MAYER·BROWN

Preparing For and Responding to a Computer Security Incident:

MAKING THE FIRST 72 HOURS COUNT

Marcus A. Christian
Partner
mchristian@mayerbrown.com

Rajesh De
Partner & Head of Global Cybersecurity & Data Privacy Practice
rde@mayerbrown.com

Stephen Lilley
Associate
slilley@mayerbrown.com

Jeffrey P. Taft
Partner
jtaft@mayerbrown.com

December 1, 2015

Today's Presenters

Raj De is a partner in Mayer Brown's Washington DC office and leads the firm's global Cybersecurity & Data Privacy practice. Raj focuses his practice on cutting-edge legal and policy issues at the nexus of technology, national security, law enforcement, and privacy. He has held senior appointments in the White House, the Departments of Justice and Defense, and the Intelligence Community. Most recently, Raj served as General Counsel of the National Security Agency before rejoining Mayer Brown.

Marcus Christian is a Washington DC partner in the firm's Cybersecurity & Data Privacy practice. He is also a member of the Litigation & Dispute Resolution and White Collar Defense & Compliance practices. Previously, he was the Executive Assistant United States Attorney at the U.S. Attorney's Office for the Southern District of Florida, the third-highest ranking position in one of the country's largest U.S. Attorney's Office. In this role, Marcus served on the senior management team and helped supervise over 220 federal prosecutors.

Jeffrey Taft is a Washington DC partner in the firm's Cybersecurity & Data Privacy practice. He is also a member of the Financial Services Regulatory and Enforcement practice. Jeff frequently counsels financial services companies on complex cybersecurity and data privacy issues generally, and on the specific challenges of preparing for and responding to computer security incidents.

Stephen Lilley is a Washington DC senior associate in the firm's Cybersecurity & Data Privacy practice, as well as its Supreme Court & Appellate practice. He focuses on helping clients navigate interrelated litigation, regulatory, and policy challenges, and frequently litigates and advises clients on cybersecurity and data privacy, and consumer financial services matters. He previously served as Chief Counsel to the Subcommittee on Crime and Terrorism of the U.S. Senate Judiciary Committee.

Agenda

- Introduction
- Readiness: Preparing for a Computer Security Incident
- Context: Understanding the Regulatory Framework for Responding to a Computer Security Incident
- Active Response: Delivering an Effective Response in Anticipation of Litigation

READINESS

Preparing for a Computer Security Incident

Readiness – Preparing for a Computer Security Incident

- Written Computer Security Incident Response Plan
- Team Elements
- Resource Considerations
- Training
- Tabletop Exercises
- Potential Pitfalls

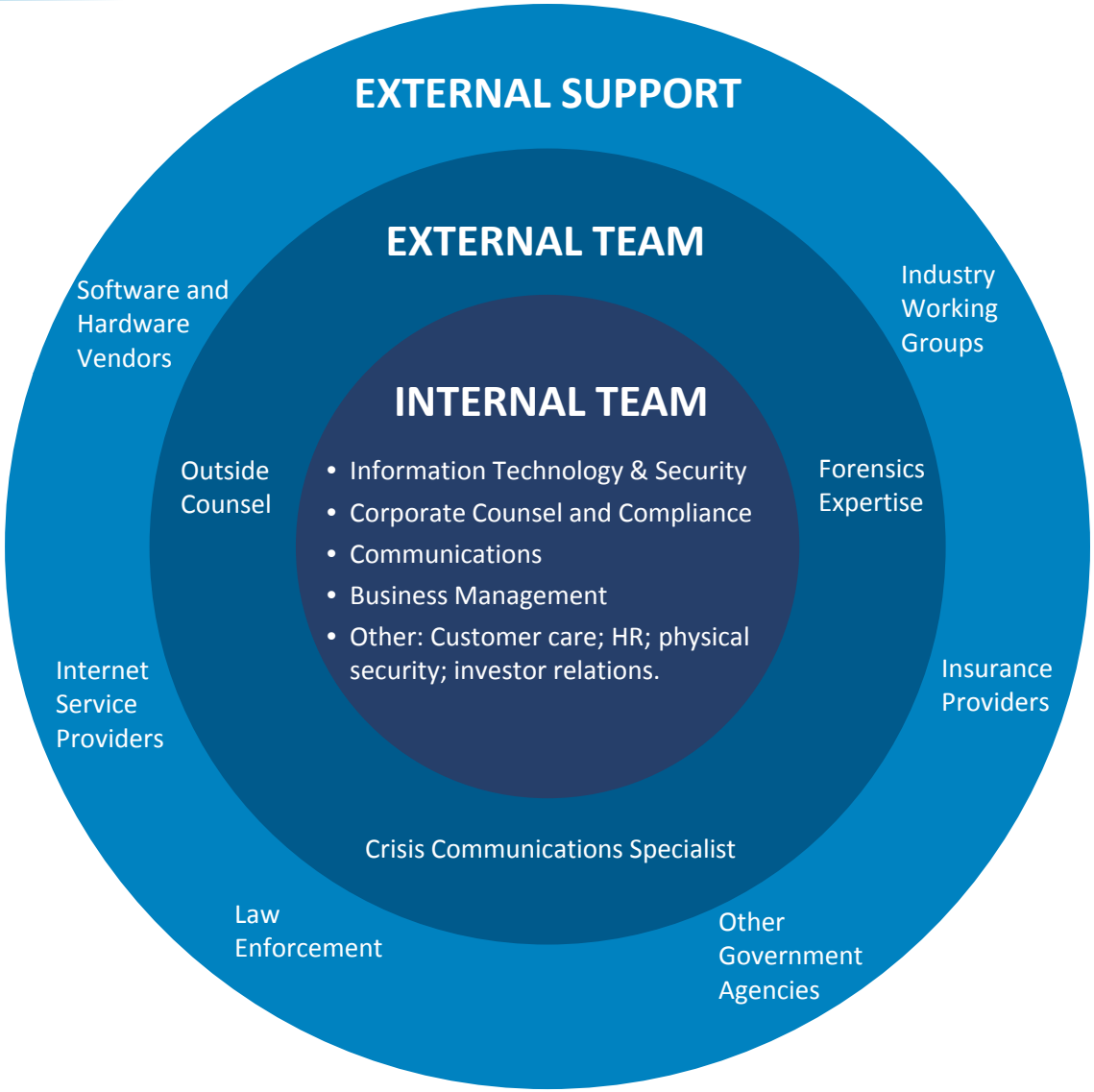
Computer Security Incident Response Plan

- A written computer security incident response plan ensures that business priorities guide the response function. This plan should:
  - Clearly state goals and objectives;
  - Categorize incidents to which the plan applies;
  - Establish incident severity categories and corresponding levels of deployment;
  - Identify response team members and their respective roles; and
  - Provide a structure that enables agile decision-making by the response team.
- The plan must be regularly assessed and revised as necessary to reflect new assets, business activities, or technologies.

Nuts and Bolts of a Response Plan

- Every computer security incident response plan will be tailored to a specific company's unique needs, but generally they all should include certain key elements:
  - Incident detection, notification, analysis, and forensics;
  - Response actions, including containment, remediation, and recovery;
  - Communications;
  - Procedures to capture lessons learned; and
  - Identification of necessary documents and key legal requirements.

Elements of a Collaborative Incident Response Team



MAYER·BROWN

Resources – Logistical Needs

- To facilitate your team's work, you will need to assure that they have the logistical support to operate when your information, technological, and even physical security might be compromised. Consider maintaining:
  - Dedicated clean laptops that can be used to record investigation activities, and others that can be used to connect to a compromised network without putting further information or assets (other than the laptop) at risk;
  - Secure communications;
  - A war room; and
  - A call center to interface with customers and employees as the incident develops.

Training and Practice

- Training and practice ensure that the effort and resources expended to prepare for a computer security incident are deployed efficiently and effectively when it counts.
- Regular tabletop exercises (e.g. twice a year) help keep the computer security incident response plan and the team's skills and relationships up to date.
- Employee training can demonstrate institutional commitment to cybersecurity in post-incident litigation.

Potential Pitfalls

- Lack of leadership “buy-in”
- Staleness of plan
- Incompleteness of investigation or remediation
- Inadequate training
- Unclear chain of command or authority

CONTEXT

Understanding the Regulatory Framework for Responding to a Computer Security Incident

Regulatory Framework for Incident Response

- Various federal and state laws establish frameworks that companies may be required to comply with, or may adopt as best practices. These include:
  - Federal Trade Commission Act
  - Gramm-Leach-Bliley Act
  - HIPAA
  - State Data Breach Notification and Data Security Laws
  - Best Practices and Industry Standards

Federal Trade Commission (FTC) Act

- Section 5 of the FTC Act, codified at 15 U.S.C. § 45, empowers the Commission to prevent all "*unfair or deceptive acts or practices in or affecting commerce*."
- For over ten years, the FTC has used its enforcement authority to bring actions against companies that it believes maintain unreasonable data security practices or deceive consumers about those practices – including practices relating to companies' response to computer security incidents. *See, e.g.*, Complaint, *FTC v. Wyndham Worldwide Corp.* (2012) (alleging that company failed to address exploited vulnerability, leading to successive breaches).
- Civil Investigative Demands (CIDs) issued by the FTC highlight the expansive inquiries into data security practices – including incident response capabilities – that companies may face in the aftermath of a breach. *See, e.g.*, CID to LabMD (requesting testimony on roles of various employees in incident response function).

The FTC's Dominant Role in Privacy and Cybersecurity Enforcement

- The FTC's scrutiny of incident response should be understood in the context of its active role in privacy and cybersecurity enforcement. It has brought over 50 cases in this field and has made clear its intention to bring more where it sees fit. For example:
  - The provider of a mobile photo and video messaging app settled charges that it deceived consumers over the amount of personal data it collected and the security measures taken to protect that data. The FTC alleged that the failure to secure the app enabled attackers to steal 4.6 million usernames and associated phone numbers.
  - The provider of a movie ticket purchasing service settled charges that it misrepresented the security of its mobile app and failed to secure the transmission of millions of consumers' sensitive data from this app. The app allegedly failed to authenticate and secure connections used to transmit this data, leaving credit card information vulnerable to exposure.

Gramm-Leach-Bliley Act (GLBA)

- This act imposes "affirmative and continuing obligation[s]" on financial institutions "to protect the security and confidentiality" of their customers' nonpublic personal information.
  - GLBA establishes compulsory standards to protect customers against "unauthorized access to or use of such records or information which could result in substantial harm."
  - The FTC, SEC, federal banking regulators and other regulators have promulgated regulations implementing this requirement.
    - For example, the FTC's Safeguards Rule requires companies to assess and respond to risks associated with "[d]etecting, preventing and responding to attacks, intrusions, or other systems failures." 16 C.F.R. § 314.4(b)(3).
    - In 2005, the FFIEC members issued *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice* to clarify regulated entities' obligations under GLBA.

HIPAA – Health Insurance Portability and Accountability Act of 1996

- The Department of Health and Human Service's Breach Notification Rule, 45 C.F.R. §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.
  - HIPAA notification requirements are triggered when a breach "is known, or by exercising reasonable diligence would have been known." 45 C.F.R. § 164.404.
- The HIPAA Security Rule, 45 C.F.R. Pt. 160, 164, establishes national standards to protect individuals' electronic personal health information. For example, under 45 C.F.R. § 164.308, covered entities must "[i]mplement policies and procedures to address security incidents." These include:
  - "Identify[ing] and respond[ing] to suspected or known security incidents;
  - Mitigat[ing], to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and
  - Document[ing] security incidents and their outcomes." *Id*.

Other Federal Agency Action

- The continuing trend has been for federal agencies to pay increasing attention to companies' response to computer security incidents.
  - Recently, the Department of Defense expanded rules requiring notification in the event of computer security incidents on contractors' networks. Interim Rule, 80 Fed. Reg. 51739 (Aug. 26, 2015).
- A variety of other federal agencies have issued regulations or undertaken enforcement actions relating to incident response and breach notification. These include:
  - Federal Communications Commission (FCC)
  - National Highway Traffic Safety Administration (NHTSA)
  - North American Electric Reliability Corp./Federal Energy Regulatory Commission (NERC/FERC)
- Other federal agencies have issued guidance:
  - The Justice Department's criminal division offered guidance in 2015 on best practices for responding to a computer security incident, including with respect to notifying law enforcement.
  - The National Institute of Standards and Technology has published various editions of its *Computer Security Incident Handling Guide.*

State Data Breach Notification and Data Security Laws

- Forty-seven states, the District of Columbia, and multiple U.S. territories have data breach notification laws, subject to enforcement by the state's attorney general. Common features of these laws include:
  - Required notice to consumers and/or the state;
  - Delayed notice obligation for law enforcement or remediation purposes; and
  - Exceptions from notice for encrypted data.
- Some states also impose data security requirements on companies holding the private information of their residents.
  - Massachusetts imposes the most comprehensive requirements, which include the mandatory creation of a written information security plan.
- Some state regulatory agencies have also begun to take action.
  - In 2015, the New York State Department of Financial Services announced its intention to consider new regulations to establish cybersecurity and breach notification standards for financial institutions.

Example State Law: California Data Breach Notification

- The California Attorney General, Kamala Harris, has "made it a priority to investigate data breaches."
- Under Cal. Civ. Code § 1798.82(a), a person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system . . . to a resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
  - "Personal information" is broadly defined.
  - Entities must notify the State Attorney General if more than 500 residents are implicated in a single breach.
  - Notice must be furnished in the "most expedient time possible and without unreasonable delay."
  - Effective 1/1/16, a specific form of notice to consumers is required.
- Cal. Civ. Code § 1798.29(a) imposes equivalent requirements on state and local agencies.

Best Practices and Industry Standards

NIST

- The NIST cybersecurity framework issued in February 2014 includes incident response as an element in the "Framework Core" and makes clear that an effective incident response capacity is a cybersecurity best practice.

PCI Data Security Standard (DSS)

- The PCI Security Standards Council is a global forum dedicated to designing security standards for the payment card industry. The PCI DSS "provides an actionable framework for developing a robust payment card data security process—including prevention, detection and appropriate reaction to security incidents."

ISO/IEC 27001:2013

- This standard, developed by the International Organization for Standardization, delineates best practices for information security management and also includes standards for evaluating organization-specific information security risks.

ACTIVE RESPONSE

Delivering An Effective Response In Anticipation Of Litigation

Priority Issues Across Each Phase of Active Response

- Investigating the Incident
- Documenting Actions and Facts
- Maintaining Privilege
- Maximizing Coordination
- Notifying Third Parties

Phases of Active Response: Detection

- Learning of an Incident
- Identification & Triage
  - Alerting the Response Team
  - Determining Incident Type
  - Estimating the Scope
  - Mobilizing Resources
  - Preserving Evidence
- Assessing Legal Ramifications

Phases of Active Response: Containment and Eradication

Containment

- Strategies for containment of an incident—with as limited a loss of functionality as possible—are case-specific. Factors to consider include:
  - Potential damage to or theft of resources;
  - Need for evidence preservation;
  - Service availability;
  - Time and resources needed to implement the strategy; and
  - Effect of the strategy.

Eradication

- After containment, the team should remediate vulnerabilities and remove malicious code from the system. This could entail:
  - Removal of malware;
  - Replacement of vulnerable equipment or software;
  - Reconfiguration and patching of equipment or software;
  - Privilege revocation; or
  - System reconstruction.

Phases of Active Response: Recovery and Lessons Learned

Recovery

- The recovery process should both restore operations and prevent repeat compromise, including by:
  - Restoring systems from appropriate backups;
  - Patching devices to remove known vulnerabilities;
  - Monitoring the network; and
  - Restarting operational systems and applications.

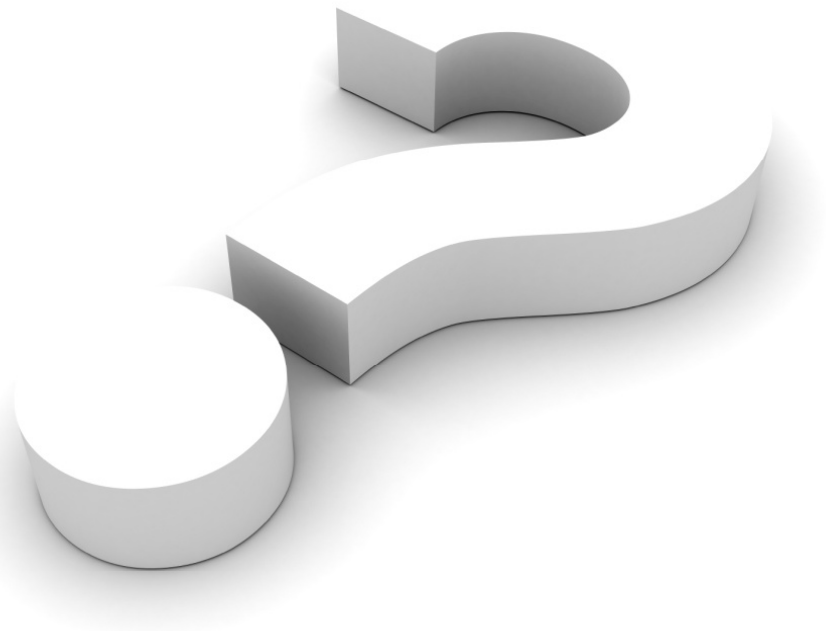
Learning from the Incident

- The response team should ensure that lessons from an incident are captured and communicated across the enterprise, including by:
  - Assessing the sufficiency of the response plan;
  - Assessing team structure and performance; and
  - Ensuring that lessons learned are transmitted across the enterprise, including by amendment of relevant policies.

Litigation in the Aftermath of a Computer Security Incident

- Recent consumer class actions confirm that expensive litigation remains a likely consequence of a data breach.
  - Shareholder derivative litigation, securities class actions, and third-party litigation are also possible.
- Most frequently, these class actions are filed based on mere speculation about the victim company's data-security and breach-notification practices.
  - Claims have specifically targeted the sufficiency of a company's response to a computer security incident, even beyond the adequacy of the notice provided.
- Strong defenses exist regarding standing and the sufficiency of common law and statutory claims, although recent decisions of the Seventh Circuit and other courts have created new uncertainty.

QUESTIONS



Marcus A. Christian
Partner
mchristian@mayerbrown.com

Rajesh De
Partner & Head of Global Cybersecurity & Data Privacy Practice
rde@mayerbrown.com

Stephen Lilley
Associate
slilley@mayerbrown.com

Jeffrey P. Taft
Partner
jtaft@mayerbrown.com

MAYER·BROWN