
go
cyber
COLLECTIVE

October Announcements

Serving Our Communities

Thank You, Taft Law!

LEADS Workshop: Nov. 4

2025 GoCyber CTF Nov. 6

Table Tops for Your Organization

GoCyber Christmas: Dec. 17

October GoCyber Collective Keynote Speaker

-Zachary Heck
-Partner – Taft Law
-Certified Information Privacy Manager (CIPM)
-Artificial Intelligence Governance Professional by IAPP
-Focus on Privacy & Data Security
-Guidance Post-Breach

Taft

From Server Room to Courtroom: Taking IT Issues to Legal Before They Take You Down

Zachary Heck, AIGP, CIPP, CIPM
Partner / Taft Dayton

GoCyber Collective

October 15, 2025

Taft/

Risk Mitigation and Compliance

- Legal counsel ensures IT efforts align with privacy and data security laws, regulations, and standards.

- Helps to minimize the risk of fines, litigation, and regulatory investigations in both routine operations and crisis scenarios.

Taft/

Security Vulnerabilities

1. Data Governance

Unauthorized use of sensitive data in model training, leading to GDPR, CCPA, HIPAA violations

2. Vendor Risk

Lack of due diligence or safeguards for third-party technology vendors

Hidden IP infringement liability

3. Internal Misuse

Employee error, lack of oversight

Biased outputs, misinformation, confidentiality breaches can result in bias outputs, misinformation, or breaches of confidentiality

Taft

International Law

- **Global Standards tend to be more onerous**
  - EU – General Data Protection Regulation (“GDPR”)
  - United Kingdom – (UK GDPR)
  - Switzerland – Federal Act on Data Protection (“FADP”)
  - China – Personal Information Protection Law (“PIPL”)
  - Brazil – Lei Geral de Proteção de Dados (“LGPD”)
  - India – Digital Personal Data Protection Act (“DPDPA”)
- **Most international laws don’t distinguish between personal data used for business purposes.**
- **Broad extraterritorial scope**
  - Many apply to companies regardless of where the company is located
- **Penalties are more severe.**
  - Some even impose criminal sanctions (e.g., Switzerland)
- **Strict requirements for transferring personal data to companies in “third countries” (e.g., United States).**

Taft/

Other US Laws and Standards

- State laws regulating consumer health data (WA, WV, CT)
- TCPA (Text/Call compliance)
- Child Online Privacy Protection Act (Website operators/minors)
- Gramm Leach Bliley (Financial institutions)
- HIPAA (Healthcare providers, payers and others)
- Payment Card Industry Data Security Standards (“PCI-DSS”)
- ISO or NIST certifications/SOC Audits
- Government Contracting (DFARS 252.204-7012)
- SEC Reporting Requirements (2023)
- FTC Safeguards Rule Updates and Breach Reporting (2024)

Taft/

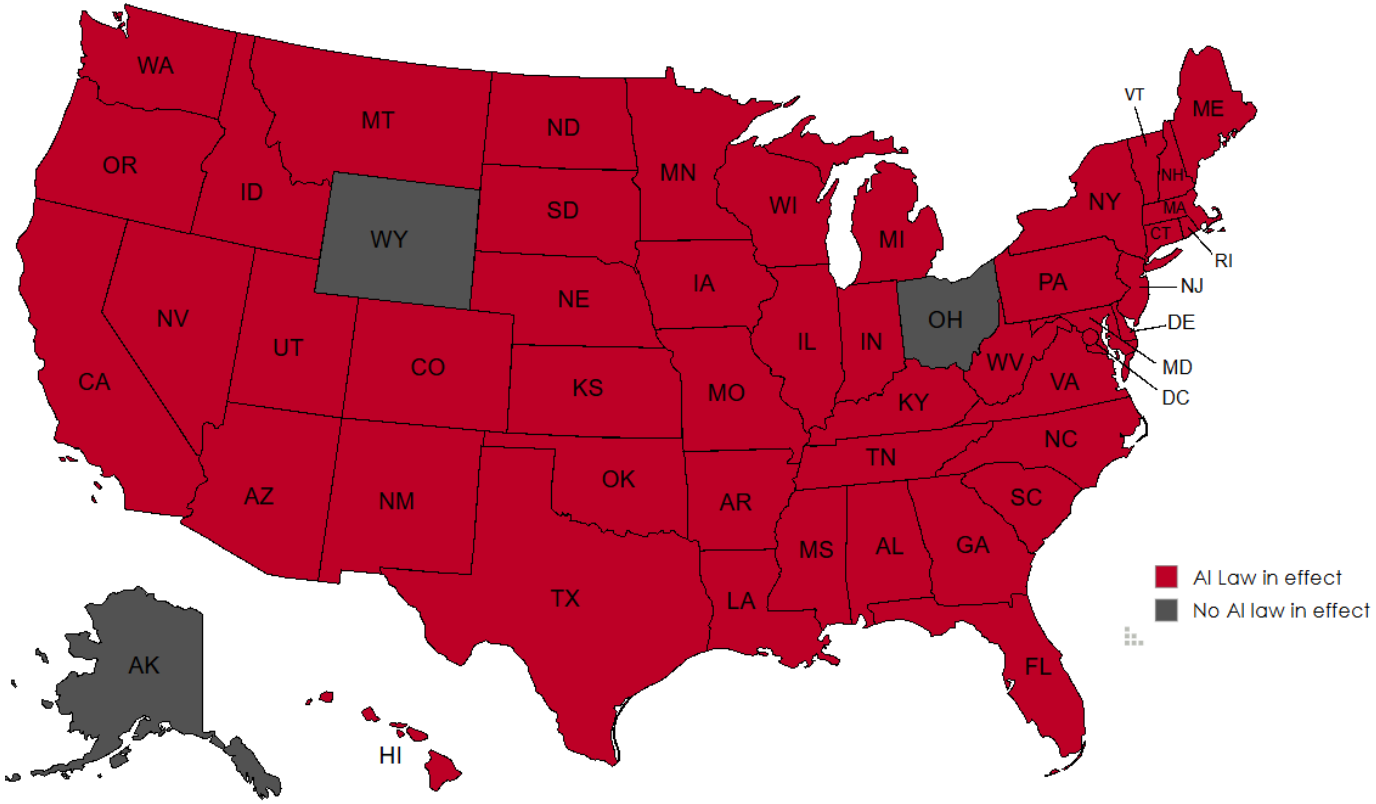
State Privacy Laws Currently or Soon to be in Effect

- California (2020)
- Colorado (2023)
- Connecticut (2023)
- Virginia (2023)
- Utah (2023)
- Oregon (2024)
- Texas (2024)
- Montana (2024)
- Iowa (2025)
- Tennessee (2025)
- Delaware (2025)
- New Jersey (2025)
- New Hampshire (2025)
- Nebraska (2025)
- Maryland (2025)
- Minnesota (2025)
- Indiana (2026)
- Kentucky (2026)
- Rhode Island (2026)

Taft/

AI Laws Across the U.S

- Over 160 AI-specific laws enacted through 2025…and counting!
  - 40% target AI images / deepfakes
  - 25% targeting government / political campaign use
  - 20 automated decision-making laws
  - 9 AI transparency-related laws
  - 2 comprehensive AI laws (CO and TX)



Taft/

Attorney-Client Privilege

- Early engagement with legal counsel protects sensitive communications and investigations under attorney-client privilege. This strategic move preserves the confidentiality of findings, especially during internal or forensic investigations after a security incident.
- Privilege can shield forensic reports and analyses from opposing parties in litigation or regulatory probes.

Taft/

Fortifying Security Frameworks with Legal Precision

- Legal counsel ensures that IT operations and initiatives comply with federal, state, and international data privacy laws, reducing risk of fines and regulatory enforcement.
- Early involvement helps organizations navigate complex regulations like GDPR, HIPAA, CCPA, and industry-specific requirements (NIST 800-171, PCI-DSS)

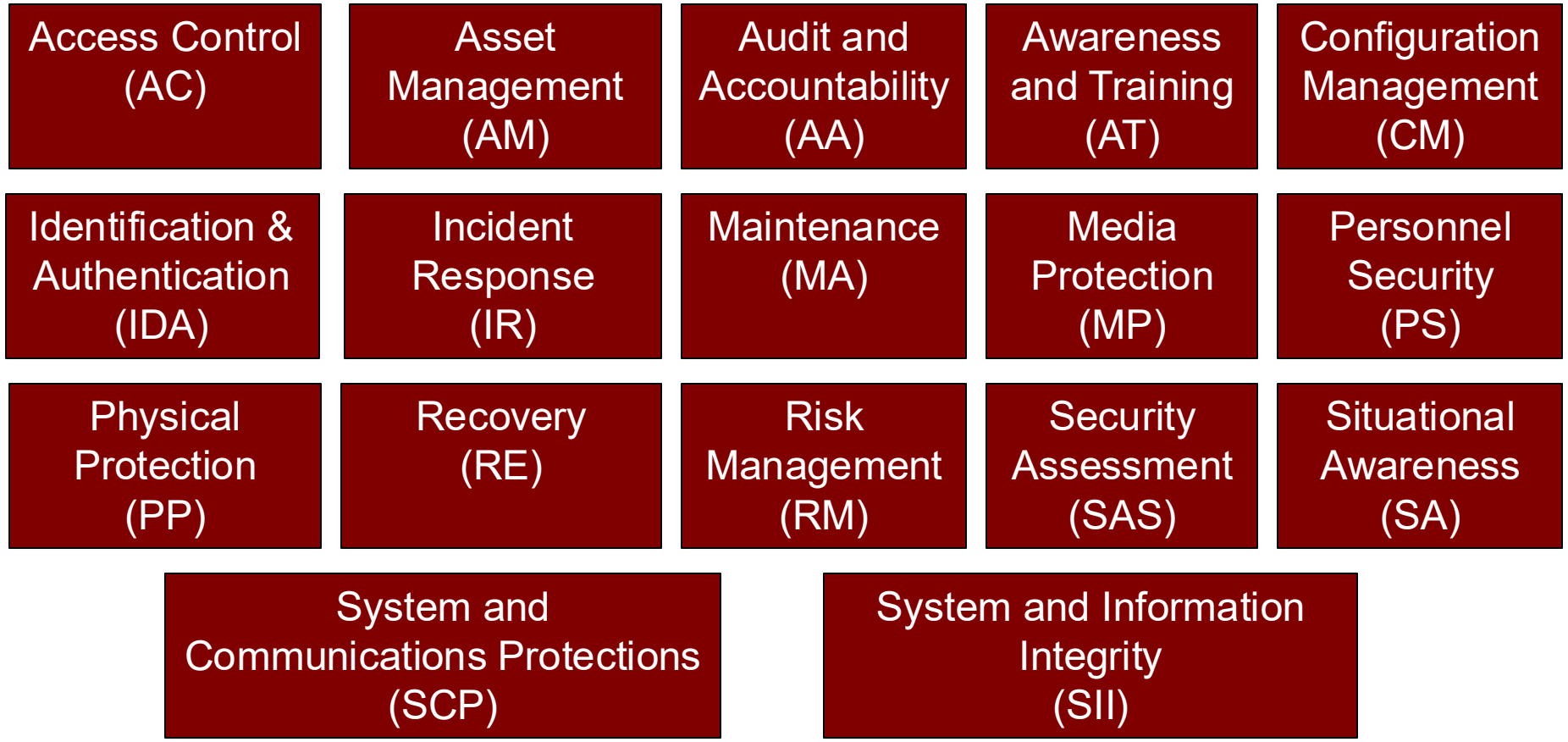
Taft/

Guidance on Contracts and Liability

- Assess and negotiate IT contracts, focusing on clauses related to data ownership, cyber liability, and third-party responsibilities.
- Legal input helps prevent disputes and manage exposure to lawsuits or regulatory action stemming from IT mishaps.

Taft/

Government Contract Security



Taft/

Control Cataloging

Control Family	Number of Controls
Access Control	22
System and Communication Protection	16
Identification and Authentication	11
Configuration Management	9
Audit and Accountability	9
Media Protection	9
System and Information Integrity	7
Maintenance	6
Physical Protection	6
Risk Assessment	3
Awareness and Training	3
Security Assessment	4
Incident Response	3
Personnel Security	2
Total	**110**

What is Required Under CMMC 2.0?

CMMC Maturity	Impacted Contractors	Security Requirements
Level 1	Contractors and subcontractors who will process, store, or transmit FCI on unclassified contractor information systems.	15 basic safeguarding requirements and procedures designed to protect covered contractor information systems. All 15 requirements are currently required under FAR Clause 52.204-21.
Level 2	Contractors or subcontractors responsible for processing, storing, or transmitting CUI on unclassified contractor information systems	110 security requirements specified in NIST SP 800-171.
Level 3	As determined by DoD on a contract-by-contract basis, based on the sensitivity of the CUI involved in the performance of that contract.	110 security requirements specified in NIST SP 800-171. AND 35 selected security requirements from NIST SP 800-172.

Agreements – Specific Data Terms

- **Data Storage Location**
  - Agreements should specify permitted storage locations for all contractor-held data, often limiting storage to approved jurisdictions or data centers prohibiting off-shore or unapproved third-party storage without written consent.
- **Data Processing Security and Scope**
  - Must process data only for explicit contract purposes, using robust security and access controls according to applicable standards and contract requirements, and not allow any form of unauthorized data transfer, modification, or access.

Taft/

Agreements – Specific Data Terms

- **Limits on Further Processing**
  - Require contracting parties to refrain from any further data processing beyond what is permitted by the contract or by law.
  - Prohibit sale, rental, or other forms of unauthorized disclosure.
  - Mandate immediate notification of any requests for data processing outside contract scope.

Taft/

Enable IT to Communicate with Leadership

Legal helps translate technical threats into business and compliance risks, enabling IT leaders to communicate effectively with executives and the board about priorities and resource needs.

Taft/

How Taft Can Help!

Visit Taft's Privacy and Data Security Insights Blog

Taft/

Thank you!

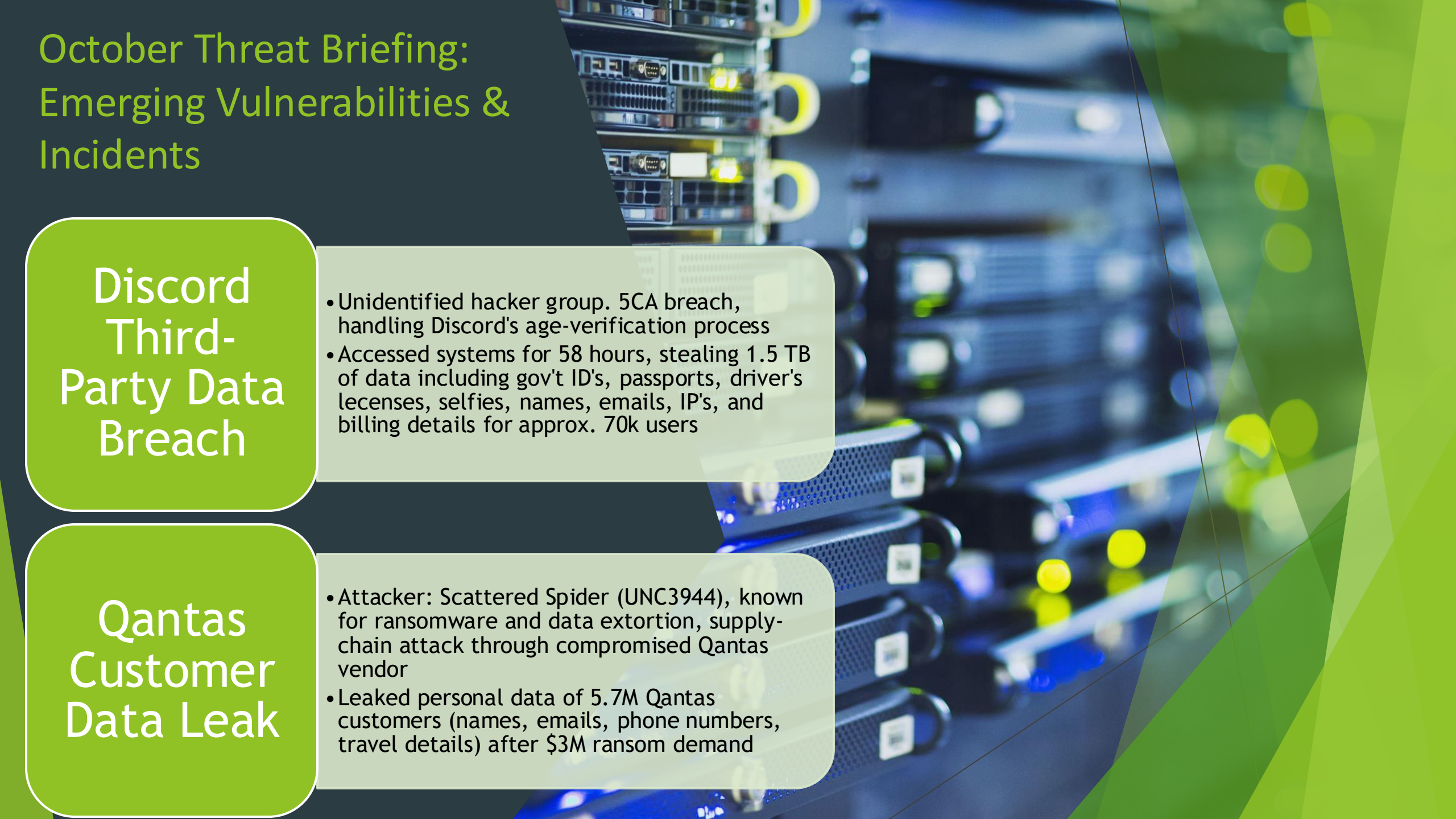
Zachary Heck, AIGP, CIPP, CIPM
Partner | Taft
E: zheck@taftlaw.com
T: (937) 641-2053

Taft/

Threat Briefing

Charles Zugaro – Cybersecurity Analyst – Warren County Telecommunications

October Threat Briefing: Emerging Vulnerabilities & Incidents



Discord Third-Party Data Breach

- Unidentified hacker group. 5CA breach, handling Discord's age-verification process
- Accessed systems for 58 hours, stealing 1.5 TB of data including gov't ID's, passports, driver's lecenses, selfies, names, emails, IP's, and billing details for approx. 70k users

Qantas Customer Data Leak

- Attacker: Scattered Spider (UNC3944), known for ransomware and data extortion, supply-chain attack through compromised Qantas vendor
- Leaked personal data of 5.7M Qantas customers (names, emails, phone numbers, travel details) after $3M ransom demand

October Threat Briefing: Emerging Vulnerabilities & Incidents

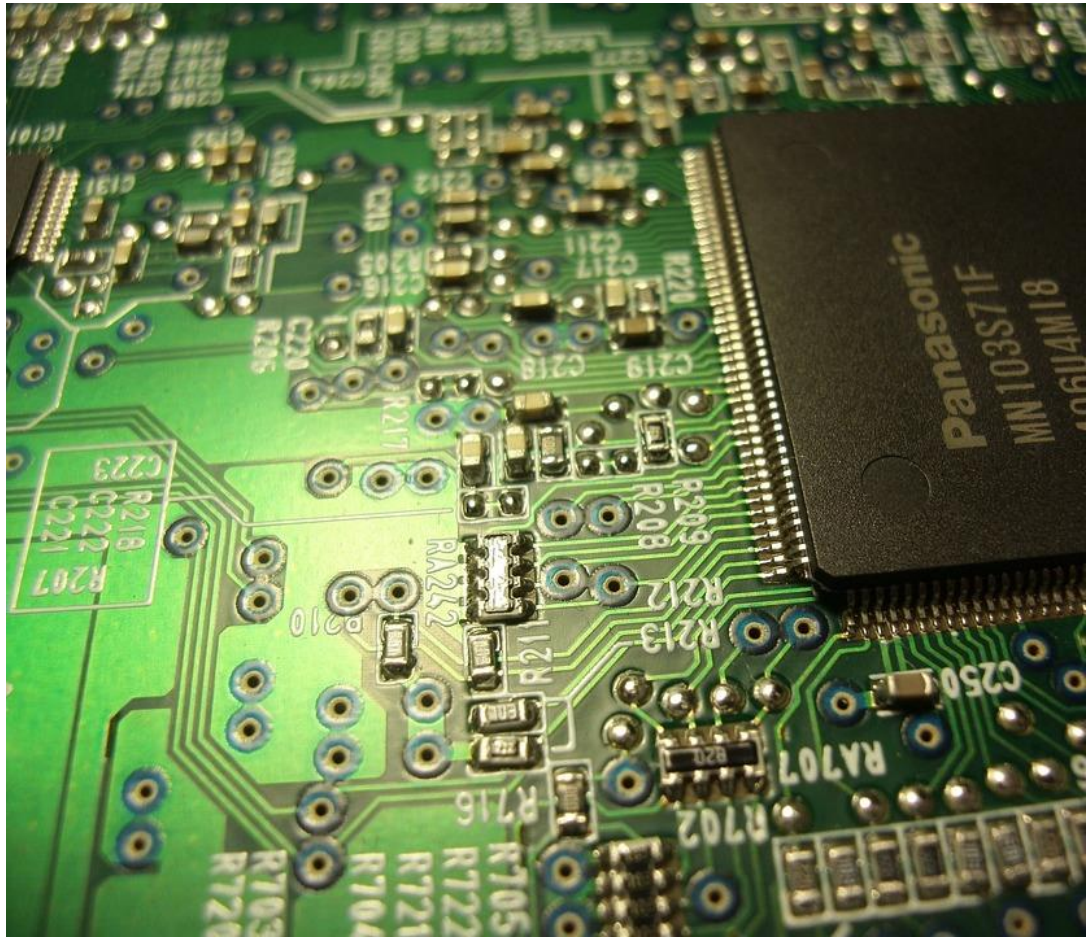
- Oracle E-Business Suite Zero-Day Exploitation
  - Threat Actor: C10p ransomware group, known for enterprise software
  - Attack Vector: Zero-Day vulnerability (CVE-2025-61882, CVSS 9.8) in Oracle E-Business Suite, enabling remote code execution (RCE)
  - Attackers chained CVE-2025-61882 with other flaws for system access, data theft, and encryption. Targeted global enterprises in finance and manufacturing: part of C10p's 2025 ransomware-as-a-service (RaaS) surge

November Speaker: Ann Carbonell – UDRI

- Geospatial Intelligence (GEOINT)
- Mapping the Future Threats
- How Adversaries Target:
  - -Critical Infrastructure
  - -Military Assets
  - -Civilian Sectors
- How Geographic Location Correlates with Cybersecurity Vulnerabilities

October Parting Shots

- Local Gov't/Public Safety SIG – Sun Watch Room
- Education SIG – Wright Patt Room
- Defense Contractor SIG – Hawthorn Room
- Register for CTF, Monthly Meetings and LEADS Workshop
- Turn in your lanyards at the desk



Information

Email me at john@GoCyberCollective.org.

If you have a suggestion on meeting topics, special interest groups, breakfast menu, or anything else we want to hear from you.

You can register for future breakfast meetings from the website.

- GoCyberCollective.org

Taft

Event Sponsors