What's Your Incident Response Recipe?

Renault Ross CISSP, MCSE, VCP5, CHSS
Chief Security Business Strategist
Symantec, North America
Is Compromise Inevitable?

<table>
<thead>
<tr>
<th>Breaches With More Than 10 Million Identities Exposed</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
</tr>
<tr>
<td>8</td>
</tr>
<tr>
<td>-</td>
</tr>
</tbody>
</table>
Total Identities Exposed

<table>
<thead>
<tr>
<th>Year</th>
<th>Total Identities Exposed</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011</td>
<td>232 million</td>
</tr>
<tr>
<td>2012</td>
<td>93 million</td>
</tr>
<tr>
<td>2013</td>
<td>552 million</td>
</tr>
<tr>
<td>2014</td>
<td>348 million</td>
</tr>
<tr>
<td>2015</td>
<td>500 million (Estimated)</td>
</tr>
</tbody>
</table>

+30% increase from 2014 to 2015.
In 2009 there were 2,361,414 new piece of malware created.

In 2015 that number was 430,555,582

That’s 1 Million 179 Thousand a day.
TWO TEAMS INDICTED!
Are all “Incidents” the same?

- Public Data Breach
- Suspected Compromise
- Malware Outbreak / Employee Investigations
Proactive or Reactive?

Crisis Mode
- Experiencing a **security incident**
- Internal teams **unable to address issue** at hand
- **Pressure to resolve** the incident quickly
- Need to address legal/compliance **reporting requirements** post-incident
- Currently battling an incident and need **extra help**
- **Media coverage** of breach

Elevated Concern
- Realization that **gaps in security** may have led to an **undetected breach**
- Industry **peer suffered a breach** and they want to know if they have been impacted
- New **security alert** or intelligence that causes concern and the customer has no way to determine if they might be impacted

Proactive Planning
- **Looking to turn plans into optimized programs**
- **Looking for ways to improve or augment internal IR capabilities**
- Want to **pre-negotiate terms and rates** for faster action when 3rd party help is needed
- Have a **regulatory or legal requirement** to have a 3rd party IR team on retainer
CAN YOU STOP ALL THREATS?

PREPARE

PREVENT

DETECT

RESPOND

RECOVER
RECOVERY IS THE KEY!

PREPARE

PREVENT

DETECT

RESPOND

RECOVER

Finding Incursions

Containing & Remediating Problems

Restoring Operations

Copyright © 2016 Symantec Corporation
"It is the policy of the United States to enhance the security and resilience of the Nation’s critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties."
## FUNCTIONS: HIGH-LEVEL GOALS

<table>
<thead>
<tr>
<th>Functions</th>
<th>ID</th>
<th>Identify</th>
<th>Develop the <strong>organizational understanding</strong> to manage cybersecurity risk to systems, assets, data, and capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>PR</td>
<td>Protect</td>
<td>Develop and implement the <strong>appropriate safeguards</strong> to ensure delivery of critical infrastructure services</td>
<td></td>
</tr>
<tr>
<td>DE</td>
<td>Detect</td>
<td>Develop and implement the appropriate activities to <strong>identify the occurrence</strong> of a cybersecurity event</td>
<td></td>
</tr>
<tr>
<td>RS</td>
<td>Respond</td>
<td>Develop and implement the appropriate activities to <strong>take action</strong> regarding a <strong>detected</strong> cybersecurity event</td>
<td></td>
</tr>
<tr>
<td>RC</td>
<td>Recover</td>
<td>Develop and implement the appropriate activities to <strong>maintain plans for resilience</strong> and to <strong>restore any capabilities or services</strong> that were impaired due to a cybersecurity event</td>
<td></td>
</tr>
<tr>
<td>Function</td>
<td>Categories</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Identify (ID)</td>
<td>Asset Management (AM)</td>
<td>The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization’s risk strategy.</td>
<td></td>
</tr>
<tr>
<td>Identify (ID)</td>
<td>Business Environment (BE)</td>
<td>The organization’s mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.</td>
<td></td>
</tr>
<tr>
<td>Identify (ID)</td>
<td>Governance (GV)</td>
<td>The policies, procedures, and processes to manage and monitor the organization’s regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cyber risk.</td>
<td></td>
</tr>
<tr>
<td>Identify (ID)</td>
<td>Risk Assessment (RA)</td>
<td>The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.</td>
<td></td>
</tr>
<tr>
<td>Identify (ID)</td>
<td>Risk Management Strategy (RM)</td>
<td>The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.</td>
<td></td>
</tr>
</tbody>
</table>
WAYS TO USE THE FRAMEWORK

- Basic Review of Cybersecurity Practices
- Establishing or Improving a Cybersecurity Program
- Communicating Cybersecurity Requirements with Stakeholders
- Identifying Opportunities for Updated Informative References
- Methodology to Protect Privacy and Civil Liberties

“How well are we doing today?”
“Can we assess and improve?”
“Can we speak the same language?”
“What else should we consider?”
“Can we protect data better?”

Let’s focus here
The Goals Of Incident Response

• Primary Goal of Incident Response:
  – Effectively remove a threat from the organization’s computing environment, while minimizing damages and restoring normal operations as quickly as possible.

• Primary Goal is Accomplished Through Two Main Activities:
  – Investigation: Involves Diagnosis, Analysis and Containment Strategy
  – Remediation: Involves Containment, Mitigation and Remediation

• What Else Should Be Involved For A More Comprehensive Incident Response?
Incident Response Today

Un-prioritized Alerts

Manual IR Call Trees

Triage Begins

External Response Team Called

Delays in Ramp-up

Manual Correlation of Evidence
Incident Response Tomorrow

- Prioritized/Correlated Alerts
- Automated Triage Workflow
- Collaborative Triage

- Clear Line of Site
- Real-time updates
- Collaborative Response
## Incident Response Recipe

<table>
<thead>
<tr>
<th></th>
<th>Incident Response Recipe</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Threat Identification &amp; Intelligence</td>
</tr>
<tr>
<td>2</td>
<td>3\textsuperscript{rd} Party Security Services</td>
</tr>
<tr>
<td>3</td>
<td>Incident Response</td>
</tr>
<tr>
<td>4</td>
<td>Cyber Team Readiness</td>
</tr>
<tr>
<td>5</td>
<td>Conclusion</td>
</tr>
</tbody>
</table>
Threat Identification & Intelligence

Security Intelligence Defined

- collection
- analysis
- impacts
- risk posture
- actionable insight
- lowers
- security risk

The goal of Security Intelligence is to provide broad and actionable insight, which lowers the security risk of an organization.
Use Vulnerability alerts and Vulnerability datafeeds to help identify and prioritize vulnerabilities based on technologies relevant to an organization.

**SETUP “TECH LIST”**
Security Analyst sets up a “Tech List” on the DeepSight portal to match the products being used in the organization.

**DISCOVERY…**
of new, relevant, Vulnerability by DeepSight Vulnerability Analysts provided in a timely manner.

**GET ALERTERED**
FOR ORGANIZATIONS, using DeepSight Portal, Security Analysts receives an vulnerability alert based on the “Tech List” that was setup via SMS or email.

FOR ORGANIZATIONS, using DeepSight Datafeeds, DeepSight Vulnerability intelligence is ‘fed’ into customer governance, risk and compliance (GRC) systems.

Irrespective of org size, product vulnerabilities including info such as: CVSS Scores, Exploit details, Work Around, Solution & Fix, Availability of a Patch, and more.

**APPLY PATCHES**
Security Analysts tracks the vulnerability via DeepSight alerts and/or feeds and applies the patch as and when it becomes available based on priority. Thus allowing security team to focus on securing IT systems.
Director of Security of a financial services company in the US, receives a Managed Adversary and Threat Intelligence (MATI) report, which lists out the details of a campaign targeting the financial vertical in the US.

Director of Security sets up a MATI report alert on the DeepSight portal. Such that he is emailed a report as it gets published.

SETUP MATI REPORT ALERT

Discovery... of a campaign by a DeepSight MATI Analyst

INFORM SECURITY OPS TEAM

Provides the “Technical Indicators” in the report to the Security Operations team to put in place counter-measures.

GET ALERTERED

Director of Security receives an MATI report alert via email

USE MATI REPORT FOR:

- Executive Communication
- Strategic Planning and Risk Mitigation
- Showcase to management the threat landscape knowledge
Threat Identification & Intelligence

Intelligence Use Cases

Detection of Unknown External Threats - Datafeeds

Security Operations Center (SOC)
Central location to collect information on threats such as: external, internal, user activity, and loss of sensitive data

External Threats from DeepSight

EXTERNAL UNKNOWN THREATS
DeepSight Datafeeds provide external threat data, not known to the security infrastructure, to SOC's/SIEM's for detection & prevention.

REPUTATION DATAFEEDS
DeepSight reputation Datafeeds provides an up-to-date list of "Command and Control" servers of botnets known to DeepSight. Allowing for the detection and the prevention of exfiltration of sensitive data.

CONTROL POINTS
SIEM is used to detect and Network control points such as Firewalls and Gateways are used to prevent exfiltration using the DeepSight data
3rd Party Security Services

Experienced People
Events, Attacks and Incidents – Defined

**Event**
- Number of Events in a typical week: 45,000
- Number of Attacks in a typical week: 14,000
- Number of Incidents in a typical week: 2

**Event**
- Event
- Attack
- Incident

**Event**
Events are something happened, either malicious or not. Some for communication passed through a particular technology. e.g. accessed a dB, an peer to peer protocol request was sent.

**Attack**
- Attack
- SQL Injection
- Denial of Service
- Security events that been identified by correlation and analysis tools as malicious activity attempting to collect destroy information – e.g. SQL Injection, denial of service.

**Incident**
- Incident
- Sev 1: Successful Attack
- Attacks and/or security events that have been reviewed by and expert human analyst and have been deemed necessary for deeper investigation or corrective action. Declaring an incident is a big decision made by several stakeholders.
3rd Party Security Services

How MSS detects attacks

- **Events are collected from customer devices**
  - Logs from firewalls and network devices
  - Alerts from products such as IDS, SEP, DLP, etc

- **MSS stores the logs and sends them to analytics**
  - Default storage period is 90 days

- **MSS analytics engines detect specific kinds**
  - Scans
  - Malicious URLs
  - Alerts
  - Hot IPs
  - Malicious Code
  - Brute Force Attacks
  - Suspicious Ports
  - Anomalous Traffic
3rd Party Security Services

Event triage (assessment phase)

- Narrow down alerts to identify potential incidents
- Research threats using Analysis & Research Console tools
  - Search knowledgebase & review known threat data
  - Query across multiple customer databases for relevant context
  - Perform DNS lookups and external searches
- Publish incident (escalate to customer)
  - In accordance with customer defined escalation rules
What happens during an investigation?

- Incidents are annotated by the SOC analyst and published to the portal where they can be viewed by the customer.
- Customer can view incidents on the portal or via the API.
- For high severity incidents, customers are notified immediately, 24x7.
- Incidents are handled by the customer’s internal CRT, Symantec IR, or a third party.
3rd Party Security Services

How would a customer detect attacks without MSS?

Key Takeaways

- Many organizations start with basic log management functions (log storage & query) and eventually adopt SIEM technology for alerting.

- Log management technology remains a necessary component for forensics and security operations, with or without MSS.

- Many SIEM deployments result in a system that is difficult to manage on an ongoing basis, leading the organization to consider alternatives such as MSS.

- Globally, computing forensic investigation skills are generally limited. Some companies, such as accounting and financial firms, have mature, established and sizable computing and accounting forensic teams that are part of their audit and assurance practices.

Source: Gartner (July 2014)
3rd Party Security Services

**WITHOUT MSS**

Manual correlation and remediation

- Network Security Group
- Endpoint Security Group
- NY State End Point Protection Manager

Determines whether malware is known and SEP has blocked it; verifies whether endpoints are compromised; understands if / where infection has spread

Launches corrective actions

Initiates endpoint actions (clean, block, quarantine, gather forensics, ...)

**WITH MSS**

Automated correlation and remediation

- MSS Advanced Threat Monitoring
- NY State End Point Protection Manager

Automatically analyzes endpoints to:
- Determine whether malware is known & SEP has blocked;
- Verify whether endpoints are compromised;
- Understand if / where infection has spread
- Identifies the malware and blocks IP address

Suspected Malware and alerts MSS Advanced Threat Monitoring

Initiates endpoint actions (clean, block, quarantine, gather forensics, ...)

Network Security Group

Endpoint Security Group

NY State End Point Protection Manager
Incident Response (IR) Defined

**Incident Response** is an *organized approach* to addressing and managing the aftermath of a security breach or attack (also known as an *incident*).

The goal is to handle the situation in a way that limits damage and reduces recovery time and costs.
Incident response (IR) is a multifaceted discipline. It demands capabilities that require resources from several operational units in an organization. One example is shown below.
Incident Response

The IR Process & Desired Outcomes

1. Improve Response Times
2. Lower Response Costs
3. Improve Response Effectiveness
4. Enable Continuous Improvement
Incident Response

A Real World Example

- Indicators of Compromise
  - Adversaries
  - Insiders
  - Campaigns
  - Log & Event Data
  - Malware Analysis
  - Tools & Tactics

Cyber Intelligence

Incident Response & Remediation

Preparation

Detection & Analysis

Containment, Eradication & Recovery

Post-Incident Activities

Shift from high-cost and reactive to programmatic and proactive

Prepare for, assess, contain, and remediate incidents quickly

Build and refine a robust Incident Response program
Cyber Team Readiness

Organizations are Fighting an Asymmetric Battle

Cyber security top IT skills shortage for 4th year in a row*

Preparation—lack of hands-on experience

Organizations uncertain of cyber-readiness

Seemingly limitless resources

Sophisticated, multi-stage attacks

Attacker tactics constantly morphing
Cyber Team Readiness

Security Simulation Strengthens Cyber Readiness

- Cloud-based, web-enabled virtual training experience
- Live-fire simulation of multi-staged, advanced targeted attack scenarios
- Players assume the identity of their adversaries to learn motives, tactics and tools
- Hands-on experience
Security Simulation strengthens cyber-readiness through live-fire simulation of today’s most sophisticated advanced targeted attacks

**THINK LIKE AN ATTACKER**

- Cloud-based, virtual training experience simulates multi-staged attack scenarios allowing players to take on the identity of their adversaries
- Gamification provides a more engaging, immersive educational experience
- Frequent scenarios updates ensure team stays current on latest adversaries, motives and techniques
- Scenarios imparts knowledge gleaned from Symantec security experts and threat analysis and current threat landscape

**ASSESS AND DEVELOP YOUR TEAM**

- Leaders and participants receive in-depth security skill assessments
- Provides structured recommendations for cybersecurity skill development
- Identify gaps in team coverage and assess skills of new-hire candidates
Conclusion