esentire®

FINANCIAL CRIME PREVENTION
The Human Factor

February 23rd 2017

WE DETECT THE CYBER THREATS THAT OTHER TECHNOLOGIES MISS

FOUNDED
2001

CUSTOMERS
600+

EMPLOYEES
290

esentire®

PROVEN CYBERSECURITY FOR MID-SIZED ENTERPRISE

YOY GROWTH
60%

CUSTOMER RETENTION
97%

CLIENT AUM PROTECTED
$3.2T

CAMBRIDGE | NEW YORK | LONDON | CORK

THREAT ACTORS

Characteristics of Insiders @ Risk of Becoming A Threat

- Introversion
- Greed/Financial Need
- Vulnerability to Blackmail
- Compulsive and Destructive Behaviour
- Rebellious, Passive-Aggressive Behaviour
- Ethical “Flexibility”
- Reduced Loyalty
- Entitlement/Narcissism (Exaggerated Self-Image)

Characteristics of Insiders @ Risk of Becoming A Threat

- Tendency to minimize mistakes or faults
- Inability to assume responsibility for their actions
- Intolerance of criticism
- Self-perceived value exceeds performance
- Lack of empathy towards others
- Predisposition towards law enforcement/authority figures
- Pattern of frustration and disappointment
- History of managing crises ineffectively

MEANS ◎ MOTIVATION ◎ OPPORTUNITY

ACCESS

EASY ACCESS TO
CYBER WEAPONRY

EASY

MINIMAL CYBER
SKILLS REQUIRED

LUCRATIVE

MOTIVATION
IS HIGH

IMPUNITY

NO NEGATIVE
REPERCUSSIONS

CURRENT CYBER ATTACKS


SPOOFING THE BOSS
BUSINESS EMAIL COMPROMISE (BEC)
1,200 FIRMS
$179M STOLEN
$179M UNITED STATES - $1.2B WORLDWIDE | SOURCE FBI 2015
$46.7M
Networking giant, Ubiquiti Networks, based in California
$17.2M
Stolen from an 800-employee Commodity Trading firm. Wired money in installments to a bank in China.

LAW FIRM

DENIAL
OF SERVICE
CASE FILE SHARE

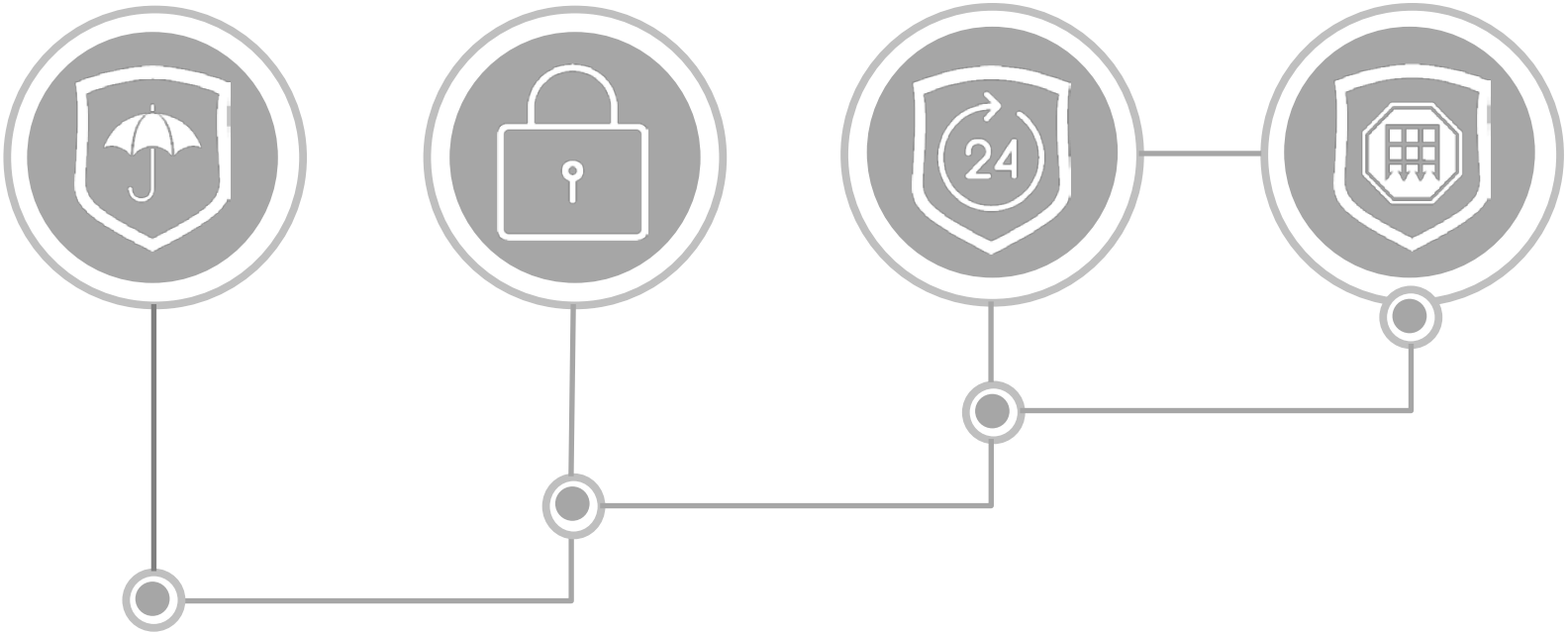
RANSOMWARE

7:43AM
AMP BLOCKS 1st 87.exe
DOWNLOADED FROM 2ND IP

7:44AM
TESLACRYPT BEACONS
TO CNC SERVER

7:54AM
SOC ALERTS ON INFECTION
AND BLOCKS TRAFFIC

8:30AM
INFECTED HOST
ISOLATED/MITIGATED



Ransomware Failure Vectors: Technical, Process/Policy, Training

- The firm's upstream email (SMTP) provider did not scan attachments for malicious content.
- The firm's next-generation firewall did not identify the attachment as malicious (or questionable) content.
- The firm's local email system (e.g. Microsoft Exchange) did not scan attachments for malicious content.
- The end user was not sufficiently trained to identify a phishing email (with malicious content).
- The user's workstation (or mobile device) did not flag the malicious content (through anti-virus or other endpoint protection methodology).
- If the delivery vector was a macro hidden within an Office document (the most common delivery method), macros were enabled within Office (or the user was enticed to enable them manually).
- The user's workstation did not have restrictions placed on the execution of downloaded content.
- The firm's next-generation firewall and/or Intrusion Prevention system did not recognize and/or block the command-and-control traffic (including key generation) of the malicious code (particularly important if the remote IP addresses were previously known to be bad).
- The firm did not detect (through filesystem analysis) that a specific user was modifying a large number of files rapidly.
- Depending on how many files were affected by the infected endpoint, it is a possibility that the end user had more access than they necessarily needed to execute their job.
- During the restore process, some newer files might have been not backed up due to a gap in backup rigor.

“Am I doing enough to stop ransomware?”

eSentire Cybersecurity Response
Ransomware Defense Matrix

esentire®

Human (Wetware) Defense Mechanisms

Minimum	Intermediate	Advanced
✓ Staff training to aid in the proactive detection of malicious content (online, videos, posters). ✓ Annual phishing testing performed for employees. ✓ Create Incident Response plans to prepare for an eventual incident.	✓ Monthly phishing testing performed for employees. ✓ Quarterly review of Incident Response plans. ✓ Investigate a Continuous Monitoring/embedded Incident Response methodology.	✓ Regular micro-training (daily) to ensure ongoing mindshare in defending against malicious content.

Pragmatic Security Event Management - RANSOMWARE

esentire

PHASE 0 PREPARATION

Ensure all systems are up-to-date

- **Workstations, Servers (including internal and DMZ)**
  - *Patching, where possible.*
  - *Antivirus, Anti-Exploit (e.g. EMET), Application Whitelisting (e.g. AppLocker)*
  - *Restrict downloading of applications and payloads (Network Application Control)*
- **Mobile Devices**
  - *MDM (Patching, Restricting Applications, Downloads)*

Ensure backups of critical systems and data are successful and available

- **Test regularly for content accuracy**
- **Back up important data offline**

Restrict Access

- **Enforce "least-privilege" access throughout filesystems**
- **Segment network**
  - *Restrict workstation-to- workstation access*
  - *Utilize jump box for important and critical parts of network*
- **Log access attempts to shares that get denied (early signs of infestation)**

Reduce Susceptibility Footprint

- **Reduce inbound vectors (e.g. personal email)**
- **Disable macros within Microsoft Office if not needed**
- **Use Microsoft Viewer software if editing of Office documents is not needed for all tasks (especially when viewing suspect documents)**
- **Improve/Harden upstream SMTP attachment scanning and quarantine**
  - *Block .zip, .exe, .js, .html*
  - *PTR/SPF records for anti-spoofing protection*

Training

- **Inoculate skepticism in end-users**
  - *Security Awareness Training*
  - *Phishing test campaigns*
  - *Weekly reminders/ postings*

Alerting

- **Implement behavior-based alerting when a certain threshold of files are modified**
- **Implement a Continuous Monitoring/Embedded Incident Response methodology**

PHASE I DETECTION

Formal Initiation of Event

- **Note timestamp and method of discovery**
- **Identify "Patient(s) Zero"**
  - *External*
    - » *FI*
  - *Workstation*
    - » *Single or Multiple?*
  - *Server*
    - » *Single or Multiple?*
  - *Mobile Device*
    - » *Single or Multiple?*
  - *Accounts*
    - » *Single or Multiple?*
  - *Blend of the above*

PHASE II CONFIRMATION / TRIAGE / ASSESSMENT

Initiate Event Data Cull if manpower permits, otherwise immediately move to PHASE III.

PHASE III MITIGATION / REMEDIATION / RESOLUTION

Contain

- **Is isolation possible?**
- **What is the impact of isolation?**
- **Is there a need for the BC/DR Plan to be put into effect?**
- **Method**
  - *Manual Disconnect*
    - » *Cable*
    - » *Wireless*
    - » *Antenna Disable (mobile device)*
  - *Switch Port Disable*
  - *Wireless Controller Access Disable*

Identify

- **Breadth of the filesystem affected**
- **Impact and sensitivity of the files lost**

Analyze

- **Affected systems for possible multi-pronged/method attack**
- **Vestigial artifacts left on affected systems**
- **Network Indicators**
  - *Payload Transfer / Droppers*
  - *Command and Control Channels / Covert Channels*
  - *Data Loss/File Extrusion*

Eradicate

- **Implement IP blocks (on firewall) if deemed appropriate**
- **Alert staff to indicators derived from attack**

Recovery

- **Initiate file recovery**
- **Verify backups not affected**
  - *Check shadow copies (system restore)*
- **Wipe affected systems**
  - *if needed*
  - *when convenient*
  - *and analytics completed*

PHASE IV POST-INCIDENT

Confirm "All Clear" Event

- **Note timestamp for formal records**

Update and Secure Documentation

Root Cause Analysis

- **Present findings to management**

Enhance Response Capabilities

- **Present findings to management**

esentire®

KINGFISHER CAMPAIGNS

ALBACORE
Multi-Phase campaign
PHISHED the CSO

CATFISH
Apple iOS campaign
Free Pencil from iTunes

ROCK FISH
ADP Template Campaign
Mimicked attack we detected

RED SNAPPER
UBER campaign
Reported fraudulent use

20% PHISH SUCCESS

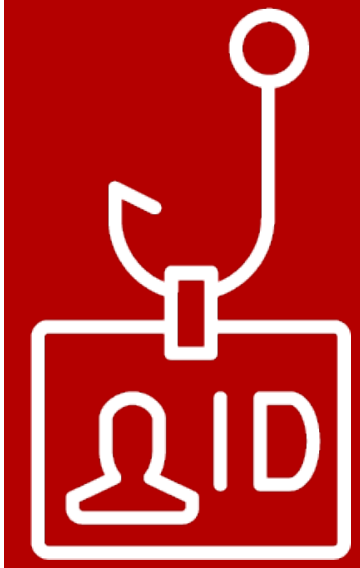
esentire®

PHISHING CAMPAIGN STATISTICS

	Avg Total Recipients	Avg % Click	Avg % Phish	Avg % Open	Avg Total Events
All Time	130.30	18.26%	9.38%	19.80%	347.20
2016	123.48	18.80%	9.62%	20.56%	363.84
2015	82.00	17.32%	8.91%	19.25%	317.26

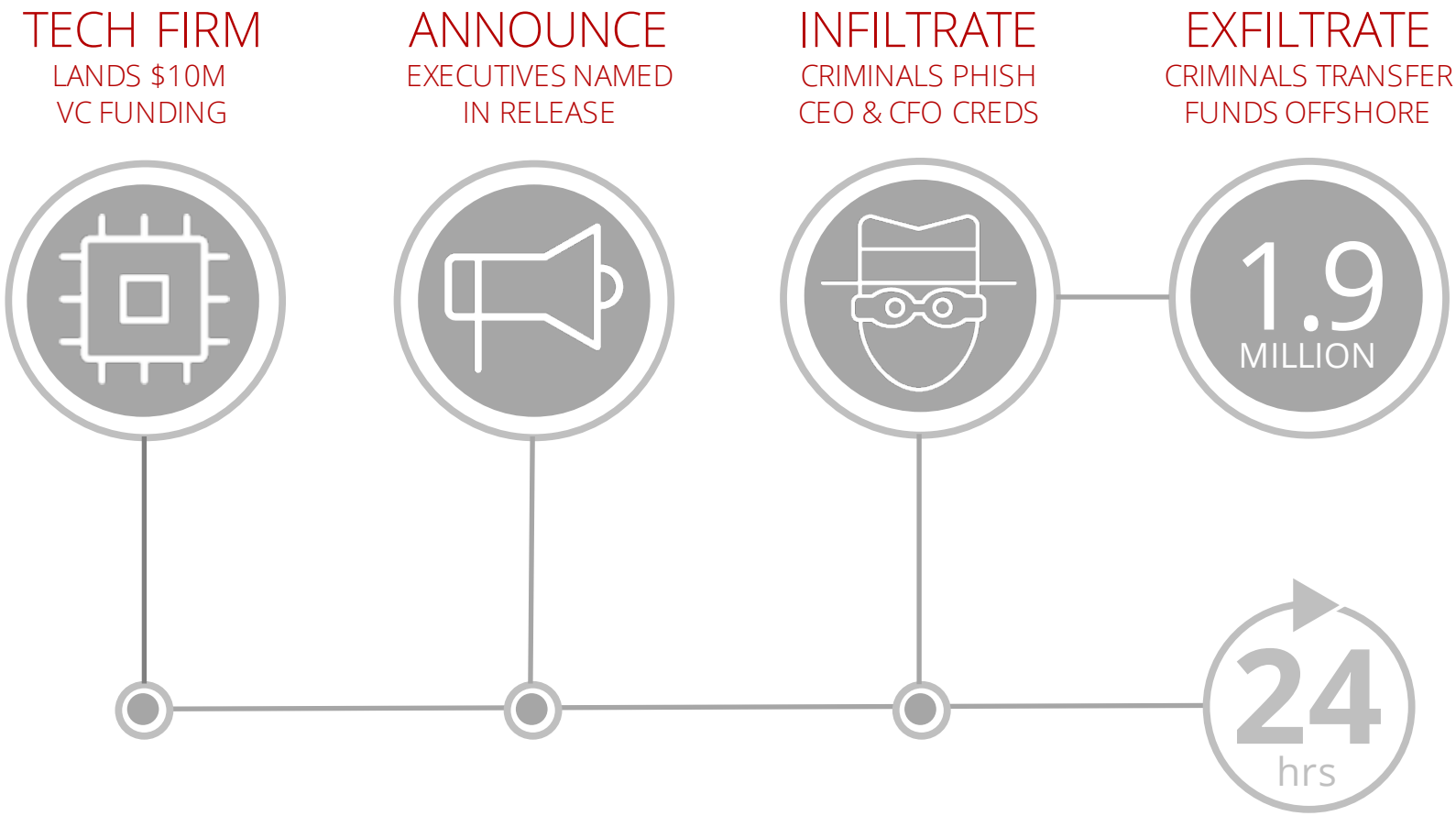
Campaign Types	# of Times Used	Avg % Click	Avg % Phish	Avg % Attach
ADP	15	25.28%	11.79%	
Air Canada	1	6.56%	0.00%	
Amazon	10	21.07%	5.98%	
AmEx	1	0.00%	0.00%	
Apple	2	19.59%	11.25%	
Attachment	1			31.25%
Background Check	1	0.00%	0.00%	
Benefits	9	18.62%	9.19%	7.55%

$1.9M
STOLEN



PHISHING
CAMPAIGN

CREDENTIAL HARVESTING



IM

FUND

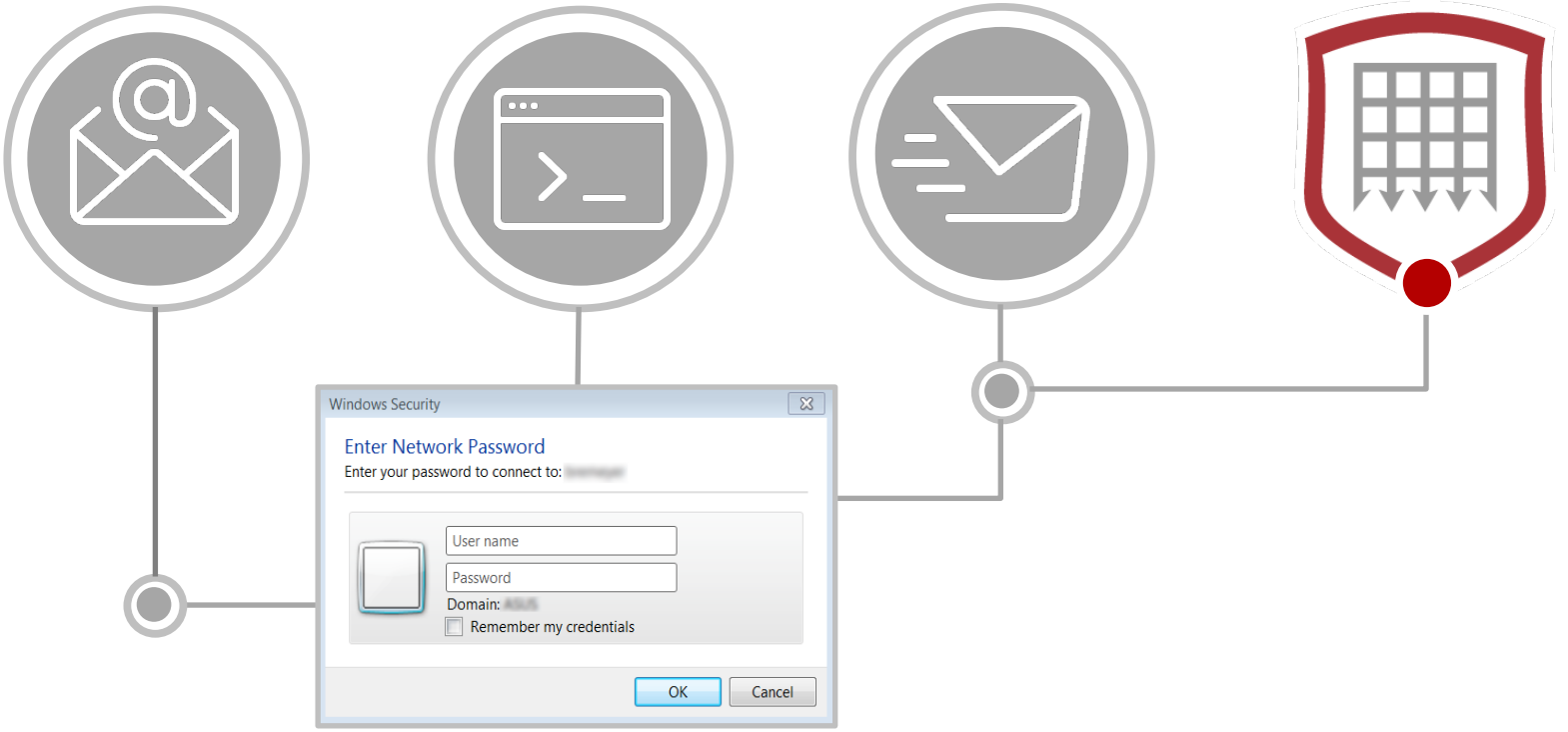
TARGETED ATTACK

TARGET
SENT EMAIL WITH
INFECTED ATTACHMENT

INFILTRATE
FAKE LOG IN
CAPTURED CREDS

EXPAND
INFECTED EMAIL SENT FROM
COMPROMISED ACCOUNT

BLOCKED
ESENTIRE DETECTED
AND REPORTED ATTACK



PUMP

DUMP

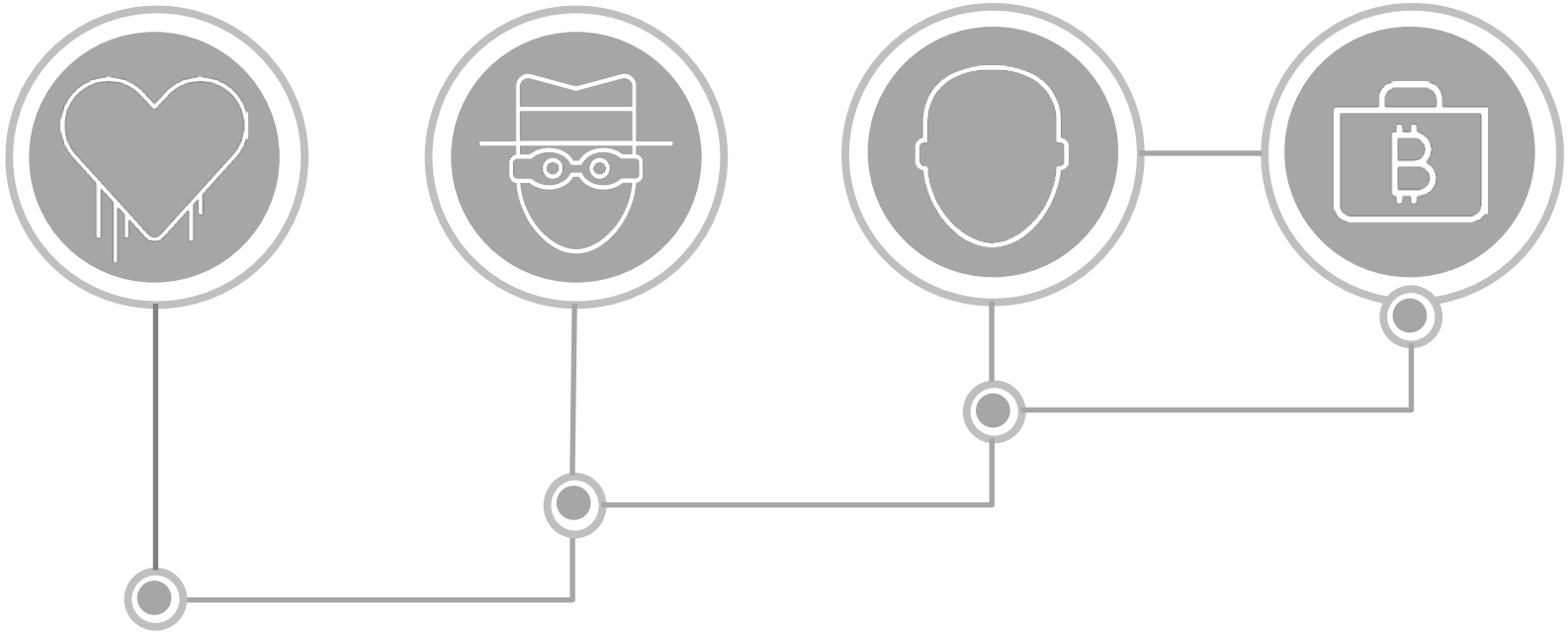
SYSTEMIC VULNERABILITIES

BANK
CLIENT RECORDS STOLEN FROM BOSTON FIRM

SIX FIRMS
INFILTRATED--USED TO MAKE STOCK BUYS

SOCIAL ENG.
INVESTORS AND MAKE RECOMMENDATIONS

PUMP/DUMP
HACKERS SOLD STOCKS AT HIGHER PRICE



CSI

CYBER

DISCOVERED CRIME RING

COLD CASE
SOC ANALYST
DISCOVERED CNC TRAFFIC

FORENSICS
TRACKED HACKER
THROUGH CELLPHONE

EVIDENCE
COLLECTED
STOLEN DATA

LAW
TURNED OVER EVIDENCE
TO LAW ENFORCEMENT

Information Security Event Scenarios (aka "The Dirty Dozen")

- Malware Compromise
  - Ransomware Attack
- Social Engineering
  - Business Email Compromise
- Infrastructure Outage (Internal)
- Local Access Without Authorization (Non-Malware)
- Remote Access Without Authorization
- Lost/Stolen Devices
- Inappropriate Behavior (Internal)
- Cloud Service Access Without Authorization
- Data Loss/Extrusion (Internal)
- Direct Financial Loss
- Denial of Service (External)
- Physical Breach


eSentire Security Procedures
Pragmatic Security Event Management

esentire

Four Phases of Event Management Team Operations

Phase 1
Detection, Event Acknowledgement and Initiation

- ☐ Conduct initial assessment to determine event's nature, scope, and severity.
- ☐ Pass notifications to the appropriate individuals, organizations and agencies.
- ☐ Activate Event Management Response Team and initiate an assessment of the incident.
- ☐ Gather information continually; keep accurate records throughout the process.

Phase 2
Preparation

- ☐ If sufficient advance warning is given, it may be possible to prepare for a declared incident.
- ☐ Event Management Team members assemble in accordance with plan.

Phase 3
Deployment of Personnel

- ☐ Senior Event Management Team members determi
- ☐ Event Management Team members de

Board of Directors Representative

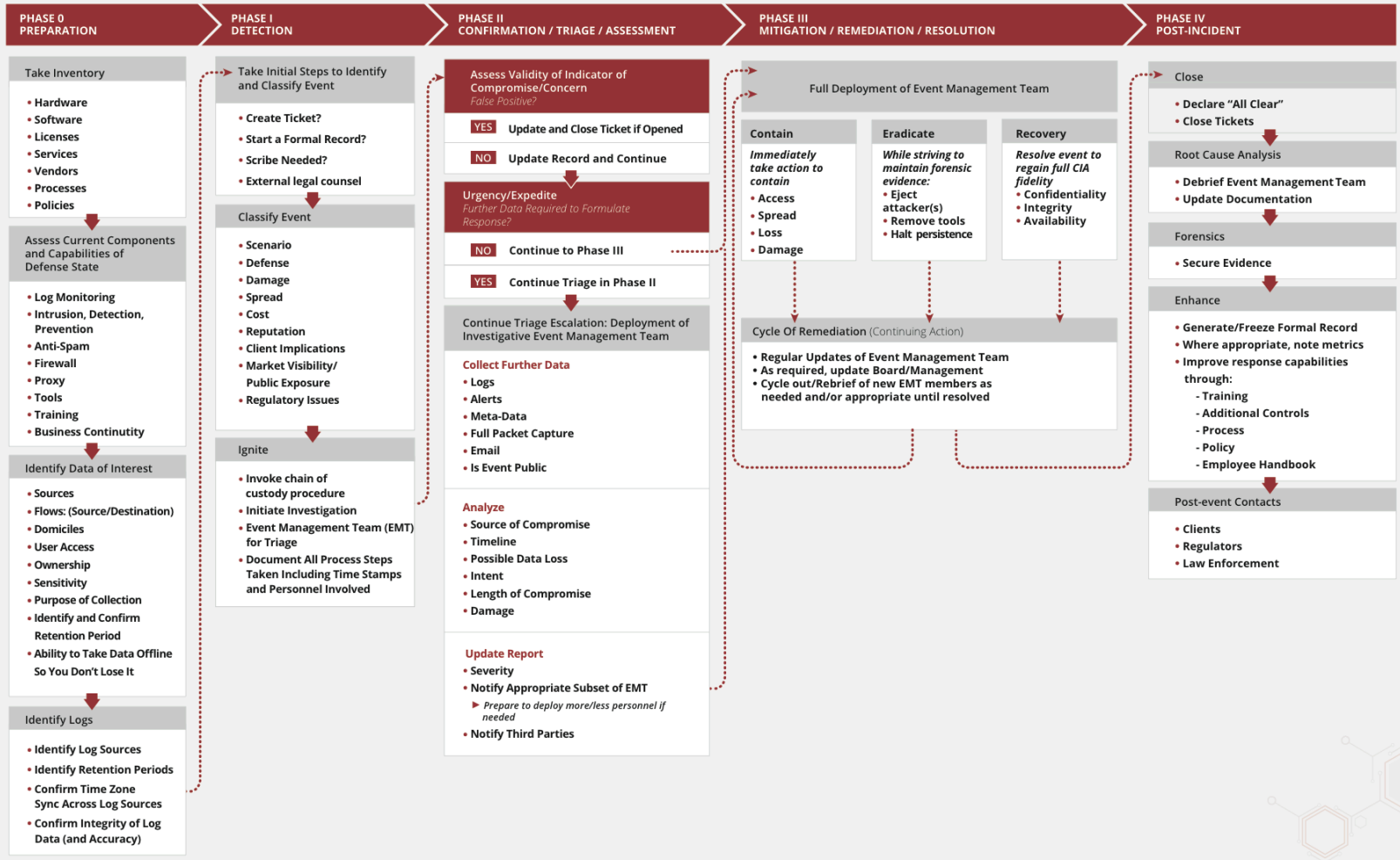
Name	
Title	
Phone 1	
Phone 2: Escalation 1	
Phone 3: Escalation 2	
Email	
SMS	

External Finance Contact I

Name	
Title	
Phone 1	
Phone 2: Escalation 1	
Phone 3: Escalation 2	
Email	

Core IR Process

esentire



Scenario Qualification Workflow

esentire

PHASE 0 PREPARATION

Review Critical Documentation

- **Complete the Data Flow Security Template Document**
  - *Identify Key Systems and Data*
- **Review AUP documentation**
- **Review BCP/DR Documentation**
- **A mapping of network switches to systems**

Complete EMT contacts

- **Legal**
- **Law Enforcement**

Central War Room

- **Conference Lines**

Identify Contact Method for Whole Company

- **Communicate Bad Email identification and deletion process**
- **Identify and Implement method to block upstream SMTP**
- **"Want-care" defenses**
  - *Identify a plan to implement an "Internet Go Dark" procedure if necessary*

PHASE I DETECTION

Identify scenario

- **Malware Compromise**
- **Infrastructure Outage (Internal)**
- **Local Access Without Authorization (Non-Malware)**
- **Remote Access Without Authorization**
- **Lost/Stolen Devices**
- **Inappropriate Behavior (Internal)**
- **Denial of Service (External)**
- **Physical Breach**
- **Social Engineering**
- **Other**

Advance Warning

- Has someone verified the available "advance notice" attack criteria and can confirm they are accurate and factual?
- Does it appear that these "advance notice" attack criteria pose a possible future threat to the organization?
- Does it appear that these "advance notice" attack criteria could provide unauthorized access to the systems?
- Are the "advance notice" attack criteria of a time-sensitive nature due to imminent threat?

Establish Initial Event Severity Level

- **Estimated Event Severity Variable: Defense**
  - **3 (High)** - No immediately identifiable defense available, time-sensitive
  - **2 (Medium)** - Mitigating defense controls exist and can be readily enabled, not necessarily time-sensitive
  - **1 (Low)** - Defended against by default, not time-sensitive
- **Estimated Event Severity Variable: Damage**
  - **3 (High)** - File/system destruction/modification, inhibiting operation, high traffic, non-repairable damage, significant effort to repair/restore
  - **2 (Medium)** - Non-critical system modification, easily-repairable damage with minimal effort
  - **1 (Low)** - No demonstrable damage, annoyance but not damaging
- **Estimated Event Severity Variable: Spread**
  - **3 (High)** - Internal and External spread, rapid speed, multiple offices/personnel affected
  - **2 (Medium)** - External-only access/spread (e.g. only Command-and-Control channels), single office/person affected
  - **1 (Low)** - No perceived spread or Not Applicable
- **Estimated Event Severity Variable: Defense+Damage+Spread**
  - **7-9: High**
  - **5-6: Medium**
  - **3-4: Low**
- **Note: Events that involve threats to employee wellbeing, financial or possible data loss (including but not exclusive to loss of PII), are automatically considered High Severity.**

PHASE II CONFIRMATION / TRIAGE / ASSESSMENT

Has eSentire been contacted?

Should all IT staff be engaged to report to work/prepare on standby?

- **Level 1: All IT staff must immediately dial into War Room conference call bridge and make their way to the appropriate office, unless instructed otherwise**
- **Level 2: All IT staff must dial into the War Room conference bridge and be on standby to report to the appropriate office**
- **Level 3: Critical IT staff must report to appropriate office and dial into War Room conference bridge**
- **Level 4: Critical IT staff must dial into War Room conference bridge**

Have critical third-party vendors been contacted?

- **Is there a need for them to connect into the War Room Conference Call Bridge, report to the appropriate office, or be on standby?**
- **Has their identity been confirmed through known-number callback or other approved means?**

Does it appear that the threat is from an internal source (or purely external)?

Have credentials been compromised?

- **Is there a need to initiate a global password reset?**

Must we prepare to contact or be contacted by any subset of the following groups:

- **Law enforcement**
- **Regulators**
- **Press**
- **Clients**
- **Staff**

Have chain of custody procedures been reviewed/refreshed if evidence is needed in any possible future legal proceedings?

PHASE III MITIGATION / REMEDIATION / RESOLUTION

Activate EMT Deployment

Declare time of next briefing

Have critical third-party vendors been contacted?

- **Briefing from each EMT Member**
- **List of emerging action items**
- **Summarize situation, response direction as appropriate**
- **Declare time of next briefing**

Update Internal and External Entities list as appropriate

Stand down or re-assign EMT members as required to support the event response

Continuing Action

- **Direct operation of the event response. If appropriate, turnover EMT members**
- **Develop a plan to ensure:**
  - *Event Leadership and Direction is clear*
  - *Timely and accurate communication*
  - *Appropriate deployment of resources*
  - *Promotion of timely resumption of "business as usual"*
  - *Log-keeping is still being conducted*
  - *All formal communication is recorded*
- **Review Event Security Level to ensure it is still appropriate**
- **Declare time of next briefing (adjust cycle timing as appropriate)**
- **Provide Situation briefing to Executive**
- **Turnover procedures include:**
  - *Outgoing EMT members: Update response status*
  - *Briefing of incoming EMT members*
  - *Review Event Severity Level to ensure it is still appropriate*
  - *Determine if deactivation of event response is appropriate*
    - » *Situation is stable and/or improving*
    - » *Risks appear to be mitigated*

PHASE IV POST-INCIDENT

Risks appear to be mitigated

- **Ensure formal communication is recorded**
- **List of emerging action items**
- **Ensure that Lines of Business are able to continue with recovery execution plan as needed**
- **Ensure that all records are collected and secured as appropriate**
- **Finalize internal and external communication**
- **Has this security incident and response impacted in any way log files that may be overwritten or aged out? Is there a procedure to "solidify" log files for purposes of evidence?**
- **Has this security event and corresponding response impacted the Company backups and/or replicated data sets required for continuity purposes?**

Root Cause Analysis

- **Identify event vector**
- **Identify data loss**
- **Update Acceptable Use Policy/Employee Handbook if appropriate**

esentire®

Top-level Regulatory Focus

ASSETS
Do you know what data you have?

REGULATORS
Do you know what legislation governs the data you have?

THREAT ACTORS
Do you know what cyber threats are targeting your firm?

PROTECTION
How are you defending your firm from cyber threats?

RISKS
Do you know what access risks exist?

REPORTING
Can you demonstrate your cybersecurity claims?