Breaches and Sensitive Documents: How to Prepare, Respond, and Protect Yourself (and your Company)

Evan Wolff
Partner and Chair, Privacy and Cybersecurity Practice
Crowell & Moring LLP
Ewolff@crowell.com

Evan Wolff, Partner

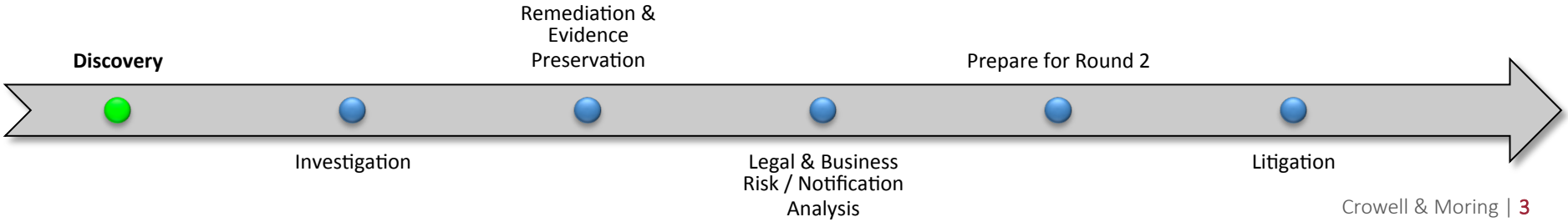
A unique Washington lawyer, Evan D. Wolff possesses the hands-on experience in the technologies and policies that govern the cybersecurity space and is an authority on cybersecurity and privacy regulations. Evan served as an advisor to the senior leadership at the stand-up of the Department of Homeland Security. He is a highly sought-after lawyer for leading defense, energy and manufacturing companies and a thought leader on federal government initiatives in public and private sector coordination in addressing cyber issues.

As Crowell & Moring's Privacy & Cybersecurity Practice Co-chair, Evan advises companies on network security, investigation coordination after intrusions, data breaches, and insurance issues. Evan recognizes that despite best efforts cyber incidents happen, so he takes an innovative approach to developing blended legal, technical, and governance mechanisms so companies are prepared with a rapid and comprehensive response. This includes conducting incident simulations and developing incident response plans. He has advised companies and their boards on more than 100 data breaches, managing the legal, technical, and management aspects of those responses.

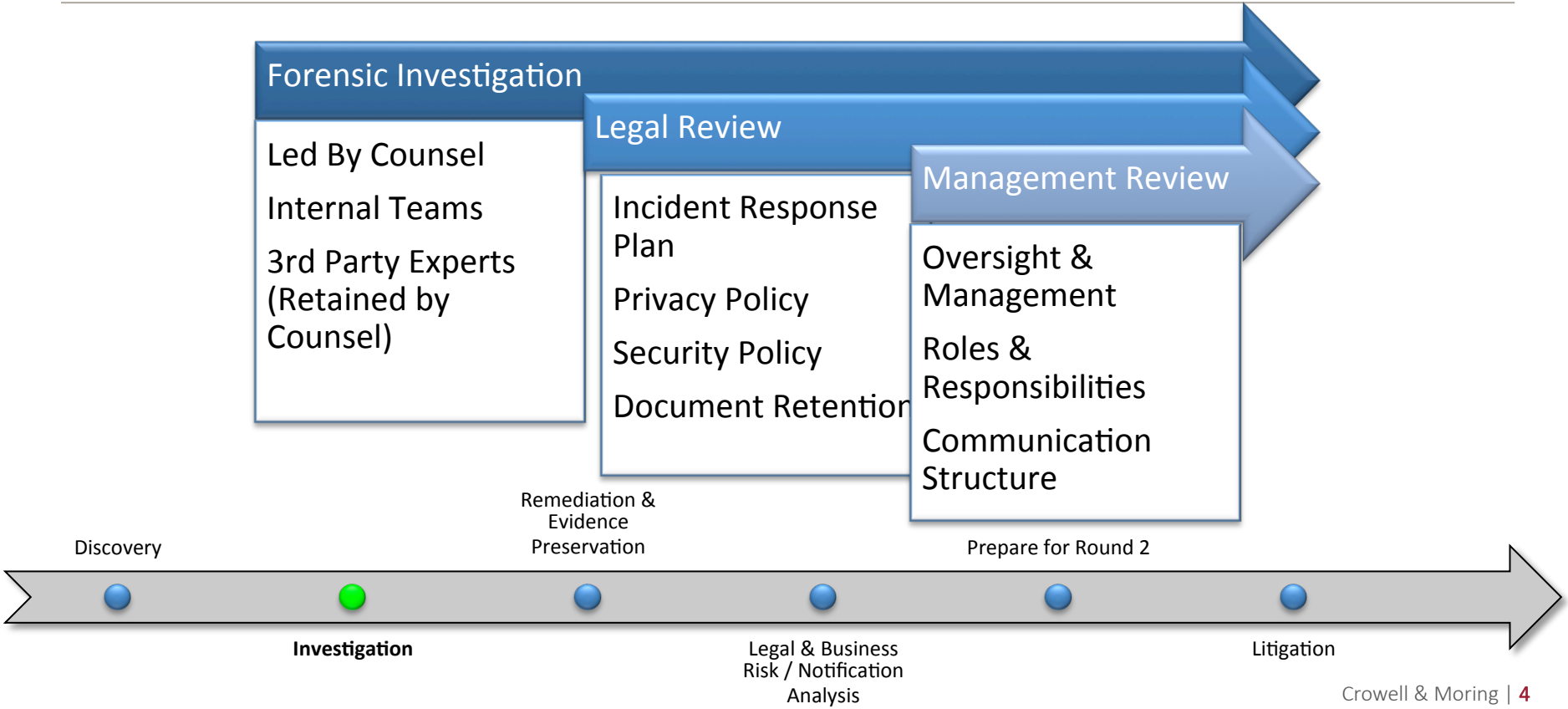
Evan believes in building a community and is co-chair of the ABA's Homeland Security Law Institute and senior advisor to the ABA Committee on Law and National Security; advisor to The Chertoff Group; an adjunct professor at George Mason University School of Law; a fellow with the Woodrow Wilson International Center for Scholars; and a member of the Sandia National Lab External Advisory Board, the U.S. Chamber of Commerce National Security Task Force, and the Aspen Institute's Homeland Security Group.

Discovery

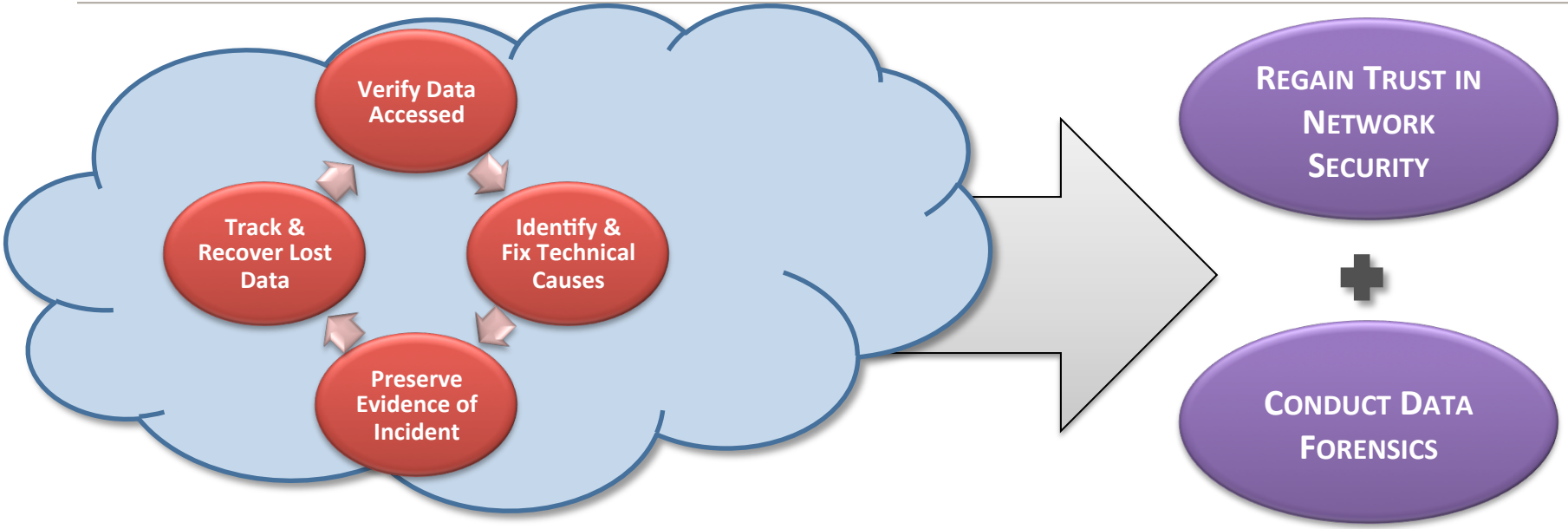

IT Help Desk Call
3rd Party Notification
IT Staff Detects
Law Enforcement Notification
INCIDENT IDENTIFIED


Discovery
Investigation
Remediation & Evidence Preservation
Legal & Business Risk / Notification Analysis
Prepare for Round 2
Litigation

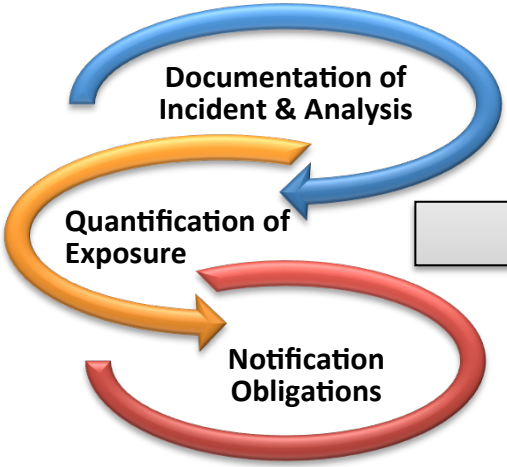
Investigation



Remediation & Evidence Preservation



Legal & Risk Analysis / Notification



NOTIFICATION CONSIDERATIONS

- Federal & State Compliance
- Who to Notify?
- Preparing Materials
- Timing (Legal, Regulatory, etc.)
- Law Enforcement/Regulator Coordination
- Media/Messaging
- 3rd Party Providers

Discovery

Investigation

Remediation & Evidence Preservation

Legal & Business Risk / Notification Analysis

Prepare for Round 2

Litigation

Prepare for Round 2

Prepare Immediately For Follow-on Incident Response After Notification

Highly Publicized Targets of Attack Typically Experience Further Attacks

Discovery

Investigation

Remediation & Evidence Preservation

Legal & Business Risk / Notification Analysis

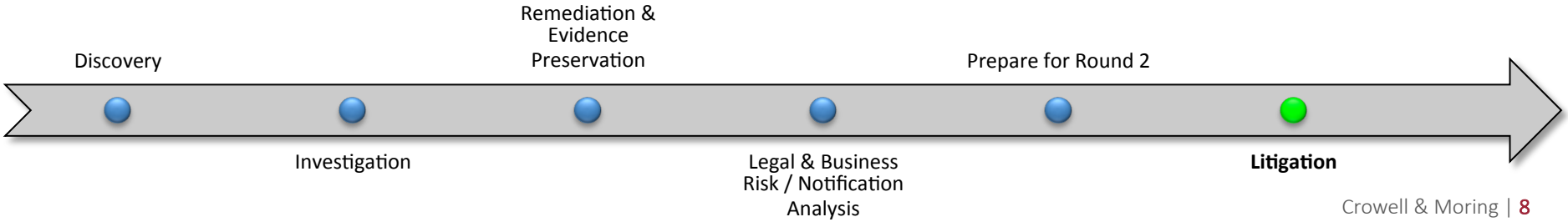
Prepare for Round 2

Litigation

Litigation

CAUSES OF ACTION

- Class Actions
- Negligence
- Breach of Contract
- Federal and State Regulatory Actions
- LE/Criminal Actions
- Breach of Privacy
- State Statutes – e.g., CMIA
- Tort Claims
- Shareholder Actions
- International Actions



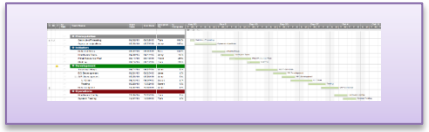
- Risk Management is a continual, systematic process of awareness, assessment, action and adapting your plan.

- Compliance ≠ security spend ≠ risk reduction

- Focus on:
  - Know your data, network and regulations
  - Establish governance
  - Create clear policies and procedures
  - Manage technical and administrative controls

Simplified Recommendation

In Protecting your Data



Continually progress forward with a plan. Identify and prioritize known area of weaknesses. Have a plan and execute … moving forward is better than paralysis through analysis

Single-factor authentication is compromised more often than any one vector. Implement stronger authentication solutions and don't make exceptions.

Know what assets you have and keep them patched. #2 most compromised vector. 1) few companies have an accurate inventory of assets, 2) they almost never keep them properly patched consistently across the enterprise, and 3) often, non-production, critical systems aren't properly prioritized

User Awareness Training and continuous role playing is critical. You can't solve for dumb, but you can reduce risk for the average user. 1) train and test 2) leverage email gateways. Strip all executables and macro-enabled documents, where applicable (exclude for corner cases, not build too, 3) Weed out the dummies and address

Most breaches are starting with a **compromised user device. Plan with the assumption that a users credential will be compromised.** Limit the sensitive data distribution and use. **Build monitoring at a user level.**

Malware is not going anywhere. We assume you have client-based anti-virus running, which is a start. **Enrich AV** with **network malware detection, sandboxing technologies** and **application whitelisting.**

Containerize and Encrypt all mobile devices! 1) Be careful to understand what MDMs do and don't do, 2) understand BYOD tradeoffs, 3) forecast – a reckoning is coming within mobile 3) containerize confidential data

Threat Intelligence if operationalized is powerful. 1) if its in the news, its probably to late, 2) customer specific intel and monitoring is critical, 3) A key is knowing what the next looming threat might look like and how to plan, recognize, respond and mitigate it as necessary.

crowell.com

Crowell & Moring LLP is an international law firm with approximately 500 lawyers representing clients in litigation and arbitration, regulatory, and transactional matters. The firm is internationally recognized for its representation of Fortune 500 companies in high-stakes litigation, as well as its ongoing commitment to *pro bono* service and diversity. The firm has offices in Washington, D.C., New York, Los Angeles, San Francisco, Orange County, London, and Brussels.