GLOBAL cyber risk LLC

THE COUNCIL

The Council of Insurance Agents & Brokers

CIAB: The Council Academy

Cyber Compliance: Here Come The Regulators And Lawsuits

Jody R. Westby, CEO, Global Cyber Risk LLC

Mark D. Rasch, Sr. Principal, Global Cyber Risk LLC

July 28, 2021

Council Academy: Exploring the Cyber Risk Environment

- 7/20/21 The Current Cyber Threat Environment & Actions to Take
- 7/21/21 Countering Cyber Attacks: What Good Incident Response Looks Like
- 7/27/21 Managing Cyber Risks Associated With The “New Normal”
- 7/28/21 Cyber Compliance: Here Come The Regulators And Lawsuits
- 7/29/21 Director & Officer Liability: The Role of Cyber Governance

Cyber Compliance: Regulators on Privacy & Cybersecurity

- 50 states with breach notification laws, varying compliance requirements
- 27 states with cybersecurity requirements for the confidentiality, availability, and integrity of data
- Comprehensive state laws: California, Virginia, Colorado, New York, more to come
- California AG released new CCPA reporting tool to allow individuals to report companies without a Do Not Sell My Personal Information button on website
- NYDFS first penalty for cybersecurity violations Reg 500 – Residential Mortgage Services, Inc. penalty $1.5 million
- July 2019 FTC fines Facebook $5B fine + new restrictions for violating consent decree
- 2021 FTC settles with ten companies for privacy and cybersecurity violations of fair trade practices
- EU GDPR Marriott Bonvoy $23.8 million to UK Information Commissioners Office – was facing $100m fine before settlement
- H&M paid $42.3 million to the ICO for illegally surveilling employees at its Nuremberg office in Germany
- EU GDPR penalties rose 40% between January 2020-2021 (DLA Piper)
- 121,165 GDPR breach notifications & $191.5 million in fines (DLA Piper); Google biggest at $56.6 million.

Trends in Legislation - 2021

- EO on Improving the Nation's Cybersecurity – May 12, 2021 following Colonial Pipeline; TSA issued 2 directives on pipeline cybersecurity.
- At least 45 states and Puerto Rico introduced or considered more than 250 bills or resolutions that deal significantly with cybersecurity. Some of the issues seeing the most legislative activity include measures:
- Requiring government agencies to implement cybersecurity training, to set up and follow formal security policies, standards and practices, and to plan for and test how to respond to a security incident.
- Regulating cybersecurity within the insurance industry or addressing cybersecurity insurance.
- Creating task forces, councils or commissions to study or advise on cybersecurity issues.
- Supporting programs or incentives for cybersecurity training and education.

Examples: CA A.B. 581 -Requires all state agencies, as generally defined, to review and implement specified NIST guidelines for, among other things, reporting, coordinating, publishing, and receiving information about a security vulnerability relating to information systems and the resolution thereof, no later than July 1, 2022.

Conn. H.B. 5868 -Requires an online listing of all cyberattacks or data breaches in the state, establishes a central location that lists all cyberattacks or data breaches in the state.

Other Cyber legislation- 2021

- CT -H.B. 6607 businesses that adopt certain cybersecurity framework allowed to plead an affirmative defense
- GA H.B. 260 - provides standards for cybersecurity programs to protect businesses from liability, provides for affirmative defenses for data breaches of private information,
- HI H.B. 454 -income tax credit for investment in qualified businesses that develop cybersecurity and artificial intelligence.
- HI H.B. 739 -manufacturers of connected devices must equip the devices with reasonable security features regarding information collected, unauthorized access, or the destruction or use of the devices.
- HI H.B. 946 - Adopts the national conference of insurance commissioners' insurance data security model law to establish insurance data security standards for state insurance licensees.
- IA D 1335 Standards for data security, and investigations and notifications of cybersecurity events for insurance companies
- IL H.B. 3030 affirmative defense for covered entity that creates, maintains, and complies with a written cybersecurity program that contains administrative, technical, and physical safeguards for the protection of either personal information or both personal information and restricted information and that reasonably conforms to an industry-recognized cybersecurity framework, prescribes requirements for the cybersecurity program.

More State Laws 2021

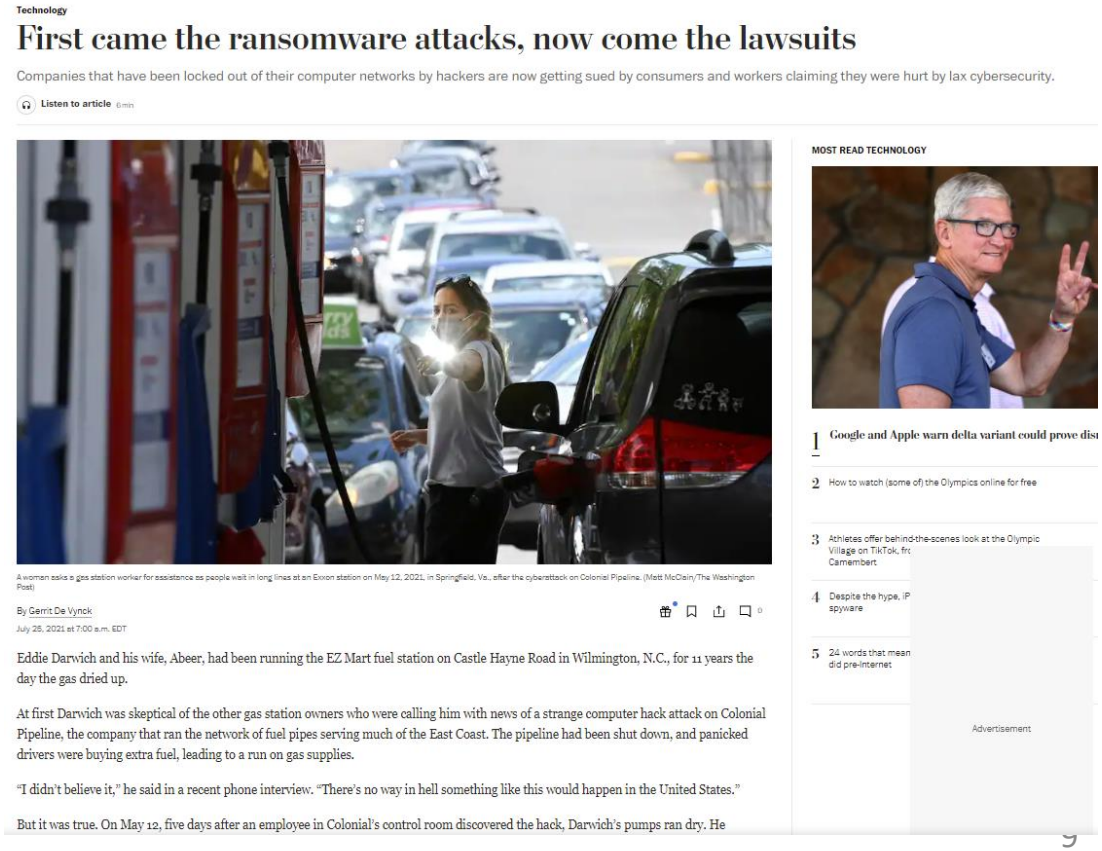
- IL H.B. 3040 - requires any insurer to conduct a risk assessment of cybersecurity threats, implement appropriate security measures, and no less than annually assess the effectiveness of the safeguards' key controls, systems, and procedures.
- IN H.B. 1169 (Enacted) requires the office of technology to maintain a repository of cybersecurity incidents, provides that a state agency and a political subdivision shall report any cybersecurity incident to the office without unreasonable delay and not later than two business days after discovery of the cybersecurity incident
- ME H.B. 17 (Enacted) establishes standards for information security programs based on ongoing risk assessment for protecting consumers' personal information, establishes requirements for the investigation of and notification to the Superintendent of Insurance regarding cybersecurity events.
- NJ A.B. 442 -Requires public institutions of higher education to establish plans concerning cyber security and prevention of cyber attacks.
- NY A.B. 4490"computer spyware protection act", prohibits the installation, transmission and use of computer software that collects personally identifiable information, damages ranging from one thousand dollars to one million dollars.

And More State Laws 2021

- ND H.B. 1314 (Enacted) Relates to cybersecurity incident reporting requirements.
- RI H.B. 5200 - Adopts the National Association of Insurance Commissioners Cybersecurity Act which establishes the current cybersecurity standard for insurers doing business in this state.
- TN H.B. 766 (Enacted) Establishes the exclusive standards for data security, licensees' investigations of cybersecurity events, and licensees' notification of cybersecurity events to the commissioner and affected consumers;
- TX H.B. 3390 (Enacted) Relates to the purchase of cybersecurity insurance coverage by the State Department of Transportation.
- UT H.B. 80 (Enacted) Creates affirmative defenses to certain causes of action arising out of a breach of system security.
- VA H.B. 1334 (Enacted) - Establishes standards for insurance data security, for the investigation of a cybersecurity event, and for the notification to the Commissioner of Insurance and affected consumers of a cybersecurity event, requires insurers to develop, implement, and maintain a comprehensive written information security program based on an assessment of its risk that contains administrative, technical, and physical safeguards.

Litigation – Class Action Post Ransomware

- Post Ransomware litigation
- SEC Derivative Suits – Failure to protect Assets
- Customers – Failure to maintain availability
- Data Subjects – Failure to protect data
- Breach of Service Level Agreement (uptime)
- Third party vendors, etc.



Technology

First came the ransomware attacks, now come the lawsuits

Companies that have been locked out of their computer networks by hackers are now getting sued by consumers and workers claiming they were hurt by lax cybersecurity.

Listen to article 6 min

A woman asks a gas station worker for assistance as people wait in long lines at an Exxon station on May 12, 2021, in Springfield, Va., after the cyberattack on Colonial Pipeline. (Matt McClain/The Washington Post)

By Gerrit De Vynck

July 25, 2021 at 7:00 a.m. EDT

Eddie Darwich and his wife, Abeer, had been running the EZ Mart fuel station on Castle Hayne Road in Wilmington, N.C., for 11 years the day the gas dried up.

At first Darwich was skeptical of the other gas station owners who were calling him with news of a strange computer hack attack on Colonial Pipeline, the company that ran the network of fuel pipes serving much of the East Coast. The pipeline had been shut down, and panicked drivers were buying extra fuel, leading to a run on gas supplies.

"I didn't believe it," he said in a recent phone interview. "There's no way in hell something like this would happen in the United States."

But it was true. On May 12, five days after an employee in Colonial's control room discovered the hack, Darwich's pumps ran dry. He

MOST READ TECHNOLOGY

1 Google and Apple warn delta variant could prove dis

2 How to watch (some of) the Olympics online for free

3 Athletes offer behind-the-scenes look at the Olympic Village on TikTok, fr Camembert

4 Despite the hype, iP spyware

5 24 words that mean did pre-Internet

Advertisement

Shareholder Derivative Suits

- Derivative suits filed after Wyndham Worldwide, Target, and Home Depot claiming breach of fiduciary duty were all dismissed. Business Judgment Rule (BJR protected the boards and officers – presumes D&Os are acting in best interests of the organization; courts will not substitute their judgment even if misinformed, misguided or actually mistaken.
- A board decision is protected by the BJR unless it is a breach of the duty of loyalty or the board acted in bad faith; must show intentional failure to act in the face of a known duty to act.
- Directors have a duty to attempt in good faith to assure that an adequate corporate information and reporting system is established and monitored
- NYDFS Cybersecurity Rule established a duty for the board chairman or officer to submit an annual signed statement certifying that the organization is in compliance with the regulation.
- Other statutory and regulatory requirements can be viewed as a requirement to act in good faith.
- Delaware law is guidepost nationally for corporate law. Four 2019 and 2020 cases collectively work to narrow, under certain circumstances, the deference given to boards, particularly with respect to meeting their duty of care and duty of loyalty.

Delaware Shareholder Derivative Cases

- *Caremark Derivative Litigation* (1996) set case law regarding board's duty to ensure that it has adequate information flows to enable it to meet its duties of care and loyalty.
- A director's obligation includes a duty to attempt in good faith to assure that a corporate information and reporting system, which the board concludes is adequate, exists and a failure to do so under some circumstances can render a director liable.
- *Marchand v. Barnhill*, 2019, listeria outbreak at Blue Bell Creameries. Court noted: Bad faith is established under *Caremark* when directors completely fail to implement any reporting or information system or controls, or having implemented such a system, fail to monitor or oversee its operations.
- In *Re Clovis Oncology Derivative Litigation,* 2019, alleged the board failed to exercise appropriate oversight of a clinical trial, resulting in false information in the market that misled investors. Company lost $1B in market value, regulatory action.
- *Clovis* court noted that, "it is appropriate to distinguish the board's oversight of the company's *management of business risk* that is inherent in its business plan from the board's *oversight of the company's compliance with positive law*– including regulatory mandates." Emphasized the board's failure to monitor oversight systems.

Delaware Shareholder Derivative Cases

- *Intermarketing Group USA v Armstrong*, 2020, pipeline company responsible for oil spill in environmentally protected area. CEO testified the responsibility for this was at lower levels of the company; board was not involved. Case allowed to proceed.
- *Hughes v. Hu*, 2020, company had persistent problems with oversight, company relied on existence of audit committee. Court noted the mere existence of an audit committee does not provide universal protection against derivative suit. Court also noted board members can be held personally liable if their neglect causes harm to the company and shareholders.
- BOTTOM LINE: Regulated industries and companies with a high-level of compliance requirements should ensure that they have implemented Board level oversight systems with appropriate information flows and reporting to enable the board to monitor compliance and key risks and respond in a timely manner.
- Experts agree that these cases may represent a warning in the area of privacy and cybersecurity compliance requirements and should be managed according to best practices and standards.
- ISO has a standard for information security governance: ISO/IEC 27014.
- NYDFS has cybersecurity requirements, so does NAIC Model Data Security Law.
- FFIEC has governance requirements.
- Plaintiiffs' bar will continue to bring these suits and even if dismissed, will appeal and settlement is likely. Reputational hit is possible from publicity.

Suits Alleging Securities Law Violations

- Securities class action lawsuits are a risk to public companies, but also can be filed against private companies.
- Increasingly filed after major cyber incidents.
- Usually claim:
  - the company made a false or misleading statement in its public filings;
  - made materially false or misleading statements in its public filings, or
  - omitted material facts about its security program.
- Often follow a steep dip in stock price or regulatory action following major incident.
- Harm can also be shown when a company fails to disclose cyber incidents or weaknesses impacts an acquisition price.
- 2018 SEC Guidance on cybersecurity enhances obligations of D&Os to manage risks, inform investors, and prevent insider trading.
- Poster children: Equifax and Yahoo!
- Equifax settled for $149 million – all funded by insurance.
- Yahoo! settled for $80 million, making it the first recovery for a breach-related suit.
- Securities lawsuits filed against Facebook, Marriott, Alphabet, and others.
- Facebook cases were filed after Cambridge Analytica and admission on earnings call re GDPR compliance that resulted in largest stock drop in history.

Summary

- Consumers are fed up
- Regulators are empowered
- The Plaintiffs' Bar is Ready, Aim…FILE!
- U.S. States and the EU are leading on privacy and cybersecurity
- The White House "Gets It" but is distracted
- Congress may or may not be ready to do something
- The FTC keeps doing its job.
- The Insurance industry sector needs to stay alert.

CIAB Resources from Leader's Edge

- Ripple Effects of Cyber Attacks, June 1, 2021, https://www.leadersedge.com/p-c/ripple-effects-of-cyber-attacks

- Ransomware Continues to Lead Cyber Attacks, Mar. 26, 2021, https://www.leadersedge.com/p-c/ransomware-continues-to-lead-cyber-attacks

- Work From Home May be Here to Stay, May 31, 2020, https://www.leadersedge.com/p-c/work-from-home-may-be-here-to-stay

- What Brokers Need to Know About Cybersecurity During COVID-19, Apr. 22, 2020, https://www.leadersedge.com/p-c/what-brokers-need-to-know-about-cybersecurity-during-covid-19

- Forgiveness After An Attack, Jan. 14, 2021, https://www.leadersedge.com/p-c/forgiveness-after-an-attack

- 2020 vs. 2021, Nov. 30, 2020, https://www.leadersedge.com/p-c/2020-vs-2021

- You Thought COVID-19 Was Bad, Sept. 24, 2020, https://www.leadersedge.com/p-c/you-thought-covid-19-was-bad

- 20 for 2020, Jan. 14, 2020, https://www.leadersedge.com/p-c/pay-now-or-pay-later

- Ransomware: It Doesn't Have to be This Hard, Nov. 21, 2019, https://www.leadersedge.com/p-c/ransomwareit-doesnt-have-to-be-this-hard

- Pay Now or Pay Later, July 11, 2019, https://www.leadersedge.com/p-c/pay-now-or-pay-later

Thank You!