



Cyber Security Trends

The Threat, Impact, and Awareness of Law Firm Security

LLAM Cybersecurity Symposium, April 8, 2016

Joseph Raczynski, Manager, Technology Client Managers

Wendy Maines, Librarian Relations Manager



THOMSON REUTERS

Roadmap

- Current cyber security landscape
- Status of law firms and corporate security
- Actions to mitigate security risks
- Why & How law librarians should get involved
- Appendix - Savvy cybersecurity resources



A Glimpse at Recent Security Breaches



Breached
32,000,000
Breached



THOMSON REUTERS

Ashley Madison

- A data dump, 9.7 gigabytes in size
- Dark web using an Onion address via Tor
- Data released:
 - full names,
 - passwords,
 - addresses and phone,
 - credit card numbers,
 - times used service



Law Firm & Corporation Security

- **97** 97% of law firm/corp networks have been compromised.*
- **225** 225 Days before a firm/corp knows that their network has been compromised*
- **84** 84% of firms/corps find out that they have been compromised by third parties.*



Identity Theft Resource Center

2016 Data Breach Category Summary

How is this report produced? What are the rules? See last page of report for details.

Report Date: 3/29/2016

Totals for Category: Banking/Credit/Financial	# of Breaches: 5	# of Records: 4,382
	% of Breaches: 2.5%	%of Records: 0.1%
Totals for Category: Business	# of Breaches: 96	# of Records: 1,916,909
	% of Breaches: 47.5	%of Records: 31.0%
Totals for Category: Educational	# of Breaches: 21	# of Records: 310,650
	% of Breaches: 10.4	%of Records: 5.0%
Totals for Category: Government/Military	# of Breaches: 8	# of Records: 102,459
	% of Breaches: 4.0%	%of Records: 1.7%
Totals for Category: Medical/Healthcare	# of Breaches: 72	# of Records: 3,850,126
	% of Breaches: 35.6	%of Records: 62.3%
Totals for All Categories:	# of Breaches: 202	# of Records: 6,184,526
	% of Breaches: 100.0	%of Records: 100.0%

2016 Breaches Identified by the ITRC as of: 3/29/2016

Total Breaches: 202
Records Exposed: 6,184,526

Law Firms Targeted



Why Law Firms?

Law firms are targeted because

- IP information
- M&A information
- Sensitive Proprietary Information
- Big & Small Cases – with major impacts on people's lives
- Venting/Anger



Security

- ILTA Survey Top Response
- People, Process, and Technology



Forms of Attack

- Spear phishing attacks
 - Internal testing
 - Cybercrime-As-A-Service
- Social Engineering
- Software – Ransomware



<u>Attacker/Threat Profiles</u>			
Group	Hacktivists	Criminals	Nation States
..... Who	Anonymous, LulzSec, Syrian Electronic Army, Turkish Ajan	Non-US Organized Crime	Military, Intelligence, Security Agencies
Why	Notoriety, Causes, Politics	Personal Profit, Financial Gain, Money	Espionage, Defense, Economic Advantages
Where	Worldwide, US UK Europe Middle East Asia	Russia, Moldova, Estonia, Romania, Ukraine, Asia	Any Country with the Capability and Motivation
Interests	DDoS, Data Exposure, Site Defacement, Data Destruction	Monetize PII/PCI/PHI, Steal Cash, ACH, Extortion, Fraud	IP, R&D, Logistics, M&A, Weapons, Legal Strategy, Etc.
Advantages	Some Technical Skills, Practice	Tech Skills, Automation, Geography, Industry Knowledge	Organizations, resources, Tech Skills, Immunity/Location
Limitations	Resources, Technical Depth/Breadth, Org Structure – weak	Non-standard technology (old school mainframe)	None (other than the fact that there are lines – warfare)
Impact	Ranges from an Irritant to Disruptive, Generally Recoverable	Massive amounts of corporation money	“greatest transfer of wealth in history” US loses 250 Billion a year in IP and commerce

Advanced Endpoint

- “Antivirus protection is almost pointless”
 - No feasible way to scan, collect, submit and maintain a log of the rapidly changing viruses
- Assume you are or will be breached!
 - Thief in your house - Firms must invest in detection and response
- Mathematical algorithms to predict what will be malicious
 - Collects samples of viruses
 - Extracts common features in the code
 - Transforms that code into feasible branch code





Mitigation Measures

- **Awareness**

- Educate all parties surrounding the law firm on the existing threats, hacker tactics, and potential outcomes from unsafe computing.
 - Employees
 - Management
 - Suppliers
 - **Clients**

- **Visibility**

- Never assume that you will know everything that is happening on your network.
- Keep an inventory of assets, logs and all alerts which when gathered together creates actionable intelligence.





**KEEP
CALM
AND
ASK YOUR
LAW LIBRARIAN**



THOMSON REUTERS



Why (& How) Should Law Librarians Get Involved?

1. Security breaches have occurred within:

- Law firms
- Agencies
- Court Systems
- Law schools
- Legal information vendors



2. Emerging practice area needing support
3. Swinging balance of security and privacy
4. Adding value to our firms





#1 Concern for Law Firm Clients

- 55% of general counsel said that data security was their top concern*
- 33% of general counsel believe that boards are not adequately managing cyber risk*
- Failure to address can even lead to personal liability for clients
 - *In re CAREMARK INTERNATIONAL INC. DERIVATIVE LITIGATION, 698 A.2d 959 (Del. Ch. 1996)*





2015 LEGAL TECHNOLOGY Survey Report



Vol. I

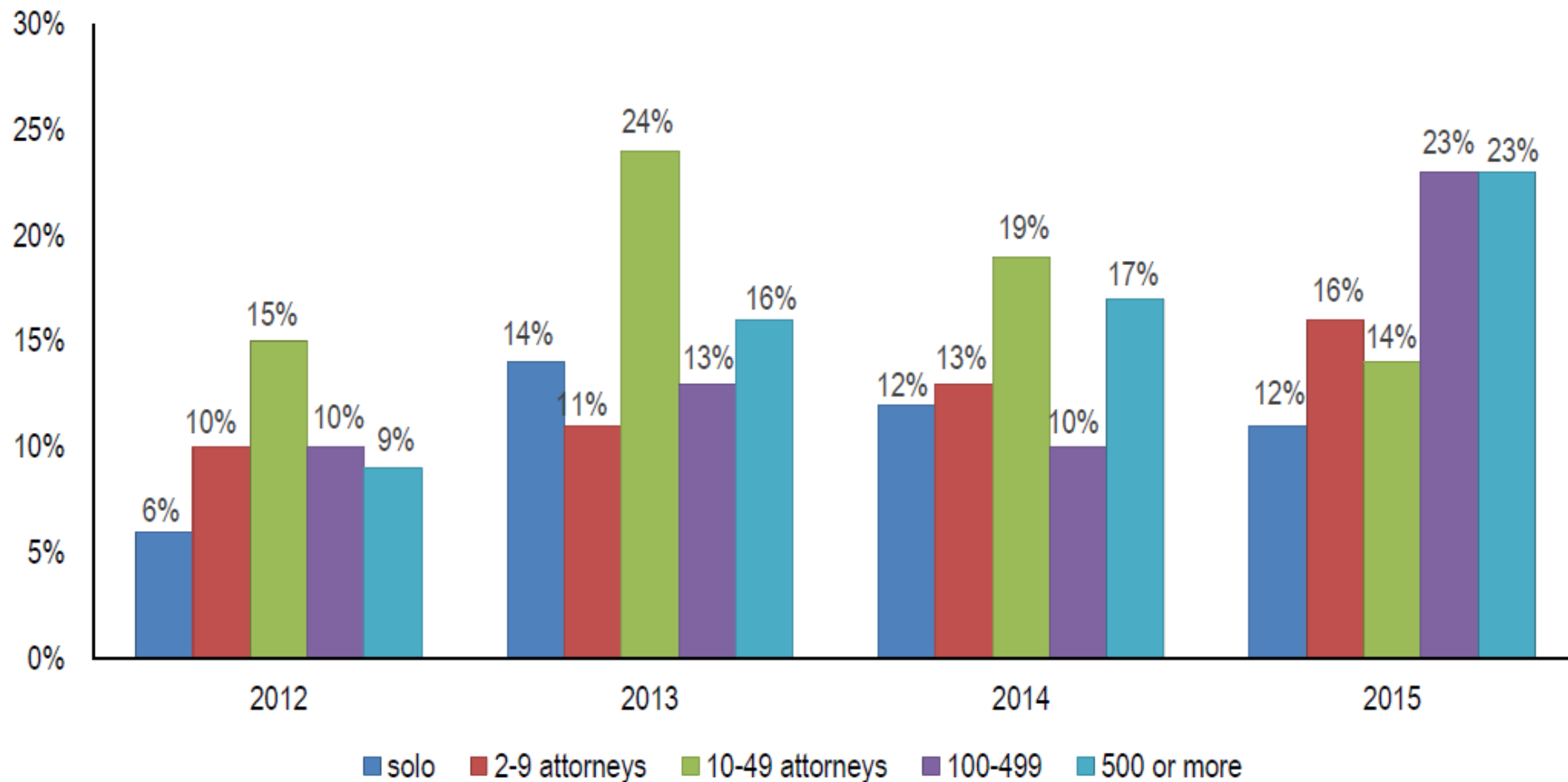
**Technology Basics
and Security**



THOMSON REUTERS



Law Firms that Experienced a Security Breach



What was the result of the security breach?

		NUMBER OF LAWYERS AT ALL LOCATIONS					
	Total	Solo	2-9	10-49	50-99	100-499	500 or more
No significant business disruption or loss	60.3%	64.0%	45.9%	58.8%	87.5%	66.7%	71.4%
Downtime/loss of billable hours	30.2%	40.0%	45.9%	29.4%	25.0%	6.7%	–
Replace hardware/software	29.3%	28.0%	37.8%	29.4%	50.0%	20.0%	7.1%
Consulting fees for repair	22.4%	20.0%	40.5%	23.5%	25.0%	–	–
Destruction or loss of files	18.1%	28.0%	24.3%	23.5%	12.5%	–	–
Unauthorized access to other (non-client) sensitive data	6.9%	4.0%	10.8%	–	12.5%	13.3%	–
Notify client(s) of breach	5.2%	4.0%	10.8%	–	–	–	7.1%
Unauthorized access to sensitive client data	2.6%	–	5.4%	–	–	–	7.1%
Other	3.4%	4.0%	2.7%	5.9%	–	6.7%	–
Don't know	7.8%	–	2.7%	5.9%	–	20.0%	28.6%
Count	116	25	37	17	8	15	14





#2 - Growing Cybersecurity Practice Groups OR....82 variations

- Critical Infrastructure Protection
- Cybercrime
- Cyber Defense Law
- Cyber Insurance
- Cyber Investigation
- Cyber Risk & Losses
- Data Breach
- Data Privacy & Protection
- Data Rights & Protection
- Data Risk Management

A rose
by any other
name would
smell as
sweet.



~William Shakespeare





Legal Developments: Timeline (Partial)

2/12/2013



Exec. Order
13636
*Improving
Critical
Infrastructure
Cybersecurity*

4/18/2013



Cyber
Intelligence
Sharing &
Protection Act
(H.R. 234)

Passed
House but
stalled & not
voted on in
Senate

2/12/2014



NIST released
*Framework for Improving
Critical Infrastructure
Cybersecurity*

Helps differing org types:

- Conduct a basic review of cybersecurity practices
- Establish / improve cybersecurity using the steps outlined
- Communicate cybersecurity requirements with stakeholders
- Identify opportunities to revise or create new standards or practices

12/18/2014



Cybersecurity
Enhancement
Act
(PL113-274)

Codifies the
Framework
development
& support
process.



THOMSON REUTERS



Legal Developments: Timeline (Partial)

10/27/2015



12/18/2015



2016



Cybersecurity Information
Sharing Act (S. 754)
PASSED SENATE

- Enhanced info sharing re: cybersecurity threats
- **Allows private companies to share info about their users' Internet activity w/ fed govt (even when data is unnecessary to i.d. or protect v. a threat)**
- **Protects companies from liabilities**

Congress attached CISA to
the Consolidated
Appropriations Act of 2016
(Pub.L. 114-113)

- Reduced chance for debate on surveillance provisions
- "Nay" votes would threaten entire fed govt budget

???



#3 - Balance of Security & Privacy Needed

- Interest in a “philosophy of freedom” of information
 - Open source products
 - Access – will security efforts interfere?
- By granting companies broad liability protection for sharing private information, CISA may endanger privacy & civil liberties of internet users



CYBERSURVEILLANCE?

The Darth Vader Bill: Why CISA is Bad



CYBERSECURITY INFORMATION SHARING ACT (CISA):

CISA

1

Allows companies to share nearly ANY type of information with the government, including significant amounts of personal information

2

NSA and FBI automatically get all shared information and can use it for any number of reasons

3

Protects companies from being sued for sharing your personal information

4

Allows "hack backs" that could damage 3rd party networks, and also creates a vast new exemption to transparency laws



#4 - Adding Value to Your Firm: Best Practices

- Participate in development of firm's security policies
 - Send encrypted data (ex. USB devices, emails)
 - Track your tech
 - Security educational efforts for ALL firm members
 - What are the risks & how to avoid them
 - Do not keep unnecessary client data
 - Use multi-factor identification for log-ins
- Product and service selection
 - Use caution in the cloud
 - Vet your vendors





#4 - Adding Value to Your Firm: Best Practices

- Password Management & Policies
 - Don't "set it and forget it"
- Contribute to "cyberattack response teams"
 - Skills in KM & document preservation = ASSETS
 - Creativity in assisting with cybersecurity issues
 - Get cyber liability insurance
 - Create a data breach response plan to mitigate damages quickly



Savvy Sources: Practical Law

Practical Law A THOMSON REUTERS
LEGAL SOLUTION

Practice Areas ▾

Resources ▾

Jurisdictions ▾

My Practical Law ▾

SEARCH IN All US ▾

cybersecurity



Resource Type

All

Legal Updates (113)

Articles (89)

Practice Notes (27)

Checklists (9)

Standard Documents and
Clauses (7)

Toolkits (7)

Cyber Attacks: Prevention and Proactive Responses

This Note discusses common cyber attack scenarios and sets out actions that companies can take to prevent or respond to attacks, including developing a cyber attack response plan. ...

Maintained | Practice notes | USA

Cyber Insurance: Insuring for Data Breach Risk

This Practice Note examines issues related to obtaining insurance coverage specific to data breach risks, including the need for coverage, whether coverage may be available under o...

Maintained | Practice notes | USA

The NIST Cybersecurity Framework

A Practice Note discussing the National Institute of Standards and Technology (NIST) Cybersecurity Framework, including its structure and purpose, recommendations for implementing ...

Maintained | Practice notes | USA



THOMSON REUTERS



Practical Law: Privacy & Data Security Toolkit

Practice Note: Overview

[Employer Access to Social Media Accounts State Laws Chart: Overview](#)

Practice Notes

[Cyber Insurance: Insuring for Data Breach Risk](#)

[Direct Marketing](#)

[GLBA: The Financial Privacy and Safeguards Rules](#)

[Protection of Employers' Trade Secrets and Confidential Information](#)

Checklist

[Data Breach Response Checklist](#)

Toolkits

[HIPAA Toolkit](#)

[Social Media Usage Toolkit](#)

State Q&A Tool

[Data Breach Notification Laws: State Q&A Tool](#)

State Data Breach Laws Agency Notice Requirements Chart

State	State Agency	Notice to State Agency Timing and Method	Affected Individual Threshold	Content of State Agency Notice Requirements
California (<i>Cal. Civ. Code §§ 1798.29 and 1798.82</i>)	Attorney General	Notice must be submitted electronically using California's security breach reporting <i>form</i> .	500	Notice must include a single sample copy of the notice to consumers, excluding any personally identifiable information.
Connecticut (<i>Conn. Gen. Stat. § 36a-701b</i>)	Attorney General	Notice should be provided no later than the time notice is provided to the individual.	None.	None specified.
Florida (<i>Fla. Stat. § 501.171</i>)	Department of Legal Affairs (Attorney General)	Notice must be provided as expeditiously as practicable and no later than 30 days after determination of a breach or reason to believe a breach occurred. The covered entity also must provide	500	Notice must include: <ul style="list-style-type: none"> • Synopsis of events surrounding the breach at the time notice is provided. • Number of individuals in Florida actually or potentially affected by the breach. • Any services related to the breach being offered

Cyber Attacks: Prevention & Proactive Responses Practice Note

Contents

What is a Cyber Attack?

Chief Compliance Officer's Role in Cyber Attacks

- Actions to Prevent or Reduce the Risk of Cyber Attacks

Cyber Incident Response Plans

- Cyber Incident Response Team
- Discovery and Reporting of Cyber Incidents
- Initial Response to a Cyber Attack
- Investigating a Cyber Attack
- Common Cyber Attack Scenarios
- Recovery and Follow-up After a Cyber Attack
- Public Announcements and Public Relations After a Cyber Attack
- Law Enforcement Investigations of Cyber Attacks
- Customize the Cyber Incident Response Plan
- Reporting Cyber Crime to Law Enforcement
- Criminal Prosecution

Civil and Criminal Remedies for Cyber Attacks

- Identifying the Hackers
- Computer Fraud and Abuse Act
- Other Civil and Criminal Remedies

Other Actions to Deter or Mitigate Cyber Attacks

- Cease and Desist Letters
- DMCA Takedown Notices
- Cyber Liability Insurance Coverage


Recent Case Law

- Data Breach Litigation
- Immediate Discovery of Hacker Identities
- Failure to Properly Secure Electronic Evidence
- Determining Value under Computer Fraud and Abuse Act
- Reasonableness of Bank Security Procedures Against Cyber Attacks
- Auto-forwarding Another Party's E-mails Prohibited by Wiretap Act

Reporting Cyber Crime to the Appropriate Law Enforcement Agency



Sample Cybersecurity Risk Factor Clause

 Note: Overview of Cybersecurity Disclosure

SAMPLE CYBERSECURITY RISK FACTOR

Security breaches and other disruptions could compromise our information and expose us to liability, which would cause our business and reputation to suffer.

[In the ordinary course of our business, we/We] [collect and] store sensitive data, including intellectual property, our proprietary business information and that of our customers, [suppliers and business partners,] and personally identifiable information of our [customers and] employees, in our data centers and on our networks. The secure [processing,] maintenance [and transmission] of this information is critical to our operations [and business strategy]. Despite our security measures, our information technology and infrastructure may be vulnerable to attacks by hackers or breached due to employee error, malfeasance or other disruptions. Any such breach could compromise our networks and the information stored there could be accessed, publicly disclosed, lost or stolen. Any such access, disclosure or other loss of information could result in legal claims or proceedings, [liability under laws that protect the privacy of personal information,] [and regulatory penalties,] [disrupt our operations [and the services we provide to customers],] [and] damage our reputation, [and cause a loss of confidence in our products and services], which could adversely affect our [business/operating margins, revenues and competitive position].

Practical Law Journal

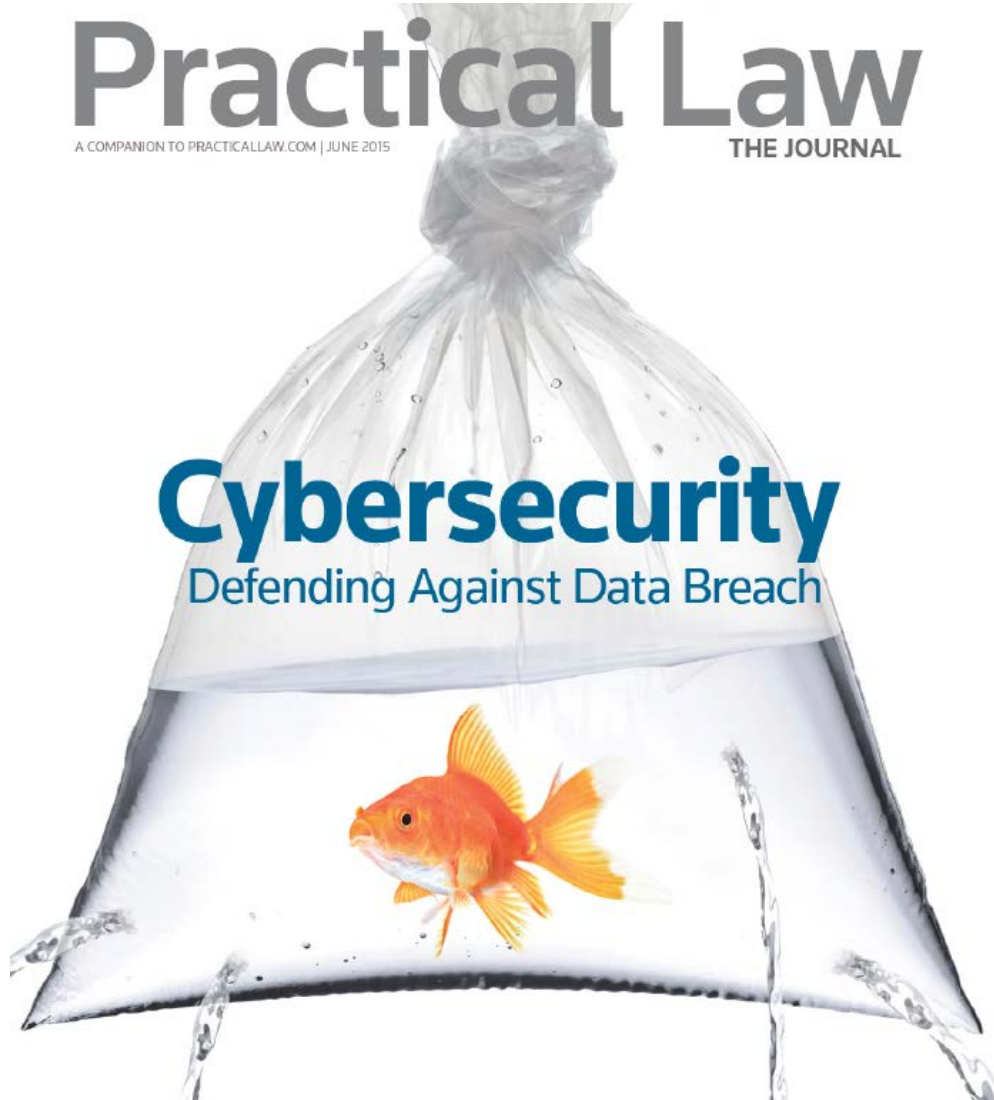
Practical Law

A COMPANION TO PRACTICALLAW.COM | JUNE 2015

THE JOURNAL

Cybersecurity

Defending Against Data Breach



THOMSON REUTERS

Upcoming



LegalSEC SUMMIT
2016

Two Days All About Security For Legal
June 9 & 10, 2016 | Baltimore, MD



THOMSON REUTERS



Questions?





Stuff We Like

Appendix

Additional Savvy Sources



THOMSON REUTERS

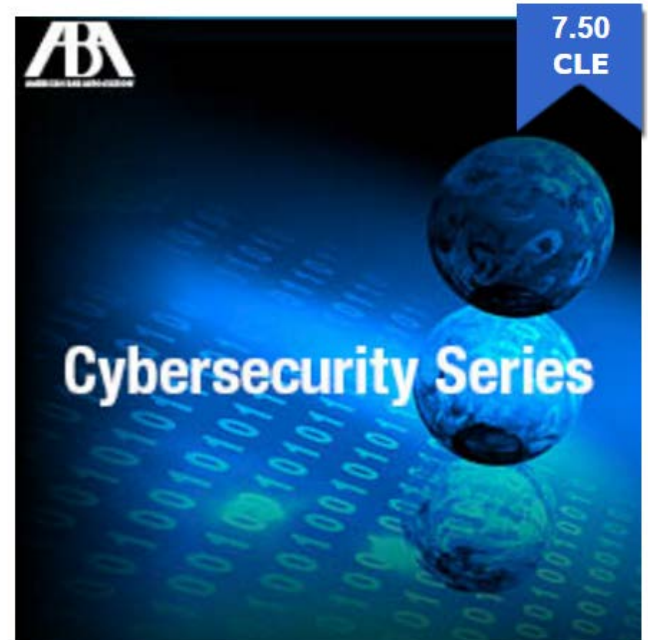
Savvy Sources: Websites & Articles

- Joe Raczynski Technologist
- Legal Executive Institute
- LegalTech News: Cybersecurity Update
- PinHawk Librarian Daily & Law Technology Digests



Savvy Sources: Online Training

- TR Risk Management provides online training for protecting & securing personal proprietary or confidential data
 - 20 courses available
- CLE
 - ABA series
 - West Legal Ed Center
 - 60 on demand programs
 - Data Security Boot Camp
 - Understanding Data Security Litigation
 - 5 live events



Tips to Minimize Your Risk of Data Breach



Conduct Customer and Third Party Risk Assessments

Identifying vulnerabilities and likely threats early help prioritize preventative and response activities to reduce the chances attackers will be successful in their goals.

Conducting risk assessments using **Risk Management Solutions from Thomson Reuters** and monitoring existing relationships to ensure ongoing compliance, is an essential part of a risk based approach.



Stay Aware of the Global Regulatory Environment

Ensure your organization's current data privacy and security measures are in line with the latest global regulations on cybersecurity with **Thomson Reuters Regulatory Intelligence**.



Implement Safeguards

Create clear internal policies and procedures in dealing with a potential data breach. Track your staff's understanding of policy updates and amend those policies to reflect new regulatory changes with **Thomson Reuters Policy Manager**.



Employ Training & Awareness Programs

Mistakes made by employees are a frequent cause of data breaches. To help mitigate this risk, provide your employees and other stakeholders who have access to sensitive data with proper compliance training with **Thomson Reuters Compliance Learning**.

Savvy Sources - Books

- ABA Cybersecurity Handbook, A Resource for Attorneys, Law Firms, and Business Professionals
- Locked Down: Information Security for Lawyers
- A Playbook for Cyber Events, Second Edition