Is Your Firm Prepared?

A cybersecurity guide for legal professionals

esentire®

How important is cybersecurity?

There are two types of law firms: those who have had a security breach and those who will. Law firms hold extremely important and confidential client information, from trade secrets, to patient data, to the formula for the next pharmaceutical breakthrough. Attacks from never-before-seen threats are constantly lurking on the dark web and can end your business in a matter of seconds.

It's important to realize that a cyber breach can happen when you least expect it. It's been reported that the cost of cybercrime for U.S. organizations has grown by 96% over the past five years. Over that time, the average organization's overall data breach outlay was $12.7 million.[2] It goes without saying that protecting your firm from cyber threats should be a top priority.

Introducing and implementing cybersecurity best practices requires multiple resources. This eBook has been designed to help your firm understand today's vast cybersecurity considerations.

Ask yourself:

- Do you know what **threat vectors** and likely attacks look like?
- Do you understand the **regulators and standards** that impact your firm?
- Are you confident that your firm is prepared for the **inevitable cybersecurity breach**?
- Do you maintain regular **user awareness training**? Or is your weakest link exposed?
- Do you know what your firm will do in the event of a breach? Do you have an **incident response plan** in place?

1. http://www.americanbar.org/publications/techreport/2016/overview.html
2. http://blog.capterra.com/growing-threat-of-law-firm-cyberattacks/

esentire

What do likely attacks look like?

Common Legal Threat Vectors

Threat vectors across all industries are constantly getting stronger, faster and more intelligent. According to the FBI, ransomware attacks made $209 million in the first quarter of 2016. They predict that it will exceed $1 billion by the end of the year.[3] Cybercriminals are able to adapt their methods on the turn of a dime to target your firm with new variants designed specifically for your firm. The legal industry is no stranger to the many variants of cyber threats available.

RANSOMWARE

PHISHING/SOCIAL ENGINEERING

MALWARE

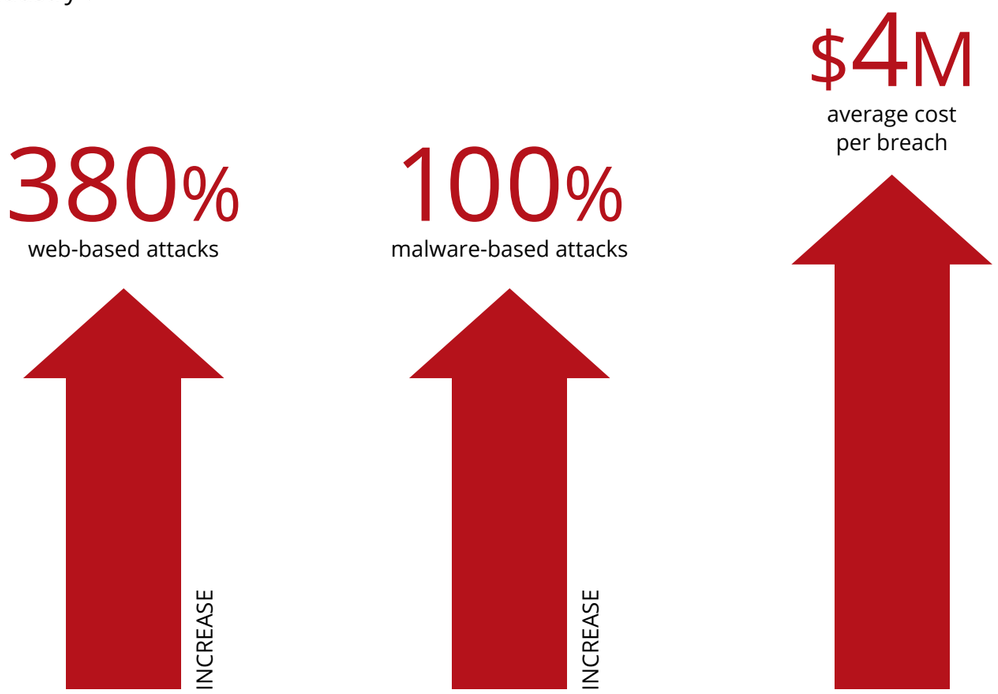
INSIDER THREAT

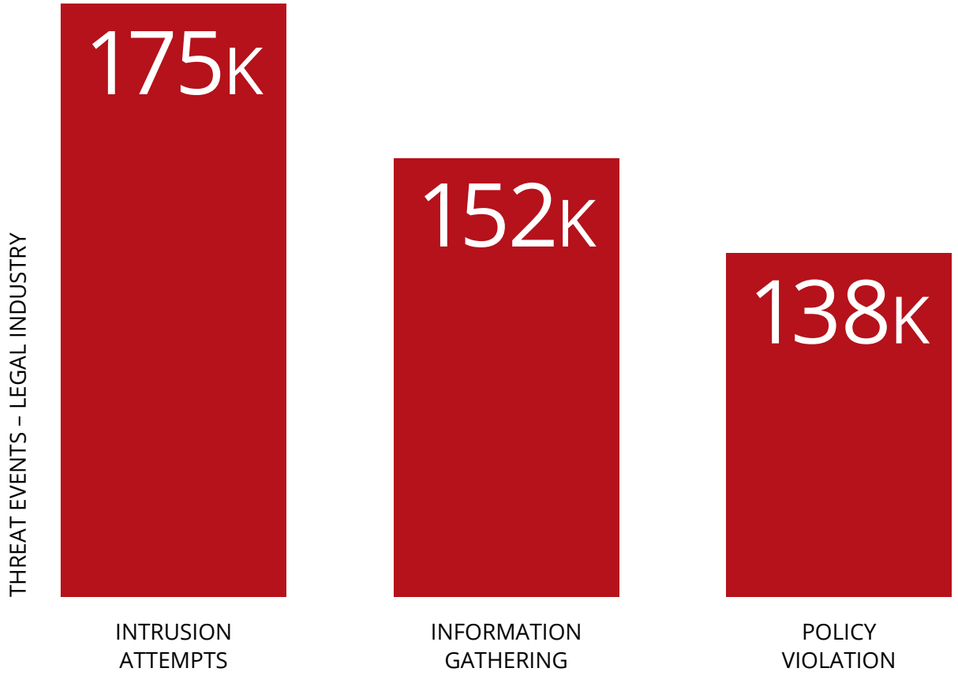
3. https://www.esentire.com/blog/dos-2-0-is-ransomware-the-next-evolution-of-dos/

esentire

A View from our SOC

The Security Operations Center (SOC) at eSentire analyzes tens of thousands of security events daily. Our analysts see everything from network intrusion attempts to malicious code, to new, never-before-seen attacks. When looking at the millions of security events investigated in 2016, we discovered interesting trends related specifically to the legal industry[4]:





Threat Findings and 2017 Trends

The data suggests that intrusion attempts, information gathering and malware attempts have steadily increased. Our threat intelligence team predicts that in 2017, law firms will face in increase in intrusion attacks orginating from web attacks, in addition to threats related to web servers, applications and databases.

4. eSentire, 2016 Legal Threats Summary Report

Regulators: what standards apply to your firm?

Regulators differ depending on the country you practice in and/or the location of your clients. Let's break down the regulatory standards in the US, Canada and UK:

United States

Regulators such as the Security Exchange Commission (SEC) and Health Insurance Portability and Accountability Act (HIPAA) uphold strict regulations in their industries. However, law firms are not governed specifically by any one regulatory authority that demands disclosure. In the United States, lawyers must meet the standards of the American Bar Association (ABA) Model of Professional Conduct to make reasonable effort to prevent disclosure of confidential client information (RULE 1.6(C)), and keep abreast of risks associated with technology (COMMENT 8 to Rule 1.1).

Canada

Office of Superintendent of Financial Institutions (OSFI), Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), Canadian Securities Administrators (CSA) and Investment Industry Regulatory Organization of Canada (IIROC) are the top regulators that Canadian firms must acknowledge and align to. CSA enforces security laws in each province and territory to provide the legal foundation to with regulatory requirements related to capital markets. Firms must review and understand the regulations and rules under each securities act.

United Kingdom

Financial Services Authority (FSA), Bar Standards Board (BSB) and Solicitors Regulation Authority (SRA) are key UK regulators. Law firms in the UK must follow BSB standards when specifically looking into the confidentiality clause. C15.5 acknowledges that your duty of confidentiality is subject to an exception if disclosure is required or permitted by law. You may be obliged to disclose certain matter by the Proceeds of Crime Act 2002.

Your Clients are your New Regulators

The SEC, FINRA, HIPAA, OSFI, CSA, FINTRAC, FSA, BSB and SRA are the big guns when it comes to regulatory bodies across the finance, banking and healthcare industries. They are taking the legal industry by storm. Signing a new client or meeting the evolving needs of existing clients in these industries is becoming a challenge for law firms.

What's next for the legal industry?
Today, more law firms are receiving cyber due diligence questionnaires (DDQs) from their clients. Regulators such as the SEC have tightened their rules with implications for vendors and specifically, legal services. In fact, SEC regulations, HIPAA and PII all have disclosure requirements, meaning that a law firm cannot quietly go about business while keeping security breaches out of the press.

Where to start?

1. Get to know your clients' business operations and understand their regulatory obligations and cyber requirements.
2. Familiarize yourself with cybersecurity frameworks such as NIST (National Institution for Standards and Technology) and SIG (Standard Information Gathering).
3. Check out our NIST Workbook to better understand the requirements and your gaps.
4. Get a copy of the ABA cybersecurity handbook for legal professionals which covers recommendations firms should consider.

Download our ABA Workbook to help you understand the guidelines and priorities. ▶

Be Prepared for your Next Due Diligence Questionnaire (DDQ)

What is a DDQ?

There is a growing trend for businesses who are working with third parties. Many of these business relationships share sensitive information. The DDQ ensures the third party risk is assessed and their security practices are up to the organization's standards, which are set by their own governing bodies. For example, a hedge fund follows the SEC standards, and in return the law firm they work with would also have to follow those same standards.

How can your firm prepare?

With DDQs growing in popularity, it's important that your firm is prepared to respond to them. Familiarize yourself with the various regulators your clients report to. Depending on the organization, DDQs can be more adhoc (conversations with key business stakeholders), or more formal (questionnaire style assessment). The extent of the evaluation may depend on the multiple factors in the relationship.

Creating your own DDQ: where do you start?

It's time the legal industry creates their own security DDQ. Start by using tools like the ABA Cybersecurity Handbook and the plethora of resources available through the ILTA LegalSec Council. There are also resources that the Alternative Investment Management Association (AIMA) has created to standardized security DDQs. The AIMA framework gives investors and clients a way of accurately measuring those firms and their cybersecurity policies and procedures.

5. https://www.law360.com/articles/705657/1-in-4-law-firms-are-victims-of-a-data-breach

Cybersecurity posture: are you prepared for the inevitable breach?

Best Practices for Preparing for a Cyber Breach

Law firms are facing the question, “are we prepared for a security breach?” Many are unable to successfully answer that question and are still in the mindset that they will never be hacked because they’re simply too small. Today’s reality is, being hacked is no longer a question of if, but when. Consider these eleven security best practices:

IDENTIFY
COMMON ATTACKS

DEVELOP
AN ACCEPTABLE USE POLICY (AUP)

ENFORCE
RIGOROUS PASSWORD POLICY

MINIMIZE
ADMIN PRIVILEGES

PATCH
SYSTEMS REGULARLY

VALIDATE
SECURITY SYSTEMS FUNCTIONING

PERFORM
REGULAR BACKUPS

LOG
SYSTEM ACCESS

PERFORM
VULNERABILITY ASSESSMENTS

MONITOR
NETWORK TRAFFIC

VALIDATE
PHYSICAL SECURITY

Is ransomware a concern? Check out our eBook for an actionable list of best practices in protecting your firm. ▶

esentire

Training: is your weakest link exposed?

Security Awareness Training

The size of your firm is irrelevant when it comes to social engineering and phishing attacks. Firms are only as strong as their weakest link. Your firm could have the best firewall and anti-virus systems in the industry, but human error can easily expose your network and client information to a lurking cybercriminal.

Firms can reduce their chances of human error through various levels of security awareness training. You can arm your employees with the warning signs of how to spot a phishing email. With this knowledge they know what to look out for, who to notify if they are targeted and how to eliminate the threat before a potential zero day attack strikes. The trick to security awareness training is that there is no end date. Attacks evolve quickly; so too should your awareness training. Staying current with the latest training available is crucial to your firm's security.

19%

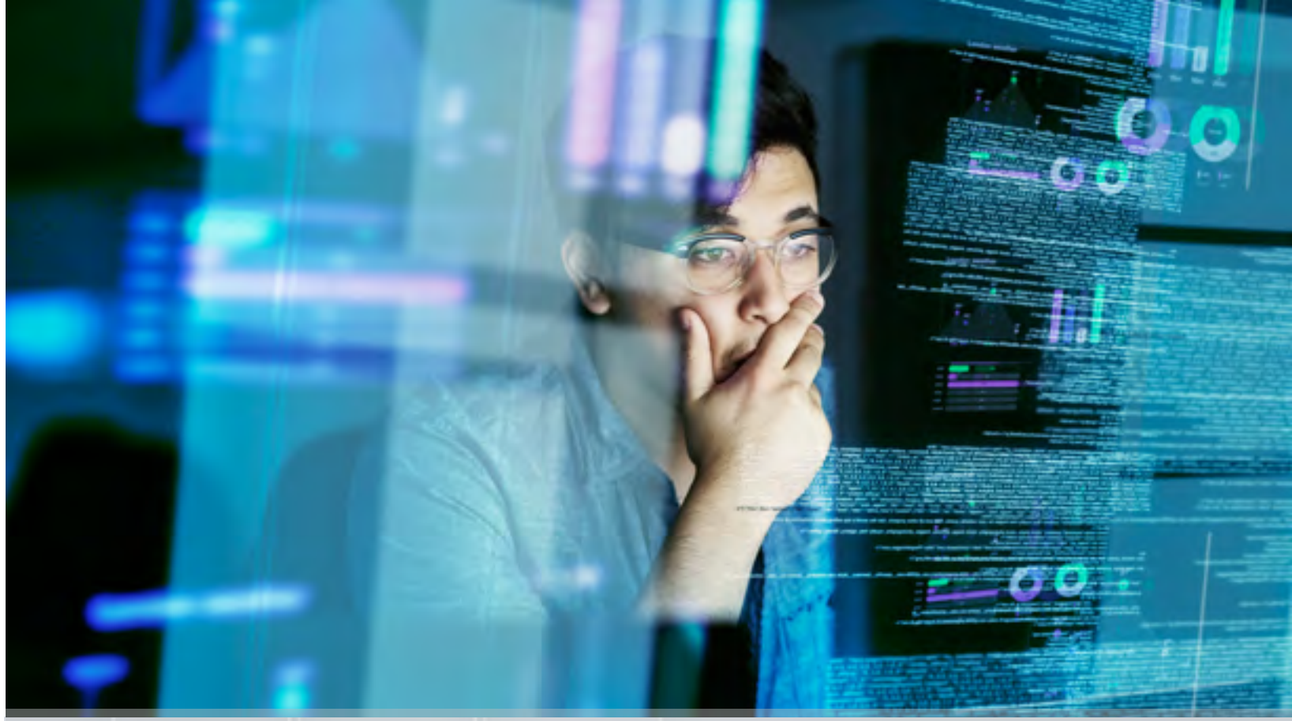
of employees will fall victim to spear-phishing and social engineering attack.

Incident response planning: you've just been breached - now what?

Best Practices for an Incident Response Plan

Your firm has just been breached. Now what? An incident response plan/policy is crucial to a firm's ability to remediate post breach. A thorough response plan requires a lot of up-front thinking and documentation, but the payoff, comes from having a roadmap to follow when a cyber-attack erupts inside your network. When building or updating your incident response plan, be sure to:

- Identify your response team
- Prepare mitigation plans for different cyber-attack categories
- Determine internal and external communication procedures
- Assemble the tools and resources needed to deal with the attack
- Implement remediation procedures
- Evaluate results and improve cyber defenses accordingly



esentire®

We defend against the threats facing law firms

At eSentire, we work with clients ranging from small practices to the AM Law 200. This gives us a unique perspective on the types of attacks that law firms face and how to detect and mitigate them.

We detect, analyze, interpret, classify, isolate and report on suspicious and malicious activity on your endpoints and network.

Our high-touch, turn-key service is designed to ensure your organization assumes the minimal amount of risk possible.

We reduce the time to respond and recover so your organization can return to a known state of good without disruption to your business.

eSentire Managed Detection and Response™ (MDR)

- **24x7x365** continuous hunting and monitoring
- **Detection of unknown attacks** leveraging patterns and behavioral analytics
- **Human-led investigation** utilizing always on full packet capture, logs and event data
- **Full forensics analysis** to confirm threats and eliminate false positives
- **Isolation and communication disruption** of the threat on your behalf, with no retainer fee
- **Full remediation support** until the threat is eliminated, not just alerting and guidance

See what you're missing

Your ability to avoid a business-altering event depends on how fast you detect and respond to a cyber breach. **Contact us** to discuss your cybersecurity and compliance needs.

About eSentire:

eSentire® is the largest pure-play Managed Detection and Response (MDR) service provider, keeping organizations safe from constantly evolving cyber-attacks that technology alone cannot prevent. Its 24x7 Security Operations Center (SOC), staffed by elite security analysts, hunts, investigates, and responds in real-time to known and unknown threats before they become business disrupting events. Protecting more than $3 trillion in corporate assets, eSentire absorbs the complexity of cybersecurity, delivering enterprise-grade protection and the ability to comply with growing regulatory requirements.

For more information, visit www.esentire.com and follow @eSentire.