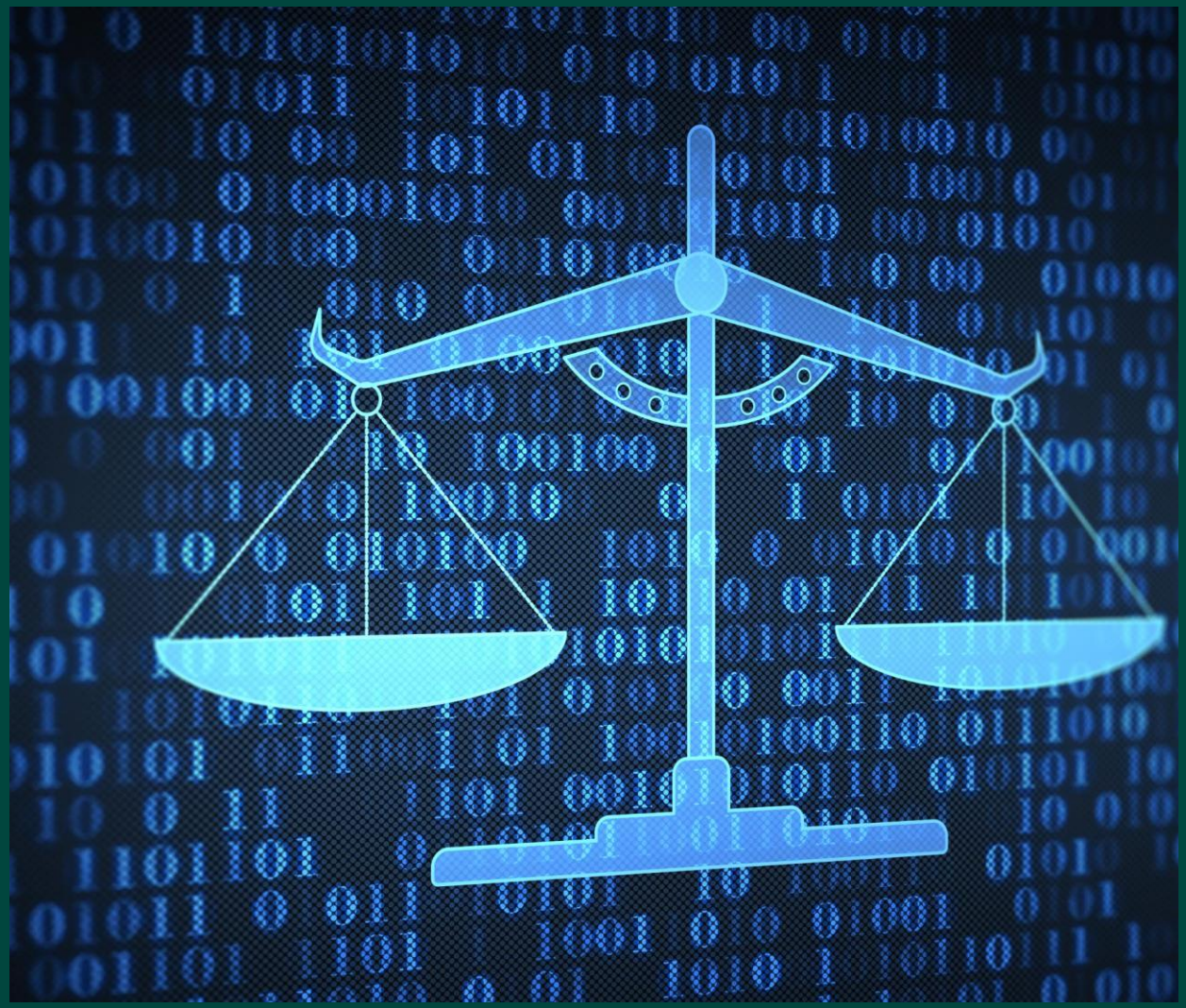


Cybersecurity Brief for Law Firms: Risks, Ethics, and Practical Frameworks

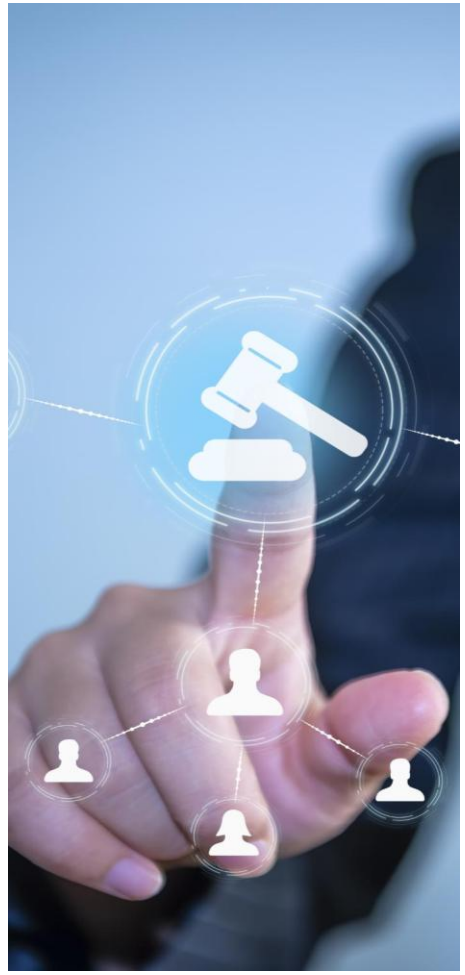
Carmine Cicalese
President, CYBER CIC

"Attorneys are never going to buy cybersecurity if they think they know more than you. If you were so smart, you would have gone to law school."

– David F., Legal Mediator

Learning Objectives and Expected Outcomes

- Understand current cyber threat environment
- Identify common attack methods
- Recognize ethical and legal cybersecurity obligations
- Understand the Cybersecurity “Triad of Triads” framework
- Visualize your firm’s cybersecurity posture



Agenda

Threat Landscape and Risks

Legal & Ethical Requirements

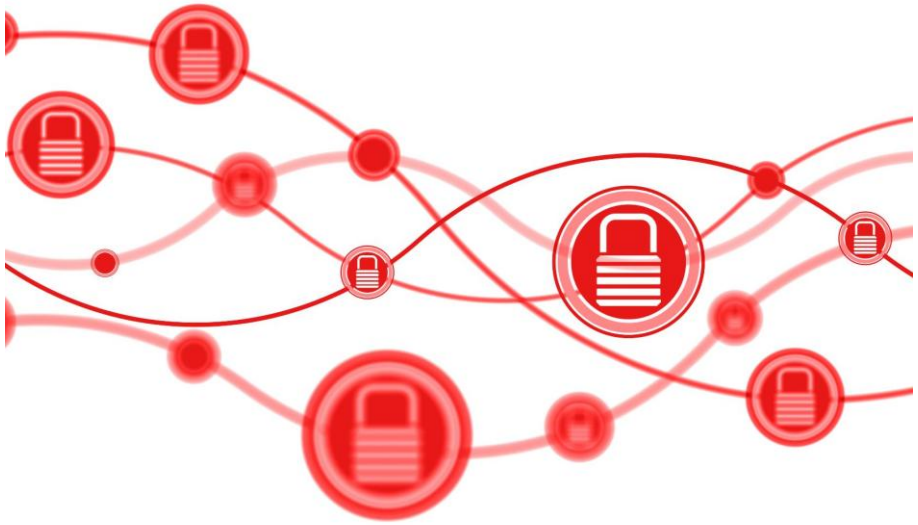
Cybersecurity Triad of Triads

Cybersecurity Framework 2.0

Questions

Threat & Ethics Landscape

Cyber Threat Landscape Facing Law Firms



Numerous Small Sophisticated Criminal Gangs

Cybercrime is a $13T business and the third largest economy after the US and China. Attacks on law firms doubled in 2025. Many nation state experts moonlight with cyber gangs.

High-Value Target

Law firms hold sensitive multi-client data but often lack the security maturity of larger sectors, making them attractive targets.

Attack Vectors

Common cyberattack entry points include phishing, social engineering, compromised credentials, unpatched systems, and insecure remote access.

Interconnected Legal Ecosystem

Information sharing with courts, clients, and vendors expands attack surfaces, risking multi-party exposure.

Common Cyber Incidents in Legal Practice

Unauthorized Access – Wolf Haldenstein Data Breach

Compromised credentials from phishing or password reuse enable attackers to steal sensitive legal data over time.

Business Email Compromise – Peebles vs. Carolina Container

Attackers impersonate staff and vendors to redirect funds and manipulate critical communications causing severe financial loss.

Ransomware Attacks – Jeff Anderson & Associates

Ransomware encrypts firm systems, disrupting operations during court deadlines and important legal proceedings.

Third-Party and Insider Risks – Fried Frank

Vendor breaches and insider errors expose sensitive data, highlighting vulnerabilities beyond direct firm attacks.

Risk - Data Offers Leverage to Attackers

Confidential and Sensitive Data

Legal files contain privileged communications making breaches severely damaging.

Time-Sensitive Impact

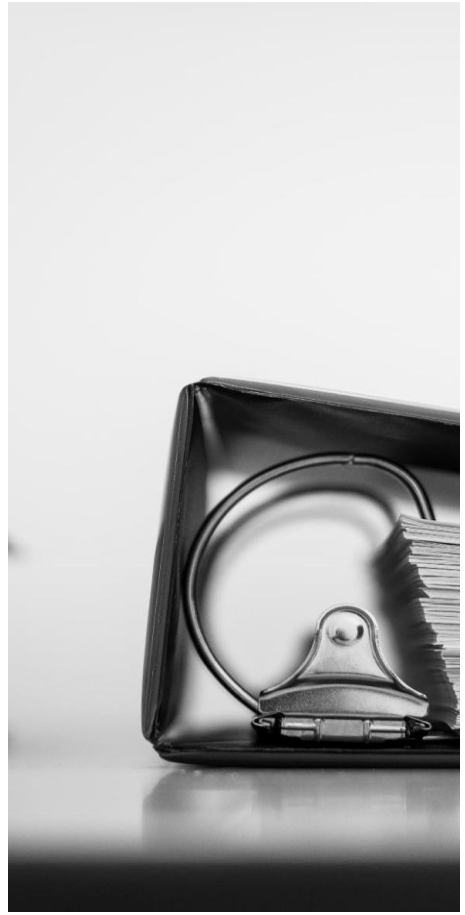
Legal deadlines create urgency, amplifying attacker leverage through extortion tactics.

Reputational Risks

Breaches undermine client trust and law firm reputation, affecting business competitiveness.

Financial Transactions

Protecting IOLTA, trust, and past and current employee banking data is essential.



Ethical Duties of Technological Competence and Confidentiality

Duty of Technological Competence (ABA Model Rule 1.1)

Attorneys must maintain knowledge of technology benefits and risks relevant to client representation.

Confidentiality in Digital Environment (ABA Model Rule 1.6)

Confidentiality extends to protecting client data across emails, cloud services, and mobile devices.

Multijurisdictional Challenges

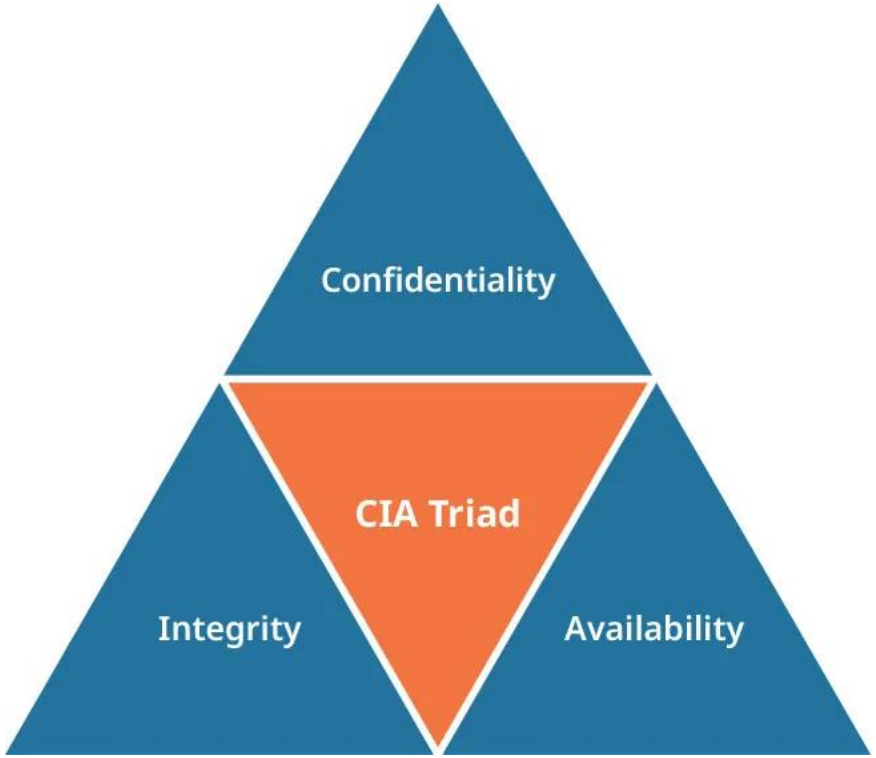
Handling data across states complicates compliance due to differing notification thresholds and definitions.

Third Party Risk Management and Preparedness

Proactive breach planning and due diligence helps law firms meet legal obligations and avoid fines or reputational damage.

Cybersecurity Triad of Triads Framework

Triad One: Confidentiality, Integrity, and Availability



Confidentiality in Security

Confidentiality prevents unauthorized data access, protecting sensitive information with encryption and access controls.

Maintaining Data Integrity

Integrity ensures information accuracy and prevents unauthorized alterations to maintain trust and reliability.

Ensuring Availability

Availability guarantees authorized users can access information and systems when needed without interruption.

Triad Two: People, Process, and Technology

Role of People in Security

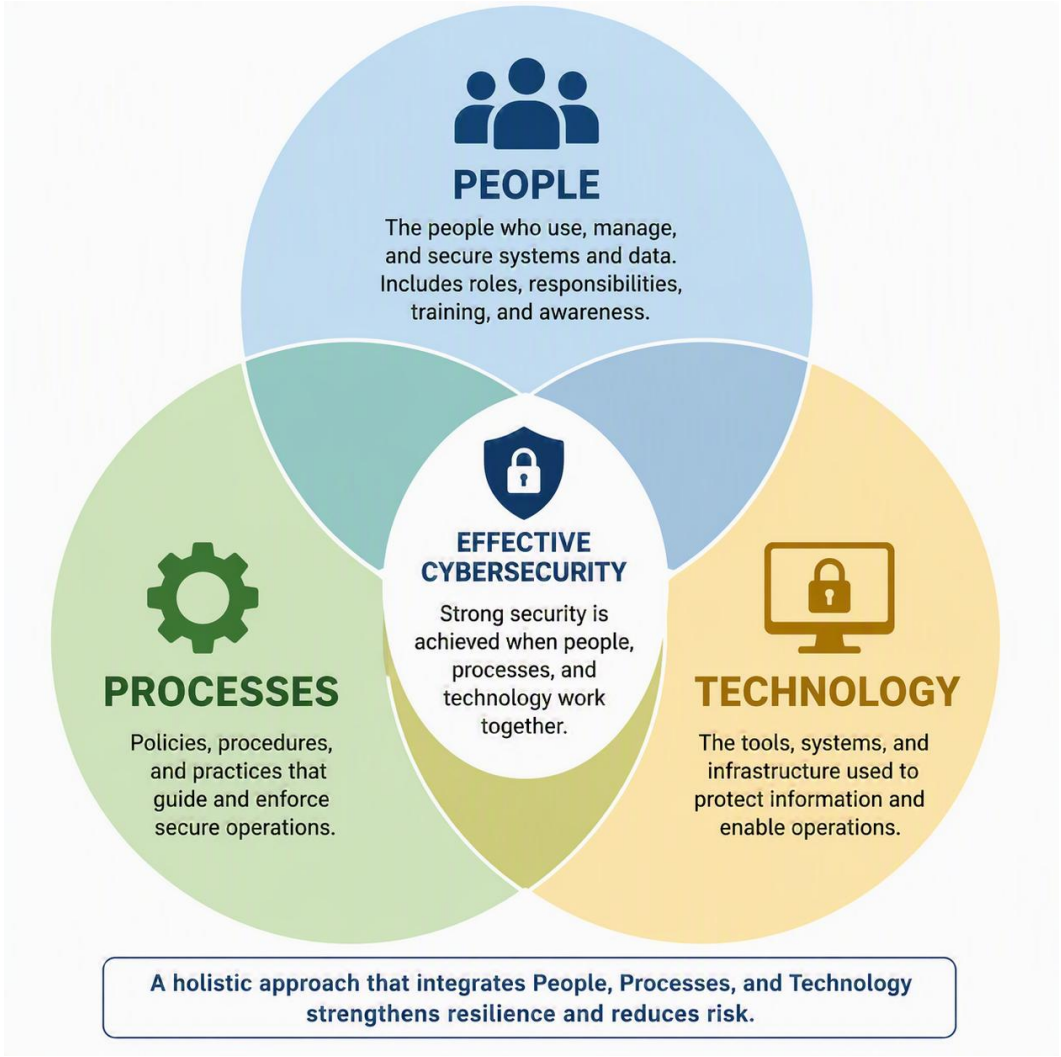
People are the greatest cybersecurity vulnerability and strongest defense requiring training and accountability.

Importance of Processes

Processes provide policies and workflows ensuring consistent security practices and clear responsibilities.

Technology as a Tool

Technology includes security tools like firewalls and access management but must be properly managed.



Triad Three: Business Pillars

Integration of IT and Security

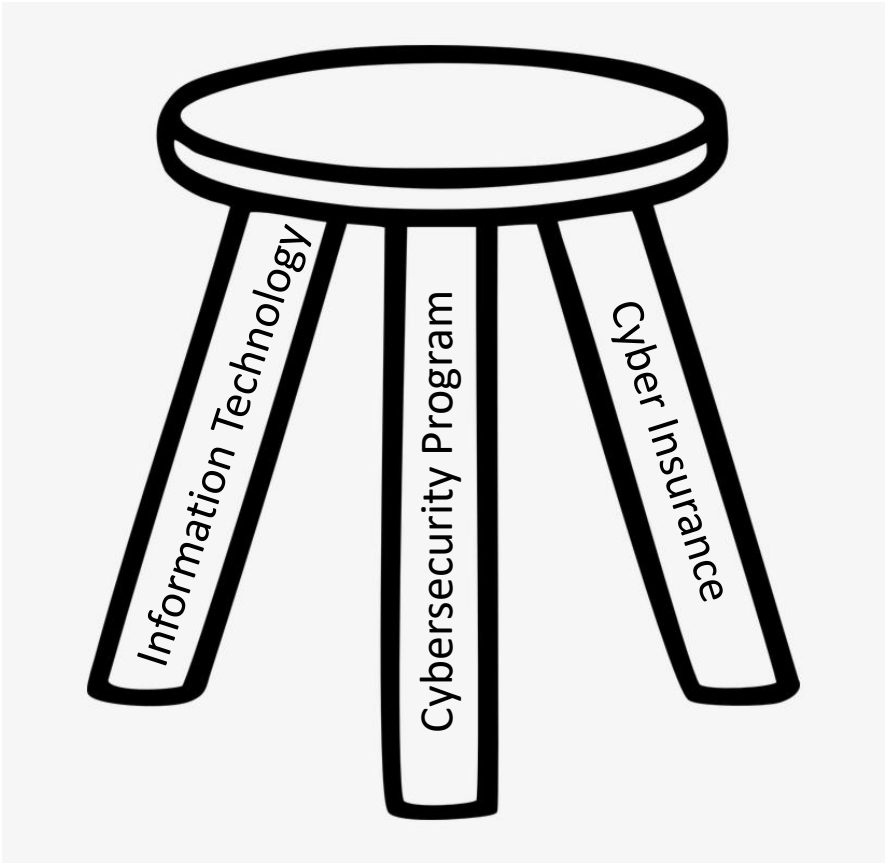
Information technology supports daily business functions, while cybersecurity protects these operations from threats and disruptions.

Financial Risk Management

Cyber insurance helps manage residual financial risks by transferring risk rather than eliminating it entirely after controls.

Business-Aligned Cybersecurity

Security decisions are risk decisions, balancing operational efficiency with protection to support business objectives effectively.



Assessment, Action, and Takeaways

Visualizing Cybersecurity Posture with NIST CSF 2.0

Structured Cybersecurity Model

NIST CSF 2.0 offers a clear framework organizing cybersecurity into governance, protection, detection, and recovery functions.

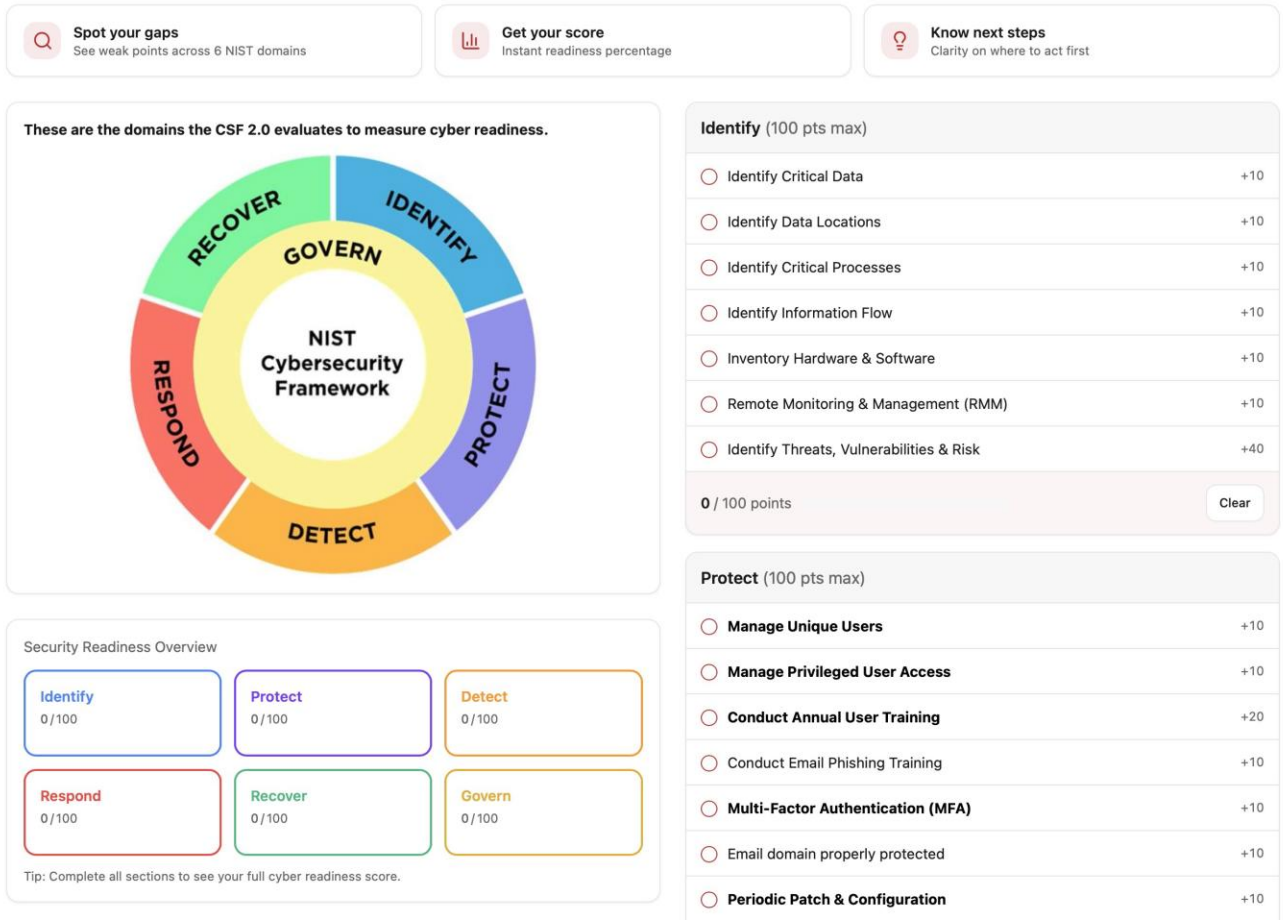
Visualization and Continuous Improvement

Visualization tools help assess maturity levels, track progress, and support ongoing cybersecurity enhancements.

Flexible Risk-Based Approach

NIST CSF 2.0 supports scalable, risk-based decisions aligned with business goals without requiring formal certification.

https://www.icat.cybercic.com



Action Plan for Law Firms

Risk Assessment and Governance

Start with a comprehensive risk assessment covering technology, people, and processes to understand cybersecurity posture.

Phased Roadmap Development

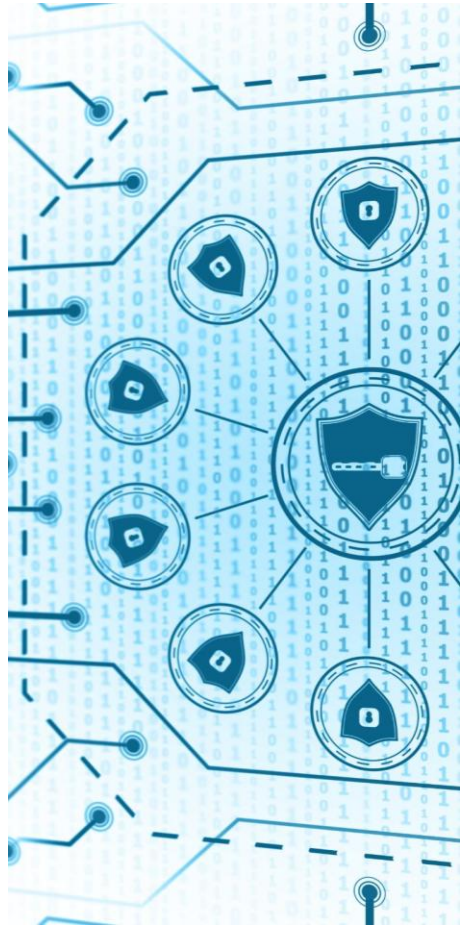
Develop a prioritized, phased roadmap focusing on high-impact improvements and resource constraints.

Technical and Process Controls

Implement access management, backups, monitoring, incident response, and vendor management controls.

Training and Continuous Improvement

Conduct regular training and update cybersecurity plans to adapt to evolving threats and technologies.



Key Takeaways and Closing Discussion

Law Firms as Cyber Targets

Legal data's sensitivity makes law firms prime targets for cyberattacks, requiring vigilant protection strategies.

Ethical and Legal Cyber Obligations

Cybersecurity is linked with ethical and legal duties, demanding proactive risk engagement by attorneys.

Risk-Based Cybersecurity Measures

Most cyber incidents can be prevented through risk-based measures integrating people, processes, and technology.

Frameworks for Cyber Risk Management

Frameworks like Cybersecurity Triad and NIST CSF 2.0 enable practical cyber risk management without deep technical expertise.

QUESTIONS???

Carmine Cicalese
carm@cybercic.com
717-706-3832