Florida Bar Committee on Cybersecurity and Privacy Law
Recommendation 25-1

Subject: Voluntary Implementation of Incident Response Plans

Date:

Introduction. The Committee on Cybersecurity and Privacy Law for the Florida Bar (the "Committee"), in recognition of the constantly evolving and dynamic risks and impacts of cybersecurity incidents, as uniquely if not especially targeting Members of the Florida Bar, seeks to encourage Florida Bar Members to adopt proactive measures aimed at safeguarding their sensitive firm data as well as that of their respective Clients and Third Parties.

Recommendation 25-1 The Committee recommends that all Florida Bar Members and/or such Member's associated law firm, prepare, and annually maintain an industry-compliant Incident Response Plan (IRP) as described below.

The Committee recognizes that its Members and/or such Member's associated law firm range from solo practices to global law firms. Accordingly, the level of sophistication of an Incident Response Plan and the reasonableness of its security measures will vary based on many factors including but not limited to practice size, sensitivity of client and third-party information, and operational resources.

As necessary predicate steps to an effective Incident Response Plan, the Committee recommends that a Data Mapping[1] Survey followed by an appropriate Maturity Assessment be initiated and completed within 2 years and an appropriate Incident Response Plan in place within 3 years. These time frames are the Committee's recommendations only but the Committee strongly encourages implementation as soon as possible. These predicate steps, in conjunction with an Incident Response Plan, are the only proven effective strategies to reduce the impacts of cybersecurity incidents.

This recommendation, in conjunction with a robust educational and programming campaign, establishes a voluntary, non-binding standard reflective of the Committee's focus on enhancing the resilience of The Florida Bar's Membership and safeguarding the information Florida Bar Members retain against cyber threats. Further, this recommendation is intended to serve as voluntary and non-binding. The Committee's recommended practices are set forth in Appendix A. The Committee recommends that Florida Bar Members should consider whether retention of qualified experts is reasonably necessary to conduct the processes outlined herein to ensure completion, accuracy and consistency with evolving best practices.

Purpose

This recommendation seeks to:

[1] Also known as Data Inventorying.

1. **Encourage Data Mapping** – Understanding the lifecycle and flow of data enables Members to assess potential vulnerabilities and to enhance targeted security measures. Exercises in understanding "what data do I have" and "where is my data" are proven disciplines in reducing exposure.

2. **Promote Maturity Assessments** – Regular evaluations of a law firm's data security maturity allow for continuous improvement in cybersecurity practices, ensuring they evolve with emerging threats and technologies. Maturity Assessments allow for an initial baseline of cyber-resilliency followed by annual review upon which improvements may be added to protect against evolving cybersecurity threats.

3. **Enhance Cybersecurity Preparedness** – Incident Response Plans help ensure that Members are well-prepared to respond promptly and effectively to cybersecurity incidents and possible data breaches. Incident Response plans help minimize operational disruptions and protect Client and Third-Party data, reducing potential revenue loss and liability risks.[2]

Conclusion

The Committee on Cybersecurity and Privacy Law recommends that all Florida Bar Members consider implementing these best practices tailored to their specific practice.

Disclaimer

This voluntary recommendation is made for the benefit and guidance of the Members of the Florida Bar and their respective Clients. This recommendation is not to be deemed a directive nor is this recommendation intended to be a "standard of care" or legal obligation governing the practice of law. Likewise, this voluntary recommendation is not to be considered an adjunct or in addition to the requirement of the Rules Regulating the Florida Bar.

[2] *See*, as one example, NIST Special Publication 800-61 and any amendments thereto.

Appendix A-1

Sample Data Mapping Guide

Objective: To identify what data the firm holds, where it resides, how it flows, and where potential vulnerabilities exist.

1. Data Inventory

Data Type[3]	Location	Access Control	Retention Policy
Client Records	Document Mgmt. System	Role-based access	7 years post-case
Financial Data	Accounting Software	Finance Dept.	5 years
Email Communications	Email Server	Authorized Users	2 years

2. Data Flow Mapping

A. Identify Data Sources: Client intake forms, emails, third-party vendors.
B. Track Data Movement:
   i. Ingestion: How data enters the firm (email, web forms)
   ii. Storage: Where data is stored (servers, cloud services)
   iii. Processing: How data is used (case management, billing)
   iv. Sharing: Who data is shared with (courts, opposing counsel, clients)
   v. Archival/Deletion: How and when data is archived or deleted.

3. Identifying Vulnerabilities

A. Common Vulnerabilities to Assess:
   i. Unencrypted Data: Ensure sensitive data is encrypted at rest and in transit.
   ii. Unauthorized Access: Review access controls regularly.
   iii. Third-Party Risks: Evaluate vendor security policies.

4. Data Mapping Best Practices

A. Update Regularly: Review data maps every 6-12 months.
B. Employee Training: Ensure staff understand data handling policies.
C. Incident Response Integration: Link data maps to your IRP for faster containment and recovery.

[3] The data types listed are provided as examples and are not an exhaustive or comprehensive list of all data types or subtypes that a law firm may handle or process. These examples are intended to serve as a reference to help law firms identify and tailor their own specific data types based on the unique needs, practices, and operations of their firm. Each law firm is encouraged to evaluate its data management practices to ensure all relevant data types are appropriately addressed in its policies and procedures.

Appendix A-2

Basic Guidance for Maturity Assessments

<u>How to Use the Maturity Assessment</u>

- Evaluate each category using the maturity levels.
- Identify gaps in policies, procedures, or controls.
- Prioritize improvements based on identified weaknesses.
- Set goals to advance to the next maturity level over time.
- Review and reassess annually or after significant changes to the firm's data practices.

<u>Basic Maturity Assessment Guideline</u>

Identify Key Maturity Levels

1. Initial (Level 1)
    - No formal policies or procedures in place.
    - Reactive approach to security incidents.
    - Data protection practices are inconsistent and undocumented.
2. Developing (Level 2)
    - Basic policies and procedures exist but are not fully documented or consistently applied.
    - Some staff training on data protection and incident response.
    - Security controls are in place but may lack consistency and enforcement.
3. Defined (Level 3)
    - Policies and procedures are formally documented and communicated.
    - Consistent application of security controls across the firm.
    - Regular staff training and awareness programs.
    - Basic incident response plan (IRP) established and tested periodically.
4. Managed (Level 4)
    - Comprehensive policies, procedures, and controls are in place and consistently enforced.
    - Regularly scheduled reviews and updates to policies based on evolving risks.
    - Incident response plans are tested and refined based on lessons learned.
    - Data protection measures are aligned with industry best practices.
5. Optimized (Level 5)
    - Continuous improvement of policies, controls, and incident response procedures.
    - Proactive risk management and threat monitoring.
    - Advanced security measures and technologies implemented.
    - Regularly audited and assessed for compliance with industry standards.

Appendix A-3

Incident Response Plans (IRPs) Recommendations

Key Components of the Incident Response Plan (IRP)

1. **Preparation**
   - Define roles and responsibilities for incident response.
   - Develop a communication plan (internal and external).
   - Conduct regular security awareness training.
   - Maintain a list of critical systems, data assets, and third-party vendors.

2. **Detection and Identification**
   - Implement monitoring tools to detect anomalies.
   - Establish clear criteria for identifying cybersecurity incidents.
   - Develop an incident classification system (e.g., low, medium, high severity).

3. **Containment**
   - Isolate affected systems to prevent further damage.
   - Implement short-term and long-term containment measures.

4. **Eradication**
   - Identify the root cause of the incident.
   - Remove malware or unauthorized access points.
   - Patch vulnerabilities and strengthen defenses.

5. **Recovery**
   - Restore affected systems and data.
   - Verify systems are clean and fully functional.
   - Monitor systems for recurrence of the incident.

6. **Post-Incident Review**
   - Conduct a “Lessons Learned” meeting within 14 days.
   - Update the IRP based on findings.
   - Document the incident and response actions for compliance.

Sample Incident Response Plan (IRP) Template for Law Firms

A. Introduction

- **Purpose**: Outline procedures for responding to cybersecurity incidents.
- **Scope**: Applies to all employees, systems, and data managed by the firm.

B. Roles and Responsibilities

Role	**Responsibility**
Incident Response Lead	Coordinates response efforts and communication
IT Support	Investigates technical aspects and restores systems
Compliance Officer	Ensures regulatory and legal compliance
Communications Lead	Manages internal/external communications

C. Incident Classification

Severity	**Description**	**Examples**
High	Significant impact on operations or data.	Data breach, ransomware
Medium	Moderate impact, limited to specific systems.	Unauthorized access attempt
Low	Minimal impact, no sensitive data involved.	Phishing email with no breach

D. Response Steps

1. Detect and Identify
   i. Monitor logs and alerts for anomalies.
   ii. Verify incident classification.

2. Contain
   i. Disconnect compromised systems.
   ii. Disable affected user accounts.

3. Eradicate
   i. Remove malicious code.
   ii. Apply patches and updates.

4. Recover
   i. Restore systems from backups.
   ii. Validate system integrity.

5. Report and Review
   i. Notify affected parties if necessary.
   ii. Conduct a post-incident review and update the IRP.