



# Energy Sector Insecurity

Managing Cyber-risk in a Utility

*Tom Kellermann, CISM / VP of Security Awareness*

- **Hannibal using the Roman Roads to cross the Alps**





- **There has been a 200% increase in intrusions into U.S. government networks.**  
*--GAO, 2010*
- *73% existed for over 9 months*  
*--OMB 2010*
- **\$6.75M in losses associated per cyber-breach.** *--Ponemon Institute 2009*
- **108 Countries with Dedicated Cyberwarfare Capabilities**  
*-- FBI*

- **Cyber-attacks have become a pervasive phenomenon based on:**
  - Increasing connectivity and availability of assailable network, systems and applications vulnerabilities.
  - The ability of cybercriminals to derive significant financial rewards through successful attacks.
  - Worldwide federation between various classes of cyber-criminals and malware developers.
  - Nation-state, terrorist and politically-driven backing of targeted cybercrime efforts.
  - A lack of cohesive law enforcement around the globe.



## ■ The Kill Chain

- » 1. Recon
- » 2. Weaponization
- » 3. Delivery
- » 4. Exploitation
- » 5. Command and Control
- » 6. Propagation
- » 7. Ex-filtration
- » 8. Maintenance

## ■ MALFI

- 1. Remote file inclusion
- 2. Local file inclusion
- 3. Cross-server attacks
- 4. Remote code execution via sys call proxy and memory injection

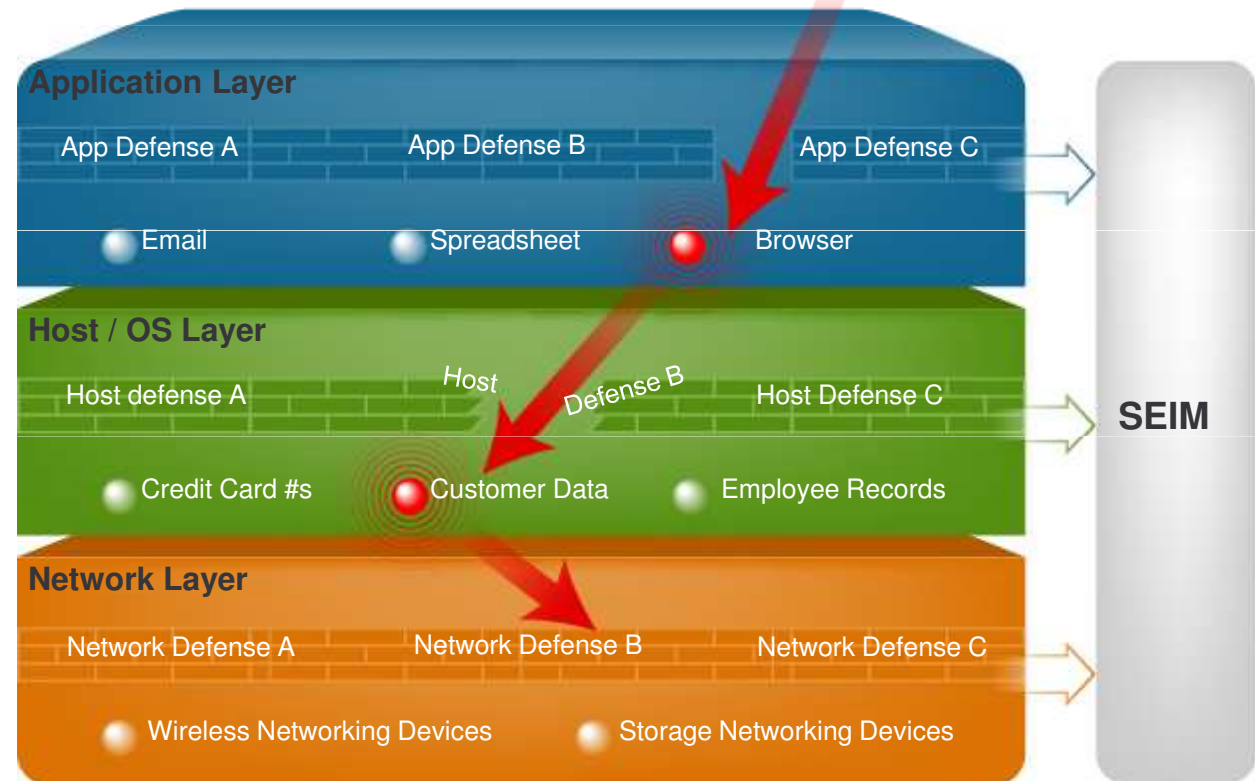
# Real-World Attack Behavior

**Cybercriminals are still finding their way around, and through, point security defenses.**

**New attack paths**

**Point defense weaknesses**

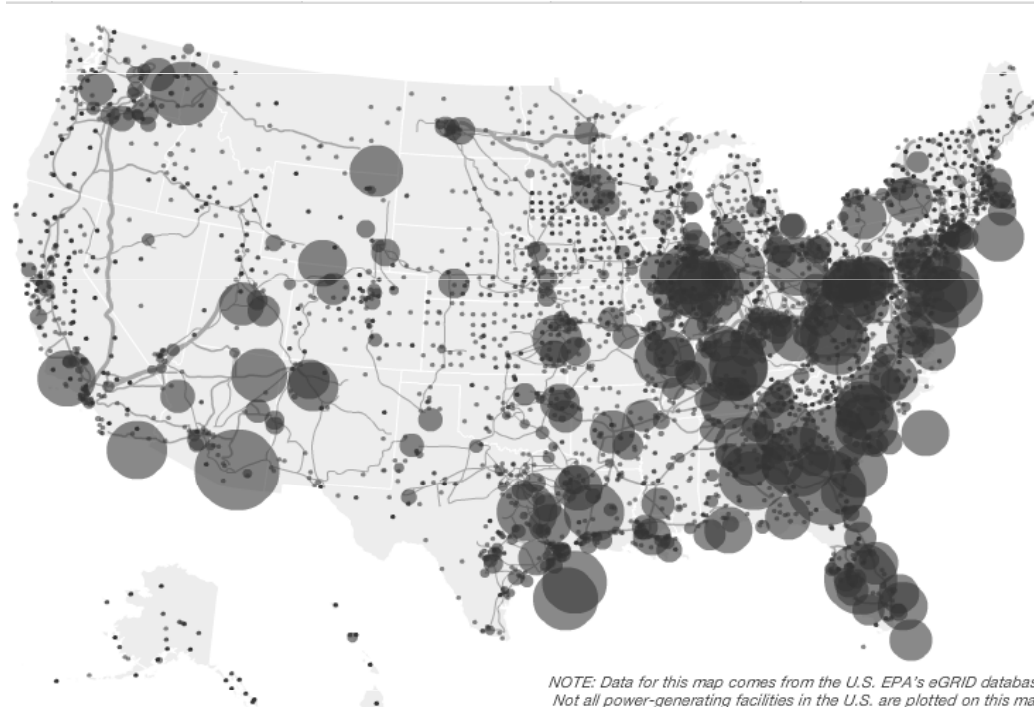
*Multi-staged threats that move across systems and IT layers to threaten critical backend assets*



**How do you know what's working, what's not, and what to do about it?**

# High Intensity Low Frequency (H.I.L.F) Event Risk to the North American Bulk Power System

- In the post 9-11 world, terrorist organizations spawned from al-Qaeda successes continue to be dangerous, adaptive, and motivated enemies and continuing to pose a threat to the U.S.'s critical infrastructure.
- Similarly, terrorist organizations from other parts of the world continue to pursue plans to attack the U.S. directly, likely focusing their efforts on government, economic, and infrastructure targets.



# Electrical Grid is a Prime Target

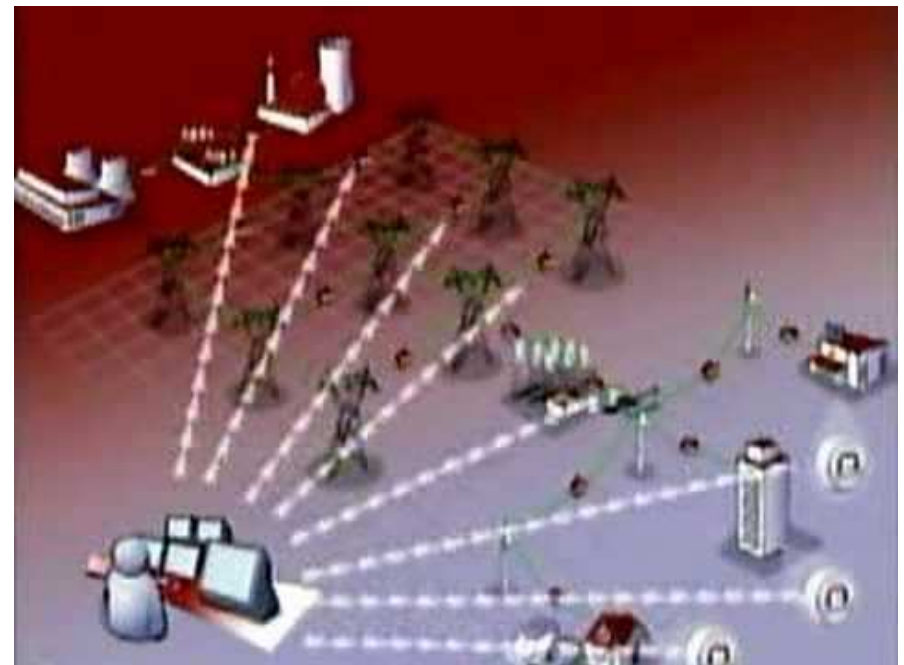
- **Overseas attackers seek to infiltrate the energy grid, in order to:**
  - **Disrupt the American way of life;**
  - **Embarrass the U.S. government by compromising its Critical Infrastructure;**
  - **Cripple and weaken U.S. financial markets and other vital business operations, wreak economic havoc; and**
  - **Distract the public in order to attempt additional electronic campaigns or coordinated physical attacks.**



- **The risk of a coordinated cyber, physical, or blended attack against the North American bulk power system has become more acute over the past 15 years as digital communicating equipment has introduced cyber vulnerability to the system.**
- **In the event, an attack, based on the aforementioned example were to succeed, the effects to the system could be long term and potentially irreparable in nature.**



- **Cyber vulnerability presents a growing and increasingly sophisticated threat.**
- **85% of all systems relays are now digital.**
- **Industry purchased products can contain inherent vulnerabilities.**
- **“ ... a single exploitation of a vulnerability can be propagated across a cyber or power system network and potentially affect an entire class of assets at once.” (HILF report 6/10)**



# Root Cause Issues

- **The U.S. electrical grid has long maintained an acceptable level of engineered resilience in the physical sense.**
- **Introduction of IT-based controls, specifically SCADA technologies featuring IP-based connectivity, has increased the risk of remote attack.**
- **The business continuity and resiliency movement following 9/11 has only served to exacerbate cyber-security concerns.**



- **The Smart Grid will deliver electricity from points of generation to consumers, via two primary systems:**
  - The transmission system, which will deliver electricity from power plants to distribution substations, and
  - The distribution system, which will deliver electricity from distribution substations to consumers.
  - *Interconnected systems with access and complexity. An aggregate will cause Stress on the Bulk Power system.*



- **2007 Aurora Project: U.S. Department of Energy tested the security of a utility.**
- **Demonstrated the threat by exploiting a power grid network vulnerability to destroy a generator.**
- **Based on the projects findings, an actual successful attack targeted at one third of the North American power grid would cost \$700 billion over three months.**



# Additional Issues Emerging

- **The U.S. Department of Homeland Security has identified a report by a research scientist in China demonstrating how an attack aimed at a small power sub-network could potentially trigger a cascading failure of the entire West Coast power grid.**
- **Jian-Wei Wang, a network analyst at China's Dalian University of Technology, used publicly available information to model how the West Coast power grid and its component sub-networks are interconnected, increasing their value as a target.**



# From Rumor to Reality

- **After years of rumored cyber-infiltrations, our worst fears are confirmed in the public eye.**
- **WSJ Story: Cyber-spies penetrated the U.S. electrical grid, left behind malware that could be used to disrupt the system, according to national-security officials.**
- **Spies traced to Eastern Europe/Russia and China.**



- **Cyber intrusion into field engineering networks and the compromise of relays and remote terminal units at multiple substations. The consequences range from simple breaker operations (open a line) to operations that cause equipment damage (aurora) only being one scenario.**
- **Man-in-the-middle attacks on data acquisition information back to an “interconnected” control room or to swim up stream and compromise a front end processor**
- **A push of bad firmware out to a significant number of remote field devices that can't be recovered by zeroing/reboot.**
- **Insider with access to several PCS systems for safety and protection.**

- **Driven by cyber-attacks, the U.S. energy sector must radically improve its overall approach to IT security.**
- **The cyber threat has been illustrated by high-profile infiltrations and regulations created in response by industry and government leaders.**
- **Risk management and assessment has to evolve in order to mitigate the threats to the Nation's energy infrastructure posed by cyber-threats.**



- Federal legislators respond to demands to improve cyber-security in the wake of rumored involvement in blackouts, etc.
- Jan. 2008: Federal Energy Regulatory Commission (FERC) approves eight new mandatory critical infrastructure protection (CIP) reliability standards to protect the nation's bulk power system against potential disruptions from cyber-security breaches.
- Standards were developed by the North American Electric Reliability Corporation (NERC), which FERC has designated as the electric reliability organization (ERO).



- Based on larger federal CIP parameters put in place for many different critical infrastructure providers.
- Meant to establish minimum requirements for cyber security programs for electrical utilities.
- Meant to ensure that security best practices are being adopted by organizations responsible for systems whose interruption *“would have a debilitating impact on security, national economic security, national public health or safety.”*



## Under CIP, the government requires grid providers to:

- Assess their vulnerabilities to both physical or cyber attacks.
- Plan to eliminate significant vulnerabilities.
- Develop systems to identify and prevent attempted attacks.
- Alert, contain and rebuff attacks, and work with the FEMA to rebuild essential capabilities.
- Establish Security Test Procedures to ensure new and changed systems do not affect security controls.



- **April 2009 letter from NERC CSO Michale Assante:**
  - **Based on initial survey, affected utilities are not making the grade in meeting the specifics or spirit of standards.**
  - **Companies have not identified enough of their assets as critical thereby requiring additional protection.**
  - **NERC will “broaden the net of assets that would be included under the mandatory standards framework in the future.”**

# NERC

NORTH AMERICAN ELECTRIC  
RELIABILITY CORPORATION

- **April 2009 letter from NERC CSO Michale Assante:**
  - **“As we consider cyber security... system planners and operators will need to consider the potential for the simultaneous manipulation of all devices in the substation or, worse yet, across multiple substations.”**
  - **“One of the more significant elements of a cyber threat, contributing to the uniqueness of cyber risk, is the cross-cutting and horizontal nature of networked technology that provides the means for an intelligent cyber attacker to impact multiple assets at once, and from a distance.”**

# NERC

NORTH AMERICAN ELECTRIC  
RELIABILITY CORPORATION

# The Gathering Storm: Cloud Computing



[www.coresecurity.com](http://www.coresecurity.com)

- **Distributed, interconnected clouds also create as many potential risks as they may eliminate.**
- **Multi-tenancy and resource usage optimization driven by economies of scale introduce a multitude of security issues due to the blurring of lines of demarcation for data entering and traversing the cloud.**
- **Where does your organizations cloud end and begin?**



# 5 Elements of the “Perfect Storm”

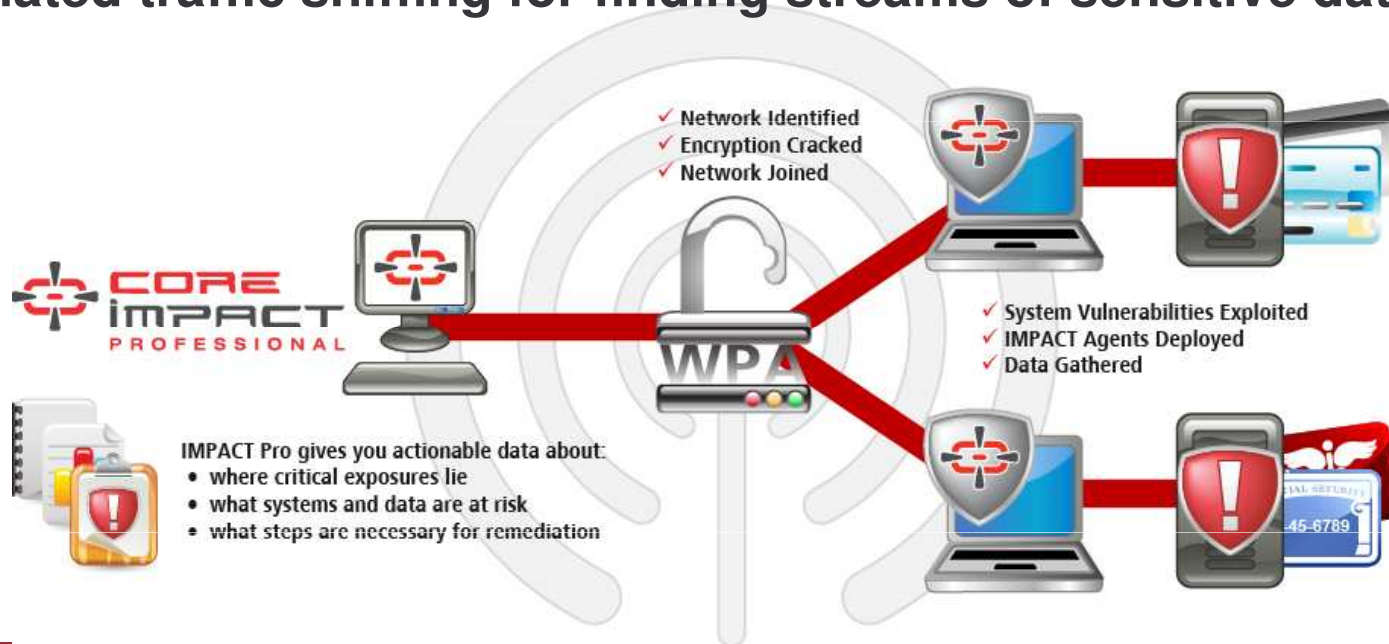


[www.coresecurity.com](http://www.coresecurity.com)

- **An overreliance on encryption: encryption can and will be defeated, by technical innovation and human error.**
- **Virtualization is still a security unknown: there are significant vulnerabilities in the systems people are using today.**
- **Outsourcing is a huge security risk: Organizations don't typically make security a major element of their SLAs and write safeguards into their outsourcing contracts. Unless they do so and invoke major penalties for breaches, a pass-the-buck approach to security will continue to dominate.**
- **The security perimeter becomes even fuzzier. With data constantly available in the cloud for user access, in multi-tenant environments, the opportunity for infiltration would seem to grow exponentially.**
- **SaaS Apps May Leak Data Even When Encrypted: their use of networks can cause "side-channel" leaks that might enable attackers to glean even the most sensitive.**

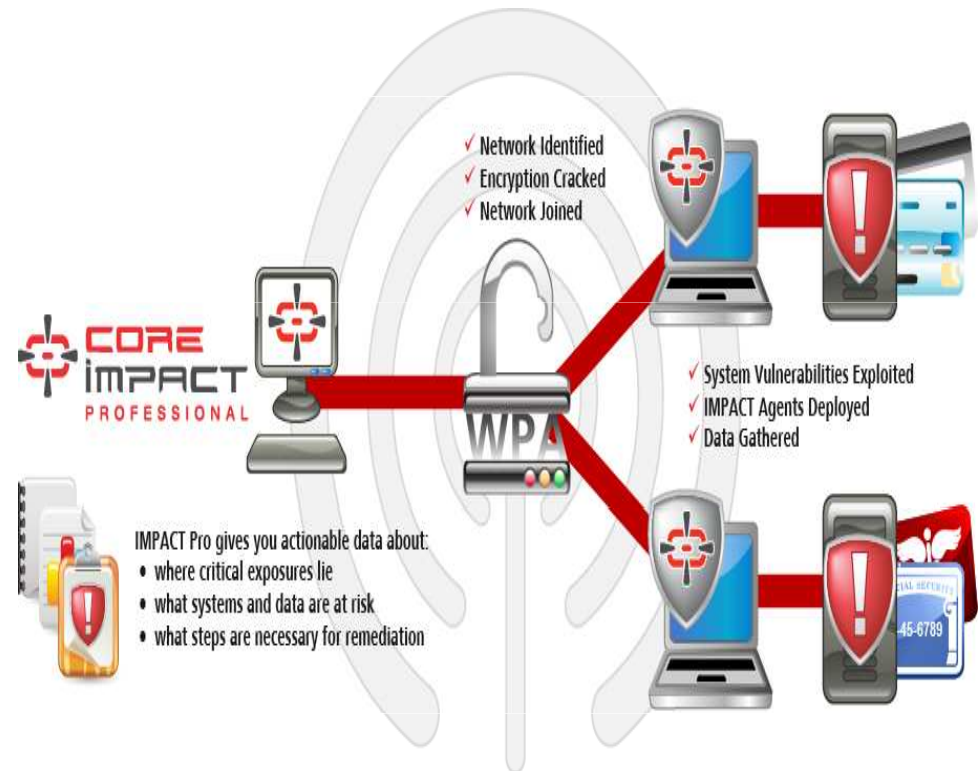
# Wireless Penetration Testing

- Discovery of both known and unauthorized Wi-Fi networks and access points
- Information gathering on network strength, security protocols and connected devices
- Attack and penetration of networks encrypted with WEP, WPA-PSK and WPA2-PSK
- Automated traffic sniffing for finding streams of sensitive data



# Wireless Penetration Testing Continued...

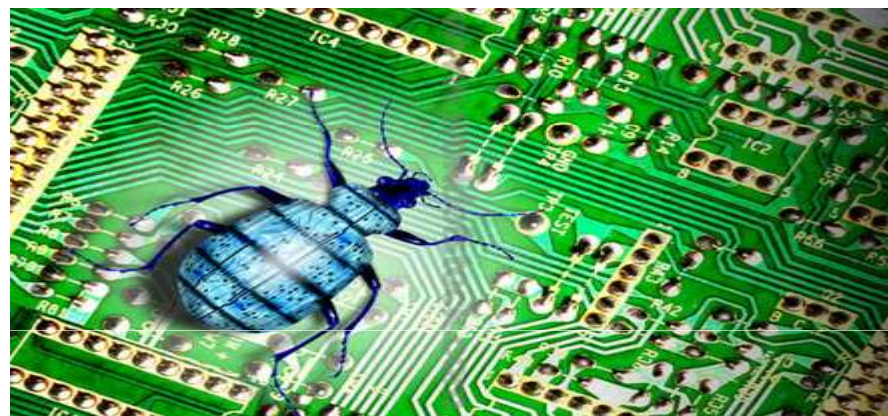
- Capabilities for joining cracked networks and testing backend systems;
- Comprehensive reporting of wireless testing activities and findings
- Seamless pivoting between wireless, network, web application and endpoint tests, replicating
- Multi-staged attacks that trace chains of vulnerabilities to sensitive backend data



- **Beyond meeting the requirements identified by NERC, energy providers are recommended to implement and utilize penetration testing in order to:**
  - **Gain the most realistic picture of the current level of vulnerability their IT systems and security controls possess versus real-world threats.**
  - **Acquire an accurate assessment of:**
    - ❖ **How well prepared the organization is;**
    - ❖ **How well the organization will respond to an incident involving cyber-terrorism; and**
    - ❖ **Identify potential risks and vulnerabilities.**



- **Understand how compromised systems can be manipulated by remote adversaries, and the potential losses associated with such an incident .**
- **Study findings to gain a better understanding of the threat associated with cyber-terrorism.**



- **Additional strategies and technologies recommended include:**
  - » The utilization of whitelisting technologies;
  - » Upgrading Wi-Fi security technology beyond WPA2;
  - » Implementing two-factor authentication on all devices; and
  - » Installing logging capabilities on all devices.



**Expect to be hit and prepare to survive**



[www.coresecurity.com](http://www.coresecurity.com)

**For more information see:**

**<http://www.coresecurity.com>**

