CALIFORNIA STATE UNIVERSITY
1965
SAN BERNARDINO

Guest Lecture:
Legal Liability and Case Laws in Cybersecurity

About Guest Lecturer

DESMOND ISRAEL ESQ.
Lawyer and Data Privacy/Information Security Practitioner
LLM (Natsec/Cybersec) | LLB | BSc (Mgt. with Computing) | BL | Advanced Diploma (IT)
CISSP | CIPM | CCT | CC | Verified Certificate (Cyberwar, Security and Intelligence)

Founder & Lead Consultant, Information Security Architects Ltd (Rapid7 Gold Partner)
Lecturer, Ghana Institute of Management and Public Administration (GIMPA) School of Law
Consulting Partner, Legal Afrique Unlimited, Ghana
Lead Researcher (Guardian Safety Framework), X-Reality Safety Intelligence (XRSI), California
MemberResearch Consultant, Child Online Africa

Previously
Fellow, Center for AI and Digital Policy, Washington DC
National Cybersecurity Researcher, Internet Security Alliance, Virginia
Head of Legal & Compliance, Halges Financial Technologies Ltd (Korba), Ghana
Technology Lawyer, Financial Mobile Limited
Associate, Nsiah Akuetteh & Co. (Solicitors & Barristers), Ghana
Board Secretary, Technology Lead, Africa Digital Rights Hub LBG, Ghana
Counsel, Etansa Technologies

Memberships:

EC-Council BETA Testing Team (Certified Cybersecurity Technician Exams)
Exam Development Volunteer, ISC2
Ghana Bar Association (GBA)
International Information System Security Certification Consortium (ISC2)
International Association of Privacy Professionals (IAPP)
Institute of ICT Professional Ghana
Internet Society-Special Interest Group (Cybersecurity & Online Safety)
AfricaHackon (Ghana Chapter)

desmond.israel@gmail.com |
Linkedin.com/in/desmondisrael |
@desmond_israel
+233244284133

Session Structure

- Introduction to Legal Liability in Cybersecurity
- Key Legal Liabilities for Cybersecurity Professionals
- Relevant Case Laws and Implications for Cybersecurity Compliance
- Practical Examples of Liability Risks in Data Protection and Privacy
- Review (Question and Answers)

Introduction to Legal Liability in Cybersecurity

Definition and Scope of Legal Liability in Cybersecurity

Legal liability in cybersecurity refers to the **legal responsibilities** and **potential legal consequences** faced by organizations and professionals involved in managing, protecting, and processing digital information. This includes the duty to secure data against unauthorized access, breaches, and cyber threats and to comply with relevant cybersecurity laws and regulations.

Legal liability in cybersecurity can arise from:

Negligence: Failure to take adequate steps to secure data, resulting in harm.

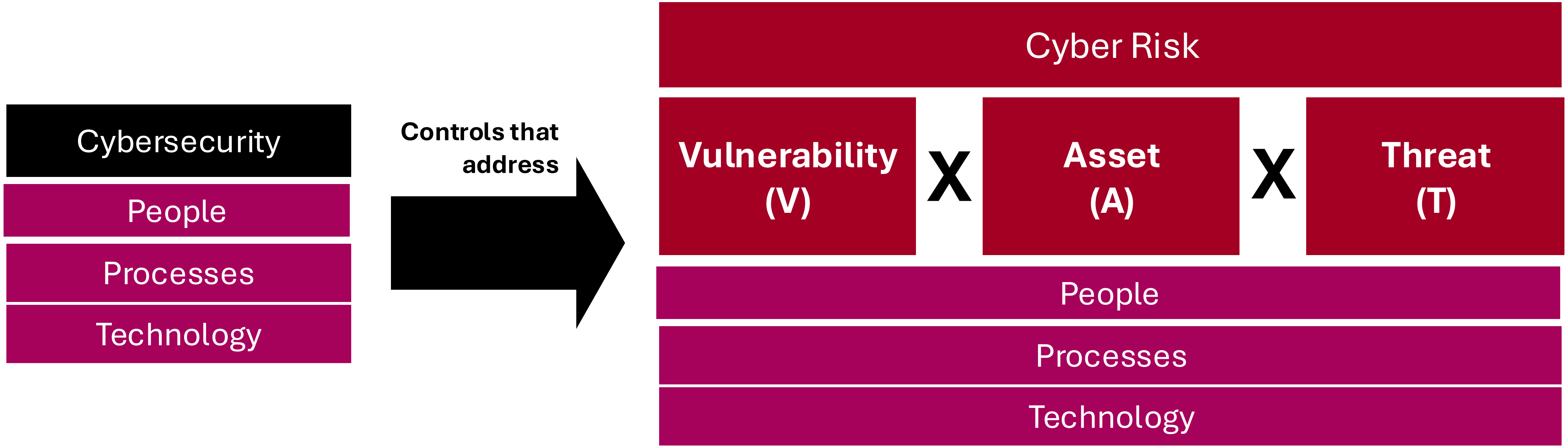
Contractual Obligations: Liability for breaches of contract related to data security or cybersecurity service commitments.

Statutory and Regulatory Compliance: Failure to comply with laws like the Federal Information Security Modernization Act (FISMA), the Health Insurance Portability and Accountability Act (HIPAA), or the California Consumer Privacy Act (CCPA) can lead to legal penalties, fines, and lawsuits.

Consumer Protection Laws: The Federal Trade Commission (FTC) Act, for instance, regulates “unfair or deceptive acts” that harm consumers, which includes inadequate cybersecurity practices in some cases.

Scope: Cybersecurity liability is broad and encompasses not only direct breaches but also the practices and processes that protect or put data at risk. Liability can extend to cybersecurity professionals themselves, company executives, and the organization at large, especially if there’s evidence of inadequate risk management or oversight.

Introduction to Legal Liability in Cybersecurity



Cybersecurity

People

Processes

Technology

Controls that address

Cyber Risk

Vulnerability (V) X Asset (A) X Threat (T)

People

Processes

Technology

Understanding Cybersecurity and Cyber Risk

Introduction to Legal Liability in Cybersecurity

Why Cybersecurity Professionals Need to Be Aware of Legal Liabilities

Cybersecurity professionals are at the front lines of data protection and have a direct impact on their organization's legal standing regarding cybersecurity compliance. Being aware of legal liabilities helps these professionals:

Prevent Financial and Reputational Damage:

Cybersecurity failures can lead to costly lawsuits, fines, and reputational harm to organizations and individuals.

Avoid Personal Liability:

In cases of gross negligence or deliberate misconduct, cybersecurity professionals may be held personally liable, facing civil or even criminal charges.

Ensure Compliance:

A thorough understanding of legal requirements, including industry-specific regulations (e.g., HIPAA for healthcare or FISMA for federal agencies), helps professionals implement policies and practices that protect the organization from legal scrutiny.

Support Organizational Strategy:

Awareness of liabilities helps cybersecurity professionals align their strategies with corporate governance and compliance efforts, ensuring that cybersecurity policies and practices support business objectives and regulatory obligations.

Build Stakeholder Trust:

Awareness and proactive management of cybersecurity liabilities demonstrate to stakeholders, clients, and regulatory bodies that the organization is committed to protecting data and upholding legal obligations, which can enhance trust and reduce risk.

Key Legal Liabilities for Cybersecurity Professionals

Negligence:	Duty of Care:	Data Breaches and Violations	Regulatory Non-Compliance	Third-Party Vendor Liability
When inadequate cybersecurity measures lead to damages, resulting in liability.	As custodians, cybersecurity professionals have a duty to protect sensitive data, critical information infrastructure, intellectual property etc	Statutes that impose penalties for unauthorized data access, modification, disclosure etc	Potential liabilities for failure to meet specific compliance regulations and standards like CCPA, FISMA, NIST, PCI-DSS, ISO27001 etc	Cybersecurity professionals may be liable for vendors' cybersecurity practices if they lead to data breaches
August 2013, hackers extract more than a billion Yahoo user accounts including security questions / answers not encrypted.	In re: Equifax Inc. Customer Data Security Breach Litigation (2020)	Facebook Consumer Privacy User Profile Litigation (2020): liability in data privacy after the Cambridge Analytica scandal.	United States v. Veterans Administration (Data Breach Case)	SolarWinds Supply chain attacks, CrowdStrike Update Glitch

Relevant Case Laws and Implications for Cybersecurity Compliance

FTC v. Wyndham Worldwide Corporation (2015)

Case Citation: Federal Trade Commission v. Wyndham Worldwide Corp., 799 F.3d 236 (3rd Cir. 2015)

Case Brief:

- **Facts**: Wyndham Worldwide, a major hotel chain, suffered three significant data breaches between 2008 and 2009, compromising over 600,000 consumers' data, including payment card information. The FTC filed a complaint, asserting that Wyndham's security practices were inadequate and amounted to "unfair and deceptive acts or practices" under Section 5 of the FTC Act.
- **Issues**:
  - Did Wyndham's alleged cybersecurity failures constitute "unfair" practices under the FTC Act?
  - Does the FTC have the authority to regulate corporate cybersecurity practices under its mandate to protect against unfair or deceptive practices?
- **Decision**:
  - The Third Circuit upheld the FTC's authority to bring actions against companies for inadequate cybersecurity under the FTC Act's "unfair practices" provision.
  - The court ruled that Wyndham's cybersecurity practices were "unfair" because they exposed consumers to harm, and Wyndham had failed to adopt readily available security measures that could have prevented the breaches.

Implications:

- This case affirmed the FTC's authority to enforce cybersecurity standards and hold companies accountable for inadequate data protection measures.
- It established that companies are expected to take "reasonable" steps to protect customer data, and failing to do so can lead to regulatory action under the FTC Act.

Relevant Case Laws and Implications for Cybersecurity Compliance

In re: Equifax Inc. Customer Data Security Breach Litigation (2020)

Case Citation: In re: Equifax Inc. Customer Data Security Breach Litigation, 362 F. Supp. 3d 1295 (N.D. Ga. 2020)

- **Facts**: Equifax, a major consumer credit reporting agency, suffered a data breach in 2017 that exposed the personal information of approximately 147 million people, including Social Security numbers and other sensitive data. Plaintiffs filed a class-action lawsuit alleging that Equifax failed to implement reasonable cybersecurity practices and failed to notify affected individuals promptly.
- **Issues**:
  - Did Equifax fail to protect consumer data in a way that constitutes negligence or breaches its duty of care?
  - Could Equifax be held liable for damages resulting from the breach due to alleged failures in its cybersecurity practices?
- **Decision**:
  - The court allowed the plaintiffs' claims, including negligence and breach of duty to consumers, to proceed, noting that Equifax had allegedly failed to implement adequate security measures and did not act promptly in disclosing the breach.
  - In 2019, Equifax settled for $700 million to address both consumer claims and state and federal regulatory penalties, one of the largest settlements for a data breach in U.S. history.

Implications:

- The Equifax case underscored the importance of proactive cybersecurity measures and timely breach disclosures, especially for companies handling sensitive consumer data.
- The substantial settlement highlighted the financial and reputational risks companies face when they fail to protect customer data adequately and respond transparently to breaches.
- The case serves as a warning to companies that data breaches can lead to significant liability, and it set a precedent for class-action litigation in data breach cases.

Relevant Case Laws and Implications for Cybersecurity Compliance

Case: United States v. Veterans Administration (Data Breach Incident, 2006)

Facts: In May 2006, an employee of the Department of Veterans Affairs (VA) took home a laptop containing sensitive data of approximately 26.5 million veterans and active-duty military personnel. The laptop was stolen from the employee's home, and this led to one of the largest data breaches involving a federal agency at that time. The data included names, Social Security numbers, and other personal information, creating a risk of identity theft for millions.

Issues:

- **FISMA Compliance**: Was the Veterans Administration in violation of FISMA requirements by failing to implement adequate security controls to protect sensitive data?
- **Data Protection and Employee Oversight**: Did the VA fail to ensure proper encryption, data protection policies, and employee training on security protocols as required by federal information security standards?
- **Privacy and Risk of Harm**: How should federal agencies address the privacy and data protection requirements mandated by FISMA and other federal laws to prevent harm to individuals affected by data breaches?

Decision:
The incident led to an investigation by the Office of the Inspector General (OIG) and heightened scrutiny from Congress. The VA was found to have significant deficiencies in its FISMA compliance. It lacked robust data encryption practices, employee cybersecurity training, and adequate access controls.

In response, Congress held hearings, and the VA implemented reforms to strengthen its cybersecurity posture. Additionally, there was significant investment in security infrastructure to ensure compliance with FISMA and to protect personal data better.

Relevant Case Laws and Implications for Cybersecurity Compliance

Recent FTC Administrative Actions:

Zoom (2020):
The FTC required Zoom to implement a comprehensive information security program.

Implication: Demonstrates the importance of transparency in security practices and can affect similar companies in the U.S.

Facebook FTC Settlement (2019):
$5 billion penalty for misleading users about privacy practices.

Implication: Highlights the severity of consequences for privacy misrepresentations.

Practical Examples of Liability Risks in Data Protection and Privacy

Data Breach Response:
Steps required by cybersecurity professionals to avoid liability, including timely reporting and user notifications.
Example: Uber's $148 million settlement for delayed breach disclosure.

Insider Threats:
Liability issues related to employees' unauthorized data access.
Example: A healthcare employee accessing patient records without authorization.

Third-Party Vendor Risks:
Example: Target's 2013 data breach due to a compromised vendor; Target paid millions to settle claims.

Practical Examples of Liability Risks in Data Protection and Privacy

Data Transfers and Compliance with International Standards:
Address risks related to data transfers and regulatory compliance.
Example: GDPR fines for companies that failed to implement required data transfer mechanisms (e.g., $267 million fine on WhatsApp for insufficient GDPR compliance).

Role of Cybersecurity Policies:
Importance of company policies and training programs in mitigating liability.

thank you