Financial institutions
Energy
Infrastructure, mining and commodities
Transport
Technology and innovation
Life sciences and healthcare

NORTON ROSE FULBRIGHT

Cybersecurity Disclosure and Internal Controls

Association of Corporate Counsel

April 26, 2019

SEC's Increasing Emphasis on Cybersecurity

- The SEC formed a dedicated cyber unit in 2017
- According to the SEC Enforcement Division's FY 2018 annual report, the SEC brought 20 cyber-related enforcement actions last year
- The SEC has over 200 open cyber-related investigations

Overview and Implications of SEC's Guidance on Cybersecurity Disclosures

- In February 2018, SEC issued interpretive guidance "to assist public companies in preparing disclosures about cybersecurity risks and incidents"
- Guidance emphasizes Board's role in cybersecurity risk oversight
- May need to disclose prior or ongoing cybersecurity incidents in order to place discussions of risk in the appropriate context
- Disclosure controls should ensure that appropriate personnel have necessary information about cybersecurity risks and incidents so fully informed disclosure decisions can be made

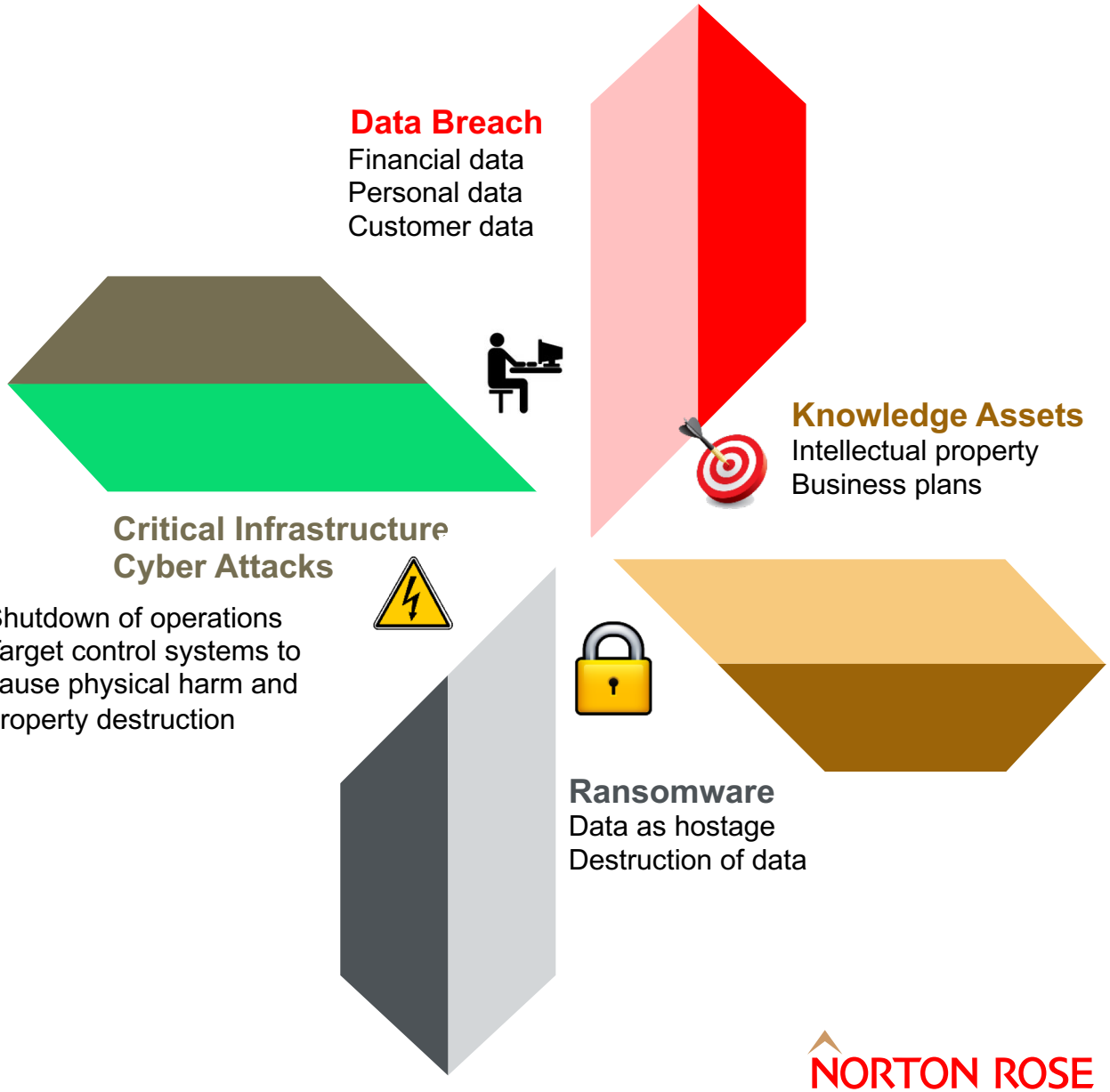
SEC Guidance: Disclosure Timing, Corrections, and Updates

- Timing of Incident Disclosures
  - "[W]e recognize that a company may require time to discern the implications of a cybersecurity incident"
  - "[A]n ongoing internal or external investigation – which often can be lengthy – would not on its own provide a basis for avoiding disclosures of a material cybersecurity incident"
- Correcting and Updating Disclosures
  - May have duty to correct prior disclosure if determine untrue at time made, such as by discovering contradictory information that existed at time made
  - May have duty to update disclosure if it becomes materially inaccurate after made
  - Should consider whether need to revisit or refresh during the process of investigating a cybersecurity incident

SEC Investigative Report on Cybersecurity Internal Controls

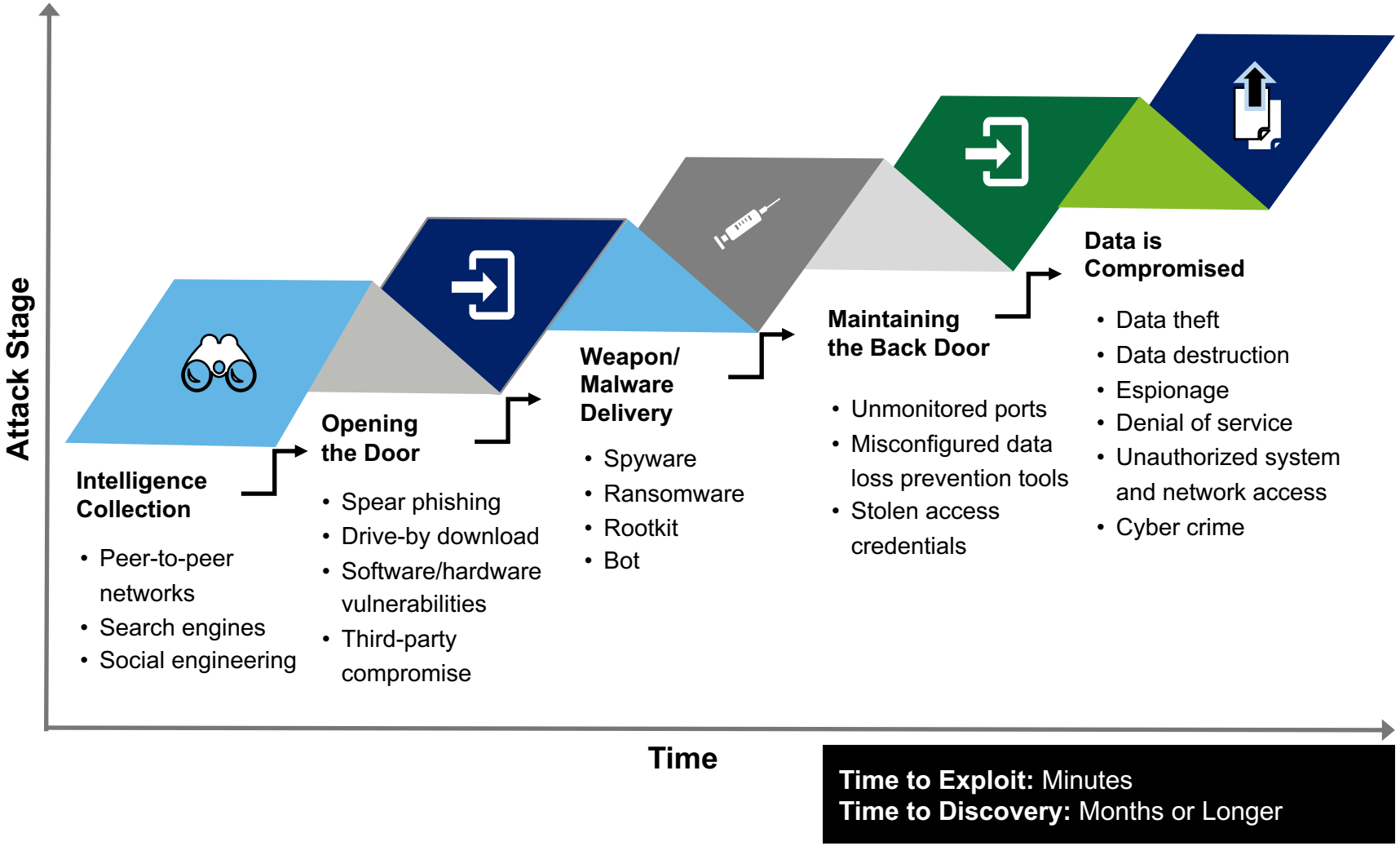
- On October 16, 2018, SEC issued investigative report emphasizing that public companies must consider cyber threats when implementing internal accounting controls
  - Companies must safeguard investor assets from cyber-related frauds
- Key Takeaways
  - Continually assess cybersecurity risks and calibrate internal controls accordingly
  - Factor human vulnerabilities into control design
    - Companies had appropriate policies in place but various aspects were ignored or misunderstood
  - Evaluate insider trading policies in relation to knowledge of cybersecurity risks and incidents

Types of Threats



NORTON ROSE FULBRIGHT

Lifecycle of a Cyber Attack



Source: Deloitte Development LLC

NORTON ROSE FULBRIGHT

Cyber Security as a Material Risk

1. Businesses are increasingly targeted

- **Fraud –** millions of dollars in losses
- **IP theft** – corporate espionage
- **Customer data theft** – financial data theft
- **Denial of service –** disruptions in operations (e.g., shutdown of industrial processes) and loss of customer trust
- **Physical harm –** attacks designed to cause harm

2. Cyber damages go beyond dollars

- Determine your **risk tolerance** and the **cost of protection**

3. Speed of attack is increasing, response times are shrinking, and the tail of a crisis-level data breach is long

- It only takes minutes to compromise and it may take years to recover
- Cyber security is a team sport. The General Counsel's office has a critical role to play in managing a cyber security incident as does the CISO.

4. Everything can't be protected equally

- Identify the '**crown jewels**' and high-impact, high-risk individuals/events – prioritize and invest in controls based on risk decisions
- Plan, budget, track, and report on the effectiveness of cybersecurity programs and internal controls

5. Traditional controls are necessary but should be augmented

- Perimeter defense is no longer sufficient
- Understand the impact of **changes in privacy laws and cybersecurity standards** and the need for continual assessment
- **Human error/lapses** continue to be one of the key reasons for breaches

6. Regulators, government, and the media are key stakeholders with ever increasing focus

- Understand the importance of communications and messaging, especially during a time of crisis

NORTON ROSE FULBRIGHT

Cybersecurity Risk Assessment Best Practices

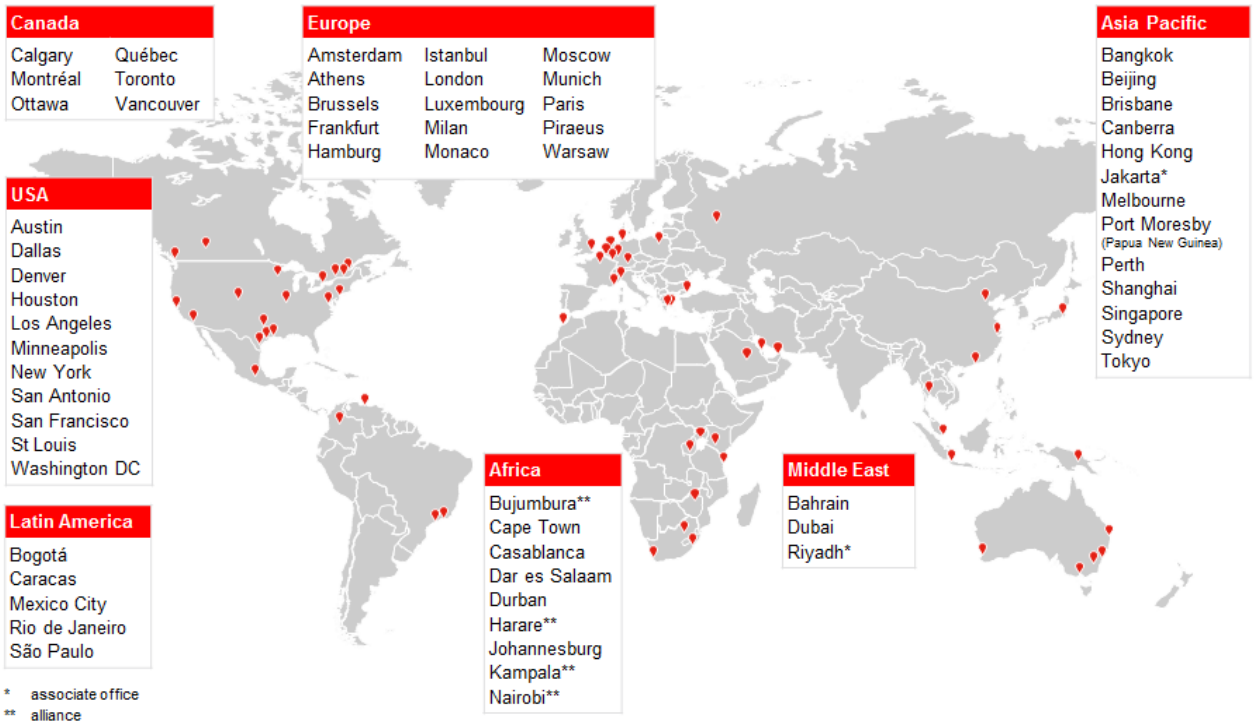
- Conduct a risk assessment to identify and prioritize important systems and information, the most likely threats to those systems, and the best controls to reduce or eliminate those threats

- Risk Identification Process
  - Create a inventory of systems and data
  - Determine the criticalness of systems and data
  - Identify key vulnerabilities and threats to systems and data
  - Collect and classify controls

About Norton Rose Fulbright

Cyber Law Firm of the Year
Insider's Cyber Ranking Awards 2018

Global footprint



* associate office
** alliance

Key industry strengths

Energy
Financial institutions
Infrastructure, mining and commodities
Transport
Technology and innovation
Life sciences and healthcare

Business principles

Quality. Unity. Integrity.

58

Offices, including locations in **major energy and financial markets**

4000+

Lawyers and other legal staff worldwide (900+ in US)

NORTON ROSE FULBRIGHT

Gerard G. Pecht

Global Head of Dispute Resolution and Litigation, Houston
T: +1 713 651 5243
gerard.pecht@nortonrosefulbright.com

Gerry Pecht concentrates his practice in the area of securities litigation, SEC enforcement and internal corporate investigations, both nationwide and globally. He regularly represents Fortune 500 companies and their officers and directors and has led many significant matters, including some highly sensitive ones, to a positive conclusion.

Litigation Experience: Gerry has extensive experience litigating in federal and state court and before arbitration panels, having tried over 30 matters to judgment. He has also argued appeals before the United States Courts of Appeal of the Second, Fifth, Tenth and Eleventh Circuits as well as the appellate courts of Texas. Gerry's litigation practice includes defending a large number of class actions, as well as shareholder derivative actions and a wide range of claims against corporations, underwriters, officers and directors. He has also represented companies in litigation over corporate control, including hostile tender offers and proxy solicitations. Gerry also has represented corporations as plaintiffs and has recovered on their behalf millions of dollars in judgments, settlements, mediations and arbitrations.

Enforcement Experience: Gerry's enforcement experience includes representing both companies and individuals in cases and investigations involving FCPA, disclosures, insider trading, market manipulation, accounting controls, and use of promotors. He has also represented companies, officers, and directors in inquires and investigations by the SEC, FINRA and the Texas State Securities Board (TSSB), as well as litigated cases against the SEC, before Administrative Law Judges and in federal courts.

Internal Corporate Investigations: Drawing on decades of experience representing issuers, officers and directors before the SEC, NASD, NYSE and in securities and derivative litigation, Gerry regularly represents the board, audit committees, special litigation committees and other committees of the board in internal investigations. His internal corporate investigations have involved a wide range of issues, including: accounting irregularities, alleged foreign corrupt practices, transactions with sanctioned countries, related party transactions, improper revenue recognition and financial disclosures, whistleblower claims, conflicts of interest, corporate malfeasance, and officer and director breaches of fiduciary and other duties.

Gerry has represented multinational companies in internal corporate investigations that have spanned the globe. He has experience in working with forensic experts, auditors, insurers, company counsel, public relations firms and regulators in connection with these investigations and he has expertise in assessing liability, fashioning disclosures, structuring remedial measures and devising corporate compliance programs. Gerry has handled corporate investigations for companies and board committees in industries such as software, oilfield service and supply, international construction, energy and medical services. In these investigations, Gerry regularly deals with US Attorneys, SEC, DOJ, Department of Commerce and Department of the Treasury.

NORTON ROSE FULBRIGHT

Mark Oakes

Partner-in-Charge, Austin
T: +1 512 536 5221
mark.oakes@nortonrosefulbright.com

Mark Oakes is the Partner-in-Charge of Norton Rose Fulbright's Austin office. His practice focuses on commercial and securities litigation.

Mark defends companies and their officers and directors in shareholder litigation arising out of mergers and acquisitions, alleged accounting irregularities and financial restatements, missed earnings guidance, internal control weaknesses, and alleged breaches of fiduciary duty in various contexts. Mark also represents companies and individuals in government investigations and performs internal investigations on behalf of audit committees and other board committees that involve a wide range of issues, including accounting irregularities, suspected violations of the Foreign Corrupt Practices Act and U.S. trade sanction and embargo laws, and alleged false statements to government agencies such as the SEC and the Department of Justice.

In addition to securities and corporate litigation, Mark represents clients in general commercial disputes. Mark's experience includes contractual lawsuits and arbitrations arising out of completed and failed business acquisitions, defending large fraudulent transfer claims made inside and outside the bankruptcy context, and various joint venture disputes.

NORTON ROSE FULBRIGHT


NORTON ROSE FULBRIGHT

Disclaimer

NORTON ROSE FULBRIGHT