPERATIVES for the Legal Profession

by Michael Gazeley
Managing Director
Network Box Corporation Limited

Law firms pulse with digital activity in the heart of bustling business districts. Computers hum, servers whir, and vast amounts of sensitive data flow through intricate networks. All are connected to the Internet on a permanent twenty-four-hour basis. This technological revolution has transformed law practice, offering unprecedented efficiency and reach. Yet, it has also exposed the profession to a new breed of threats; silent, invisible, and potentially devastating.

The modern law firm is no longer just a target for traditional crimes. It has become a prime mark for cybercriminals, drawn by the treasure trove of confidential client information that resides within each law practice's digital walls. Our collective 'rice bowls' have now become 'digital rice bowls.' Malware, phishing attacks, and Ransomware are the new adversaries that legal professionals must now confront.

Ensuring the security of client data and confidential information is essential for all legal practitioners. With the rapid adoption of technology, law firms are increasingly vulnerable to cyber threats that can result in data breaches, financial losses, and reputational damage. A law firm can become 'frozen' by a modern cyber-attack.

With the unrelenting onslaught of Ransomware, not only can all your clients' confidential data be stolen by Hackers, but all your computer systems can also be 'locked' simultaneously. This can render your entire law firm utterly unable to function.

Even if you rushed out and bought some new computers, you would still be unlikely to be able to work, as you would probably no longer have access to the client files you need. To underline just how insidious the latest iterations of Ransomware are, many will render your data backups unusable, including any Cloud backup systems you may be relying on, before they even let you know you have become a cyber-attack victim. Imagine having to tell your clients that you cannot work because you no longer have access to their files, while some hacking collective halfway around the world is now also threatening to publish everything that was stolen online. In recent cases, confidential data has been posted on the Dark Web to be shared by Hackers and on the Surface Web for everyone to see.

Information Security Guidelines for Legal Practitioners serve as a crucial roadmap, guiding firms through the complex terrain of digital security. These are not mere suggestions but essential survival strategies in an increasingly hostile online environment. Lawyers have a legal and professional duty to maintain strict confidentiality of client information. Professional Conduct guides make this extremely clear. Unauthorized disclosure of confidential client information could lead to disciplinary proceedings and even potential civil liability. The duty of confidentiality extends to electronic communications and continues indefinitely, even after the client's death.

At the core of these guidelines lies an unwavering commitment to confidentiality; a lawyer's duty to protect client information is absolute and enduring. This obligation transcends the bounds of the professional relationship, persisting even beyond the client's lifetime. It is a sacred trust that forms the legal profession's bedrock. Complementing this professional duty are Personal Data (Privacy) Ordinances, which are a legislative bulwark against the misuse of personal information. They mandate stringent protection measures, compelling law firms to treat client data with the utmost care and security.

But how does a law firm transform these principles into practice?

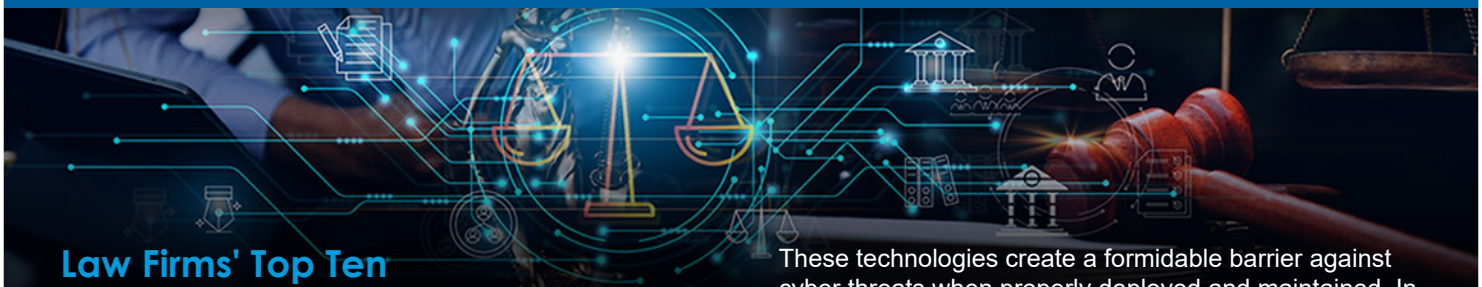
It begins with introspection. Regular security risk assessments serve as critical health checks for IT infrastructure, identifying vulnerabilities before they can be exploited. These assessments should inform a comprehensive information security policy - a clear, actionable set of rules that governs how the firm handles sensitive data at every level.

Hackers and cybercriminals are increasingly targeting legal practices due to their wealth of sensitive client data; ironically, many law firms leverage significantly weaker IT security and cyber-security practices than their clients. Common threats include a lack of protection against zero-day malware, known software vulnerabilities, weak passwords (123456, Batman, password), human error, lax third-party control, and the list goes on. Many lawyers will try to absolve themselves from responsibility by saying, 'I don't know much about computers,' but if ignorance of the law is no excuse, then neither is ignorance of cyber-security. What you do not know can and will hurt you.

For a law firm to diligently protect itself from malware, hackers, and criminals, it needs to not only protect its networks, servers, and devices from a wide range of cyber-attacks, complying with international standards for Quality Management, IT Management, IT Security Management, and Risk Management, but also perform regular risk management checks on all its systems, at least once a quarter. Quarterly Best Practice Reports are an essential keystone, clearly highlighting everything that needs to be improved, enhanced, or augmented. In addition, weekly scans should be performed on each organization's 'Attack Surface,' ensuring that any new vulnerabilities can be quickly found and dealt with, hopefully before they have been taken advantage of.

Years ago, it was not likely that a staff member could (either deliberately or by accident) open an access point on your office network for a Hacker halfway across the world to take advantage of. But this has become an unfortunate yet regular occurrence in today's hyper-technological world. Indeed, the 'Internet of Things' also brings a host of computers, which do not even look like computers, into the mix. Some examples include IP Telephones, Smart TVs, Projectors, Printers, CCTVs, Multifunction Photocopiers, Document Imaging Systems, and a host of other smart devices, which are all but sure to be part of every lawyer's work environment. If a device is 'smart' and is connected to your network, hackers and malware can and will exploit them. And once a hacker has access to your network, they can do unlimited damage.

Implementation of effective cyber-security policies requires a concerted effort. It demands clear assignment of roles and responsibilities, regular training sessions, and the establishment of robust incident response protocols. These administrative measures lay the groundwork for a culture of security awareness throughout the organization. Red Teaming, a term used to describe Offensive Cyber-Security, is a critical part of staying secure. In the same way, a physical security team can check your office's CCTV, Alarms, and Locks, a cyber security Red Team can check your Firewalls, Intrusion Detection and Prevention systems, and Anti-Malware for their effectiveness against the worst that the Internet has to offer.



Law Firms' Top Ten Essential Cybersecurity Essentials

01. Properly set up, **updated and monitored firewalls** to ensure that what should be outside your local area network stays outside.
02. **Anti-Malware systems** that are updated second by second to ensure Ransomware and other computer viruses cannot infect your devices.
03. **Enhanced Policy Controls** to ensure that your law firm follows the law and your internal rules and regulations.
04. **Virtual Patching** - performed around the clock at your Internet Gateway so that any sudden vulnerabilities do not put your computers and networks at risk.
05. **Virtual Private Networking** protects all communications between your people and your offices, including when staff are travelling overseas, from snooping.
06. **Internet of Things protection** includes printers, photocopiers, smart televisions, CCTVs, and all other types of computers that don't look like computers.
07. **Cloud Security Information and Event Management**, which logs all the attacks on your technology platforms and keeps a detailed record for reference.
08. **KPI Reporting** gives your law firm (and your auditor) regular, comprehensive reports on your cybersecurity, compliance, and business continuity.
09. **Dark Web Monitoring**, so that you will know which of your staff and ex-staff have had confidential credentials stolen and posted by Hackers on the Dark Web.
10. **ISO Compliant Cybersecurity Management**, covering Quality Management, IT Management, IT Security Management, and Risk Management, for peace of mind.

Next generation cyber-security technology also plays a pivotal role. Advanced security tools, such as Virtual Patching (blocking known flaws in software such as Windows), Dark Web Monitoring (advanced warning when your staff's confidential credentials have been posted on the Dark Web by Hackers), state-of-the-art encryption (ensuring your clients' information stays safe), all form the vanguard of a firm's digital defences.

These technologies create a formidable barrier against cyber threats when properly deployed and maintained. In most cases, however, it turns out that it was not a 'highly sophisticated cyber-attack' that allowed the victim to be hacked, breached, and have confidential data stolen - it was a lack of a required technology.

Imagine you are wearing the world's most effective bullet-proof jacket; the attacker can still poison your breakfast, push you off a skyscraper, or set your house on fire in the middle of the night. You can see how not having the needed protection against the actual threat putting you at risk will all but ensure that the attacker is successful. Having effective protection means having complete protection.

The cyber threat landscape is in constant flux, evolving at a pace that can be dizzying for legal professionals. Yet, with the right approach, combining sound policies, cutting-edge technology, and expert support; law firms can rise to meet this challenge. It is not merely about protecting data; it's about preserving the trust that is the lifeblood of the legal profession.

Legal professionals bear a weighty responsibility as guardians of confidential information in this digital age. The tools and knowledge to fulfil this duty are within reach. Indeed, fully managed monthly protection for a small law firm can cost as little as half an hour of a single lawyer's time. Effective cyber-security doesn't have to be expensive, but getting hacked or infected certainly is. By embracing robust cybersecurity measures, law firms can ensure they remain bastions of trust and confidentiality in an increasingly interconnected world.

In the realm of cybersecurity, vigilance is not just a virtue; it's a necessity. As the digital landscape continues to shift, so too must the strategies to protect it. The future of legal practices depends on the profession's ability to adapt, innovate, and stand firm against the rising tide of cyber threats.

Network Box HIGHLIGHTS

Network Box Hong Kong
Cybersecurity Workshop

Network Box Hong Kong hosted a cybersecurity workshop in partnership with *Tradelink Electronic Commerce Limited*. Those who attended the event were briefed on the current threat landscape and introduced to Network Box cybersecurity solutions that can mitigate those threats, and keep their network secure.

Newsletter Staff

Mark Webb-Johnson
Editor

Michael Gazeley
Kevin Hla
Production Support

Network Box HQ
Network Box USA
Contributors

Subscription

Network Box Corporation
nbhq@network-box.com
or via mail at:

Network Box Corporation
16th Floor, Metro Loft,
38 Kwai Hei Street,
Kwai Chung, Hong Kong.

Tel: +852 2736-2083
Fax: +852 2736-2778

www.network-box.com

Box Mail
Network Box Mail Portal App

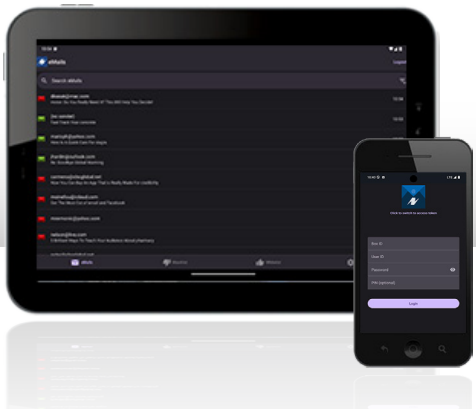
Last month, Network Box officially launched the new version of our Mail Portal platform – **Box Mail**. Tailored for users who have subscribed to our email scanning services, Box Mail simplifies managing your email security with a range of powerful features. Today, we are thrilled to announce the launch of the Box Mail mobile app for both Android and iOS. With this powerful new app, you can now effortlessly manage your email security on the go, anytime and anywhere.

Key Features

Custom Whitelist/Blacklist: Effortlessly control your inbox by adding emails to your whitelist or blacklist whenever needed.

View Blocked Emails: Quickly search and view emails flagged by the system to ensure you never miss important messages.

Release Quarantined Emails: Easily release quarantined emails and keep your inbox running smoothly.



GET IT ON Google Play

LINK:
https://play.google.com/store/apps/details?id=com.networkbox.user

Download on the App Store

LINK:
https://apps.apple.com/us/app/box-mail/id6741088219