SANS ICS Security Summit 2019

Data Breach Notification

Critical Infrastructure Protection

Bryan Owen PE
OSIsoft - Principal Cyber Security Manager
bryan@osisoft.com
@bryansowen

15 years process control engineering
20+ years focused on OSIsoft PI System

Affiliations
• ICSJWG Industry Steering Team
• ISA99 Voting Member
• AFPM Cybersecurity subcommittee
• CRED-C Industry Advisory Board
Agenda

• Not all data breaches are equal
• Notification complexities
• Before reporting a breach
• Lessons learned
• Pay it forward
Accident Investigators

U.S. Chemical Safety and Hazard Investigation Board

National Transportation Safety Board
Airbus Has Been Hit By A Data Breach -- Here's What it Could Mean

The company announced yesterday that it had detected a cyber incident on Airbus 'commercial aircraft business' information systems, which resulted in unauthorized access to data, but it claimed there was no impact on Airbus' commercial operations.

Sooraj Shah
January 31, 2019
What happened at OSIsoft?

• Phishing ‘victim zero’ in a remote office
• Months dormant in between ‘low and slow’ activity
• IT account take over and movement to HQ
• Detected theft of Active Directory hashes for employee accounts
• Lengthy forensic investigation
• Public notification and media frenzy
• Coordination with NERC E-ISAC
Data breach monetization model

Key Factors Driving Breaches and Notification

- No Monetization (Lulz)
- Indirect Monetization
- Direct Monetization
- Service Level Agreement
- Security Provider
- Investigative Journalism
- Regulation
- Geopolitical Currency
Notification challenges

• Internal communication first
  • How effective is email in your organization?
  • Briefings

• External communication
  • Reporting to authorities
  • Briefings
  • Direct email and private feeds
  • Media coverage

*Lesson Learned: Focus on actionable information*
Data breach notification practices

Private Sector (process based)

- Google
  - Accidental or unlawful access to Customer Data
  - Security personnel will react **promptly** to known incidents

- Azure
  - Disclosure **process starts** on determination of unauthorized or unlawful access to customer data
  - Executive **approval required**

Government & Regulation (time based)

- NERC CIP
  - Current: **1 hour** on determination bulk electric functions affected
  - In Draft: report attempted breach by **end of next day**

- US CERT Federal
  - Preliminary report within **1 hour**
  - actual or imminent jeopardy without lawful authority
Personal data breach reporting involves a patchwork of requirements.

<table>
<thead>
<tr>
<th>Timeliness (Days)</th>
<th>Regions</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Kentucky and <strong>EU GDPR</strong></td>
</tr>
<tr>
<td>10</td>
<td>Puerto Rico</td>
</tr>
<tr>
<td>30</td>
<td>Colorado, Florida</td>
</tr>
<tr>
<td>45</td>
<td><strong>Eleven States</strong></td>
</tr>
<tr>
<td>60</td>
<td>Delaware, Louisiana, South Dakota</td>
</tr>
<tr>
<td>90</td>
<td>Connecticut</td>
</tr>
<tr>
<td>Without unreasonable delay</td>
<td><strong>Thirty States</strong></td>
</tr>
</tbody>
</table>
Should response time norms vary by impact?

1. Separate SLAs for each IT service
2. An SLA must be quantitative, well researched, and authoritative
3. SLAs must be measurable
4. SLAs require periodic review and adjustment
5. SLAs should account for usual and unusual exceptions

*Major Incidents are different: The effort required to manage and resolve the incident is likely to be large And SLA target resolution times are likely to be breached.
# OSIsoft SLA threat models (examples)

<table>
<thead>
<tr>
<th>Interaction</th>
<th>Threat</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSIsoft Cloud Service data subscriber</td>
<td>Data sent to wrong customer, data as code vulnerability</td>
<td>Critical</td>
</tr>
<tr>
<td>Automatic update push</td>
<td>Malware sent to customer</td>
<td>Critical</td>
</tr>
<tr>
<td>Diagnostic telemetry data</td>
<td>Unauthorized information disclosure</td>
<td>High</td>
</tr>
<tr>
<td>eMail recipient</td>
<td>Abuse of trusted sender, phishing, fake invoices</td>
<td>High</td>
</tr>
<tr>
<td>File downloads</td>
<td>Malware downloaded by customer, document phishing</td>
<td>High</td>
</tr>
<tr>
<td>Unattended remote access</td>
<td>Miscreant ‘hands on keyboard’, espionage, sabotage</td>
<td>High</td>
</tr>
<tr>
<td>Conference apps</td>
<td>Malicious app on device, stolen credentials, contacts</td>
<td>Medium</td>
</tr>
<tr>
<td>Access OSIsoft websites</td>
<td>Watering-hole, stolen credentials, malicious javascript</td>
<td>Medium</td>
</tr>
<tr>
<td>OSIsoft alert subscriber</td>
<td>Abuse of trusted sender, phishing</td>
<td>Medium</td>
</tr>
<tr>
<td>Visit customer and logon to guest network</td>
<td>Eavesdropping and worm exposure</td>
<td>Medium</td>
</tr>
</tbody>
</table>
Breach notification caveats and inhibitors

- Shared responsibility dilemmas and ‘security theater’
- Potential harm to other stakeholders
- Victim shame and ‘acknowledgement of fault’ confusion
- Law enforcement and gag orders
- Coordination with multiple organizations tends to take longer
Breach notification and supply chain complexity

Is there a trusted coordination mechanism?
Ecosystem approaches to notification

**Online Trust Alliance (OTA)**

**Anti-Botnet Initiative**
- ISPs, carriers, service providers
- Test to determine the most effective methods of user notification
- Notifications easily recognized by users as legitimate
- Ensure notifications lead to successful remediation
- Construct notifications in tone, reading level and language appropriate to the target audience

**Defense Industrial Base (DIB)**

**Safeguarding Defense Information**
- DoD supply chain
- Compromise of Controlled Unclassified Information (CUI)
- Violation of policy where compromise of CUI may have occurred
- Adverse affect on operationally critical support
- Cyber threat indicators believed to be valuable in alerting the Government and others
- Rapidly report cyber incidents (72hrs)
Recommended strategy for breach notification

• Leverage a coordination authority

• Rapidly report indicators believed to be valuable and actionable

• Converge on 72 hours as a norm for incident reporting

• Allow for incomplete details at the time of notification
“Perhaps at no time in our history has trust become such a valued and scarce commodity.”

General Anthony C. Zinni, Marine Corps, retired; chairman, BAE Systems