Counsel in the Crosshairs: Legal Decisions During a Data Crisis

UT Law CLE – Essential Cybersecurity Law

October 22, 2025

Jay Johnson
Managing Director, Deputy Chief Counsel,
Technology, Intellectual Property, Contracts Legal Group
Charles Schwab

John Ansbach
Managing Director for Cybersecurity Consulting Services and
Digital Forensic Investigation & Incident Response
Stroz Friedberg, a LevelBlue company

1

Cybersecurity Threat Landscape

Cybercrime is set to cost businesses up to $10.5 trillion by 2025 and could reach as high as **$15.63 trillion** by 2029. (Statista)

Up to 98% of cyberattacks – against businesses and otherwise – involve **social engineering** (Sprinto)

Ransomware costs victims an average of $1.85 million per incident, with attacks rising by 13% over a five-year period. (Astra)

America leads the way in terms of the most expensive cybercrime costs worldwide, but even globally, companies are paying almost **$5 million** per breach. (IBM)

Businesses are paying **$53,000 per hour**, on average, due to downtime caused by ransomware. (PentestPeople)

Only 29% of small to medium-sized businesses (SMBs) rate their current cyber defenses as mature enough to protect against breaches (VikingCloud)

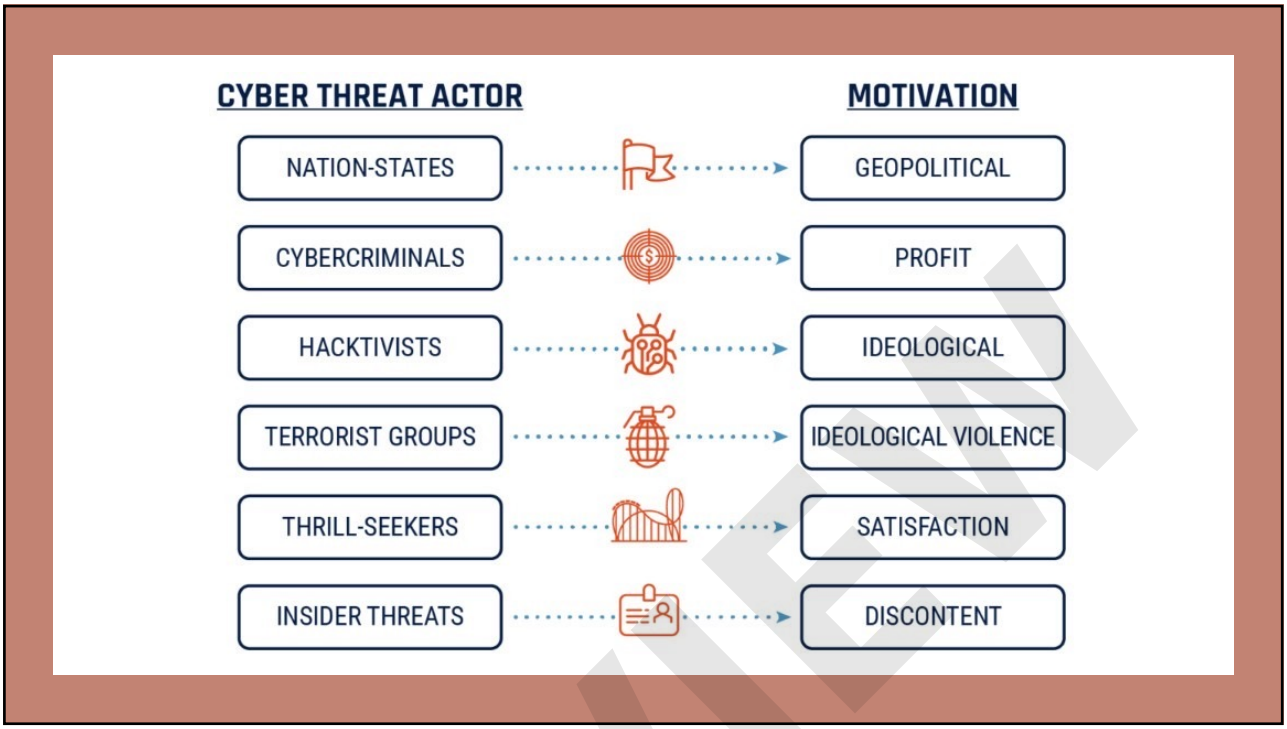
Ransomware attacks are **more than doubling** year-on-year (Forbes)

It's estimated that **80%** of phishing attacks are AI-generated, with the trend likely to continue. (Abnormal Security)

DDoS (Distributed Denial of Service) attacks are increasing by **20% year-on-year**. (Cloudflare)

U.S. data breaches impacted an estimated **353 million** individuals in one year alone. (Statista)

2



3

Common Threats

Malware	Brute Force Attacks
Lost Laptops, Backup Tapes	Denial-of-Service ("DDoS")
Fraudulent Wire Transfers	Ransomware
Advanced Persistent Threats	Phishing
Zero-Day Vulnerabilities	Spyware & Other Invasive Software
Third-Party Vulnerabilities	Insider Threats

4

Cyber Threats Specific to AI

Evasion attacks, which occur after an AI system is deployed, attempt to alter an input to change how the system responds to it. Examples would include adding markings to stop signs to make an autonomous vehicle misinterpret them as speed limit signs or creating confusing lane markings to make the vehicle veer off the road.

Poisoning attacks occur in the training phase by introducing corrupted data. An example would be slipping numerous instances of inappropriate language into conversation records, so that a chatbot interprets these instances as common enough parlance to use in its own customer interactions.

Privacy attacks, which occur during deployment, are attempts to learn sensitive information about the AI or the data it was trained on in order to misuse it. An adversary can ask a chatbot numerous legitimate questions and then use the answers to reverse engineer the model so as to find its weak spots — or guess at its sources. Adding undesired examples to those online sources could make the AI behave inappropriately, and making the AI unlearn those specific undesired examples after the fact can be difficult.

Abuse attacks involve the insertion of incorrect information into a source, such as a webpage or online document, that an AI then absorbs. Unlike the aforementioned poisoning attacks, abuse attacks attempt to give the AI incorrect pieces of information from a legitimate but compromised source to repurpose the AI system's intended use.

5

LONGHORN
WIDGET CO.

Let's Build a Company

6

Title search: Counsel in the Crosshairs: Legal Decisions During a Data Crisis

First appeared as part of the conference materials for the
2025 Essential Cybersecurity, Privacy, and AI Law session
"Counsel in the Crosshairs: Legal Decisions During a Data Crisis"