Effective Compliance: Mitigating Risks of Criminal Conduct & Cyber Attacks

Presented by:
Holly Drumheller Butler & Veronica D. Jackson
ACC Baltimore | September 15, 2022

MILES & STOCKBRIDGE

Holly Drumheller Butler

Principal

Co-leader, White Collar, Fraud and Government Investigations Practice

hbutler@milesstockbridge.com

410-385-3829

Veronica D. Jackson

Principal

Employment, Cybersecurity and Privacy Practices

vjackson@milesstockbridge.com

410-385-3499

MILES & STOCKBRIDGE

Failure to detect and prevent criminal conduct comes with a risk.

- Forfeitures
- Disgorgements
- Injunctive Relief
- Penalties
- Criminal Charges against entity and executives
- Reputation Cost

Effective compliance and ethics program requires:

- Due diligence to prevent and detect criminal conduct; and
- An organizational culture that encourages ethical conduct and a commitment to compliance with the law.

Practical translation?

MILES & STOCKBRIDGE

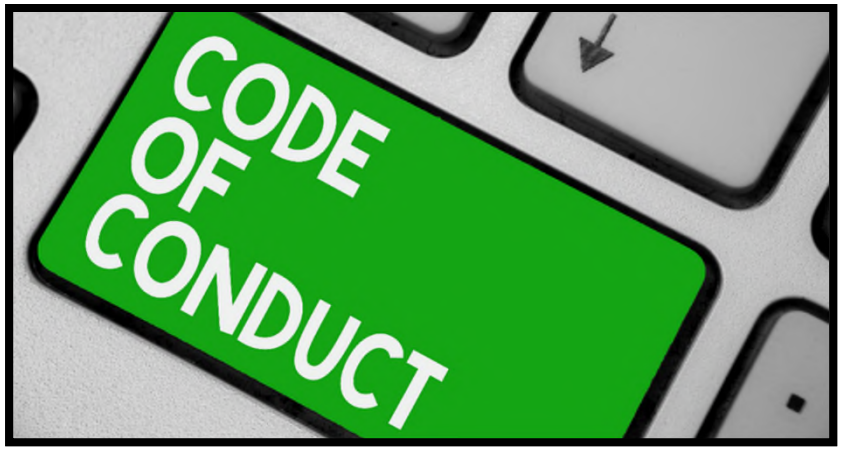
Minimum Requirements

- Code of Conduct
- Written Policies
- Oversight/Monitoring

Code of Conduct

Statement of company's values and belief

- Corporate Identity
- Plain English
- Accessible
- Top Down Messaging



Written Policies

Address singular issue for the Company

- Define Scope
- Available and Known
- Incentives/Disciplinary Measures

Oversight/Monitoring

- Executive Responsibility & Budget
- Complaint Hotline
- Third-Parties
- Living Document

One size does <u>not</u> fit all.

MILES & STOCKBRIDGE

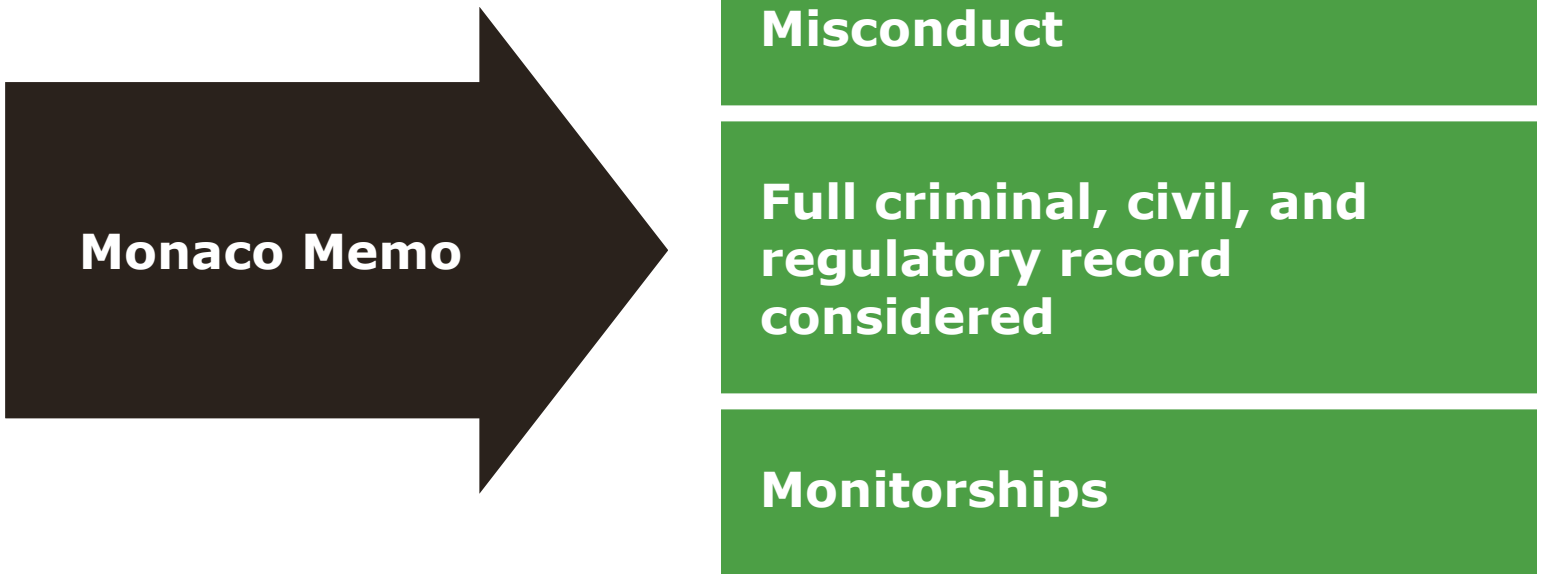
Respond Appropriately

Cycle of Compliance

A Cautionary Tale

MILES & STOCKBRIDGE

Individual Liability



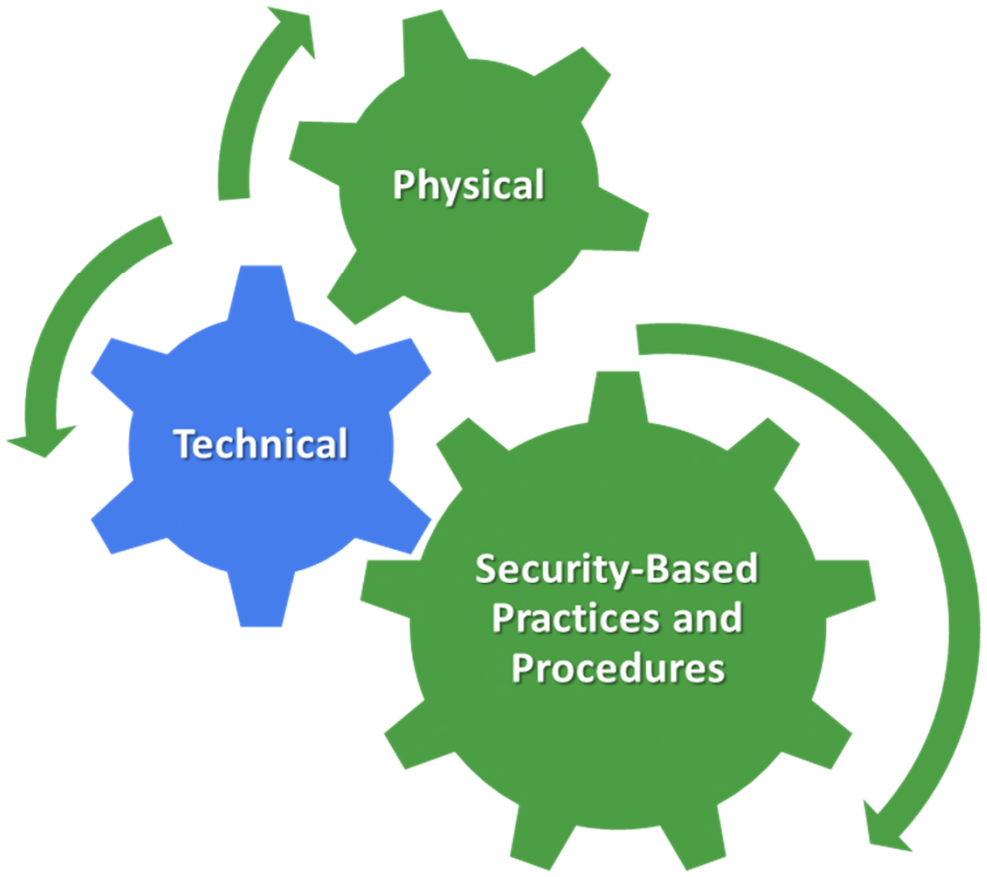
Individual Liability

MILES & STOCKBRIDGE

Personal Liability vs. Corporate Accountability

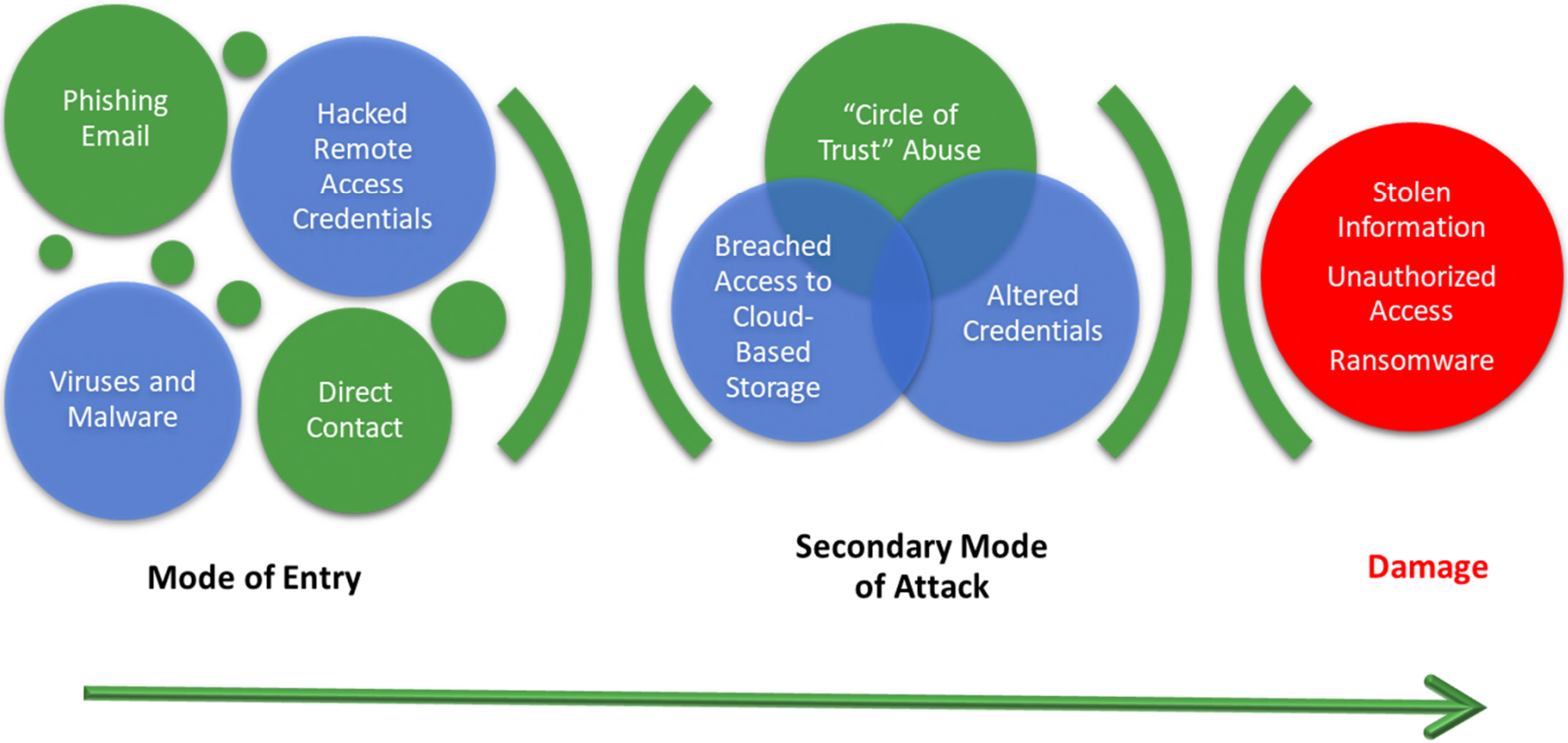
Data Security Tools

MILES & STOCKBRIDGE



Lifecycle of a Hack

MILES & STOCKBRIDGE



Pre-Breach Compliance

MILES & STOCKBRIDGE

- Identify most critical cyber assets and risks.
- Data Mapping
- ***Thirty party contract requirements, due diligence, auditing***
- Implement a Written Information Security Program (WISP)
- Establish an Incident Response Team and test an Incident Response Plan
- Implement training and auditing protocols
- Evaluate need for cyber insurance
- Identify relevant law enforcement authorities for incident reporting

Pre-Incident Data Security Compliance

MILES & STOCKBRIDGE

Written Information Security Program (WISP)

- A living program – not just policies – that defines security practices & exposures
- Best defense to litigation & regulatory actions
- Required by many state laws, DOD, SEC, GLB, FED, FDIC, OCC, FISMA, HIPAA, GDPR, CCPA, PCI – DSS, *etc.*
- Defines current regulatory & liability environment
- Identifies IRT members, including IT, Security, Legal, Compliance, Communications
- ***Training is essential!***

Employees as First Line of Defense

Tips to promote compliance and early reporting of issues:

- Clear and accessible policies
- Training
- Limited access
- "See something, say something."
- Reporting incentives?
- Violation consequences?

DOJ's Civil Cyber-Fraud Initiative

MILES & STOCKBRIDGE

- Announced October 2021
- False Claims Act as new tool for cybersecurity enforcement.
- No breach required.

Whistleblower Actions

Aerojet Rocketdyne Settlement (July 2022)

- $9 Million
- Misrepresented its compliance with cybersecurity requirements
- Relator Markus received $2.6M

Questions?

MILES & STOCKBRIDGE

Miles & Stockbridge

Miles & Stockbridge is a leading law firm with offices in the mid-Atlantic region, including offices in Baltimore, Washington, D.C. and Richmond. Our lawyers help global, national, local and emerging business clients preserve and create value by helping them solve their most challenging problems.


Miles & Stockbridge


Miles & Stockbridge


@mstockbridgelaw