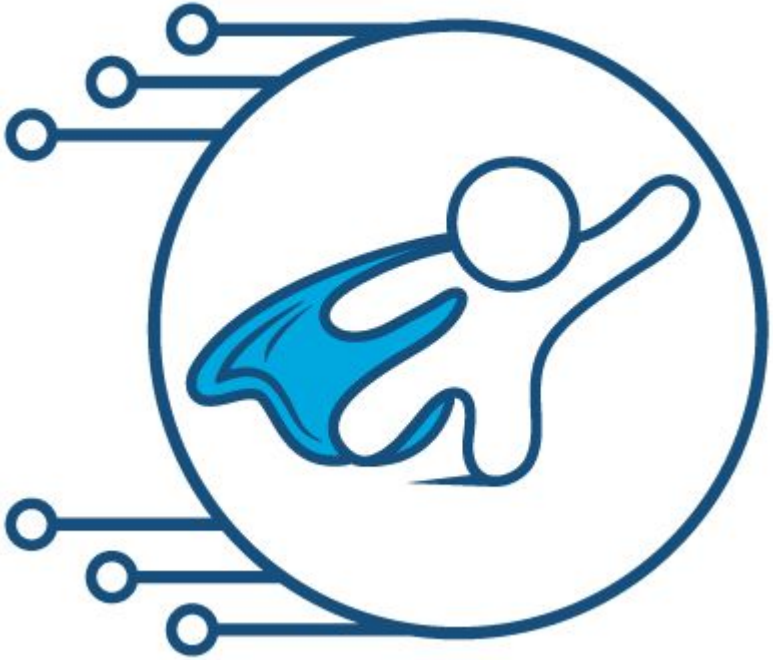
PXL DIGITAL

Blue Teams



INFOSEC WHEEL

@aprilwright
@proxyblue

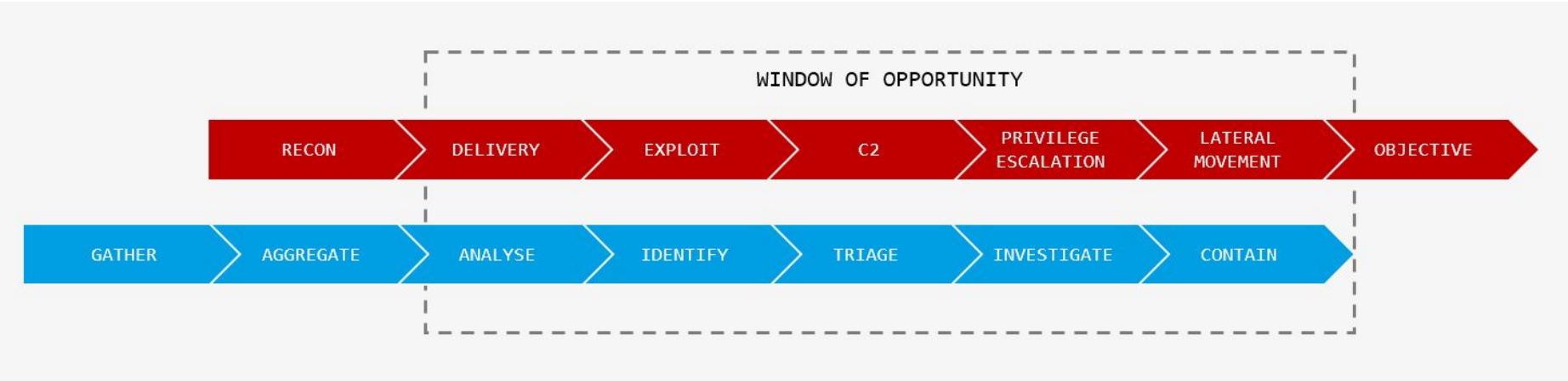
PXL DIGITAL

BLUE TEAM

- Defensive Security
- Infrastructure protection
- Damage Control
- Incident Response(IR)
- Operational Security
- Threat Hunters
- Digital Forensics

PXL DIGITAL

Blue team Incident workflow



The 5 phases in the incident response plan

1. Preparation
2. Detection & Analysis
3. Containment, Eradication, Recovery
4. Post-Incident Review
5. Update the plan !

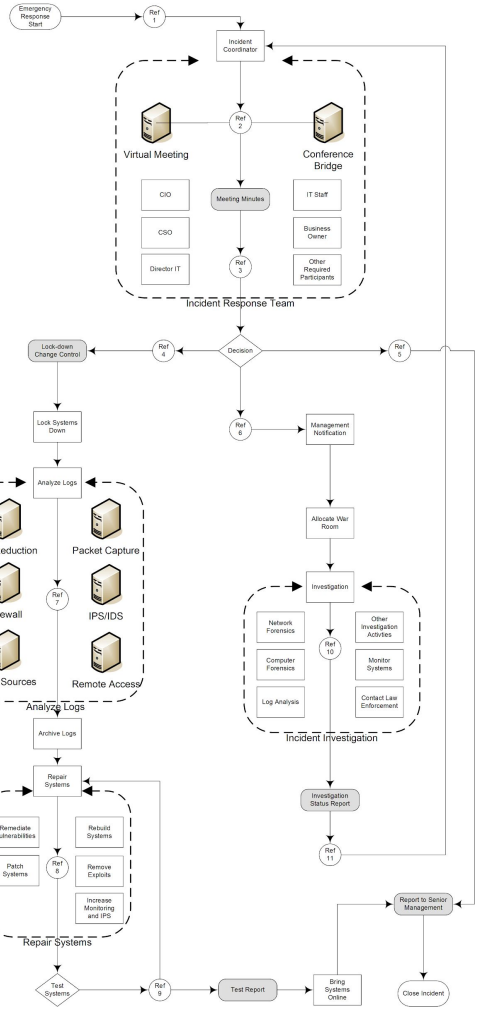
Phase 3: Containment, Eradication & Recovery

Protect the Present

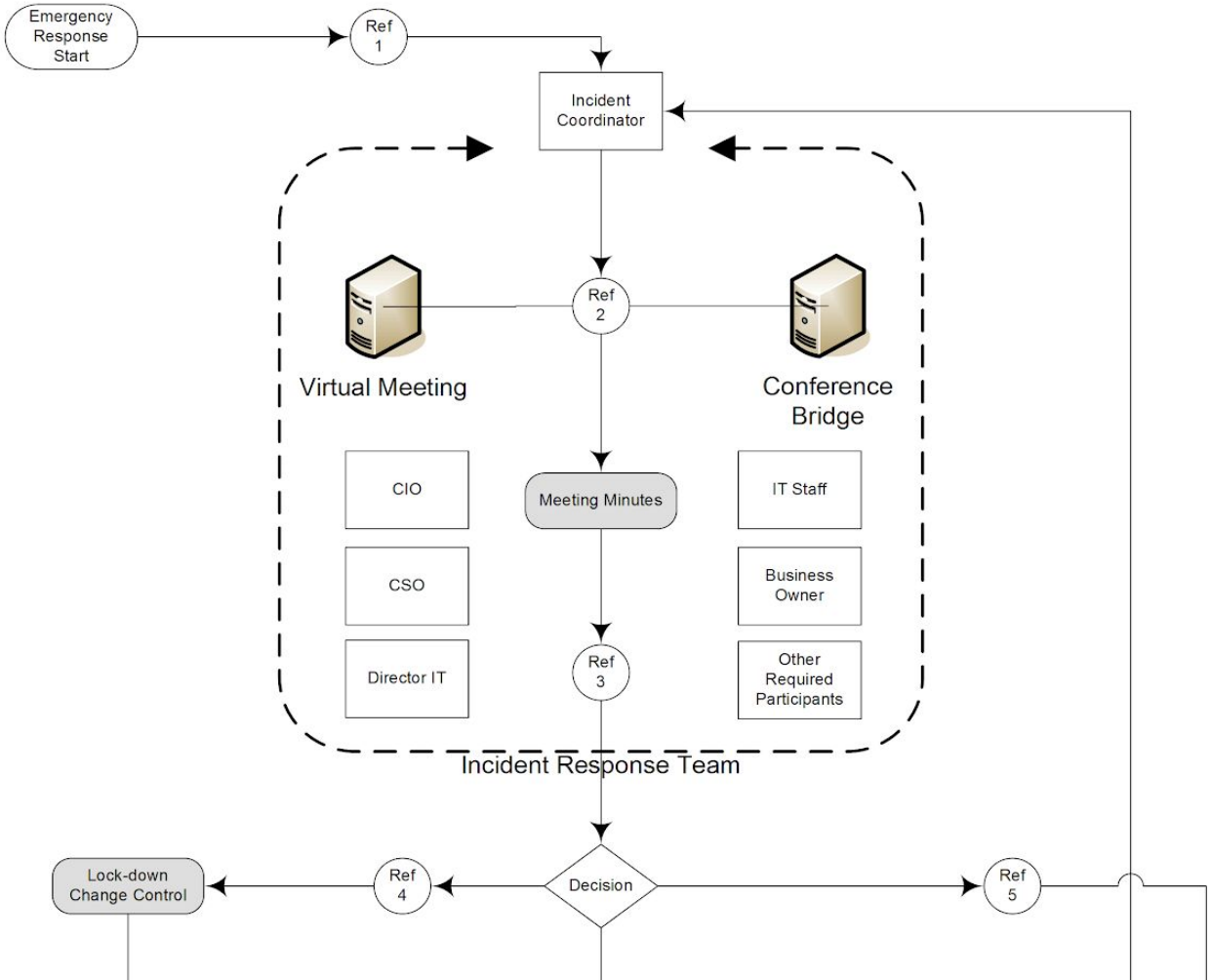
- Lock down systems
- Analyze logs
- Archive logs
- Repair/Rebuild systems
- Test Systems
- (repeat if needed)

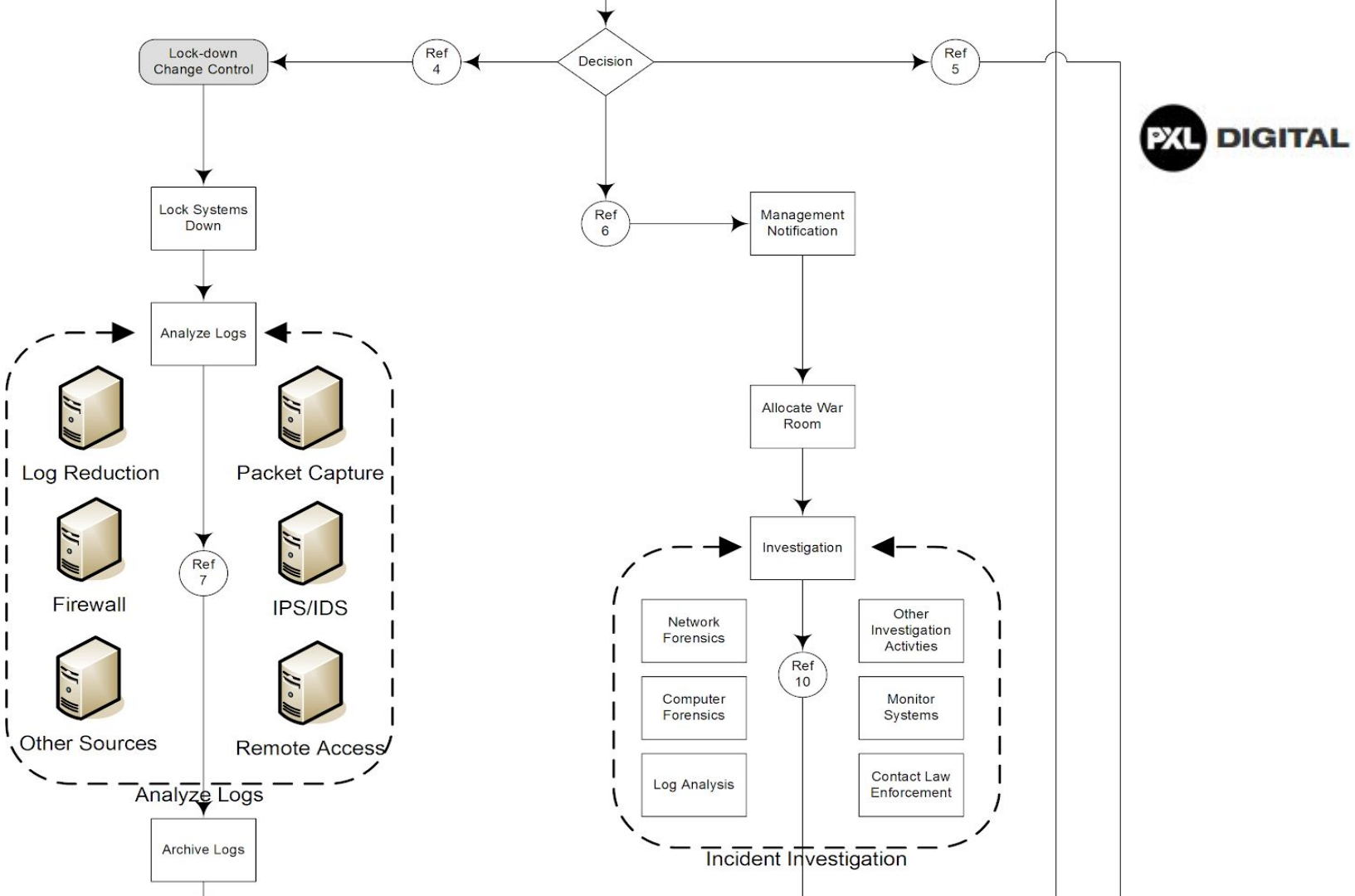
Recovered

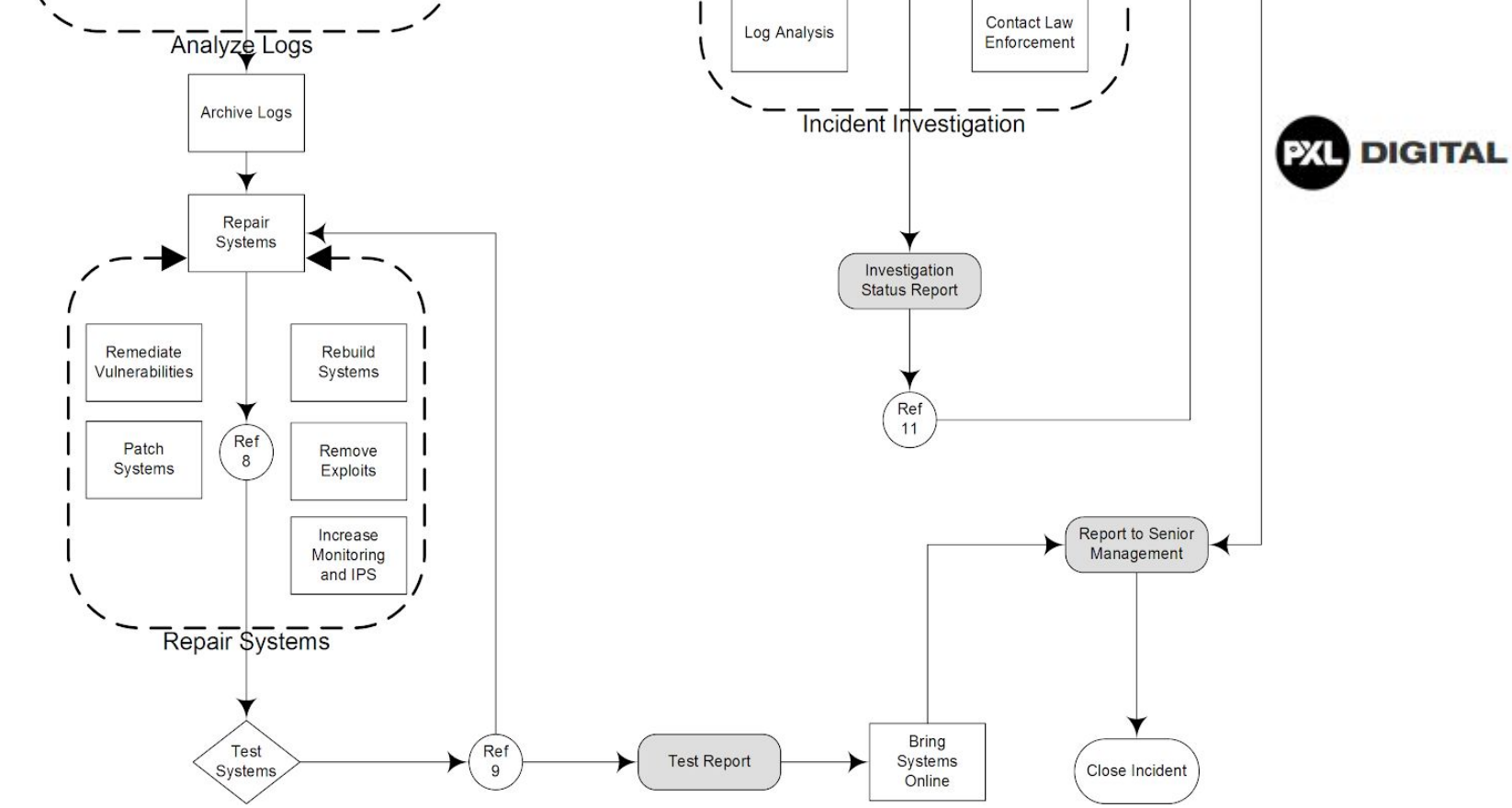
Emergency response detail



Emergency response detail




Lock-down Change Control
Ref 4
Decision
Ref 5
Lock Systems Down
Ref 6
Management Notification
Analyze Logs
Allocate War Room
Log Reduction
Packet Capture
Investigation
Ref 7
Firewall
IPS/IDS
Network Forensics
Other Investigation Activties
Ref 10
Computer Forensics
Monitor Systems
Other Sources
Remote Access
Log Analysis
Contact Law Enforcement
Analyze Logs
Incident Investigation
Archive Logs


Analyze Logs
Archive Logs
Repair Systems
Remediate Vulnerabilities
Patch Systems
Ref 8
Rebuild Systems
Remove Exploits
Increase Monitoring and IPS
Repair Systems
Test Systems
Ref 9
Test Report
Bring Systems Online
Log Analysis
Contact Law Enforcement
Incident Investigation
Investigation Status Report
Ref 11
Report to Senior Management
Close Incident
PXL DIGITAL

Phase 3: Containment, Eradication & Recovery

- Protect the future
  - Incident Investigation

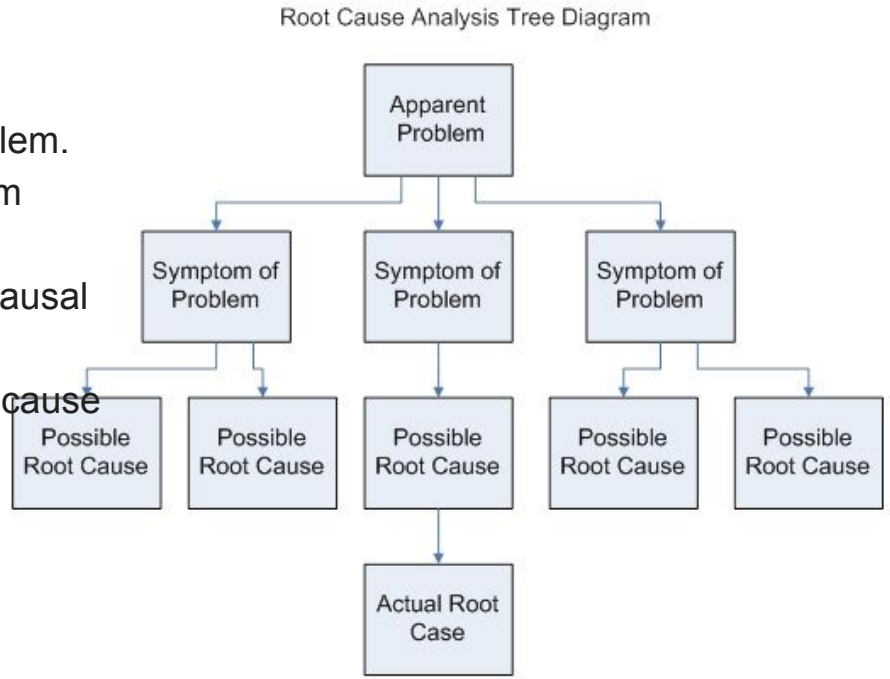
Get the facts!

- Network forensics
- Computer forensics
- Log analysis

Phase 3: Containment, Eradication & Recovery

- Protect the future
  - Root Cause Analysis

- **Identify** and describe clearly the fault/problem.
- Establish a **timeline** (history of events) from normal situation until the fault/problem.
- **Distinguish** between the root cause and causal factors (e.g., using event correlation).
- Establish a causal graph between the root cause and the fault/problem.



Phase 4 & 5: Post-Incident Review & update plan

Investigation status report

- Discusses by Incident Response Team
- When satisfied -> Send to management

- **When all is given the OK -> Incident closed**

Step 4 & 5: Post-Incident Review & update plan

- **Step 4 & 5 Post-Incident Review and update plan**
  - After-Action Meeting

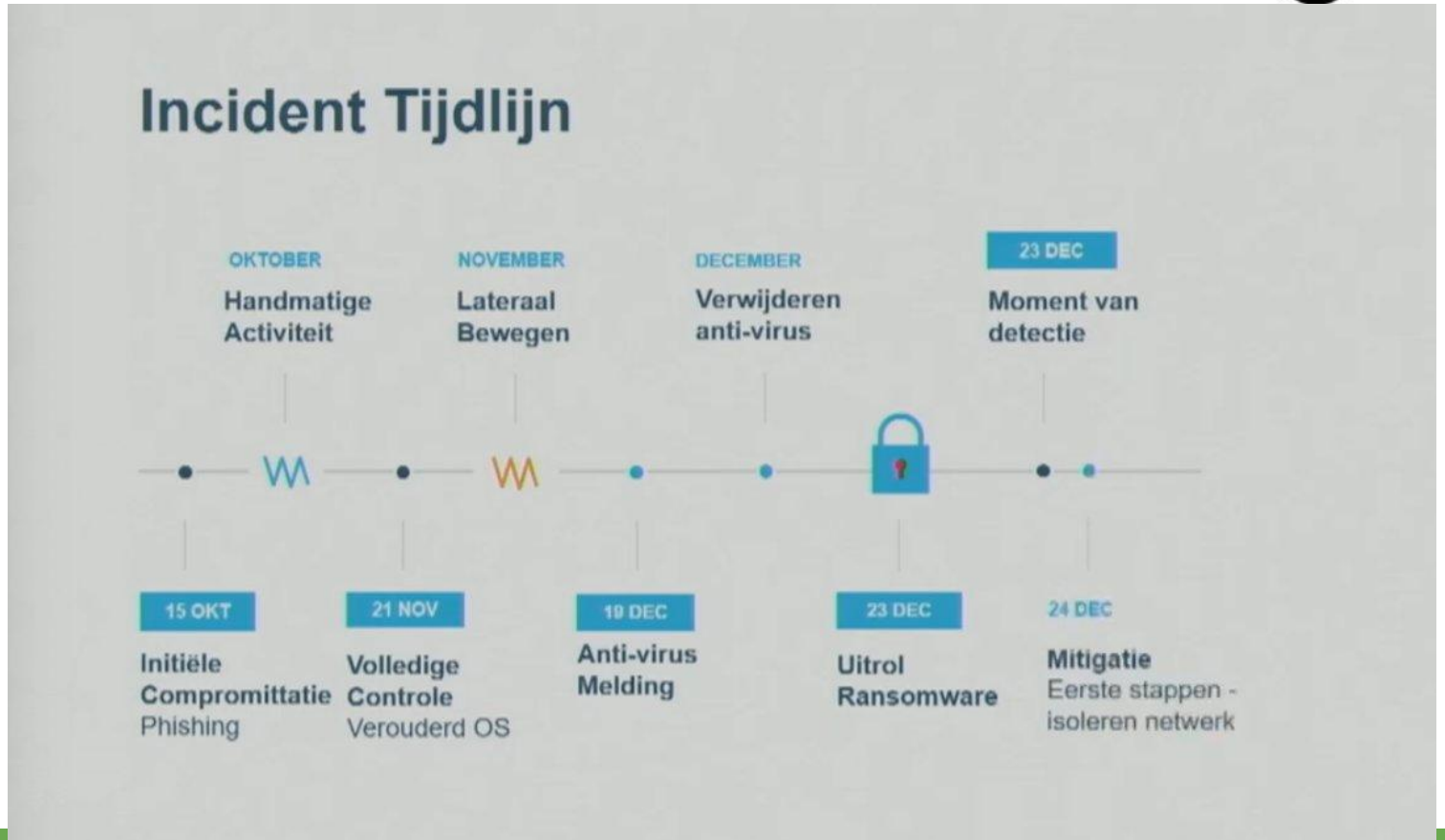
Hold an after-action meeting with all Incident Response Team members and discuss what you've learned from the data breach.

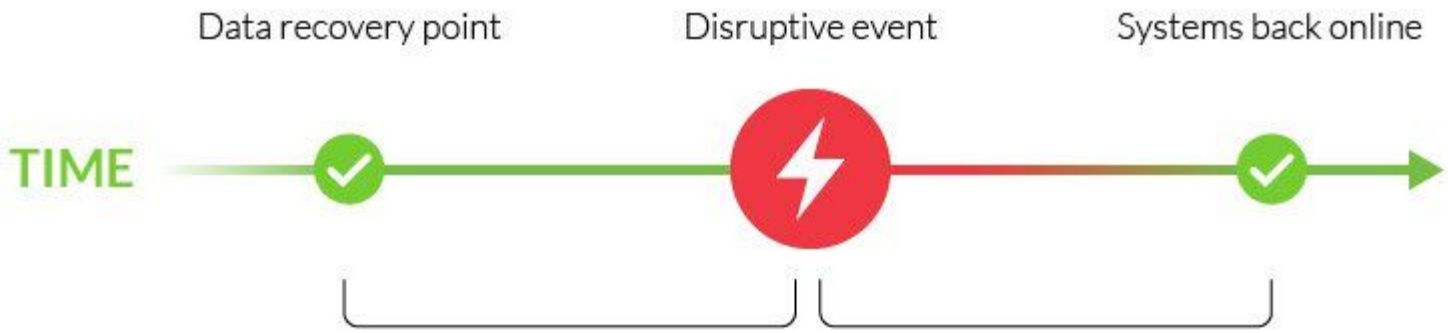
Determine what worked well in your response plan, and where there were some holes.

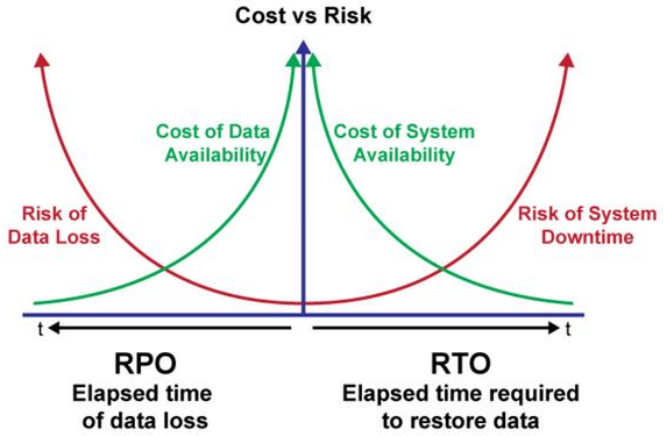
Questions to ask:

- What changes need to be made to the security?
- How should employee be trained differently?
- What weakness did the breach exploit?
- How will you ensure a similar breach doesn't happen again

Incident Response - example




Data recovery point
Disruptive event
Systems back online
TIME
Data restoration
Recovery Point Objective
(RPO)
Max. time to recover
Recovery Time Objective
(RTO)


Cost vs Risk
Cost of Data Availability
Cost of System Availability
Risk of Data Loss
Risk of System Downtime
t
t
RPO
Elapsed time of data loss
RTO
Elapsed time required to restore data

DATA BREACH INCIDENT RESPONSE PLAN TOOLKIT

LAWYERS MUTUAL LIABILITY INSURANCE COMPANY OF NORTH CAROLINA

RISK MANAGEMENT PRACTICE GUIDE OF LAWYERS MUTUAL

PXL DIGITAL

An **INCIDENT RESPONSE PLAN** aims to reduce the exposures to an organization, customers/employees, and partners that arise out of a data theft or data loss incident.

An **INCIDENT RESPONSE PLAN** specifically includes policies and procedures to:

- Assess the nature and scope of an incident, and identify what customer information systems and types of customer/employee information have been accessed or misused
- Contain and control the incident to prevent further unauthorized access to, or misuse of, customer information, while preserving records and other evidence
- Notify appropriate law enforcement agency
- Maintain or Restore Business Continuity
- Notify customers/employees when warranted

COMPONENTS of an INCIDENT RESPONSE PLAN

1. Incident Response Team
2. Incident Response Contact Sheet
3. Suspecting or Detecting an Incident
4. Incident Response Discovery Form
5. Incident Assessment and Analysis
6. Data Breach Incident Response Flow Chart
7. Notification
8. Customer/Employee Notice Content
9. Customer/Employee Notification Letter
10. Additional Policies and Procedures

DOWNLOAD THE *DATA BREACH INCIDENT RESPONSE PLAN* TOOLKIT

DATA BREACH INCIDENT RESPONSE PLAN TOOLKIT

LAWYERS MUTUAL | LIABILITY INSURANCE COMPANY OF NORTH CAROLINA

RISK MANAGEMENT PRACTICE GUIDE OF LAWYERS MUTUAL

An **INCIDENT RESPONSE PLAN** aims to reduce the exposures to an organization, customers/employees, and partners that arise out of a data theft or data loss incident.

An **INCIDENT RESPONSE PLAN** specifically includes policies and procedures to:

- Assess the nature and scope of an incident, and identify what customer information systems and types of customer/employee information have been accessed or misused
- Contain and control the incident to prevent further unauthorized access to, or misuse of, customer information, while preserving records and other evidence
- Notify appropriate law enforcement agency
- Maintain or Restore Business Continuity
- Notify customers/employees when warranted

1. **Incident Response Team**
2. **Incident Response Contact Sheet**

DOWNLOAD THE *DATA BREACH INCIDENT RESPONSE PLAN* TOOLKIT


PURPLESEC

Infrastructure Security

Vulnerability Scanning

Infrastructure Security

CWE & CVE & CVSS

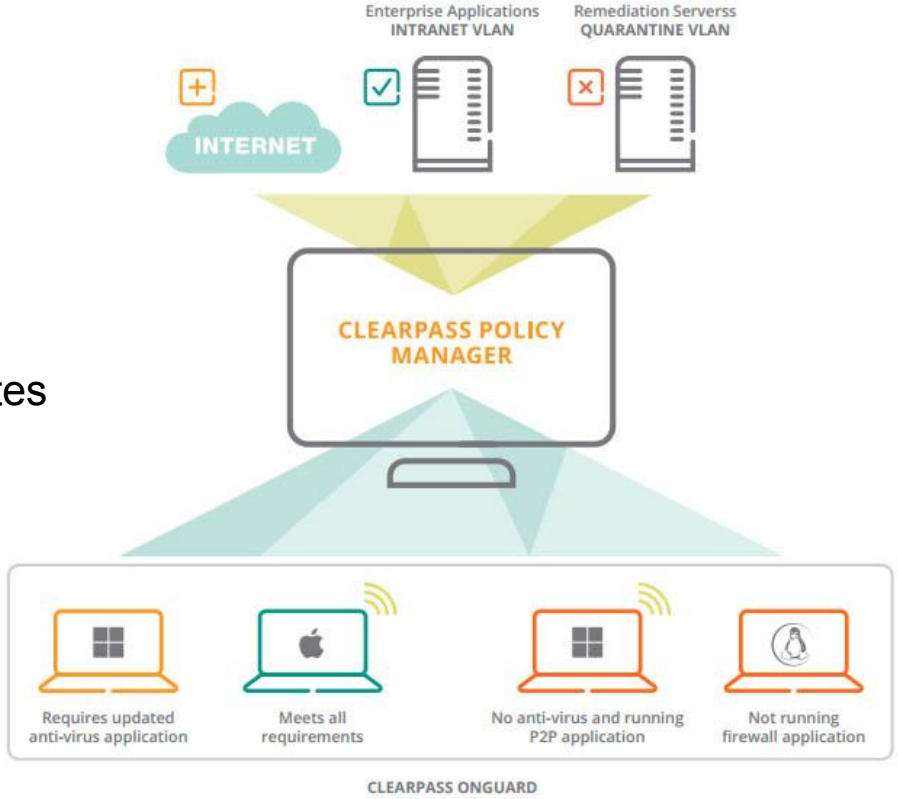
Phase 2: Detection

NAC

Network Admission Control (NAC)

Common NAC systems checks include:

1. Updated virus detection
2. Operating systems patches and updates
3. Complex password enforcement



Pluralsight video’s

PLURALSIGHT

PXL DIGITAL

Pluralsight video: link
Relevant : Digital Forensics: The Big Picture

Pluralsight video: link
Relevant : Digital Forensics: Getting Started with File Systems

Pluralsight video: link
Relevant : Getting Started with Memory Forensics Using Volatility

Pluralsight video: link
Relevant : Network Security Monitoring (NSM) with Security Onion