# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rationale</td>
<td>2</td>
</tr>
<tr>
<td>Methodology</td>
<td>3</td>
</tr>
<tr>
<td>Key Findings</td>
<td>4</td>
</tr>
<tr>
<td>Law Firm Industry Score</td>
<td>11</td>
</tr>
<tr>
<td>Analysis</td>
<td>12</td>
</tr>
<tr>
<td>Recommendations</td>
<td>13</td>
</tr>
<tr>
<td>About LOGICFORCE</td>
<td>15</td>
</tr>
</tbody>
</table>

---

**LAW FIRM CYBERSECURITY SCORECARD**

© Copyright 2018, LOGICFORCE. All rights reserved.

**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 have become a risk to every law firm throughout 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 hire Information Security Officers, which is a critical factor to the cybersecurity health of their respective businesses. We believe their reluctance to invest in this mission critical resource 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 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 across small and medium-sized law firms (20-200 attorneys) located throughout the United States.
KEY FINDINGS

Most law firms aren’t implementing top-weighted cybersecurity protocols.
Less than half of law firms are implementing some of the top-weighted cybersecurity protocols – these being multifactor authentication (47%), 3rd party risk assessment (37%), having the proper security executive (34%), and SOC monitoring (24%).

Many law firms don’t have formal measures in place to keep their data secure.
The majority of law firms are investing in certain cybersecurity measures, such as penetration and vulnerability testing (88%) and have some sort of password management tool in place (99%). However, fewer law firms are investing in more formal cybersecurity areas. For example, 36% of firms do not have cybersecurity insurance, 45% of firms do not have formal cybersecurity policies, and 46% do not have cybersecurity training formally documented.

The majority of law firms require better cybersecurity management.
Currently, the majority (67%) of law firms place the responsibilities for implementing and managing cybersecurity policies on either IT Directors or Managers or some other non-IT executive at the firm. Roughly 1 in 3 (34%) firms leave these responsibilities to personnel who have specialized knowledge on cybersecurity, such as a Chief Information Security Officer or an Information Security Manager.

Recent American Bar Association opinion reaffirms lawyers’ duty to protect client information.
In Formal Opinion 483, issued in October 2018, the American Bar Association (ABA) states that lawyers are ethically obligated to monitor data breaches and notify current and former clients if data is compromised.

“As a matter of preparation and best practices, however, lawyers should consider proactively developing an incident response plan with specific plans and procedures for responding to a data breach,” states the opinion. “The decision whether to adopt a plan, the content of any plan and actions taken to train and prepare for implementation of the plan should be made before a lawyer is swept up in an actual breach.”
Big law firms have been the target of cyberattacks in recent years. Twenty-two percent of law firms were attacked in 2017, which is a 14% increase from the previous year, according to the ABA 2017 Legal Technology Survey. Law firms are particularly vulnerable to breaches because their servers hold incredibly sensitive and private information, and many don’t invest the capital to properly secure their data.

As part of this recent opinion, the ABA provided new guidance to help attorneys take reasonable steps to meet this obligation, including proactively developing an incident response plan with strategies for responding to a data breach.

LOGICFORCE finds that most law firms don’t have response plans or necessary cybersecurity and backup procedures in place, which means their business and clients are at risk. The complexity of cybersecurity assaults is constantly expanding. Understanding this growing complexity of technology solutions, software, security threats and threat management requires a high level of real-time legal and tech industry expertise.

Preparedness is the best way to help prevent and lessen the blow of cyber-attacks. This report provides data and recommendations that will protect your clients, business and reputation.
Law Firm Cybersecurity Standards

LOGICFORCE believes law firms will not realize the most secure environment or satisfy corporate clients unless they fully adopt these 12 cybersecurity standards:

1. INFORMATION SECURITY EXECUTIVE

This is defined as 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: More than 3 in 4 (76%) do not have a designated person monitoring event logs from all devices at the firm. 34% of law firms have a proper security executive.

2. CYBERSECURITY POLICIES & 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: 55% of law firms surveyed have documented policies and procedures.
MULTIFACTOR AUTHENTICATION

Multifactor 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: 47% of law firms currently use multifactor authentication to access documents or resources.

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: 54% of law firms have formally documented training programs for staff.
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 possible.

State of The Industry Today: 65% of law firms have cybersecurity insurance policies.

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

State of The Industry Today: 88% of law firms conduct penetration and vulnerability testing, but less than half have sourced a qualified third-party provider.

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

State of The Industry Today: Nearly all firms (99%) have some sort of password management tool in place.
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: 24% of law firms have implemented SOC monitoring.
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: 37% of law firms are vetting the cybersecurity and data management policies of their third-party service providers.
LAW FIRM INDUSTRY SCORE

LOGICFORCE's Law Firm Cybersecurity Scorecard calculates an "Industry Score" that reflects the health of cybersecurity practices across the legal industry.

<table>
<thead>
<tr>
<th>Categories</th>
<th>Implementation Score</th>
<th>Weighted Value</th>
<th>Weighted Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>PASSWORD MGMT. SECURITY</td>
<td>99%</td>
<td>5%</td>
<td>4.95</td>
</tr>
<tr>
<td>PENETRATION &amp; VULNERABILITY TESTING</td>
<td>88%</td>
<td>10%</td>
<td>8.8</td>
</tr>
<tr>
<td>CYBERSECURITY INSURANCE</td>
<td>65%</td>
<td>5%</td>
<td>3.25</td>
</tr>
<tr>
<td>RECORDS MANAGEMENT POLICY</td>
<td>64%</td>
<td>5%</td>
<td>3.2</td>
</tr>
<tr>
<td>CYBERSECURITY POLICIES</td>
<td>55%</td>
<td>10%</td>
<td>5.5</td>
</tr>
<tr>
<td>FORMAL TRAINING</td>
<td>54%</td>
<td>10%</td>
<td>5.4</td>
</tr>
<tr>
<td>DLP TECHNOLOGY</td>
<td>47%</td>
<td>5%</td>
<td>2.35</td>
</tr>
<tr>
<td>MULTI-FACTOR AUTHENTICATION</td>
<td>47%</td>
<td>15%</td>
<td>7.05</td>
</tr>
<tr>
<td>FULL DISK ENCRYPTION</td>
<td>40%</td>
<td>5%</td>
<td>2</td>
</tr>
<tr>
<td>3RD PARTY RISK ASSESSMENT</td>
<td>37%</td>
<td>10%</td>
<td>3.7</td>
</tr>
<tr>
<td>PROPER SECURITY EXECUTIVE</td>
<td>34%</td>
<td>10%</td>
<td>3.4</td>
</tr>
<tr>
<td>MONITORING (SOC)</td>
<td>24%</td>
<td>10%</td>
<td>2.4</td>
</tr>
</tbody>
</table>

The scoring system is designed to illustrate how well law firms are implementing the 12 most critical systems and data security mediation methods according to LOGICFORCE Cybersecurity Standards for a secure law firm.

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.

INDUSTRY SCORE 52%
ANSALYSIS

While we continue to see improvements in cybersecurity preparedness, most law firms are not implementing many of the protocols that will comprehensively protect them and their clients over time. This is a major concern since many firms’ clients and potential clients are not shy about demanding secure data practices. Fifty-four percent of law firms report being audited by one or more clients at least once – a 13% increase since the last scorecard.

There are clear areas of improvement and we anticipate that they will continue to strengthen. Since the last scorecard, there has been a 22% increase in law firms that report having formal cybersecurity training (54%). We have also seen a significant increase in firms that report having cybersecurity insurance: 65% of firms now incorporate cybersecurity insurance in preparedness efforts, up from 41% since the last scorecard.

Rapidly changing technology and modes of cyberattack demand that law firms treat cybersecurity as a core component of their legal practice. To strengthen defenses, it’s imperative that law firms adopt cybersecurity protocols that preserve client trust, protect the most sensitive data and, ultimately, allow them to stand out as legal services providers.
RECOMMENDATIONS

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

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.

→ Enable encryption on all devices, including laptops, desktops, phones, tablets, and anything else that can potentially store sensitive information.

→ Implement data loss protection systems, which are critical for identifying sensitive data leaving the law firm.

→ Set up a network security perimeter to block penetration from outsiders and install endpoint protection to protect the devices themselves.

Plan & strategize:

→ Organize a cross functional team consisting of law firm management, practice chairs, IT, procurement, administration, and human resources.

→ Set the tone for cybersecurity from the top and appoint a CISO/CIO to be the person in charge.

→ Create a plan and next steps if your law firm is hacked, including contact information for IT advisors and technical experts to guide you through this process.

→ Establish an incident response team including management, Internet service providers, law enforcement, insurance providers, public relations, legal advisors, technical and forensic experts.

→ Implement a communication strategy to notify employees and clients that may be affected.
Conduct ongoing reviews & training:

→ Have an IT security expert regularly run a risk assessment on your firm’s technology systems.

→ Schedule regular training programs for all staff.

→ Create security policies that align with where the law firm is today and update as the security posture changes.

→ Conduct a yearly penetration test by an independent third party. Penetration testing can show gaps in current technical controls, or weaknesses in training programs.

→ Conduct monthly vulnerability testing to ensure systems are protected from the latest known threats.
ABOUT LOGICFORCE

LOGICFORCE has provided comprehensive information technology services to the legal industry 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 space, 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.