Securing Critical Infrastructure
Agenda

- Some History
- Cyber Threats
- A Little Bit of Physics
- Mitigation Strategies
- Your Actions
- Questions (and Answers!)
An Average Day in an Enterprise

• Every 24 seconds
  A host accesses a malicious web site
• Every 34 seconds
  An unknown malware is downloaded
• Every 1 minute
  A bot communicates with its command & control center
• Every 6 minutes
  A known malware is downloaded
• Every 36 minutes
  Sensitive data are sent outside the organization
At the VA

• 308 million intrusion attempts
• 956,000 instances of malware
• 52 million malicious or suspicious emails
At the VA

- 308 million intrusion attempts
- 956,000 instances of malware
- 52 million malicious or suspicious emails

In Just 1 Month!
Top Data Breaches in 2018

- Marriott International (500 million users)
- Twitter (330 million users)
  - Note: Twitter said it mistakenly stored user passwords in plain text on an internal log accessible only to employees, and that no outsiders accessed them
- My Fitness Pal (150 million users)
- Facebook (147 million users in multiple breaches)
- Firebase [aka Google] (100 million users)
- Quora (100 million users)
- MyHeritage (92 million users)
- Uber (57 million users)
- Ticket Fly, owned by Eventbrite (27 million users)
- Google+ (500,000 users)
- British Airways (380,000 users)
More Ugly News

NEWS

Hackers break into water system network
Pennsylvania breach occurred via compromised laptop

2006

NEWS

Insider charged with hacking California canal system
Ex-supervisor installed unauthorized software on SCADA system, indictment says

2007

NEWS

Water treatment plant hacked, chemical mix changed for tap supplies

2016
The Kemuri Hack

Water treatment plant hacked, chemical mix changed for tap supplies

- Accessing the AS400 server provided attackers with approximately 2.5 million customer records, the ability to manipulate SCADA controls, additional password files, back-office system configuration settings, and other sensitive data.
- Ineffective security awareness training facilitated the attacker’s success with phishing.
- Internal server credentials in plain text were found on the public facing web server.
Uglier News

- 74% of organizations have no formal Incident Response Plan
- Some organizations take 200 days to patch their systems
Most SCADA attacks are aimed at capacity overload. The goal is to

- Swamp hardware, compute, software, and/or bandwidth so that it can no longer respond to legitimate requests, or process data.
- Disable key features (e.g., centrifuges).
- Mask intent while probing for other weaknesses that would allow a break-in.
Shooting Phish in a Barrel

phishing
/ˈfiSHiŋ/ noun

the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.
Shooting Phish in a Barrel

- On average, 23% of employees open phishing emails
- 11% of employees click on the attachments

So, if I send a phishing email to 100 people in your company, will I find 11 victims?
## THE THREAT ACTORS

<table>
<thead>
<tr>
<th>Actor</th>
<th>Motive</th>
<th>Targets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nation States</td>
<td>Economic or Military</td>
<td>IP or infrastructure</td>
</tr>
<tr>
<td>Organized Crime</td>
<td>Financial Gain</td>
<td>IP, Banks, PoS</td>
</tr>
<tr>
<td>Terrorists/Extremists</td>
<td>Cause Support</td>
<td>Highly Visible Targets</td>
</tr>
<tr>
<td>Hackers/Hacktivists</td>
<td>Publicity, Watch it Burn</td>
<td>Anything &amp; Everything</td>
</tr>
<tr>
<td>Trusted Insiders</td>
<td>Revenge, Financial Gain</td>
<td>Your Data</td>
</tr>
</tbody>
</table>
The Insider

- Someone you trust to whom you have given credentials to your most sensitive networks and accounts
- A good person one day who changes their intent the next
- Could be operating alone or as an extension of one of the organizational categories described previously
- Cannot be stopped by technology alone (but it can help)
  - Requires policies, process, and a highly functioning team of good people to catch the bad ones
Connectivity

Toe bone connected to the foot bone
Foot bone connected to the heel bone
Heel bone connected to the ankle bone
Ankle bone connected to the shin bone
Shin bone connected to the knee bone
Knee bone connected to the thigh bone
Thigh bone connected to the hip bone
Hip bone connected to the back bone
Back bone connected to the shoulder bone
Shoulder bone connected to the neck bone
Neck bone connected to the head bone
In the universe, everything is connected to everything.
Brian Edward Cox

- English physicist who serves as professor of particle physics in the School of Physics and Astronomy at the University of Manchester
- Best known to the public as the presenter of science programs and for popular science books, such as
  - “Why Does E=mc²?”
  - “The Quantum Universe”
- Author or co-author of over 950 scientific publications
- Former keyboard player for D:Ream and Dare
Certain particles cannot be at the same place at the same time, with the same energy.
In the universe, everything is connected to everything.
In the universe, everything is connected to everything.

And so it is with the Internet of Things (IoT).
Connectivity

Electric Toothbrush: Automatically reorders brush heads, shares brushing habits with your dentist.

Automobile: Maps traffic in real time; others can track your location.

Computer: Centralized control for remote interface to any other device.

Media Player: Remotely orders new songs & video.

Alarm Clock: Remote programs, custom tones, turns on coffee maker.

Refrigerator: RFID tags reorder groceries as needed, and suggests recipes.

VoIP phone: Automatic updates, integration and forwarding.

Printer: Automatically reorders toner and paper as needed.

Microwave: Automatically sets cook cycle with RFID recognition.

Coffee Maker: Custom setting for each coffee type, starts when alarm goes off.

Oven: Oven settings from computer or phone if running late.

HVAC: Controls temperature & lights for maximum efficiency.


Television: Immediate “one-click” ordering of products seen on commercials.

Smart Scale: Measures and sends weight info for progress tracking.

Cell Phone: Secure performs identification & verification for payments.

Vending: Automatically reorders supplies before it’s empty.

Exercise Equipment: Recognizes individual user and tracks workout schedule.

Source: Backwards Time Machine
Cyber Intelligence

- You need three levels of cyber intelligence
  - Strategic: serving longer term decisions
  - Operation: serving day-to-day leadership decisions
  - Tactical: direct support to defenders in the fight

- Benefits
  - Ensures right allocation of required resources to accomplish cyber intelligence objectives and to serve decision-makers
  - Ensures the right architecture is put in place to support the different kinds of decisions made
### Attaining Cyber Intelligence

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assess</td>
<td>Conduct assessments of cyber intelligence activities &amp; prioritize improvement plans.</td>
</tr>
<tr>
<td>Get Informed</td>
<td>The more you know about the threat the better you can educate others.</td>
</tr>
<tr>
<td>Threat Briefs</td>
<td>Ensure executives understand cyber threats to their business objectives.</td>
</tr>
<tr>
<td>Understand Yourself</td>
<td>Know which data, systems, capabilities are most important to protect.</td>
</tr>
<tr>
<td>Automate</td>
<td>Automate your IT and Cyber management.</td>
</tr>
<tr>
<td>Collaborate</td>
<td>No single organization can defend against all attackers. Sophisticated attacks require collaboration.</td>
</tr>
<tr>
<td>Network</td>
<td>Find your peers and build a community before you need it. Seek inputs on how they leverage cyber intelligence in their organization.</td>
</tr>
<tr>
<td>Prepare for breach</td>
<td>Plan for how you would respond to the worst case scenario and exercise your responses.</td>
</tr>
<tr>
<td>Love your people</td>
<td>Consider assigning an insider threat manager to lead your insider mitigation program and remember. If you love and lead your good people they will help find the bad people.</td>
</tr>
</tbody>
</table>
Culture of Security

Need 4 – 5 Guiding Principles

- Protect the Brand
- Protect Operations
- Protect Trade Secrets & Financials
- Protect Employee Information
- Protect Customer Information

Create an enduring framework to protect the company and its brand without regard for who occupies executive functions
Your employees must understand security

- Educate your employees and test them
- Educate your employees again and test them again
- And again
- Every employee should be a security officer
- Security should be part of an employee’s official evaluation
Incident Response

- Make it a priority to build an incident response team consisting of experienced, full-time members.
- Assess the readiness of incident response team members on an ongoing basis.
- Table top exercises are a must; include your service providers.
- Create clearly defined rules of engagement for the incident response team.
- Have meaningful operational metrics to gauge the overall effectiveness of incident response.
- Get the support and endorsement of a senior executive
- Practice, Practice, Practice!!
Verizon Said

- Align Process with Policies
- Achieve “essential”, then do “excellent”
- Secure Outside Connections
- Create a Data Retention Plan
- Control Data with Transaction Zones
- Monitor Event Logs
- Create an Incident Response Plan
- Increase Awareness
- Engage in Mock Incident Testing
Verizon Said

- Align Process with Policies
- Achieve “essential”, then do “excellent”
- Secure Outside Connections
- Create a Data Retention Plan
- Control Data with Transaction Zones
- Monitor Event Logs
- Create an Incident Response Plan
- Increase Awareness
- Engage in Mock Incident Testing

In 2008!!!
Compliance ≠ Security

Regulatory Compliance Is Necessary But Not Anywhere Near Sufficient
Drinking Water System Risk Assessments and Emergency Response Plans Required Under America's Water Infrastructure Act (AWIA)

In Summary

**The Threat**
A great deal is known about who is attacking and what their motivations are. By studying them we can build better defenses before attack and respond smarter during attack. Get the right info for strategic, operational and tactical decisions.

**The Situation**
Every sector of the economy and every government and every citizen is under almost constant attack. Most suffer ongoing infections with malware. Attackers get in fast and remain undetected for months. But risk can be reduced/mitigated.

**Adversaries Are:**
- Nations
- Crime Groups
- Extremists
- Hackers
- Insiders

**Successful Attacks Are By Organizations**

**Unique Tech Factors**
Governments, businesses, homes, aircraft, cars, roads, trains, ships increasingly interconnected. But cyberspace is hard to observe. Well instrumented systems overseen by trained/experienced people are key to defense.

**Defenders Should Collaborate on Lessons**

**Top Lessons Are:**
- Attackers are persistent, we must prepare for breach

**Your Action**
Lead with understanding that cybersecurity is not just a tech function. Must have executive leadership and engagement by entire team. Ensure external verification and validation of strategy, policy, process and tech.

**Top Actions**
- Engage with CSA, Collaborate with Peers, Study Threats

**Ensure Tech is Independently Assessed**

**Tools To Consider:**
- Encryption
- IDAM
- SDP
- 2FA
- Automated Patching

**Victory Must Be Earned**
Thank You!

Bob Flores
Applicology Incorporated
bob@applicology.com