LAW FIRMS AS PRIME TARGETS FOR HACKERS: 7 STEPS TO REDUCING CYBER RISKS

Aniket Bhardwaj, *Charles River Associates*

shutterstock.com/SuppachokN

Due to the nature of their business, law firms possess a tremendous volume of valuable documents and data, which are extremely attractive to hackers of a variety of motivations. Successful cyber-attacks can cause a severe negative impact to a law firm's operations and catastrophic damage to a law firm's reputation.

According to the recently published 2020 *ABA Legal Technology Survey Report*, the number of law firms experiencing a known security breach increased to 29 per cent in 2020. The survey notes that "despite the ethical issues and pending challenges, the use of certain security tools remains at less than half of respondents," and only 36 per cent of the respondents have committed to cyber insurance policies.

This paper seeks to help all organisations and institutions, not just law firms, better understand the threats they face and why they should work toward better cyber hygiene, and a more proactive incident and threat management strategy. First, I review why law firms are attractive cyber targets and how compromising these firms is a high priority to threat actors. I will define the concept of "cyber hygiene" and show why it is critical to maintaining IT security best practices. Second, I examine some of the more notable and notorious cybersecurity thefts and leaks in recent years as well as the easily avoidable weaknesses that led to these unfortunate events. Third, I argue that organisations and institutions around the world should be more proactive in their overall security strategy. Finally, I highlight key tactics for building a robust incident and threat management program.

WHAT MAKES LAW FIRMS VULNERABLE TO CYBER-ATTACKS?

Law firms are natural targets of both internal and external bad actors. The documents housed on their corporate and personal computers are repositories of sensitive and potentially incriminating information. If a cybercriminal or nation-state is looking for confidential information regarding a potential merger or acquisition, breaching the law firm is made more attractive by the prospect of gaining access to the firm's client information. Although not an attack on a law firm, the largest sustained global cyber espionage campaign, referred to as Operation Cloud Hopper, showed how customers of global firms can also suffer significant damage from a strategic attack. Operation Cloud Hopper targeted IT-managed service providers who, in many cases, allowed direct and unfettered access to their customers' networks. It's easy to see how law firms, who have highly sensitive client data, provide threat actors both unprecedented visibility into multiple targets and a tremendous strategic advantage for future attacks. Obviously, this concern applies to many industry sectors and institutions around the globe.

THE IMPORTANCE OF CYBER HYGIENE

"Cyber hygiene" is a prerequisite for a successful incident and threat management program. The worst thefts and infiltrations are often due to poor cyber security. In the same way that personal mental and physical hygiene maintain a healthy body and mind, good cyber hygiene practices keep computer systems up to date, promote full visibility and ensure data protection.

Cyber hygiene helps maintain best practices in keeping sensitive data safe from external attacks and in complying with the latest security standards, including monitoring access privileges on different applications and systems. Cyber hygiene will identify high-risk vulnerabilities and determine whether those vulnerabilities are present within an IT estate; it can also verify whether unencrypted PII (Potentially Identifiable Information) exists on unsecured systems. Moreover, diligently following cyber hygiene best practices helps maintain compliance with frameworks such as the National Institute of Standard's Technology Cybersecurity Framework (NIST CSF) and ISO 27002/1. Overall, robust cyber hygiene lays the foundation for a successful threat management program within an organisation. Without it, the organisation is at considerable risk of successful infiltration and data theft.

A SERIES OF UNFORTUNATE CYBER EVENTS

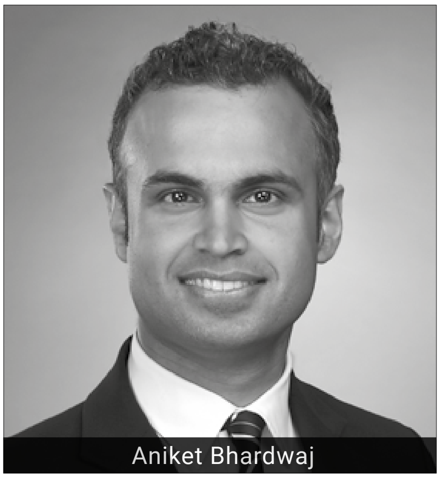
In 2016, an attack on the Mossack Fonseca law firm led to the breach of more than 11 million confidential and privileged documents, including emails, database files, PDFs and thousands of text documents. Based on reporting done by security researchers, there were multiple reasons for the breach, including external-facing servers running outdated software, while missing critical security updates. In other words, Mossack Fonseca did not have adequate cyber hygiene protocols and procedures as there was a clear lack of visibility across the estate, as well as missing patches and vulnerabilities including poor network segmentation.

In 2017, the NotPetya Ransomware attack, the most devastating cyberattack to date, infected hundreds of thousands of computers, including a major international law firm. Other large corporations such as the shipping giant Maersk, the pharmaceutical giant Merck, FedEx's European subsidy TNT Express, the French construction company Saint-Gobain, food producer Modelez, manufacturer Reckitt-Benckiser and multiple government agencies were also targeted. The attack crippled ports, paralysed corporations, infiltrated government agencies and wreaked havoc on organisations throughout the world, inflicting more than $10 billion in total damages in the process, according to Wired magazine. The threat actors exploited unpatched vulnerabilities in order to breach systems across multiple organisations, as well as a vulnerability in Microsoft systems (aka CVE-2017-0144, whose patch had been released in March 2017).

Had these organisations implemented a robust patch and vulnerability management program, this devastating attack could have been prevented. (It is important to emphasise here that nation-state actors have shifted toward exploiting similar unpatched vulnerabilities rather than funding the development of a zero-day exploit.) Government security agencies later attributed the attack to the Russian military, saying it was "almost certainly responsible for the 'NotPetya' cyberattack of June 2017." The effects of inadequate cybersecurity hygiene were felt across multiple organisations around the world.

Like NotPetya, many ransomware variants rely on unpatched vulnerabilities to successfully launch an attack. In recent years, the surge in ransomware attacks has been partly a result of vulnerabilities in external-facing systems. Threat actors have been able to leverage unauthorised permissions, move laterally within the environment and successfully launch a ransomware attack. On other occasions, these attacks have exploited the vulnerabilities in internal systems following a successful email phishing campaign.

Threat actors easily exploit weaknesses in security management programs, especially in those which fail to deploy patches early. A window is left open, and systems are vulnerable and easily compromised. The common theme of poor system visibility and inadequate cyber hygiene continues to be a significant problem for organisations. In the remainder of the article, I will address how security leadership should drive a culture of change to include security hygiene as a minimum baseline expectation across the offensive and defensive security teams.


Aniket Bhardwaj

A PROACTIVE SECURITY STRATEGY

Despite increased budgets, better tools and more focus, many organisations still struggle with cyber hygiene basics, not to mention more advanced security tasks like detection and response. In fact, 71 per cent of organisations lack end-to-end visibility of endpoints and health. Moreover, employees sometimes install unapproved applications that can weaken an organisation's overall security.

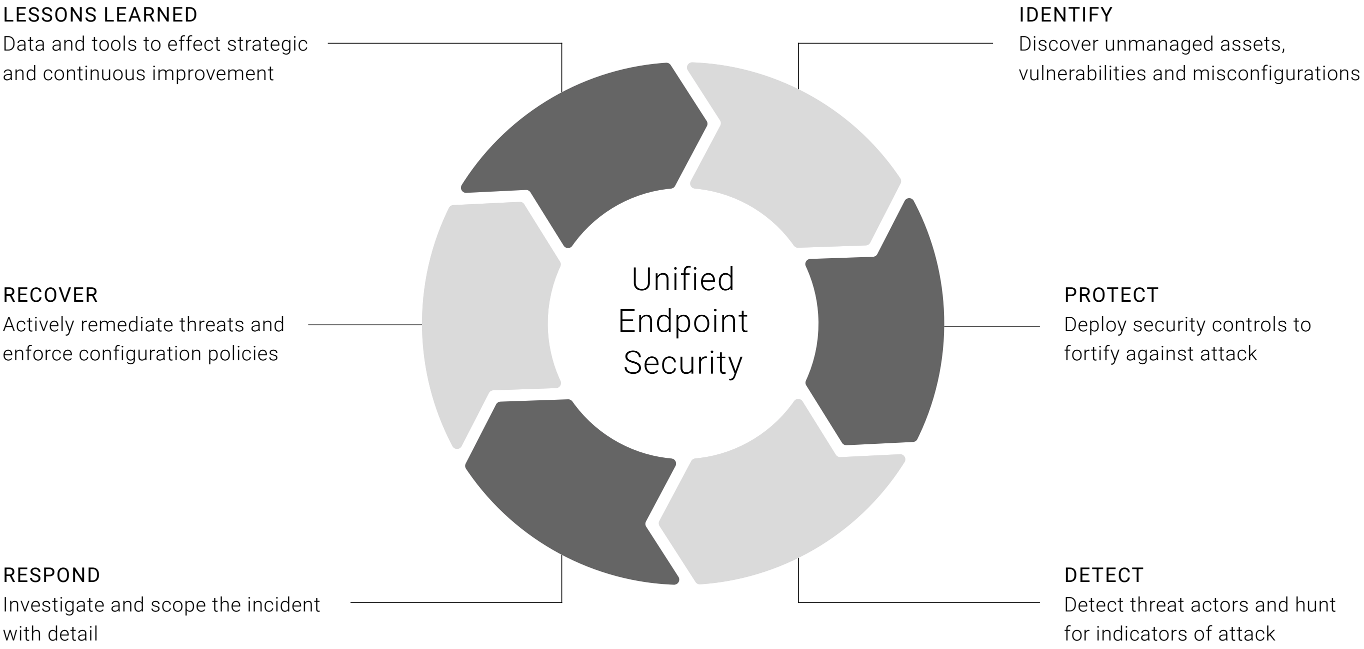
A proactive cyber hygiene program starts with an inventory of all hardware, software and applications, as well as a unified solution, providing visibility across these components to reduce the attack surface of an organisation. A solution that helps execute live queries, verify the total number of systems (including an operating system breakdown) and then quantify the list of running applications (including the list of user accounts across the identified systems), provides a clear view of the attack surface of an organisation. The IT and operations teams can then understand missing patches on the endpoints as well as system- or application-level vulnerabilities, the presence of full-disk encryption software and sensitive data identification such as PII. They will be able to work towards identifying systems that are not compliant with the organisation's security policy. A proactive cyber hygiene program can drastically reduce the risk of missing security updates and improve the incident and threat management of an organisation.

TOTAL CYBER HYGIENE

To integrate hygiene best practices into an overall security process, organisations should create a total cyber hygiene policy. As a best practice, a cyber hygiene policy can include monitoring and proactively managing the following seven steps:

1. Identify asset inventory such as unmanaged servers, laptops and desktops.

Figure 1: Unified Endpoint Security (UES)


LESSONS LEARNED
Data and tools to effect strategic and continuous improvement
IDENTIFY
Discover unmanaged assets, vulnerabilities and misconfigurations
RECOVER
Actively remediate threats and enforce configuration policies
Unified Endpoint Security
PROTECT
Deploy security controls to fortify against attack
RESPOND
Investigate and scope the incident with detail
DETECT
Detect threat actors and hunt for indicators of attack

2. Address software updates and operating system-specific updates.
3. Address hardware and firmware updates to identify security risks and priorities.
4. Inventory applications and their acceptable use.
5. Address insider threats and data exfiltration risks such as removable storage media and security controls on storage devices.
6. Identify unencrypted sensitive information and follow industry-specific security compliance program.
7. Generate routine encryption reports to confirm the presence of encrypted volumes.

After creating the cyber hygiene policy, key IT and security operations stakeholders should agree on process and a set of reasonable time frames. Additionally, a routine check for security updates every five days should be put in place, including ownership of the tasks mapped to all cyber hygiene policy categories. A structured framework will help individual functions ensure proactive cyber hygiene within the organisation.

Any effective cyber hygiene policy allows the organisation to secure and fortify all endpoints, and permits security teams to identify, protect, detect, respond to and recover from threats affecting systems, running both legacy and modern operating systems. The best way to accomplish this is with Unified Endpoint Security (UES), which helps to control the full stack of security operations that manage technologies and monitor the environment for compliance. Most importantly, UES helps correlate activities between endpoints and other data sources, such as application logs or network-related events.

UES provides an on-going and effective approach to security management and promotes alignment with frameworks such as the NIST CSF. UES can also help an organisation implement best practices to start a cyber hygiene program, encompassing detection and response programs for security defence teams. UES starts with an identification of endpoint assets and then builds a complete attack surface inventory. A UES solution can aid in linking endpoint activities to identify and remediate security gaps (such as missing patches) and protect the endpoint through required controls, including antivirus and full-disk encryption. This solution facilitates detection, response and recovery from threats in the IT estate.

An effective cyber hygiene program begins with addressing the following questions and works toward reducing the attack surface with a robust cyber hygiene policy:

Q1: How many authorised and unauthorised servers, workstations and software versions do you have installed across your network?
Q2: How do you continuously assess and remediate security vulnerabilities, apply patches, and ensure that your endpoints are configured according to best practices and are compliant with industry baselines/standards?
Q3: Can you detect and protect the data leaving your environment?
Q4: Do you have visibility into where sensitive data resides and do you have the ability to quickly remediate issues as they arise?
Q5: Do you know who has elevated administrative access to your servers and endpoints, and do they need that level of access?
Q6: Are you prepared for security compliance or maturity assessment within industry best practice frameworks?
Q7: Can you identify and mitigate insider threats to your organisation?

Having the answers ready by employing the techniques examined above and including the associated metrics in your weekly reporting to senior leadership, will help lay a solid foundation for building a security management program.

Aniket Bhardwaj is vice president in the forensic services practice at Charles River Associates. The views expressed herein are the views and opinions of the author and do not reflect or represent the views of Charles River Associates or any of the organisations with which the author is affiliated.

Email: abhardwaj@crai.com

shutterstock.com/seamuss