James Robinson
Director, Information Security
Accuvant Office of the CSO
Email:james.robinson@accuvant.com
Team Email: CSO@accuvant.com
Linkedin:  
ww.linkedin.com/pub/james-robinson/5/779/697/
Twitter: @0xJames

Stephen O'Connor
Technical Consultant
RSA The Security Division of EMC
stephen.m.oconnor@rsa.com
WHY ARE WE HERE?

• Review Methodology
• Apply It To A Known Threat And Threat Actor
• Understand Position Against Threat
• Put Forward A Strategy You Can Adopt
• Take A Look At An Operating Model Which Can Drive A Data-drive Security Posture.
METHODOLOGY

OVERVIEW

1. Determine Assets
2. Understand Actors
3. Understand Position
4. Build Strategy
5. Begin to Operate with Data Intelligence
6. Monitor and Change for a Better Position
ASSETS AND ACTORS
# Intel Threat Agent Library_07-2202w.pdf

## ACTORS

![Table Image]

*Source: Intel IT Threat Assessment Group, 2007*
## Inside Actors

- **Reckless Employee**
- **Untrained Employee**
- **Disgruntled Employee**
- **Internal Spy**
- **vendor**
- **Thief**
- **Government Spy**

![Source: Intel IT Threat Assessment Group, 2007](image-url)
ASSETS AND ACTORS (EXAMPLE)

Edward Snowden and the NSA Leak

\[ \Delta V = \sum [(P_x - P_y) \times W_n] \]
INSIDER THREAT ATTACK PATTERN

TURNING POINT

RECON

PACKING

DATA THEFT

RESURRECTION
“It was more of a slow realization that presidents could openly lie to secure the office and then break public promises without consequence.”

“Excusing the prior administration from investigation wronged the public. It set an example that when powerful figures are suspected of wrongdoing, releasing them from the accountability of law is ‘for our own good.’ That’s corrosive to the basic fairness of society.”

Source: The Washington Post
Snowden may have persuaded between 20 and 25 fellow workers at the NSA regional operations center in Hawaii to give him their logins and passwords by telling them they were needed for him to do his job as a computer systems administrator, a second source said.

Source: Reuters
“Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on.”

Source: The Guardian
“Is it possible to reroute -all- traffic through a remote proxy? By all, I mean traffic such as SMTP as opposed to the standard HTTP/FTP/SSH/Socks. How could you go about doing this (Is special software required)?

That's about it for now... Ultimately, my goal is to further my own understanding of what would be logged at any given point during transmission. I wouldn't want God himself to know where I've been, you know?”

Source: Ars Technica
[The Guardian Editor Alan] Rusbridger said the leak amounted to about 58,000 files and the newspaper had published "about 1%" of the total.

Source: USA Today
COUNTERMEASURE MAPPING

TURNING POINT
- Technology: Security Intelligence
- Technology: Behavioral Analysis
- Process: Rights Management
- Process: On/Off Boarding

RECON
- Technology: Security Intelligence
- Technology: Behavioral Analysis

PACKING
- Technology: DLP
- Technology: Behavioral Analysis
- Process: Incident Response
- Process: Forensics

DATA THEFT
- Technology: DLP
- Technology: Behavioral Analysis
- Process: Incident Response
- Process: Forensics

RESURRECTION
- Process: Incident Response
- Process: Forensics
THREAT POSITION

- **TURNING POINT**
  - Technology: Security Intelligence
  - Technology: Behavioral Analysis
  - Process: Rights Management
  - Process: On/Off Boarding

- **RECON**
  - Technology: Security Intelligence
  - Technology: Behavioral Analysis

- **PACKING**
  - Technology: DLP
  - Process: Incident Response

- **DATA THEFT**
  - Technology: DLP
  - Technology: Behavioral Analysis
  - Process: Incident Response

- **RESURRECTION**
  - Technology: Behavioral Analysis
  - Process: Forensics
  - Process: Forensics
INSIDER THREAT TECHNOLOGY ARCHITECTURE

Internet

Off Host

Behavioural Intelligence

SIEM

Forensics

On Host

Corporate Workstation

Mobile Computer

Personal Mobile Device

Network DLP

Web Gateway

Web Gateway

Cloud DLP

IAM

PAM

DAM

Host DLP

IAM

PAM

DAM

Host DLP

Container

Data

People

Data

People

Data

People
<table>
<thead>
<tr>
<th>Base Capabilities</th>
<th>Level 1 Capabilities</th>
<th>Level 2 Capabilities</th>
<th>Level 3 Capabilities</th>
<th>Level 4 Capabilities</th>
</tr>
</thead>
</table>
| • Have ownership and support for program
• Have resource(s) that can run the program
• Have resource(s) that can perform analysis and investigations
• Be able to determine critical data
• Be able to determine users that have access to critical data
• Be able to proactively identify how insiders will attack. | • Have a program steering committee for directions and updates
• Have a policy
• Execute an education and communication plan for organization
• Have a source of leads (internal)
• Have tooling to support base response capabilities
• Have internal incident response process | • Evaluation of program for additional capabilities and tooling
• Have external IR flows (legal council, law enforcement engagement, Public Relations)
• Track training delivery to org.
• Be able to identify users in higher risk situations
• Test incident response process and update | • Have training for higher risk personnel (briefing and debriefing)
• Be able to get leads from external sources
• Have contractual obligations for 3rd parties
• Include insider threat modifications for mergers and acquisitions
• Be able to track trends of incidents and attacks | • Optimize and adjust program based on trends
• Have 3rd parties participate in intelligence, response, and other program activities
• Provide business intelligence |
BUT WAIT, I WORRY ABOUT ADVANCED ACTORS.

Patterns analysis shows external actors become internal…that is their goal!
# Pattern and Analysis

*When the attacker becomes an insider.*

## Actors and Motivations:
- Hacktivists
- Criminal Orgs
- State Sponsored

<table>
<thead>
<tr>
<th>RECON</th>
<th>LURE</th>
<th>Exploit Executed</th>
<th>Inject Through Backdoor</th>
<th>Establish Command and Control</th>
<th>Explore and Move</th>
<th>DATA THEFT</th>
<th>Mutation</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Recon Icon]</td>
<td>![Lure Icon]</td>
<td>![Exploit Executed Icon]</td>
<td>![Inject Through Backdoor Icon]</td>
<td>![Establish Command and Control Icon]</td>
<td>![Explore and Move Icon]</td>
<td>![Data Theft Icon]</td>
<td>![Mutation Icon]</td>
</tr>
</tbody>
</table>
PATTERN AND ANALYSIS
Attacker becomes an insider.

ACTORS and MOTIVATIONS:
- Hacktivists
- Criminal Orgs
- State Sponsored
CALL TO ACTION: CHANGE OUR APPROACH

Shift Your Resources and Focus

Detective
Preventative
Reactive
Response
Intelligence
Visibility
Prevention

RSA
THREAT PROGRAM

1. Drive for Operational Intel Focus (SecOps)
2. Define Security Metrics and KPIs (SecOps and GRC)
3. Document Attack Maps and Patterns Analyze Data against Control (SecOps and Architecture)
4. Understand Position and for Plan (Architecture)
5. Implement Plan and Feed Ops (GRC, Architecture, Design, Implementation)
6. Program Begins Again
### HOW TO APPLY WHAT YOU HAVE LEARNED

#### Within three months, you should:
- Green check mark
  - Understand your threat models
- Green check mark
  - Map out the best controls for the threats
- Green check mark
  - Understand your position

#### Beyond three months, you should:
- Green check mark
  - Review your threat models and see if it is changing
- Green check mark
  - Identify maturity steps in your program
- Green check mark
  - Establish your strategy and start to communicate with Sr./Executive Management.