

Ignorance isn't bliss – it's expensive

Including business in the incident
response & management program

Edward B. McCabe, CGEIT, CISM
Director, GRC Services
www.proteus-ocm.net
ebmccabe@proteus-ocm.net



Who is Edward McCabe?

- CISM
- CGEIT
- Information Security Management Consultant
- Veteran of U.S. Navy
- Computer Security Enthusiast
- Volunteer/Contributor
- Buckeye



HACKERS FOR CHARITY.ORG



Software Engineering Institute

Carnegie Mellon

Overview

- Defining the IR Program
- IR Operations
- Business Integration
- Engaging The Business
- Setting Realistic Expectations
- Incident Response Service Offerings



What is an Incident Response & Management Program?

- It depends...
- The goal of an Incident Response and Management Program depends on the types of services offered and the expectations of the business constituency that you're supporting.



Incident Response in Operation

- Cost-effective
- Business focused
- Efficient
 - Training
- Repeatable
- Predictable



Okay, so what is an Incident then?

- It depends...
- An incident is an event that impacts the business and jeopardizes an organizations information or assets.

An unplanned event that can cost the business money.



Example Incidents

- Website defacement where the business wants to go after the offender
- A employee is suspected of surfing inappropriate web sites at work
- A virus infection on the local network
- A spear-phishing attack
- Someone driving a forklift through the walls of your data center and stealing the servers
- An external hardwired network intrusion
- An external wireless network intrusion



Decomposing “not so similar” similar Incidents

- External Hardwire Network Intrusion
- External Wireless Network Intrusion



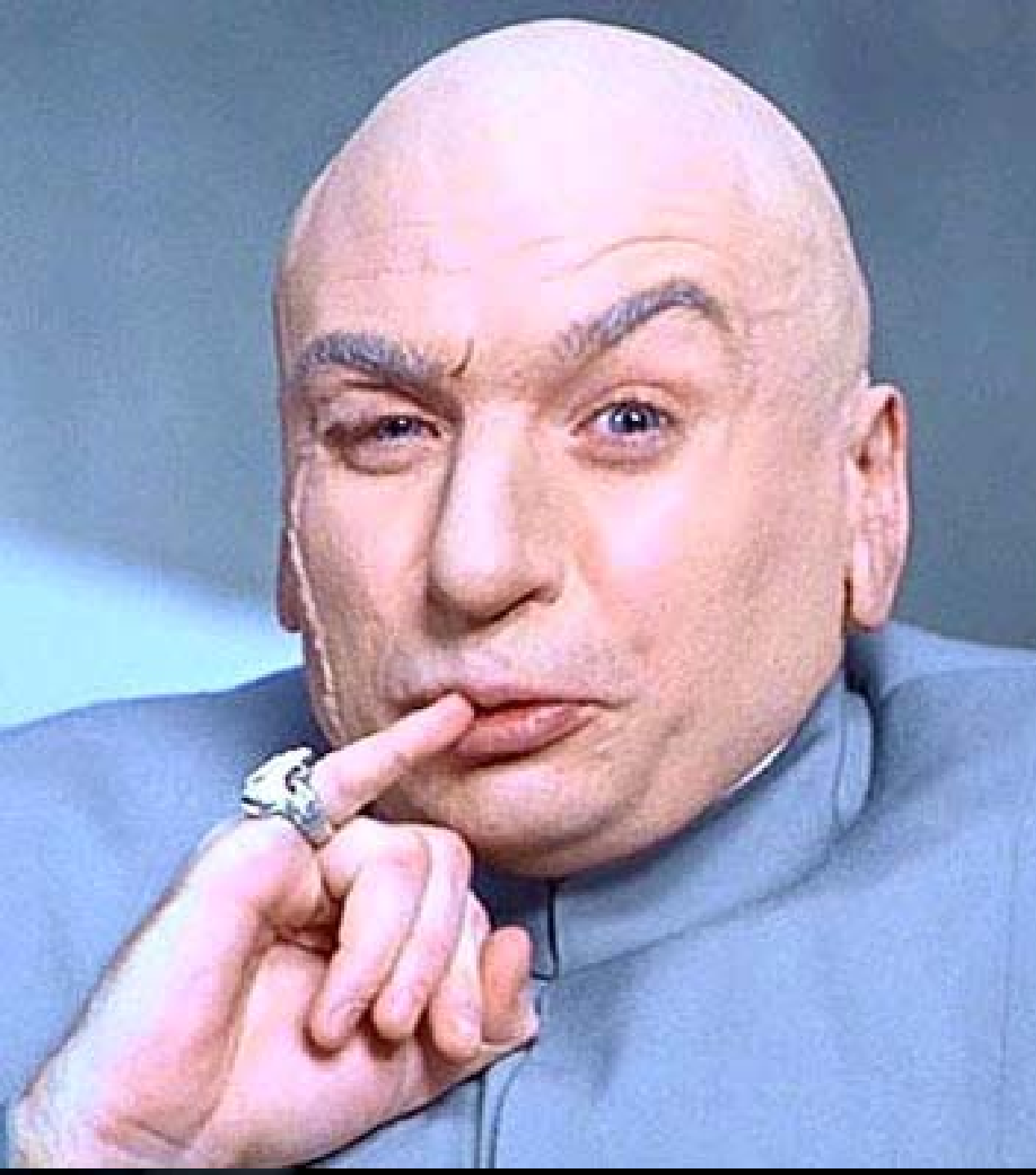
Ext. Hardwire Network Intrusion

- So the call comes in
“Hey Bob, this is Tom up in Network Operations Center. We’re seeing a lot of network traffic going overseas and we’re trying to figure out why this one server is pegging at nearly 100% resource utilization, anyways we want you to look into it for us. I’m concerned we may have been breached.”
- *Cry “Hacker” and let slip the dogs of Incident Response!*





- Your team identifies the vulnerable system, how it was exploited, pulls the logs from the centralized log server, performs a legally admissible digital duplication, conducts a thorough forensic analysis of the system and determines it is being used as the personal MP3 server for someone who you are able to identify living in Kreplachistan.
- The IR team recommends to patch the system and return the system to proper business use.




Dr. Evil, one of your more common script kiddies, not bright enough to pull off a serious hack, but a pain none the less.


Ext. Wireless Network Intrusion

- So yet another call comes in...
“Hey Bob, this is Tom up in NOC. Looks like we have another network intrusion. One of our stores in Hawaii is having some odd activity. Its one of the stores that offers wireless. We’re seeing some activity and think that it is targeting the POS systems directly. Why do I think that? The admin account has been changed and we can’t remote access it. Can you guys take a look at it for us?”



- 
- Your team starts to go into action and you submit your request for some new wireless equipment and tickets to Hawaii.
 - You discover that Corporate decided to “save money” by tying the wireless network to the same network as their POS systems.
 - The decision is made to continue the practice of “saving money” by denying your request and having a local IT company “Wipe & Reload”

6 months Later... ..with the C-Suite



“Bob, I thought the CSIRT handled network intrusions? Can you tell me how this ‘Hawaiian Hackers’ group was able to get all the way into our corporate systems and to our customer Credit Card Database? We’re facing fines, our stock has dropped, we’re in the news almost every night, and we’re losing customers quicker than Frosty the Snowman melting in Bermuda. What happened?”

You pull your incident report from 6 months ago and explain the technical details of what most likely happened .

Take-away's

- Not all incidents are the same, even when they are related
- *Prior Proper Planning Prevents Poor Performance*
- Business trumped IT, both in:
 - **Technical Architecture**
 - **Incident Response**
- Business Expectations were not level set
 - **C-Suite assumed that the CSIRT handled all network intrusions**



Integrating the business within the Incident Response Program

- The business is why the organization exists
- The various lines of business have different needs
- The various lines of business have different levels of organizational influence



Who should we include?

- Legal/General Counsel
- Human Resources
- Public/Media Relations
- Investor Relations
- Business Owners
- Mid & Senior Management
- End-users



How to Engage the Business

- IR Business Leadership Committee
- IR Meetings
- One on One
- Role-Playing



Setting Realistic Expectations

- An Incident Response Program is many things to many people
- Business should drive the services offered by the Incident Response Program



Building an IR Program

- Gathering Information
- Establishing the IR Framework
- Defining Service Offerings
- Organizational Structuring
- Identifying Needed Resources
- Developing an Implementation Plan
- Implementation
 - Training
- Operations



Types of IR Programs

Reactive

- **Focused Response Efforts**
- **Rapid, standardized & coordinate response efforts**
- **Functional Knowledge Base**

Proactive

- **Enables Business Goals**
- **Provides authentic risk data & Business Intelligence**
- **Promotes Situational Awareness**



Ranges, Services & SLA's

- What range of services should the IR Program offer?
 - Reactive
 - Proactive
 - Security Quality Management



Common IR Services

Reactive Services	Proactive Services	Security Quality Management Services
<p>Alerts & Warnings</p> <p>Incident Handling</p> <ul style="list-style-type: none">- Incident Analysis- On-site Incident Response- Incident Response Support- Incident Response Coordination <p>Vulnerability Handling</p> <ul style="list-style-type: none">- Vulnerability Analysis- Vulnerability Response- Vulnerability Response Coordination <p><i>Materials provided courtesy of the Software Engineering Institute.</i></p>	<p>Announcements</p> <p>Technology Watch</p> <p>Security Audit & Assessments</p> <p>Configuration & Maintenance of Security Tools, Apps & Infrastructure</p> <p>Development of Security Tools</p> <p>Intrusion Detection Services</p> <p>Security-Related Information Dissemination</p>	<p>Risk Analysis</p> <p>Business Continuity & Disaster Recovery Planning</p> <p>Security Awareness</p> <p>Awareness Building</p> <p>Education/Training</p> <p>Product Evaluation</p> <p>Systems Certification & Accreditation</p>

IR Service Level Agreements

- **Have Severity Levels Defined**
 - Effective & efficient triage is the key to success!
- **It is important to follow-through with the lines of business you support**
 - Don't forget to follow up
 - Speak only to the facts
 - Speak only to whom you're supposed to
 - Work on building trust and credibility
- **Know the IR Programs limitations**
 - Don't attempt to take on a incident the IR Team is not suited to support



Sample Triage & Impact Schedule

	Type I	Type II	Type III
Confidentiality	<p>Attempted access to restricted area (Failed login attempts).</p> <p>Copying data from one security zone to a lower security zone (i.e., records from a database to shared drive).</p>	<p>User by-passes existing security controls to access restricted area.</p> <p>User installs network sniffing software on their system.</p>	<p>Unauthorized Access:</p> <ul style="list-style-type: none"> * External, unauthorized 3d party accessing database(s). * External, unauthorized 3d party accessing network resources.
Integrity	<p>Incorrect data entered into system (Accidental).</p> <p>Restoring incorrect data from backup to production systems.</p>	<p>Internal, unauthorized access to restricted area (by-pass security control).</p> <p>Users installs password cracking software on system.</p>	<p>External, unauthorized 3d party access to network environment.</p>
Availability	<p>Power supply failure (Router/Switch/Server) to a non-business critical system</p> <p>Loss of failover upstream provider (backhoe syndrome)</p>	<p>Power supply failure (Router/Switch/Server) to a business critical system.</p> <p>User introduces malware into the network environment.</p> <p>User creates/causes a denial of service on a network resources.</p>	<p>External, unauthorized 3d party accessing database records or network resources.</p> <p>Active Distributed/Denial of Service Attack.</p> <p>ISP fails to provide data communications within agreed upon SLA timeframes.</p>

In Review

- Business Integration
- Engaging The Business
- Setting Realistic Expectations
- Incident Response Service Offerings





QUESTIONS?

Resources for IR Programs

- FIRST/Forum of Incident Response and Security Teams – www.first.org
- US/CERT – www.uscert.gov
- DOD/CERT – www.cert.mil
- CERT/CC – www.cert.org
- Georgia Tech CERT - <http://www.oit.gatech.edu/service/incident-response/incident-response>
- The rather portly guy giving the presentation



Edward McCabe, CGEIT, CISM

Office: (877) 283 1501 Ext 706

ebmccabe@proteus-ocm.net

www.proteus-ocm.net

www.linkedin.com/EdwardMcCabe



PROTEUS | OCM