AlertEnterprise!

Physical Security is from Mars, Cybersecurity is from Venus

Brian Harrell, Vice President of Security, AlertEnterprise

For Discussion

1. Magnitude of the Issue
2. Preventing Physical Attacks
3. Preventing Cyber Attacks
4. Compliance vs. Security
5. Best Practices
6. Emerging Threats
7. Threat and Vulnerability Assessments
8. Security Convergence

AlertEnterprise!

The Real Challenge

Securing a Remote or Urban Asset!

AlertEnterprise!



What are the threats to Critical Infrastructure?

You can’t protect it without knowing what the threats are

AlertEnterprise!

Threats to Critical Infrastructure

Physical

- Chemical theft and release
- Gunfire, sabotage, and the destruction of critical equipment
- Insider theft of assets, information, or availability
- Theft of key equipment
- Electric Disruptions
- Pandemic
- Natural Disasters
- Aging Assets
- Workplace violence and hostile intruder
- Insider threat

Cyber

- Cyber-attack as a prelude to war (conventional and asymmetrical)
- Hackers & Hacktivists
- Information theft (proprietary and customer data)
- Intrusion opportunities created by advent remote access and smart meter technology
- Phishing on the corporate side to gain access to SCADA systems
- Ransomware
- BYOD to work
- Use of USB drives

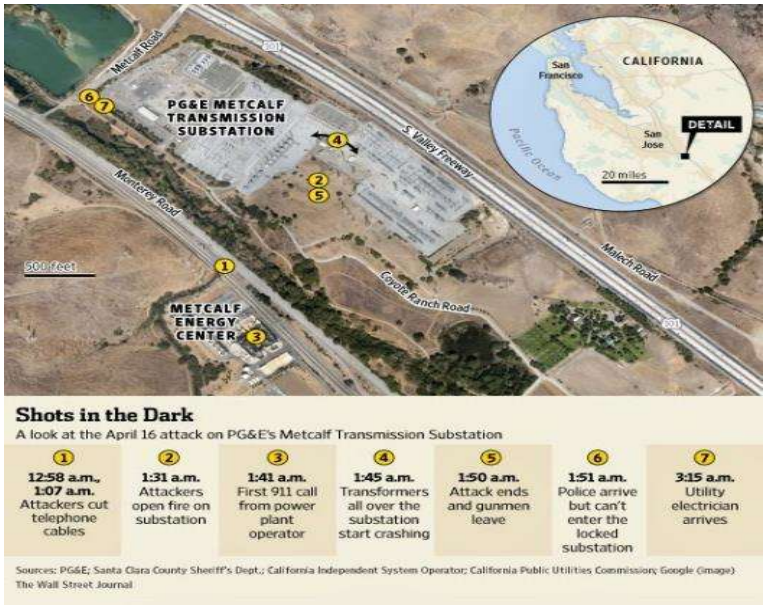
AlertEnterprise!

Deter, Detect, and Delay

Metcalf Substation Shooting

- Unusually well informed attacker(s)
- Two fiber optic lines cut prior to attack by entering telecom vaults
- Left the scene before LE arrived
- Targeted in-service transformers
- Nearby Generation station out of service
- Approximately $15 million in damage

- Substation located south of San Jose, CA
- Unknown shooter(s)
- 116 impacts on 22 pieces of equipment
- Lost 52,000 gallons of transformer oil
- 10 of 11 - 500/230kV units damaged



AlertEnterprise!

Security vs Compliance

Minimum Standard vs. Effective Security

AlertEnterprise!

Industry Best Practices

Site Specific Layered Approaches To:

- **Deter** potential adversaries from considering the facilities in their pre-operational planning
- **Detect** adversaries in their planning, surveillance, or approach stages
- **Delay** adversaries from gaining access to critical facilities and equipment
- **Minimize** the impact of any intrusions or attacks on BPS reliability
- **Rapidly** respond to any attacks or intrusions
- **Preserve** and assist law enforcement in evidence recovery for potential apprehension

AlertEnterprise!

Deterrence

Current systems and technologies used by industry security professionals:

1) Motion activated video surveillance with intrusion deterrence technologies
2) Limited access smart locks and access card systems/readers
3) Employee screening (insider threat)
4) Security fencing to include solutions with blast and ballistic resistance
5) Environmental and physical vehicle barriers
6) Security lighting to include motion activated strobe illumination
7) Security signage
8) Prohibit non-critical storage and staging to reduce criminal draw
9) Annual security program and vulnerability assessment reviews
10) Security guards
11) Neighbor awareness security program

AlertEnterprise!

Detection

- External/internal video analytic systems (HD FLIR, Thermal)
- External/internal motion sensing systems
- Intrusion detection on perimeter fencing
- Seismic detection systems
- Gunshot detection systems
- UAS (drone) detection systems

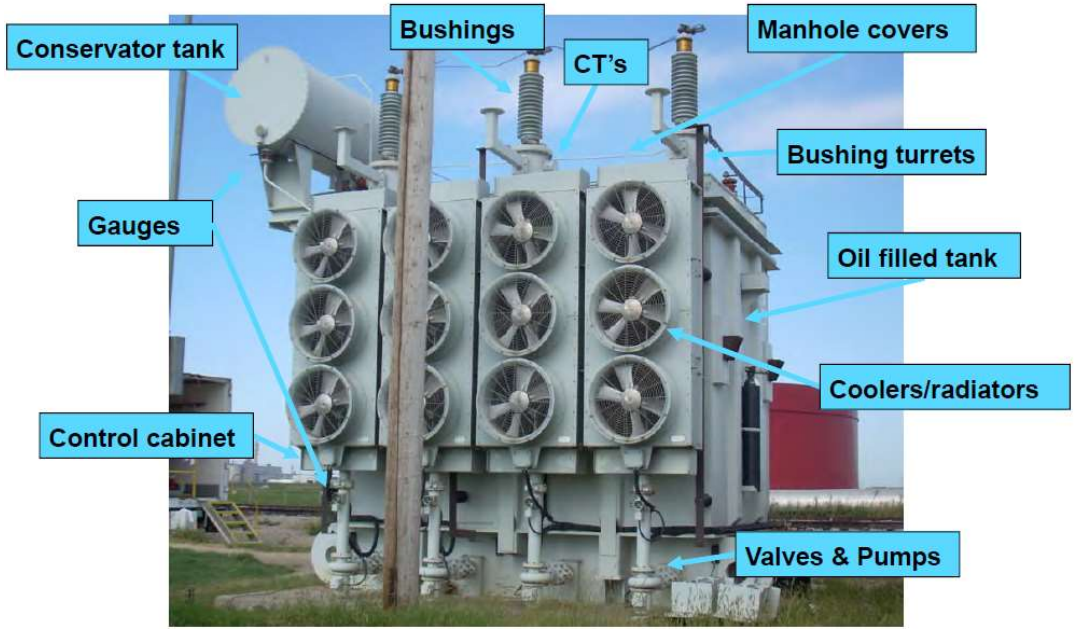
AlertEnterprise!

Delay & Design

- CPTED (Crime Prevention Through Environmental Design)
- Spacing and Distance (blast mitigation)
- Engineering involvement
- Access barriers
- Fencing Barriers

AlertEnterprise!

Protecting the Crown Jewels



AlertEnterprise!

Threat and Vulnerability Assessment

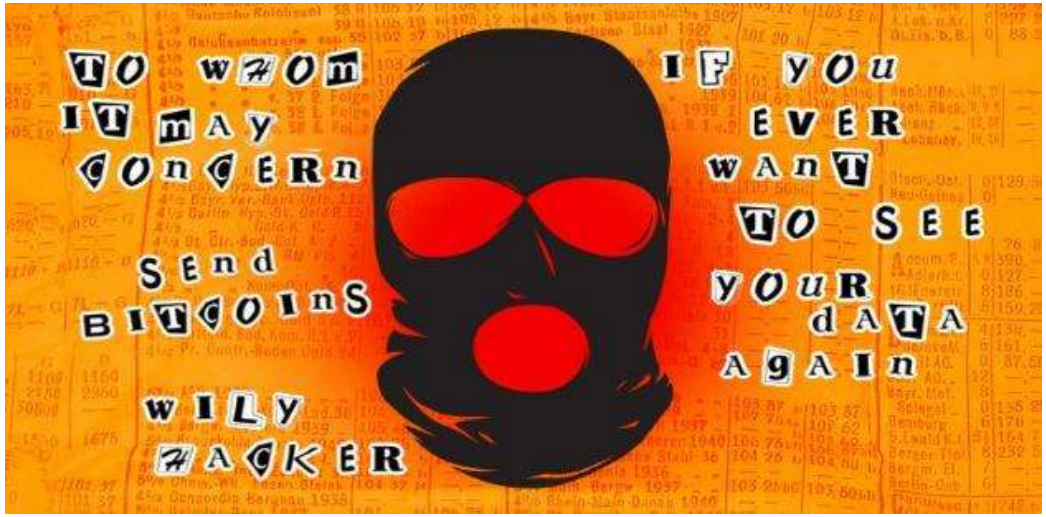
The foundation of any security program

Comprehensive review of:

- Apply Methodology
- Identify Assets in Scope
- Identify Threats and Adversaries
- Facility or System Vulnerabilities?
- Current or Planned Mitigations
- Current Policy Gaps?
- Think Like a Criminal or Terrorist

Cybersecurity

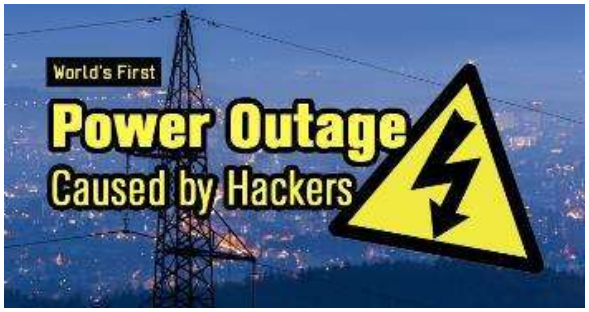
Ransomware



- Malicious software designed to block access to a computer system until a sum of money is paid
- Ransomware is a growth industry
- Paying the Ransom? Business continuity vs. security
- Prevention?
  - Patches and updates, avoid falling victim to phishing emails, and regular backups

AlertEnterprise!

Ukraine Grid Attack



Attack # 1 Dec. 23, 2015

- Deep reconnaissance six months prior to the attack
- Affected 225,000 customers
- 3 distribution service areas
- 27 substations were taken offline
- Adversaries used ICS/OT systems to open breakers

Attack #2 Dec. 17, 2016

- Focused on Transmission facilities
- Shut down Remote Terminal Units (RTU)
- Hour long power outage

AlertEnterprise!

Emerging Threats and Trends

The Good, Bad, and Ugly - Drones

- Applications continue to evolve at an exponential rate
- Have many legitimate and cost effective uses for many industries, including critical infrastructure
- Have been utilized by terrorist organizations
- Are being the subject of intense manipulation and invention for both commercial and sinister use “killer drones”

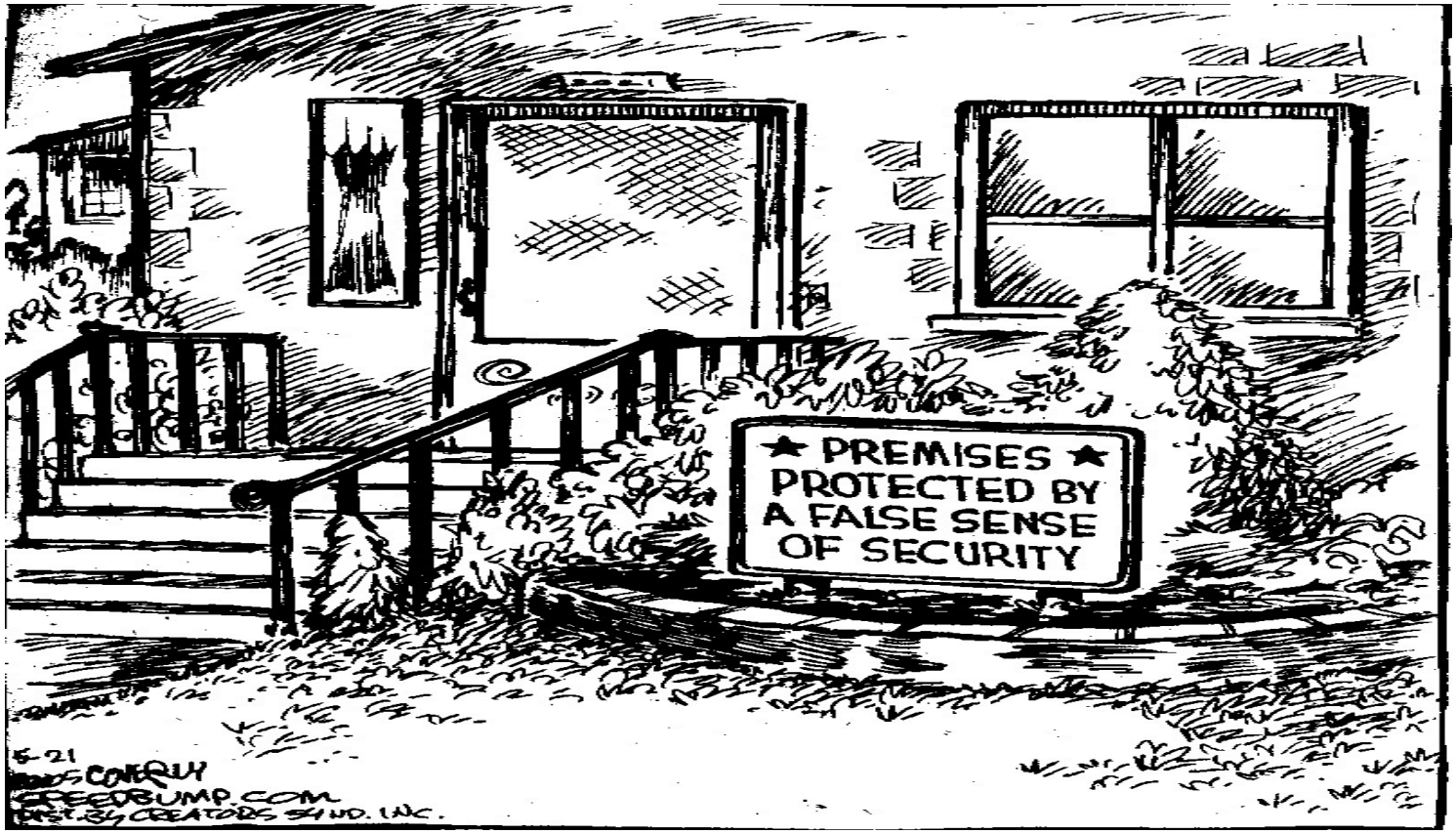
AlertEnterprise!

The Art of Convergence

- Bringing together different security silos into one combined Org
- A significant number of breaches are occurring due to internal threats
- Physical security technology uses IT systems and platforms
- Departments should collaborate to ensure physical access is linked closely with logical access to computers and network resources
- A company's cyber infrastructure, CIP program, and industrial control systems rely on physical security mitigation measures to keep systems inaccessible to physical threats
- Security Convergence requires leadership and political will
- The need to make risk-based decisions dictate an integrated approach to security management

Eliminating Silos

- Problem is across all Critical Sectors & fortune 500s
- You don't have the luxury to wait considering threat landscape (Bad guys are not going to wait for you to get ready….)
- Don't live in Silos – Silo approach has miserably failed
- Leverage Technology – "Technology doesn't have fatigue, can't be bribed/disgruntled…"
- Added awareness brings operational efficiency, productivity, and safety
- "Make Security a Business Enabler"
- Leverage forward looking utilities & other critical sectors who have already addressed these challenges successfully.



Questions?

Thank You!

Brian Harrell, CPP
Vice President of Security
AlertEnterprise
brian@alertenterprise.com
@gridsecure
703.965.7474