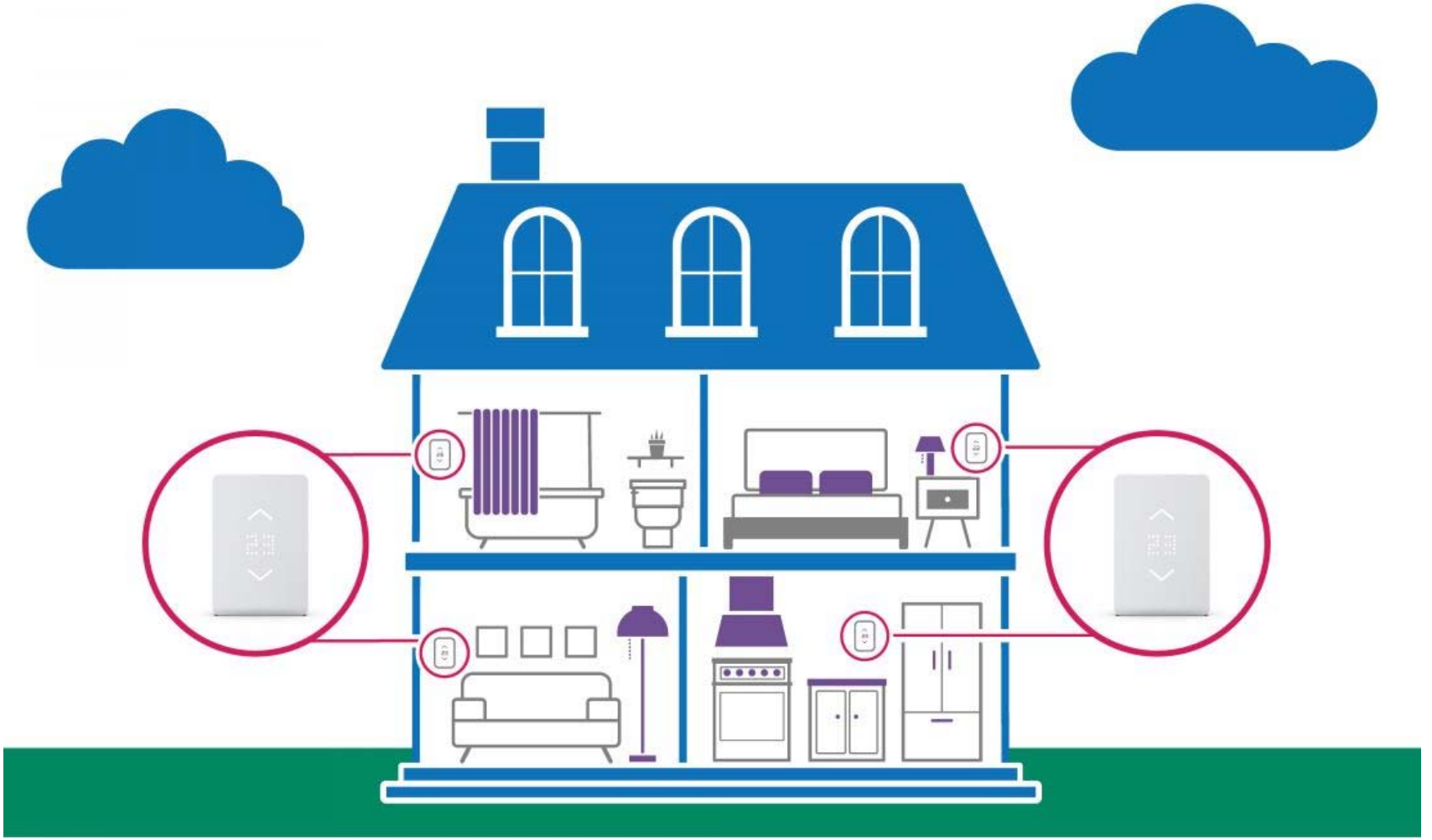
The Modern Grid

David McLeod, Director IT Security & Risk Mgmt
CISSP, PMP, GISCP, Sector Chief (Energy) Infragard

PPL companies

The Modern Grid



The Modern Grid

1880's – first electrical thermostat with the first programmable thermostat patented in 1906

1980's – first electrical thermostat with digital display

2011 – first generation of the NEST (now on the third generation)

The Modern Grid

Advantages

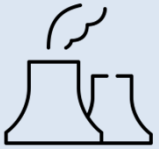
- Wireless
- Interfaces with other device
- Communicates with the Internet to report energy usage
- Can be controlled by an app on your phone
- It can tell if you're home
- You can talk to it through Alexa, Google, etc.
- It's self-learning and much more

Security Concerns

- Patching
- Shorter life span
- Privacy
- Internet password safety

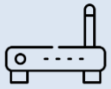
Digital Asset Universe

REGULATORY / CONTROL



Examples:
Sarbanes-Oxley (SOX)
CIP Assets
Compliance driven

CORPORATE IT



Examples:
Servers
Workstations
Databases
Routers
Switches
Firewalls

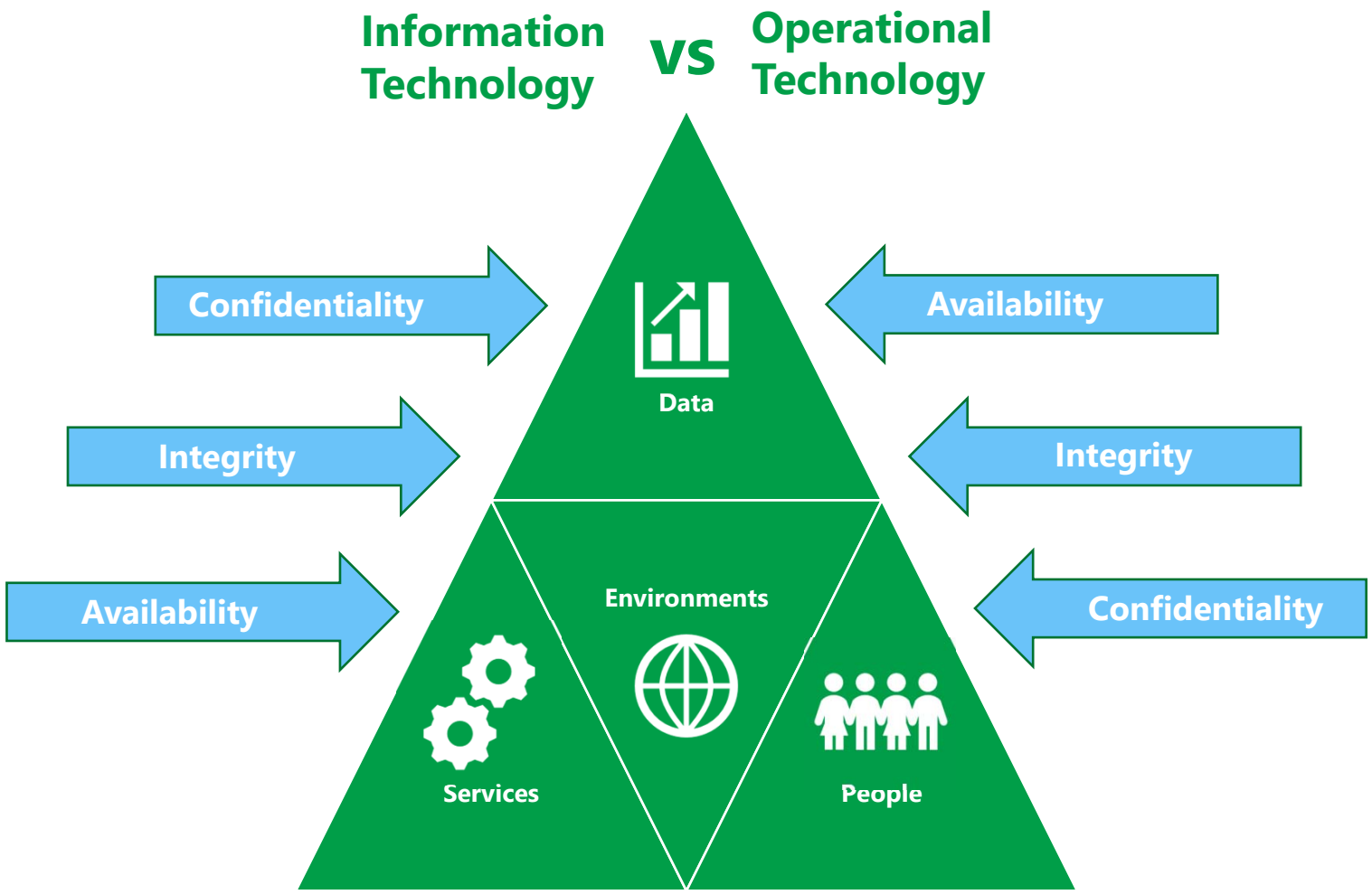
INDUSTRIAL CONTROL SYSTEM/ OPERATIONAL TECHNOLOGY

Examples:
Remote Terminal Units (RTU's)
Programmable Logic Controller (PLC)
Human Machine Interface (HMI)
Distributed Control networks (DCS)
Energy Management System (EMS)
Relays
Pole top devices
Reclosers

INTERNET OF THINGS/ INDUSTRIAL IoT

Examples:
Smart HVAC/Thermostats
Programmable Window Blinds
Security Cameras

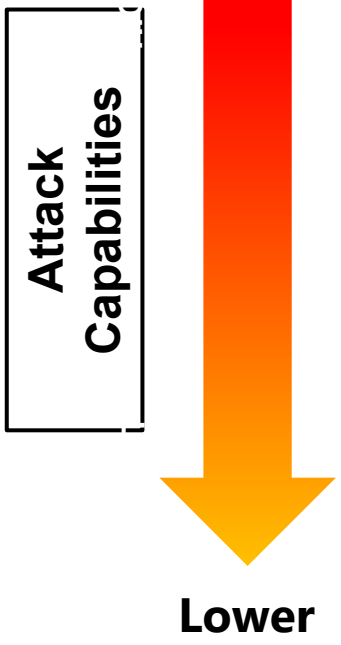
Architecting Security for New OT Security Requirements



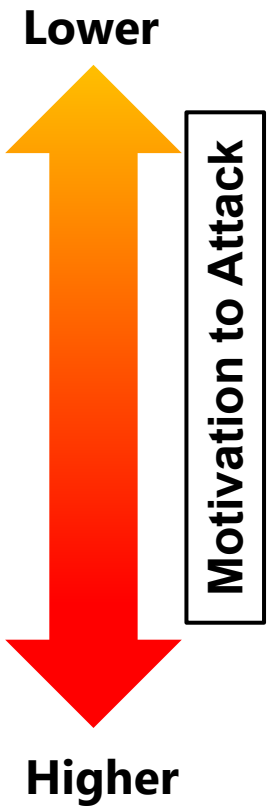
Legacy OT constraints

- Design
- Life Cycles
- Skill set
- Maintenance

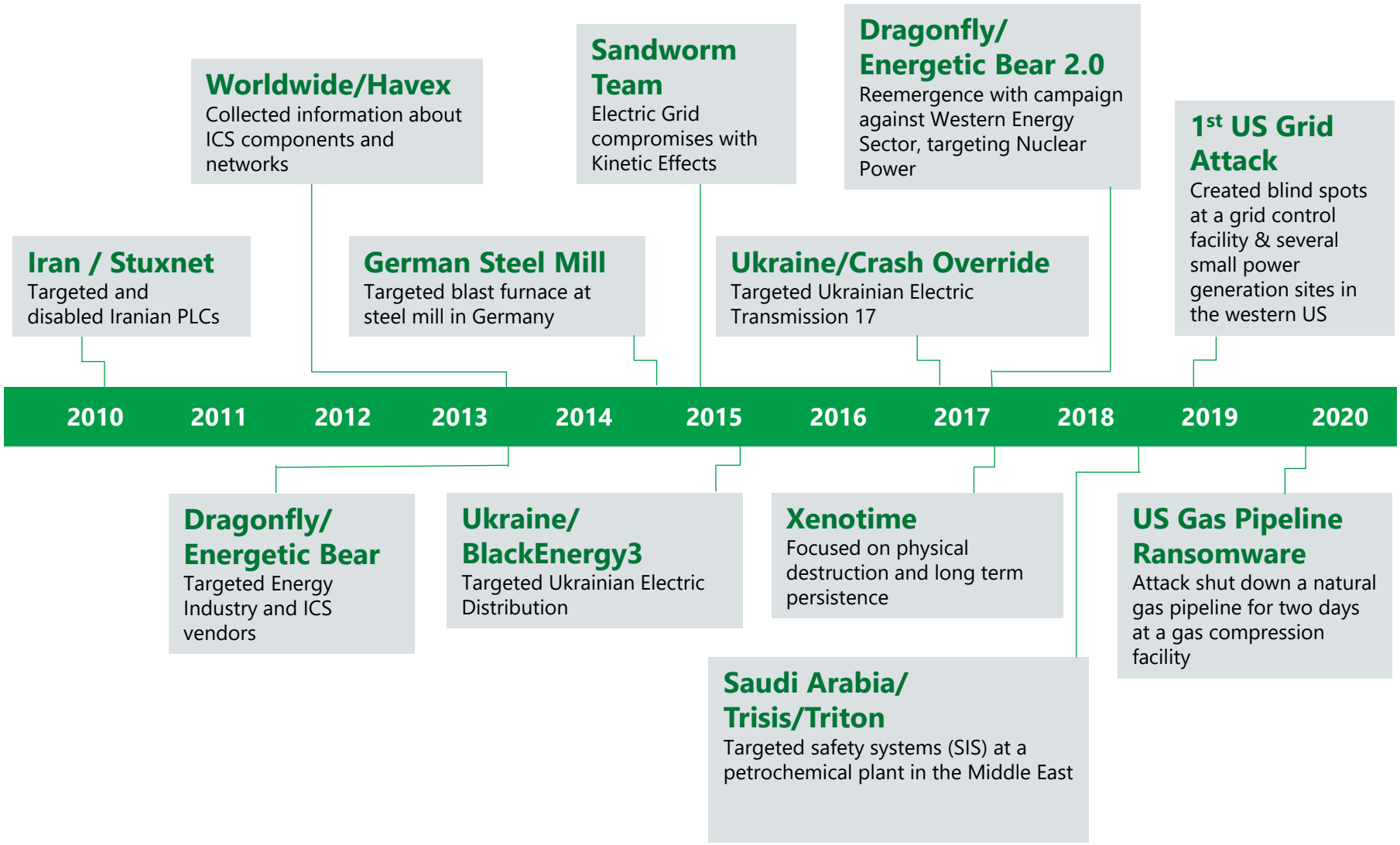
Who are the adversaries?



Who are they?	What do they seek?
State-Sponsored	Power, influence, security and gaining advantage over other nations (Economical, Political or Military)
Rogue Nations	Foster an ideological agenda (political or religious)
Criminals	Economic gain
Hactivists	Push a political or personal agenda
Terrorists	Inflict damage or injury to nations or to drive an ideological agenda



Timeline of ICS Cyberattacks and Threat Groups




On December 23rd, 2015,
hackers caused a blackout
for roughly a quarter
million Ukrainians.

Common Security Controls for ICS/OT

The NSA, FBI, and DHS, have advised the following controls would have largely mitigated previous cyberattacks on ICS/OT

- Build a defendable environment
- Reduce your attack surface area
- Implement secure remote access
- Proper configuration/patch management
- Implement application whitelisting
- Manage authentication
- Monitor for adversarial activity & respond quickly

https://www.us-cert.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf

91% Of Cyber Attacks Start With A Phishing Email

- **Susceptibility** to phishing email drops almost 20% after a company runs just one failed simulation. So people do learn.

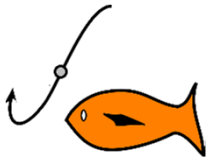
- Active reporting of phishing email threats can **reduce** the standard time for detection of a breach to 1.2 hours on average.

  È A significant improvement over the current industry average of 146 days.

Source: http://phish.me/9CU53073vZx

How does LG&E defend against phishing?

Education is key in LKE's line of defense against phishing attacks.



Employees are phished by the company on a monthly basis to help them learn how to recognize a phishing email.

A red warning banner is added to every external email alerting employees to the possibility of it being a phishing email.

EXTERNAL email. STOP and THINK before responding, clicking on links, or opening attachments.

A "Report Phishing" button has been added to the Outlook ribbon to easily report if an email is suspected to be malicious.

Additional training is required for employees who continually click on phishing emails.

An average of **28.4 million** websites per month are blocked (this includes malicious sites, ads, etc…)

An average of **4 million** emails per month are blocked
✓ *5 e-mails are blocked for every 1 delivered e-mail.*

Threat Intelligence

- **Government Sources –**
  DHS, FBI, Fusion Centers… Infragard

- **Technical Sources –**
  Cisco Talos, PA wildfire

- **Industry –** CRISP, E-ISAC,

Reference

https://icsmap.shodan.io/

https://www.wired.com/story/video-hackers-take-over-power-grid-computer-mouse/

https://www.us-cert.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf

http://phish.me/9CU53073vZx