HUNTON& WILLIAMS

THE CYBERSECURITY EXECUTIVE ORDER: UNDERSTANDING ITS IMPACT ON YOUR BUSINESS

HUNTON & WILLIAMS LLP
LISA J. SOTTO, JOHN J. DELIONADO AND EVAN D. WOLFF

PwC
JACK L. JOHNSON, JR., EMILY STAPF AND NEAL A. POLLARD

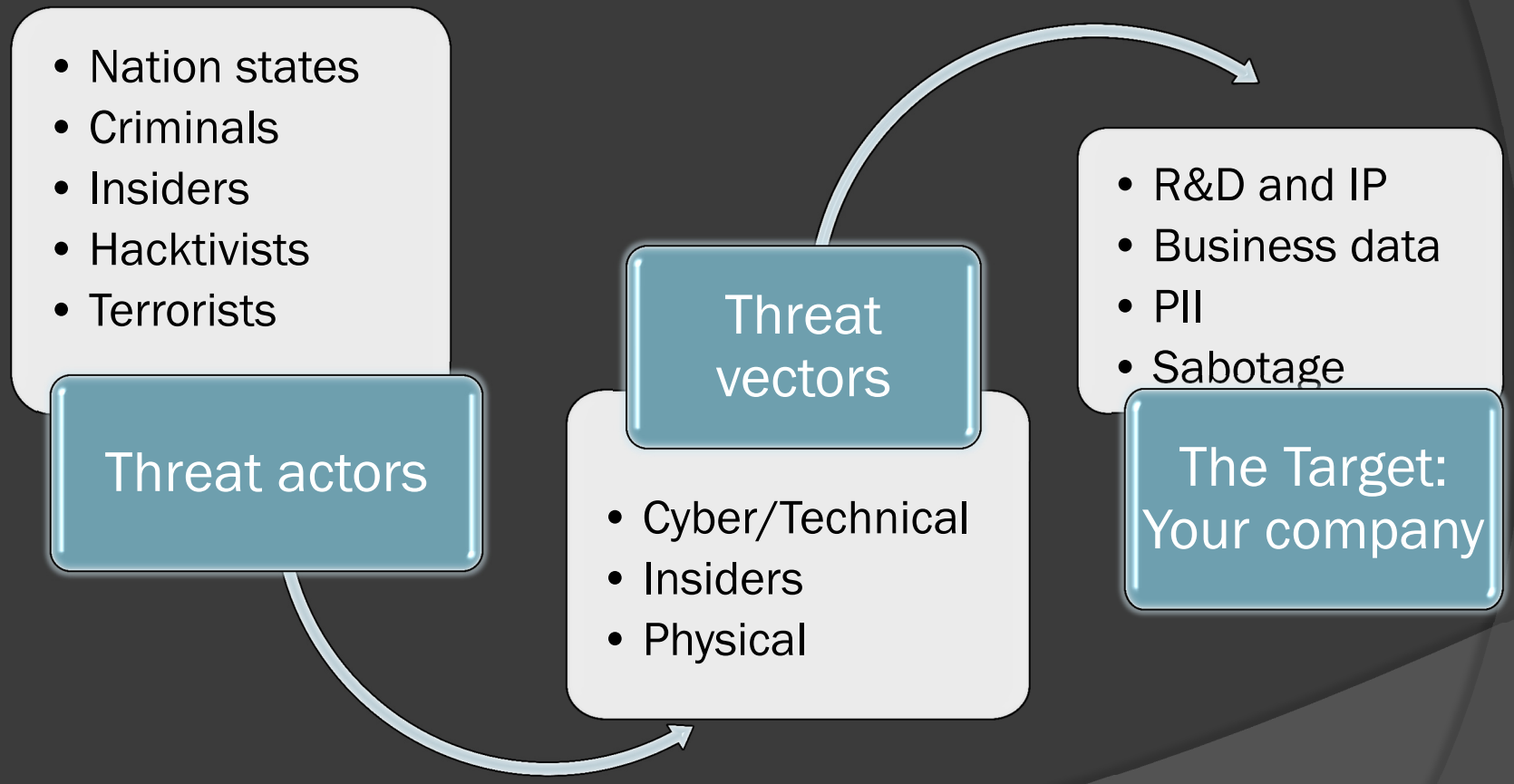
February 20, 2013

Our Practice

- H&W's Cybersecurity Risk Management and Investigations Team
  - Interdisciplinary practice
    - Privacy, Data Security, Investigations, Homeland Security, Litigation and SEC
  - Representing clients across multiple industry sectors
    - Including financial services, health care, energy, technology and retail
- The Centre for Information Policy Leadership at Hunton & Williams
- www.huntonprivacyblog.com
  - @hunton_privacy

HUNTON& WILLIAMS

Analyzing the Threat Landscape: The First Step in a Risk-based Approach



HUNTON& WILLIAMS

Threat Targets

- Threat targets
  - Financial institutions, energy sector, news media, payment card industry, technology, health care, retailers
  - Also government agencies at all levels (U.S. and abroad)
- High-profile attacks led to action in D.C. and Brussels

HUNTON& WILLIAMS

U.S. Government Efforts to Date

- Legislative efforts have failed to date
- EO drafting began in September 2012
- Final EO was issued on 2/12/13
- Congress has now stepped up its efforts

HUNTON& WILLIAMS

The Executive Order

- Three primary objectives
  - Improves cybersecurity information-sharing between government and business
  - Directs NIST to create a Cybersecurity Framework
  - Directs DHS to identify the critical infrastructure at greatest risk
- Implications

HUNTON& WILLIAMS

Opportunities for Both Private and Public Sectors

- The EO sets **broad guidelines** for Homeland Security, Commerce and other agencies to adapt detailed cybersecurity procedures to stakeholders' needs, and establishes coordination efforts
- Calls for use of **risk-based** rather than compliance-based approach to cybersecurity
- Emphasis on **voluntary information-sharing** and **public-private consultation to identify and mitigate risk** to critical infrastructure
  - Significant voice for private sector
- Implementation and impact will be influenced or supported by possible 2013 legislation, including proposed Cyber Intelligence-Sharing and Protection Act

HUNTON& WILLIAMS

Specific Opportunities from the EO

- Building a Cybersecurity Framework (*Section 7*)
  - Consistent standards across industries improve certainty of processes and procedures for infrastructure owners/operators
  - Consultative process—including public review, input from across USG—improves likelihood of developing effective approaches to mitigating cyber risk.
- Identifying and Incentivizing Critical Infrastructure (*Sections 8 and 9*)
  - Help shape the "voluntary critical infrastructure security program" including establishment of incentives for participation
  - DoD and GSA will recommend ways to incorporate cybersecurity requirements in federal procurements / contracting by mid-July

HUNTON& WILLIAMS

Specific Opportunities from the EO (continued)

- Expanding cybersecurity information-sharing (*Section 4*)
  - Focused on US government providing information to critical infrastructure
  - Clearly identify the type of information needed to protect critical functions, data
  - Participate in setting rules and procedures for information-sharing, including best use of private-sector employees who can be embedded in federal agencies

HUNTON& WILLIAMS

Impact of Congress

- Legislative activity might pick up on key themes from 2012
  - FISMA reform
  - Education and building the workforce
  - R&D
- Some elements of the EO are ripe for legislative reference
  - Risk assessment, controls, and improvements in the Framework, per Sec. 7
  - Identification and designation as a critical infrastructure owner/operator, under Sec. 9
  - Need for regulatory or other authorities identified pursuant to Sec. 10
- Cyber Information-Sharing and Protection Act of 2013 (CISPA)
  - Reintroduced February 14
  - Addresses a significant concern of businesses: liability limitation

HUNTON& WILLIAMS

EU Regulatory Efforts

- On Feb. 7, 2013, EC issued a draft Directive on cybersecurity
- Broad set of companies will need to adopt strict network security standards
- Requirements to report security incidents to regulators and, in some cases, the public
  - Regulators authorized to request security audits and issue binding instructions
- Member States will impose sanctions for non-compliance

HUNTON& WILLIAMS

Identifying an Attack

- Watch for aberrant activity
  - Financial losses
  - System shutdowns
  - Customer complaints
  - Notice from payment card brands
  - Results of scans for malware and vulnerabilities
- Cyber threat notifications from law enforcement
- Determine the nature and scope of the attack
  - May require assistance from outside experts and law enforcement
  - Duration and sophistication of attack
  - Attackers' efforts at concealment
  - Access or acquisition of data, trade secrets and other proprietary information
- Restore the integrity of the system

HUNTON& WILLIAMS

Conduct an Investigation

- Potentially significant legal ramifications
- Understand:
  - Nature of the compromise
  - Data and systems at issue
  - Whether communications systems are secure
  - Whether insiders are involved
- Importance of preserving privilege
- Retention and oversight of forensic experts
- Consider forensic imaging, records retention and e-discovery obligations

HUNTON& WILLIAMS

Early Legal Considerations

- Understand your legal obligations arising out of a cyber event
  - Breach notification and other regulatory obligations
    - State, federal, international law
    - Industry standards
    - Contractual obligations
- Proactive measures
  - Offensive litigation
  - Hacking the hacker
    - But understand legal issues

HUNTON& WILLIAMS

Coordination with Regulators and Law Enforcement

- New obligations resulting from enhanced information-sharing
- Law enforcement often has a broader view into cyber threats
- Establish an early line of communication
- Determine the most appropriate agency
  - Depends on the nature of the compromise
  - Local, federal and international law enforcement may be necessary

HUNTON& WILLIAMS

Notification Process

- Where appropriate or required, craft formal notification and reporting documents
  - Must be done carefully (and quickly)
  - Consider PR experts as well
- Take proactive measures to mitigate risk
  - Manage media response
  - Assemble call center
  - Develop FAQs and train agents
  - Consider identity protection service

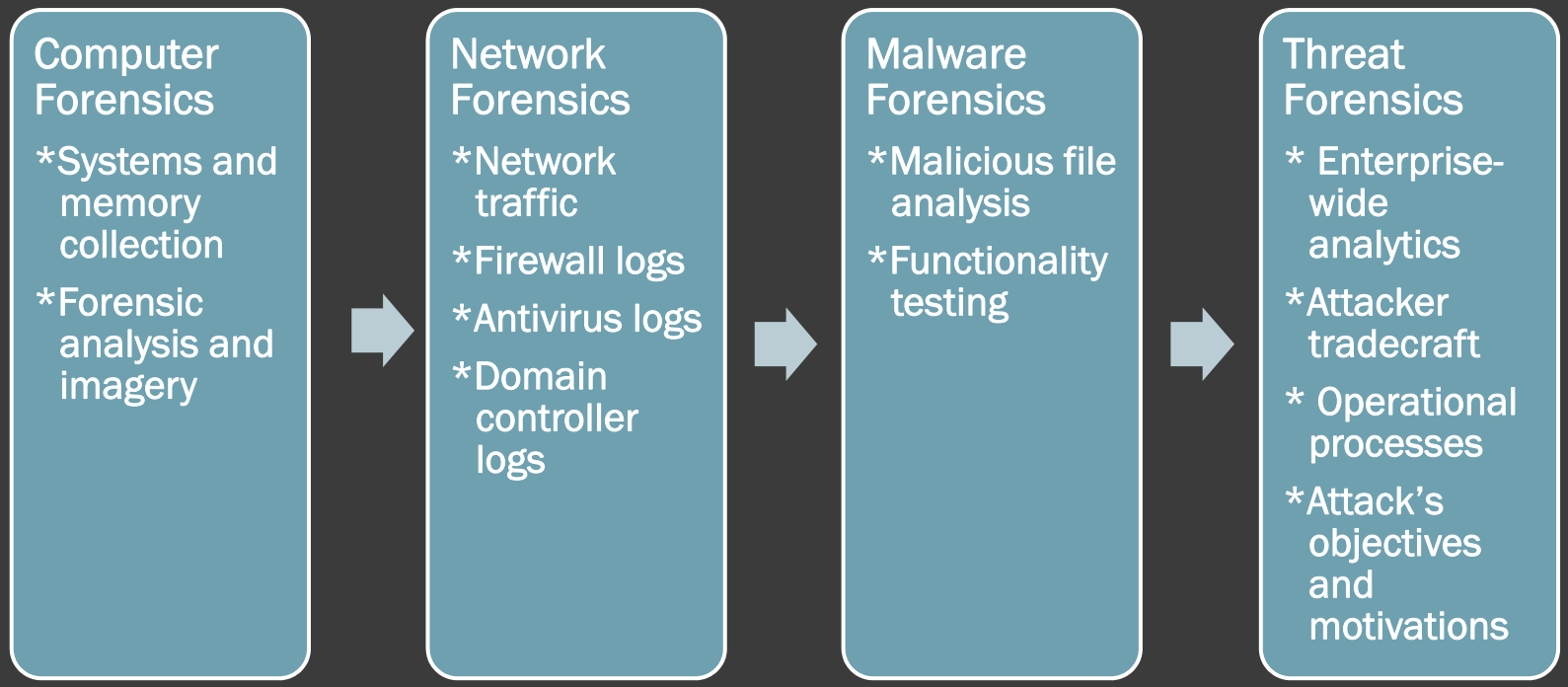
HUNTON& WILLIAMS

Risk and Dispute Management

- Assess potential insurance claims
- Assist law enforcement with criminal prosecution of attackers
- Defend against legal actions
  - Regulatory enforcement
  - Class action litigation
- Manage disputes with business partners and other third parties

HUNTON& WILLIAMS

A Case Study of State-sponsored Cyber Espionage



- **Client Issue:** FBI advised a US-based energy company that a Foreign State actor had compromised its network. The FBI offered to share information about the attacks with specialists who held clearances. The company hired PwC's cleared cybercrime team to help investigate.
- The threat actor used an Advanced Persistent network intrusion to compromise hundreds of systems and steal economic details related to myriad business deals.

HUNTON& WILLIAMS

Looking Ahead: Anticipation Is the Best Mitigation

- Implementation of the EO should provide opportunities for organizations to improve their cybersecurity—but the threat will remain
- Successful, resilient enterprises recognize this and will seek additional, proactive measures to protect their IT systems
- Using integrated threat intelligence and analysis will be one key way to stay ahead of criminals, hostile nation-states, hacktivists, and other threat actors
  - Threat modeling to identify threat actors, motivations and threat vectors (cyber and non-cyber)
  - Threat-informed asset identification and valuation to understand what corporate crown jewels are being targeted today and in the future
  - Threat analysis that integrates open source intelligence (OSINT), and proprietary cyber threat intelligence
  - Strategic analysis to provide context to emerging threats and identify future security challenges

HUNTON& WILLIAMS

Questions?

- **Hunton & Williams LLP**
  - **Lisa J. Sotto**
    Partner and Head of the Privacy and Data Security Practice
    (212) 309-1223, lsotto@hunton.com
  - **John J. Delionado**
    Partner
    (305) 536-2752, jdelionado@hunton.com
  - **Evan D. Wolff**
    Partner and Director of Homeland Security Practice
    (202) 955-1908, ewolff@hunton.com
- **PwC**
  - **Jack L. Johnson, Jr.**
    Principal, Washington Federal Practice
    (703) 918-1303, johnson.jack@us.pwc.com
  - **Emily Stapf**
    Director, Forensic Services Practice
    (703) 868-0269, emily.stapf@us.pwc.com
  - **Neal A. Pollard**
    Director, Forensic Services Practice
    (571) 217-4456, neal.a.pollard@us.pwc.com

HUNTON& WILLIAMS

HUNTON& WILLIAMS