

Death Taxes and a Computer Incident: Designing your Incident Response Plan

Thomas Sammel, CISSP, GCFE

Director, Incident Response
& Digital Forensics

SecureWorks





The Entity: State Level University Enterprise

The Event

- A security team for a State University system detected a large file transfer leaving the University network
- Further investigation discovered a Query Server that was “unintentionally” internet facing for two years
- This Query Server had the ability to pull data from every SQL database in the University system



Response

- Consultant was put on the ground within 24 hours
- Recreated the query run by the malicious actor
- Discovered that 298K plus PII records exported in the malicious query
- Determined that log retention not adequate to conduct data loss assessment
- Recommended that the University make notification as required assuming the loss of 298K PII records



Agenda

- Gathering Threats
- Framework for Defense
- Cost of a Breach
- Common Pitfalls
- Incident Response Work Flow
- Building Your Plan
- Exercising Your Plan
- Models to consider
- Case Study

Gathering Threats



Threat Categories

May be some overlap in APT and Insider threat detection



- Phishing with Dynamite
- Automated control for scale
- Can be defended with good Signature based controls
- Buys trade craft
- Can be sophisticated and polymorphic
- Favorite vectors
 - ✓ Server compromises
 - ✓ Non-targeted phishing
 - ✓ Web drive bys
- Smash and grab

- Playing chess
- Human controlled (just for you)
- Custom trade craft
- Favorite vectors
 - ✓ Highly targeted phishing
 - ✓ Water holing web drive bys
 - ✓ Some server compromises
- Highly targeted efforts
- Attempts to cover their tracks
- Will compromise partners to get to you
- **Goal is to log on, become an insider**

- Fly on the wall
- Hardest to detect, tries to hide in normal activity
- Usually has elevated privileges
- In most cases, assumes not being monitored
- Rarely uses tradecraft: when they do, normally crawlers
- Usually has access to data that does not pertain to their job, that is what they take
- Attempts to cover their tracks
- Managers/HR usually not surprised when insider is caught

Intent and Motive

Hacktivists/Revenge Cyber Warfare



- Disrupt
- Destroy
- Deny
- Revenge
- Embarrass
- Intimidate

Intellectual Property Theft



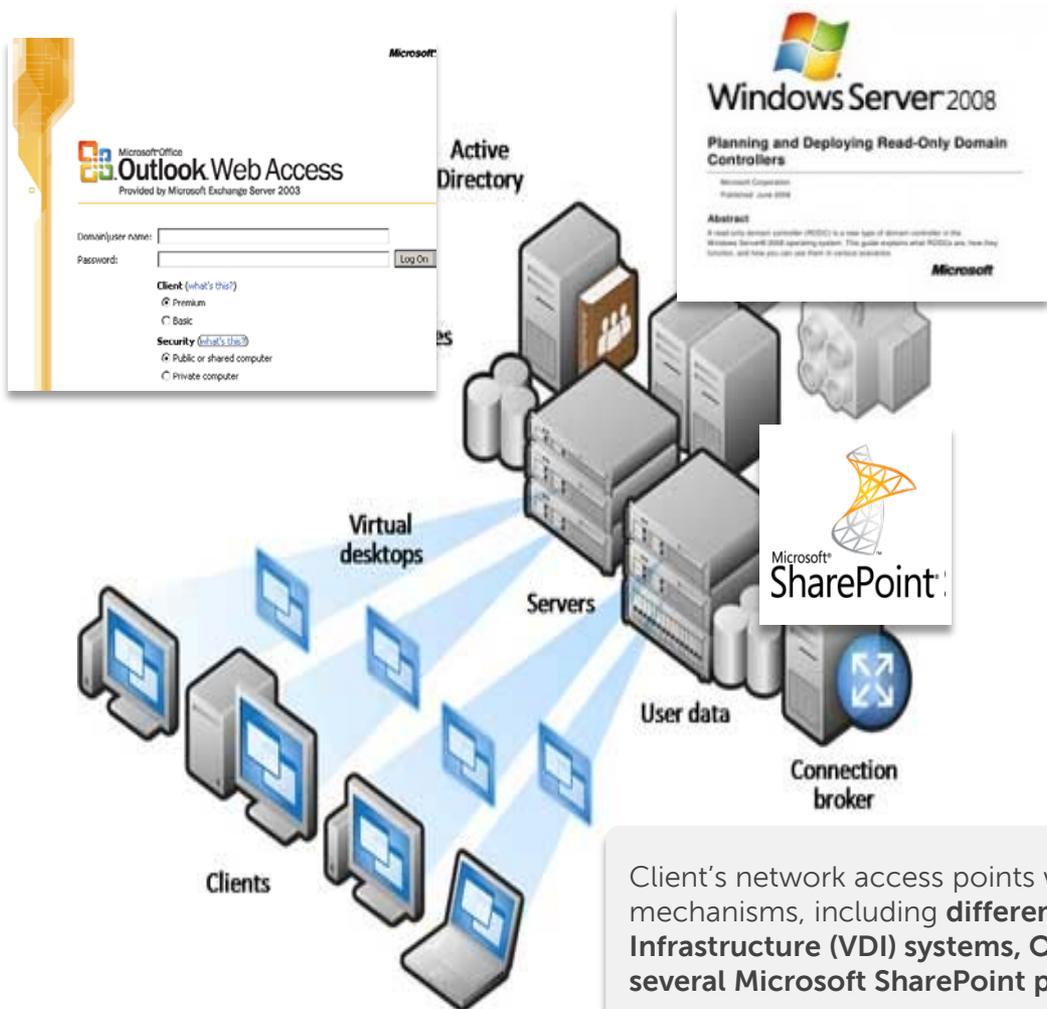
- Competitive advantage
- Fill in an innovation gap
- Nation-state level espionage

Crime



- Steal your Money
- Steal your clients money
- Identity Theft
- Fraud

Targeted threat wants to log on as you



- Compromised **numerous domain admin accounts**
- **Dozens of external IPs** from different network address blocks and geographic locations, associated with attacker
- Attackers **deleted their tools and recovered credentials after use.**
- Forensic review identified attacker presence **over 180 days**

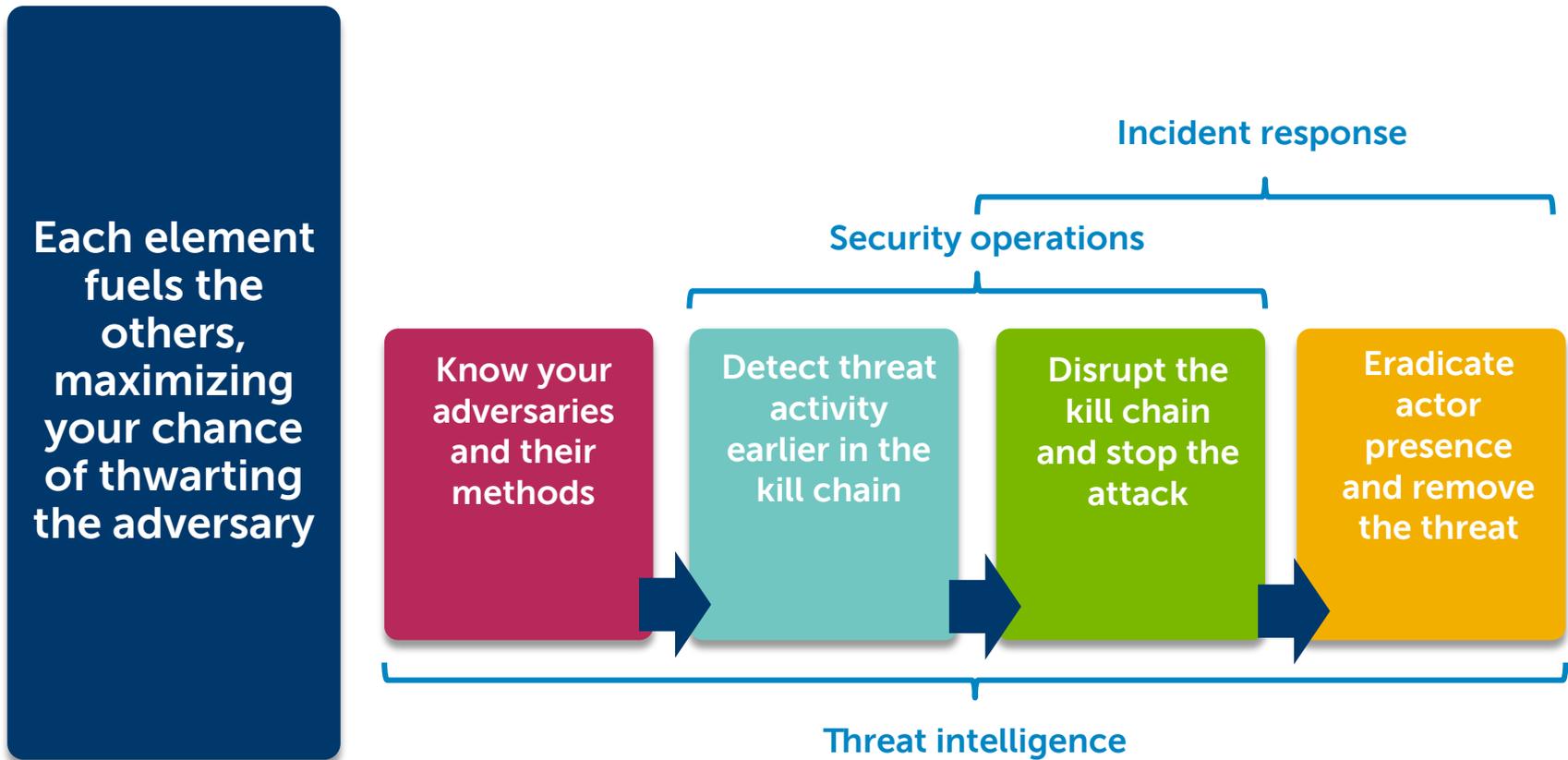
Client's network access points were distributed across multiple sites and access mechanisms, including **different VPN endpoints, Virtual Desktop Infrastructure (VDI) systems, Outlook Web Access (OWA) interface, and several Microsoft SharePoint portals.**

Framework for Defense



Your best defense

Successful defense against advanced threats requires integrated threat intelligence, security operations and incident response



Cost of a Breach



Average Cost of a Data Breach (2012)

- German companies had the most costly data breaches
 - \$188 and \$199 dollars per record respectively
- The highest cost breaches were deliberately malicious and criminal attacks
 - \$277 per record in the United States
- Average records breached per incident
 - 23,647
- Average cost of a breach (US)
 - >\$4.4M
- Average breach notification cost (US)
 - >\$500,000

Common Pitfalls



General observations

- Most struggle with an IT architecture designed for delivery, not security
- Poor asset visibility and network access control
- Security Operations Centers have SIEMS, but no analytics
- No Structured Approach for Security Incident Tracking
 - Difficult to spot trends and relevant threats sooner rather than later
 - No clear picture on detection and containment metrics
- Most focus on compliance monitoring instead of Security Monitoring
 - Implementation and process immaturity for security investigation use cases
- Most customers have an incident response plan
 - Few exercise it regularly, Many are outdated
- Most customers don't have forensics



Commodity Threat Observations

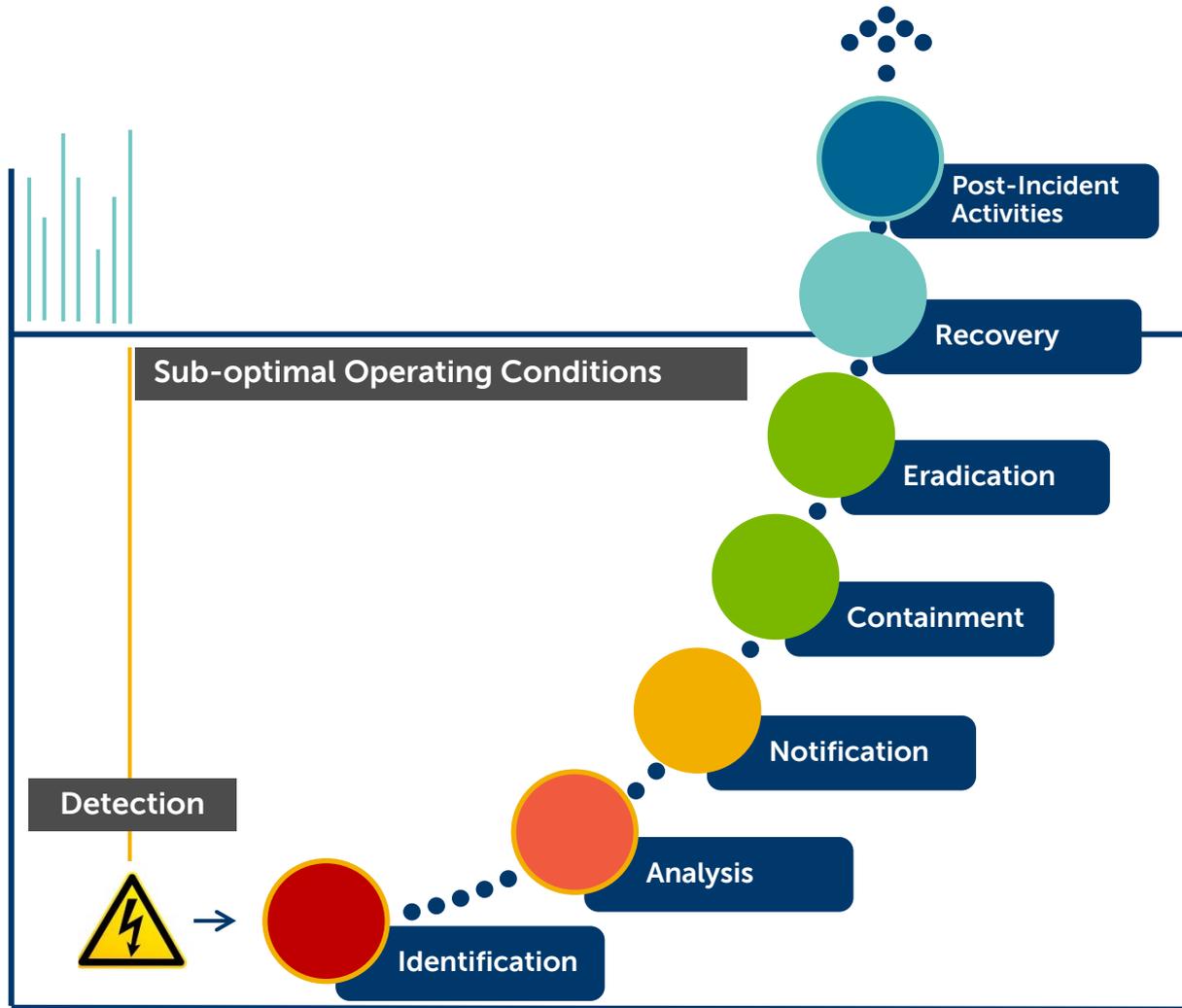
- Attackers leveraging vulnerabilities (zero-days/published) for exploit kits with advanced functionality and agile maintenance cycles
- Commodity/criminal threat actors are becoming more sophisticated
 - Drive-by attacks enumerating platforms and vulnerabilities
 - Polymorphic malware
- Key characteristics are an aggressive style of attack to compromise many victims as fast as possible for financial gain before exploit kit malware is removed



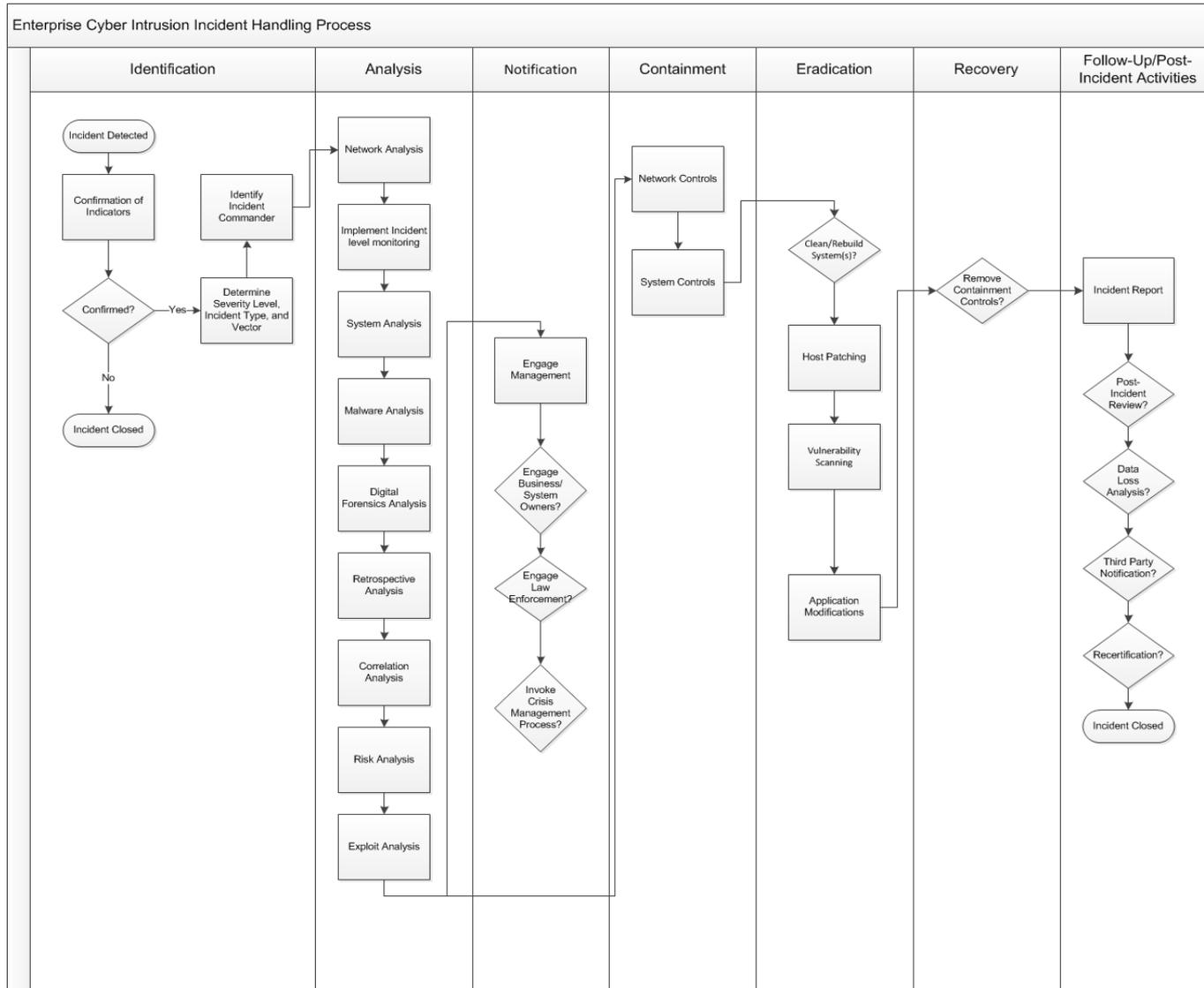
Incident Response Workflow



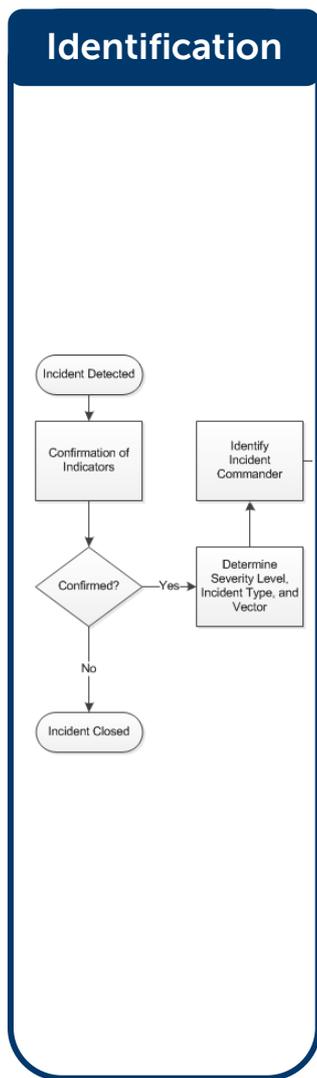
Incident Response Work Flow



Sample Workflow – IR Engagement



Phase: Identification



People and Skillsets

- Educated User – Detects and Report Anomalies
- Incident Analyst – Correlates Events
- Trained IT Staff – Corroborate Activities
- Incident Manager – Leads



Process

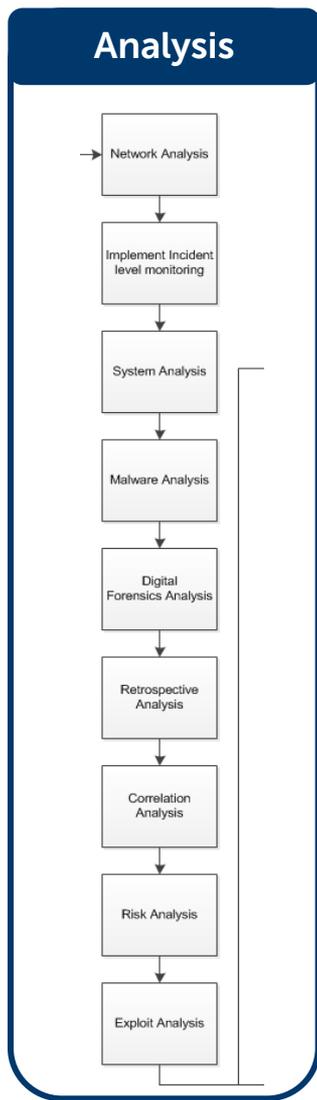
- Risk Analysis
- Incident Team Activation
- Artifact Preservation
- Escalations
- Notifications



Technology and Tools

- Well Configured Devices
- Logging Infrastructure
- SIEM
- Network Access to Required Information

Phase: Analysis



People and Skillsets

- Incident Analyst
- Incident Manager
- Network Forensics Analyst – Review Network Traffic
- Systems Forensics Analyst – Host Forensics
- Malware Analysts



Process

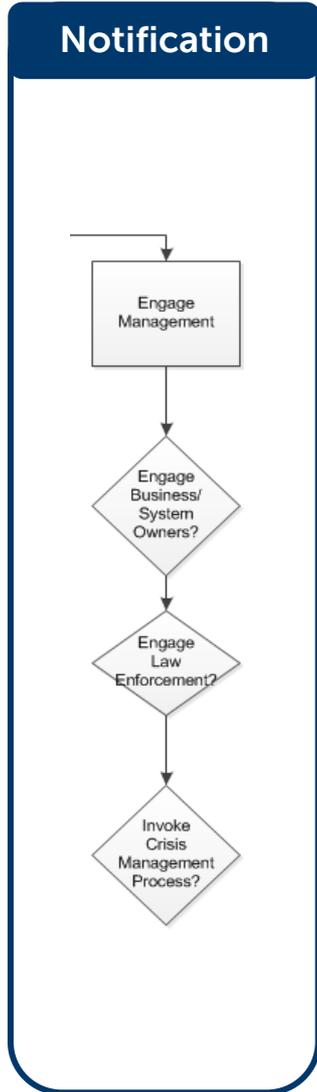
- Risk Analysis of Current Threat
 - Threat to Business Operations
 - Select Response Option
- Incident Response Playbook (Checklists)
- Artifact Collection, Storage, and Preservation
- Iterative



Technology and Tools

- System Forensics (FTK, EnCase)
- Log Parsing (Splunk, LogLogic)
- Intelligence Correlation (Palantir)
- Host/Network

Phase: Notification



People and Skillsets

- Incident Manager – Consolidate Technical Input
- CISO/CSO – Prepare Executive Recommendations
- Legal – Provide Risk Assessments
- Business Owners – Operational
- Corporate Communications – Messaging



Process

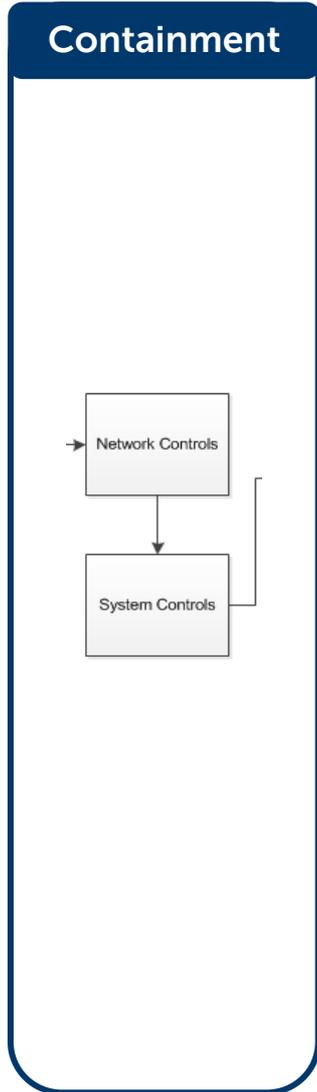
- Notifications
 - Internal Employees
 - Customers
 - Vendors
 - Law Enforcement
- Public Affairs Statement



Technology and Tools

- Pre-Prepared Notifications
- Method
 - E-Mail
 - SMS
 - Snail Mail

Phase: Containment



People and Skillsets

- CIO/CISO – Strategic Guidance
- Incident Manager – Develop Implementation Plan
- IT Staff – Knowledge of System Capabilities
- Security Staff – Internal Research



Process

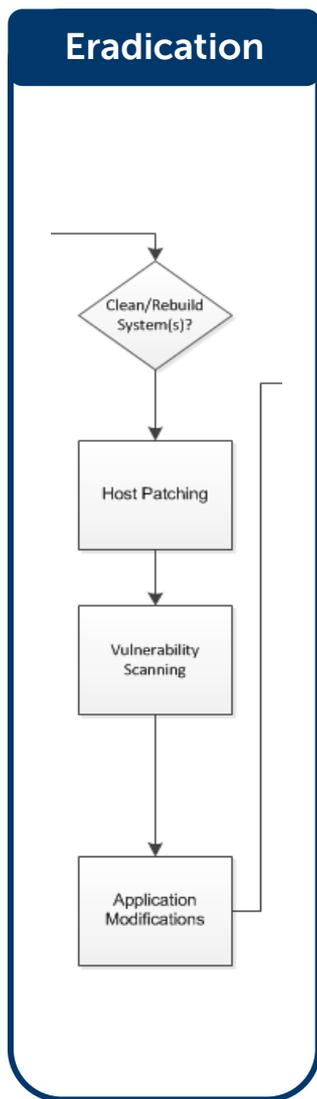
- Containment Requirements & Phasing
 - IP/DNS Blocks
 - AV DAT Push
- Change Criticality
 - Immediate
 - Deliberate



Technology and Tools

- Active Directory
- Access Control Lists
- FW/IPS/Proxy Changes
- Anti-Virus
- DNS Black holing

Phase: Eradication



People and Skillsets

- IT Staff – Implementers
- Security Staff – Validate Actions
- External Vendors
 - AV
 - FW/IPS



Process

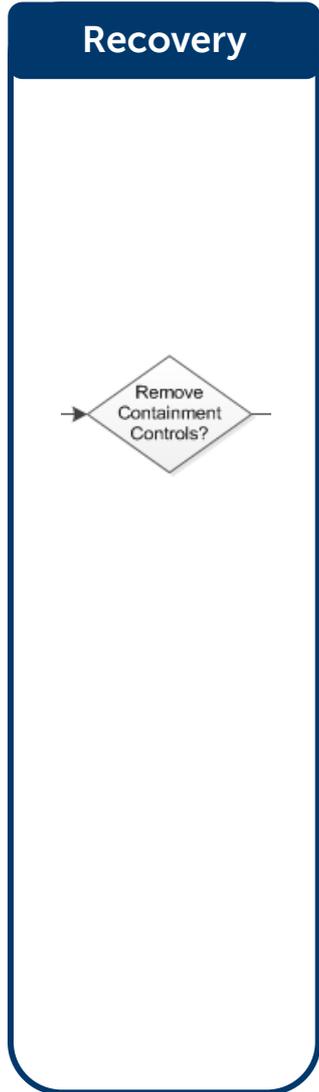
- System Remediation
 - Clean versus Rebuild
- Rescan
 - Internal
 - External
- Validation



Technology and Tools

- Vulnerability Scan (Qualys, NESSUS)
- Penetration Testing (Red Teaming)
- Web App Testing
- Malware Reverse

Phase: Recovery



People and Skillsets

- Users – Notification and Heightened Alerting
- IT Staff – Restore Systems to Full Function
- Incident Analyst – Focus on Previously Affected Systems



Process

- Normal IT Operations

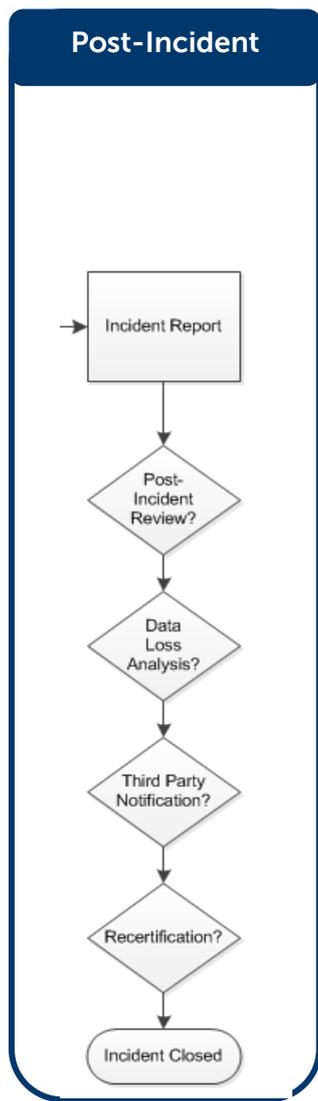


Technology and Tools

- Normal IT Operations



Phase: Post-incident activities



People and Skillsets

- CEO/CIO – Interest in Post-Mortem
 - Executive Buy-In
- CISO – Refine Incident Response Processes
- IT Director
 - System/Network Changes
 - Purchase/Upgrade



Process

- Refine Incident Playbook
- Refine Signatures on FW/IPS/Proxy
- Conduct Data Loss Analysis
- Conduct Gap Analysis on Infrastructure
- Update



Technology and Tools

- Follow-Up Notifications
 - E-Mail
 - SMS
 - Snail Mail

Building Your Plan



CSIRP Construction



COMPUTER SECURITY INCIDENT RESPONSE PLAN (CSIRP)

Classification: //Dell SecureWorks/Confidential - Limited External Distribution.
For Internal Company Use Only: The information contained in this document is the exclusive property of «Client Name» and contains confidential information. Its use is intended solely for the purpose of documenting the procedures and actions required for the recovery of «Client Name» Information Technology Systems and Services in the event of computer incidents.

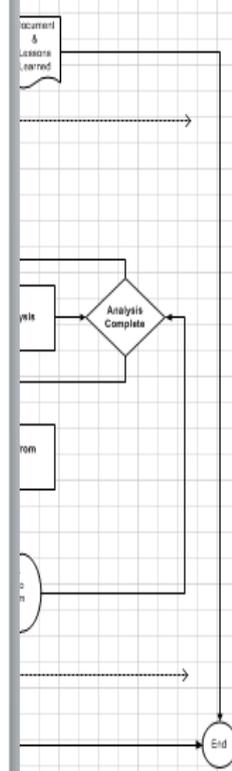
Distribution:
Page 2 

CSIRP Plan
Table of Contents

.../other technologies

Distribution:
Page 2 

Incident & Lessons Learned



Distribution:
Page 2 

Organizational Chart
Appendix No: III.A

olved in a particular have a backup contact

* based on the organizational charts

by developing

(CSIRP)

ISO/IEC/Technical

(NIST) Special Computer Security Incident Handling Guide

response Teams

specific expertise will be severity of the

and skills. It includes

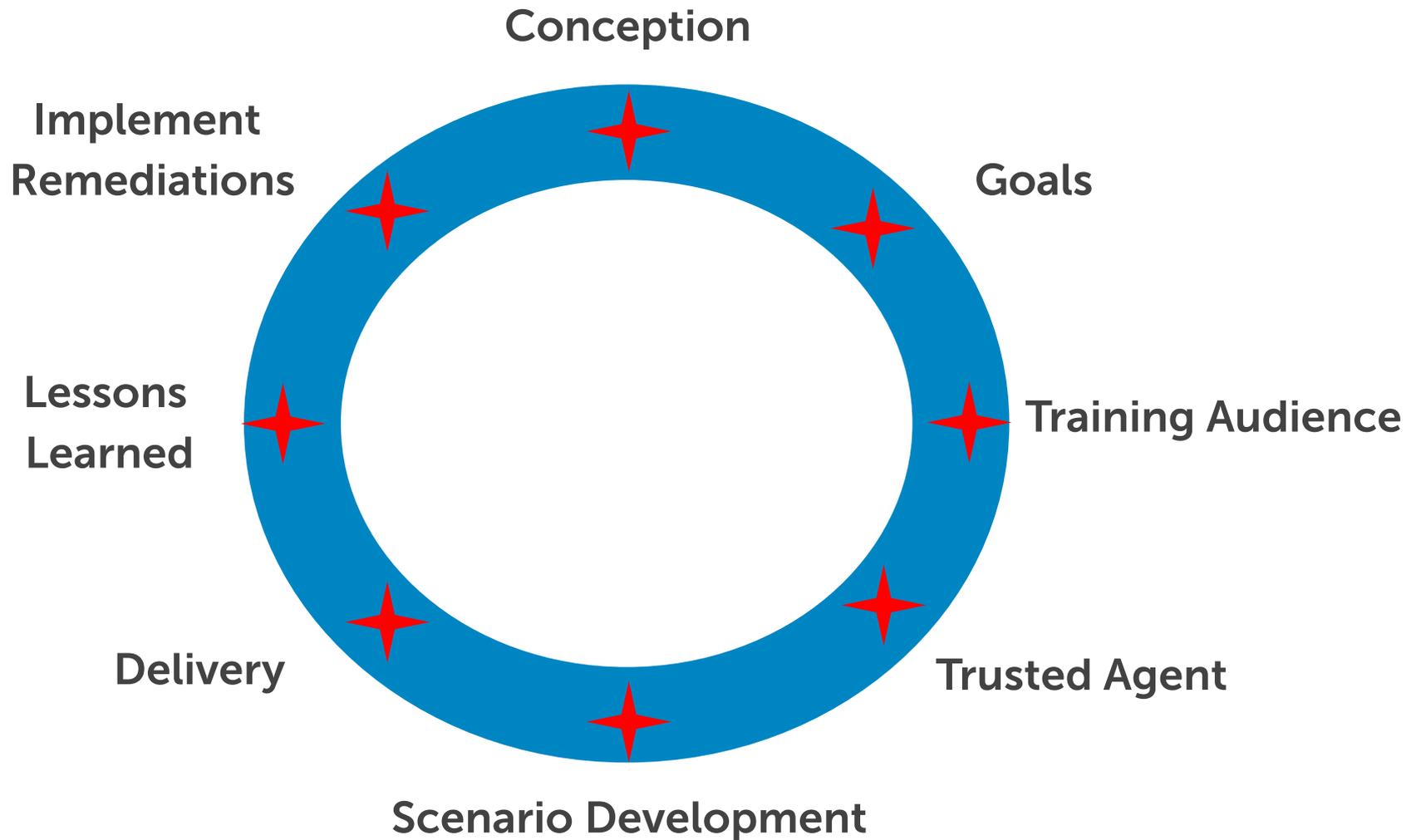
Distribution:
Page 2 



Exercising Your Plan



Tabletop Lifecycle



Models to consider

Incident Response models to consider



100% insource your Response Team

- Advantage: most responsive
- Disadvantage: \$\$\$\$, may not have the repetition to stay current



Insource your Incident Management, out source perishable and high-dollar Forensics skills

- Advantage: Maintain the leadership/responsibility within the organization
- Disadvantage: Full team not together except during a live incident and rehearsals



100% outsource your Response Team

- Advantage: Turn key solution, allows an IT Service team to focus on delivery, optimal for small staffs with no security personnel
- Disadvantage: \$\$\$\$\$\$, and you maintain no staff expertis



Case Study





The Entity: Health Care provider in the Northeast

The Event

- The client discovered an outbreak of w32.changeup (VOBFUS) on their networks, not detected by Anti-virus (AV)
- Client disconnected from the Internet to prevent further spread of the worm
- Contacted Dell SecureWorks IR team to assist
- Critical that the client be reconnected by Monday to conduct business

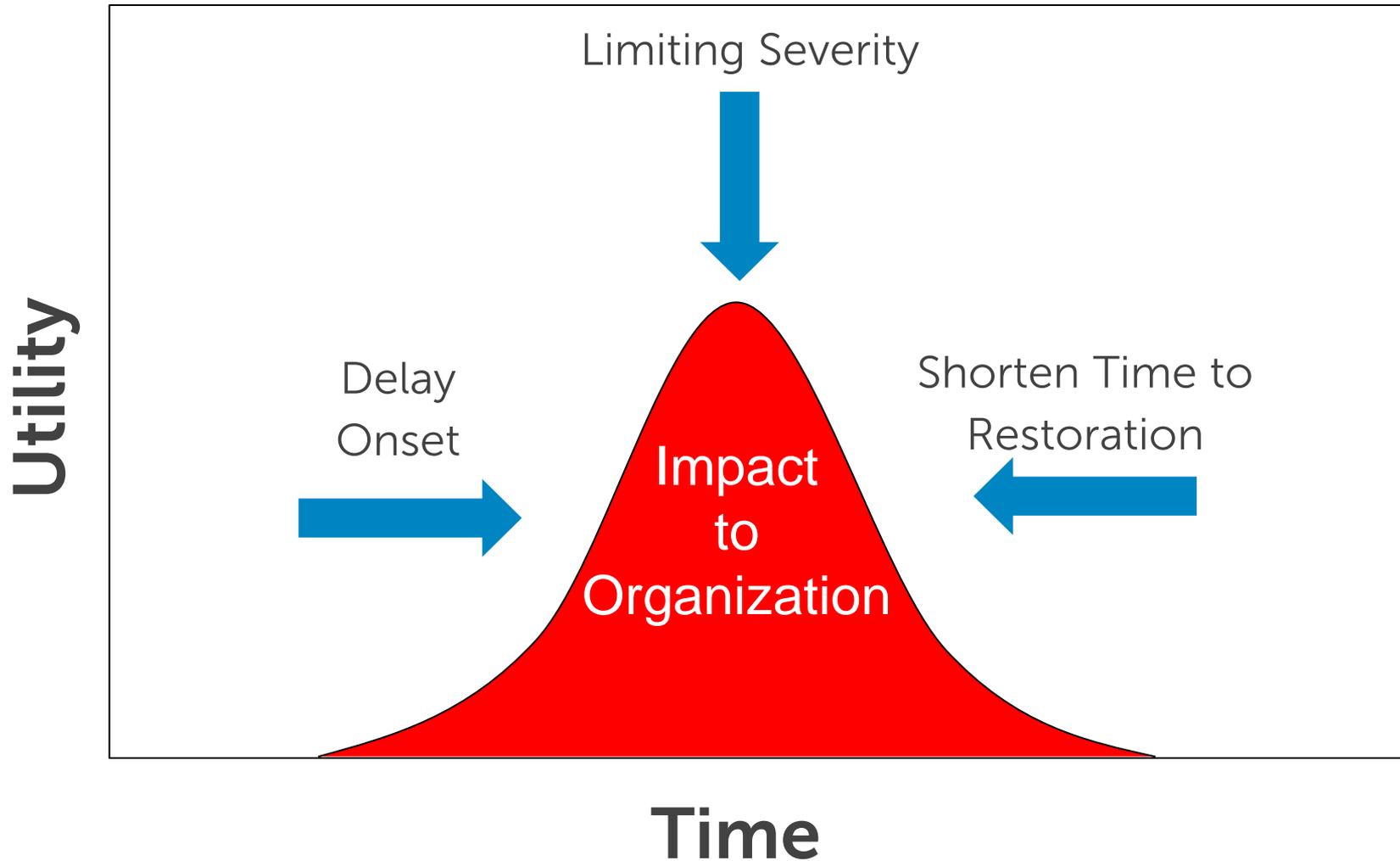


Response

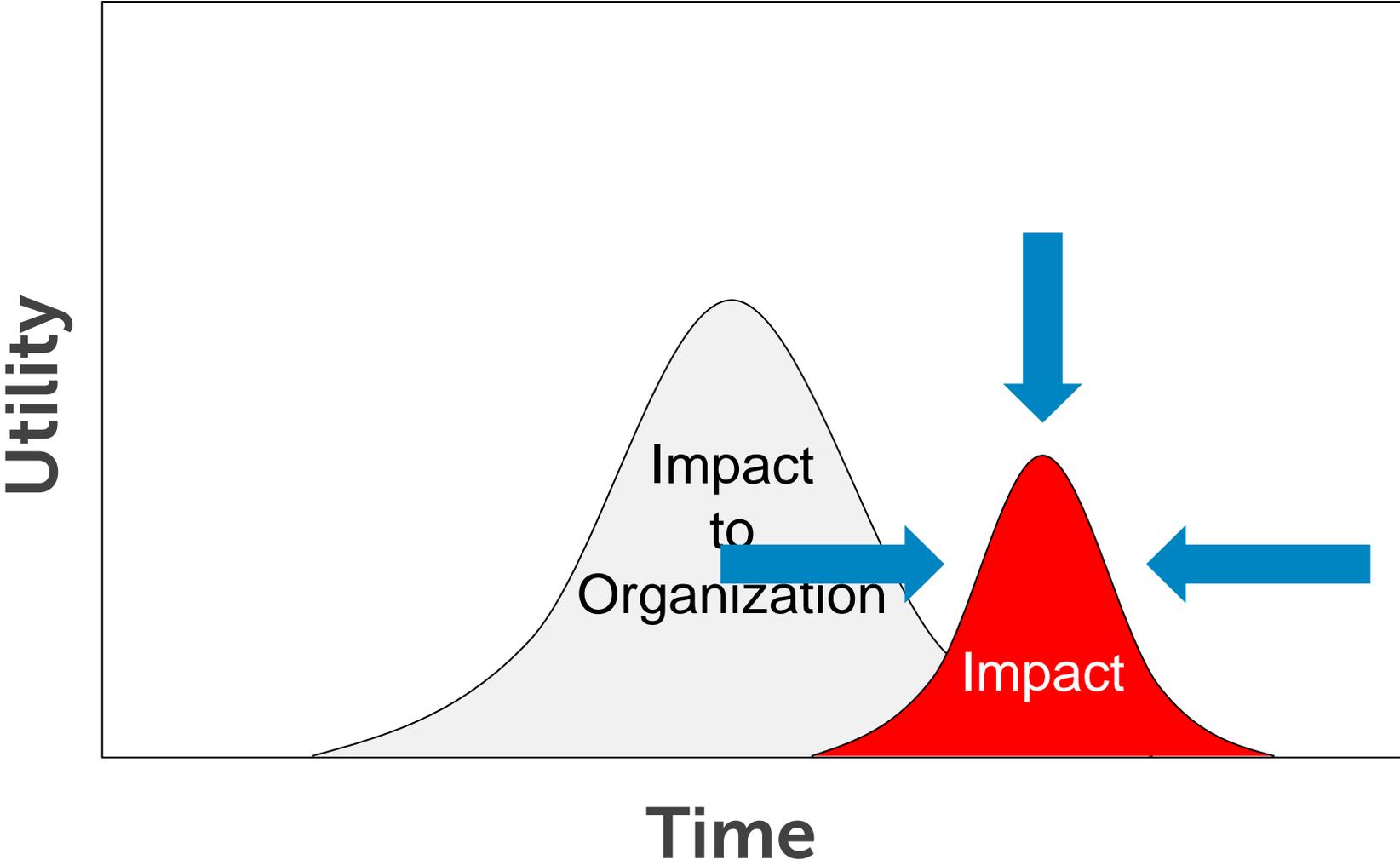
- Consultant was put on the ground within hours
- IR team discovered the w32.changeup worm was polymorphic in nature, allowed it to allude AV detection
- IR team also found Zeus and Medfos Trojans as a stage two infection (Criminal Tradecraft)
- Initial infection vector was through normal user activity (web drive-by infection)
- Command and Control blocked and systems cleaned before exfiltration of financial data
- Client reconnected before business started on Monday



Forces that Work on an Incident



Preferred End State



Conclusion

Pick your model

- 100% insourced
- Insource Incident Manage/outsourcing critical forensics skills
- 100% outsourced

Develop a plan with your model in mind

Exercise your plan with all of the key players

- IT staff
- Security Staff
- Business owners/Decision makers
- Outsource players

Continue improving your plan after every incident and rehearsal



Thank you.

Contact Dell SecureWorks at:

US - (877) 838-7947

