Legal Cybersecurity Checklist

Meeting your clients' compliance requirements is becoming a regular part of doing business. The challenge is that there are no regulated mandates for cybersecurity policies and procedures in the legal industry, so firms are left to figure it out on their own.

Are you prepared?

From trade secrets to client information, you have an ethical and legal obligation to protect your firm's privileged data. Cyber-attackers who struggle to breach an organization's network more commonly see their outside counsel as an easy target.

Unfortunately, cybersecurity is an inherently difficult problem in the legal industry. Recent breaches have put third-party due diligence in the spotlight and as a result, legal firms are being held to the various regulatory obligations of their clients (e.g. HIPAA, GDPR, PCI, FINRA and SEC). And, cybersecurity isn't always top of mind, as firms naturally focus their investment on client defense, rather than cyber protection.

This evolution in client requirements has led to new selection criteria for doing business with a firm. While due diligence is a common exercise, there's no common framework or regulated mandates for cybersecurity policies and procedures that firms can adopt that meets all clients' regulatory requirements.

To help legal firms meet client requirements, we've developed a checklist based on the six pillars laid out in *The ABA Cybersecurity Handbook*.

31%

more targeted malware attacks than other industries[1]

62%

of firms over 500 lawyers provided with cybersecurity requirements by their clients[2]

40%

of law firms breached in 2016 didn't even know about it[3]

$134K

Average cost of a breach

Do your cybersecurity measures meet your clients' compliance requirements?

Review your security approach with one of our security experts.

GET STARTED

[1]2016 eSentire Legal Threat Summary Report
[2]ABA Journal, March 2017
[3]LOGICFORCE Law Firm Cybersecurity Scorecard

Build Your Cybersecurity Program

The Legal Cybersecurity Checklist will help you understand your legal obligations, meet your client's third-party requirements and detect and respond to security threats in real-time.

Part 1: Cybersecurity Governance		eSentire Advisory Services	eSentire MDR
1.0	Cybersecurity Governance	✓	
1.A	Chief Information Security Officer or Equivalent	✓	
1.B	Cybersecurity Governance Committee (CGC)	✓	
1.C	Documented Cybersecurity Roles/Responsibilities	✓	
1.D	Documented Cybersecurity Risk Profile	✓	
1.E	Documented Cybersecurity Program	✓	
1.F	Documented Business Continuity Plan (BCP)	✓	
1.G	Documented Incident Response (IR) Plan	✓	
2.0	Classify/Inventory Information Assets	✓	
2.A	Identify Attorney-Client Data	✓	
2.B	Identify Personal Data/Identifiable Info (PD/PII)	✓	
2.C	Identify Sensitive Financial Data	✓	
2.D	Identify Transaction Records	✓	
2.E	Identify Tax Records	✓	
3.0	Map Regulatory Requirements	✓	
3.A	Map of Federal Regulations (HIPAA/GLBA) to Info Assets	✓	
3.B	Map of Jurisdictions in Which Firm/Clients Operate	✓	
3.C	Map of Federal Statutes (Appendix A)	✓	
3.D	Map of State Statutes (Appendix B)	✓	
4.0	Cyber Liability Insurance		
4.A	Documented Policy & Carrier		
4.B	First Party Loss Coverage		
4.C	Third Party Loss/Professional Liability		

Part II: Risk Assessment		eSentire Advisory Services	eSentire MDR
1.0	Conduct a Risk Profile	✓	
1.A	Identify Cyber Attack Targets (Assets)	✓	
1.B	Identify Likely Cyber Attack Vectors	✓	
1.C	Identify Internal Threat Actors		✓
1.D	Identify External Threat Actors		✓
1.E	Evaluate Potential Resulting Damages	✓	

Part II: Risk Assessment Con't		eSentire Advisory Services	eSentire MDR
2.0	Periodic Cybersecurity Vulnerability Assessment	✓	
2.A	Assessment Details (Who/Date)	✓	
2.B	Describe High to Critical Risks	✓	
2.C	Penetration Testing Details (Results/Date)	✓	
3.0	Periodic Physical Vulnerability Assessment		
3.A	Assessment Details (Who/Date)		
3.B	Describe High to Critical Risks		
4.0	Test Environment for New Software/Applications	✓	
4.A	Test/Dev for New Software	✓	
4.B	Test/Dev for Web Application	✓	
Part III: Protection of Network and Data		**eSentire Advisory Services**	**eSentire MDR**
1.0	Risk Management Models (NIST/ISO) & Strategy	✓	
2.0	Network and Security Assets	✓	
2.A	Inventory Physical Devices and Systems	✓	
2.B	Inventory Software Platforms And Applications	✓	
2.C	Third Party Loss/Professional Liability	✓	
2.D	First Party Loss Coverage	✓	
2.E	Third Party Loss/Professional Liability	✓	
3.0	Network & Information Protection Policies/Procedures	✓	
3.A	Physical Access Controls	✓	
3.B	Network Access Controls	✓	
3.C	Restricted Access/Least Privilege Access Controls	✓	
3.D	Test/Dev Environment for New Software/Apps	✓	
3.E	Controlled Baseline System Configurations	✓	
3.F	Controlled System Maintenance (Patching)	✓	✓
3.G	Controlled Removal/Disposal of Assets	✓	
3.H	Policies and Controls for Mobile/Removable Devices	✓	
3.I	Documented Policies/Controls for Data Disposal	✓	
3.J	Testing of Back-Up Systems	✓	
3.K	Periodic Compliance Audits	✓	
4.0	Data Encryption	✓	
4.A	Encrypted Data and Files	✓	

Part III: Protection of Network and Data Con't		eSentire Advisory Services	eSentire MDR
5.0	Remote Banking & Fund Transfers	✓	
5.A	Inventory of Financial Services Vendors	✓	
5.B	Two-Factor Account Authentication	✓	
5.C	Client Request and Account Validation	✓	
5.D	Policies and Procedures to Protect Financial Info	✓	
5.E	Policies to Redress Client Losses	✓	
6.0	Mobile Device Management	✓	
6.A	Strong Password Protection on Devices	✓	
6.B	Jailbroken Devices Blocked from Network	✓	
6.C	Ability to Perform a Remote Wipe	✓	
Part IV: Detection of Unauthorized Activity and Response		**eSentire Advisory Services**	**eSentire MDR**
1.0	Detection of Unauthorized Activity		✓
1.A	Continuous Monitoring to Detect Cybersecurity Event		✓
1.B	Aggregation/Correlation of Logs from Multiple Sources		✓
1.C	Systems to Detect Malicious Code		✓
1.D	Network Forensics Logging		✓
1.E	Host Based Detections		✓
1.F	Host Based Forensics		✓
2.0	Incident Response	✓	✓
2.A	Documented Incident Response Protocol	✓	✓
2.B	Documented Team of First Responders	✓	✓
2.C	Documented Breach Reporting Decision Tree	✓	✓
2.D	Procedures to Determine the Scope of a Breach	✓	✓
2.E	Procedures to Remediate Breach	✓	✓
2.F	Periodic Fire Drills to Test IR Protocols and Teams	✓	✓
3.0	Threat Intelligence and Prevention		✓
3.A	Subscription to Threat Intelligence Feeds		✓
3.B	System to Whitelist and Blacklist Urls		✓

Part V: User Training		eSentire Advisory Services	eSentire MDR
1.0	User Training	✓	
1.A	Documented User Training Program	✓	
1.B	Regular Testing of Cybersecurity Awareness	✓	
1.C	Periodic Friending Attacks to Test Awareness	✓	
Part VI: Risks Associated with Vendors & Third Parties		**eSentire Advisory Services**	**eSentire MDR**
1.0	Cybersecurity Risk Assessment	✓	
1.A	Physical Access Controls	✓	
1.B	Network Access Controls	✓	✓
1.C	Restricted Access/Least Privilege Access Controls	✓	✓
1.D	Test/Dev Environment for New Software/Apps	✓	
1.E	Controlled Baseline System Configurations	✓	
1.F	Controlled System Maintenance (Patching)	✓	
1.G	Controlled Removal/Disposal of Assets	✓	
1.H	Policies and Controls for Mobile/Removable Devices	✓	
1.I	Documented Policies/Controls for Data Disposal	✓	
1.J	Testing of Back-Up Systems	✓	
1.K	Periodic Compliance Audits	✓	
2.0	Contract Elements Covering Cybersecurity	✓	
3.0	Segregation/Limitations to Third Party Network Access	✓	✓
4.0	Third Party Remote Maintenance Policies and Procedures	✓	
5.0	Incident Response Protocols	✓	
5.A	Documented Incident Response Protocol	✓	
5.B	Documented Team of First Responders	✓	
5.C	Documented Breach Reporting Decision Tree	✓	
5.D	Procedures to Determine the Scope of a Breach	✓	
5.E	Procedures to Remediate Breach	✓	
5.F	Periodic Fire Drills to Test IR Protocols and Teams	✓	
6.0	SSAE SOC II Security Audit and Report		

We defend against the threats facing law firms

With limited resources, it's difficult to know if you're prepared for the next big breach.

At eSentire, we work with clients ranging from small practices to the AM Law 200. Regardless of resources or a formalized security team, we work to find the right solution to ensure risk is mitigated to the firm and its clients. From managing, detecting and responding to threats in real-time to building measurable programs and policies, our goal remains the same: protect the firm and its clients from threats that traditional security technologies miss.

Leveraging the collective knowledge of our threat intelligence team, security operations center, and industry-leading cybersecurity advisors, we're committed to delivering enterprise-grade protection and expert guidance on compliance to help you:

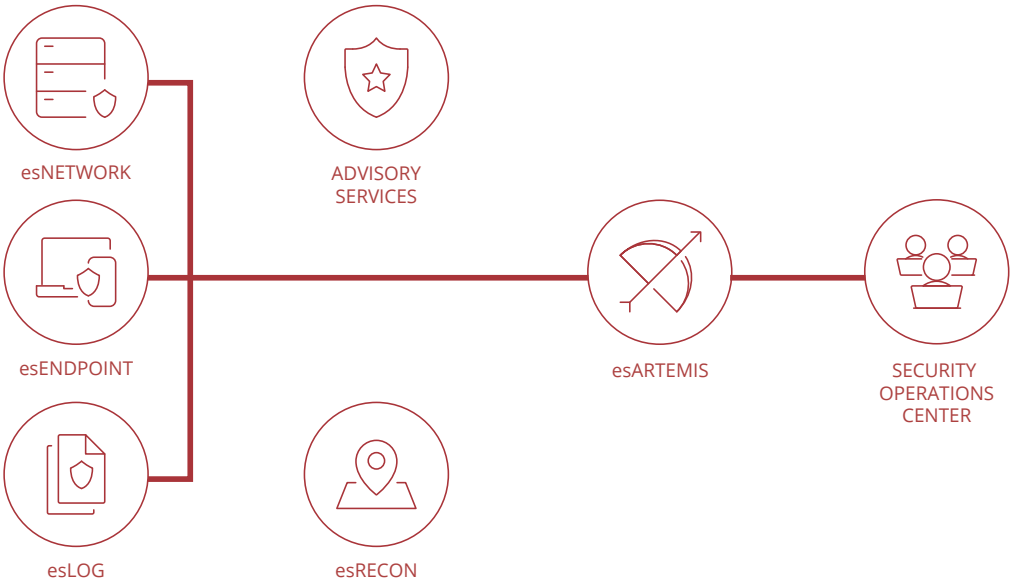
- Manage, detect and respond to threats in real-time
- Build measurable programs and policies
- Meet and exceed third-party compliance requirements
- Identify, manage and mitigate risk from vulnerabilities
- Design effective security architecture and controls

We detect the threats that other technologies miss.

Learn more

The eSentire Solution

eSentire Managed Detection and Response™ (MDR) keeps organizations safe from constantly evolving cyber-attacks that technology alone cannot prevent. Our 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.



eSentire Managed Detection and Response

esNETWORK™

Real-time network threat detection and response

- Enables real-time inspection of every packet using full packet capture, stopping threats that others miss
- Behavioral and rule-based detection and alerts of not just known but suspicious activities
- Disrupts malicious traffic and isolates threats, in near real-time preventing network spread
- Allows for seamless escalation to active engagement by certified security analysts, 24x7x365
- Provides recommendations and full remediation support based on forensic analysis

esLOG™

Purpose-built log management for MDR

- Analyzes raw log data from networks, endpoints, cloud and applications, allowing analysts to hunt and investigate threats
- Monitors in real-time for suspicious activities and anomalies discovered from log data
- Gives analysts the ability to conduct root cause analysis and provide full remediation recommendations and support
- Provides full security log and event aggregation capabilities of a SIEM without the traditional management complexity and cost

esENDPOINT™

Next-gen endpoint threat detection and response

- Continuously monitors, records, centralizes and retains activity for every endpoint
- Provides continuous hunting and detection of unknown attacks leveraging patterns and behavioral analytics
- Isolates threats on client's behalf, in near real-time, preventing lateral spread with always on 24x7 service
- Provides recommendations and full remediation support after threats are isolated

esRECON™

Integrated MDR Vulnerability Scanning

- Scans 55,000+ vulnerabilities including web applications, databases, UNIX, Windows and Mac
- Delivers optimized reporting and remediation guidance based on an organization's prioritization of risk
- Provides eSentire experts with additional information to better hunt, investigate, and respond to threats that have bypassed security controls

We Hunt & Detect
Using signature, behavioral and anomaly detection capabilities

We Absorb
The complexity to eliminate the false positives and identify the real attacks

We Respond
In real-time to block these attacks and alert the client

We Help Remediate
Based on full forensic analysis, with detailed recommendations until the threat actor is eliminated

eSentire Advisory Services

Beyond MDR, our dedicated security experts will help you assess risks, address known gaps and build a comprehensive program that meets stringent regulatory requirements.

- Security Program Maturity Assessment
- Security Policy Guidance
- Security Incident Response Plan
- Security Architecture Review
- Health Check
- Executive Briefing
- Penetration Testing & Vulnerability Assessments
- Risk Assessments
- Phishing Campaigns

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 $5 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.