TECHSHOW2018

Guarding Your Castle: Law Firm Cybersecurity

Presenters: Judy Selby and Jody Westby

Legal Practice: Risky business

- Risks associated with cybersecurity viewed by many as number one concern for law firms.
- Already a number of well known firms in headlines
- ABA 2016 Legal Technology Survey Report
  - more than 500 respondents said had suffered breach
  - 40% had significant business interruption and loss of billable hours
  - 25% pad large amounts to remediate the problem.
- Clients are increasingly concerned and asking for security program documentation

ABA Resolution 109

- RESOLVED, That the American Bar Association encourages all private and public sector organizations to develop, implement, and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations and is tailored to the nature and scope of the organization and the data and systems to be protected.

What is a Cybersecurity Program?

- Roles & responsibilities
- Security plans, strategies, budgets
- Basic activities to be performed
- Policies, Standards, and Procedures
- Risk assessments
- Analysis of compliance requirements
- Inventory of applications, data, and hardware
- Determination of security controls needed
- System architecture and security configuration of hardware and software
- Monitoring and enforcement
- Intrusion detection and incident response

Cybersecurity Best Practices & Standards

- The International Organization of Standardization ISO 27001/002
- Information Technology Infrastructure Library (ITIL)
- International Society of Automation (ISA)
- Information Systems Audit and Control Association (ISACA), the Control Objectives for Information and Related Technologies (COBIT)
- Payment Card Industry Security Standards Council (PCI SSC),
- National Institute of Standards and Technology (NIST) Special Publication 800 (SP-800) series and Federal Information Processing Standards (FIPS),
- Information Security Forum (ISF) Standard of Good Practice for Information Security
- Carnegie Mellon University's Software Engineering Institute, Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE
- North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP)
- U.S. Nuclear Regulatory Commission

Cyber Attacks & Ethics Rules

Confidentiality of Attorney Client & Work Product Data

- New **commentary to Rule 1.1** states:

  A lawyer's duty of competence requires attorneys to "keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology."

- **Model Rule 1.6(c)** on the confidentiality of client communications:
  "(c) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."

- Commentary on the Rule notes that:
  "[18] Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure."

Negligence, Disclosure & Ethics Rules

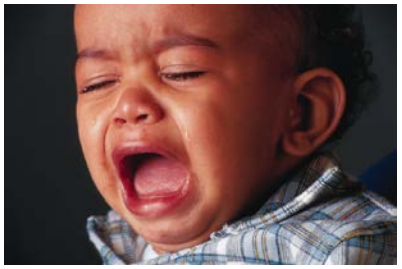
- Rules 1.1 and Rule 1.6 may **allow a law firm to avoid an ethics violation** stemming from a breach **if it has acted in a competent manner** (e.g., having a strong security program) to protect its client data from disclosure.
- Rule 1.6(c), however, does not address whether attorneys have to tell their clients about such an event.

Informing Client of a Breach: Self-Reporting of Negligence

- **Rule 1.4** (communications with the client) & fiduciary law governing the lawyer-client relationship: Self-reporting of negligence
- **Restatement (Third) of the Law Governing Lawyers** states: "If the lawyer's conduct of the matter gives the client a substantial malpractice claim against the lawyer, the lawyer must disclose that to the client."

A strong security program will help avoid ethics violation for failure to competently protect client information & negligence, BUT it will not shield against reporting breach to client

- The attorney has a duty to inform clients under 1.4 that their confidential information has been compromised.



Bottom Line

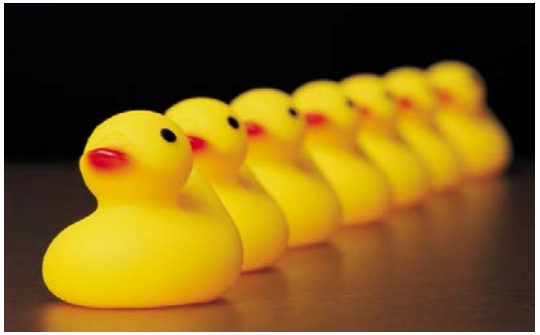
- A strong enterprise security program is the best defense that a law firm can have in the event of a cyber attack

- Whether large or small, taking measures to establish a strong security posture is not only the right thing to do; it is the ethical thing to do.

- It may help save the firm cases, clients, and its reputation.

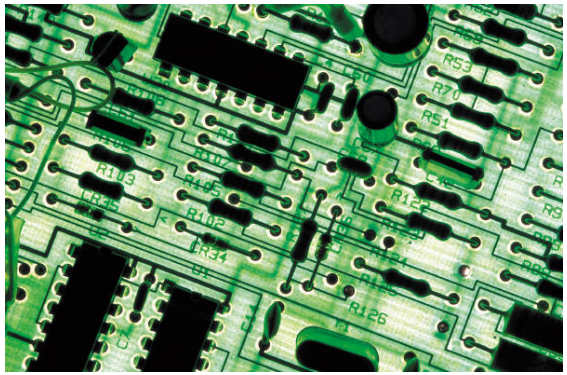
Managed Security Service Providers

- Cybersecurity programs require time, expertise & money
- A managed security service provider (MSSP) can help lift the load & expense
- MSSPs monitor and manage the security of companies, including devices and systems
- Attractive option for small firms due to low cost, cloud-based deployments & advancements in technology
- Helps level the playing field for smaller firms that may need to meet cybersecurity requirements of larger counterparts



MSSP Services

- Firewall management
- Intrusion detection & log analysis
- Virtual private networks
- Vulnerability scanning
- Anti-virus services
- Security monitoring
- Security Information & Event Management (SIEM) –real time analysis of security alerts generated by applications and hardware
- Security audits
- Disaster recovery, business continuity, backup support
- Training & targeted security education
- 24/7 Help Desk Support
- Best practices consulting



Potential Benefits of MSSP

- Up-to-date Expertise, highly trained professionals, abreast of latest security trends & threats
- Professionals with expertise across many security areas, so can get a team instead of one person; enables internal personnel to work with experts
- Proactive Approach – Efficient delivery of services. MSSPs can quickly apply patches or remedies to counter threats, can cover many locations.
- Unified Solution – Avoids a patchwork of vendors to manage a range of issues (mobile devices, patching, log analysis, vulnerability scanning, etc.). MSSP can be central hub for security best practices with unified solution.
- Cost savings – MSSPs can spread costs of technical tools, personnel, and facilities across many clients. Proactive services can prevent costly cyber incidents.

MSSP Cost Worksheet

Infrastructure	Internal Cost	Supporting Vendor Cost	MSSP Cost
Servers			
Database administration			
Backup software			
Anti-virus & Anti-malware tools			
Power			
Facilities			
Operational / Administrative	**Internal Costs**	**Supporting Vendor Costs**	**MSSP Cost**
Network			
Systems			
Staffing	**Internal Costs**	**Supporting Vendor Costs**	**MSSP Cost**
Salaries			
Staffing fees			
Overhead			

Selecting an MSSP

- Conduct thorough due diligence
- Look for good cultural & operational fit, not just at qualifications & competence
- Discuss services provided and match to your needs; 24/7 support may be important
- Ask whether other partner companies are involved in service delivery
- Determine whether MSSP understands your compliance requirements, esp. if PCI or HIPAA & controls needed
- Check if MSSP has experience with particular applications firm uses
- What cyber insurance do they have?
- How are incidents and notifications handled?
- Ask for references and check them! Inquire about responsiveness, employee turnover, ability to stay within budget, etc.

Contract Considerations

- Determine if MSSP will sign SLA with exit strategy
- Willingness to provide annual report on security program (SOC-2)
- Flexibility to cut back on services that are underutilized and scale up on others to meet firm operations
- Security background checks of employees, physical security measures at their location
- Period of time logs are retained
- Flagging of issues and resolution
- Length of contract
- Dispute resolution
- Termination provisions
- Transfer of data to another provider or back in-house on termination
- Governance and account management

THANK YOU!

TECHSHOW2018

- YOU play the most important part in keeping TECHSHOW exciting. *Please complete the Speaker evaluation before you leave.*

- Reserve the dates!

TECHSHOW 2019: February 27 – March 2, 2019