Cyber security practices and incident response

Presented by Javier A. Vijil & Brian Ramkissoon

Kennedys

Recommendation 25-1: Voluntary Adoption of Incident Response Plans

- Florida Bar Committee on Cybersecurity and Privacy Law
- Framework for proactive cybersecurity preparedness in law firms—27 March 2025
- “As necessary predicate steps to an effective Incident Response Plan, the Committee recommends that a Data Mapping 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.”

Rationale for Recommendation 25-1

- Law firms are increasingly targeted due to valuable confidential and strategic data
- Cyber incidents cause financial, reputational, operational, and ethical consequences
- Threats range from phishing and credential theft to ransomware and data exfiltration
- Bonus: Implementing these recommendations will also assist with third-party liability and regulatory inquiries.

Size Doesn’t Matter

Even small firms are targeted due to lower defensive maturity

Proactive preparation reduces downtime and recovery cost

Recommendation encourages readiness without imposing legal obligations

Understanding Recommendation 25-1

- The recommendation is voluntary and non-binding
- It does not create a new standard of care or regulatory requirement
- The intent is to support responsible stewardship of client data
- Scalable approach: appropriate to firm size, data sensitivity, and resources
- Focus is on awareness, risk evaluation, and coordinated response capability
- Encourages improvements over time rather than immediate maturity

Data Mapping : Purpose & Value

- Identifies what data the firm holds and where it resides
- Reveals vulnerabilities where unauthorized access or exposure may occur
- Supports better access control, retention, and breach response decisions

Data Mapping: How to Conduct

- Identify data systems: email, case management software, document servers, billing platforms
- Document storage locations: cloud services, local servers, external drives, paper archives
- Record access permissions: who can view, edit, export, or share each category of data
- Map retention timelines: what is kept, why, and for how long

Cybersecurity Maturity Assessment

Evaluates how well current security practices protect firm and client data

Establishes a baseline for improvement planning

Considers policies, technical safeguards, training, and vendor oversight

Incident Response Plan

- Defines roles, responsibilities, and priority actions during a cyber incident
- Ensures structured response instead of improvised reaction
- Reduces miscommunication and delays during emergencies
- Includes communication procedures (internal & external)
- Details how to isolate affected systems and begin restoration
- Requires testing through table-top or simulation exercises annually

Implementation Timeline

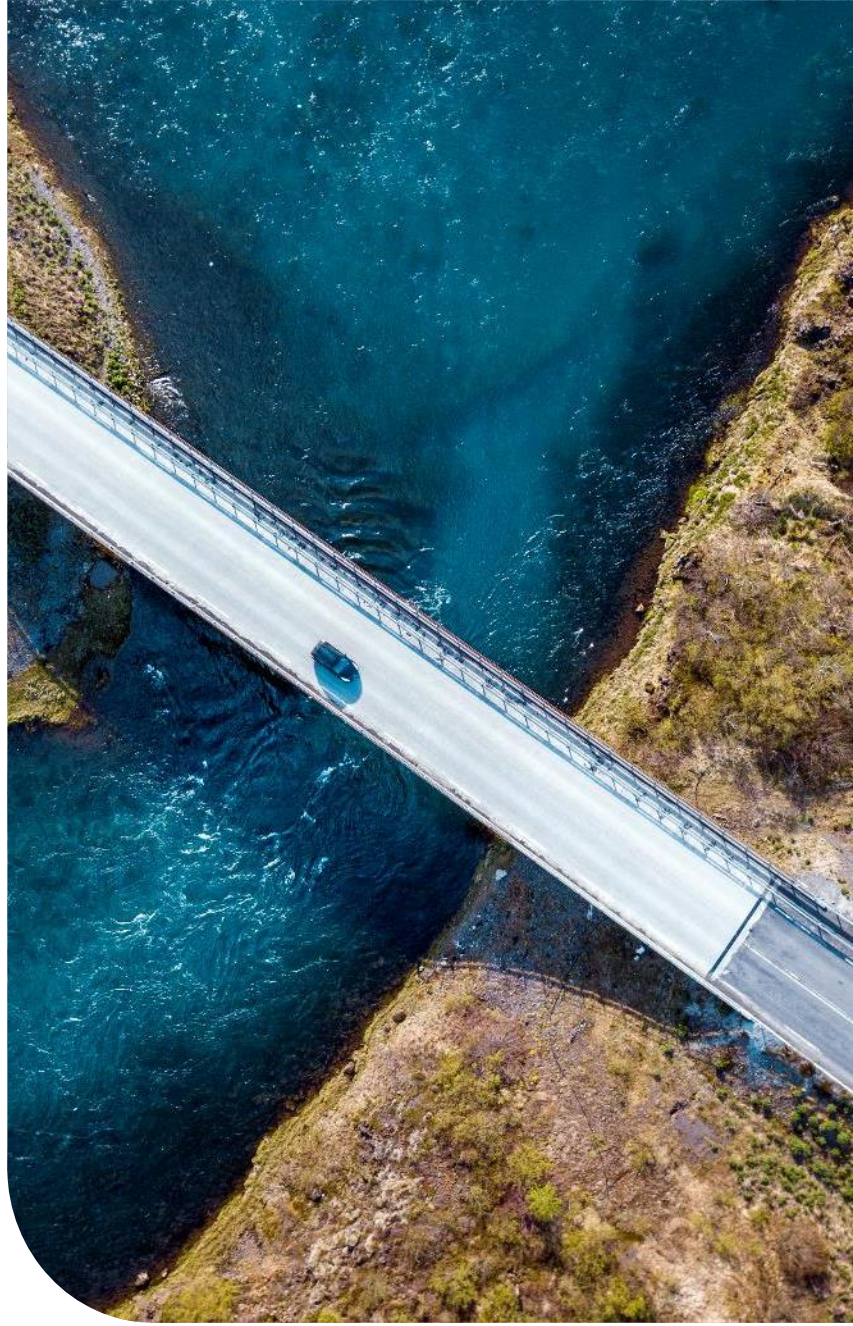
- Months 1–6: Conduct initial Data Mapping and review system inventory
- Months 6–12: Complete full Data Mapping including vendor and access review
- Months 12–18: Conduct Cybersecurity Maturity Assessment
- Months 18–30: Draft and refine Incident Response Plan
- Month 30–36: Conduct first tabletop exercise and finalize IRP
- Annually: Update IRP, retrain staff, repeat Maturity Assessment

Benefits to Law Firms

- Reduces downtime and operational disruption during incidents
- Protects confidentiality and trust in attorney-client relationships
- Supports ethical duties under professional conduct rules
- Improves insurer confidence and claim defensibility
- Clarifies vendor cybersecurity expectations
- Positions firm to adapt to future regulatory changes

Next Steps

- Appoint a cybersecurity responsible individual or small internal team
- Begin data inventory using spreadsheets or existing system logs
- List critical vendors and request their security documentation
- Draft response roles and communication procedures before technical playbooks
- Train all staff regularly on secure data handling and phishing recognition
- Schedule yearly tabletop IRP practice sessions



Questions & Discussion

- Discussion and questions welcomed

Kennedys

Kennedys
KennedysLaw
KennedysLaw
KennedysLaw

kennedyslaw.com