Elements of a Cyber Incident Response Plan

Theresa A. Masse, CISO

Port of Portland

October 29, 2018

Presentation Overview

- Why You Need a Plan
- Core Plan Elements
- Exercises Are Essential
- Overview of Port Cyber IR Exercise

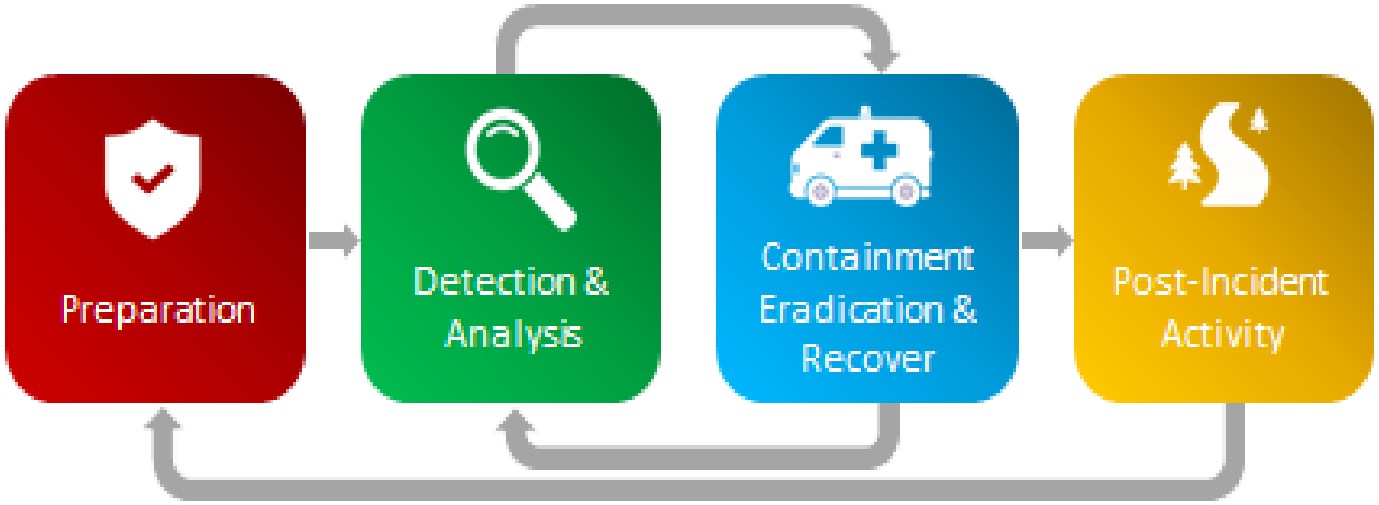
Why You Need A Plan

- A cyber incident can happen at any time
- Key staff may not be available
- More than just Info Security & IT are involved
  - It’s a business risk issue!
- Helpful to have a playbook in the midst of a crisis – you won’t remember everything
- The Plan is a living document – conduct regular exercises and update based on lessons learned

Core Plan Elements

- Every cyber incident is different - you can’t cover every possibility
- Cyber is dynamic and systems change
- Make it comprehensive - but not overwhelming
- Map it to the FEMA – Incident Command System (ICS)
- Checklists are helpful
- Determine what other entities to notify
- Include Data Breach Notification laws

Core Plan Elements



Core Plan Elements – Purpose

- 1 Purpose
- 1.1 Objectives
- 1.2 Priorities
- 1.3 Scope
- 1.4 Definitions

Core Plan Elements – Preparation

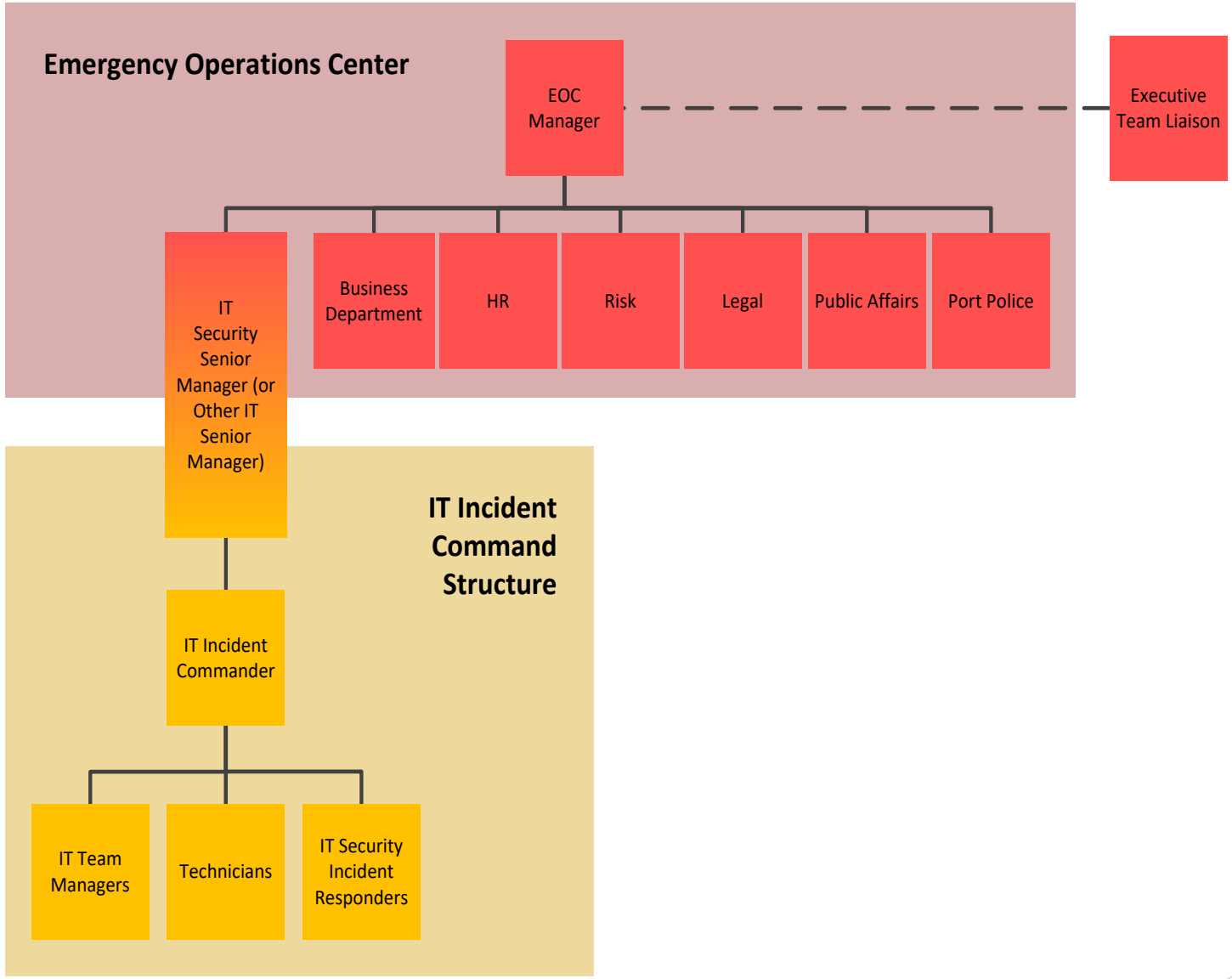
- Preparation
- 2.1 Incident Command System (ICS)
- 2.1.1 Key Concepts of ICS
- 2.1.2 Stand-up of ICS
- 2.2 Incident Commander (IC) Roles and Responsibilities
- 2.2.1 Designation of an IC
- 2.2.2 Transfer of IC Designation
- 2.2.3 Incident Commander Responsibilities
- 2.3 IT ICS Team

Core Plan Elements – EOC

- Emergency Operations Center (EOC)

- 2.4.1 IT Incident EOC Staff (Port only)
- 2.4.2 Third Party Security Vendors, Legal Assistance, External Resources
- 2.4.3 EOC and ICS Team Coordination
- 2.5 IT Incident Escalation

Core Plan Elements – Incident Escalation



Core Plan Elements – Communication & Reporting

- 2.6 IT Incident Communication & Reporting
- 2.6.1 Initial Report of Potential Event/Incident
- 2.6.2 Federal Reporting Requirements
- 2.7 Testing the Plan

Core Plan Elements – Detection & Analysis

- Detection and Analysis
- 3.1 Identification and Escalation of an Incident
- 3.2 Risk Assessment
- 3.3 Management Reporting
- 3.4 Confidentiality & Privilege
- 3.5 Coordination with External Parties
- 3.6 Handling of Systems Involved in the Incident
- 3.7 Documentation
- 3.8 Collect and Preserve Information

Core Plan Elements – Containment, Eradication & Recovery

- Containment, Eradication and Recovery
- 4.1 Containment
- 4.2 Eradication
- 4.3 Remediation
- 4.4 Recovery

Core Plan Elements – Post-Incident

- Post-Incident Activity
- **Appendix A** Incident Command System Team Members
- **Appendix B** Information Technology Incident Response Supplemental Information
- **Appendix C** Incident Response Checklist
- **Appendix D** IT Incident Response Workflow
- **Appendix E** Evidence Collection Supplemental Information

Initial Incident Response Ticket

Incident Ticket Field	Action
Impact Ratings	Input initial Functional Impact, Information Impact, and Recoverability ratings
Threat Vector	Input if known
Stage of IR	Change to “Stage Three”
Incident Response Activity Log	Enter all relevant activities that have been performed during this step
Root Cause Analysis and Related Indicators	Enter all appropriate findings
Damage Assessment	Enter all appropriate findings
File Attachments	Attach any relevant Incident files

Core Plan Elements – Forms

- **EVIDENCE COLLECTION FORM**
- **Appendix F** Legal and Regulatory Incident Response Supplemental Information
- **Appendix G** External Communications Supplemental Information
- **Appendix H** IT Cyber Incident Notification Form
- **Appendix I** Law Enforcement Notification
- **FBI CJIS DIVISION REPORTING FORM**
- **Appendix J** Data Breach Notification Laws

Exercises Are Essential

- Practice-Practice-Practice – exercise as often as possible!
  - increase complexity over time
- Plan realistic scenarios for your organization
- Involve key players:
  - internal business partners -- including sr. management
  - external business partners
  - secondary team members - as observers
- Ideally - have a facilitator
- Always have a scribe
- Document ‘lessons learned’
  - follow-up on any issues
  - update your plan

Overview of Port Cyber IR Exercise

- **Scenario – Airport Badging Application Breached**

- Four hour tabletop exercise
- Think - Federal Office of Personnel Management (OPM) breach - only smaller!
- External consultant – plan, facilitate, scribe, & document lessons learned
- Key player – external legal counsel – (Cyber Insurance)
- Key message – *business risk issue* - - not IT or info sec

Overview of Port Cyber IR Exercise – cont'd

- Internal & external implications
- Port players – IT, Info Sec., Airport Ops, Legal, Risk, HR, PR, Finance, Police, Emergency Management, Exec. Management
  - observers – internal & external
- External players – TSA, FBI, & External Legal Counsel
- Lots of lessons learned!!

Part 2: What to do in a Data Incident

- The Threat Landscape - Recent Trends
- Mitigating Risk - Insurance Considerations
- Life-cycle of a Data Incident
- Questions

Simone McCormick, Esq.,CIPP/US

- Partner at Lewis Brisbois Bisgaard & Smith LLP in Portland, Oregon;
- Member of LBBS's national Data Privacy and Cybersecurity Team;
- Represents clients in privacy and employment matters in state and federal courts, administrative hearings and in government investigations;
- Acts as breach coach in data incidents, conducts risk analysis, audits, trainings and investigations;
- Prepares contracts (e.g. BAAs), specifically tailored policies, procedures and handbooks;
- Counsels clients in compliance, risk management and best practices;
- Is a Certified Information Privacy Professional (CIPP/US) by the International Association of Privacy Professionals (IAPP).

LEWIS BRISBOIS

Trends in data security

Trends

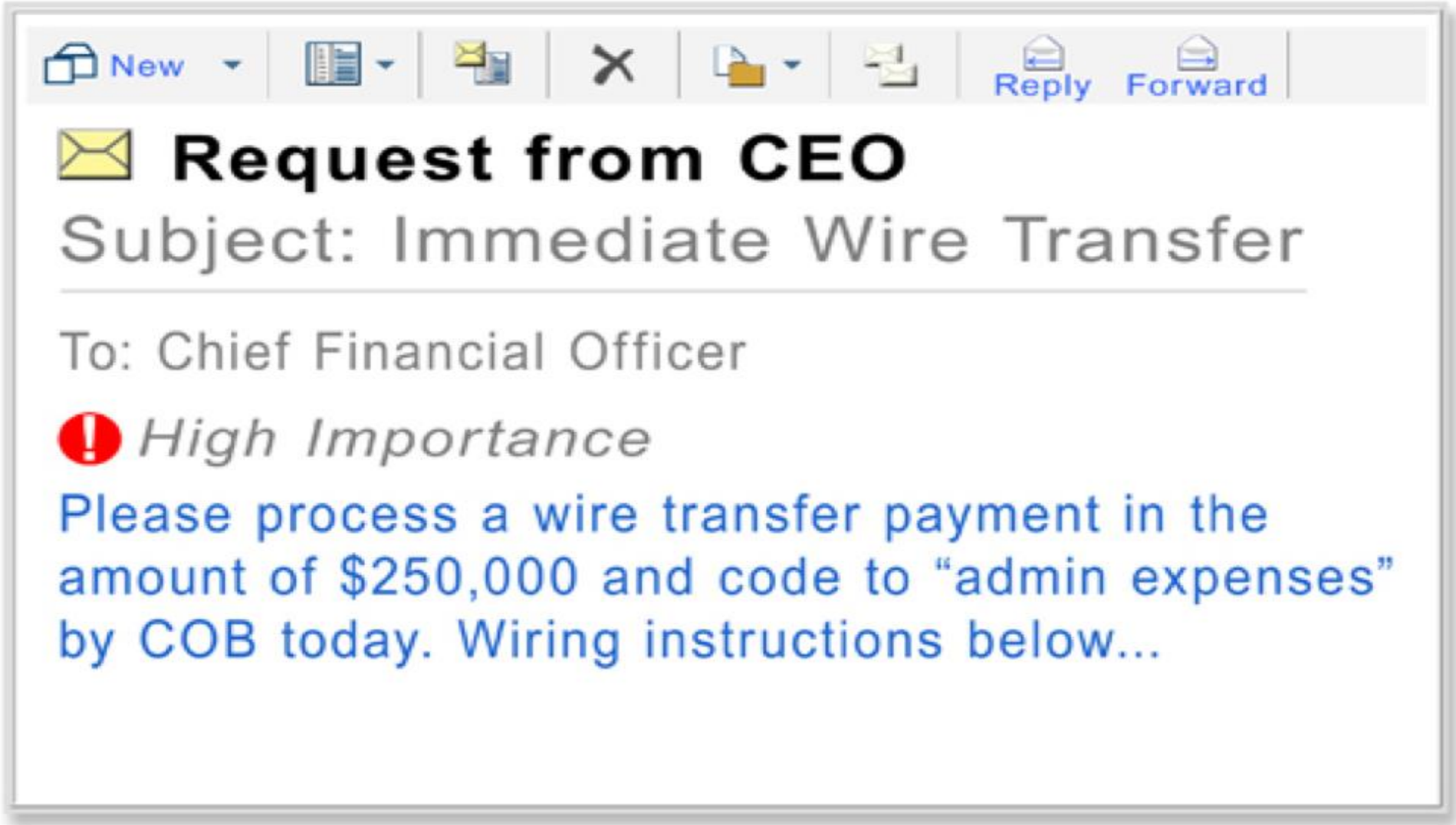
- Data breaches
  - Databases
    - Data monetization
      - Social Security numbers
      - Payment card data
    - Malicious use of legitimate sites
      - BotNet launching sites
      - Stolen records storage
  - Data theft
    - Digital
    - Paper
      - immediate impact
    - Mobile devices

Trends in data security

Trends

- Social engineering – largest attack vector
  - Email account compromises
    - User credential harvesting
    - Data monetization
    - Direct deposit redirect
    - Wire transfer redirect
  - W-2 image exploit
    - Easily preventable with “human dual factor authentication”
  - Wire transfer exploit
    - Easily preventable with “human dual factor authentication”

Phishing E-mails



Trends in data security

Trends

- Extortionate attacks
  - Ransomware
  - Threatened distributed denial of service (DDoS)
- Encryption attacks
  - Ransomware ruse
    - Cover evidence of compromise
  - Malicious encryption
    - Intent to maliciously damage

Ransomware


ALL YOUR FILES HAVE BEEN LOCKED!
This operating system and all of important data was locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Arcticle 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP adress was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! This computer is aimed to stop your illegal activity.
To unlock your files you have to pay the penalty!
You have only 96 hours to pay the penalty, otherwise you will be arrested!
You must pay the penalty through Bitcoin Wallet.
To pay the penalty and unlock your data, you should send the following code:
to our agent e-mails:
thematrixhasyou9643@yahoo.com or
cremreihanob1979@yandex.ru
You will recieve all necessary instructions!
HURRY UP OR YOU WILL BE ARRESTED!!!
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION

Regulatory environment

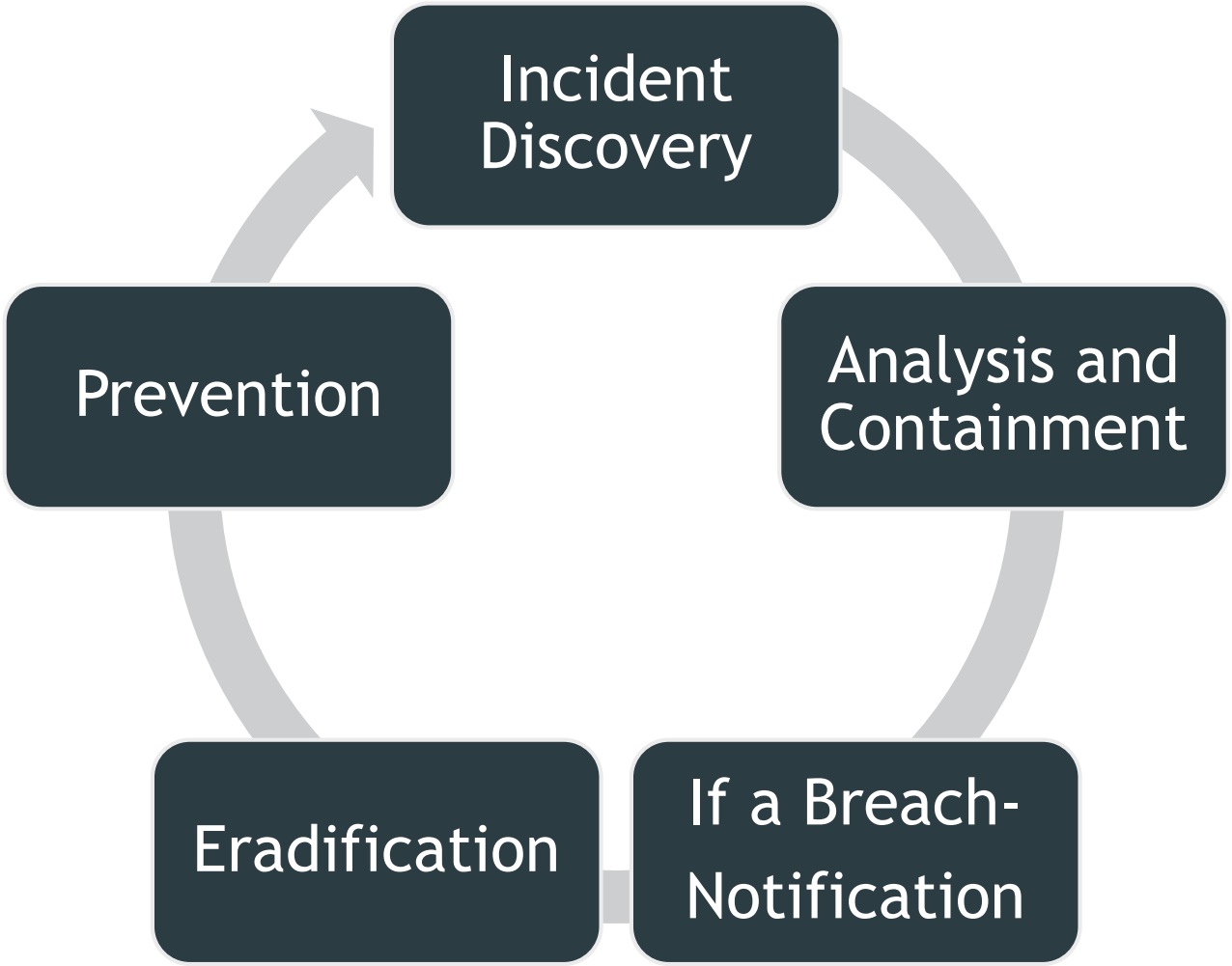
- State Regulations
  - **50 state data breach notification statutes** (plus Washington D.C., Guam, Puerto Rico, and the Virgin Islands) – All cover electronic, 10 also cover paper
  - **Require notification of consumers** regarding breaches of unencrypted personal information
    - 1 requires notification even of encrypted information
  - **Notification** obligation **determined by residential location of consumer**, not location of business
  - **Personal information** generally defined as first name or initial and last name, combined with one or more of the following data sets:
    - All state include SSN, DL or State ID Card Number, financial account with means to access the account; 8 add medical information; 5 add online credentials; 13 add other information, including health insurance, biometric, and taxpayer ID
  - **Timing of notification**: 40 require "most expedient time possible"
    - 7 also have outer time limit
  - **Notice content requirements**: 19 have specific notice content requirements
  - **Regulatory notification**: 25 require notification of state regulatory officials
- **Federal Regulations**
  - HIPAA – Privacy Rule, Security Rule, Breach Notification Rule; FTC Act; Securities Exchange Act, etc.

Financial Implications

- **First-party costs**:
  - Data loss; software loss; hardware loss;
  - Income loss; business interruption costs; restoration costs;
  - Cyber extortion; other crime loss.
- **Third-party costs:**
  - Media liability (copyright and trademark infringement); privacy liability for breach of privacy; bodily injury;
  - Defensive litigation: class actions; derivative actions; and regulatory actions.
- **Remediation costs**:
  - Legal services; forensics services; crisis management services; consumer and regulatory notification – The actual hard copy costs; call center services; credit monitoring and identity theft protection services.
- **Fines and penalties**:
  - Expenses of regulatory investigations; civil judgments; fines and penalties levied by regulatory authorities; and fines and penalties for payment card industry compliance violations.

Cyber Insurance

- Risk cannot be completely mitigated by technology
  - Cyber insurance can mitigate residual economic risk
- Critical component of incident response planning
- Coverage components
  - First party losses and costs
    - Business Interruption Loss
    - Extortion Demands
    - Breach Notification
  - Third party costs
  - Remediation costs
  - Fines and penalties
  - Risk management services
- Primary purposes: breach response expenses
  - Legal, forensics, consumer remediation, crisis communication



LEWIS BRISBOIS®

Incident Discovery

- Mobilize designated Incident Response Team
  - Includes outside experts
- Refer to scalable Incident Response Plan
- Notify insurer, involve Counsel + Forensics Experts

Analysis and Containment

- Conduct a thorough investigation
- Forensic analysis: examine each system impacted
- Determine incident scope
- Preserve everything
- Identify type of data involved
- Legal analysis – breach? What laws involved?
- Mitigate/remediate security compromise and data losses
- Reach out to Law Enforcement and Regulators, if appropriate
- Create an internal and external PR Plan (follow IRP)

NOTIFICATION

- Internal and external PR/communication strategy – must be clear, effective and carefully done (evidence)
- Timely notify all required individuals/entities
- Notification of individuals depends on applicable federal or state law based on type of data involved and residency of affected individual
- Notification to local, state/federal agencies – APS, AG, HHS, Media
- Notification of other Entities/CE
- Set up phone banks, credit monitoring
- Devise escalation tree for questions, per IRP

Eradication/Containment

- IT forensic team identify the breach source
- Perform a full system audit to identify vulnerabilities
- Remedy them
- Address Sub-Contractor Issues

Prevention

Case Studies

- An Encryption Attack
  - How it occurred
  - What it affected
  - Lessons learned
- An Email Compromise
  - How it occurred
  - What it affected
  - Lessons learned

LEWIS BRISBOIS®

Questions?

Simone McCormick:

Simone.McCormick@lewisbrisbois.com

971.712.2800