BUILDING TRUST

ROLE OF CYBER SECURITY IN CIVIL PROTECTION

Mo Cashman
Director, Global Defense Solutions
McAfee
What builds Trust?

- RESILIENCE
- TRANSPARENCY
- GOVERNANCE
WHY RESILIENCE?
What is Resilience?

RESIST FAILURE

RAPID RESPONSE

SURVIVABILITY
Stakeholders:
- Government
- Industry
- Service Providers
- CERTs
- Standards Orgs
Smart Grid Challenges

- Scale
- Life Cycle
- Culture
- Data Privacy
- Standards
Current Grid Environment
Resilience (Cyber) Framework

- Design Government Strategy
- Develop, Enforce Controls Standards
- Generate Awareness
- Multi-Zone Defenses
- Cyber Operations
- Monitoring, Analytics and Control
- Intelligence-Driven Response
- Visibility
- Integrated Decision Support Systems
Protected Environments

- Enterprise Environment
- Operations Environment
- Supply Chain Environment
How important is Response?

6-9 months is average time an adversary maintains a presence on the network before they are detected.
What’s important in a Crisis?
### Response OODA Loop

<table>
<thead>
<tr>
<th>OBSERVE</th>
<th>Detect that an incident occurred</th>
</tr>
</thead>
<tbody>
<tr>
<td>ORIENT</td>
<td>Rapid Analysis and Comprehension</td>
</tr>
<tr>
<td>DECIDE</td>
<td>Validate with Intelligence &amp; Context</td>
</tr>
<tr>
<td>ACT</td>
<td>Find, Contain, Fix and Prevent</td>
</tr>
</tbody>
</table>
Speed = Survivability

How fast can we *FIND, CONTAIN* and *FIX* a security breach to contain damage?

How fast can we *ACQUIRE and INTEGRATE* new capability to maintain safety?
Intelligence is Critical

- Integrated intelligence and analytics allowed JSOC to increase hunt missions from a few a week to multiple per night
TERRORIST, INSURGENT

BOMB MAKER

SUPPLY CHAIN COMPONENTS

PAYLOAD

SELF PROTECTION

DISTRIBUTION NETWORKS

COMMAND AND CONTROL

IMPACT
CRIMINAL, SPY
MALWARE AUTHOR
SUPPLY CHAIN COMPONENTS
PAYLOAD
SELF PROTECTION
DISTRIBUTION NETWORK
COMMAND & CONTROL
IMPACT
Roles of Intelligence

1. Prevent Something Bad from Happening
   *Proactive Defense*

2. Find Something Bad Inside the Network
   *Incident Response*

3. Find The Bad Guy
   *Root Cause Investigation*
Agile Intelligence Sharing

**Analog**
“Speed of Paper”

**Digital**
“Speed of the Network”
Barriers to Intelligence Sharing

Politics

Standards

Governance

Classifications
Summary of Key Points

- Stakeholders
- Trust
- Standards
- Resilience