RESPONSE TO HIGH PROFILE INCIDENTS

Marcus H. Sachs
CSO, Pattern Computer
Organizations prefer to minimize and control public commenting about a data breach or security incident. But what if news of the incident hits the media outlets nearly immediately? How do you quickly develop public statements while simultaneously trying to figure out exactly what happened?

Do you “spin” the story to protect the impacted organization, or do you say, “no comment” and leave everybody guessing?
Incidents impacting critical services require rapid action
- Often the impacted parties are already calling
- Social media starts buzzing
- Reporters call for comments

Are you ready to make a statement?
Massive ransomware attack hits Atlanta, GA

More than a third of 424 software programs impacted
  - 30% were “mission critical”
  - Core city services including police and courts

Cost estimate to repair could go over $10 million
  - Bitcoin ransom request was about $50k
City of Atlanta computer systems dealing with cyberattack; ransom note asks for Bitcoin payment

Posted: Mar 22, 2018 1:53 PM EDT
Updated: Apr 19, 2018 1:52 PM EDT

By WGCL Digital Team

The City of Atlanta is currently experiencing outages on various customer-facing applications, including some that customers may use to pay bills or access court-related information. We will post any updates as we receive them.

OUTAGE ALERT

The City of Atlanta is currently experiencing outages on various customer-facing applications, including some that customers may use to pay bills or access court-related information. Our @ATL_AIM team is working diligently with support from Microsoft to resolve this issue. Atlantaga.gov remains accessible. We will post any updates as we receive them. Thank you for your patience.

ATLANTA (CBS46) - Cyber criminals have waged war on Atlanta after a cyber attack crippled the city's computer systems.

The cyberattack is causing outages on various computer systems. It all started around 5:40 a.m. Thursday morning.
DAY 1 MAYOR’S STATEMENT
DID THE MAYOR SAY THE RIGHT THINGS?

- Press briefing was about 12 hours after the incident started
- Mayor should have used a script rather than just speaking “off the cuff”
- Several unneeded mentions of checking bank statements, credit cards, etc.
- Unsure of response to ransom demands
LEAD STORY ON THE EVENING NEWS

- TV news has few facts to report
- Covers key comments made earlier by the Mayor
- Shows a screenshot of ransomware
  - Reporter has hard time explaining what is going on
  - We will re-visit this screenshot in a moment...
In most incidents, the first report is usually wrong.

As the situation develops, the fog begins to clear.

In this interview, should the title of the Acting CIO include the word “Acting”?
  - What information could this give an adversary?
The mayor is getting regular briefings
Has a better idea of what happened
Still not using prepared remarks
  But much more accurate with off the cuff statements
If you are running a story about malware or a cyber incident, don’t use a computer that is displaying an error message

Channel 46 in Atlanta needs to install a Windows Update

Did you see the error message?
DO YOU SEE IT?
SUMMARY

- Incident started at 5:40 am
- First Tweet at 12:54 pm
- Top news story for several days
- Impact was immediate
  - Affected about 6 million people
- Activity associated with the SamSam ransomware
  - $50k ransom was not paid
Incidents are often discovered by a third party rather than by the victim.

The best outcome is for the victim to have time to notify impacted parties before the media gets notified.

But what happens when the story is “leaked”?
   Or worse, when a reporter is the third party?
Breaking news on a Friday evening

The US power grid was hacked by the Russians!

But what really happened?

Russian hackers penetrated U.S. electricity grid through a utility in Vermont, U.S. officials say

A code associated with the Russian hacking operation dubbed Grizzly Steppe by the Obama administration has been detected within the system of a Vermont utility, according to U.S. officials.

While the Russians did not actively use the code to disrupt operations of the utility, according to officials who spoke on condition of anonymity in order to discuss security matters.
NBC NIGHTLY NEWS REPORT
Seven weeks earlier Donald Trump won the US Presidential elections

Fingers were pointing at Russia for “hacking” the election and causing the election upset

FBI and others were aware of, and were investigating, active Russian hacking
A “Joint Analysis Report” (JAR) was issued one day earlier.

Included a long list of Indicators of Compromise (IOCs).

Over 900 IOCs were provided to critical infrastructure owners/operators on Dec 29

System administrators were asked to review network logs and report findings

One small Vermont utility found a single indicator on a single laptop...
Voluntary Incident Reporting

- We are all familiar with the power of voluntarily shared incident information.
- The SANS Internet Storm Center (isc.sans.org) is the premier place to share your findings!
- Information Sharing and Analysis Centers (ISACs) are also great places to share.
Vermont utility called their ISAC and reported the finding

A security consultant for the utility advised them to also file a report with the Department of Energy

Not mandatory to do so for small utilities

Reporting is supposed to be confidential
## OE-417 Electric Emergency and Disturbance Report - Calendar Year 2016

<table>
<thead>
<tr>
<th>Month</th>
<th>Date Event Began</th>
<th>Time Event Began</th>
<th>Date of Restoration</th>
<th>Time of Restoration</th>
<th>Area Affected</th>
<th>NERC Region</th>
<th>Alert Criteria</th>
<th>Event Type</th>
<th>Demand Loss (MW)</th>
<th>Number of Customers Affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>December</td>
<td>12/28/2016</td>
<td>4:03 AM</td>
<td>12/31/2016</td>
<td>6:00 AM</td>
<td>California:</td>
<td>WECC</td>
<td>Fuel supply emergencies that could impact electric power system adequacy or reliability</td>
<td>Fuel Supply Deficiency</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>December</td>
<td>12/30/2016</td>
<td>8:55 AM</td>
<td>12/30/2016</td>
<td>8:56 AM</td>
<td>Vermont: Chittenden County:</td>
<td>NPCC</td>
<td>Cyber event that could potentially impact electric power system adequacy or reliability</td>
<td>Other</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>December</td>
<td>12/30/2016</td>
<td>2:30 AM</td>
<td>12/30/2016</td>
<td>7:00 PM</td>
<td>Maine:</td>
<td>NPCC</td>
<td>Loss of electric service to more than 50,000 customers for 1 hour or more</td>
<td>Weather or Natural Disaster</td>
<td>Unknown</td>
<td>85253</td>
</tr>
</tbody>
</table>

Russian hackers penetrated U.S. electricity grid through a utility in Vermont, U.S. officials say

By Juliet Eilperin and Adam Entous  December 30, 2018  AP

A code associated with the Russian hacking operation dubbed Grizzly Steppe by the Obama administration has been detected within the system of a Vermont utility, according to U.S. officials.

While the Russians did not actively use the code to disrupt operations, according to officials who spoke on the condition of anonymity to discuss a security matter, the discovery underscores the vulnerabilities of the nation’s electrical grid. And it raises fears in the U.S. that Russia could use the hacking tools to disrupt the electrical system in the future, experts say.

Editor’s Note: An earlier version of this story incorrectly said that Russian hackers had penetrated the U.S. electric grid. Authorities say there is no indication of that so far. The computer at Burlington Electric that was hacked was not attached to the grid.

Russian operation hacked a Vermont utility, showing risk to U.S. electrical grid security, officials say

By Juliet Eilperin and Adam Entous  December 31, 2018  AP

A code associated with the Russian hacking operation dubbed Grizzly Steppe by the Obama administration has been detected within the system of a Vermont utility, according to U.S. officials.

While the Russians did not actively use the code to disrupt operations, according to officials who spoke on the condition of anonymity to discuss a security matter, the discovery underscores the vulnerabilities of the nation’s electrical grid. And it raises fears in the U.S. that Russia could use the hacking tools to disrupt the electrical system in the future, experts say.
“There is no indication that either our electric grid or customer information has been compromised. Media reports stating that Burlington Electric was hacked or that the electric grid was breached are false.”
GENERAL MANAGER SETS THE STORY STRAIGHT
WASHINGTON POST retracted the entire story three days later.

Variations of the incorrect story continued to circulate for several weeks.
Was a Vermont Power Grid Infiltrated by Russian Hackers?

The Washington Post was heavily criticized for jumping the gun and suggesting a Vermont power company had been targeted for disruption by Russian hackers.

CLAIM

A computer infected by malware proved a Vermont power company has been targeted for disruption by Russian hackers.

RATING

MOSTLY FALSE
Incident handling is a process-oriented action plan for dealing with:

- Intrusions, breaches, or malware
- Theft or ransomware
- Denial of Service attacks
- Fire, floods, and other security-related events

Have procedures and policies in place BEFORE an incident occurs
Sooner or later an incident is going to occur
  - Do you know what to do?

It is not a matter of “if” but “when”

Planning is everything

Similar to backups
  - You might not use it every day, but if a major problem occurs you are going to be glad that you did
THE SIX PRIMARY STEPS OF INCIDENT HANDLING

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons Learned

Steady State

Create your own memorization tool
SEVEN DEADLY SINS — CHRONOLOGICAL ORDER

- Failure to report or ask for help
- Incomplete/non-existent notes
- Mishandling/destroying evidence
- Failure to create working backups
- Failure to contain or eradicate
- Failure to prevent re-infection
- Failure to apply lessons learned
INCIDENT PREPARATION

- First step in the incident handling process
- Too late to prepare once the incident has started
- More than just technical preparation (patches, passwords, perimeter, etc.)
  - Policies
  - Communications plans
Establish an organizational approach to incident handling

Decide generally how you will handle the “big issues” up-front
  - Notify law enforcement or maintain secrecy
  - Contain and clear OR watch and learn
    - Pre-authorization to contain

Get management/legal buy-in and sign-off!
Establish a policy for outside "peer" notification

Establish a policy for dealing with incidents involving remote computers that belong to
- Your company
- Your employees
- Contractors and other non full-time employees
PREPARATION:
POLICY – PUBLIC NOTIFICATION

- Establish a policy for notifying the public
  - Maintain control of the message

- Establish a policy for dealing with incidents involving customer data and information
  - Be mindful of breach notification laws
  - New privacy laws require rapid notification
PREPARATION: EMERGENCY COMMUNICATION PLAN

- Develop an Emergency Communications Plan
  - Create a call list and establish methods of internally informing people quickly
  - Create an incident notification call tree
  - Test your call list and tree to make sure it works

- External communication includes your website as well as social media

- You MUST be in charge of your message
Learn from this experience, so you won’t get caught unprepared the next time an incident occurs.

Review the incident from start to completion and identify areas where you can improve.
- Then make the improvements, and don’t just admire your list!

Final meeting and report
AN EPIC EMERGENCY RESPONSE

- Imagine that you are a small town
- Your city gets hit with a ransomware attack
- Everything comes to a stop
  - City services
  - Utility billing
  - Library
- What do you do?
MATANUSKA-SUSITNA, ALASKA
QUESTIONS

Marcus H. Sachs
CSO, Pattern Computer

marc@sans.org