28º Congreso de Energía MEM

Cyber Risk in the Energy Sector

Trends and Best Practices in Incident Readiness

FTI CONSULTING™

November 2, 2023

Why is Cyber a Priority for the Energy Sector?

Top target

#4 target of cyber attacks globally among all industries
#2 among OT-related industries*

Highest Impact

Energy utilities among the 5 sectors, out of the 71, considered of very high exposure to cyber incidents**

Skills Shortage

#1 industry missing critical people and skills to deal with a cyberattack (25%) ***

Investment Lag

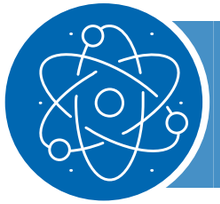
58% of energy professionals believe investment is not flowing at the levels required****

* X-Force Threat Intelligence Index 2023, IBM
** Special Report 2022, Moody's Investors Service
*** Global Cybersecurity Outlook, WEF
****The Cyber Priority 2023, DNV

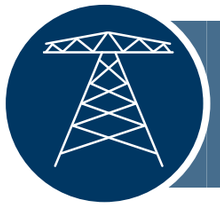
The Energy Sector is a Particularly Attractive Target for Hackers…

The Digital Nature of Energy Transition is Increasing Cyber Risk Across the Sector

1. **Domino Effect** – Disruptions anywhere in the value chain can cause chaos up and down, from producer to consumer. The sector's "enabling function" role for other critical industries increases the pressure for a quick solution in case of an incident, which makes it particularly appealing to all sorts of attackers (for-profit, political)



2. **Large Attack Surface** – The energy sector is heavily reliant in distributed, complex infrastructure, which offers significantly more possible entry points for attackers. This vulnerability continues to grow with the deployment of digitized solutions and even more decentralization – i.e Distributed Energy Resources (DER)



3. **Digital and Physical Interdependence** – Its unique interdependencies between physical and digital infrastructure make energy companies even more vulnerable to exploitation. Gaps between operating infrastructure and IT networks increase risk.

4. **Transformation of Heritage Infra** – There are inherent vulnerability related to that fact that critical infrastructures were not designed with digital transformation in mind. Operating systems designed for peak access (not security) intersect with IT systems with different rules. Adapting takes a lot o money and time.

… Who Are Increasingly Sophisticated

Threat Actors Improve Their Abilities Faster then the Organizations Increase Their Readiness for Attacks

Double & Triple Extortion Ransomware

Double extortion attack: Threat actor exfiltrates data and encrypts company systems, rendering them inoperable. The attacker then threatens to expose the data

Triple extortion attack: Threat actor initiates a string of follow-up attacks. Not only do they demand payment from the initially compromised organization, they may also demand payment from those who may be affected by the leaking of that company's data, i.e., customers, employees

Ransomware as a Service (RaaS)

The growth of ransomware-as-a-service is enabling criminals without deep technical skills to make money by purchasing malware strains from the well-known ransomware gangs

A cut of any profits must be shared with the developer of the malware

Supply Chain Attacks

Threat actors are increasingly looking to exploit third-party software providers rather than larger enterprises themselves, knowing they provide a path into multiple potential victims

Increased Sophistication in Phishing Schemes

Threat actors are deploying increasingly sophisticated tactics to conduct phishing campaigns, including machine learning, highly targeted and thus, believable, spear phishing, etc.

Phishing has also spread beyond email to texts, phone calls and other forms of personal communication

Aggressive and Varied Extortion Tactics

To increase leverage in the ransom negotiation process, threat actors are employing a variety of sophisticated extortion tactics, including Distributed Denial of Service attacks to take down an organization's website, direct outreach to executives, employees and customers (in some cases, asking customers to pay for their own data that's been exfiltrated), media engagement, among others

Globally, Authorities Have Advanced Norms to Force Change in the Industry

Compliance to Regulation does not Effectively Respond to Rapidly Evolving Cyber Threat

Governments have taken an active role in mandating the security of energy systems through legislative and compliance efforts:

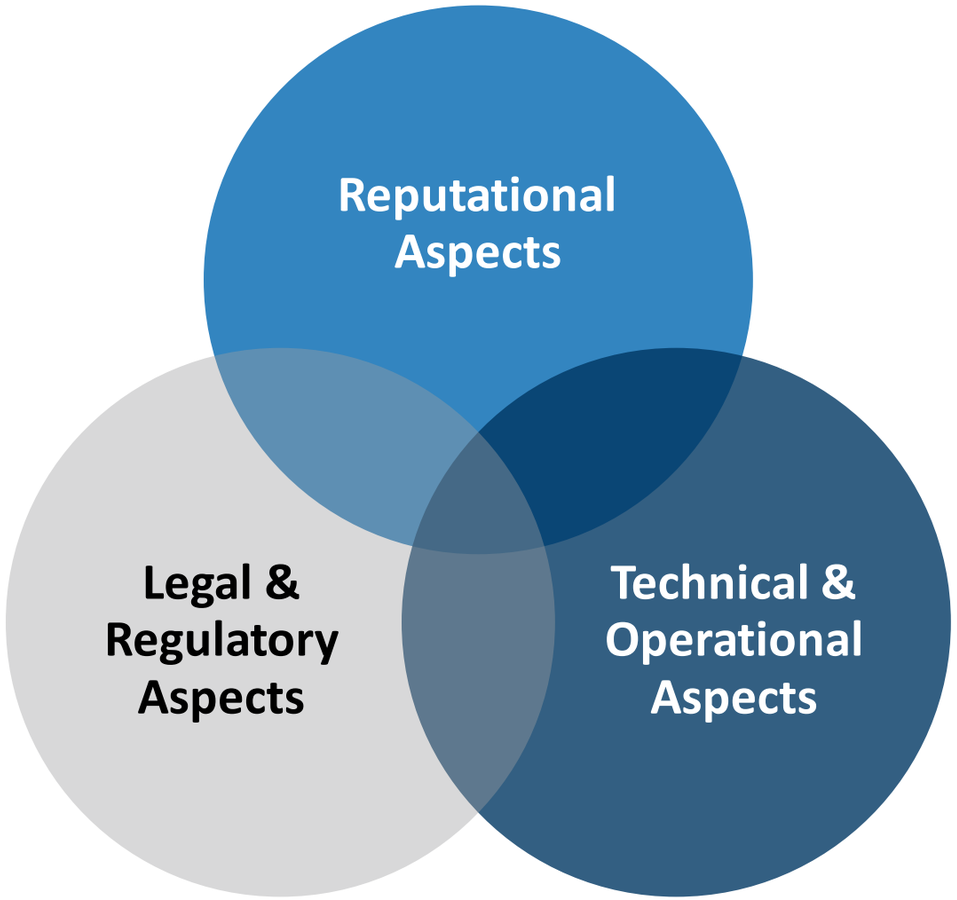
- Global Standards/Coalitions
- Federal Regulations
- Sector-Specific Norms

However, **reactively responding to regulation will not increase the sector's readiness** at the necessary level and pace.

> *It can take two years for a regulation to be developed. Standardization can take 18 months. A cyberattack takes seconds. The speed at which emerging technologies are implemented often outpaces our ability to build security measures around them. We need to go beyond simple compliance with regulations if organizations are to be cyber resilient.*
>
> Hoda Al Khzaimi
> *Director, Center for Cybersecurity, New York University (NYU), Abu Dhabi*

How to Effectively Prepare: Integration and Preparedness are Key Concepts

Cooperation is key not Only Within Organizations, but Among Key Sector Actors



Activities such as:

- Vulnerability assessments;
- Mapping and classifying risks;
- Threat intelligence models;
- Development of cybersecurity policies;
- Supply Chain Audit and Enhancement;
- Review “Air Gaps”;
- Adequacy to applicable norms and standards (i.e CIRCIA, LGPD, GDPR, SEC, CISA etc.);
- Training to develop cybersecurity culture for all levels of organization;
- **Development of an integrated incident response plan;**
- **Cyber crisis simulations and stress tests**
- Pen tests

SUCH EFFORTS MUST BE CARRIED OUT IN AN INTEGRATED WAY – WITHIN THE ORGANIZATION AND WITH THE SECTOR

You Will be Judged by How you Respond

Preserving Trust While Dealing with Competing Priorities Demands Preparation

1 Stakeholder Pressure

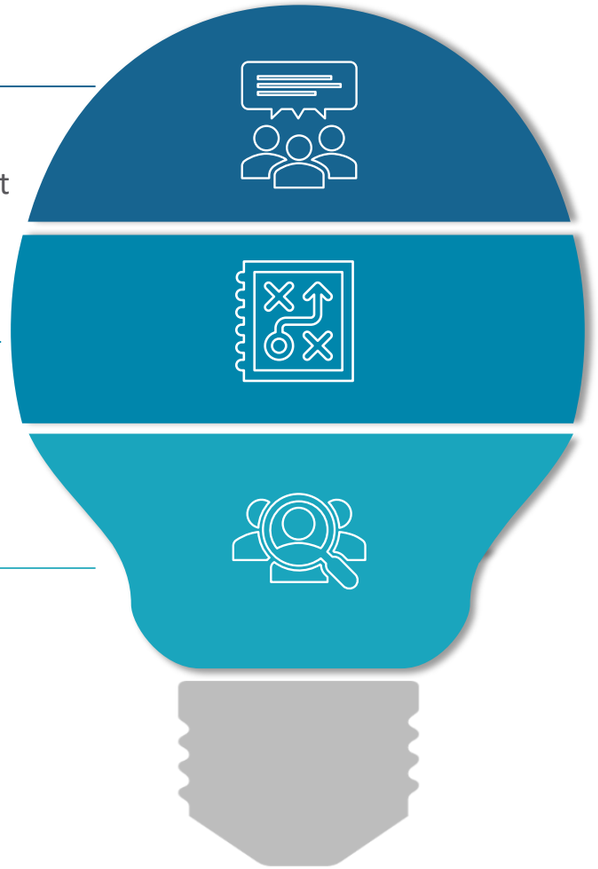
The expectations placed upon a company that experienced a cyber attack have evolved over recent years. Stakeholders expect to be informed of an incident in a timely manner, with transparency about what information is known and frequent updates throughout the investigative process. There are clear examples of “good” and “bad” breach responses, and stakeholders will judge companies accordingly.

2 Challenging Opponents

Threat actors’ evolving communications tactics have changed how we previously thought of cyber communications. The cyber criminal organizations responsible for many cyber attacks are nimble and creative about how they choose to add pressure on their targets.

3 Story Gaps

In today’s digital work, it is hard enough to control narratives. Influencing perceptions on cyber incidents might be additionally difficult, as organizations have to deal with various information gaps. Aspects of the story might never be completely understood.



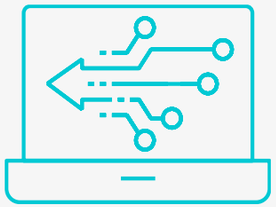
Incident Response Preparedness Best Practices

Assess Response Infrastructure

- Establish relationships with key external partners (insurance, legal, communications, forensics) ahead of crisis
- Identify out-of-band communications solutions for if/when traditional comms channels become unavailable

Put Your Plan on Paper

- Establish a clear governance structure by outlining communications processes, roles and responsibilities
- Scenario plan in advance
- Define communications protocols with relevant market players



Practice Makes Perfect

- Utilize tabletop exercises and simulations to build muscle memory
- Pinpoint communications strengths and weaknesses

Incident Response Plan

While **it is not possible to define "right" or "wrong" responses** to a cybersecurity incident in advance, developing an Incident Response Plan will help the company make more informed decisions to mitigate risks.

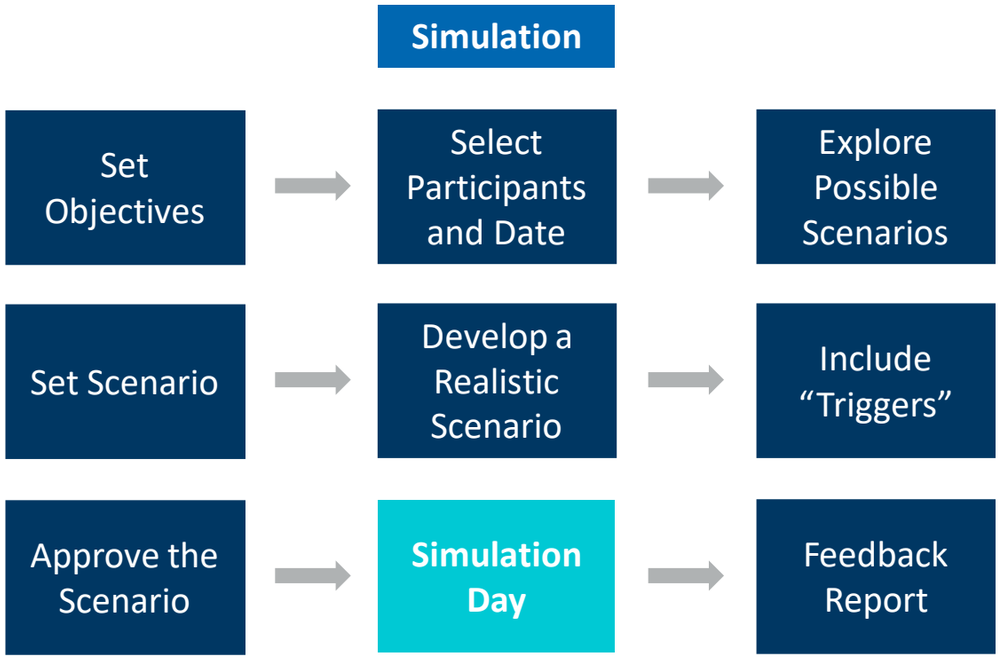
The Incident Response Plan must address topics such as:

- Composition of an incident response team, which MUST include the Communications team;
- Creation of response protocols, including message development, approval and sharing flows, in order to speed up the company's response and ensure consistency in communications;
- Mapping of possible scenarios and developments, considering the specific context of the company;
- Mapping of key stakeholders (internal and external) and their expectations regarding the issue;
- Benchmark of emblematic cases (in different countries and industries), to understand what has worked and what has not;
- Development of communication templates for different stakeholders and potential scenarios;

Cyber Crisis Simulations

Conducting cyber crisis simulation exercises with incident response team members is also a key component of developing enterprise cyber crisis readiness. Through this exercises, it is possible to:

- Assess the company's current ability to respond to cyber incidents of different natures (data leaks, incidents involving third parties, ransomware, insider attacks, etc.);
- Test the company’s current incident response protocols;
- Identify vulnerabilities and points for improvement, such as updates to incident response plans, tools and additional training;
- Creation of a “muscle memory”, so that the organization's leaders feel more confident to make quick and effective decisions in the event of a crisis, as they are already familiar with the possible scenarios and developments.



It is recommended that companies keep their preparation “up to date” by carrying out at least annual simulations

Experts with Impact™

FTI CONSULTING™