NORTHERN NEW ENGLAND
SCHOOL OF BANKING

MONARCH ISC
INFORMATION SECURITY CONSULTING

John Hill Rogers, CISSP
john@monarchisc.com
Senior Consultant

Incident Management

Moving from Computer Incident Response to Organizational Intelligence

MONARCH ISC
INFORMATION SECURITY CONSULTING

Session Agenda

- Module 1:
  - Some Scenarios Beg the Question(s)
  - Some Questions that Beg for Answers
  - Incident Management Job Description
  - Preparation & Practice
- Module 2:
  - Incident Response Exercise

MONARCH ISC
INFORMATION SECURITY CONSULTING

True?

"It takes many good deeds to build a good reputation, and only one bad one to lose it."

— Benjamin Franklin

MONARCH ISC
INFORMATION SECURITY CONSULTING

Corrected

"It takes many good deeds to build a good reputation, and only one poorly managed bad deed to lose it."

— Some other guy

MONARCH ISC
INFORMATION SECURITY CONSULTING

Some Scenarios Beg the Question(s)

MONARCH ISC

Some Scenarios that Beg the question

1. Customer allows remote access with single-factor authentication only.
   - Successful phishing attack, fraudster takes control of CFO's PC
   - Changes payroll routing information for 10 employees
2. Customer falls for Microsoft Support fraud pre-texting call
   - Fraudster impersonates Bank customer service in a conference call
   - "Bank Customer Service Rep" recommends customer buy support package
   - Customer pays $1,200 for fraudulent support contract
3. Commercial lender accidentally sends entire commercial loan database/spreadsheet to the wrong "Steven Thomas" who happens to be a list salesman in Florida.

MONARCH ISC
INFORMATION SECURITY CONSULTING

Other Scenarios that Beg the question

- “Whaling” or “Whale Phishing”– An exploit spoofing executive email used to request transactions or actions to serve the perpetrator.
- Insider theft of customer information
- Compromise of a hosted POS system
- Disruption of service at vendor’s data center
- Social Engineering : On-site or customer & network phone pretexting

MONARCH ISC
INFORMATION SECURITY CONSULTING

The Questions

- Why is IT still considered the most important part of Incident Management?
- Why do tactics/procedures often drive Incident Response planning?

MONARCH ISC
INFORMATION SECURITY CONSULTING

Questions that Beg for Answers

MONARCH ISC

Questions that Beg for Answers

1) What is the process at your organization for obtaining, analyzing, and sharing threat intelligence?
2) Who manages your threat intelligence feeds?
3) Should the threat of malware have any impact on user browsing activity?
4) What are your social media controls? Do you review user posts prior to publishing? Are you alerted when there is a post? Can you tell how many shares and views?
5) What are your procedures for risky transactions/functions?
6) How do you manage accidental disclosure of sensitive/protected data?
7) Do you have scripts, outgoing messages, web-site specific messages pre-written, pre-recorded, and/or pre-configured?

MONARCH ISC
INFORMATION SECURITY CONSULTING

Questions that Beg for Answers

9) Would you pay the ransom?

10) Do you have a Bitcoin Account?

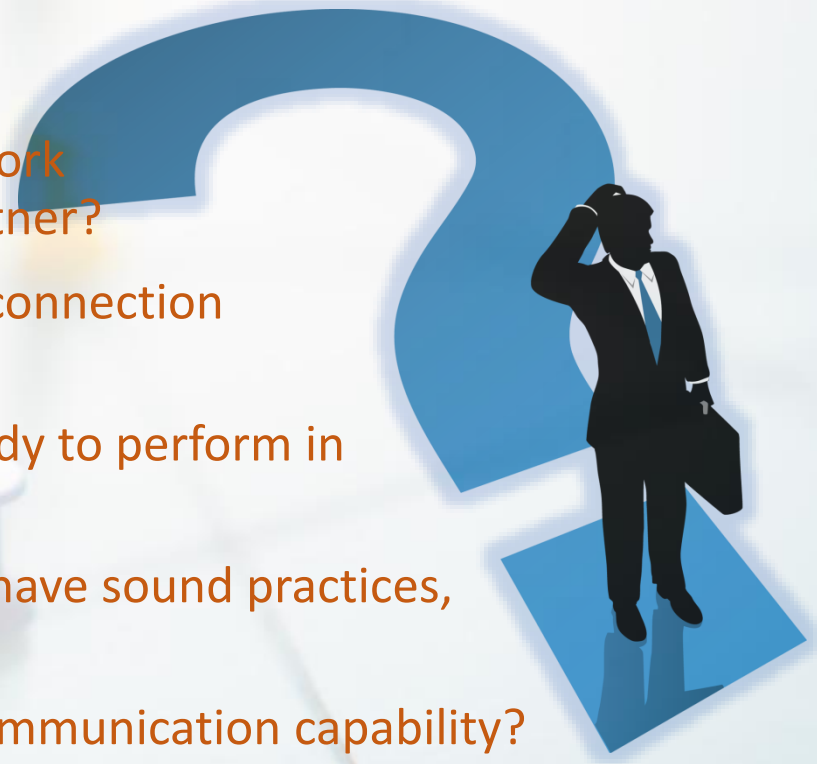
11) Do you know when to contact and work with your insurer? Your forensics partner?

12) Do you have data flow and external connection diagrams/maps with all end-points?

13) Is each member of your IRT truly ready to perform in their role, with its responsibilities?

14) Are you confident your TSP/Vendors have sound practices, and are some required by contract?

15) Do you have an internal broadcast communication capability?
    - Is it capable of enumerating responses?



MONARCH ISC
INFORMATION SECURITY CONSULTING

Incident Management Job Description

MONARCH ISC

Incident Management Job Description

Your Organization: Required Skills and Experience

- Expert leadership
- Expert operations
- Expert legal counsel
- Expert internal communications, written and verbal
- Expert Information Technology design, engineering, and administration
- Expert analysis and investigation
- Expert customer service and public relations
- Expert learner
- Expert trainer
- Expert relationship builder

MONARCH ISC
INFORMATION SECURITY CONSULTING


THIS IS TOO
MUCH
IT Professional

Incident Management Job Description

IT Professional: Required Skills and Experience

- Expert leadership
- Expert operations
- Expert legal counsel
- Expert internal communications, written and verbal
- Expert Information Technology design, engineering, and administration
- Expert analysis and investigation
- Expert customer service and public relations
- Expert learner
- Expert trainer
- Expert relationship builder

MONARCH ISC
INFORMATION SECURITY CONSULTING

Strategy & Tactics

MONARCH ISC

Strategy & Tactics

"Strategy is doing the right things. Tactics are doing those things right." - Anonymous

MONARCH ISC
INFORMATION SECURITY CONSULTING

Strategy & Tactics

"Strategy is doing the right things. Tactics are doing those things right." - Anonymous

MONARCH ISC
INFORMATION SECURITY CONSULTING

Strategy & Tactics

Strategic:

- ✓Foresight
- ✓Long-term goals and objectives
- ✓Big picture
- ✓Holistic
- ✓Integrated
- ✓Plan

Tactical:

- ✓Immediate
- ✓Short-term goals and objectives
- ✓Small picture
- ✓Situational
- ✓Segregated
- ✓Procedure

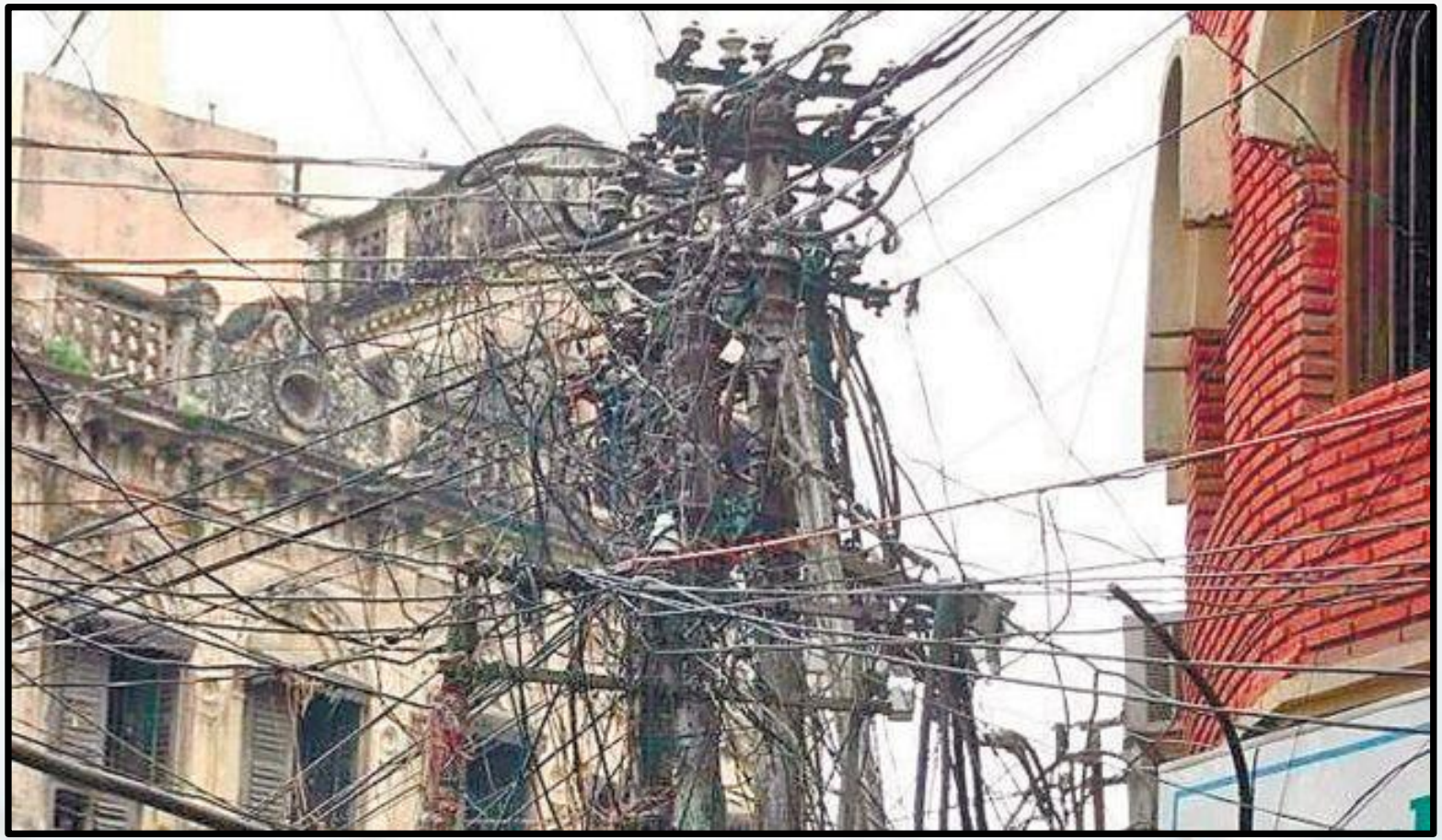
MONARCH ISC
INFORMATION SECURITY CONSULTING

Strategy & Tactics

If tactics aren’t executed in support of a good strategy, here’s what happens….

MONARCH ISC
INFORMATION SECURITY CONSULTING

Tactical-Based Governance



MONARCH ISC
INFORMATION SECURITY CONSULTING

Preparation & Practice

MONARCH ISC

Preparation

“Failing to prepare, is preparing to fail.”

MONARCH ISC
INFORMATION SECURITY CONSULTING

Preparation

- Incident Management Plan
- Response Team
  - Build the team to the strategic resume of required skills and experience. Know your people!
  - Cross-departmental – whole organization
- Training specific to each role
- Mentoring & institutional memory
- Runbooks for Common Incident Types
- Internal communications plan
  - Call trees with contingency contacts
  - Contact information
  - Consistency across departments

MONARCH ISC
INFORMATION SECURITY CONSULTING

Preparation

- External communications plan
  - Develop scripts for customer service
  - Auto-attendant and outgoing messages
  - Web site pages
  - Understand applicable disclosure laws
  - Craft the messaging across all media
  - Assign messengers
- Information Technology
  - Redundancy and fault tolerance
  - “air gap” backups
  - Network segmentation
  - Application white-listing

MONARCH ISC
INFORMATION SECURITY CONSULTING

Practice

“You can’t think your way into playing the piano.” – Me, just now

MONARCH ISC
INFORMATION SECURITY CONSULTING

Speaking of Practice: IR Exercise

MONARCH ISC