WHEN CYBER ATTACKS GET PHYSICAL

ICS ATTACK SCENARIOS AND CIP-007 R1

ADVANCED THREAT PROTECTION, SECURITY AND COMPLIANCE

The premise of a January 27, 2015, article by CNBC is that there is good evidence that a cyber attack against nearly any country's critical infrastructure could be imminent. This kind of reporting has become so commonplace, but this doesn't seem like just more FUD (fear, uncertainty, and doubt) journalism.

According to Eugene Kaspersky, CEO of global IT security firm Kaspersky Labs, the evidence supporting these claims is a dramatic uptick in targeted attacks against power grids, banks and transportation networks around the world. He told CNBC that "the worst terrorist attacks are not expected," but he also points out that those targeting crucial infrastructure will inflict "very visible damage."

Kaspersky recommends that every country audit their critical infrastructure in order of importance—with the most important and vulnerable being the power and energy sector. He also notes that governments need to appropriate the budget necessary to secure critical infrastructure over the next decade, inferring that this threat isn't going to be effectively mitigated anytime soon.

There have been a number of recent public disclosures that highlight the ongoing dangers connected with very real cybersecurity threats against critical infrastructure:

PHYSICAL DAMAGE FROM CYBER ATTACK IN GERMANY

Just before the end of 2014, amid all the noise about the Sony breach, a quiet 2014 report by Germany's Federal Office for Information Security was issued. One of the incidents described was a successful attack that infiltrated the industrial controls at an unnamed German steel mill. The attack caused 'massive' damage by making it impossible to shut down a blast furnace.

Wired magazine cited a translation of the report, saying it appeared that "the hackers obtained access via a spearphishing attack" before quickly moving across a "multitude" of sensitive corporate networks. Who the hackers were, how long they were in the system, whether they intended to destroy the furnace and what, if any, other equipment they accessed all remains unclear.

◆ **2008 TARGETED** *attack on the majority BP-owned Baku-Tbilisi-Ceyhan pipeline in Turkey.*

CYBER ATTACKERS CAUSED PIPELINE EXPLOSION IN TURKEY

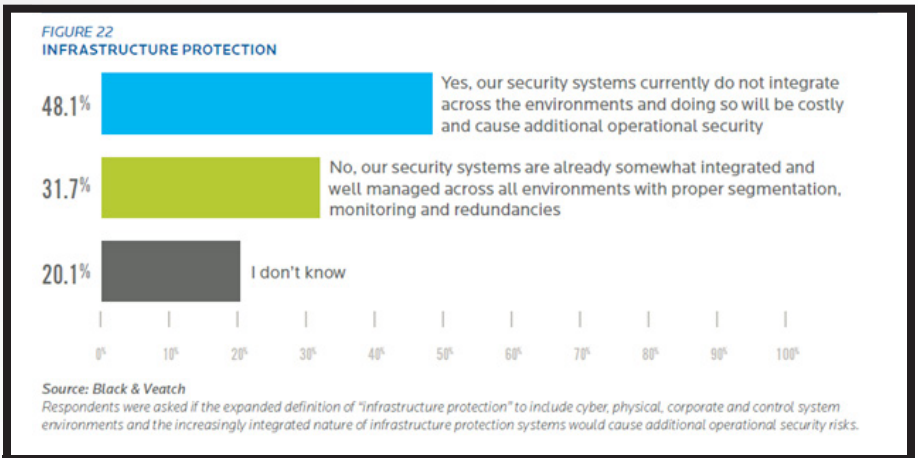
A Bloomberg News article on December 10, 2014, highlighted just how destructive digital attacks can be. A recently disclosed 2008 targeted attack on the majority BP-owned Baku-Tbilisi-Ceyhan pipeline in Turkey caused an explosion with flames as high as 150 feet. At the time, Baku-Tbilisi-Ceyhan was thought to be one of the most secure pipelines in the world. Still, attackers infiltrated the pipeline through a wireless network, tampered with the systems, and caused severe physical damage.

In the U.S., there are millions of miles of pipelines that distribute everything from oil, hazardous liquids, natural gas and chemicals. Many of them are approachable above ground, calling their physical security into question. These same pipelines are unquestionably vulnerable to cyberattacks that can inflict the same kind of serious physical damage as physical attacks.

NATIONAL SECURITY AGENCY DIRECTOR WARNS "THIS IS NOT THEORETICAL"

In a November 20, 2014, hearing for the House Intelligence Committee, NSA Director Admiral Michael Rogers said several foreign governments had already hacked into U.S. energy, water and fuel distribution systems, potentially damaging essential services, according to Bloomberg.

"This is not theoretical," Rogers said. "This is something real that is impacting our nation and those of our allies and friends every day."



◆ **48% OF** *respondents indicated they did not have integrated security systems with the "proper segmentation, monitoring and redundancies" needed for cyber threat protection.*

DHS WARNS U.S. UTILITY WAS HACKED

In May 2014, the Department of Homeland Security and its Industrial Control Systems Cyber Emergency Response Team issued an ICS-CERT report warning of several known attacks against U.S. utilities in the first quarter of 2014. They cited details of one unnamed utility that had been breached and warned U.S. utilities to be on guard for intrusion activity. The complete article on this information is available here.

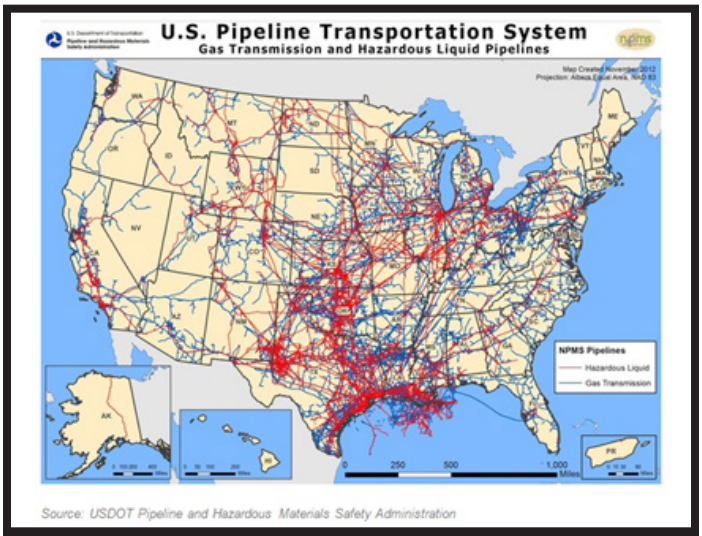
CYBER THREATS CAN BE PHYSICAL

Increasing cyber threat concerns are having an impact on critical infrastructure organizations because the physical implications have the potential to be catastrophic—cybersecurity rated as the fourth highest issue for energy executives in 2014, up from sixth place in 2013.

This shows dramatic progress; it was not even in the top ten concerns for utilities two years ago. According to the 2014 annual report from industry consultants Black & Veatch conducted in May of 2014.

48% OF ELECTRIC UTILITIES SURVEYED NEED CYBER THREAT PROTECTION

Still, a survey of electric utility representatives showed that 48% of respondents indicated they did not have integrated security systems with the "proper segmentation, monitoring and redundancies" needed for cyber threat protection. Only 32% said they had these protections in place.



◆ **IN THE** *U.S., there are millions of miles of pipelines, many of which are approachable above ground.*

> *"We are seeing an industry that is actively moving forward with the deployment of comprehensive asset protection plans following several high-profile cyber and physical threat events."*

STRONGER CYBERSECURITY STANDARDS FOR ELECTRIC UTILITIES COMING IN THE U.S.

A new set of cybersecurity standards from U.S. federal regulators will impose expanded requirements on U.S, Canadian, and some Mexico utilities, with more assets "in scope" as well as new and stricter security regulations that will help mitigate some of these cybersecurity threats. These new regulations are due to go into effect in April of 2016 for High and Medium Critical Cyber Assets, and utilities need to begin preparing to meet these requirements now.

Every proactive step toward protecting critical infrastructure is a move in the right direction and there is no better time than now to begin.

HOW CYBER GETS PHYSICAL

There is not a deep digest of every attack or infection vector used within these and other global attacks posed on critical infrastructure, however, the U.S. Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) organization is focused on breach activity detected within ICS environments. In particular, ICS-Alert-14-281-01B "Ongoing Sophisticated Malware Campaign Compromising ICS" published December 10, 2014 provided this information as an update to prior alerts, indicating variants of the BlackEnergy malware has been seen as an ongoing attack since at least 2011.

"ICS-CERT has become aware of a sophisticated malware campaign that has compromised numerous industrial control systems (ICSs) environments using a variant of the BlackEnergy malware. This campaign has been ongoing since at least 2011. Multiple companies working with ICS-CERT have identified the malware on Internet-connected human-machine interfaces (HMIs)."

Summary of a few targets of this malware campaign, and other vendors should be contacted to determine if they have updates to aid in thwarting possible compromise. Infection vectors are offered in this ICS-CERT Alert.

- Users of GE Cimplicity
- Users of Advantech/Broadwin WebAccess
- Siemens WinCC

"Typical malware deployments have included modules that search out any network-connected file shares and removable media for additional lateral movement within the affected environment. The malware is highly modular and not all functionality is deployed to all victims."

NERC CIP-007 — SYSTEMS SECURITY MANAGEMENT

The US North American Electric Reliability Corporation (NERC) has issued its most current Critical Infrastructure Protection (CIP) compliance requirements (CIPv5), required for compliance audits as of April 2016 for all electric utilities who are registered entities. One of the most difficult and most frequently violated is CIP-007, System Configuration Management, Requirement 1: Ports and Services. This requirement states that each Responsible Entity shall implement… processes that identify, assess, and correct deficiencies applicable to the requirement parts in CIP-07-5 Table R1 – Ports and Services.

REGARDING CIP-007 R1 AND TRIPWIRE

Tripwire solutions can automate and eliminate manual effort in checking system configurations for ports, protocols, services (such as remote access software), files, dlls, daemons, USB ports, and other possible infection vectors systems may be offering to possible attackers. Tripwire's solutions can also create inventories of all IP-addressable systems within the network, essential for knowing where High- and Medium-Impact Cyber Assets may be.

CIP-007-5 TABLE R1– PORTS AND SERVICES

Part	Applicable Systems	Requirements	Measures
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	Examples of evidence may include, but are not limited to: » Documentation of the need for all enabled ports on all applicable Cyber Assets and Electronic Access Points, individually or by group. » Listings of the listening ports on the Cyber Assets, individually or by group, from either the device configuration files, command output (such as netstat), or network scans of open ports; or » Configuration files of host-based firewalls or other device level mechanisms that only allow needed ports and deny all others.
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.

TRIPWIRE COVERAGE OF NERC CIPv5 REQUIREMENTS

10 Standards | 32 Requirements | Tripwire covers 20

CIP-002 BES CYBER SYSTEM IDENTIFICATION AND CATEGORIZATION	CIP-003 SECURITY MANAGEMENT CONTROLS	CIP-004 TRAINING AND PERSONNEL SECURITY	CIP-005 ELECTRONIC SECURITY PERIMETER	CIP-006 PHYSICAL SECURITY OF BES CYBER SYSTEMS	CIP-007 SYSTEMS SECURITY MANAGEMENT	CIP-008 INCIDENT REPORTING AND RESPONSE PLANNING	CIP-009 RECOVERY PLANS FOR BES CYBER SYSTEMS	CIP-010 CONFIGURATION CHANGE MANAGEMENT AND VULNERABILITY ASSESSMENTS	CIP-011 INFORMATION PROTECTION
1. BES CYBER SYSTEM IDENTIFICATION	1. CYBER SECURITY POLICY FOR HIGH/MEDIUM SYSTEMS	1. AWARENESS	1. ELECTRONIC SECURITY PERIMETER	1. PHYSICAL SECURITY PLAN	1. PORTS AND SERVICES	1. CYBER SECURITY INCIDENT RESPONSE PLAN	1. RECOVERY PLAN SPECIFICATIONS	1. CONFIGURATION CHANGE MANAGEMENT	1. INFORMATION PROTECTION
2. REGULAR APPROVAL	2. CYBER SECURITY POLICY FOR LOW SYSTEMS	2. TRAINING	2. INTERACTIVE REMOTE ACCESS MANAGEMENT	2. VISITOR CONTROL PROGRAM	2. SECURITY PATCH MANAGEMENT	2. CYBER SECURITY INCIDENT RESPONSE PLAN IMPLEMENTATION AND TESTING	2. RECOVERY PLAN IMPLEMENTATION AND TESTING	2. CONFIGURATION MONITORING	2. BES CYBER ASSET REUSE AND DISPOSAL
	3. IDENTIFICATION OF SENIOR MANAGER	3. PERSONNEL RISK ASSESSMENT PROGRAM		3. MAINTENANCE AND TESTING PROGRAM	3. MALICIOUS CODE PREVENTION	3. CYBER SECURITY INCIDENT RESPONSE PLAN REVIEW, UPDATE, COMMUNICATION	3. RECOVERY PLAN REVIEW, UPDATE AND COMMUNICATION	3. VULNERABILITY ASSESSMENTS	
	4. DELEGATION OF AUTHORITY	4. ACCESS MANAGEMENT PROGRAM			4. SECURITY EVENT MONITORING				
		5. ACCESS REVOCATION PROGRAM			5. SYSTEM ACCESS CONTROLS				

RECENT AWARDS

SC MAGAZINE AWARDS 2014 WINNER Honored in the U.S.

SC MAGAZINE AWARDS 2014 FINALIST Honored in the U.S.

Info Security Products Guide 2014 GLOBAL EXCELLENCE GRAND

Info Security Products Guide 2014 GLOBAL EXCELLENCE GOLD

THE GOLDEN BRIDGE AWARDS GOLD BEST 2014 BUSINESS WORLD

THE GOLDEN BRIDGE AWARDS GOLD BEST 2013 BUSINESS WORLD

OREGON'S MOST ADMIRED COMPANIES 2012

Security Bloggers Network
All the security news fit to print

tripwire®

Tripwire is a leading provider of advanced threat, security and compliance solutions that enable enterprises, service providers and government agencies to confidently detect, prevent and respond to cybersecurity threats. Tripwire solutions are based on high-fidelity asset visibility and deep endpoint intelligence combined with business-context, and enable security automation through enterprise integration. Tripwire's portfolio of enterprise-class security solutions includes configuration and policy management, file integrity monitoring, vulnerability management and log intelligence. Learn more at tripwire.com.

SECURITY NEWS, TRENDS AND INSIGHTS AT TRIPWIRE.COM/BLOG ◆ FOLLOW US @TRIPWIREINC ON TWITTER

WPWCAGF1c 201503