



Cybersecurity Do's and Don'ts

PAMIC – Financial Management Seminar

September 18, 2025

Baker Tilly Advisory Group, LP and Baker Tilly US, LLP, trading as Baker Tilly, are members of the global network of Baker Tilly International Ltd., the members of which are separate and independent legal entities. Baker Tilly US, LLP is a licensed CPA firm that provides assurance services to its clients. Baker Tilly Advisory Group, LP and its subsidiary entities provide tax and consulting services to their clients and are not licensed CPA firms.



Introduction



Russ Sommers
Principal, Baker Tilly

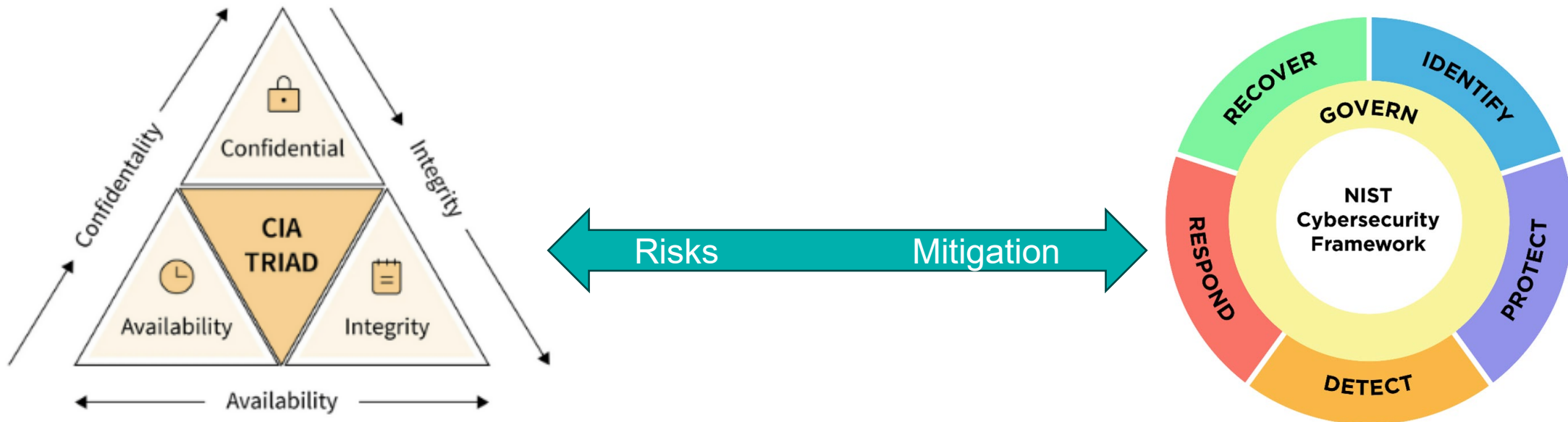
P: +1 (848)235-0178

E: Russell.Sommers@bakertilly.com

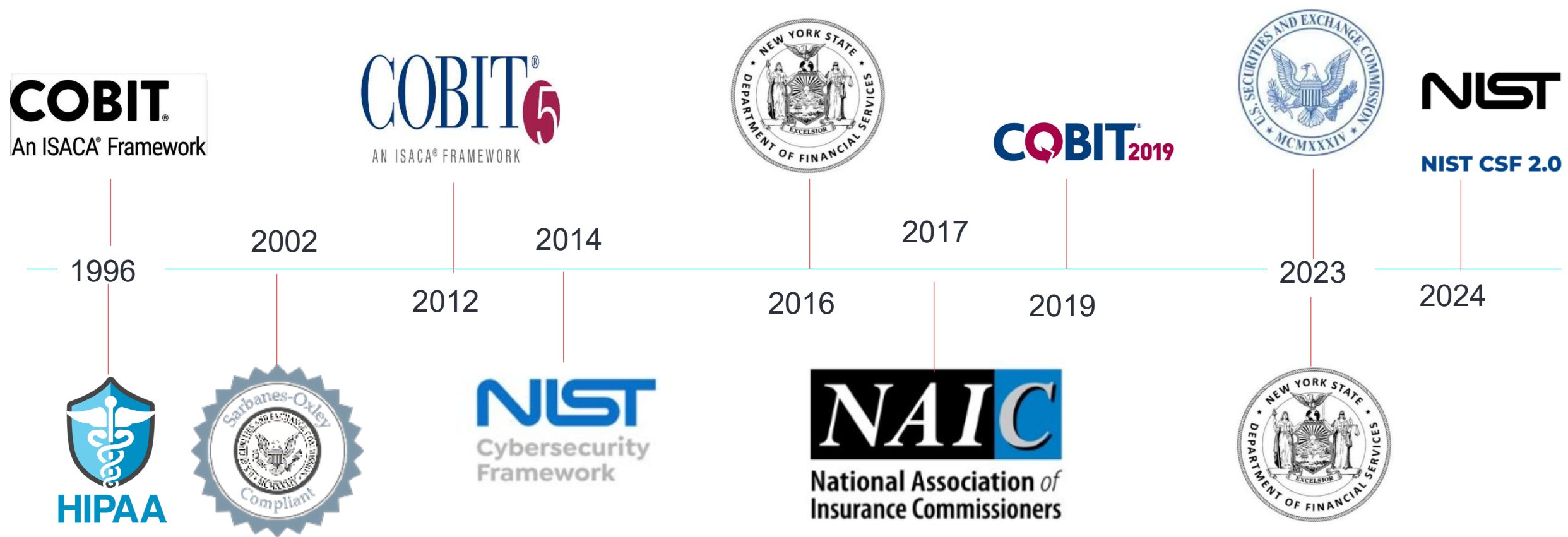
Background History and Evolution

What is cybersecurity

- Cybersecurity is the practice of protecting systems, networks, and data from digital threats like hacking, malware, and data breaches.
- It involves tools, policies, and practices to prevent, detect, and respond to cyber incidents.



Evolution of Cybersecurity



Cybersecurity State of the State

Recent Cyber Breaches and Trends

Recent Cybersecurity Events in 2025

Key Takeaways

2025 Data Breach Investigations Report | Verizon

- 17% of breaches were Espionage motivated
- 20% of breaches involved exploitation of vulnerabilities (34% increase from prior year)
- 22% featured attacks on VPNs and edge devices (up 8x from prior year)
- 30% of breaches involved vendors (double from prior year)
- 44% featured ransomware (up from 32% prior year)
- 60% of breaches involved human errors or social engineering
- 95% of breaches include Server as the most common asset



WHAT COULD GO WRONG?

Types of Cybersecurity Attacks

1. Phishing
2. Malware based attacks
3. Denial of service based attacks
4. Spoofing
5. Identity based attacks
6. Code injection attacks
7. Supply chain attacks
8. Social engineering attacks
9. Insider threats
10. DNS tunneling
11. IOT based threats
12. AI powered attacks



Example - Cybersecurity Threats

Fake AI content generator applications

Text-to-Malware: How Cybercriminals Weaponize Fake AI-Themed Websites

Fake AI video generators infect Windows, macOS with infostealers

Espionage – North Korean IT Worker infiltration

The ultimate insider threat: North Korean IT workers

Impersonation – FBI Internet Crime Complaint Center

FBI Warns of Scammers Impersonating the IC3

Cybersecurity Expectations in the Insurance Industry

Evolving Program Expectations



Governance

Cybersecurity program

Cybersecurity policy

Risk assessment



People

Access control

Cybersecurity personnel

Cybersecurity intelligence

Training



Process

Asset Management

Audit trail

Secure development

Incident response and
required notifications



Technology

Vulnerability management

Multi-factor authentication

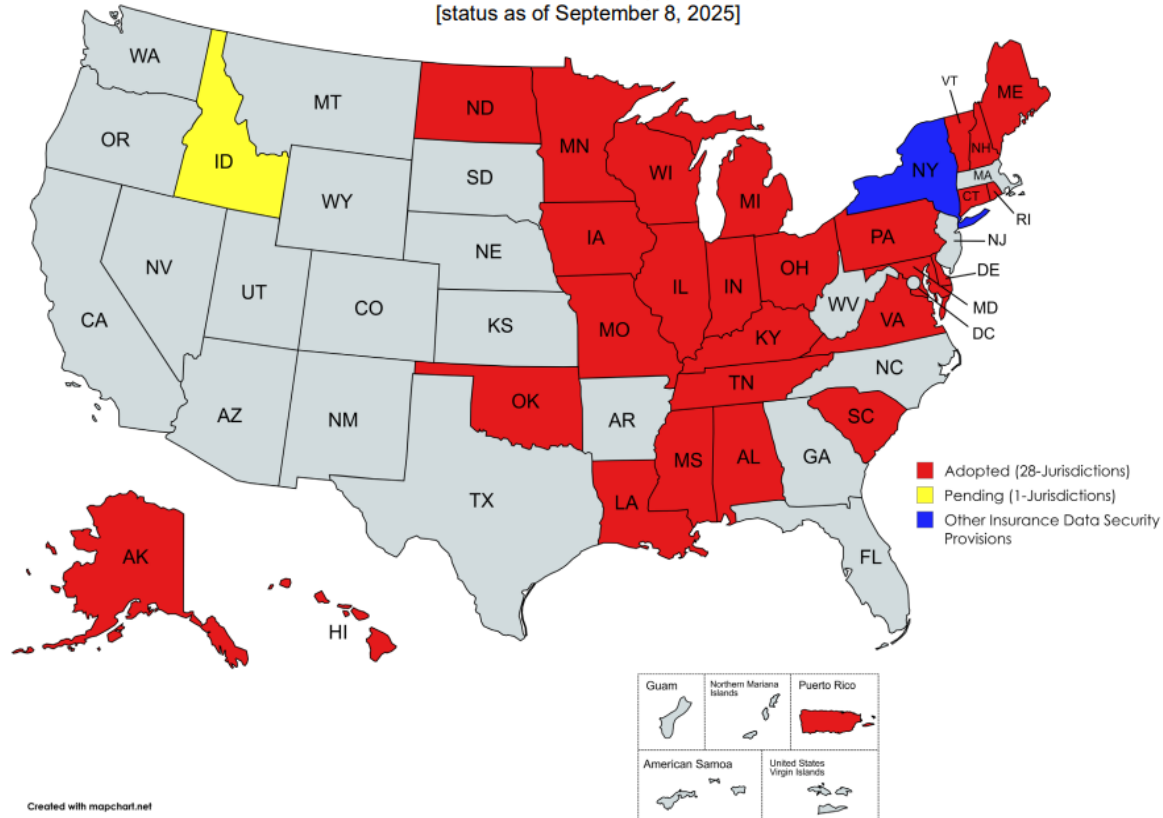
Ongoing monitoring and
alerting

Encryption

Cybersecurity Expectations in the Insurance Industry

NAIC – Insurance Data Security Model Law

Implementation of Model Act #668
Insurance Data Security Model Law
[status as of September 8, 2025]



This map represents state action or pending state action addressing the topic of the model. This map does not reflect a determination as to whether the pending or enacted legislation contains all elements of the model or whether a state meets any applicable accreditation standards.



Section 1. Title

Section 2. Purpose and Intent

Section 3. Definitions

Section 4. Information Security Program

Section 5. Investigation of a Cybersecurity Event

Section 6. Notification of a Cybersecurity Event

Section 7. Power of Commissioner

Section 8. Confidentiality

Section 9. Exceptions

Section 10. Penalties

Section 11. Rules and Regulations

Section 12. Severability

Section 13. Effective Date

- A. Implementation of an **Information Security Program**
- B. Objectives of Information Security Program
- C. **Risk Assessment**
- D. Risk Management
- E. Oversight by Board of Directors
- F. Oversight of **Third Party** Service Provider Agreements
- G. Program Adjustments
- H. **Incident Response Plan**
- I. **Annual Certification** to Commissioner of Domiciliary State

Source: http://www.naic.org/cmte_ex_cswg.htm

NYDFS Part 500 – Amended November 2023



500.02 –
Cybersecurity
program

500.03 –
Cybersecurity
policy

500.04 –
Cybersecurity
governance

500.05 –
Vulnerability
management

500.06 – Audit trail

500.07 – Access
privileges and
management

500.08 –
Application
security

500.09 – Risk
Assessment

500.10 –
Cybersecurity
personnel and
intelligence

500.11 – Third-
party service
provider security
policy

500.12 – Multi-
factor
authentication

500.13 – Asset
management and
data retention
requirements

500.14 –
Monitoring and
training

500.15 –
Encryption of
nonpublic
information

500.16 – Incident
response and
business continuity
management

500.17 – Notices
to superintendent



Cybersecurity Best Practices – Boards of Directors

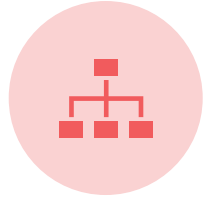
Cybersecurity Best Practices for Boards of Directors

- Oversight of the covered entity's cybersecurity risk management.
- Have sufficient understanding of cybersecurity risk and related matters to exercise such oversight.
- Require management to develop, implement and maintain a robust cybersecurity program aligned with a comprehensive framework.
- Receive regular updates about cybersecurity risks and the effectiveness of the organization's cybersecurity program.
- Foster a culture of cybersecurity and determine how management embeds cybersecurity risk into strategic decision making.
- Ensure management has allocated sufficient resources to implement and maintain an effective cybersecurity program.
- Understand the company's organizational resilience expectations, capabilities and forward-looking enhancements.
- Encourage management to seek independent assessments of program effectiveness.

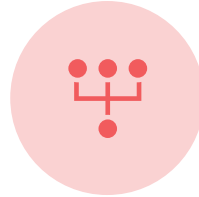


Common IT and Cybersecurity Audit and Examination Observations

Common Audit/Examination Findings



IT governance,
including policies
and procedures



Access control,
provisioning and
review



Authentication
standards



Organizational
Resiliency testing



Risk assessment



Third-party risk
management



Logging and
monitoring



Asset
Management

Key Takeaways And Q&A

Maintaining a Comprehensive Information Technology & Cybersecurity Program

IT governance

- Policies and procedures
- People
- Role of executive management and those charged with governance

Access control

- User access provisioning/deprovisioning and review
- Segregation of duties
- Security administration
- Elevated privileges
- Access review
- Physical security – access and monitoring

Change management and SDLC

- Planning
- Development
- Testing
- Approval
- Production
- Segregation of duties and environments

Contingency planning

- Backup and restore processes
- Recovery: Disaster Recovery and Business Continuity
- Response: Incident Response and Crisis Management

Security operations

- Network security: IPS/IDS, FW
- Encryption solutions
- Monitoring and alerting solutions: SIEM, network performance, DLP, endpoint
- Vulnerability management: scanning, patching

IT operations

- System integrations
- Job scheduling and monitoring
- Environmental controls

Vendor management

- Planning
- Due diligence
- Contracting and onboarding
- Monitoring: performance, strategy/financial, information security
- Termination

Training and awareness

- Technical training
- Security awareness and reinforcement
- Anti-phishing training

Data governance

- Key report management
- Data flow mapping
- Data intake, sharing and processing

Asset management

- Inventory
- Configuration management
- Acquisition, maintenance and disposal
- Record retention and destruction



Key Takeaways



Stakeholder Involvement

Cybersecurity is a business issue, not just an IT issue



Continuous Improvement

Test, assess results, change then retest



Train Your People

What does good look like?
Train, test, reinforce



Questions?