CONNECTIONS SUMMIT

Cybersecurity – Why it Fails
Cyber Risk Management – Why it Succeeds

Carter Schoenberg, CISSP
EVP – Cybersecurity Solutions
IPKeys Power Partners

ELECTRICITIES of NORTH CAROLINA, INC.

LEARNING OBJECTIVES

By the end of this session you will be able to:

- Understand how to obtain buy-in from leadership
- Focus more on “risk” versus “threat”
- Dramatically reduce your organization’s exposure to harm

CORPORATE OVERVIEW

Overview

Established in March 2005

- Approx. 160 employees
- Cybersecurity
- Dept. of Defense (DOD)
- Public Safety Divisions
- Energy
  - IPKeys Power Partners
  - Hardware & Software

National Facilities

- California
- Maryland
- New Jersey
- Virginia
- Louisiana
- Texas

INC. Magazine Fastest 500
Growth in 2010 & 2011

UTILITY CLIENTS

Strategic Alliances

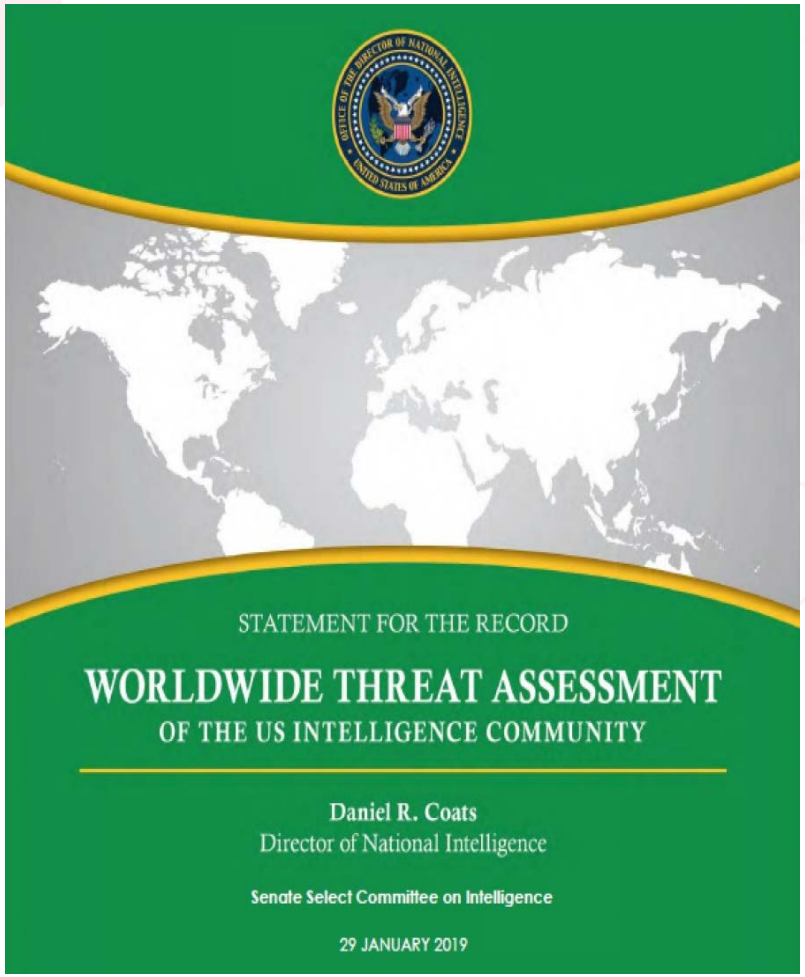
About Today's Presentation

IPKeys POWER PARTNERS

Getting from this

To this

Threat Landscape



Cyberattacks: China and Russia can disrupt US power networks warns intelligence report

Countries could launch damaging attacks against gas pipelines and electricity grid, says assessment.

By Steve Ranger | January 29, 2019 -- 17:29 GMT (09:29 PST) | Topic: Security

Russian Hackers Breach US Utility Networks via Trusted Vendors

Hackers were able to access confidential information, such as the equipment being used and how utility networks are configured.

JULIA PYPER | JULY 24, 2018

Officials say the cyberattack is likely still ongoing.

Russian hackers obtained access to the U.S. electric grid last year by penetrating the networks of key vendors that service power companies, homeland security officials said in a

TOP ARTICLES
MOST POPULAR MOST COMMENTS

Threat Landscape

you, your organization, and your personnel may be exposed or targeted during increased tensions can help you better prepare. In many cases, implementing the Cybersecurity and Infrastructure Security Agency (CISA) Cyber Essentials can dramatically improve your defenses. Should an incident occur, engage with partners, like CISA, and work with cyber or physical first responders to gain technical assistance. Review your organization from an outside perspective and ask the tough questions—are you attractive to Iran and its proxies because of your business model, who your customers and competitors are, or what you stand for?

Iranian Threat Profile and Activity

Recent Iran-U.S. tensions have the potential for retaliatory aggression against the U.S. and its global interests. Iran has exercised increasingly sophisticated capabilities to suppress social and political perspectives deemed dangerous to its regime and to target regional and international adversaries. Iran and its proxies and sympathizers have a history of leveraging cyber and physical tactics to pursue national interests, both regionally and here in the United States, such as:

- **Disruptive and destructive cyber operations** against strategic targets, including finance, energy, and telecommunications organizations, and an increased interest in industrial control systems and operational technology.
- **Cyber-enabled espionage and intellectual property theft** targeting a variety of industries and organizations to enable a better understanding of our strategic direction and policy-making.
- **Disinformation campaigns** promoting pro-Iranian narratives while pushing anti-U.S. sentiments.
- **Improvised explosive devices (IEDs)**, which are a staple tactic of the Islamic Revolutionary Guard Corps (IRGC), its Quds Force (focused on external, global operations), and proxy entities such as Hizbollah.
- **Attacks against U.S. citizens and interests abroad** and similar attacks in the Homeland.
- **Unmanned aircraft system (UAS) attacks** against hardened and soft targets.

CISA strongly urges you to assess and strengthen your basic cyber and physical defenses to protect against this potential threat

Sidebar

I am not a Medium or High – Therefore I have no obligations to be NERC-CIP compliant

NERC-CIP – This is “Compliance” and not “Cybersecurity”

I do not have inherent dependencies on a supply chain – “Our equipment has been operating just fine”

Relevant Trivia/Factoids for Businesses up to 500 employees:

1) 60% say they do not have a cyberattack prevention plan
2) Only 9% rank cybersecurity as a top business priority
3) Only 7% of CEOs say a cyberattack is likely

~ Keeper 2019 SMB Cybersecurity Study

Don’t let PRIDE be a downfall

Procrastination –“We’ll get to it later.”

Rationalizing – “We are not connected to the Internet in any way”

Ignoring the Issue – “Cybersecurity doesn’t apply to us. We don't have anything anyone would want.“

Denial – “Spending money on cybersecurity won’t stop an attack, so why bother.”

Excuses – “It’s too complicated,” "We don't have the budget or expertise.“

Threat and Legal Landscape

Legal Exposure

“Everyone in the IoT supply chain is at risk if they don’t meet the applicable “standard of care,” a legal term that varies somewhat depending on the particular legal claims at issue, but essentially means responsible cybersecurity design.” – *Ijay Palansky (Litigation Attorney 3/28/19)*

Standard of Care

The watchfulness, attention, caution and prudence that a reasonable person in the circumstances would exercise. *If a person's actions do not meet this standard of care, then his/her acts fail to meet the duty of care which all people (supposedly) have toward others*. Failure to meet the standard is negligence, and any damages resulting therefrom may be claimed in a lawsuit by the injured party. - (Dictionary Law)

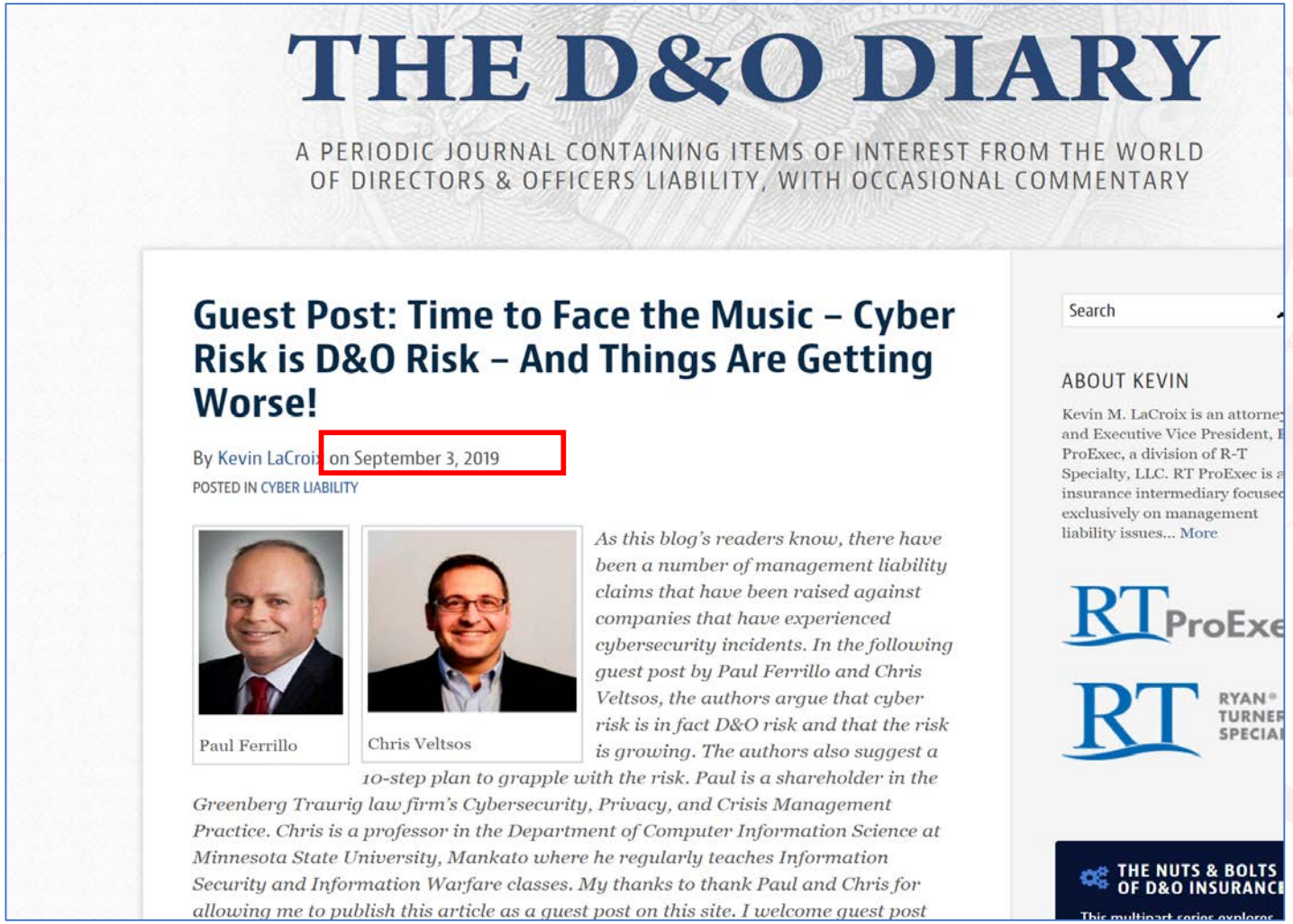
Due Diligence + Due Care (taking action) = “Standard of Care”

Threat and Legal Landscape

IPKeys POWER PARTNERS

Legal Exposure - Continued

Backstops for offsetting financial risks is becoming more problematic as regulators, state prosecutors, and insurance become more acutely aware of risk mitigation best practices.



THE D&O DIARY

A PERIODIC JOURNAL CONTAINING ITEMS OF INTEREST FROM THE WORLD OF DIRECTORS & OFFICERS LIABILITY, WITH OCCASIONAL COMMENTARY

Guest Post: Time to Face the Music – Cyber Risk is D&O Risk – And Things Are Getting Worse!

By Kevin LaCroix on September 3, 2019

POSTED IN CYBER LIABILITY

Paul Ferrillo

Chris Veltsos

As this blog's readers know, there have been a number of management liability claims that have been raised against companies that have experienced cybersecurity incidents. In the following guest post by Paul Ferrillo and Chris Veltsos, the authors argue that cyber risk is in fact D&O risk and that the risk is growing. The authors also suggest a 10-step plan to grapple with the risk. Paul is a shareholder in the Greenberg Traurig law firm's Cybersecurity, Privacy, and Crisis Management Practice. Chris is a professor in the Department of Computer Information Science at Minnesota State University, Mankato where he regularly teaches Information Security and Information Warfare classes. My thanks to thank Paul and Chris for allowing me to publish this article as a guest post on this site. I welcome guest post

Search

ABOUT KEVIN

Kevin M. LaCroix is an attorney and Executive Vice President, ProExec, a division of R-T Specialty, LLC. RT ProExec is insurance intermediary focused exclusively on management liability issues... More

RT ProExec

RT RYAN TURNER SPECIAL

THE NUTS & BOLTS OF D&O INSURANCE

Defining Cyber Risk Versus Cybersecurity

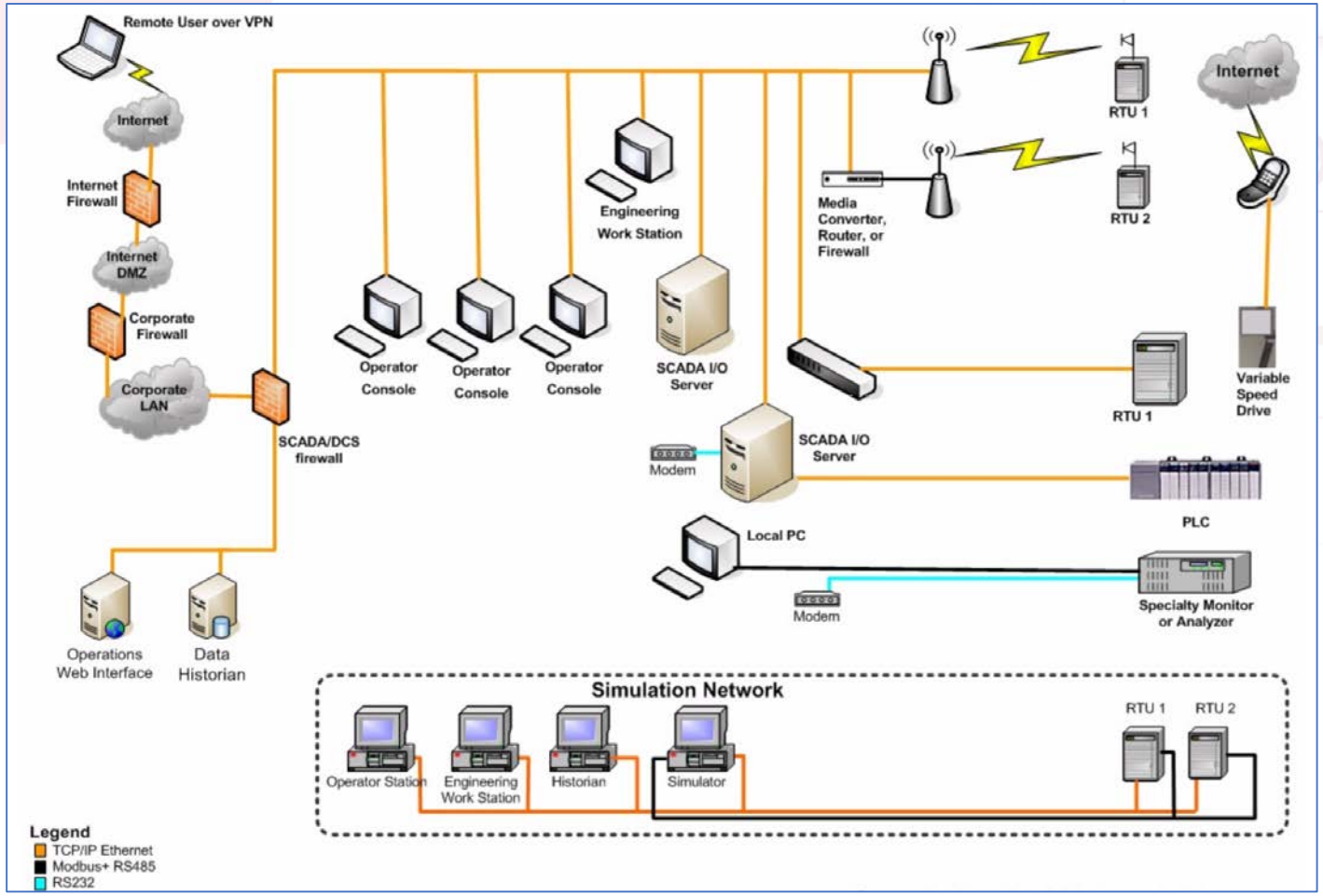
Cybersecurity - the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.

Cyber Risk – Presence of a material weakness exists that has a heightened potential to have a significant impact on the enterprise resulting in one or more of the following:

- **Cyber incident resulting in system disruption or data spillage of sensitive information that required proper safeguarding**
- **Cyber incident resulting in a "harm trigger" resulting in increased exposure to private causes of action and/or investigation (with financial sanctions) from state attorney generals or Federal Trade Commission.**

Simply assessing the "technology position" of an enterprise does not equate to a reduction in cyber risk

20th vs. 21st Century Networks



20th Century Approach

- Easily Defined
- Partitioned from the Internet
- Limited “transition points” to serial based networks

Thought Process

- Security through Obscurity
- “We have a firewall”

20th vs. 21st Century Networks

21st Century Approach

- Enablement of IoT
- Support of Smart Cities
- Highly Integrated Distributed Energy Resources (energy supply chain)
- Demand Management (Smart Meters)
- Mobile devices

Thought Process

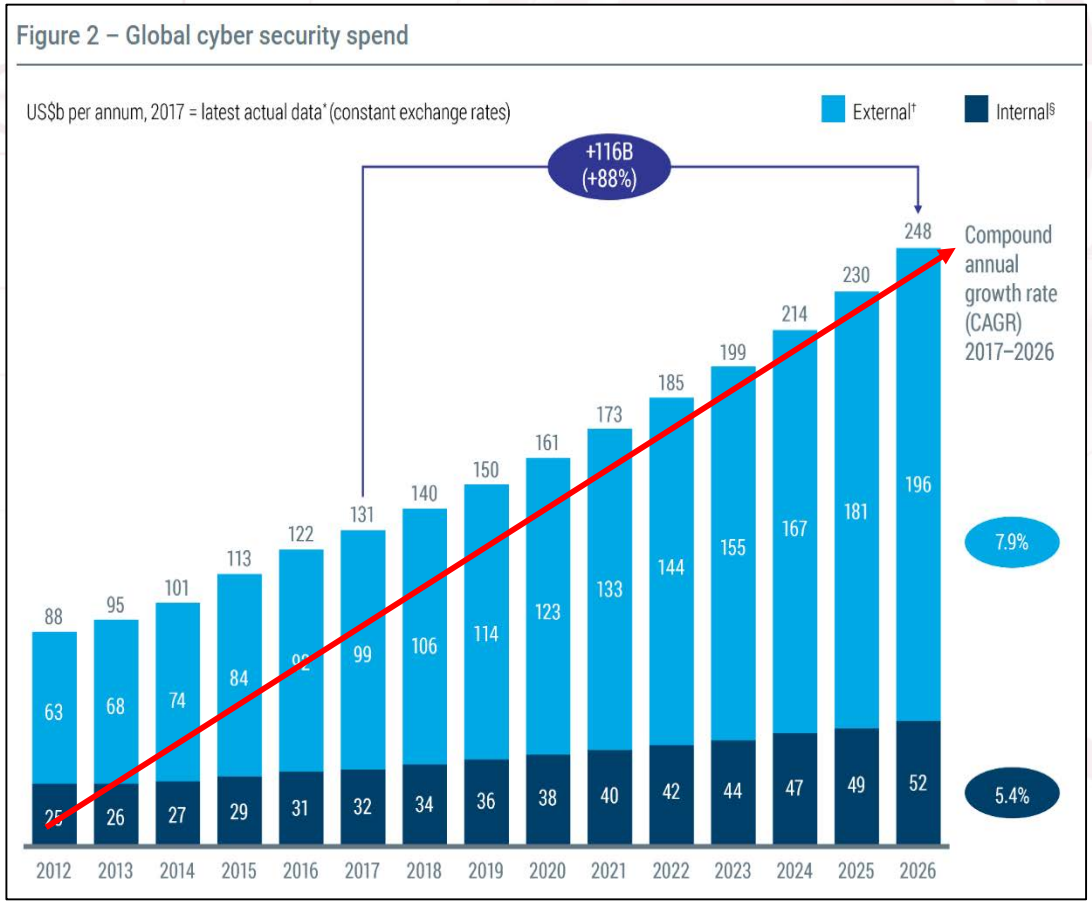
- Follow NERC
- Compliance vs. Risk Management

The Marketplace

More money is spent today on Cybersecurity now than ever before!

Monies spent, *but wisely*? How are risk profiles Improved? (Majority of investment in new Tech only)

How does OT or IoT figure in?



Shaping Cyber Risk for C-Suite and BOD

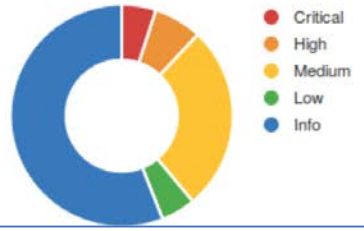
Stop trying to tell a “technical storyline”

Severity	Plugin Name	Plugin Family	Count
CRITICAL	CentOS 6 / 7 : openssl (CE…	CentOS Local Security Checks	1
CRITICAL	CentOS 7 : glibc (CESA-201…	CentOS Local Security Checks	1
HIGH	CentOS 7 : graphite2 (CESA…	CentOS Local Security Checks	1
HIGH	CentOS 7 : kernel (CESA-20…	CentOS Local Security Checks	1
HIGH	CentOS 7 : mariadb (CESA-…	CentOS Local Security Checks	1
MEDIUM	CentOS 5 / 6 / 7 : bind (CES…	CentOS Local Security Checks	1
MEDIUM	CentOS 6 / 7 : ipa / libldb / li…	CentOS Local Security Checks	1
MEDIUM	CentOS 6 / 7 : libssh2 (CES…	CentOS Local Security Checks	1
MEDIUM	CentOS 6 / 7 : nss-util (CES…	CentOS Local Security Checks	1
MEDIUM	CentOS 6 / 7 : samba (CES…	CentOS Local Security Checks	1

Host Details

IP:	192.168.56.102
DNS:	st91.i
MAC:	08:00:27:db:3e:a2
OS:	Linux Kernel 3.10.0-327.4.5.el7.x86_64 on CentOS Linux release 7.2.1511 (Core)
Start:	May 11 at 10:34 PM
End:	May 11 at 10:39 PM
Elapsed:	6 minutes
KB:	Download

Vulnerabilities

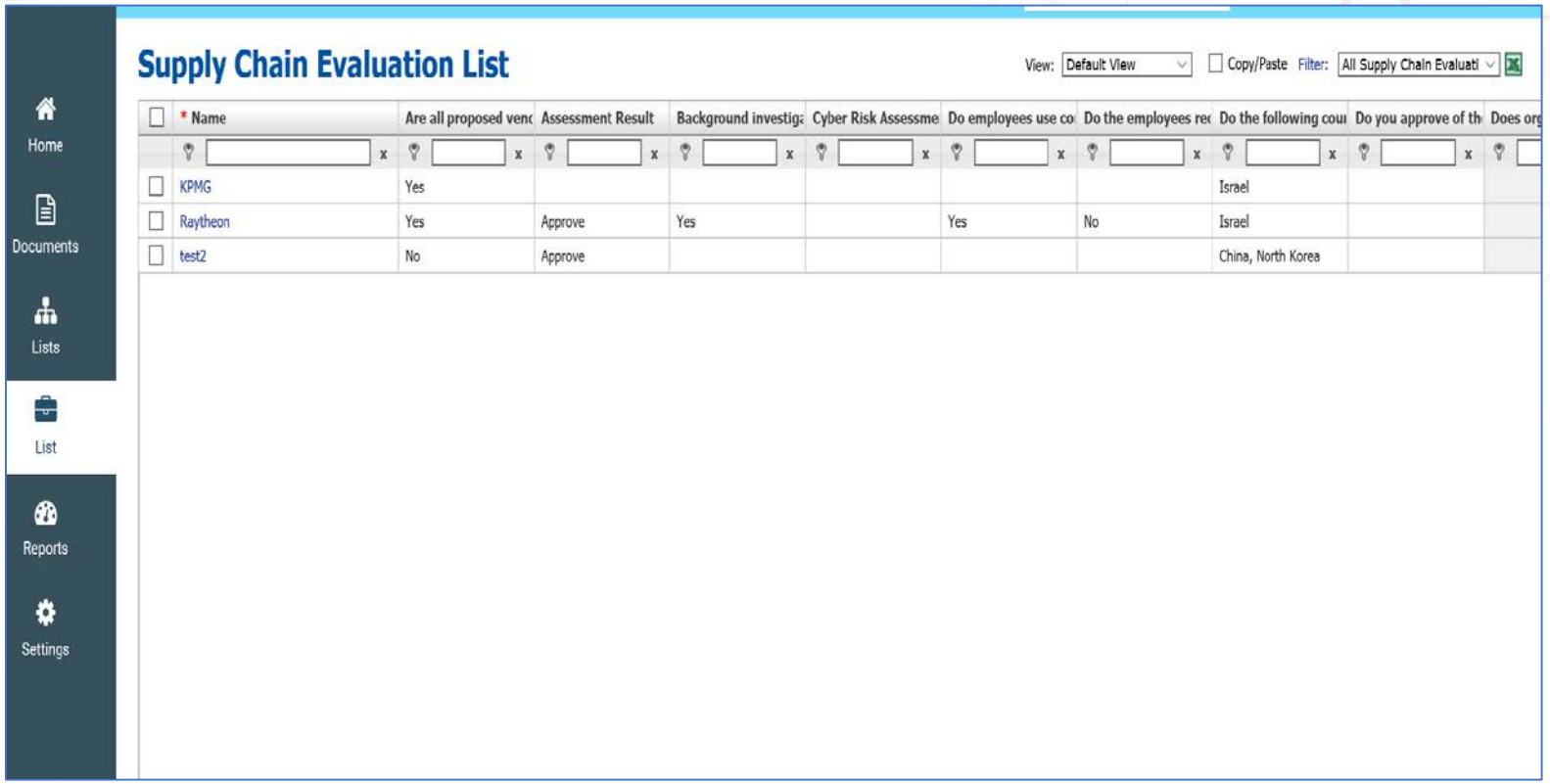


Do not expect business owners and leaders to “***get it***”

Automation to Improve Fidelity and Efficiency

IPKeys POWER PARTNERS

Humans are only as efficient as the technology at their disposal



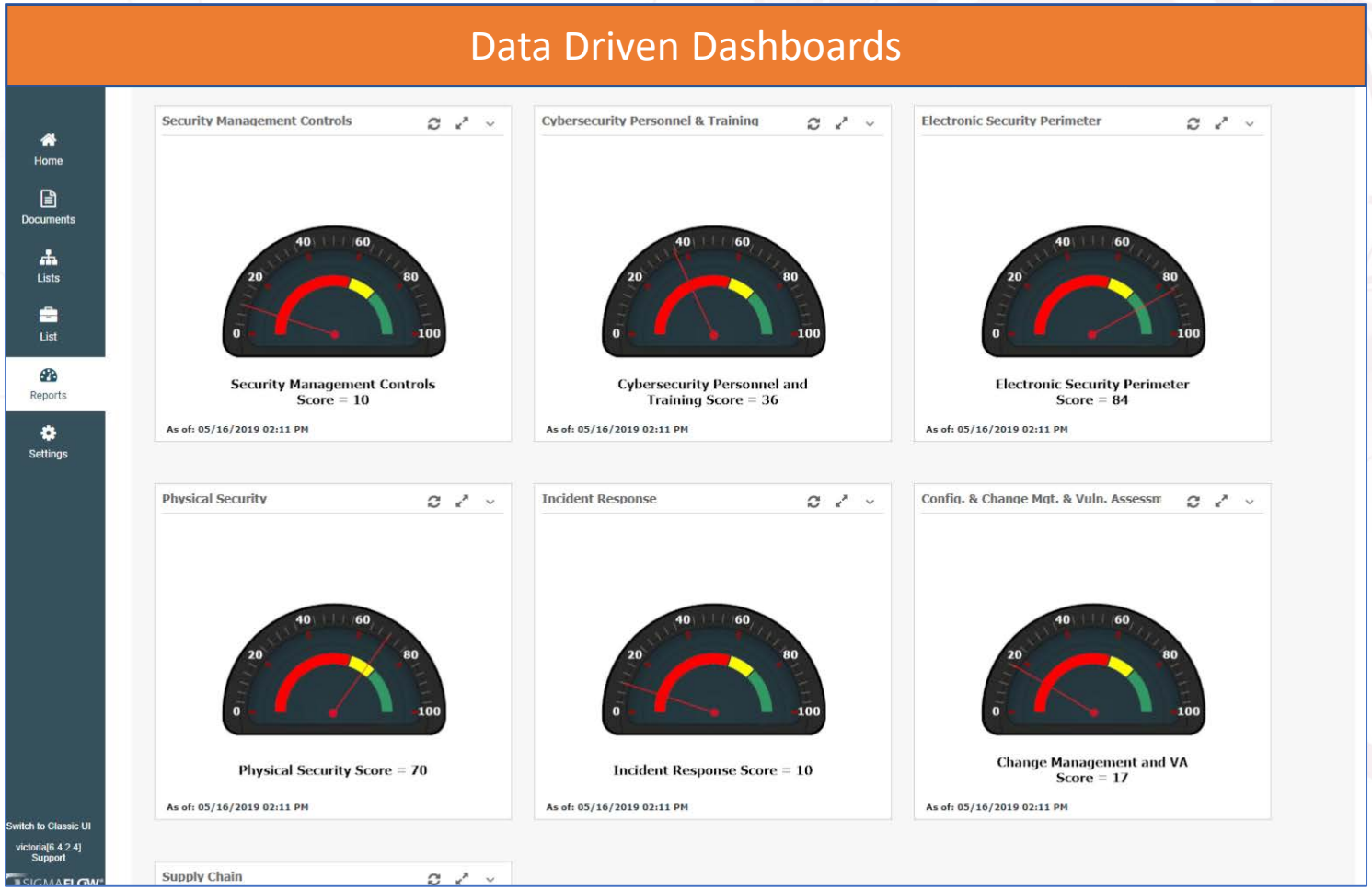
* Name	Are all proposed venc	Assessment Result	Background investig	Cyber Risk Assessme	Do employees use co	Do the employees rec	Do the following cou	Do you approve of th	Does org
KPMG	Yes						Israel		
Raytheon	Yes	Approve	Yes		Yes	No	Israel		
test2	No	Approve					China, North Korea		

Automation Saves Time =
Saving Cost

Automation to Improve Fidelity and Efficiency

IPKeys POWER PARTNERS

Automation enables “snap-shot visibility



Shaping Cyber Risk for C-Suite and BOD

Frame the Costs and the Liability

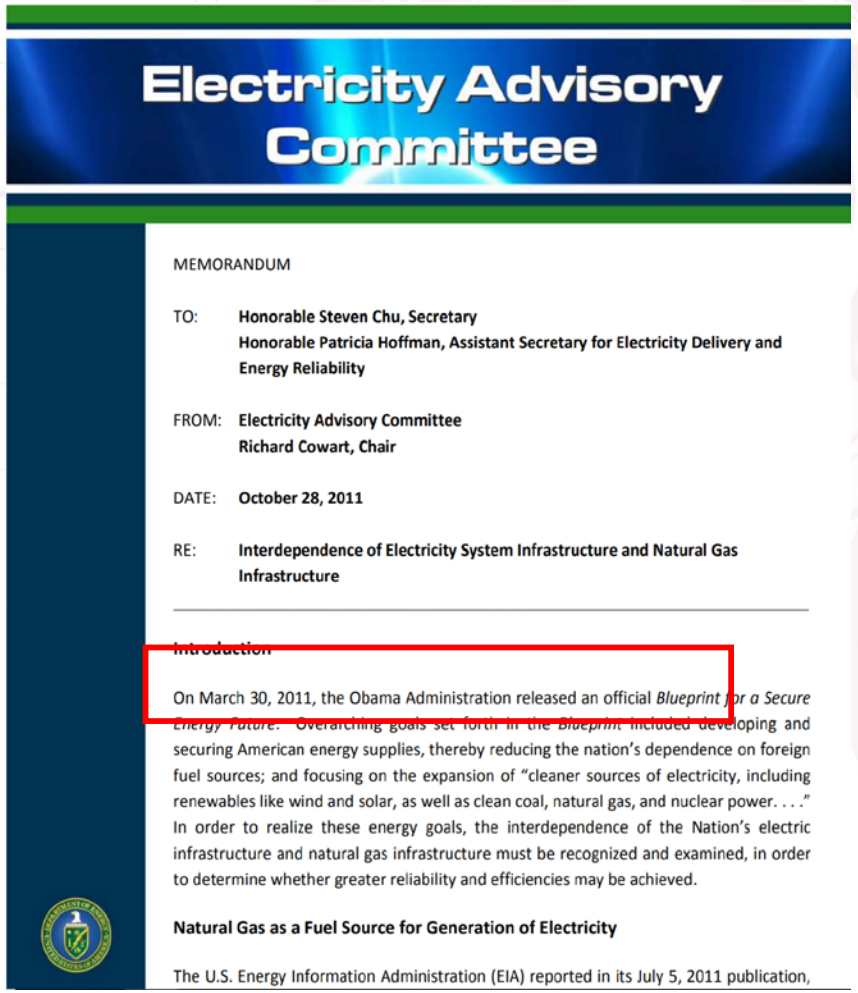
Finding	Resolution	Cost to Implement
Current server acting as a High Value Asset in support of BES is running MSFT 2008 r2	Upgrade to MSFT 2016	$37,216 (IT staff Man hours and license)
Lack of Configuration/ Change Management automation created a number of change logs that could not be attributable	Identify automation solution (Sigmaflow)	$275,000
Lack of established contract language to limit supply chain cyber risk exposure	Revise SLAs or other legally binding agreements	$26,513
Cost Considerations		**$338,729**

Cost of Crisis Management	Comments
$173,245 (Same IT staff, + downtime of up to 1.2 hours impacting bill rate at $163,245 per hour)	• Liability exposure to notifying NERC or “Other” resulting in lost manpower due to audit • Sanctions estimated at $8,300 per day
See comments	• Current level of effort can be reduced by 64% = savings of $347,000 (annually)
• Incident response $427,000 • Incident notification and audit response $198,000	• Ensure any changes to language include requirements for cyber(1st and 3rd party) damages above $625,000
$1,145,245	**TCO Reduction $806,516 or ROI: 3.38:1**

Supply Chain

While CIP-013-1 is designed to focus on products and services purchased by the entity, the "threats" may go beyond.

- Service Level Agreements
- Terms & Conditions
- RFP's



Electricity Advisory Committee

MEMORANDUM

TO: Honorable Steven Chu, Secretary
Honorable Patricia Hoffman, Assistant Secretary for Electricity Delivery and Energy Reliability

FROM: Electricity Advisory Committee
Richard Cowart, Chair

DATE: October 28, 2011

RE: Interdependence of Electricity System Infrastructure and Natural Gas Infrastructure

Introduction

On March 30, 2011, the Obama Administration released an official *Blueprint for a Secure Energy Future*. Overarching goals set forth in the *Blueprint* included developing and securing American energy supplies, thereby reducing the nation's dependence on foreign fuel sources; and focusing on the expansion of "cleaner sources of electricity, including renewables like wind and solar, as well as clean coal, natural gas, and nuclear power. . . ." In order to realize these energy goals, the interdependence of the Nation's electric infrastructure and natural gas infrastructure must be recognized and examined, in order to determine whether greater reliability and efficiencies may be achieved.

Natural Gas as a Fuel Source for Generation of Electricity

The U.S. Energy Information Administration (EIA) reported in its July 5, 2011 publication,

“Liability/Risk” vs. Compliance

Mapping of NIST Cybersecurity Framework v1.0 to NERC CIP version 5 & C2M2 Practices						
Function	Category	Subcategory	C2M2 Practices **			NERC CIP v5
			MIL 1	MIL 2	MIL 3	
IDENTIFY (ID)	**Asset Management (AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	ACM-1a	ACM-1c	ACM-1e ACM-1f	CIP-002-5.1 R1 Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: i. Control Centers and backup Control Centers; ii. Transmission stations and substations; iii. Generation resources; iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements; v. Special Protection Systems that support the reliable operation of the Bulk Electric System (BES); and vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

NIST Technical Note 2051

Cybersecurity Framework Smart Grid Profile

Jeffrey Marron
Avi Gopstein
Nadya Bartol
Valery Feldman

This publication is available free of charge from:
https://doi.org/10.6028/NIST.TN.2051

Contact Details

Carter Schoenberg, CISSP
Executive Vice President – Cybersecurity Solutions
cschoenberg@ipkeys.com
(732) 982-3148 Desk
(202) 660-8066 Cell

www.ipkeyspowerpartners.com

ELECTRICITIES
of NORTH CAROLINA, INC.
The energy behind public power

www.electricities.com

FOLLOW US ON SOCIAL MEDIA:

@ElectriCitiesNC

facebook.com/company/ElectriCitiesNC

@ElectriCitiesNC