
Morgan Lewis
YOUR COMPANY HAS BEEN HACKED. WHAT NEXT?
Mark L. Krotoski
Susan D. Resley
Kurt B. Oldenburg
May 2, 2019
© 2019 Morgan, Lewis & Bockius LLP

Preliminary Note

- Comments during this presentation are based upon:
  - Publicly available information;
  - General observations and experience; and
  - Not on any specific client case information.

Are You Prepared for Regulatory and Litigation Risks?

1. Hypothetical scenario
2. Key cyber risks
3. Determining and containing the scope of the breach
4. Enforcement risks and responding to SEC, DOJ, other Regulators
5. Notification and disclosure obligations
6. Establishment of effective internal controls
7. Insider trading prevention
8. Recommended best practices

HYPOTHETICAL SCENARIO

You've Been Hacked: What Next?

1. Hackers infiltrate a corporate network without detection
2. IT flags suspicious activity and discovers hack, but it's too late. What now?
3. IT later learns that an employee/corporate insider participated in the hack. Any corporate liability?
4. When and how to disclose?
5. Improving controls.
6. Other considerations.

KEY CYBER RISKS

Key Cyber Risks

Significant consequences of unauthorized cyber intrusion, e.g.:

- **Ransomware** (unauthorized encryption of corporate data);
- **Theft** (intellectual property (IP) and trade secrets, bank transfers, other assets);
- **Privacy** (personally identifiable information (PII) entrusted by consumers /employees);
- **Business email compromise** (impersonation of executives/other gatekeepers);
- **Insider trading** (nonpublic information stolen and used to time stock trades);
- **Infrastructure** (attacks on critical infrastructure carry heightened stakes); and
- **Public relations** (lasting reputational harm/brand damage for security lapses).

Key Cyber Risks

There is no one-size-fits-all solution. Some threats include:

- **Phishing attacks** (manipulation of human targets via email, instant messaging, etc.);
- **Unpatched software and devices** (software and firmware must be constantly updated to patch vulnerabilities);
- **Botnets** (coordinated surge of activity at corporate networks or devices);
- **Application threats** (vulnerabilities in web-based applications enable unauthorized access);
- **Inside threats** (corporate insiders may grant access to external confederates);
- **Inadvertence** (lost devices, publication of sensitive information, etc.);
- **Advanced persistent threats** (prolonged and sophisticated efforts by professionals); and
- **State-sponsored attacks** (infrastructure disruption, IP theft, etc.).

Considerations for Victims of Cyber Breach

The victim of a cyber breach incident must navigate several challenging legal, factual, and strategic determinations:

- **Whether the incident has or can be promptly contained**;
- **Preservation of evidence**;
- **Whether to contact law enforcement**;
- **Budgeting the costs and expenses of remediation**;
- **Planning for litigation, including potential class actions**;
- **Whether, when, and how to make a public disclosure**; and
- **How to cooperate with state and federal regulatory agencies.**

DETERMINING AND CONTAINING THE SCOPE OF THE BREACH

Preparing an Incident Response Plan

Cybersecurity plans and procedures are essential *before* any incident occurs:

- Educate senior management
- Identify "crown jewels"
- Deterrence and detection infrastructure
- Identify contact points with federal/local law enforcement and Information Sharing and Analysis Centers (ISACs)
- Workplace/personnel policies
- Regularly update/patch software and infrastructure

**See* US Dept. of Justice Cybersecurity Unit, Best Practices for Victim Response and Reporting of Cyber Incidents (Version 2.0) (Sept. 2018)

Determining and Containing the Scope of the Breach

If a potential breach is detected, the incident response plan might include:

- **Internal notifications**
- **Stop continuing damage**
  - Halt use of compromised systems
  - Re-routing / blocking external network access
- **Preserve and collect information**
  - Logs relating to intrusion activity
  - Image the affected systems
  - Check backups
  - Forensic report (potentially discoverable)

**See* US Dept. of Justice Cybersecurity Unit, Best Practices for Victim Response and Reporting of Cyber Incidents (Version 2.0) (Sept. 2018)

ENFORCEMENT RISKS AND RESPONDING TO SEC, DOJ, OTHER REGULATORS

Enforcement Risks and Considerations

- Federal Law Enforcement (FBI/DOJ)
- Securities and Exchange Commission
- Federal Trade Commission
- Other Federal/State Agencies (HHS, FCC, FINRA, etc.)
- State Attorneys General
- Civil Class Actions

Principal Enforcement Risks and Considerations

- **DOJ Cybersecurity Unit**
  FBI Cyber Action Team
  - Specialized training in 94 US Attorney's Offices/56 FBI field offices
  - Criminal investigation/prosecution of hackers
- **SEC Cyber Unit**
  - Established Sept. 2017 to "target cyber-related misconduct"
  - Civil enforcement of insider trading, market manipulation, public company disclosure and controls, safeguarding financial consumer information

Principal Enforcement Risks and Considerations

- **Federal Trade Commission**
  - Civil enforcement: significant penalties for lax security of consumer data or failure to notify consumers re: compromised personal information
- **State Attorneys General**
  - State law enforcement: data security and notification rules vary by state
- **Civil Plaintiffs**
  - Privacy and consumer class actions
  - Securities class actions
  - Derivative actions

ADDRESSING NOTIFICATION AND DISCLOSURE OBLIGATIONS

Notification and Disclosure Obligations

If a breach occurs, who should be notified?

- **Law Enforcement?**
  - FBI/Local Authorities (potential criminal activity)
- **Investors?**
  - SEC Filings (disclosure of *material* cybersecurity risks and incidents)
- **Potentially Affected Parties?**
  - Individuals (personal identifying information of consumers, employees)
  - Organizations (e.g., vendors, contractors, financial institutions)
  - Civil Regulators (responsible for oversight of individual notifications)

Notification Considerations: Law Enforcement

- **Criminal Law Enforcement & National Security**
  - FBI Cyber Action Team (56 field offices)
  - Local Police
  - DHS National Cybersecurity and Communications Integration Center
- **Civil Regulators**
  - SEC (e.g., potential insider trading)
  - Federal Trade Commission
  - State AGs and Regulators (varies by state)
  - Industry- and breach-specific (e.g., FDIC, IRS, GSA)

Notification Considerations: Affected Third Parties

- **Federal Law**
  - Federal Trade Commission (regulation of consumer notifications)
  - Other industry-specific regulations (e.g., HHS, FCC)
- **State Law**
  - All 50 states have enacted notification laws
  - Various definitions of (e.g.) "personal information"; what constitutes a breach; timing and content of notice; and exemptions
- **Foreign Law**
  - General Data Protection Regulation (EU)

Disclosure to Investors

Feb. 21, 2018 SEC Staff Interpretive Guidance

- Material risks and incidents must be disclosed
- Timely and complete disclosures
- The obligation to disclose cybersecurity risks and incidents arises from "a number of" requirements under existing reporting rules
- Emphasizes importance of cybersecurity to SEC (but offers limited *new* guidance)
  - SEC has acknowledged: "meaningful disclosure has remained elusive," "provides only modest changes to the 2011 staff guidance," and "essentially reiterates years-old staff-level views on this issue"

Disclosure to Investors: Materiality

What is a material event?

- "Tailored" to the company's "particular cybersecurity risks and incidents"
- The "nature, extent, and potential magnitude" relative to the size of operations
- The "range of harm" that such incidents have caused or could cause
  - Reputation
  - Financial performance
  - Customer and vendor relationships
  - Possibility of litigation or regulatory investigations or actions
- Companies *need not* give a "roadmap" of internal systems to future intruders

Disclosure to Investors: Timing

When should disclosure occur?

- Periodic (Form 10-Q or 10-K) or immediate (Form 8-K) disclosure?
  - Cybersecurity risk versus incident
- Companies "may require time to discern the implications of a cybersecurity incident" before making a disclosure
  - But: an ongoing internal or external investigation cannot "provide a basis for avoiding disclosures of a material cybersecurity incident"
- Duty to Update: after an incident "companies should consider whether they need to revisit or refresh previous disclosure"

Disclosure to Investors: Timing

***In the Matter of Altaba Inc., f/d/b/a Yahoo! Inc.* (Apr. 2018)**

- December 2014: Yahoo! officials allegedly discover theft of "crown jewels" (PII and encrypted passwords for 500+ million user accounts)
- September 2016: Yahoo! discloses breach in connection with potential acquisition by Verizon
- April 2018: Altaba (f/k/a Yahoo!) agrees to $35M SEC fine for failure to disclose cyberattack to investors (e.g., 10-K and 10-Q risk factors; MD&A re impact on liquidity and net revenues)
  - $80M settlement of securities class action; $29M settlement of derivative class action; $50M settlement* of consumer class action (*rejected by court)

Disclosure to Investors: Timing

SEC EDGAR Cyberintrustion

- 2016: SEC detects EDGAR intrusion
- August 2017: SEC discovers possibility of illicit trading
- September 2017: Public disclosure of breach
- January 2019: Insider trading charges filed

Disclosure to Investors: SEC Guidance

Where should disclosure occur?

- The description of general risk factors to investors;
- Management's discussion and analysis (MD&A) of potential financial or operational trends;
- The description of the registrant's business and market conditions;
- Potential legal proceedings;
- Financial statement disclosures before, during, and after a cyber incident; and
- Disclosure of controls and procedures jeopardized or impaired by cyber incidents.

ESTABLISHMENT OF EFFECTIVE INTERNAL CONTROLS

Establishment of Effective Internal Controls

Per the 2018 Guidance, SEC expects companies to:

- "maintain comprehensive policies and procedures related to cybersecurity risks and incidents" that include:
- "appropriate and effective disclosure controls and procedures that enable them to make accurate and timely disclosures of material events, including those related to cybersecurity."

Effective controls must ensure that incidents and risks are:

- timely "recorded, processed, summarized, and reported," and
- "accumulated and communicated to the company's management . . . as appropriate to allow timely decisions regarding required disclosures."

Establishment of Effective Internal Controls

Companies should evaluate whether their controls:

- "appropriately record, process, summarize, and report the information";
- "identify cybersecurity risks and incidents";
- "assess and analyze [the risks'] impact on a company's business";
- "evaluate the significance associated with such risks and incidents";
- "provide for open communications between technical experts and disclosure advisors"; and
- "[cause] timely disclosures regarding such risks and incidents."

Effectiveness of controls must be certified by the CEO and CFO (and information therefore must be processed up the corporate ladder)

Establishment of Effective Internal Controls

In the Matter of Voya Financial Advisors, Inc. (Sept. 2018)

- First SEC enforcement action under SEC's Safeguards Rule and Identify Theft Red Flags Rule (Fair Credit Reporting Act regulations)
- Cyber thieves allegedly impersonated Voya contractors to obtain password resets via Voya support line and stole personal information of 5,600 customers
- Voya allegedly did not update its Identify Theft Prevention Program after 2009
  - Voya did undertake prompt remedial acts, including (a) blocking the malicious IP addresses; (b) prohibiting provision of a temporary password by phone; and (c) issuing breach notices to the affected customers
- Voya nonetheless agreed to pay $1M and retain independent consultant for evaluation of cybersecurity policies and procedures

Establishment of Effective Internal Controls

SEC Declination: Nine Public Companies (Oct. 2018)

- SEC found that nine publicly listed companies (not identified) were defrauded of nearly $100M combined via spoofing/phishing email attacks
  - Hackers "spoofed" email accounts of executives and tricked finance personnel into transferring money to foreign bank accounts
  - Hackers broke into email accounts of actual vendors to demand payment for invoices
- SEC stressed that federal securities laws require companies to have procedures designed to prevent employees from making unauthorized transactions
- The victimized industries included technology, machinery, real estate, energy, financial and consumer goods; two companies lost more than $30 million each

Disclosures to Investors: Cybersecurity risk factors

With regard to forward-looking risks, factors include:

- the occurrence of prior cybersecurity incidents;
- the probability and potential magnitude of cybersecurity incidents;
- the adequacy of preventative actions;
- the aspects of the company's business and operations that give rise to material risks;
- the costs associated with maintaining cybersecurity protections;
- the potential for reputational harm;
- existing or pending laws and regulations; and
- litigation, regulatory investigation, and remediation costs.

Disclosures to Investors: Management Discussion & Analysis

Cybersecurity disclosures may be required in MD&A discussion of financial condition and results of operations, specifically including:

- "the cost of ongoing cybersecurity efforts (including enhancements to existing efforts), the costs and other consequences of cybersecurity incidents, and the risks of potential cybersecurity incidents, among other matters."

Other relevant costs might include:

- "loss of intellectual property,
- the immediate costs of the incident, as well as the costs associated with implementing preventative measures,
- maintaining insurance, responding to litigation and regulatory investigations, preparing for and complying with proposed or current legislation, engaging in remediation efforts, addressing harm to reputation, and the loss of competitive advantage that may result."

Disclosures to Investors: The Board of Directors

The 2018 SEC Guidance specifically notes that disclosure about how the board of directors oversees management's actions relating to cybersecurity risks is important to investors' assessment of risk oversight.

The SEC recommends that this discussion include:

- the nature of the board's role,
- how the board engages with management on cybersecurity issues, and
- as much transparency as practicable into the board's oversight of corporate cybersecurity assessments, policies, and procedures.

INSIDER TRADING PREVENTION

Insider Trading on Hacked Information

Elaborate International Hacking and Trading Scheme

- 2015: SEC charged 32 defendants in an international scheme to steal and trade on news wire information relating to corporate earnings releases.
- Hackers infiltrated news wire services to obtain corporate announcement information in advance of release
- Hacking ring provided information to traders who reaped over $100 million over a **five-year period**
- Several traders and hackers were charged criminally

Insider Trading After Learning of Hack

Equifax Inc. Insider Trading Cases (March 2018)

- August 2017: Equifax detects data breach; former CIO exercises stock options
- September 2017: Equifax publicly discloses data breach
- March 2018: Criminal (DOJ) indictment and Civil (SEC) complaint charging former CIO with insider trading violations
- June 2018: SEC charges second Equifax employee for insider trading

Insider Trading Prevention

SEC Requirement for Registered Entities:

- Required to establish, maintain, and enforce written policies reasonably designed to prevent securities law violations (including insider trading)
  - SEC has charged a number of broker-dealers, investment advisers, and hedge funds for violating these rules

SEC's 2018 Guidance for All Companies:

- They should "take steps to prevent directors and officers (and other corporate insiders. . .) from trading its securities until investors have been appropriately informed about the incident or risk"
- Companies should have "well designed policies and procedures to prevent trading on the basis of all types of material nonpublic information, including information relating to cybersecurity risks and incidents"

RECOMMENDED BEST PRACTICES

Best Practices

- **Governance**
  - Board cyber risk management
  - Cybersecurity risk oversight and personnel
  - Cyber-risk management practices
  - Preparedness for cyber incident or attack
- **Internal Controls and Policies**
  - "[M]aintain[] comprehensive policies and procedures related to cybersecurity risks and incidents"
    - Tailored to your cyber security needs
    - Identify, Protect, Detect, Respond and Recover
  - Review controls to prevent and detect cybercrime (Section 21(a) Report)
  - Emerging Reasonable Cybersecurity Standard
- **Insider Trading**
  - Insider Trading Policies and Procedures Related to Cyber Risks and Incidents
  - "[P]olicies and procedures to prevent trading on the basis of all types of material nonpublic information, including information relating to cybersecurity risks and incidents."
- **Legal Review**
  - Insider Trading Programs
  - Internal Control Programs

Best Practices

- **Training**
  - Prepared for cyber risks
  - Prevention
  - Responding to cyber risks
    - Phishing and Business Email Compromise
- **Managing Cyber Incident**
  - Multiple regulators
  - Incident Response Plans and Testing
  - Attorney-Client Privilege Cyber Investigations
- **Address Disclosure Issues**
  - Timing
  - Periodic Reports
    - Form 10-K
    - Management's Discussion and Analysis (MD&A) section
  - Materiality Standard
  - Cybersecurity Risk Factors

Prepared for All Cyber Incident Phases

- Assist before, during, and after a data breach.
- Data breach-prevention guidance:
  - Implementing policies and training regarding data breaches, including governance and risk assessments, data loss prevention, and vender management.
- Guidance on managing data breach
  - Conducting confidential, privileged cyber incident investigations.
- Assist on enforcement investigations and actions by federal and state regulators
- Assist on class litigation or other litigation that often results from a data beach.
  - Successfully defended more than two dozen data privacy class actions – either winning motions to dismiss or defeating class certifications in lawsuits brought after data breaches or based upon alleged violations of a company's privacy policy.

Mark L. Krotoski

Mark L. Krotoski
Silicon Valley
+1.650.843.7212
mark.krotoski@morganlewis.com

- Litigation Partner, Privacy and Cybersecurity and Antitrust practices with more than 20 years' experience handling cybersecurity cases and issues.
- Advises clients on mitigating and addressing cyber risks, developing cybersecurity protection plans, responding to a data breach or misappropriation of trade secrets, conducting confidential cybersecurity investigations, responding to regulatory investigations, and coordinating with law enforcement on cybercrime issues.
- Experience handling complex and novel cyber investigations and high-profile cases
  - At DOJ, prosecuted and investigated nearly every type of international and domestic computer intrusion, cybercrime, economic espionage, and criminal intellectual property cases.
  - 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.

Susan D. Resley

Susan D. Resley
San Francisco
+1.415.442.1351
susan.resley@morganlewis.com

Leading Morgan Lewis's Securities Enforcement Practice, Susan D. Resley advises individuals and organizations in securities-related investigations and litigation. Her clients include companies, boards and their committees, individual directors, senior officers, and employees of companies, as well as accounting firms, brokerage and investment advisory firms, and other financial institutions. Susan represents clients in proceedings brought by the Securities and Exchange Commission's (SEC) Division of Enforcement, the Department of Justice (DOJ), and the Public Company Accounting Oversight Board (PCAOB).

Kurt B. Oldenburg

Kurt B. Oldenburg
San Francisco
+1.415.442.1258
kurt.oldenburg@morganlewis.com

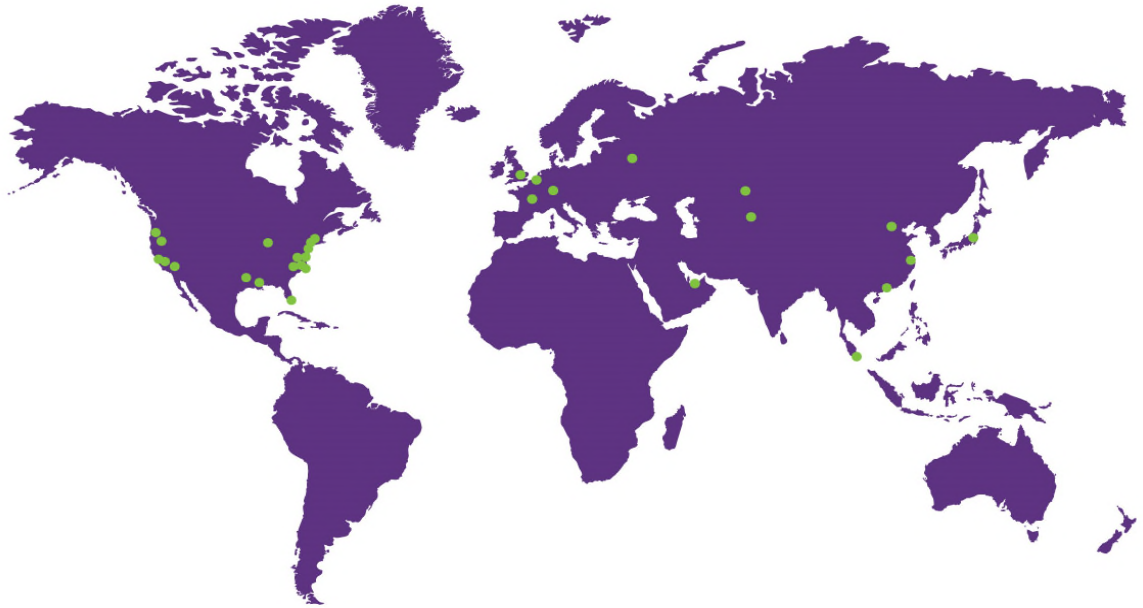
Kurt Oldenburg represents clients in complex commercial litigation, pre-litigation disputes, and white collar investigations. Kurt has litigated extensively in California and federal courts, most often representing clients in the technology, life sciences, and financial services sectors. Kurt also represents companies and individuals through high-stakes internal investigations and related proceedings before the US Department of Justice (DOJ) and Securities and Exchange Commission (SEC). Kurt devotes time to pro bono legal aid and he formerly worked for a non-profit dedicated to increasing access to justice among Californians.

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Almaty
Astana
Beijing*
Boston
Brussels
Century City
Chicago
Dallas
Dubai
Frankfurt
Hartford
Hong Kong*
Houston
London
Los Angeles
Miami
Moscow
New York
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Shanghai*
Silicon Valley
Singapore
Tokyo
Washington, DC
Wilmington



Morgan Lewis

*Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan Lewis operates through Morgan, Lewis & Bockius, which is a separate Hong Kong general partnership registered with The Law Society of Hong Kong as a registered foreign law firm operating in Association with Luk & Partners. Morgan Lewis Stamford LLC is a Singapore law corporation affiliated with Morgan, Lewis & Bockius LLP.

THANK YOU