Cordence
WORLDWIDE

A Cordence Point of View on

Cyber Security in Utilities Sector

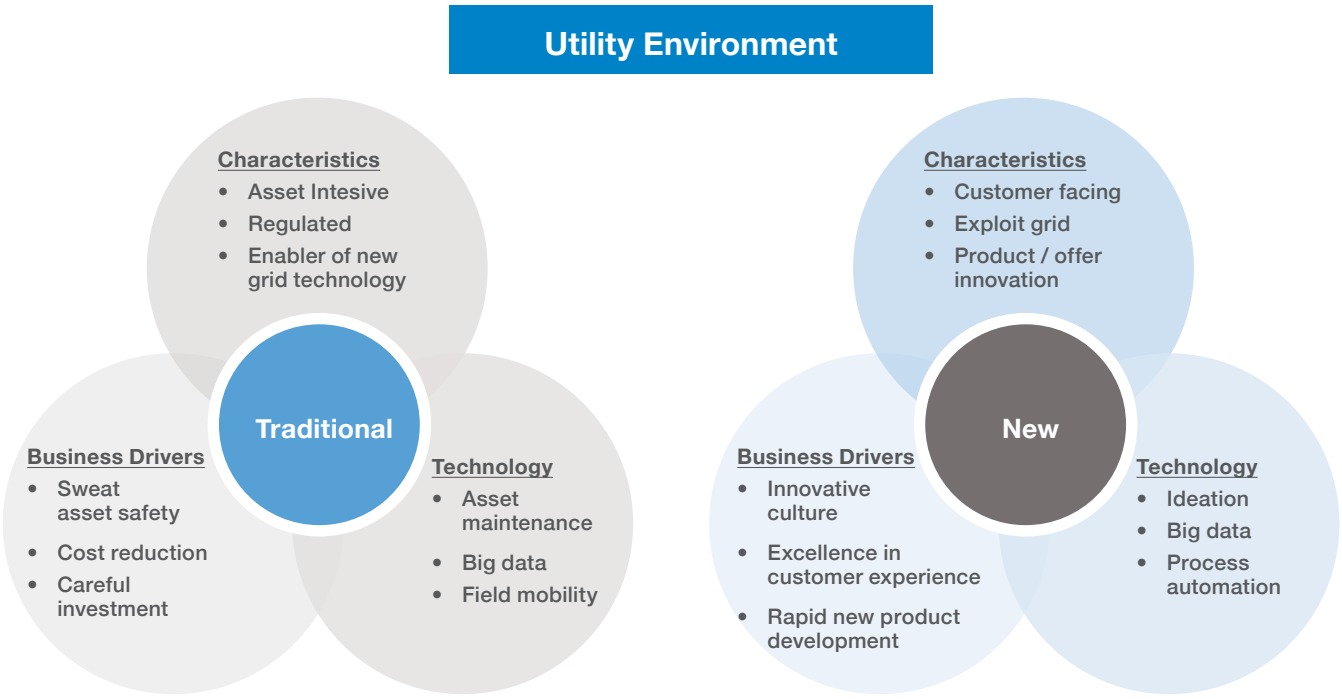
Utilities are evolving fast through digitization. More assets are getting connected today than ever in order to become agile, customer focused and innovative. This leaves the sector vulnerable to cyber attacks, as has been witnessed throughout the world in recent years.

Role of the Utilities sector

As nations develop and bring prosperity to people, the contribution made by the utilities sector (Primarily energy, water, sanitation, and even telecommunications) needs to be acknowledged. These infrastructure heavy industries play a critical role, albeit a silent one, in building the backbone of any country. It is also noteworthy, that the utilities sector acts as a multiplier for most other downstream industries and businesses. The energy industry alone contributes approximately 3-5% of the GDP for countries like USA, UK, Germany[1] etc. Therefore, with so much at stake, it is very important to keep these assets in peak working condition for the betterment of the economy.

Mega trends in Utilities

In the future there will be two distinct styles of utility.



The energy industry has witnessed significant changes across the value chain - in the way energy is created, transported, stored and consumed. Furthermore, there have been developments in technologies available to execute supporting functions – from cloud computing to digital technologies.

Clear and present danger

In the new paradigm of a connected world, where different ideas and interests jostle for dominance, the threat of cyber attacks looms large, particularly with the utilities sector infrastructure, given its critical role in the economy. Any serious act of cyber terrorism can cripple a nation and cause immense economic and social harm. Over the past decade or so, around the globe, there have been multiple incidents where unknown actors have hacked into critical systems and stolen information.

1 https://www.statista.com/statistics/217556/percentage-of-gdp-from-energy-in-selected-countries/

Industry viewpoint

Given the threat profile, Industry experts have expressed concern over the current state of cyber security preparedness.

58%
Utilities respondents recently underwent a significant cyber attack

89%
Respondents believe existing cyber security solutions are not fully effective

39%
Utilities respondents lack a communication plan in the event of a cyber attack

84%
Respondents believe employee actions to be most common reason for cyber attacks

53%
Utilities respondents have a security operations centre

35%
Respondents feel that lack of executive awareness impacts cyber security effectiveness

Survey Statistics for Utilities: 1,735 participants across 20 industry sectors capturing responses from 1,735 participants worldwide, including 81 from the power and utilities sector.

The utilities sector is vulnerable to two types of cyber attacks driven largely by convergence of OT/IT infrastructure by way of digitization.

- IT systems used for business and administrative purposes. These involve corporate breaches where networks are attacked, office computers are compromised or business information is stolen.
- OT systems such as sensors, Supervisory Control and Data Acquisition (SCADA) systems, software and other controls that facilitate pipelines, power plants, and Transmission & Distribution (T&D) grids.

Silver lining

The US energy subsector adopted the Cyber security Capability Maturity Model (C2M2) developed via a public–private partnership initiative. The model aims to enhance the subsector's cyber security capabilities while providing a clear way to understand the cyber security preparedness of the infrastructure.

The C2M2 model helps organizations to evaluate, prioritize and improve their own cyber security capabilities. Importantly, the model provides a common language and appropriate initiatives that non-technical decision makers can readily use to combat the issue. Encompassing much more than just technical solutions, the model helps organizations assess and manage their true vulnerabilities: people, processes and reporting.

Cordence Point of View

Through years of consulting experience in the Industry on specialist IP and a research base, blended with practical on-ground experience, Cordence Worldwide has the following point of view regarding cyber security issues within the utilities sector:

- Cyber security is a business issue and not just a technical matter. It needs to be looked at from a holistic standpoint because today, cyber capabilities are the weakest point that can elevate risks and increase the impact of malicious incursion in any organization. We have seen in most cases that human beings, and their inability to maintain and comply with appropriate process discipline, are the root cause.

- Boards need to include cyber security as a board level agenda item and manage cyber risk in the same way that other risks are managed. This includes the risk of the entity not complying with various national and international government requirements and standards.

- We recognize the unique nature of utility assets. These assets are critical to the economic well-being of the jurisdictions in which they operate and any failure of these assets can cause catastrophic impacts on the economy and the people that economy serves.

- The megatrends in the industry mean that the opportunity for this risk to be significant will only increase over time unless appropriate risk management techniques are put in place.

- We think that good cyber risk management involves the following –

  - A cyber security risk management program to identify analyze and mitigate cyber security risks across the organization and its supply chain.

  - A program covering both operational technology (OT) and information technology (IT) assets.

  - Ability to manage threats and vulnerabilities with appropriate plans and procedures.

  - Capability to be situationally aware, and constantly scan potential future threats.

  - Create a culture that views cyber security risk management in the same way as other core functions.

  - Work with other utility organizations to share critical information, strategy development and operational activities.

Cordence capabilities

Cordence Worldwide's cyber security expertise helps companies build the operational competencies that enable leaders to protect their businesses. We focus on building security-driven systems and cultures, powered by adaptive strategy and operational agility.

Our solutions address the realities of today's security environment:

A MUTATING THREAT

Risks are changing at a viral pace, driving the need for adaptive and agile cyber security.

DATA DRIVES REGULATION

Regulators are looking for holistic compliance that goes beyond technical fixes.

INTERNET OF (BAD) THINGS

Blending distributed, automated technology with aged infrastructure is exposing major security vulnerabilities.

REPUTATION UNDER ATTACK

Corporate brand can be ruined by the compromise of customer data or internal leaks.

PRESSURE TO PERFORM

To protect years of security investments, reaction times must be seconds.

SECURITY TALENT

Security talent is the single largest expenditure and defining asset of a high-performing security organization.

Cordence Worldwide combines valuable security insights with industry-specific expertise to develop solutions from strategy through delivery. Specific security solutions delivered to our clients include:

- **Security Strategy.** We help clients chart a course for improving security while navigating organizational and regulatory constraints. Our expertise tells you where to focus next in your security journey, and the steps needed to get there.
  Sample deliverables: Cyber security Assessment, IT Security Roadmap, Cyber security Budget Prioritization, GDPR Assessment

- **Security Culture.** With a focus on employee engagement, talent strategy, and cross-functional alignment, we work to instill a culture of information security across your workforce.
  Sample deliverables: Security Awareness Campaign Plan, Dynamic Security Refresher Training, Security Operations Center Insourcing Analysis

- **Security Operations.** Whether you're looking to improve security performance or recover from a recent data breach, our work generates quick-hit, execution-oriented security insights that drive organizational agility and efficiency.
  Sample deliverables: Lean Incident Response Playbook, Sensitive Data Inventory, Data Breach Forensic Report

- **Security Technology.** By connecting security solutions with enterprise architecture, we align security strategy, operations, and culture with the digital tools and services that drive security.
  Sample deliverables: SIEM Rationalization Strategy, IAM Program/ Project Delivery, Red Team/ Penetration Testing Findings

With respect to the energy industry, Cordence works with companies worldwide to address business issues ranging from operating models for smart metering to sustainable energy initiatives. Within the utilities sector Cordence Worldwide partners with Axio Global, a boutique provider of specialized utility risk assessment tools.

Axio uses the Cybersecurity Capability Maturity Model (C2M2), developed by the US Department of Energy, as the basis for cyber program evaluations. The model is widely adopted and is unique in its coverage of both traditional IT security and the security of operational technology (OT or industrial control systems). Most utilities have at least some OT systems for building or power controls. The model comprises 312 practices organized into 10 sections.

The Cordence-Axio partnership combines Cordence Worldwide's industry expertise and geographic reach with Axio's unique tool set to assist energy companies in measuring their organization's cyber security risk exposure. Importantly, C2M2 is designed for the electricity sector and supports non-technical decision makers to assess vulnerabilities and prioritize investments to improve its security capabilities. This partnership focuses on three utility-focused business solutions:

- **Exposure Quantification.** Understanding the types and scale of impacts that could arise from a complex cyber event is a critically important step in managing cyber risk.

- **Cyber Program Evaluation.** The cyber security program is an organization's first line of defense against cyber risk. Ideally, the maturity of the cyber security program should be scaled to the organization's risk profile, which becomes much more effectively accomplished after gaining an understanding through the quantification process.

- **Insurance Analysis & Stress Test.** To understand the organization's ability to recover from a complex and costly cyber event, we must understand how the insurance portfolio will respond.

The global cyber security landscape is changing rapidly, particularly in the energy sector. Cordence Worldwide offers a range of capabilities that help organizations navigate business challenges related to securing critical utility infrastructure. Our teams bring the right combination of expertise, experience, and capability to support our clients end-to-end, from strategy through delivery.

Alfa Consulting
Av. Diagonal, 567
08029 Barcelona
SPAIN
+ 34 93 3220202
alfaconsulting.com

Bonfiglioli Consulting
Via Isonzo, 61
Casalecchio di Reno (BO)
ITALY
+ 39 335 430582
www.bcsoa.it

Horváth & Partners
Phoenixbau
Königstr. 5
70173 Stuttgart
GERMANY
+ 49 711 669 190
www.horvath-partners.com

Litmus Group
Level 7, 8 Chifley,
8–12 Chifley Square,
Sydney NSW 2000
AUSTRALIA
+ 61 432 181 162
www.litmusgroup.com

Oresys
48, Rue de Londres
75008 Paris
FRANCE
+ 33 1 44 90 18 18
www.oresys.com

Twynstra Gudde
Stationsplein 1
P.O. Box 907
3800 AX Amersfoort
NETHERLANDS
+ 31 33 467 77 77
www.twynstragudde.nl

Avalon Consulting
101, Suraj Prakash,
1st floor, 86 Shankar
Ghanekar Marg, Prabhadevi,
Mumbai 400 025. INDIA
+91-22-4946 6600
www.consultavalon.com

Genex Partners
Shirokane Takanawa
Station Bldg 3F
1-27-6 Shirokane
Minato-ku, Tokyo 108-0072
JAPAN
+ 81 3 5795 3211
www.genexpartners.com

Key To Way
6,7F, 79, Banpo-daero
Seocho-gu, Seoul 06670
KOREA
+ 82 10 8931 0834
www.keytoway.kr

North Highland
3333 Piedmont Rd. NE
Suite 1000
Atlanta, GA 30305
USA
+ 1 404 233 1015
www.northhighland.com

S. Point
1000 Changping Road,
Building A, Jingan District,
Shanghai, CHINA 200042
+ 86 21 6272 8858
www.spointdesign.com

Cordence WORLDWIDE

Cordence Worldwide is a global management consulting partnership. Its Member Firms are the leading independent consultancies in the Americas, Asia-Pacific, and Europe. Combining global delivery, focused accountability, and an uncommon dedication to clients, Cordence Worldwide Member Firms help organizations all over the world achieve remarkable business results.

www.cordenceworldwide.com