Deloitte.

Cyber Risk: Protecting our Critical infrastructure

Sharon Chand
shchand@deloitte.com
Deloitte Advisory LLP

Brad Singletary
bsingletary@deloitte.com
Deloitte & Touche LLP

Executive Summary

Investments in security are at an all-time high, yet successful cyber-attacks are still on the rise, both in number and sophistication. While today's fast-paced technology innovation powers strategic initiatives in the Grid, it also opens new doors for cyber attackers. They target financial assets and personal data, but also intellectual property and critical infrastructure. A *Secure.Vigilant.Resilient.™* approach helps companies get ahead of cyber risk so they can keep moving forward.

Agenda

Energy industry threats –
the specific threats facing Energy

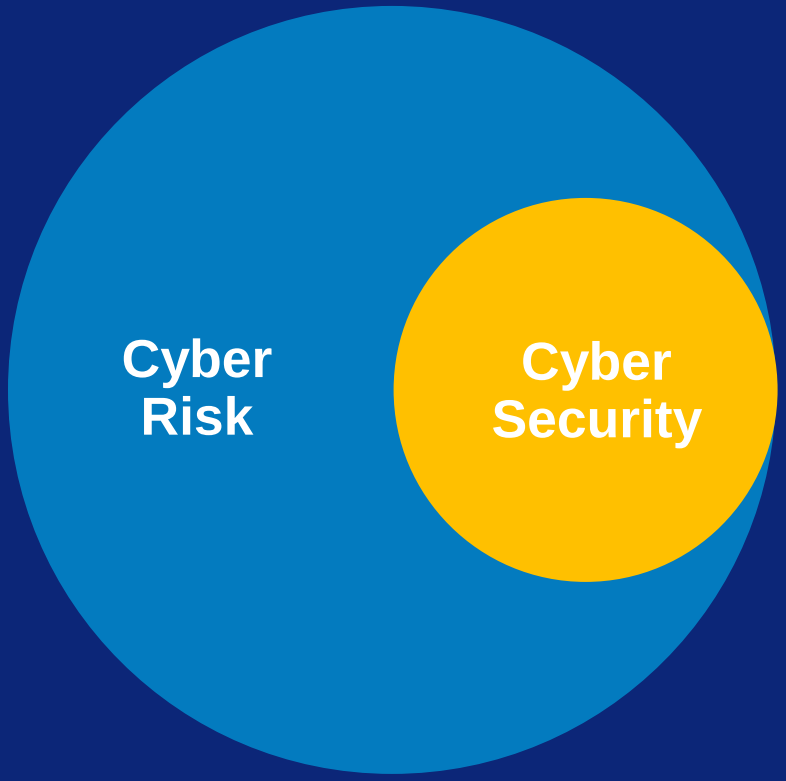
Trends in cyber risk –
initiatives with momentum in our industries

Secure. Vigilant. Resilient™ -
a holistic approach to managing cyber risk

Alternative Energy impacts –
unique cyber risk impacts from alternative energy

Cyber Risk ≠ Cyber Security

Cyber risk and cyber security are often used interchangeably however they are two different concepts

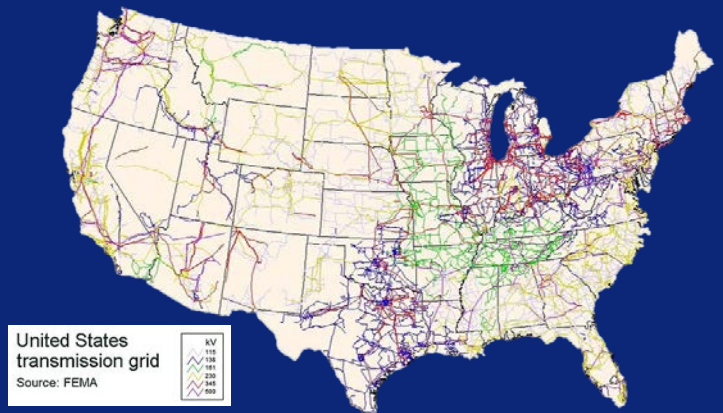


Cyber security is a category of solutions that partially address cyber risk. Cyber security is based on the principles of confidentiality, integrity and availability

Cyber risk is a category of business risks that have strategic, operational and regulatory implications. Cyber risk management assesses threats, vulnerabilities and its potential impact to the broader organization

Cyber Risk Impacts
Energy Critical Infrastructure

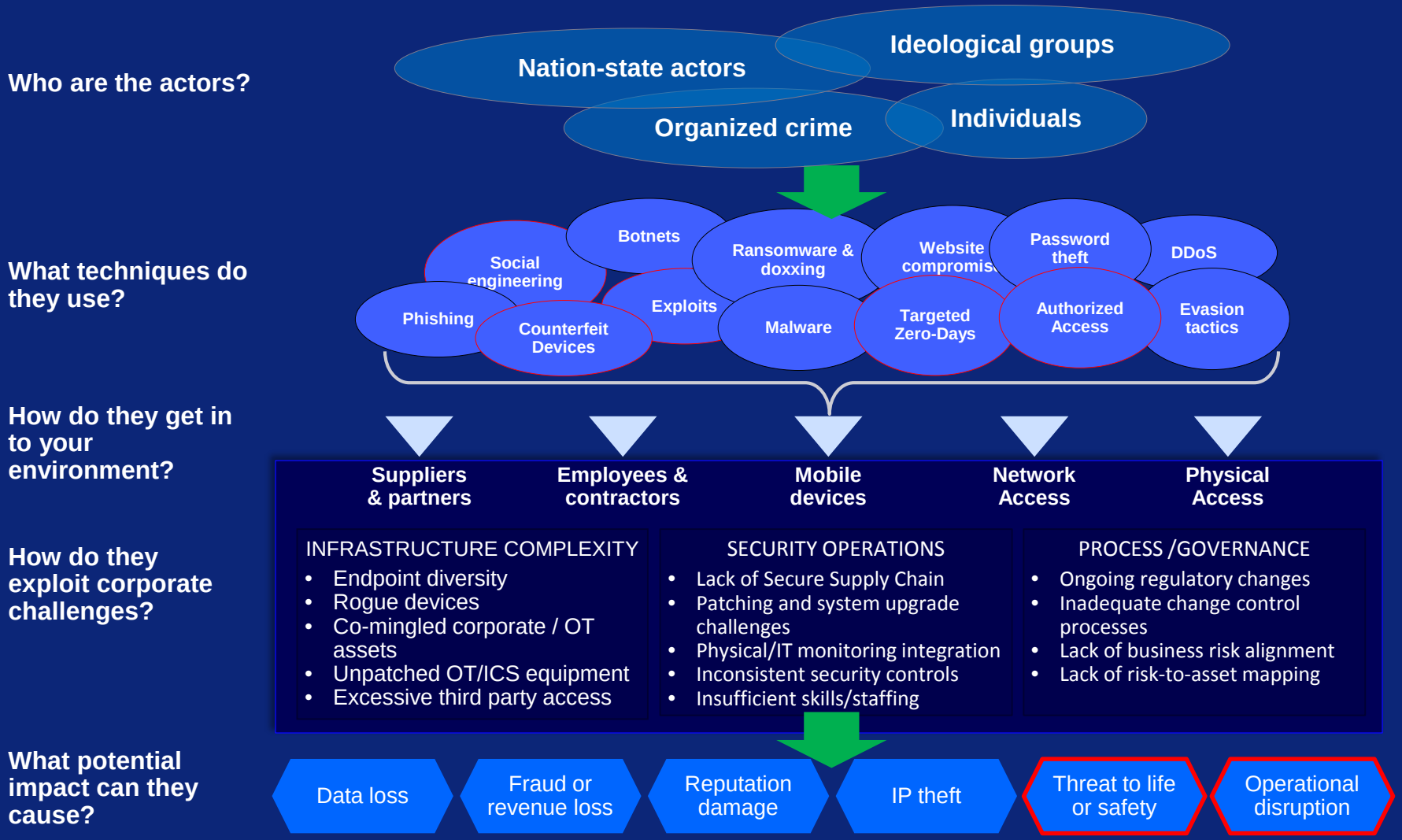
Energy Critical Infrastructure provides safe and reliable Generation and Transmission



Energy Critical Infrastructure
Regulated for Reliability
Regulated for Safety, Security, and Emergency Preparedness

Cyber Threat Landscape

How Threat Becomes Impact for Critical Infrastructure



Cyber Threats are Not Monolithic

Understanding cyber risk starts with identifying the specific threats facing an organization, which allows us to prioritize what to secure, identify which internal controls to deploy, determine how to monitor, and decide scope of incidents for which to prepare.

Energy industry sample heat map

IMPACTS / ACTORS	Financial Theft / Fraud	Theft of customer data	Business disruption	Destruction of critical infrastructure	Reputation damage	Threats to life /safety	Regulatory
Organized criminals							
Hacktivists							
Nation states							
Insiders / Partners							
Competitors							
Skilled individual hackers							

KEY — Very high — High — Moderate — Low

Energy Cyber Threat Current Events

Is this starting to get real?

Documented high level events with public view

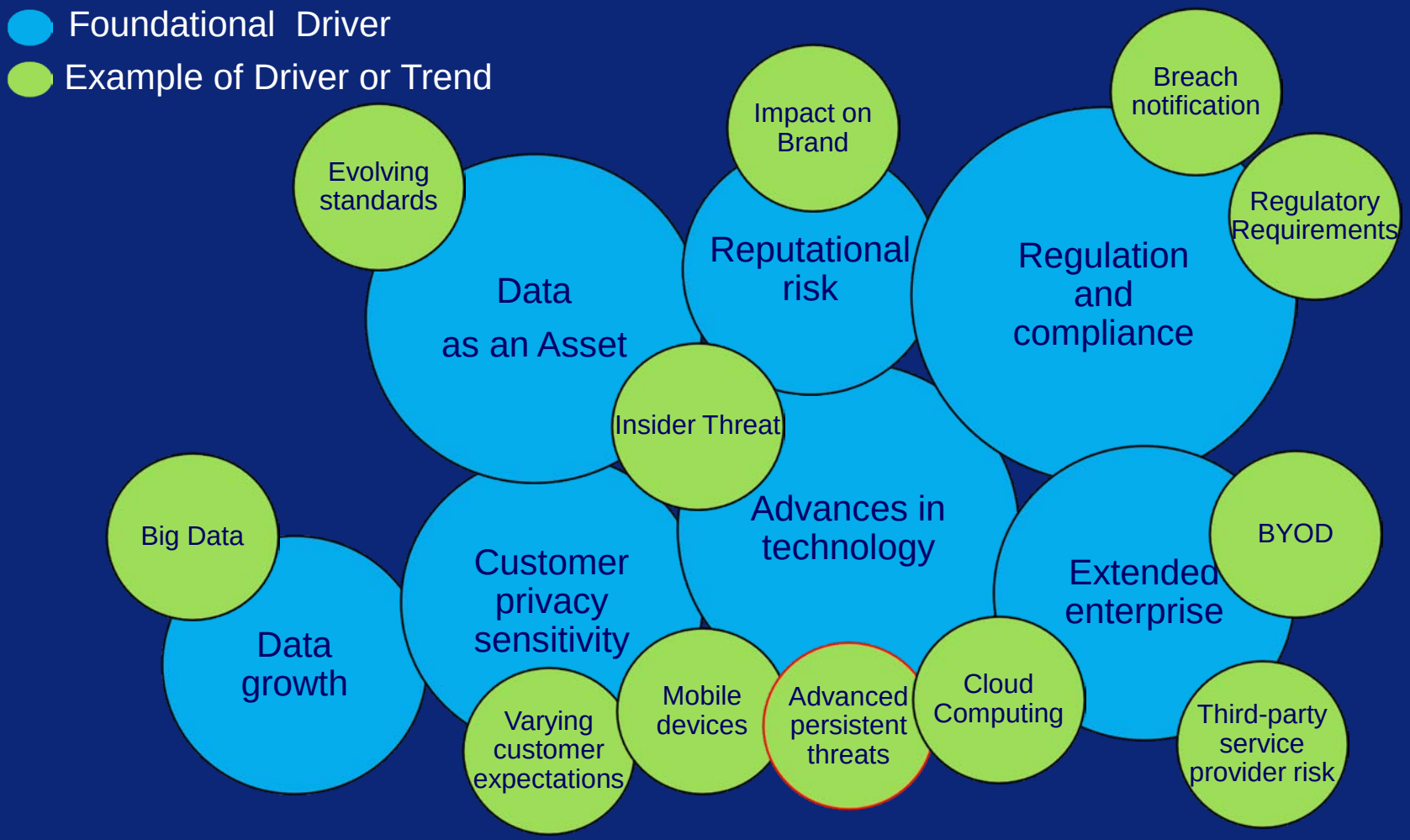
- StuxNet jumps airgap to destructively compromise Nantanz nuclear facility
- Dragonfly APT incursions against Energy providers and provider supply chains
- ShaMoon destructively compromises 30,000 platforms at Saudi Aramco
- Physical attack on electrical and cyber infrastructure at PG&E 500 kV Metcalf Substation

Emerging Vulnerabilities

- Test/configuration tools and other critical infrastructure testing tools
- Infrastructure vulnerabilities reported in ICS/OT/PLC Vendors weekly
- Increasing vectors for Supply Chain
- Internet of Things (IoT) drawing increased research for security vulnerability

Business Drivers

Unique business needs in your company will change your cyber risk



Common Impacts Due to Cyber for Energy

It is important to understand the actual threats for specific organizations, and sometimes for individual lines of business or support functions

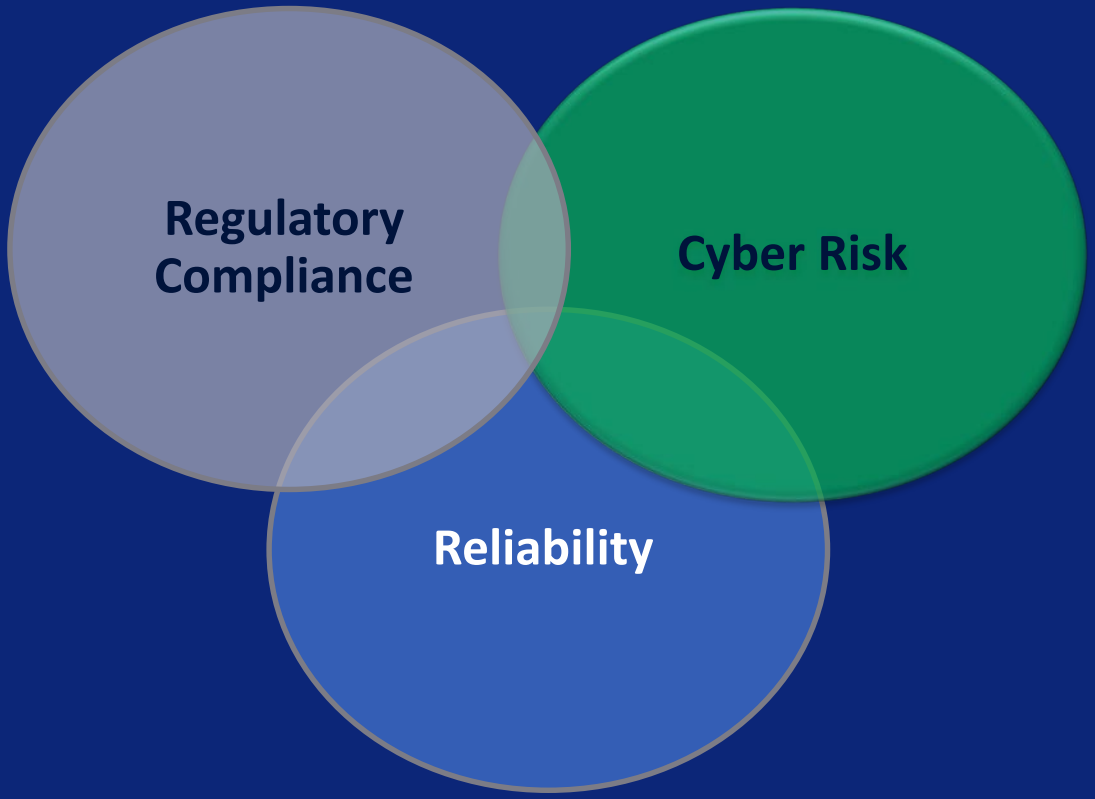
- Loss of rate payer or board confidence
- Customer data breach
- Regulatory fines
- Intellectual Property theft
- Impact to reliable operations
- Impact to life and safety
- Theft/non-technical losses

Cyber Risk Trends

- Physical & Cyber Convergence
- Industrial Control System Vulnerabilities
- Governance of Cyber Risk
- Internet of Things
- Cyber Risk Behavior Change
- Availability of Cyber Professionals
- Measuring the “right” things
- Third Party Risk Management
- Monitoring Data
- Managed Services

Cyber Risk and Compliance

A successful risk management strategy for critical infrastructure must understand the intersection of cyber security, regulatory compliance, and reliable operations



Deloitte's Holistic Approach to Cyber Risk

Secure. Vigilant. Resilient.™

Cyber Risk is more than a technology issue and it's about more than just security. It is a first order business risk. In a world where it is infeasible for organizations to secure all their information and assets all the time, we encourage our clients to invest in protecting their most critical assets while becoming much better at detecting attacks and responding effectively to minimize their business impact. Deloitte calls this approach *Secure. Vigilant. Resilient.™*

Managing, Not Eliminating, Cyber Risk

Cyber risk is a first order business risk that is integrally tied to performance and operations. As a result, it cannot be fully eliminated. Rather, it must be understood and managed

Why cyber risk cannot be fully eliminated

Business must grow and innovate

The things businesses do to innovate and grow are the very things that create or exacerbate cyber risk - e.g., adoption of new technologies, expanding into new markets, developing new client engagement/delivery models, mergers and acquisitions

Sharing information is imperative

We have connected our economy, our businesses, and our society using technologies that were fundamentally designed for sharing information, not protecting it - it is not impossible to secure information, but it is costly (in terms of both resources and business efficiency)

People must be trusted

Some of the biggest risks are related to people - both employees and business partners - whom companies must trust and rely on to operate their business every day

For these reasons, a “secure everything” approach is usually not feasible. Therefore, we advise our clients to focus not only on being secure, but on being Secure.Vigilant.Resilient™.

Deloitte’s *Secure.Vigilant.Resilient™* approach

Secure

Take a measured, risk-based approach to what you secure and how you secure it

Vigilant

Monitor systems, applications, people, and the outside environment to detect incidents more effectively

Resilient

Be prepared for incidents and minimize their business impact

Alternative Energy Impacts

What unique cyber risk impacts does Alternative Energy bring?

- Alternative Energy Providers
  - Larger potential surface area of attack with Distributed Generation control networks
  - Internet of Things (IoT): Increased data and control dependencies
  - New equipment leads to new targeted attack vectors
  - Smaller providers will have less ability to build and govern security infrastructure
  - Supply chain risk
- Vendors
  - Emerging market with emerging supplier reputations
  - Supply chain risk

Five Actions, Five Questions for Executives

Key actions you need to own

1. **Establish purpose and direction.**
   Clearly articulate your cyber risk appetite and strategy. Support it by requisite action through funding and resourcing.

2. **Break down silos.**
   Cyber risk is an enterprise level issue. Lack of information-sharing is a top inhibitor for effective risk management.

3. **Trust but verify.**
   Conduct monthly or quarterly reviews about key risks and risk metrics, and address roadblocks.

4. **Be creative about cyber risk awareness.**
   Your weakest link is the human factor. Consider war-gaming, and other creative ways to raise awareness across the enterprise.

5. **Educate your team.**
   Provide targeted cyber risk training for your high risk populations to combat your high priority threats.

Key questions you need to ask

1. **Are we focused on the right things?**
   Often said, but hard to execute. Understand how value is created in your organization, where your critical assets are, how they are vulnerable to key threats. Practice defense-in-depth.

2. **Do we have the right talent?**
   Quality over quantity. There is not enough talent to do everything in-house, so take a strategic approach to sourcing decisions.

3. **Are we proactive or reactive?**
   Retrofitting for security is very expensive. Build it upfront in your management processes, applications and infrastructure.

4. **Are we incentivizing openness and collaboration?**
   Build strong relationships with partners, law enforcement, regulators, and vendors. Foster internal cooperation across groups and functions, and ensure that people aren't hiding risks to protect themselves.

5. **Are we adapting to change?**
   Policy reviews, assessments, and rehearsals of crisis response processes must be regularized to establish a culture of perpetual adaptation to the threat and risk landscape.

Questions?

Deloitte.