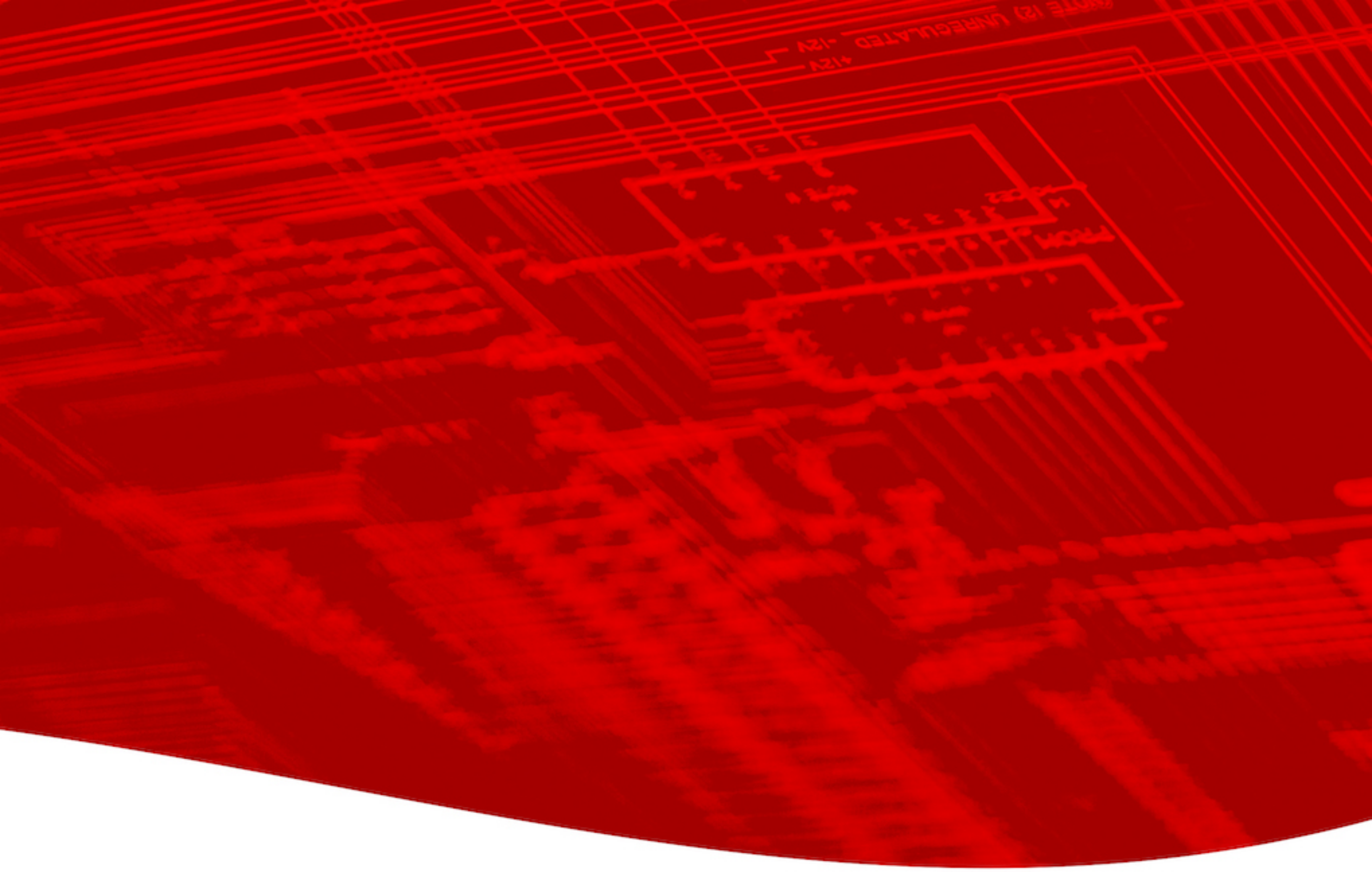

LAW FIRM
CYBERSECURITY SCORECARD 2019

LOGICFORCE

LEGAL. TECHNOLOGY. RESULTS.

TABLE OF CONTENTS

LAW FIRM CYBERSECURITY SCORECARD

TERMS & CONDITIONS

All content contained in this document is the intellectual property of LOGICFORCE. By using this document, you agree to the following terms and conditions. 1. You may download, print, and copy this report one time for your personal use provided that you retain all copyright notices and do not modify the e-book in any way. 2. This report is provided "as is" without any warranties of any kind whatsoever, including warranties of title or fitness for a particular purpose. LOGICFORCE makes no warranties of any results that may be obtained from the use of this report. 3. In no event will LOGICFORCE, the authors, or any officers, employees, or agents of LOGICFORCE be liable for any indirect, consequential, special, incidental, or punitive damages from the use of this report.

If you cannot abide by these terms and conditions than you agree to, and are hereby charged with, destroying all copies, both electronic and physical, of this report. **LOGICFORCE vigorously defends our intellectual property and copyrighted material and will prosecute offenders to the full extent of the law.**

RATIONALE

Data breaches continue to plague law firms across the world regardless of the number of attorneys, revenues or practice areas. The Law Firm Cybersecurity Scorecard is developed by LOGICFORCE and published regularly to educate the legal industry on the current state of cybersecurity preparedness.

LOGICFORCE cybersecurity experts are seeing more law firms provide training and issue cybersecurity and data governance policies with emphasis on ensuring their lawyers meet the ethical duties stipulated in the ABA Model Rules of Professional Conduct, specifically Rule 1.1 and Rule 1.6.

However, many law firms remain reluctant to implement information security best practices which are critical to the cybersecurity health of their respective businesses. We believe their reluctance to invest in these mission critical initiatives is primarily due to the expense control provisions most law firms have implemented over time due to the stagnation of profits that have plagued the legal industry for almost a decade. This is a risky proposition, and we predict law firms will continue to be a focal target of cyber criminals.

Based on the findings of our previous Cybersecurity Scorecards, our contention is that law firms' increased prioritization of comprehensive cybersecurity programs is being driven primarily by the demands of their corporate clients and the need to keep their sensitive data protected. We are seeing that cybersecurity is no longer a concern of only regulated industries - it is now a top priority in boardrooms around the world.

Our intention is to continue to advocate meaningful dialogue throughout the legal industry about cybersecurity issues plaguing law firms and their corporate clients to promote substantive change for the better, by gaining buy-in and adherence to the Cybersecurity and Data Management Standards outlined in the Law Firm Cybersecurity Scorecard.

METHODOLOGY

The information in this study is a compilation of critical data points and expert insight determined by LOGICFORCE and gathered through client surveys, our proprietary SYNTHESIS E-IT SECURE assessments, and market research. They were specifically selected by our security experts to accurately reflect the current efforts by law firms to limit risk of exposure to breach and subsequent loss of data according to the cybersecurity standards we have established as the baseline for well-managed legal IT operations. LOGICFORCE commissioned a survey and assessed more than 200 IT decision makers, including CIOs, IT directors and information security managers across small and medium-sized law firms (20-200 attorneys) located throughout the United States.

BY TITLE, OUR 2019 SURVEY AUDIENCE INCLUDES:

IT DIRECTORS OR MANAGERS

CIOs/CTOs

INFORMATION SECURITY MANAGERS

PARTNERS, COUNSEL AND LEGAL ADVISORS

KEY FINDINGS

THE LEGAL INDUSTRY SCORE FOR CYBERSECURITY HEALTH AMONG LAW FIRMS HAS INCREASED FROM 54% IN 2018 TO 60% IN 2019.

This positive movement is largely attributable to law firms' improved adoption of formal cybersecurity policies and training this year. The percentage of law firms that have formally documented cybersecurity policies increased from 55% in 2018 to 70% in 2019. In addition, about 7 in 10 law firms (68%) have invested in formal cybersecurity training for their employees, up 14 points from last year (54%).

MANY LAW FIRMS FAIL TO IMPLEMENT CRITICAL RISK PREVENTION AND MONITORING STANDARDS.

The legal industry remains very vulnerable to cyberattacks, not only because of its low adoption of these critical practices but also due to the fact law firms hold extremely sensitive client information that is valuable to hackers. Compared to 2018, fewer law firms report implementing more advanced cyber-risk prevention techniques such as Data Loss Prevention (DLP) technology (21% in 2019 vs. 47% in 2018) and multi-factor authentication (36% in 2019 vs. 47% in 2018) this year. Only 39% of law firms currently implemented full disk encryption on all devices.

Law firms are also lagging when it comes to risk monitoring. While most have records management policies, only 54% say they include electronically stored information. In addition, only about 1/3 of law firms (34%) have designated personnel to monitor the event logs collected on all devices. Low implementation scores for both 2018 and 2019 indicate that it is not currently a strategic priority for law firms. A change in cybersecurity leadership may be needed to help make the recommended shift.

TO BATTLE INCREASINGLY COMPLEX CYBER-RISKS, LAW FIRMS NEED THE RIGHT PERSONNEL TO LEAD THEIR MULTI-DIMENSIONAL CYBERSECURITY PRACTICES.

Only about half (49%) of law firms have an information security officer who is responsible for their cybersecurity practices. Many still rely on IT managers or non-IT executives who may not have the specialized knowledge and expertise to design and implement proper cybersecurity policies and standards.

People and processes are the foundation of mature cybersecurity programs. Firms must have policies that focus on best practices and governance and subsequently train all employees on these policies or

KEY FINDINGS

the technology will be of little use in protecting the firm. Setting the right tone for cybersecurity from the top is critical. It's recommended that small and medium-sized law firms take a step further and hire information security professionals or a reputable third-party security officer who has the right knowledge and skills to implement cybersecurity practices and protocols that cover risk assessment, threat prevention and incident response.

CLIENT AUDITS DEMAND IMPROVED CYBERSECURITY BEST PRACTICES

Over half (51%) of the firms surveyed have been audited at least once in the last year by a client or potential client. While this is nothing new, we've seen an increase in the amount of effort required in the response - a yes or no answer will no longer suffice. Today, clients are asking for more details including whether a firm has policies regarding how data is processed and handled, what the retention policies are and whether employees are trained on secure data practices.

LAW FIRM CYBERSECURITY STANDARDS

Cyber criminals are finding more ways to steal data and continue to target law firms. How can clients trust firms who can't secure their private information?

LOGICFORCE believes law firms will not realize the most secure environment or satisfy corporate clients unless they fully adopt these 12 Cybersecurity Standards.

INFORMATION SECURITY EXECUTIVE

Law firms should have a credentialed senior-level executive with the designated responsibility of establishing and maintaining the enterprise vision and strategy of a comprehensive cybersecurity program for the entire organization to ensure information assets, systems and technologies are adequately protected.

STATE OF THE INDUSTRY TODAY:

While more law firms are making better hires compared to last year (34%), only about half (49%) today have an information security officer or manager who is responsible for their cybersecurity practices. The rest of them still rely on IT managers or non-IT executives who may not have the specialized knowledge and expertise to design and implement proper cybersecurity policies and standards.

CYBERSECURITY POLICIES AND BACKUP PROCEDURES

The law firm's cybersecurity policy should be documented, accessible, and understood by all employees. Backup procedures and the restoration process should be tested quarterly. Both should be reviewed, maintained and revised on a periodic basis.

STATE OF THE INDUSTRY TODAY:

This year, 70% of law firms report having formally documented cybersecurity policies, as many have shifted from their informal policy practices. This corresponds with a rise in information security professionals, as law firms are getting more serious about governing their cybersecurity approach.

LAW FIRM CYBERSECURITY STANDARDS

MULTI-FACTOR AUTHENTICATION

Multi-factor Authentication (MFA) is a method of computer access control which requires users to provide authentication methods from at least two of the following categories: knowledge (something they know), possession (something they have), and inherence (something they are).

STATE OF THE INDUSTRY TODAY:

Most law firms today are not using multi-factor authentication, meaning more than a password, to protect their important documents or resources. Last year, over half of law firms (53%) said they would implement this practice in the future, but the implementation score remains low today.

According to the Verizon 2019 Data Breach Investigation Report, stolen credentials remain one of the most prominent channels for hacking-related breaches. MFA is a simple addition to a cybersecurity program that can combat credential related attacks with little impact on the user experience.

CYBER TRAINING

Cybersecurity training programs establish safe and secure methods to carry out user's daily responsibilities and heighten awareness of common practices to gain unlawful access to systems. Training programs should be mandatory for all employees and conducted regularly.

STATE OF THE INDUSTRY TODAY:

Law firms are now more likely to offer formally documented cybersecurity training and less likely to offer informal training when compared to 2018. This is a noticeable increase from last year, with 68% law firms offering formal training.

CYBER INSURANCE

A proper cybersecurity insurance policy should include reimbursement for investigation, business loss, required notification and credit monitoring to clients, legal expenses, cost of extortion and cover human error where

LAW FIRM CYBERSECURITY STANDARDS

STATE OF THE INDUSTRY TODAY:

Today, 2 in 5 law firms still don't have insurance to protect them from potential data breaches.

PENETRATION AND VULNERABILITY TESTING

Penetration testing examines your perimeter defenses and actively seeks out weak security settings and requires a high-level of expertise. Vulnerability testing, which includes scanning all networked devices for potential vulnerabilities, should be completed on a regular basis, as often as once a week.

STATE OF THE INDUSTRY TODAY:

Over 4 in 5 law firms (83%) conduct vulnerability testing, with most of them performing internal tests (62%). Of those that do not, most say they plan to do so in the future.

PASSWORD MANAGEMENT TOOL

A password management tool generates strong passwords and encrypts and secures all passwords.

STATE OF THE INDUSTRY TODAY:

Password management is a common practice of the legal industry today. Almost all (98%) law firms use a password management tool to protect their data.

RECORDS MANAGEMENT POLICY

This policy should define responsibilities and assign them accordingly, define what a record is and how it is categorized, provide a framework for systematic retention and defensible records destruction practices that include electronically stored information "ESI".

LAW FIRM CYBERSECURITY STANDARDS

STATE OF THE INDUSTRY TODAY:

Nearly all law firms (99%) surveyed have a records management policy in place; however, only about half (54%) currently include electronically stored information in their records management policy – a practice recommended for better cybersecurity management. This is a decline from 2018.

SECURITY OPERATIONS CENTER MONITORING

Security Operations Centers (SOC) monitoring is a facility where a firm's information systems including websites, databases, networks and other end points are monitored to detect and respond to cyber threats.

STATE OF THE INDUSTRY TODAY:

Among all the law firms surveyed, only 34% currently have designated personnel to constantly monitor event logs collected from all devices. More than half of law firms (58%) don't even collect event logs from all devices at all.

FULL DISK ENCRYPTION

Full Disk Encryption (FDE) implies encryption at the hardware level on all equipment that contains law firm information including mobile devices.

STATE OF THE INDUSTRY TODAY:

Full disk encryption needs to be implemented across all computers, servers and storage systems and mobile devices to effectively protect law firms from unauthorized access. However, only about 2 in 5 law firms (39%) currently do this.

LAW FIRM CYBERSECURITY STANDARDS

DATA LOSS PREVENTION SERVICES

Data loss prevention (DLP) is a technology that scans documents, emails and other types of data leaving the law firm for things like Social Security numbers, PII, PHI, and blocks the transmission of data if these types of patterns are found. DLP can also include scanning data going onto removable media for physical transport.

STATE OF THE INDUSTRY TODAY:

Only about 1 in 5 (21%) law firms are currently using DLP technology to protect their personally identifiable information, a noticeable drop from 2018.

THIRD-PARTY RISK ASSESSMENTS

A third-party risk assessment is an audit conducted of third-party service provider's systems and data security practices to ensure they are in adherence with the cybersecurity and data management policies of the law firm.

STATE OF THE INDUSTRY TODAY:

Conducting a risk assessment on third-party providers is widely accepted within the legal industry today. Currently, 9 out of 10 law firms perform risk assessments on their third-party providers, and most of them do so through a third-party (62%). The rest of the law firms have plans to conduct the assessment in the future.

INDUSTRY SCORE

LOGICFORCE'S LAW FIRM CYBERSECURITY SCORECARD CALCULATES AN "INDUSTRY SCORE" THAT REFLECTS THE HEALTH OF CYBERSECURITY PRACTICES ACROSS THE LEGAL INDUSTRY.

The 2019 legal industry score for cybersecurity health is 60.1%. While we see some improvement in cybersecurity leadership and governance, law firms are behind on more advanced measures such asDLP, multi-factor authentication, and records management.

2019 INDUSTRY SCORE: 60.10%

2018 INDUSTRY SCORE: 54.25%

CATEGORY	WEIGHTED VALUE	2019 WEIGHTED AVG.	2019 IMPLEMENTATION SCORE	2018 IMPLEMENTATION SCORE
Cybersecurity Investment	5%	5	100%	99%
Password Management Security	5%	4.9	98%	99%
3rd Party Risk Assessment	10%	9	90%	-
Penetration Testing	5%	4.3	86%	-
Vulnerability Testing	5%	4.15	83%	-
Cybersecurity Policies	5%	3.5	70%	55%
Formal Training	10%	6.8	68%	54%
Cybersecurity Insurance	5%	3.05	61%	65%
Records Management Policy	5%	2.7	54%	65%
Proper Security Executive	10%	4.9	49%	34%
Full Disk Ecyrption	5%	1.95	39%	40%
Multi-Factor Authentication	15%	5.4	36%	47%
Monitoring (SOC)	10%	3.4	34%	24%
DLP Technology	5%	1.05	21%	47%

SCORING: The values found in the "Implementation Score" column indicate the percentage of implementation for each category across the legal industry. The values found in the "weighted value" column is based on LOGICFORCE's assigned level of importance for each mediation technique. The "weighted Average" for each category is calculated by multiplying the "Implementation Score" for each category by the respective categories' "weighted Average". The "Industry Score" is then calculated by summing the "weighted Average" for each category.

ANALYSIS

TO STRENGTHEN DEFENSES AND STAND OUT AS A SUPERIOR LEGAL SERVICE PROVIDER, IT'S IMPERATIVE THAT LAW FIRMS ADOPT CYBERSECURITY PROTOCOLS THAT PRESERVE CLIENT TRUST AND PROTECT THEIR MOST SENSITIVE DATA.

Not only can a breach cripple a firm's reputation and shake its client base, but there are also significant financial consequences. According to IBM, companies with less than 500 employees suffered losses of more than $2.5 million on average – a potentially crippling amount for small businesses, which typically earn $50 million or less in annual revenue.

We're continuing to see improvement in the overall score year-over-year. Areas of improvement from 2018 to 2019 include implementing formal cybersecurity policies, up 15% this year, formal staff training, up 14%, and engaging a proper security executive, up 15% from last year. Growth in these areas points to an improved foundation of which law firms are building their cybersecurity programs on, leading to increased use and effectiveness of the technology and tools used when developing cybersecurity protocols. In addition to proper technology, the people and processes are the foundation of a solid cybersecurity program. Firms must continue to focus on best practices and governance and t rain employees on their policies.

However, there are still many firms failing to implement many cybersecurity best practices. The areas facing decline that signal major concern include the use of a records management policy, down 11%, the use of multi-factor authentication (MFA), also down 11%, and the use of data loss prevention technology (DLP), down 26%. Neglecting the use of these technologies poses a problem for law firms attempting to pass client audits.

Not only did about half of the firms surveyed this year report that they have been audited at least once, but we're finding that clients are requiring increased proof of data protection from law firms. They're now asking detailed questions about retention policies, types of security technologies used, names of staff that will have access to their data and staff training practices. Increased investment in cybersecurity best practices may help increase implementation of these technologies. However, for law firms to acquire new business and remain a trusted ally to their clients, improvement in these areas is critical.

RECOMMENDATIONS

To combat the threat of cyber breaches, we recommend taking the following actions:

PLAN & STRATEGIZE:

- Appoint a CISO/CIO or partner with a MSSP to provide vCISO/vCIO service to assure a qualified individual is steering the cybersecurity ship.
- Organize a cross functional team consisting of law firm management, practice chairs, IT, procurement, administration, and human resources.
- Create, or review and update, firmwide cybersecurity policies. Be sure acceptable use, passwords, exceptions, data loss prevention, mobile device management, business continuity, incident response, and records management are all covered topics.
- Build a training program to assure all employees understand all policies and procedures.

ASSESS CURRENT TOOLS & PROTOCOLS:

- Implement multifactor authentication for any application that can be accessed directly from the Internet.
- Procure cyber insurance, as most general liability policies and professional liability policies now expressly exclude coverage for data breach claims.
- Provide a password management application to enable users to more easily adhere to stringent password policies.
- Implement a data loss prevention system to help enforce records management policies.

CONDUCT ONGOING REVIEWS & TRAINING:

- Have a third-party IT security expert run an annual risk assessment and penetration test on your firm's technology systems. Remediate identified deficiencies.
- Develop and schedule regular training to enforce policies and increase efficiencies.
- Conduct monthly vulnerability testing to ensure systems are protected from the latest known threats.
- Implement a monitoring solution that can alert to any breaches in security or abnormalities in the IT infrastructure.

ABOUT LOGICFORCE

LOGICFORCE has provided comprehensive information technology services to midsize law firms across the country since 1995. Our New Style Legal IT® (NSLIT) offering is a fresh approach for law firms looking to realize new operating efficiencies and significantly enhance business development. Our teams use a proprietary methodology known as Synthesis E-IT Secure® to assess and reengineer legal operations with a scalable design to accommodate every organization's unique work demands, while maximizing efficiency and boosting profitability in a cyber secure environment.

With more than 20 years of experience in the legal industry, we provide expert-level technology services for unique litigation technology needs. Our litigation support services include e-Discovery collections, processing, hosting, project management, and trial tech support. Our digital forensics lab provides expert-level forensic analysis and testimony for both large and small matters. We are a holistic solution for law firms that find it cost prohibitive to insource all the services that we provide or frustrating to manage a shifting landscape of many vendors that supply these services.

For more information about this report or to contact us, please email us directly at contact@LOGICFORCE.com or call (615) 238-3539.

LOGICFORCE

LEGAL. TECHNOLOGY. RESULTS.