Tackling cybersecurity threats in the Utility industry

Trusted partner for your **Digital Journey**

Atos

This document should be read in conjunction with the Atos publication "Cybersecurity for Energy and Utilities" which explains how to address the utilities cyber threats discussed in this white paper.

A digital transformation improving operational efficiency...

As the utilities industry is transitioning, its supporting operational and information technology architecture is changing as well. The experience of utility workers and customers has been impacted by the adoption of cloud services, IoT and mobility in recent years. The multiplicity of actors, combined with this digitalization, brings new challenges to this industry.

The utilities industry distribution model has been impacted by the growing share of distributed and intermittent renewables. The deregulation of this market brings multiple and smaller production sources, various energy flows, new entrants on the business, new models (e.g. distributed load shedding) and new roles.

The energy transition is supported by new technologies that are driving a huge increase in operational efficiency for energy and utilities (gas, electricity, water) companies. With the rising value of data and the adoption of IoT, these organizations can monitor the performance of their assets and gain greater insight into their customers' consumption habits. As part of this evolution, emerging technology trends are shaping new digital business models for utilities.

Industry 4.0: embracing the technologies that shape tomorrow's manufacturing world

Today, most industrial companies are embracing the concept of Industry 4.0 which supports the overall digital transformation and elevation of production efficiency and proficiency with the introduction of automation and data exchanges.

This gave birth to the new concept of Cyber 4.0 which aims to provide the relevant protection for the world of innovation and the threats that may arise from it.

Focusing on security to protect the utilities business

All these new technologies and developments will only keep their promises if fully secured. Security must be included in every part of the utilities system, whether they are industrial assets, platforms or devices.

Data must be protected, from critical information of nuclear plant to customer personal data. For that, security must have a core place within new and existing developments, processes and implementations and not be thought afterwards.

Getting nomad through mobility enablement

Mobile technologies, such as phones and tablets, help utilities employees to work faster and more efficiently on the field. With the adoption of reliable and high-quality ruggedized solutions, they can manage their tasks remotely and all their devices are simultaneously synchronized, often bridging the air gap between IT and OT.

Moving IT closer to OT for an increased profitability

Industrial systems and IT information systems are exchanging more and more information. This convergence is reflected in industry and infrastructure, but especially in the energy and water sectors. Systems are often decentralized and assets dispersed throughout the territory.

In this context, remote management and asset supervision are increasingly centralized. It involves a convergence of systems that provides better control of infrastructures and an optimization of maintenance interventions and human resources. IT/OT convergence also makes it possible to optimize business processes by adapting energy production and distribution and thus increasing the profitability of the service.

Empowering customers with valuable applications

Utilities consumers have now more opportunities to engage with their energy providers through dedicated applications. They are getting more control over their energy usage, from the monitoring of their consumption in real time through smart meters to local production management with their own solar panels.

With the introduction of smart homes, consumers are expecting more value and flexibility from utilities, with personalized packages and rewards. As data quality and analytics improve, they are empowered with better accuracy and granularity of their power consumption.

Adopting the Cloud for flexible processes

All data collected from IoT, blockchain and utilities assets needs to transition towards the cloud to be treated and analyzed for more efficiency. The use of these new technologies leads to a wider adoption of cloud solutions. According to a 2018 IDG Cloud Computing Study, utilities are parts of the three industries experiencing the greatest pressure from executive management to become 100% cloud-based.[1]

Moreover, with cloud adoption, utilities companies will benefit from quicker application implementations and faster IT services and infrastructure.

[1] IDG 2018 Cloud Computing Survey : www.idg.com/tools-for-marketers/2018-cloud-computing-survey/

Enriching data with IIoT and moving to the Edge

IIoT enables utilities companies to place data sensors on all their assets, across a wide range of sites. Maintenance is made more efficient, since managers can check when a piece of equipment needs to be maintained or replaced. IIoT also changes the way utilities companies address their customers as they collect data on their habits to tailor their experience. The capability to introduce predictive maintenance to the organization is a key factor in that aspect.

With edge computing directly linked to IoT devices, data and processing are decentralized. It allows utilities companies to easily and handle data flows that are becoming more important and complex everyday with the arrival of new production streams new, such as locally generated renewables. It brings more agility and intelligence on how data is managed.

Anticipating the future with Artificial Intelligence and Digital Twin

Artificial intelligence paves the way to digital transformation in utilities with big data. On the one hand, it can improve operational efficiency, save costs through reduction of waste or help to anticipate power demands.

On the other hand, AI can be used to prevents grid outages. In 2017, a Department of Energy laboratory project implemented AI and machine learning in the electric grid to detect its weaknesses and fix them before failures happen. The final objective was to create an autonomous grid able to quickly respond to disruptive events.[2]

To go further, digital twins, that create a replica of an existing physical system, are used to simulate conditions on utilities equipment to better anticipate specific scenarios and optimize their uses.

25%

of utilities will leverage public Clouds by 2019

30%

of mobile utility workforce will use augmented reality by 2019

$4.6bn

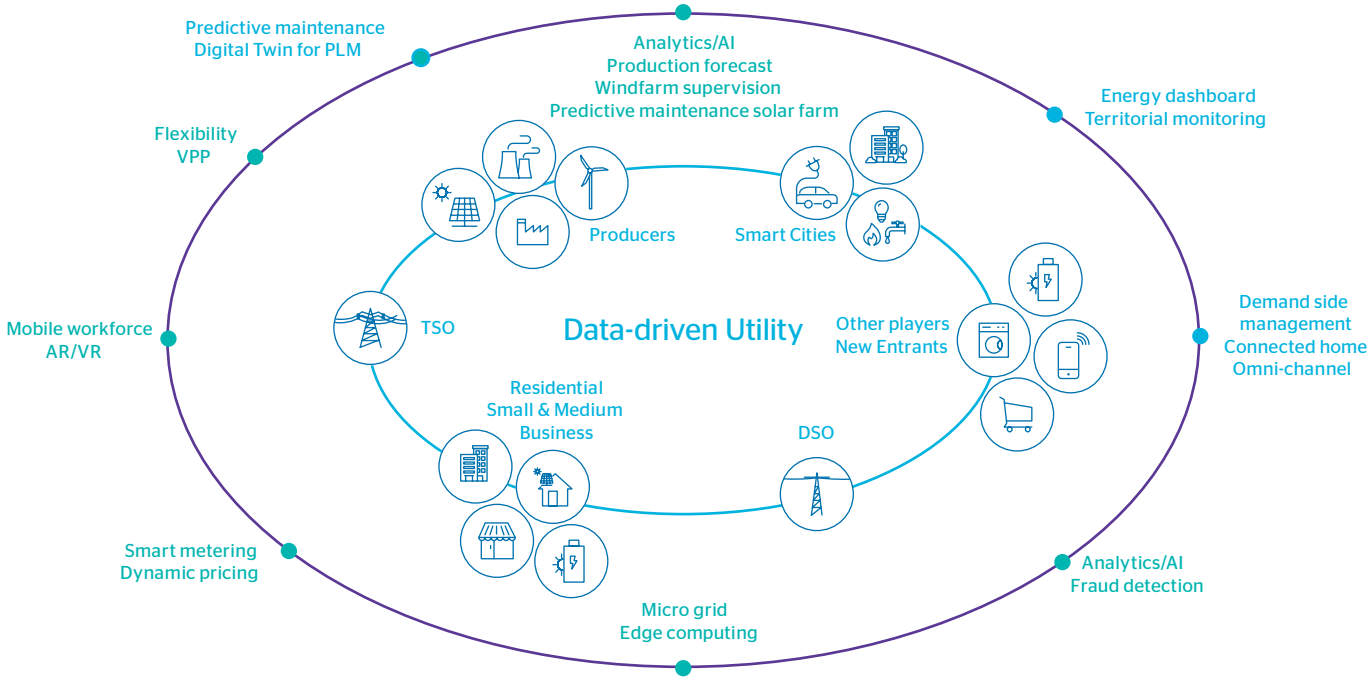
will be spent on smart grid data analytics in 2022

$ = USD

85%

of utilities will speed up digital innovations by 2019

Sources: IDC, Markets and Markets, Transparency Market Research, European Union



[2] Project will use AI to prevent or minimize electric grid failures, September 2017: phys.org/news/2017-09-ai-minimize-electric-grid-failures.html

... but raising new security challenges

With their digital transformation, utilities companies can be targeted by hackers on a very large attack surface. What are the physical and digital threats they can face?

In the last few years, data breaches and cyberattacks targeting utilities have consequently spread, sometimes with huge costs. Some security best practices can be learnt from these fruitful lessons (types of attacks targeting utilities, assets where cybersecurity should be prioritized, security technologies that were missing...).

Power generation

In October 2019, the Nuclear Power Corporation of India Limited confirmed that its newest power plant had been the target of a cyberattack and more specifically of a malware designed for data extraction[3]. The malware, named Dtrack, had previously been used to steal financial data in India from ATM networks.

What can be learnt from this cyberattack for Power Generation organizations?

Cyber espionage: a reality

This specific attack highlights the high and existing risks of cyber espionage. The Lazarus Group, known to be close to North Korean groups, is suspected to be at the heart of this malevolent action.

Hackers: always a step ahead

Even if the Dtrack malware may not have enabled hackers to directly access to sensitive data on the nuclear power control networks, it raises the question of critical organizations security. These cyberattacks are often preemptive to others to come and enable hackers to have one foot in the system, potentially providing them with useful information (operations, maintenance...) for future attempts.

Transmission and distribution

In March 2019, the U.S. power grid experienced the first cyberattack that affected its operations[4]. The cyberattack did not disrupt the electricity flow but "only" triggered periodic losses of visibility of the supervisory control and data acquisition (SCADA) system by exploiting a firewall vulnerability. This cyberattack is somewhat reminiscent to what happened in December 2015 on Ukraine's power grid[5]. Hackers were able to successfully compromise the information systems of three distribution utilities in Ukraine and knock out power to customers for several hours.

What can be learnt from this cyberattack for Transmission and Distribution organizations?

DDoS, malwares, advanced persistent threat... Be ready for any attack

The Ukraine cyberattack was complex and exposed a cautiously prepared strategy: spear-phishing emails to introduce the BlackEnergy malware into the corporate network, theft of credentials, SCADA hijacking, disconnection of substations from the grid, denial-of-service attacks targeting call centers to hamper information and restoration... It seems that the cyberattack was designed to inflict enough damages to last for weeks or months.

Two-factor authentication and security monitoring: a must for utilities

It appears that many vulnerabilities in the system allowed the adversary to conduct investigation on the environment prior to the attack[6]. For instance, the VPNs used in the business network were lacking two-factor authentication, enabling an easier access to the system. Moreover, the utility network was not continuously monitored, hindering the search for abnormalities and threats.

[3] Financial Times, India confirms cyber attack on nuclear power plant – October 31st 2019 - https://www.ft.com/content/e43a5084-fbbb-11e9-a354-36acbbb0d9b6
[4] E&E News, Experts assess damage after first cyberattack on U.S. grid – May 6th 2019 - https://www.eenews.net/stories/1060281821
[5] https://en.wikipedia.org/wiki/December_2015_Ukraine_power_grid_cyberattack
[6] https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

Retail and services

Cryptojacking, a relatively new attack compromising computers and forcing them to mine cryptocurrency for hackers, infected U.S. residents after they used a water bill service named Click2Gov[7]. This online payment processing service had been breached for at least a year. After having affected municipal employees' computers, the cryptojacking software transformed to steal users' personal data, such as credit card numbers.

What can be learnt from this cyberattack for Retail and Services organizations?

End users' personal data is also at risk

Data protection in utilities is not only about nuclear power plants confidential data but also for end users. With the GDPR regulation, organizations need to identify the risks related to personal data collection and processing while being able to prevent any unauthorized access to it.

The evolving threat landscape is quickly evolving

With the appearance of new technologies, the threat landscape is getting more complex. Cross cloud attacks, cryptojacking, opaque algorithm compromising integrity, AI powered attacks... The security system and policy of utilities must be agile enough to evolve with these new risks.

Oil and Gas

As OT systems are becoming more internet-connected, their increased connectivity with the IT environment make them possible attack vectors. In 2017, the WannaCry ransomware attack was facilitated through outdated Windows software vulnerabilities. It affected multiple industrial control systems (ICS) leading to operations disruptions and even shutdowns. But the damages can even go further. In 2018, an OT-specific malware named Triton targeted a petrochemical plant in Saudi Arabia, owned by Tasnee[8]. The objective of the cyberattack was to take control of the safety system, which keep equipment safe by regulating voltage, pressure and temperatures, to trigger an explosion and kill employees.

What can be learnt from this cyberattack for Oil and Gas organizations?

IT/OT convergence, the backdoor to new vulnerabilities

As off-the-shelf technologies like Ethernet, TCP/IP, and Windows are now used in OT, new threats from the IT world are also introduced. Infections can happen unsafe smartphones or laptops. Limited cybersecurity controls exist on the OT side (processes, skills, tools, visibility...) which can lead to tremendous damages as seen on these cyberattacks.

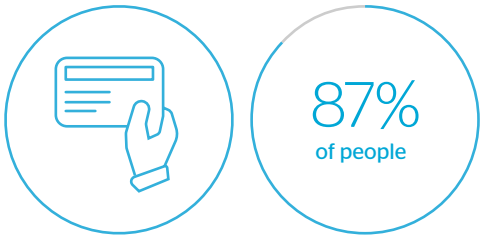
IoT security, a pre-requisite

As IoT expands utilities organizations connectivity, potential entry points are making the power grid more vulnerable. Companies need to make sure connected devices, such as smart meters or industrial assets, are secure.

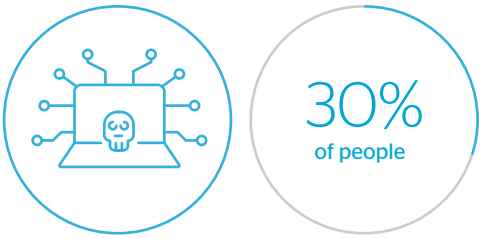
https://sanangelolive.com/news/business/2018-08-21/city%E2%80%99s-water-payment-data-breach-may-be-work-cryptocurrency-pirates [7]
The New York Times, March 2018, A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try. [8]
https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html

Cybersecurity: not only a question of regulation but also of customer's loyalty

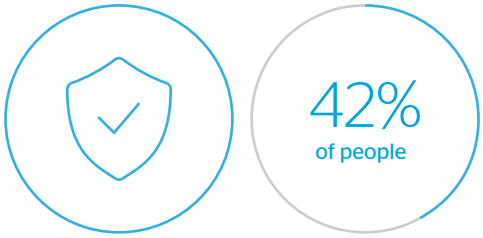
With the amount of data breaches on the rise, consumers are becoming wary of the potential vulnerabilities of the utilities sector. Indeed, 42% ranked utilities as high risk. In a sector where customers are given the possibility to switch more flexibly than ever before from an energy supplier to another, any data compromise could seriously damage an organization's reputation and persuade citizens to go away. 43% of customers who had fallen victim to cyber crime did not return to the organization in question.



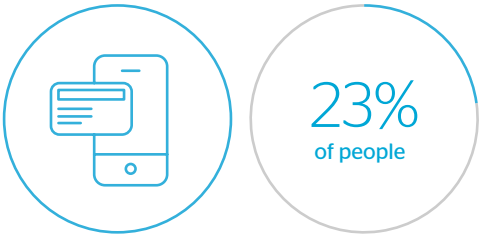
state their bank details are most valuable to them, with those aged 55 and over valuing them more highly



would rate access to their utilities as at high risk of a cyber attack



ranked utilities as high risk when asked what organisations are most able to protect themselves from a cyber attack



expect mobile phone verification in place within the utilities sector

"Duke Energy was fined $10 million by the North American Electric Reliability Corporation (NERC) for security violations between 2015 and 2018 regarding critical infrastructure assets. [...] The 127 security violations, including critical cyber assets, were largely self-reported by the utility and caused by lack of managerial oversight, process deficiencies, inadequate training and lack of internal controls."

- Utility Dive, February 2019

In this climate, utilities organizations must strike a balance.

Even if the new technologies brought by their digital transformation can become the cause of future cyberattacks, they cannot entirely reject them and what they can result in: efficiency and competitiveness.

That's why cybersecurity's objective is to make utilities thrive from connected technology's opportunity whilst securing the data they create in the process.

About Atos

Atos is a global leader in digital transformation with 110,000 employees in 73 countries and annual revenue of € 12 billion.

European number one in Cloud, Cybersecurity and High-Performance Computing, the Group provides end-to-end Orchestrated Hybrid Cloud, Big Data, Business Applications and Digital Workplace solutions. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and operates under the brands Atos, Atos|Syntel, and Unify. Atos is a SE (Societas Europaea), listed on the CAC40 Paris stock index.

The purpose of Atos is to help design the future of the information technology space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

Find out more about us
atos.net
atos.net/careers

atos.net/en/solutions/cyber-security
atos.net/en/industries/utilities

Let's start a discussion together

CT-200310-RY-J3662-ENERGY-WP-TACKLING