

Cyber Security Panel Discussion

Gary Hayes, SVP & CIO Technology Operations

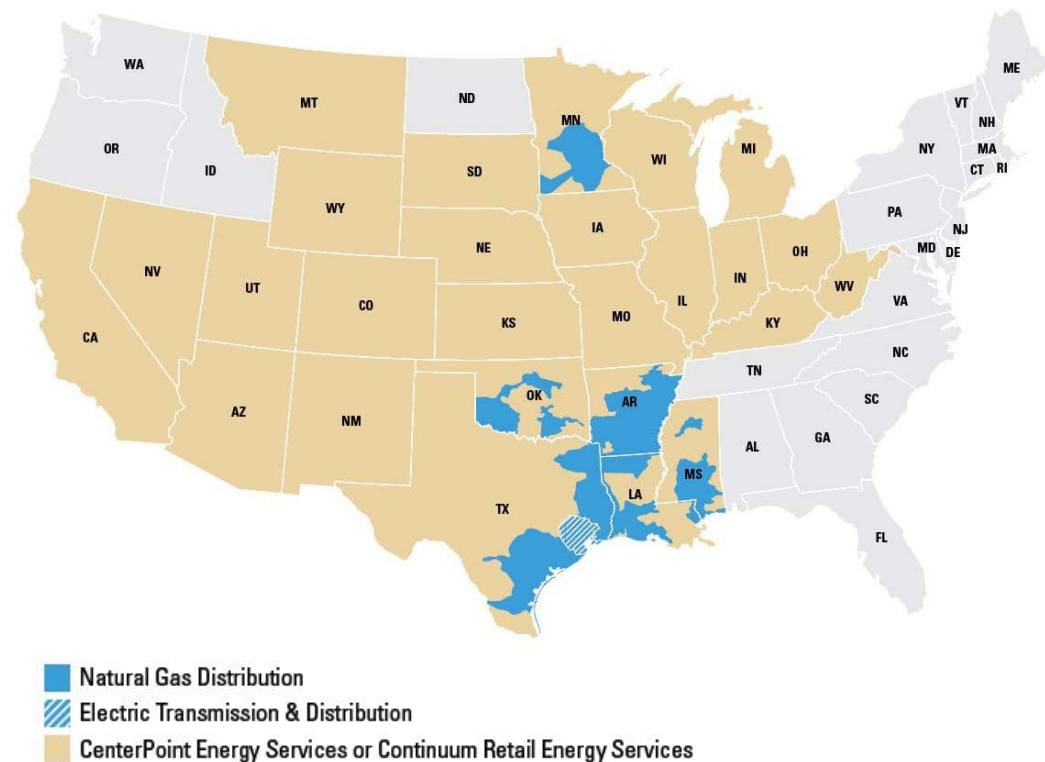
Arkansas Joint Committee on Energy

March 16, 2016



CenterPoint Energy, Inc. (NYSE: CNP)

Regulated Electric and Natural Gas Utility Serving more than 5.7 Million Customers



CNP - Arkansas

Providing reliable, safe and economic gas distribution services to over 420,000 customers in 229 communities.

Electric Transmission & Distribution:

- Electric utility operations with ~2.3 million metered customers across ~5,000 square miles in and around Houston, Texas
- 19th largest U.S. investor-owned electric utility by customer base ⁽¹⁾
- 84,190,647 MWh delivered in 2015

Gas Operations:

- 10 regulated gas distribution jurisdictions in six states with ~3.4 million customers
- 6th largest U.S. gas distribution company by customer base ⁽¹⁾
- Non-regulated competitive natural gas supply and related energy services serving nearly 24,000 commercial and industrial customers across 26 states ⁽²⁾
- Gas distribution company and energy services company delivered ~1.1 TCF of natural gas in 2015

⁽¹⁾ As of Dec. 31, 2014 per EEI and AGA

⁽²⁾ Includes Continuum's energy services customers and operational footprint; acquisition expected to close in March or April 2016

What organizations shape cyber security governance for the natural gas industry?

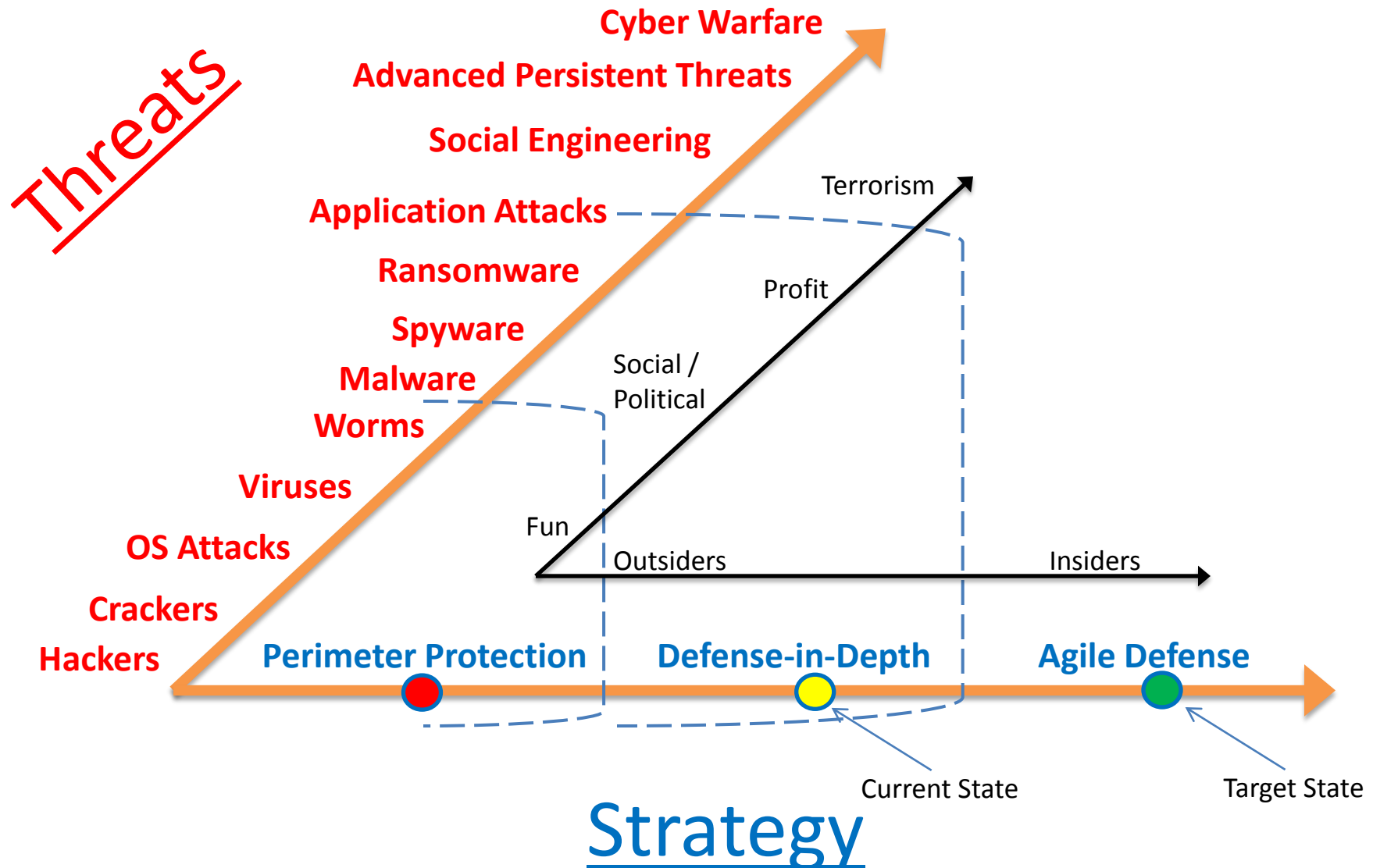
- **DHS Transportation Security Administration (TSA)** has regulatory authority over pipeline security
- **DHS Infrastructure Security Compliance Division (ISCD)** regulate various portions of LDC operations with chemical storage
- **DOT Pipeline and Hazardous Materials Safety Administration (PHMSA)** has regulatory authority over pipeline and facility safety
- **DHS U.S. Coast Guard** has regulatory authority over safety and security of LDCs within maritime jurisdiction
- **DOE Office of Electricity Delivery & Energy Reliability** oversees energy (natural gas) reliability and supply
- **State Utility Commissions** have various regulatory authorities over pipeline safety and security

What is a cyber security threat?

- It is an **employee unknowingly clicking a link in an email or web page** bringing a malicious program onto their laptop and spreading it across the corporate network
- It is a **thumb drive from a co-worker** which contains a chip with an embedded program intent on gaining access so it can broadcast intellectual property files out to a third party
- It is an **internal or external person committing cyber crime** by injecting malicious code into your system. Someone who is an employee, janitor, contractor...with the intent to disrupt the business
- It is an **“organization making a statement”** about your company, or a company you do business with, by attacking your web site disrupting or denying service to your customers or partners
- It is **organized crime penetrating customer account files** to facilitate fraudulent monetary exchanges or find insider information for their financial advantage
- It is a **nation state seeking intellectual property** to advance politically, financially or technically. They are seeking those who are leaders in technology (smart meters, intelligent grid...)
- It is a **nation state or terrorist group seeking to disrupt the U.S. financial system or critical infrastructure** (electric, gas, pipeline, water..). A sophisticated “advanced persistent threat”

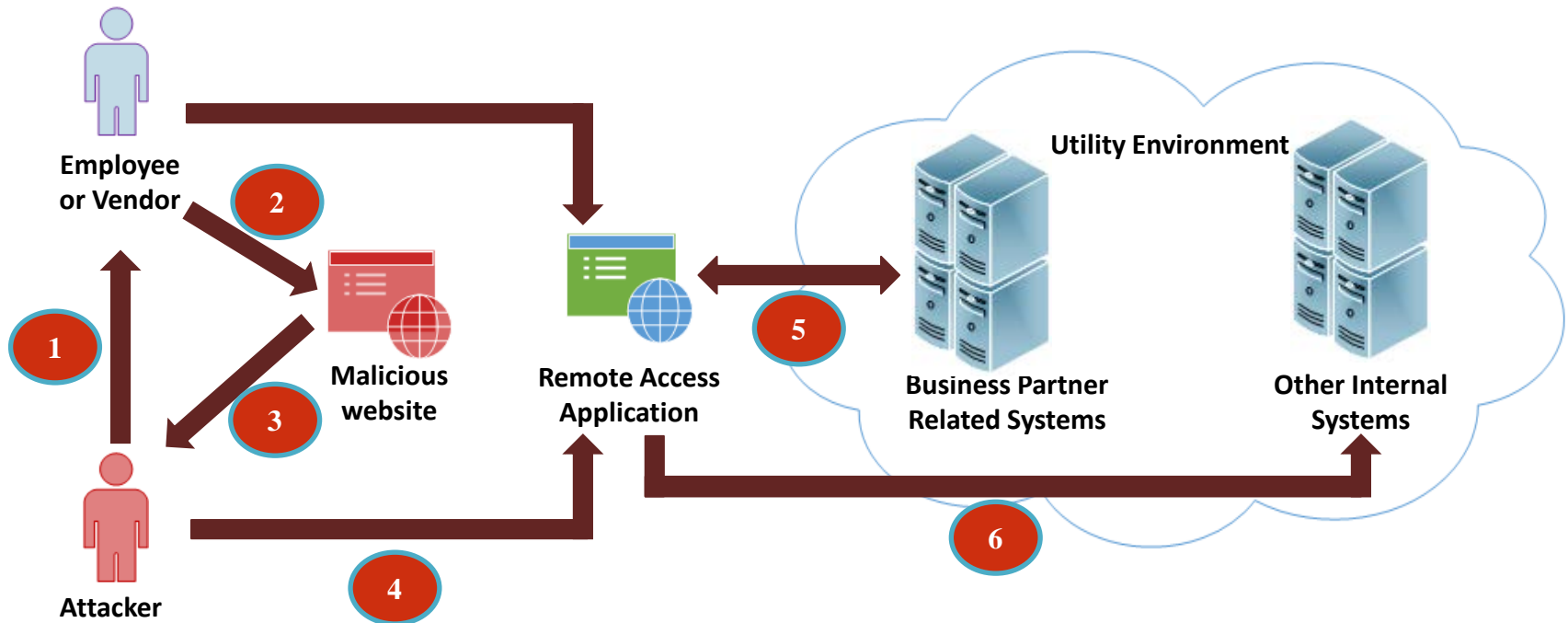
How do we understand cyber security?

Threats, Motivators, Actors, and Strategies



How does a cyber event happen?

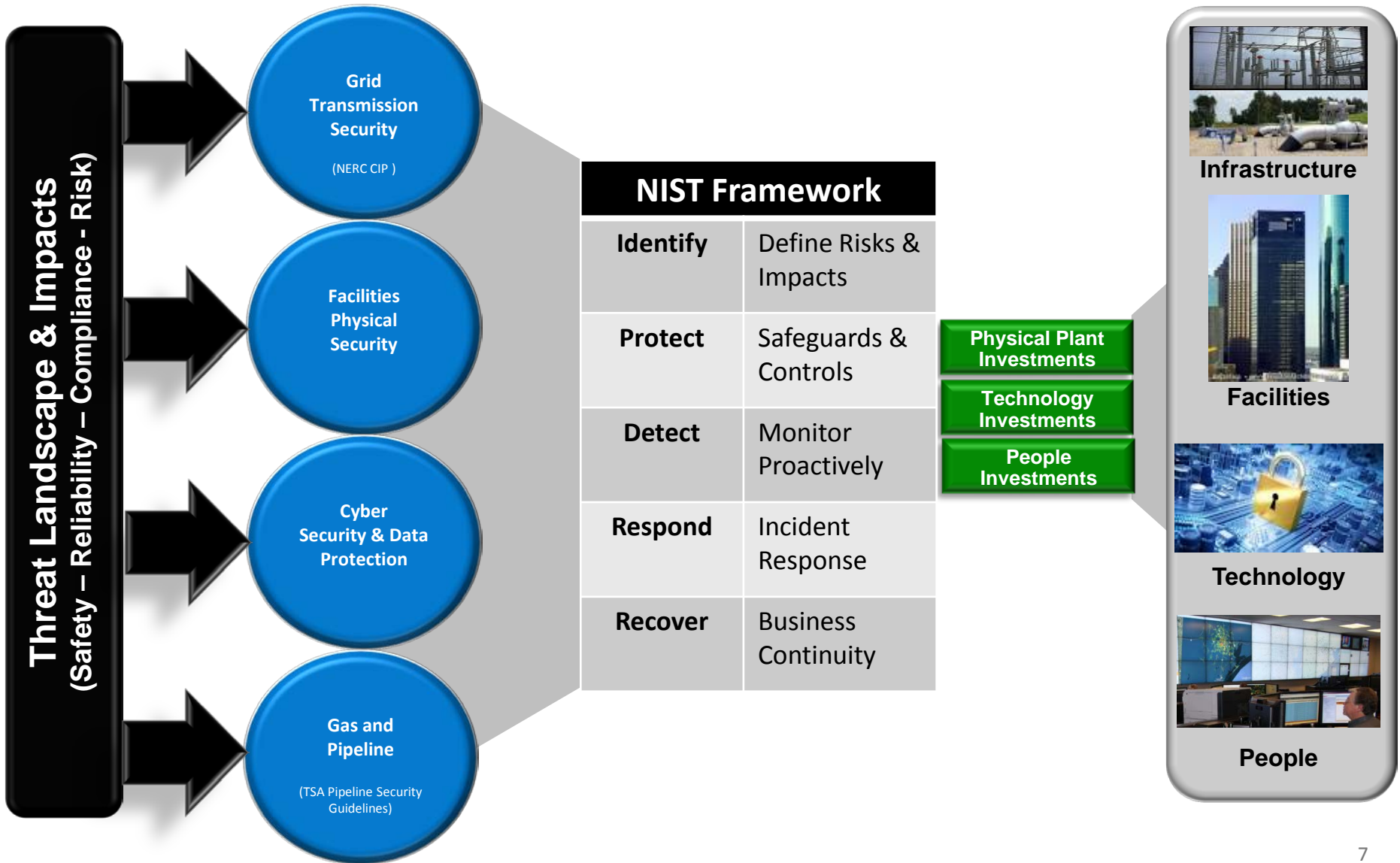
Social Engineering : Gaining Login Credentials



Step	Description
1 2 3	Attacker manipulates employee / vendor and gains login credentials
4	Attacker accesses remote access application using the stolen credentials
5	Attacker accesses the systems related to the employee / vendor
6	Attacker discovers and compromises other internal systems in the environment

What is the emerging threat landscape

A broader context of the NIST Framework provides an understanding of the significant focus on physical and cyber security...

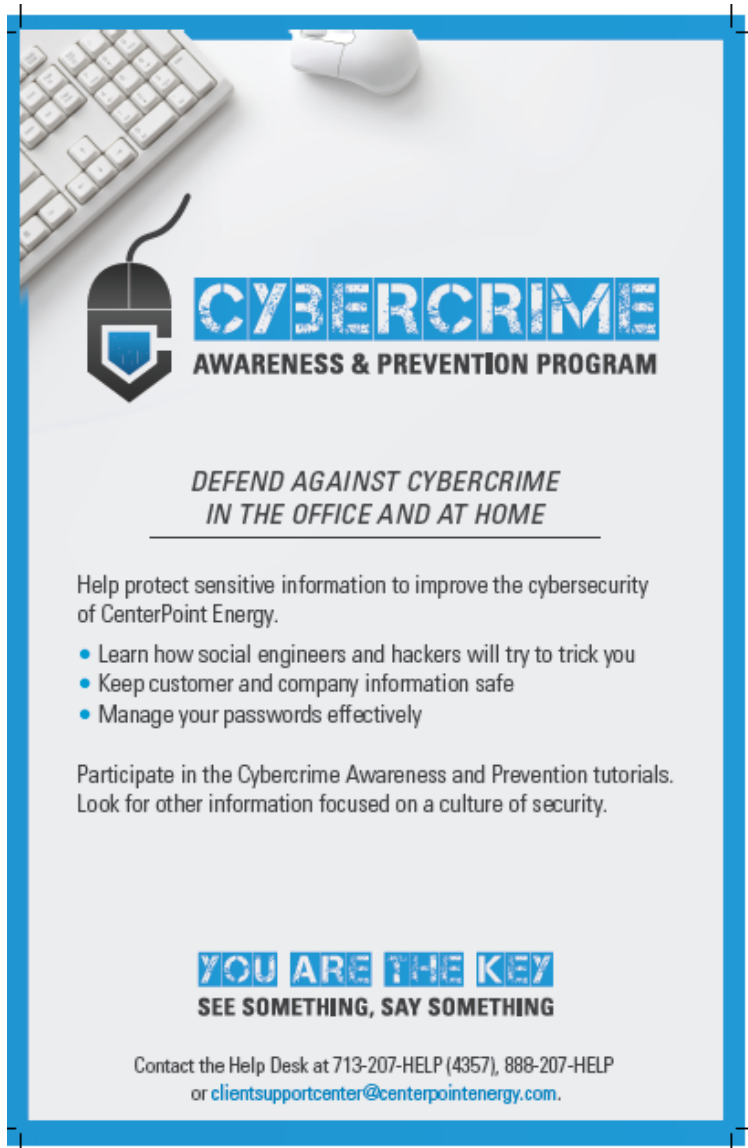


Example: Threat and Risk Matrix

Threat	Risk	Mitigation	Rationale
3rd Party Access Vulnerability	Access to a network via a third party connection inside our firewall. Example: A vendor supporting building HVAC systems.	Multi-Factor Authentication	A multi-factor authentication requires secure access by validating several attributes. These attributes significantly reduce the risk.
Non-Authorized Access the Business Network	A user with an ID and password could interrogate sections of technology systems and attempt an exploit.	Segment critical applications and data sets for the operational and user network.	Controlled network segments reduce the number of users who can access critical data and systems. Note: Control system segmentations for critical infrastructure.
Data Theft	Valuable data is moved to unsecure networks or endpoint devices.	Monitor and control sensitive data movement via the Data Loss Prevention system.	Monitoring data movement and storage allows security analysts to establish a common operating model and prevent non-business data access.
Integrated Cyber and Physical Security Event	No correlation of cyber and physical security events. Security events are logged but not detected.	Security Information and Event Management (SIEM) Implementation. Building an "Integrated Security Operation Center" joining Cyber and Physical.	Through event correlation technology and human monitoring, events are detected and responded to prior to the failure of established security controls.

Employee & Contractor Cybercrime Campaign

Our greatest cyber defense...see something, say something



The poster features a white computer keyboard and mouse in the top left corner. The main title is "CYBERCRIME AWARENESS & PREVENTION PROGRAM" with a logo of a computer mouse with a shield on its cord. Below the title is the text "DEFEND AGAINST CYBERCRIME IN THE OFFICE AND AT HOME". A paragraph states: "Help protect sensitive information to improve the cybersecurity of CenterPoint Energy." followed by a bulleted list: "• Learn how social engineers and hackers will try to trick you", "• Keep customer and company information safe", and "• Manage your passwords effectively". Another paragraph says: "Participate in the Cybercrime Awareness and Prevention tutorials. Look for other information focused on a culture of security." At the bottom, it says "YOU ARE THE KEY SEE SOMETHING, SAY SOMETHING" and provides contact information: "Contact the Help Desk at 713-207-HELP (4357), 888-207-HELP or clientsupportcenter@centerpointenergy.com."

CYBERCRIME
AWARENESS & PREVENTION PROGRAM

*DEFEND AGAINST CYBERCRIME
IN THE OFFICE AND AT HOME*

Help protect sensitive information to improve the cybersecurity of CenterPoint Energy.

- Learn how social engineers and hackers will try to trick you
- Keep customer and company information safe
- Manage your passwords effectively

Participate in the Cybercrime Awareness and Prevention tutorials. Look for other information focused on a culture of security.

YOU ARE THE KEY
SEE SOMETHING, SAY SOMETHING

Contact the Help Desk at 713-207-HELP (4357), 888-207-HELP
or clientsupportcenter@centerpointenergy.com.

Employee Comments:



This is a serious threat. we should all be concerned and all be committed to preventing this type of cybercrime. looking forward to the tutorials

Great video and initiative to make everyone aware that cybercrime isn't just something to be concerned with while at work.

Great information, this is an ever growing threat we all need to be more aware of.

Cyber Mitigation for Customer Accounts

Multi-factor Authentication...

An authentication approach that ensures that **a user is who they claim to be**. The more factors used to determine a person's identity, the greater the trust of authenticity.

Knowledge Authentication	Authentication Tokens	Biometric Authentication	Inferential Authentication
Textual Words, phrases, numbers and so on	OOB Authentication Using another channel	Biological Trait A physiological trait of the user	Q&A Known answers to specific questions
Graphical Images, patterns or gestures	OTP Token Using a secret key to generate an OTP	Behavioral Trait The way the user performs an action	Contextual Authentication Analysis of contextual data
	X.509 Token Using PKI credentials		
	Other Token Using some other mechanism		

Multi-factor authentication can be achieved using a combination of the following factors:

Something You Know – password or PIN
Something You Have – token, smart card or knowledge (two-factor authentication)
Something You Are – biometrics, such as a fingerprint (three-factor authentication)



Information sharing is critical! DNG-ISAC, E-ISAC...



"Information sharing is a fundamental pillar of a robust cyber and physical defense effort. The DNG ISAC is tailored to address the distinct operational needs of the downstream natural gas sector and provides the technological sophistication and coordination necessary to meet the ever-changing threats of the 21st century."

Dave McCurdy
AGA President and CEO



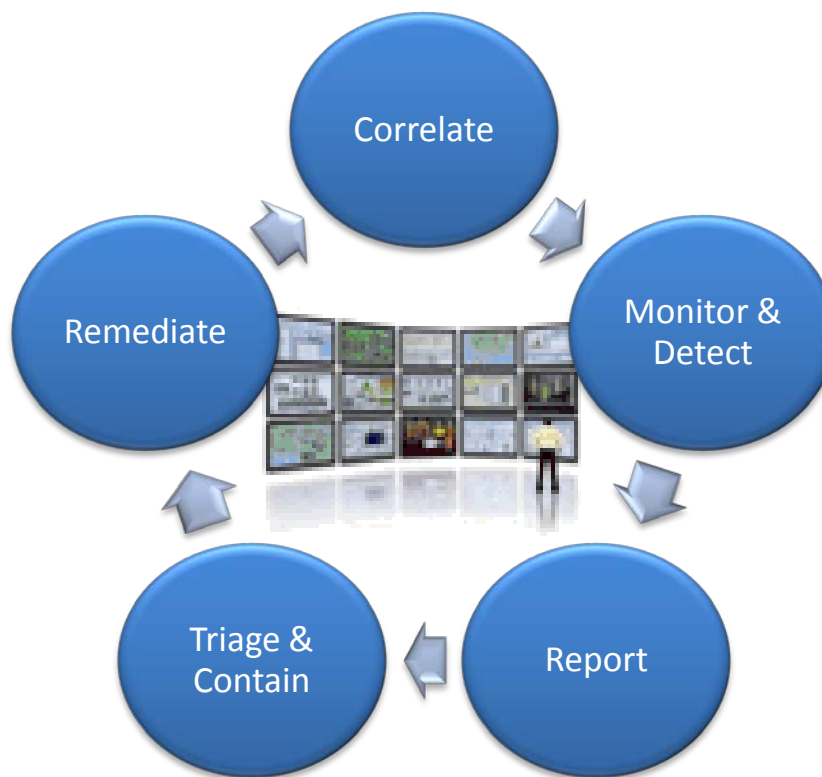
In 2014, AGA launched the Downstream Natural Gas Information Sharing and Analysis Center.

The DNG ISAC is an online platform that will help natural gas utilities share and access timely, accurate and relevant threat information and further enhance the security of natural gas utilities.

"UNITY OF EFFORT"

Next Generation Security Operations Center

CenterPoint is in the process of advancing and maturing a Cyber Security Operations Center (“CSOC”) to identify, correlate, report and remediate vulnerabilities across the enterprise and operations.



CenterPoint Security Monitoring

Public information on current global attacks.



This now includes Cyber Risk & Information Sharing Program (CRISP) and other sources of threat information (E-ISAC, DNG-ISAC, CERT..



Security Operations Information – These windows display information from the Internet Storm Center.

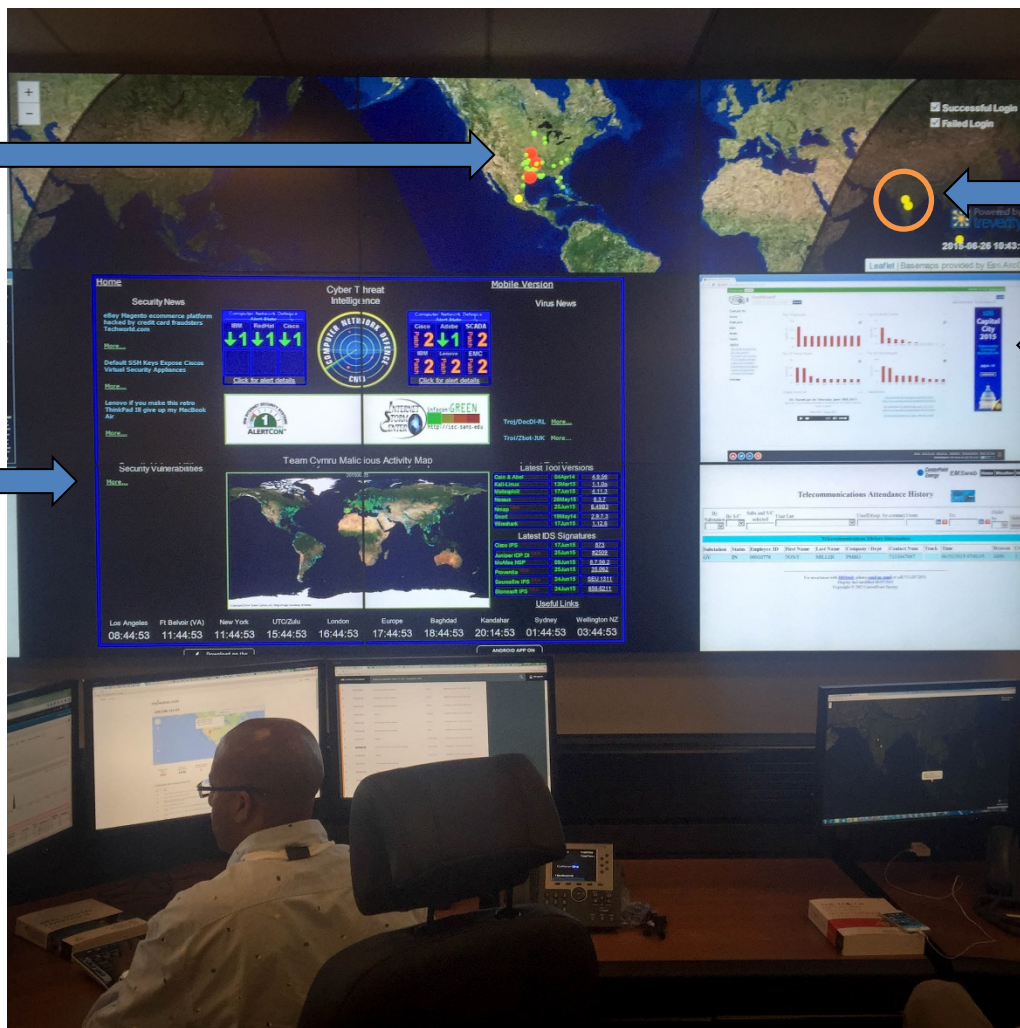
Sample of Threat Information Provided to Monitoring Team

Geospatial map of remote connections to CenterPoint

SANS Internet Storm Center (Situational Awareness)

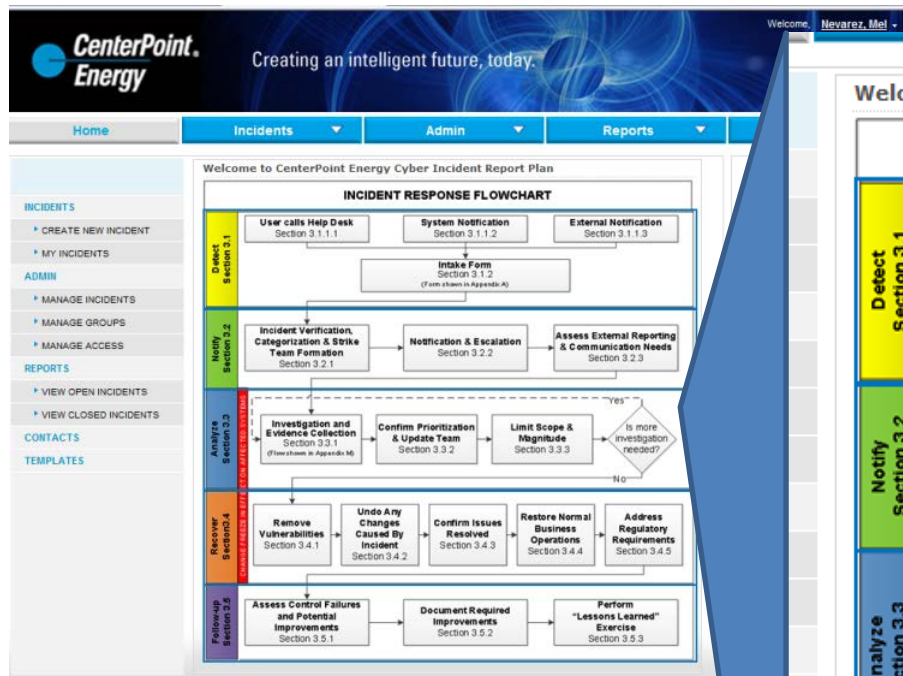
Example of CenterPoint third-party providers.

Current frequency of Attack Vectors



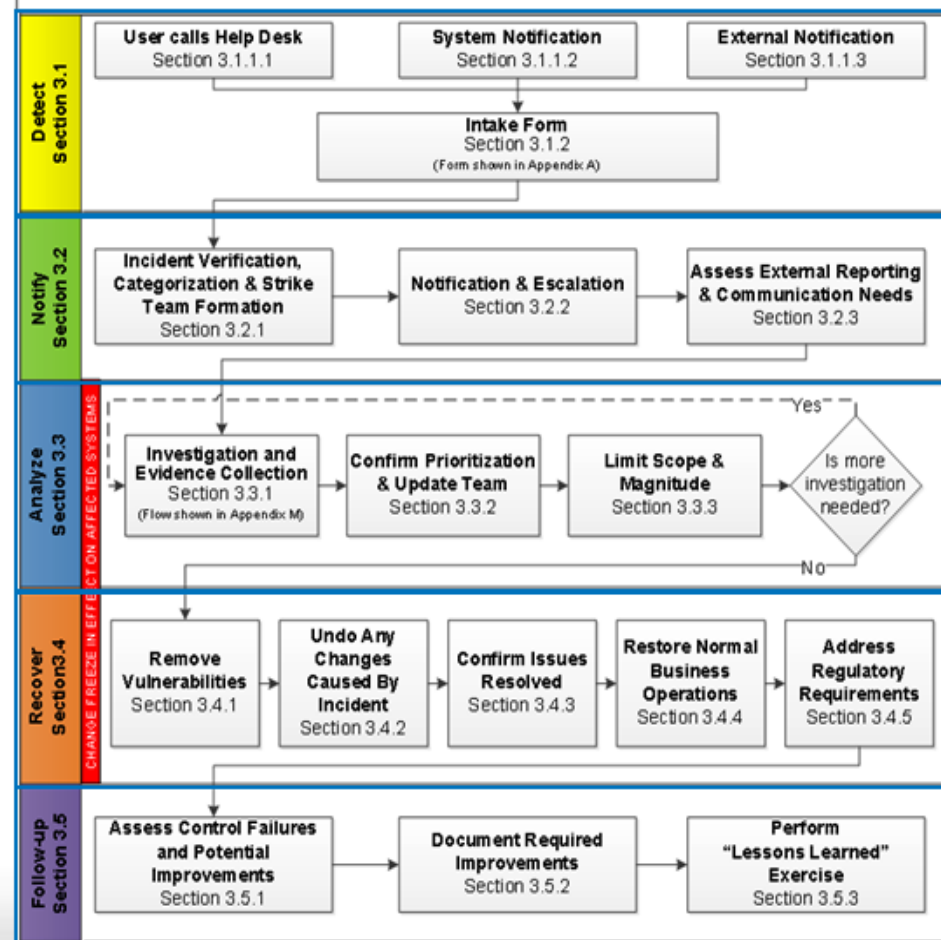
Cyber Incident Response Plan (CIRP)

Structured interactive plan to manage the cyber incident...

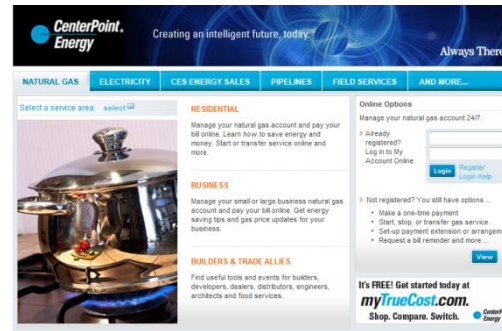


Welcome to CenterPoint Energy Cyber Incident Report Plan

INCIDENT RESPONSE FLOWCHART



What about the customer?



"Is it safe to pay my bill on-line?"

CenterPoint Energy is aware of the security vulnerability called "Heartbleed"...to date we have found no evidence that this bug has resulted in the improper access of any of our systems or data.

Do I need to change my password?

Our My Account Online system does not use OpenSSL and isn't vulnerable to this bug. So there's no need to change your password at this time. However, it is good security practice to regularly update all your Internet passwords.



What are the key takeaways?

- **Recognize our challenges and efforts:**
 - We face an ever growing, ever more serious, threat to the security of our systems and data
 - We continue to implement more sophisticated layers of defense and response to what we learn from government and other sources about these threats
 - We continue to work with and through all industry groups (gas, electric and others), as well as government agencies, to be completely responsive to these threats
 - We provide employee awareness and education. Employees are our first line of defense and the key to all our security efforts. We continue to emphasize criticality of cyber security training and require it for all new hires as well as annual training & testing
- **Understand that:**
 - Cyber threats and cyber warfare are risks that are here to stay. It is complex and ever changing
 - Cyber security is a highly charged and volatile topic – everyone is scrambling for the ball! Our objective – keep focused on the task at hand, leverage our Industry Groups, State and Federal Partners to rally around the “Unity of Effort” required to support critical infrastructure
 - Realize there is a ever increasing probability, in the utility industry (water, gas, electric, pipeline) that an event will happen
 - To meet evolving requirements and/or to achieve levels of cyber protection, unplanned expenditures may be required and responsive recovery mechanisms will be needed to support these demands