2017 NYS Cybersecurity Conference

Incident Management

Moving from Computer Incident Response to Organizational Intelligence

Presented by:
John H Rogers, CISSP
Manage of, Professional Services
john.rogers@sagedatasecurity.com

sage DATA SECURITY

Agenda

- Some Scenarios Beg the Questions
- Some Questions Beg for Answers
- Expertise & Experience: How's Your Organization's Incident Management Resume?
- Preparation & Practice
- Continuity of Operations Planning: Unifying Response Strategies

sage DATA SECURITY

True?

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

– Benjamin Franklin

Amended

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

– Some other guy

Scenarios That Beg The Question(s)

FINANCIAL SERVICES ISAC | *Cyber Incident*

FS-ISAC Green: Recipients may share FS-ISAC GREEN information with peers, trusted government and critical infrastructure partner organizations, and service providers with whom they have a contractual relationship, but not via publicly accessible channels.

Title:

Health insurer Premier HealthCare Announces Cyberattack

Type of Incident:

Data Breach

Summary:

Premier HealthCare announced on Tuesday, March 17, 2014 that it was a victim of a cyberattack that may have exposed medical data and financial information of 11 million customers.

It said the attackers may have gained access to claims data, including clinical information, along with banking account numbers, Social Security numbers, birth dates and other data…

Premier HealthCare has published a website to communicate the latest information on the attack: http://www.premupdate.com. Premier HealthCare is working with the FBI to investigate the attack.

The FS-ISAC will continue monitoring the situation, and will share any additonal information as it becomes available.

Description:

You should be aware that you may receive scam and phishing emails claiming to be from Premier HealthCare. If you receive an email claiming to be related to this attack that appears to be from Premier HealthCare we recommend you take the following steps:

- DO NOT reply to the email or reach out to the senders in any way.
- DO NOT enter any information on any website that may open, if you have clicked on a link in the email.
- DO NOT open any attachments that arrive with email.

Premier HealthCare has established a dedicated call center for our members and other affected individuals to contact. The information involved dates back to 2002 and individuals who believe they are affected by this incident but who have not received a letter by April 20, 2015, are encouraged to call 1-800-768-5817, Monday through Friday, between 5:00 a.m. and 8:00 p.m. Pacific Time (closed on U.S. observed holidays).

Scenarios That Beg The Question(s)

by **Brian Donohue** Follow @TheBrianDonohue

Criminals are injecting malicious redirect code into advertisements in order to route user traffic toward sites hosting the Magnitude exploit kit, which, in turn, infects those users with strains of file-encrypting ransomware.

Magnitude predominately relies on drive-by-download attacks in which it infects its victims by exploiting vulnerable browser plug-ins. Before infection via Magnitude, ZScaler researchers explained in a recent analysis, attackers are using malicious ads, in a scheme commonly known as malvertising, to direct users through "302 cushioning" to sites hosting the Magnitude exploit kit.

Once the user interacts with an infected site, Magnitude delivers a malicious Flash payload as well as a highly obfuscated JavaScript payload

Scenarios That Beg The Question(s)

On Wednesday March 2nd, your CEO receives this email

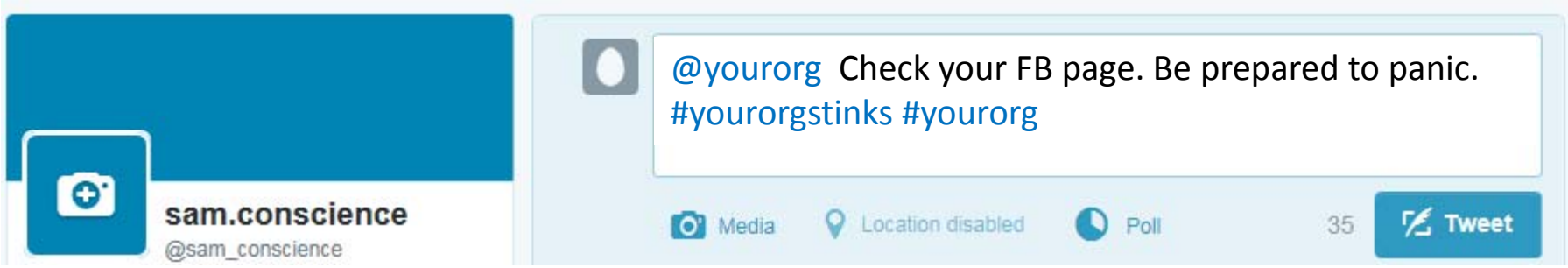
From: The Collective Conscience
Sent: Wednesday March 2nd, 2016 10:14:18 AM
To: CEO
Subject: You should have listened

Mr. CEO,
You should have listened when we asked politely. Now you must pay!
We will announce the consequences of your actions on Facebook and Twitter at 1:30pm today. #Yourorgstinks

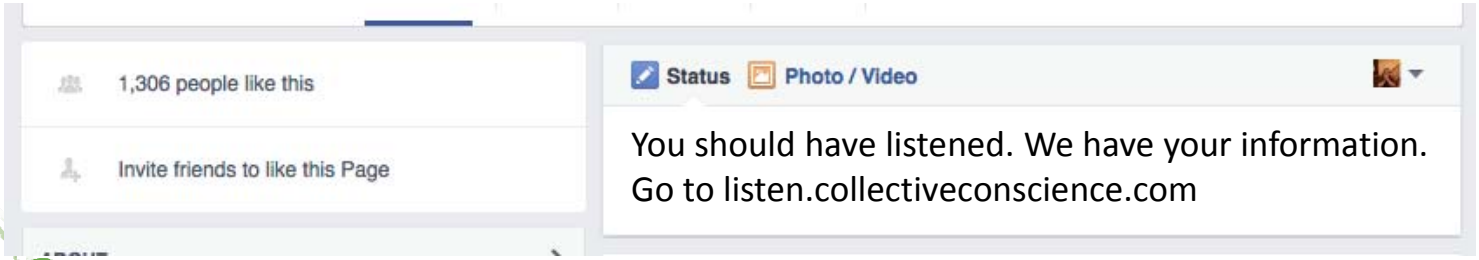
Sincerely,
Sam Conscience
Representative of the Collective Conscience

Scenarios That Beg The Question(s)

At 1:30pm, the following posts appears on the Sam.Conscience Twitter feed



At 1:35pm, the following message is posted by Sam Conscience on the Your Organization's Facebook page.



Scenarios That Beg The Question(s)

In the video at the link, this unsavory person displays a list of what appears to be your customer's protected information.

sage DATA SECURITY

Scenarios That Beg The Question(s)

Mainstream media have latched on to the news and it is spreading like wildfire. The Call Center and Website are flooded

Breaking News: Your Organization hacked by the Collective Conscience.

Other Scenarios That Beg Question(s)

- "Whaling" or "Whale Phishing"– An exploit spoofing executive email used to request transactions or actions to serve the perpetrator.
- Accidental disclosure of sensitive/protected data
- 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

The Questions

- What are the questions these scenarios beg?
- Why is IT still at the center of Incident Management?
- Why do tactics/procedures often drive Incident Response planning?

Some 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?

Some 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 a some required by contract?

15) Do you have an internal broadcast communication capability?

- Is it capable of enumerating responses?

sage DATA SECURITY

Your Incident Management Resume

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

sage DATA SECURITY


THIS IS TOO
MUCH
IT Professional

Your Incident Management Resume

IT Department: 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

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

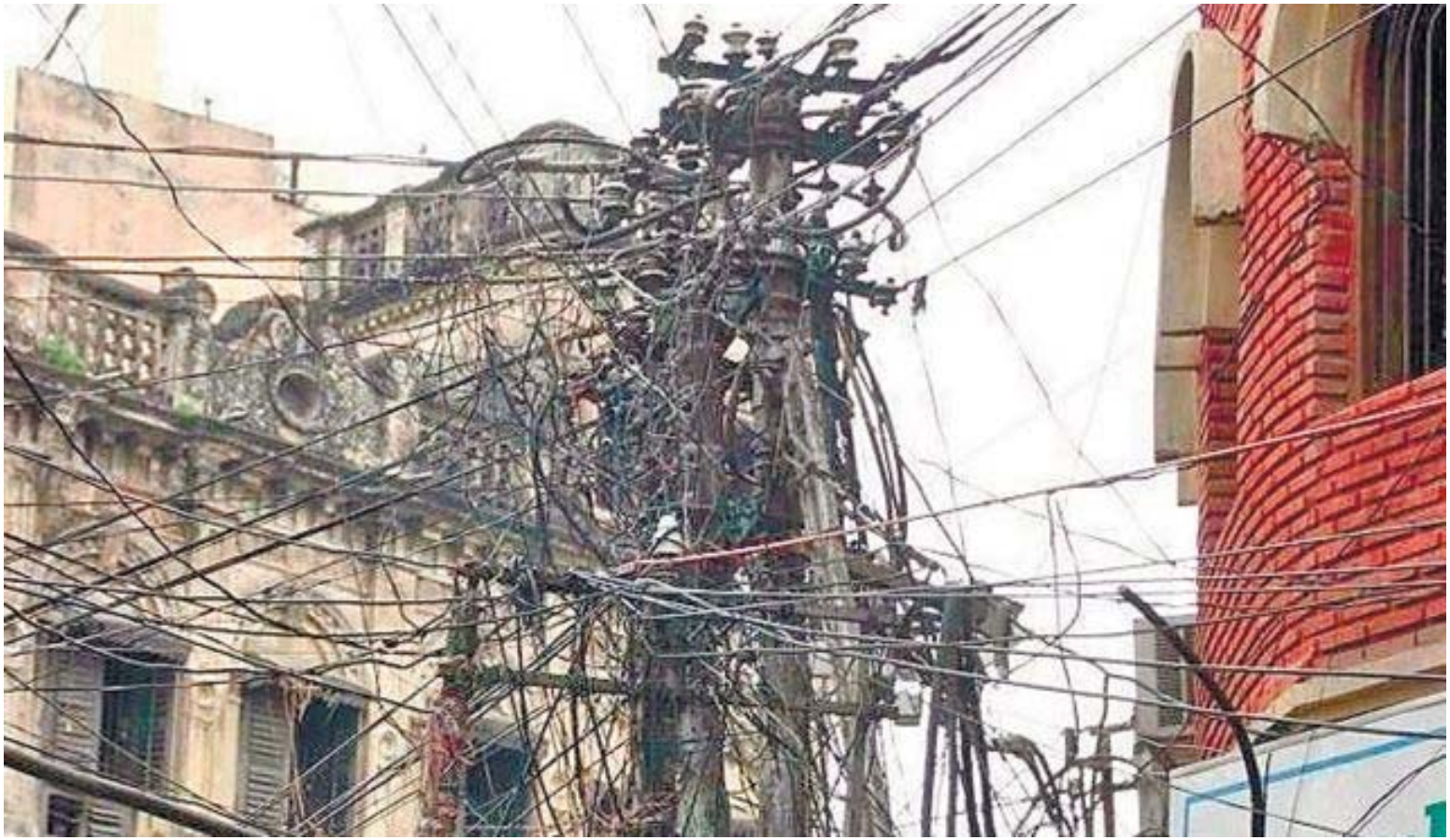
Strategic vs Tactical

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

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

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

Tactical Governance - Result



Strategic

Tactical

Preparation

"Failing to prepare, is preparing to fail."

Preparation

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

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

Practice

"You can't think your way into playing the piano." – Me, just now

Practice

- Testing is not practice, it is testing
  - It is critical to test, but by nature people approach tests differently than practice
  - Training and practice are the way new skills and habits are acquired
  - Ever do well on a test you didn't practice/prepare for?
  - Test results will dramatically improve with practice
- What is practice?
  - To exercise a capability in order to improve without overtly measuring performance (practice inherently reveals the level of preparedness).
  - IT Procedures are a good example of ongoing practice. IT professionals are always practicing some form of response procedure.

Continuity Of Operations (COOP)

- *Unified strategy for event management that consolidates common elements across:*
  - *Disaster Recovery & Business Continuity plans*
  - *Pandemic Plan*
  - *Incident Response Plan*
  - *Aspects of Vendor Management Plan*

Continuity Of Operations (COOP)

- One team
- One decision tree
- One communication plan
- One set of network and data flow documentation
- Sub-plans are implemented tactically as required

Questions & Answers

Thank you for attending!

Presented by:
John H Rogers, CISSP
Manager of Professional Services
john.rogers@sagedatasecurity.com