Morgan Lewis

FAST BREAK:
DOJ CIVIL CYBER-FRAUD INITIATIVE AND IMPLICATIONS FOR THE HEALTHCARE INDUSTRY

Thursday, January 27, 2022
3:00–3:45 pm ET

Morgan Lewis

TODAY'S PRESENTERS & HOST

Mark Krotoski
Partner| Morgan Lewis

Katie McDermott
Partner | Morgan Lewis

Jake Harper
Associate | Morgan Lewis

Agenda

- Background on New Civil Cyber-Security Initiative Using the False Claims Act
- Scenarios and Implications for the Health Industry
- False Claims Act Legal Decisions That May Be Used to Support Liability
- DOJ's Invitation for Cyber Expert Whistleblowers and IT Function Implications
- Important Measures to Take Now to Manage Cyber Risks
- Steps On Conducting A Cyber Investigation Following An Incident
- References

Morgan Lewis

OVERVIEW OF THE CYBERSECURITY LANDSCAPE

Cyber Risks and Landscape

- Phishing Schemes
- Business Email Compromise
- Ransomware
- Targeted cyber attacks
- Insider threat
- Third Party Vendors
- Stolen unencrypted laptop

Key Actors
Organized Cyber Crime
State Sponsored
Hackers for Hire
Hacktivists
Third Party Vendor Attacks
Insider Threat
Inadvertence

2020 Cost of Data Breach Report

Key findings:

$7.13 million

The average cost of a data breach in the healthcare industry, an increase of 10% compared to the 2019 study

80%

Share of breaches that included records containing customer PII, at an average cost of $150 per record

$5.52 million

Average total cost of a breach at enterprises of more than 25,000 employees, compared to $2.64 million for organizations under 500 employees

$291,870

Increase to the average total cost of a data breach associated with complex security systems

51%

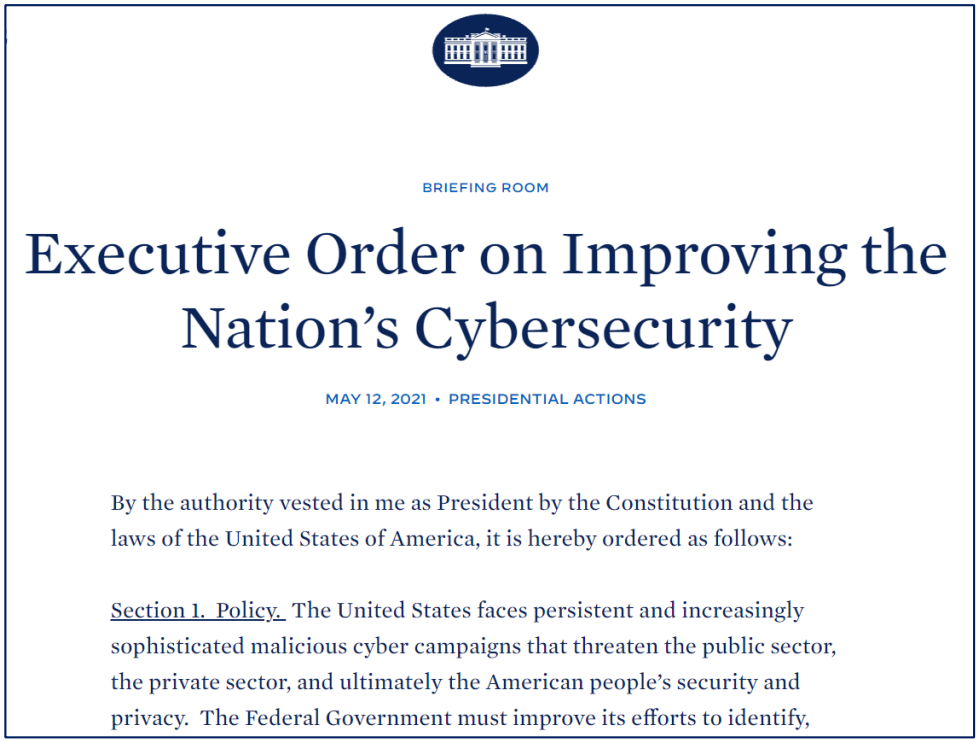
Share of organizations with cyber insurance that used claims to cover the cost of consulting and legal services

46%

Share of respondents who said the CISO is most responsible for the data breach

https://www.ibm.com/security/data-breach

Cybersecurity Focus



BRIEFING ROOM

Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify,

https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

DOJ Cybersecurity Review May 2021

PowerPost • Analysis

The Cybersecurity 202: The Justice Department launched a 120-day review into its cybersecurity strategy

By Tonya Riley

Technology and cybersecurity policy researcher

May 3, 2021 at 7:12 a.m. EDT

with Aaron Schaffer

https://www.washingtonpost.com/politics/2021/05/03/cybersecurity-202-justice-department-launched-120-day-review-into-its-cybersecurity-strategy/

Cyber Security Is Not A New Issue, But….

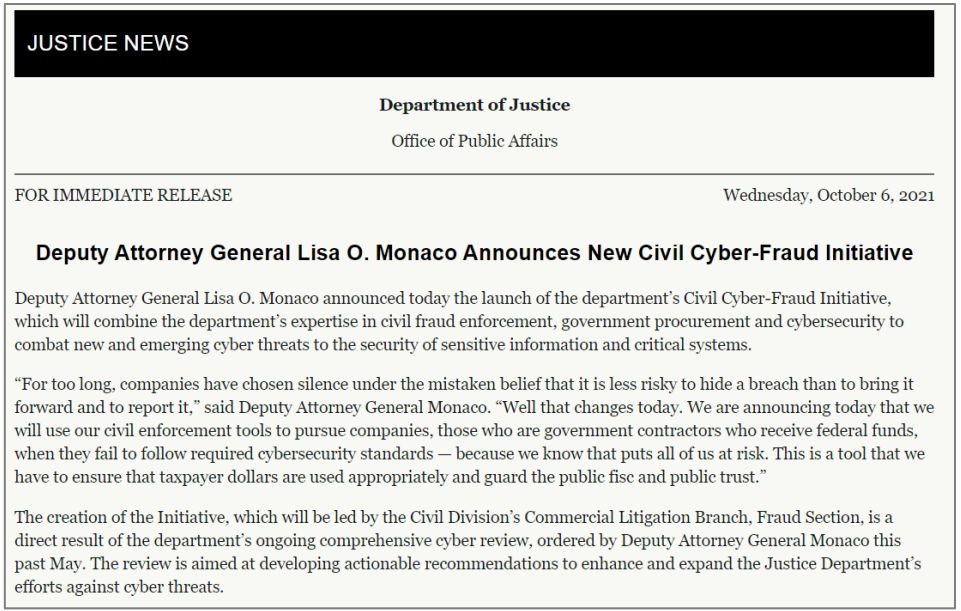
- Government contractors, especially in the defense industry, have long had special contract provisions related to cyber security and the risk of Trojan Hardware and other security risks, requiring certifications related to basic cyber security requirements. The FCA has been used in this context with mixed results where the focus has been contract performance.
- In 2021, DOJ cyber security policy has shifted risk to the government contractor or grantee with the threat of enhanced exposure under the FCA.
- The health industry has not generally accounted for cyber security risks beyond privacy related statutes in contract management, risk management or compliance standards and procedures. Yet, most stakeholders are contractors, grantees or providers.
- A cyber security incident investigation is not a civil fraud investigation under the FCA. The DOJ Cyber Fraud Initiative requires looking at cyber security from a different lens because of the much greater punitive consequences.

Morgan Lewis

NEW CIVIL CYBER-FRAUD INITIATIVE

New Civil Cyber-Fraud Initiative: October 6, 2021

- "The initiative will hold accountable entities or individuals that put U.S. information or systems at risk by **[a]** knowingly providing deficient cybersecurity products or services, **[b]** knowingly misrepresenting their cybersecurity practices or protocols, or **[c]** knowingly violating obligations to monitor and report cybersecurity incidents and breaches."



JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE — Wednesday, October 6, 2021

Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative

Deputy Attorney General Lisa O. Monaco announced today the launch of the department's Civil Cyber-Fraud Initiative, which will combine the department's expertise in civil fraud enforcement, government procurement and cybersecurity to combat new and emerging cyber threats to the security of sensitive information and critical systems.

"For too long, companies have chosen silence under the mistaken belief that it is less risky to hide a breach than to bring it forward and to report it," said Deputy Attorney General Monaco. "Well that changes today. We are announcing today that we will use our civil enforcement tools to pursue companies, those who are government contractors who receive federal funds, when they fail to follow required cybersecurity standards — because we know that puts all of us at risk. This is a tool that we have to ensure that taxpayer dollars are used appropriately and guard the public fisc and public trust."

The creation of the Initiative, which will be led by the Civil Division's Commercial Litigation Branch, Fraud Section, is a direct result of the department's ongoing comprehensive cyber review, ordered by Deputy Attorney General Monaco this past May. The review is aimed at developing actionable recommendations to enhance and expand the Justice Department's efforts against cyber threats.

https://www.justice.gov/opa/speech/acting-assistant-attorney-general-brian-m-boynton-delivers-remarks-cybersecurity-and

Expected Focus of FCA Cyber – Enforcement Efforts

- Non-compliance with cybersecurity standards on goods and services provided by federal contractors
  - Failure to adhere to specific contractual requirements
  - Failure to protect government data and unauthorized access
- Misrepresentation of security controls and practices.
  - False representations regarding System Security Plans and security controls
  - Misrepresentations in the bidding process – fraudulent inducement
  - Misrepresentations re periodic reporting
  - Failure to disclose violations
- Failure to timely and accurately report suspected breaches of cybersecurity protocols

Implications for Health Industry

- FCA cyber exposure is now a parallel exposure to federal HIPAA and HiTech and state law breach exposures. But, the scope of exposure is much broader with graver consequences.
- Directly impacts all healthcare contractors whether governed by FAR or not. Health plans, suppliers to the VA/FSS, life science product contracts. No reason to think that DOJ and whistleblowers will not push to all healthcare providers.
- Impacts grantees-Academic Medical Centers- that get research funds or other health program funding from the federal government.
- Directly impacts life science companies providing product to healthcare providers reimbursed by federal funds.
- Health industry compliance is predominantly focused on managing fraud and abuse issues. Need to update to incorporate cyber security civil fraud exposure in risk management.

Special Invitation to Internal Or Vendor Cyber Experts to Whistleblower

- DOJ's Deputy Attorney General Monaco expressed a specific objective to use cyber experts in a whistleblower capacity to work with DOJ, citing the unique technical complexity of cyber and the unique position of in-house or vendor IT personnel to know of potential cyber security exposures and non-compliance.
- Unusual invitation for whistleblower collaboration that is designed to accelerate the civil cyber fraud initiative with immediate investigations and quick results.
- The FCA private citizen whistleblower provisions allow for significant recoveries, attorney's fees and retaliation damages for employees and contractors.
- For the health industry, need to assess IT personnel and vendor issues for FCA whistleblowing and incorporate into compliance disclosure procedures cyber security issues.

FCA Cases and Enforcement

- **U.S. ex rel. Adams v. Dell Computer, No. 15-cv-608 (D.D.C. 2020)** declined qui tam case alleging sale of computer products with undisclosed cybersecurity hardware vulnerabilities. Dismissed on materiality grounds.
- **U.S. ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc.,** 381 F. Supp. **3d 1240 (E.D. Cal. 2019)** declined qui tam alleging noncompliance with contractual cybersecurity requirements. Relator was insider - former Senior Director of Cyber Compliance/Controls. Alleged fraudulent inducement and non-compliance with standards. Court allowed some FCA claims to survive motion to dismiss.
- **Duke University.** $112.5 million FCA settlement for false research grant **certifications** on research results and progress reports. https://www.justice.gov/opa/pr/duke-university-agrees-pay-us-1125-million-settle-false-claims-act-allegations-related. Are specific certifications needed or is cyber security inherently material to payment or receipt of government funds?

Breach Notices May Be Expanded Under FCA

- In addition to federal and state regulatory notices, FAR and Government Contract provisions may or will govern cyber breach notice obligations for healthcare contractors, grantees and vendors.
- A failure to make timely and complete disclosures on cyber incidents, similar to regulatory non-compliance disclosures, may trigger FCA exposure.
- Other public agency notices should be assessed (Device manufacturers FDA digital health issues).
- Critical to incorporate cyber notification procedures into traditional compliance disclosure policies and procedures.

Morgan Lewis

HOW TO MANAGE CYBER FCA RISKS?

The Best Offense is a Good Defense-Assess and Update!

- Update Compliance Program disclosure procedures to expressly encourage internal cyber reporting of concerns by employees and contractors.
- Establish a Cyber Security Compliance Committee to benchmark all contract and regulatory requirements to benchmark and monitor.
- Assess and update relevant contracts to account for FCA exposure for cyber breaches including assessment and correction action plan rights.
- If FAR or DFA applies to operations, update contracts for specific new cyber security provisions.
- Assess whistleblower management issues
- Include in compliance program work plan an independent review of cyber security exposure.
- Assess insurance policy for cyber FCA coverage.
- Update notification procedures to included assessment of disclosure to DOJ civil fraud section or local USA civil division.

Other Pro-Active Actions to Manage Risk

- Assess and update cyber security response plan. If one does not exist, make it an urgent priority.
- Assess and update training to include drills, exercises and contingencies for all functions in the event a cyber event decommissions operations. Ransomware.
- Include an independent cyber expert in proactive assessments and in incidents. Internal IT is a mystery and management cannot assure its navigation is objectively reliable if it relies only on the IT team.
- Develop experts to aid in internal investigations and incidents. Cyber matters require immediate and urgent action. Need your legal, technical, insurance, media experts in the bull pen as part of incident response plan.

Morgan Lewis

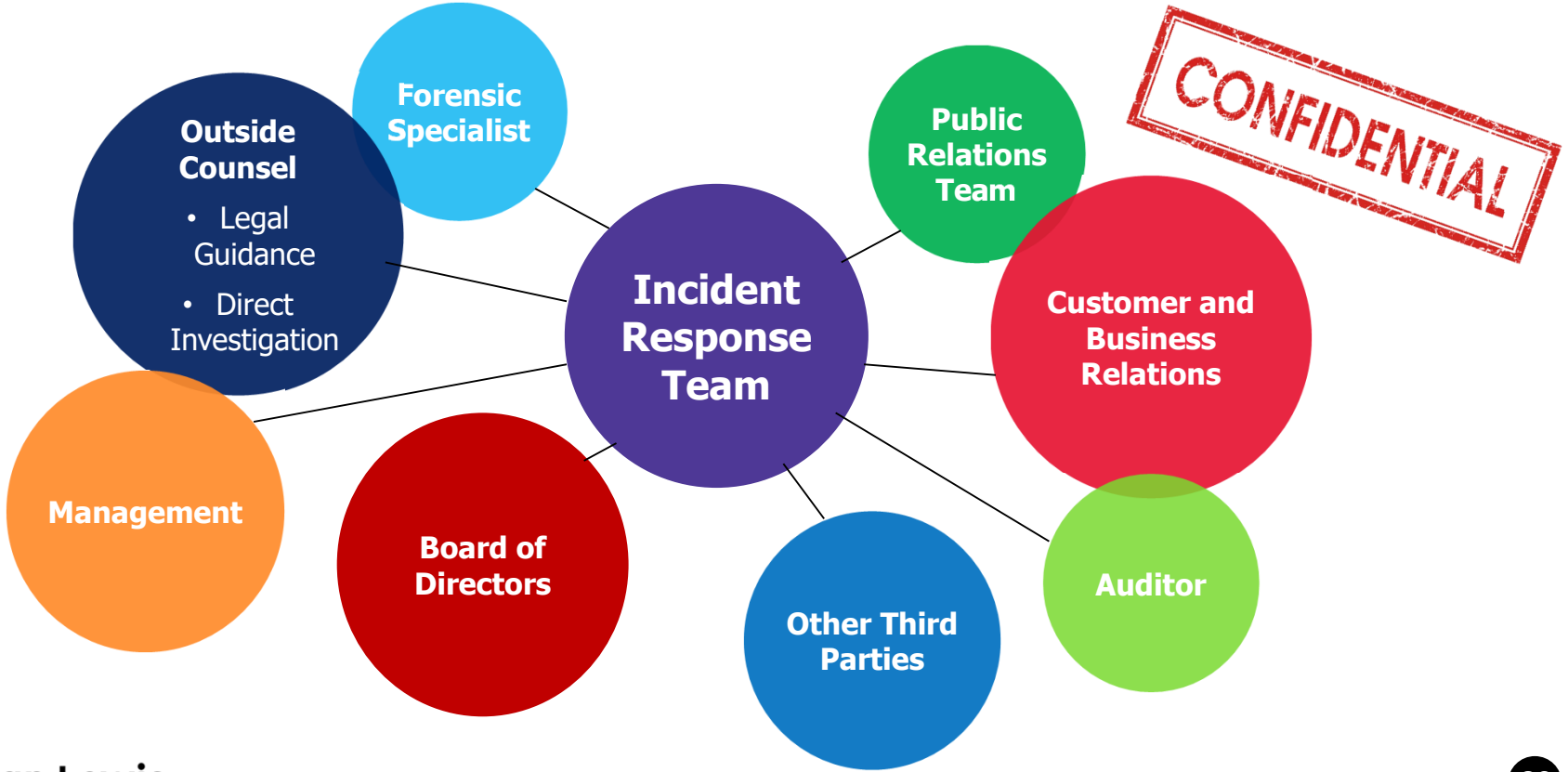
STEPS ON CONDUCTING A CYBER INCIDENT INVESTIGATION

Legal Issues During Incident Response Phases

Range of Legal and Forensic Issues

- Was data "exfiltrated" or "accessed" or "acquired"?
- What data?
  - PII, PHI, Contractual Information?
- Did a data "breach" occur?
- What notification requirements may be triggered?
- How to mitigate loss or damages?
- Conducting a risk assessment
- Compliance issues
- Obligations during third party vendor attack
- Anticipated regulatory inquiry issues
- Anticipated litigation issues

Consider Range of Incident Communications



Common Vulnerability and Remediation Areas

- Governance
- Internal Controls, Policies, Procedures and Standards
- Risk Assessment and Management Program
- Access Management
- Training
- Third Party Vendors
- Disclosure Issues

Join us next month!

Please join us for next month's webinar:

***Fast Break:* Risk Adjustment and Liability**

Featuring

Tesch Leigh West and Michelle Arra

- Thursday February 24, 2022 at 3:00 pm ET

Morgan Lewis

QUESTIONS?

References

- Press Release, Department of Justice, Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative (Oct. 3, 2021), https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative.

- Remarks of Acting Assistant Attorney General Brian M. Boynton at the Cybersecurity and Infrastructure Security Agency (CISA) Fourth Annual National Cybersecurity Summit (Oct. 13, 2021), https://www.justice.gov/opa/speech/acting-assistant-attorney-general-brian-m-boynton-delivers-remarks-cybersecurity-and.

- The White House, FACT SHEET: Biden Administration and Private Sector Leaders Announce Ambitious Initiatives to Bolster the Nation's Cybersecurity (Aug. 25, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/25/fact-sheet-biden-administration-and-private-sector-leaders-announce-ambitious-initiatives-to-bolster-the-nations-cybersecurity/.

Thanks And Be Well!

Katie McDermott
Partner | Morgan Lewis
Washington, DC
+1.202.739.5458
kathleen.mcdermott@morganlewis.com
Click here for full bio

A former Assistant US Attorney and US Department of Justice (DOJ) Healthcare Fraud Coordinator, Katie McDermott represents healthcare and life sciences clients throughout the United States in federal and state government investigations and litigation matters relating to criminal, civil, and administrative allegations, including violations of the False Claims Act and its whistleblower provisions.

Katie also advises Boards of Directors and senior corporate management on corporate compliance and regulatory matters relating to internal investigations, voluntary government disclosures, consent decrees, and government mandated compliance measures.

Active as a legal educator, Katie has serves as an adjunct professor of law at the University of Maryland Carey School of Law, teaching an advanced seminar on healthcare industry fraud and abuse issues.

Thanks and Be Well!

Mark L. Krotoski
Partner | Morgan Lewis
Silicon Valley, CA
+1.650.843.7212
mark.krotoski@morganlewis.com
Click here for full bio

Litigation Partner, Privacy and Cybersecurity and Antitrust practices

- Co-Head of Privacy and Cybersecurity Practice
- Litigates, responds to a data breach, directs confidential cybersecurity investigations, responds to federal and state regulatory investigations, coordinates with law enforcement on cybercrime issues, mitigates and addresses cyber risks, and develops cybersecurity protection plans.
- 25 years' experience handling a broad range of complex and novel cyber cases and investigations under the Computer Fraud and Abuse Act, Economic Espionage Act, Defend Trade Secrets Act, and other statutes.
- Served as the national coordinator for the Computer Hacking and Intellectual Property (CHIP) Program in the DOJ's Criminal Division, and as a cybercrime prosecutor in Silicon Valley, in addition to other DOJ leadership positions.

Thanks and Be Well!

Jake Harper
Associate | Morgan Lewis
Washington, DC
+1.202.739.5260
jacob.harper@morganlewis.com
Click here for full bio

Jake advises stakeholders across the healthcare industry, including hospitals, health systems, large physician group practices, practice management companies, hospices, chain pharmacies, manufacturers, and private equity clients, on an array of healthcare regulatory, transactional, and litigation matters. His practice focuses on compliance, fraud and abuse, and reimbursement matters, self-disclosures to and negotiations with OIG and CMS, internal investigations, provider mergers and acquisitions, and appeals before the PRRB, OMHA, and the Medicare Appeals Council.