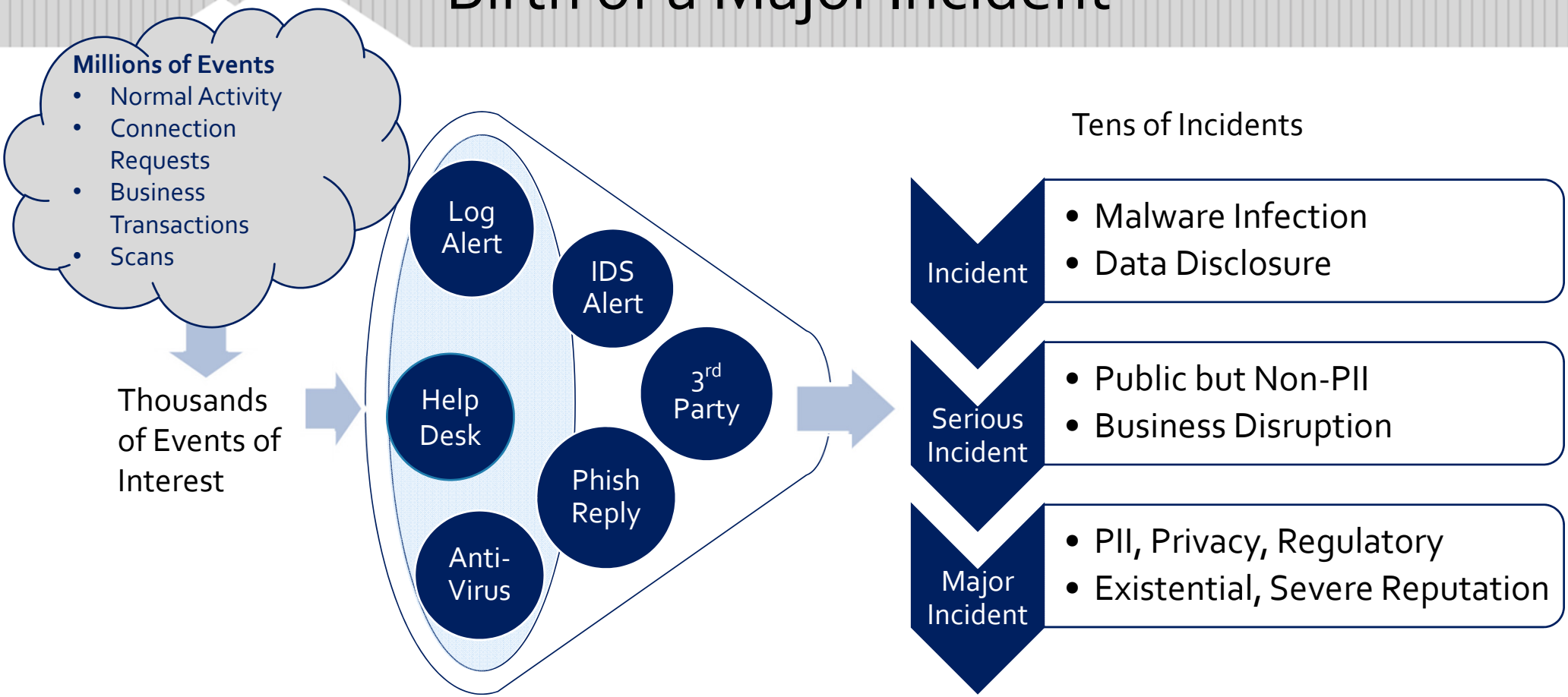
Post-Breach Response

Incident Handling and Data Breach Communications

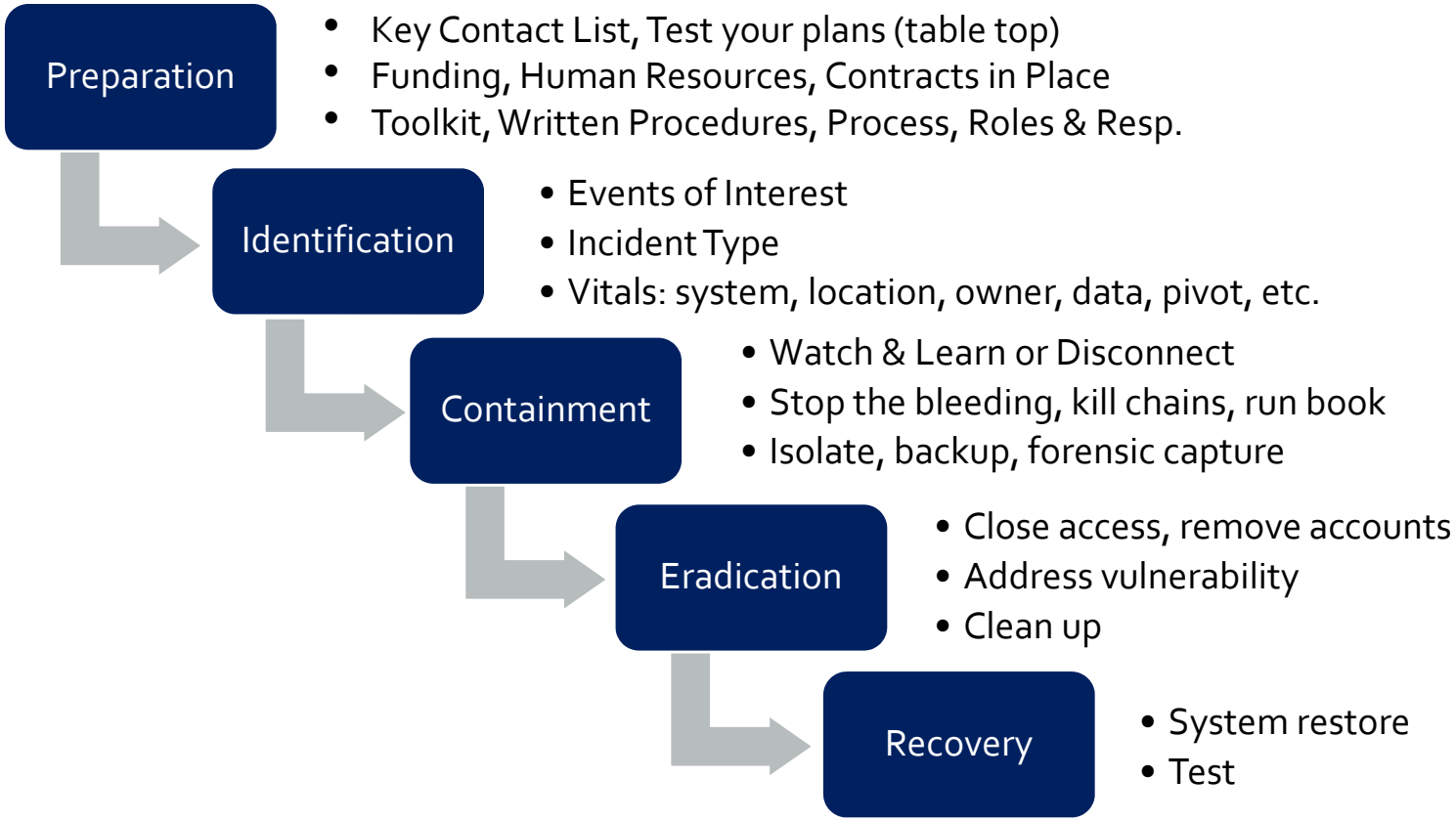
The material contained herein represents the personal opinions of the presenter and are offered for educational purposes only. In all cases of suspected or actual data breach the advise of competent legal counsel should be sought. All attempts have been made to cite original sources.

HOLLAND&HART LLP

Birth of a Major Incident



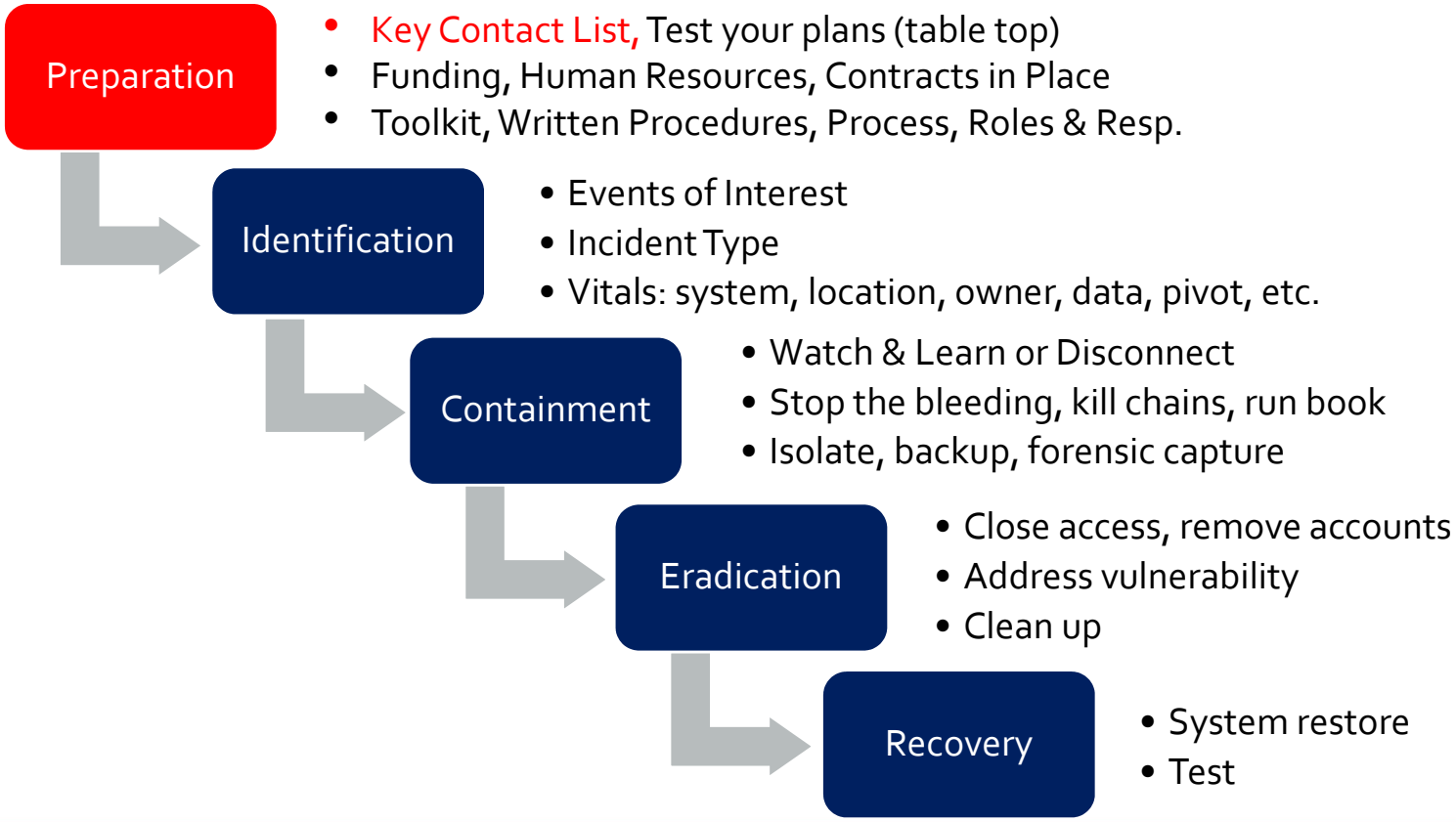
Incident Handling Lifecycle



https://www.sans.org/score/incident-forms/

https://www.sans.org/media/score/checklists/APT-IncidentHandling-Checklist.pdf

Incident Handling Lifecycle



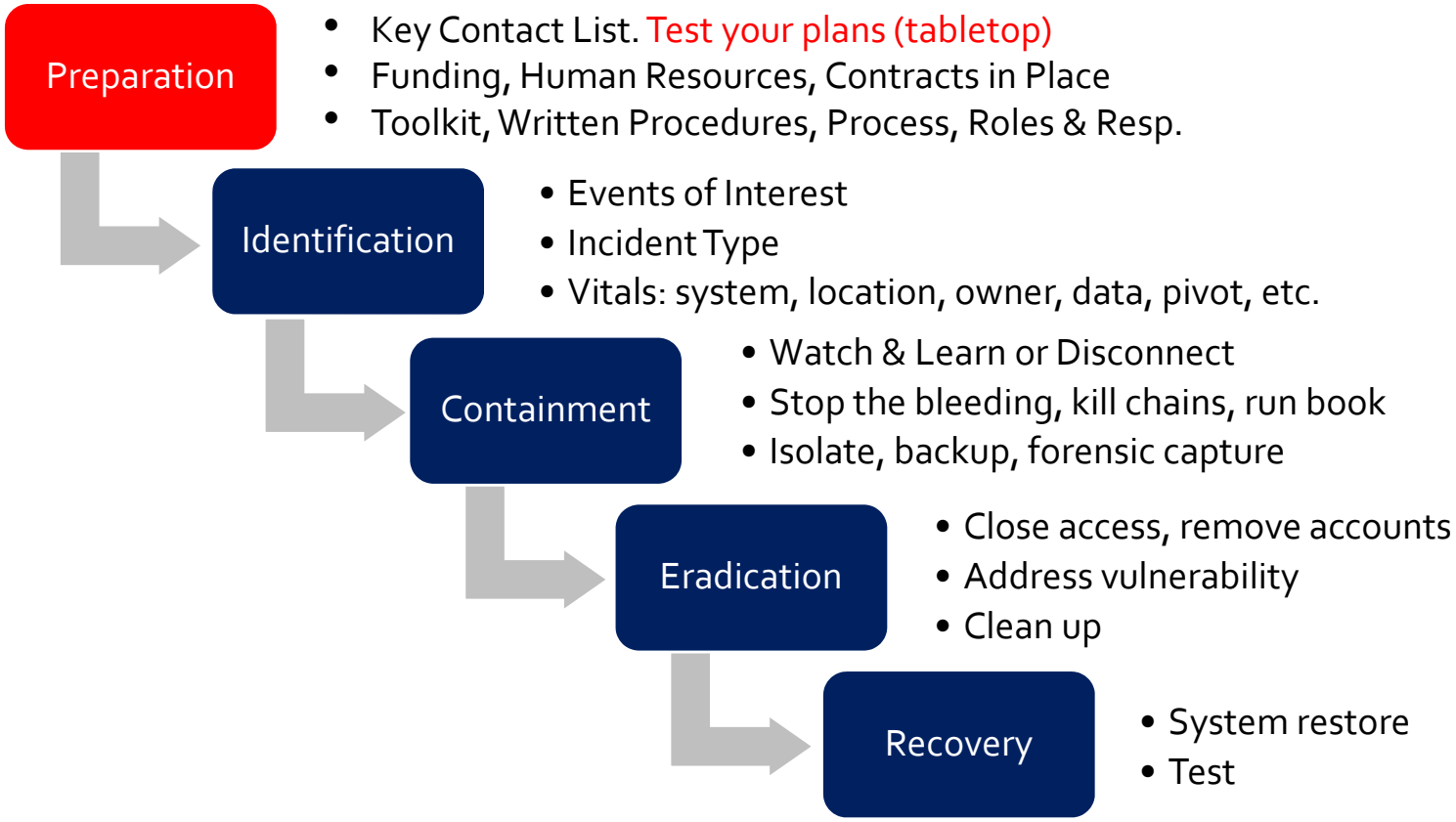
Key Contact List

- Corporate Security Officer or CISO
- CIRT, CSIRT, Incident Handling Team (in house or contract)
- Corporate Legal Officer
- Outside Data Security or Privacy Counsel
- Insurance Agent
- Privacy Officer
- CIO or Systems Manager
- Public Affairs/Corp. Comm.
- ISP Technical Contact
- Local FBI Field Office
- Local Law Enforcement Computer Crime
- Key Vendor Contacts (Software, Infrastructure, Data Center)
- Optional:
  - Local Computer Forensics Contractor (funded, contracted)
  - Malware Reverse Engineering Contractor (funded, contracted)

Key Contact List (cont.)

- Regulators
- Bulk print and mail facility
- Crisis management firm, or public relations consultant
- List of third-parties who must be notified of any breach due to contractual requirements
- Pre-selected credit monitoring service provider

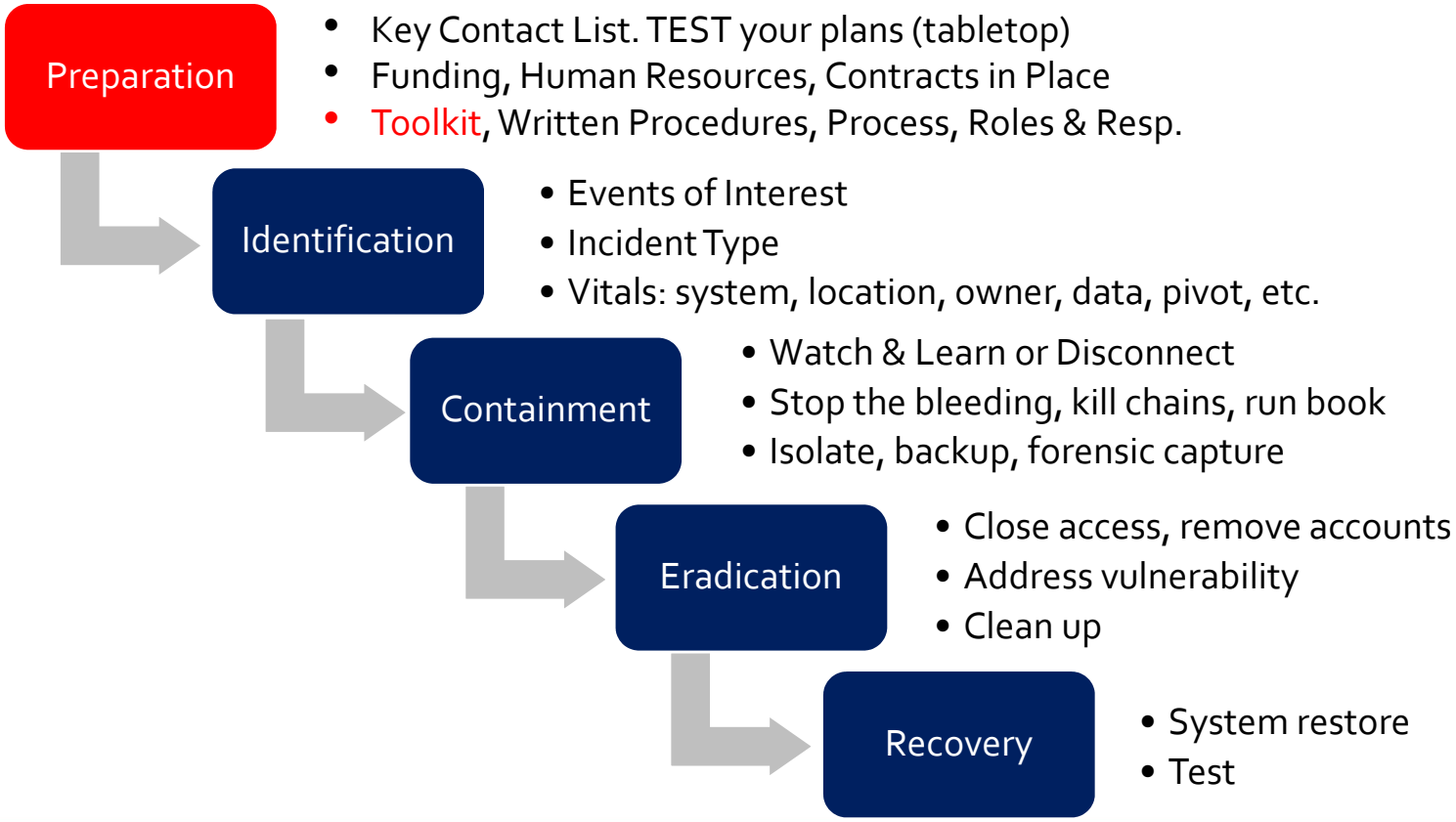
Incident Handling Lifecycle



Tabletop Testing

- Advantages
  - Low cost
  - Real scenarios in non-disruptive format
  - Educational for participants
- Variants
  - Simulations
  - Blind study – some participants not in the know
  - Real Simulation: Red Team vs. Blue Team
- Disadvantages
  - Difficult to simulate real-time pressure and stress
  - Actual technical readiness difficult to ascertain

Incident Handling Lifecycle



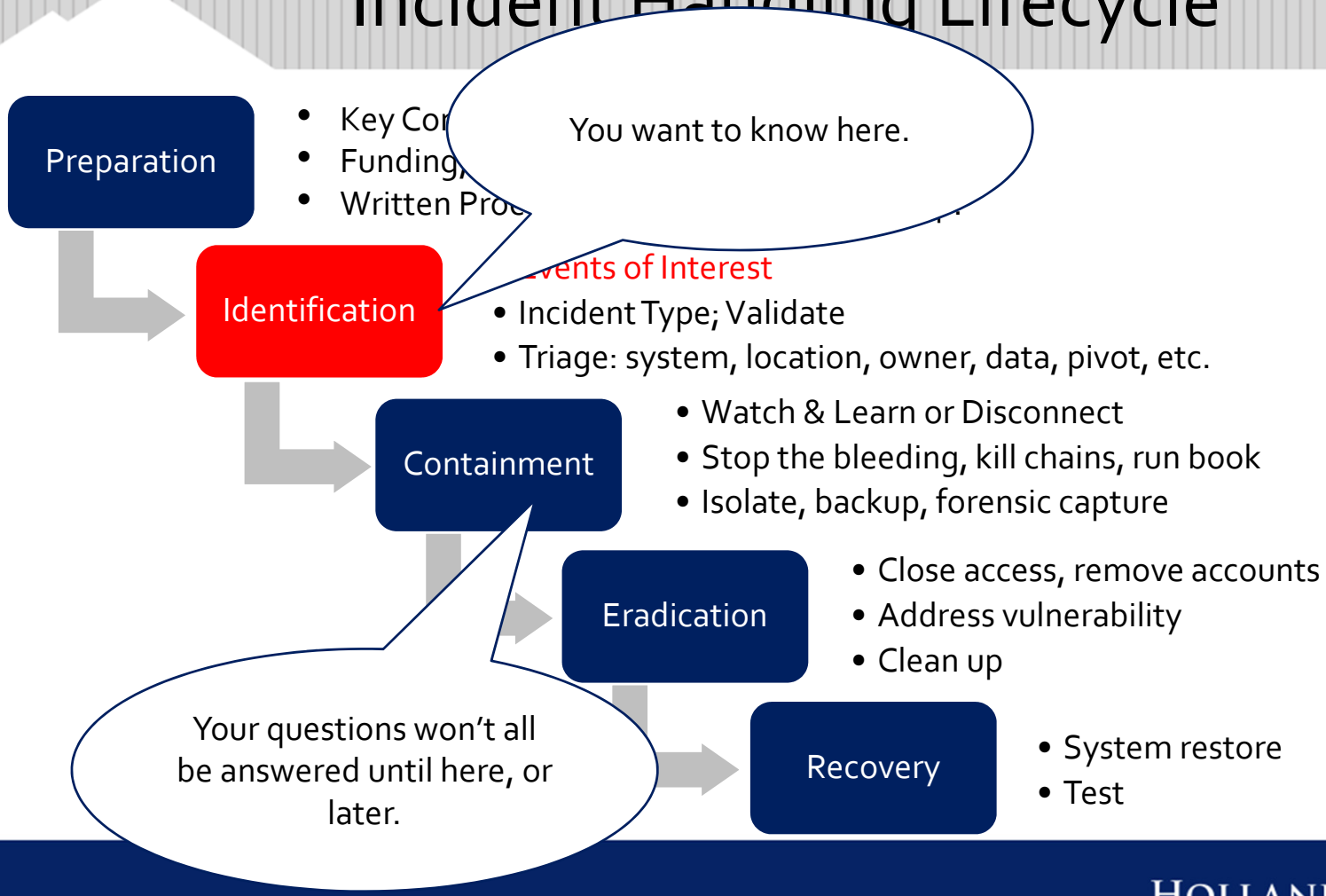
Data Breach Response Toolkit

- Incident Response Plan
- Response Team Roster, Contact Info
- Key Contact List
- Draft Notification Templates
  - Notification letters to affected individuals; by state, tailor to each state's unique requirements
  - Security incident notification for employees
- Depending on Size of Breach:
  - Draft letters to Experion, Equifax, Transunion
  - Draft letters to State AG or other government authorities as required
- Review and update templates frequently as state laws are constantly changing

Victim Notification Letters

- Many states have different requirements for content, notification period, procedure, hotline for questions
- Tone of letter: conciliatory, respectful, focused
- Include contact information, special twitter feed, or website for continuous updates

Incident Handling Lifecycle



Events of Interest (Identification)

- Remote Access Trojan (RAT)
- Command and Control (C+C)
- Encrypted Communications discovered
- Covert Channel discovered
- Host based IDS/ IPS alert of unexpected system call, data access, port open
- Direct External Notification (Law Enforcement, Business Partner)
- Indirect External Notification (Open Source Intelligence of behavior, search in your environment)
- Data Discovered Outside Of Organization (pastebin, news)
- Blackmail offer, Ransomware, Server disk suddenly full

Internal Communications (Identification)

- Upon Identification:
  - Validate suspected incident first!
  - Incident classification determines stakeholders
  - Don't raise false alarms
  - Categorize Severity & Impact (per policy)
    - Minor
    - Serious
    - Major
- Upon Identification
  - CIRT Lead
- Upon Validation
  - CISO, IT Director
  - System Owner
  - Affected Business Line

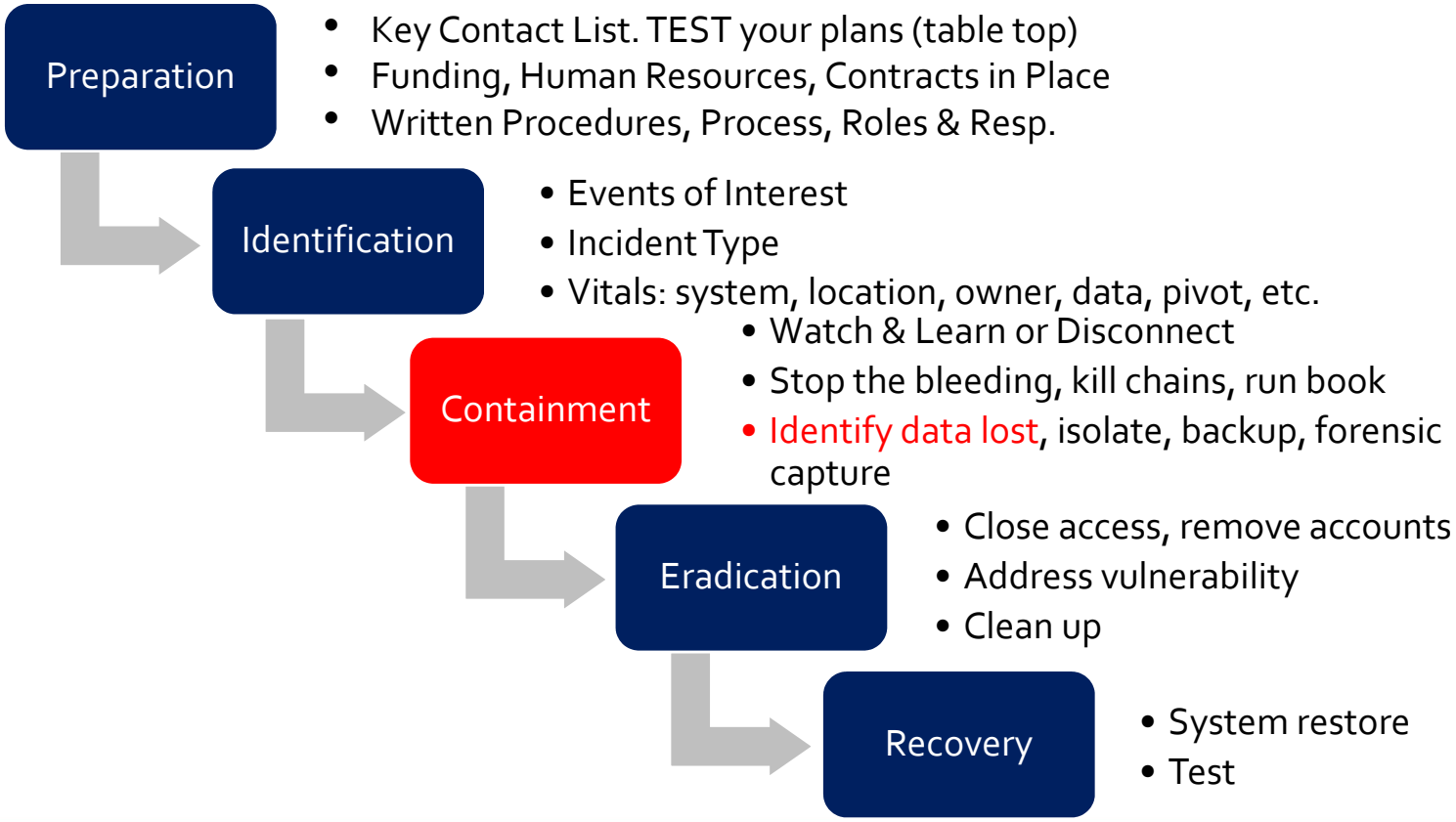
Internal Communications

- Upon Validation Expand Internal Communications
- Establish formal communication channel early and update often through Containment phase
- Serious Incident
  - Legal
  - Privacy
- Major Incident
  - Executive/Board
  - Public Affairs
  - May wait for Containment (much more information)

Incident Triage

- What systems are involved?
- What data is at risk?
- What are the physical locations?
- Where on the network?
- Who are the business owners of the systems and data?
- What possible pivots?

Incident Handling Lifecycle



Identify What Has Been Lost (Contain.)

- Update NIDS/HIDS to search
- Full packet capture
- Break encrypted channels
- Host-based forensics
- Identify legal ramifications
  - International (PII, data sovereignty)
  - PCI
  - HIPAA
  - GLBA
  - SEC
  - Contractual Notifications
  - State Breach Notification
- Determine scope of notification:
  - Victims
  - Domestic and foreign regulators
  - Business partners
  - Contractual third parties
  - Public/Press

Containment (cont.)

- Decide whether to isolate, remove from network
- Decide who needs to be contacted on Key Contacts List
- Decide if/when to go public, if not legally required to do so
- Timing is important: not too soon, not too late

Containment (cont.)

- Know reasonably well before going public:
  - Incident is not ongoing
  - Type of incident
  - Size of breach
  - Medium of data: hard copy, electronic or both?
  - Location, jurisdictions and controlling law
  - Timing of incident:
    - First discovered
    - Internal communications
  - Data affected, elements compromised

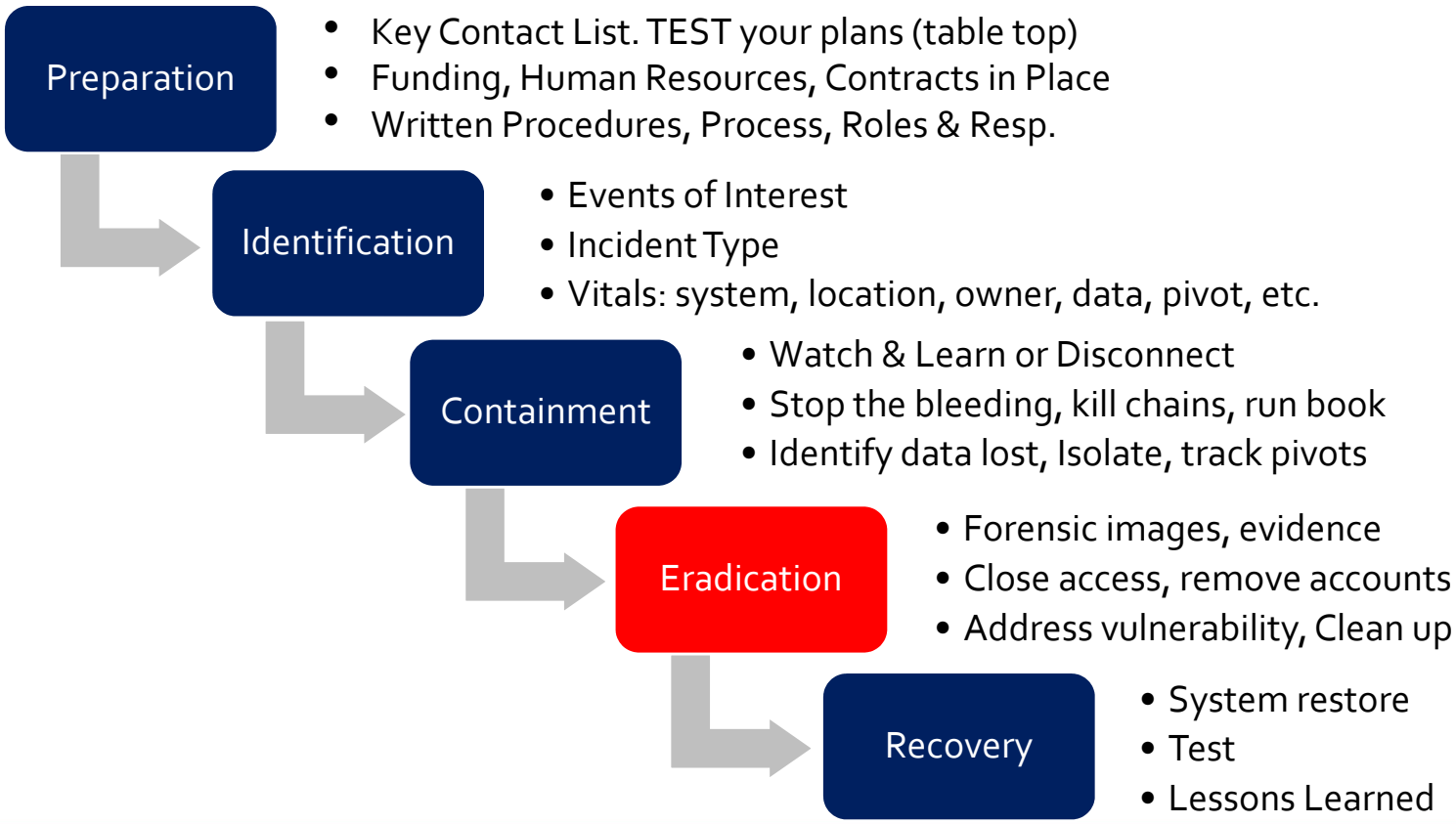
Notification (Containment)

- Do not go public prematurely
- Maintain an expedient internal investigation, do not delay
- Facts are needed, they come as investigation progresses
- Multiple notifications as facts arrive are viewed suspiciously, convey sense of uncertainty, frustration among victims
- However, all delays must be justified

Public Notification (Containment)

- Establish a call center
- Notify all at once, not in waves driven by statutory time limits
- Use consistent language to describe the nature of the incident and the affected data, across all external communications to the public, regulators, international entities
- Communicate internally to employees
- Some employees may also be customers, consistent messaging, proximate in time
- Instruct employee to refer inquiries to designated spokesperson/group

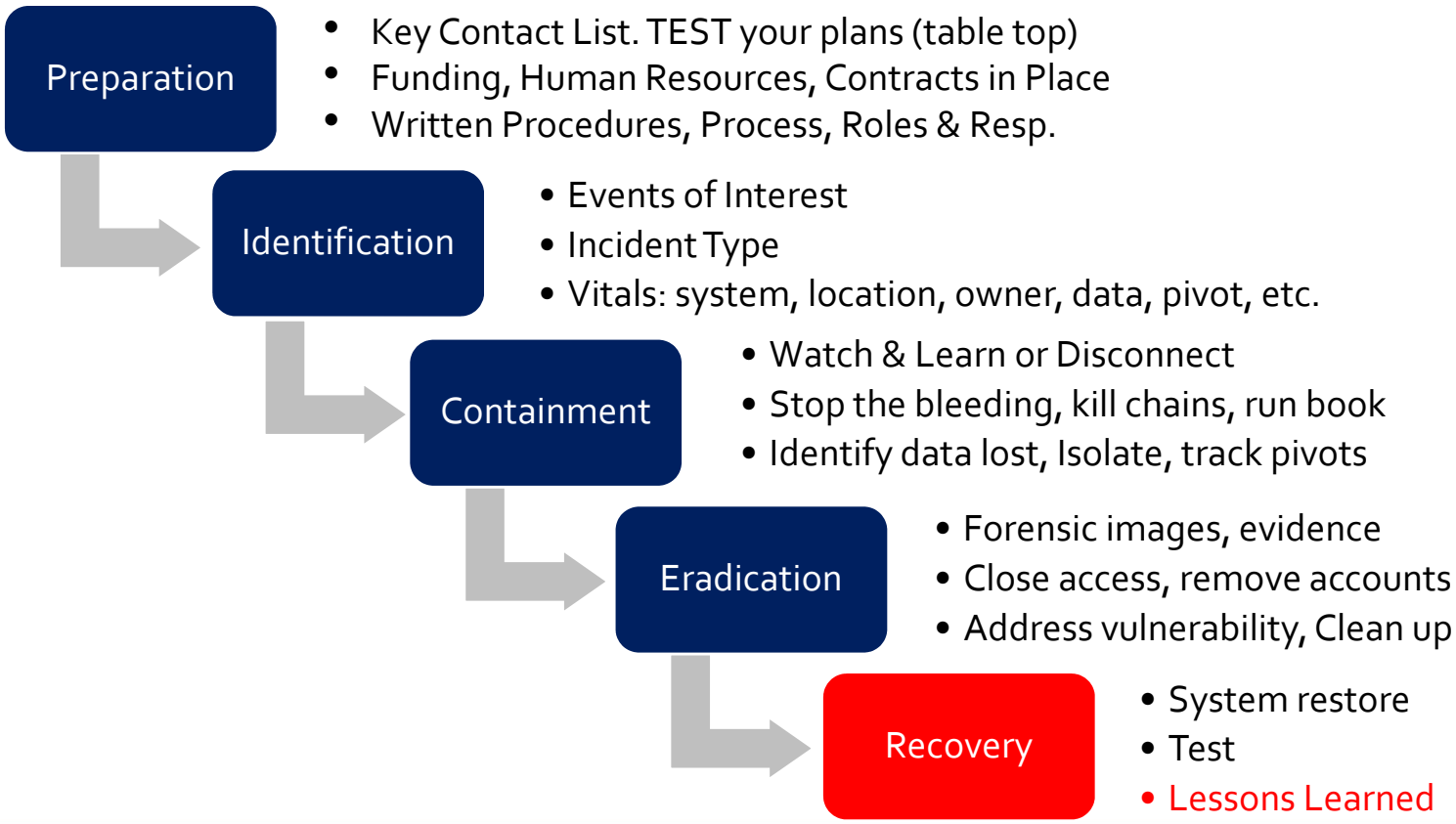
Incident Handling Lifecycle



Eradication

- Capture evidence of wrong doing
- Forensically image impacted disk drives, replace with clean installs
- Maintain chain of custody on all drives and forensic images
- Use working copies for analysis while preserving original drives
- Advanced attacks are only discovered in RAM, do not write to drive
- Close all outbound data exfiltration channels
- Close and patch all vulnerabilities

Incident Handling Lifecycle



Post-Mortem

- Executive
  - Is this a cost of doing business?
  - Is this a case for meaningful change?
  - Avoid blame, use incident to improve capability
  - Explain details by analogy
- Technical
  - Learn from tactics used against you
  - Address vulnerabilities with 20 Critical Controls
  - Make a solid business case for information security investment
  - Translate security goals into business goals

Recent Updates to State Breach Notification

- Rhode Island: requires implementation of risk-based information security program
- Connecticut: requires one year of identify theft protection to victims
- Wyoming: requires the establishment of a toll-free contact number
- Nevada, Oregon: expands types of data covered by notice requirements
- Maryland: requires AG notification prior to consumer notice

- "While attempting to work on analyzing what . . . happened you always have your senior executive and/or clients hanging over your shoulder constantly bugging you for more details. The containment plan needs to be worked out, someone needs to liaise with Legal/HR/PR, management wants an update, the technical staff need direction or assistance, teams need to be coordinated, everyone wants to be in the loop, lots of yelling is going on, external IRTs want to know why your network is attacking theirs, nobody can locate the backups, keeping track of activities, taking notes, and the list goes on… No wonder people regularly burn out during incidents! Incident handling is obviously not a solo sport."

Source: Adrien de Beaupre, https://isc.sans.edu/forums/diary/Incident+Response+vs+Incident+Handling/6205

Summary

- Principle: Know Before You Go
  - Create a Model Process (Stakeholders, Communications)
  - Contract now with service providers
  - Stay on top of changes in Data Breach Notification Laws
  - Know your regulator; FTC Enforcement Actions
  - Draft all templates now
  - Tabletop test your plan

Action Plan

- **When you get back to your office**
  - Inquire about your incident response plan, review it
  - Call a stakeholder meeting to plan improvements to breach readiness
- **In the first 30 days**
  - Update incident response plan
  - Update key contacts
  - Initiate review of data breach notification requirements (state, federal, intl., contract)
- **By 90 days**
  - Draft all templates
  - Identify and source external service providers
  - Finalize roles & responsibilities
- **End of year**
  - Complete table top exercise
  - Complete post-mortem on all incidents
  - Improve security program to prevent incidents (CSF and 20CC)

Thank You

- Questions?

Matt Sorensen

Holland & Hart

cmsorensen@hollandhart.com