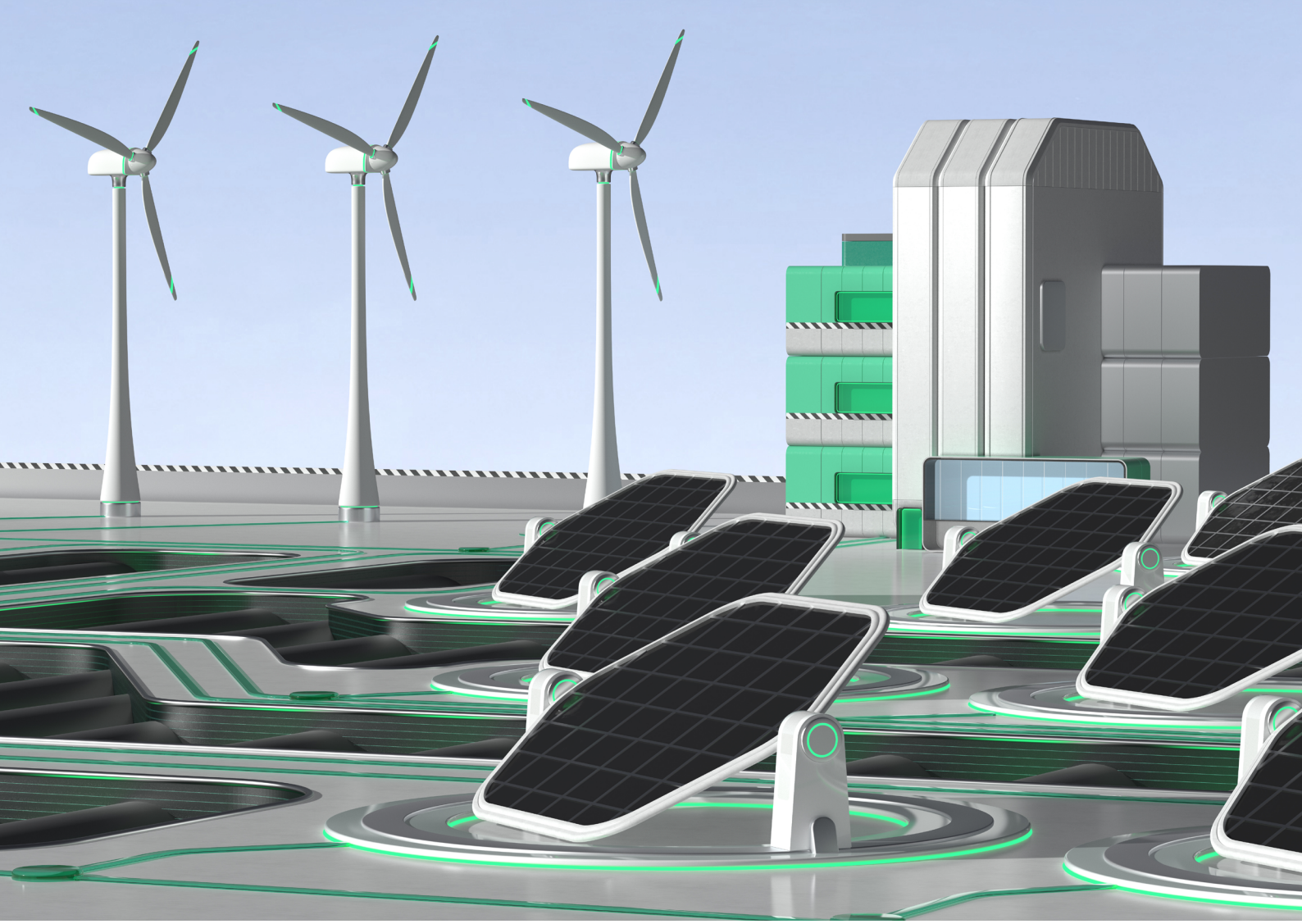

Building a safer future in Utilities

kaspersky BRING ON THE FUTURE

go.kaspersky.com/utilities 2021

Introduction

The output of the utilities industry – warmth, power, light, water and sewage services – runs through the veins of every industry on the planet like blood without which nothing would function. However cybersecurity incidents in 2021 have demonstrated that the utilities industry is a growing target both for cybercrime and for acts of cyberwarfare.

The utilities industry is undergoing rapid change that shows no sign of deceleration. In addition to disruptive digital transformation, the utilities industry is under unique pressure to transform the very assets it produces. Decarbonization, renewables, energy-efficiency and decentralization are the order of the day, and only the very smartest and innovative technology can answer the call. Compounding this are the numerous regulatory requirements that utilities operators must juggle with in an increasingly global market.

In this paper, we look at the key trends transforming the utilities industry today and uncover the challenges and risks they bring with them. Our vision is of a world where utilities operators are free to maximize their adoption of efficiency-driving smart technology, without fear of the devastation that can be wrought by malicious cyber actors.

Artificial Intelligence

Data analytics

Decarbonization

Distributed Energy Resources

Regulatory challenges

Trend #1: Artificial Intelligence (AI)

Artificial Intelligence is disrupting the way the industry achieves the constant (and efficient) supply upon which suppliers' reputations and contracts depend. These technologies have been made possible by the availability of massive computational power via the cloud, the proliferation of big data, and the increasing sophistication of algorithmic acumen.

On the production side, utilities operators leverage AI to forecast loads, optimize yields, analyze consumption, predict demand, prevent theft or malicious interference, and carry out prophylactic maintenance and repair tasks. Utilities operators also look to implement these disruptive technologies into other business function; including sales, operations, customer services, facilities management, procurement and IT.

AI applications for utilities:

- Remodelling customer experience;
- Streamlining maintenance tasks;
- Anticipating energy loads;
- Integrating distributed energy resources (DERs);
- Optimizing generation, transmission and distribution.

Common applications of AI include analysing historical weather patterns to calculate future grid impact and customer behaviour and put in place equipment and manpower to minimize future weather-related downtime. Utilities are experimenting with unmanned drones coupled with AI to collect data and images of field equipment and identify risks of failure much more efficiently than by manual inspections. Utility operators are also just beginning to realise AI's potential role in coordinating distributed energy resources such as wind, battery and solar. But this is only the start. Utilities sit on huge amounts of invaluable customer data and have the capacity to use AI to improve all aspects of their customer engagement and to transform their business model.

"A power plant that will run on "artificial intelligence" is about to get underway in West Africa. The joint venture between Swiss-based Xcell Security House and Finance and U.S.-based Beyond Limits will embed intelligence and awareness into the operations — something that will create more efficiencies, greater productivity, and increased environmental protections." Forbes

AI also facilitates robotic process automation (RPA). RPA is flexible, scalable and can be adapted to specific requirements of each utility. It reduces costs and makes service upgrades feasible. It also helps address labour shortages, managing simple tasks for customers such as automatic meter readings and some aspects of regulatory control and compliance. Utilities are fast transferring routine, systematic rule-based processes to RPA.

In the overwhelming majority of cases, utilities operators turn to third parties to supply the innovative technologies they require. These third parties include seasoned blue-chips (like General Electric), as well as newcomers (like Open Energi). Let us look at these two examples:

General Electric's Digital Wind Farm uses constantly collected data on weather, component messages, service reports, and performance of similar models, to build a predictive model that empowers customers to improve performance, lower risk, and reduce cost. In General Electric's own words, "The Digital Wind Farm is an end-to-end wind energy system that leverages data, analytics, and software applications in partnership with our hardware and services solutions to enhance efficiency, cybersecurity, reliability, and profitability of your assets over their lifetime."

Open Energi 'manages distributed energy to radically reduce electricity costs and provide flexible capacity to enable a 100% renewable energy system.' Open Energi's Dynamic Demand platform exploits AI to maximise asset utilization, slash costs and optimise performance. In July 2021 British Petroleum acquired Open Energi and plans to expand its business model globally.

Threat spotlight: AI is like nuclear energy — 'both promising and dangerous' (Bill Gates)

The risks of AI are universal, irrespective of application: if the computational system behind these technologies is compromised, the systems that depend on them will be crippled. The problem for the utilities industry is that the stakes are so high. Without electricity, water, sewage, power and light, our societies will crumble. This precariousness is deepened by the immaturity of these disruptive technologies.

The fact that the survival of entire populations (not to mention businesses) depends on the secure supply of water, power and gas, makes utilities companies red-hot targets, not only for cybercrime, but cyber-war. State actors know that paralysing a country's utilities

infrastructure from the comfort of a malicious computer could destroy more than any bomb. A recent study by Forrester found that 88% of security professionals expect AI-driven attacks will become mainstream.

On May 6, 2021 a warning shot was fired, when the Colonial Pipeline, the largest fuel pipeline in the United States, was shut down as a result of a ransomware attack, attributed to DarkSide, a Russian speaking hacking group.

Trend #2: Data analytics

Data is the essential fuel propelling digital and technological advance in the utilities sector. The utilities sector is witnessing a revolution in the collection and analysis of real time data at an increasingly faster pace to enable proactive planning and decision making. Advanced analytics combined with human experience enables utilities not just to improve customer engagement, but also manage supply chain and grid risk better, and upgrade preventive maintenance and asset planning tasks. To facilitate data collection, utilities are installing and upgrading analytics platforms designed for ease of use and traceability.

Smart Metering is a crucial area of power reforms. The technology is transforming the way power, gas and water utilities operate to meet new ambitious goals. Globally installation of smart metering is picking up pace. Between 2021 and 2025, more than 572 million smart electricity meters will be deployed in China, India, Japan and South Korea. Not only are smart meters appealing to customers who can use them to drive down energy bills, but the large amount of data they collect also allows suppliers to drive efficiencies on the demand side, as part of the Smart Grid.

The Smart Grid is the essential counterpart to the smart meter revolution. The Global Smart Grid market is expected to reach $92+ billion by 2026. Industrial internet of things technology is being implemented across the utilities value chain, from generation through distribution and consumption. The IoT Utilities Market is anticipated to register gains at over 20% to 2024 according to a report by Global Market Insights. Sensors on equipment in power plants, hydroelectric installations, wind turbines and solar panels allow for informed, and sometimes automated decision-making, empowering operators to save costs, optimize supply, and meet demand. Data collection provides invaluable insights into improving safety and resilience.

Orbis Research's report on Global Big Data in the Power Sector Market demonstrates how big data has helped utility companies to track consumption pattern and forecast, to accordingly shift supply in both space and time, resulting in efficiently utilizing assets.

Threat spotlight: more devices, more trouble ("make no mistake, it's a war")

Adding devices to a network is like adding windows to a building. The more windows, the greater the risk of break-in (or cyber breach). We might also add, 'more data, more trouble'; after all, data is to cybercriminals what cash is to burglars. Every data collection tool added to the network provides a significant attack surface to be exploited.

Decarbonization is also increasing the number of intrusion points exponentially. For example, more devices like EV charging stations are being connected all the time. This scenario is compounded by the fact that device technology is evolving and potentially vulnerable to new and unknown cyberthreats. Utilities securing large numbers of endpoints with limited resources are particularly at risk. Cloud-based solutions are empowering utilities to engage customers in new ways but bring with them additional security issues.

The risks are self-evident. It is estimated about 25% of US power utilities were exposed to the SolarWinds massive breach in 2020-2021. Ransomware attacks are up 116% in the first five months of 2021 according to Nozomi Networks security review.

Industry-specific threat intelligence is a vital part of the cyber-immunity arsenal for utilities companies. Only expert intelligence can help operators stay ahead of new and unknown threats. Disaster recovery and incident response training are also critical. And, with the proliferation of devices and apps, Behavioral and Anomaly Analysis have a crucial role to play. These cybersecurity technologies combine data analytics and AI to 'learn' user behavior in order to immediately identify and block anomalies that indicate the presence of any threat, even if as yet unknown.

Trend #3: Decarbonization

A report by McKinsey refers to the decarbonization of industry as 'the next frontier.' Of course, the responsibility for decarbonization of industry does not fall exclusively on the shoulders of the utilities industry, however, there is a natural link, and utilities operators have a pivotal role to play. In order to achieve decarbonization, McKinsey's report recommends that "the link between the industry sector and the power sector would need to be significantly strengthened, given the interdependencies both ways."

"Parties share a long-term vision on the importance of fully realizing technology development and transfer in order to improve resilience to climate change and to reduce greenhouse gas emissions."
Article 10 of the Paris Agreement

Renewables and distributed energy resources (DERs) have a critical role to play in the move towards decarbonization, however, it is evolving technology that is making climate change possible on the scale required by our planet. As part of the Paris Agreement, signed by 174 countries and the EU, included the establishment of a Technology Mechanism, managed by the United Nations Framework Convention on Climate Change (UNFCCC).

"The US power sector is halfway to net zero emissions, but it gets harder now."

Although renewables represent more than 20% of electricity generated in Europe and the US, the targets are ambitious – 33% by 2025 and 95% net increase in global power capacity through 2050. Meeting the challenge of decarbonization requires profound changes in how utility operations operate – encompassing stake holder collaboration, customer engagement and a huge technological revolution involving digitization, sensors, IoT devices and connectivity, extending to encompass all aspects of our lives to automate efficiency-driving initiatives.

Three technological developments are seen as key: EVs to overtake the combustion engine, driving down the generation and storage cost of renewables and slashing the cost of locally produced energy eliminating the necessity to transport energy. All the above represent ongoing challenges for the energy industry.

Threat spotlight: “hyper complexity + hyper connectivity + hyper data volumes = hyper vulnerability” (ITU)

The UN Habitat programme estimates cities consume about 75% of global primary energy and emit between 50 and 60% of the world’s total greenhouse gases, with the figure rising to approximately 80% when indirect emissions generated by urban inhabitants are included. Cities are the key loci for the implementation of the new technologies that utilities companies are increasingly adopting to meet climate change guidelines and requirements.

Unfortunately, this creates a perfect cyber-storm, which the ITU describes as “Hyper complexity + hyper connectivity + hyper data volumes = hyper vulnerability.” Utilities companies lie at the heart of this storm, navigating countless interconnected connected devices, hoarding and crunching enormous datasets, and facing increasingly strict regulations, which change at a dizzying pace.

The ITU maintains that cybersecurity, information protection and system resilience are political and governance issues. The ITU report, ‘Cybersecurity, data protection and data resilience in smart cities’ stresses ‘the potential effects of malicious attacks and disasters on critical ICT systems and infrastructure, including citizens’ deprivation of essential services, from transportation to utilities (e.g. smart grid, water management).’

Emerging technology magazine Wired predicts: ‘Ever-more connected infrastructure will make it easier for hackers to take down whole towns. And cities aren’t doing enough to be prepared…’

A German cloud security provider has identified the energy industry as number one target for cyberattacks in 2019, attracting 16% of all attacks worldwide. More cyberattacks are forecast on battery and solar supply chains. The massive integration of grid networks with renewable distributed energy resources is expected to make energy networks more vulnerable to attacks. In a context of hyper-connectivity and unavoidable interdependencies with governmental and municipal systems, robust perimeter security is absolutely critical for utilities companies.

Trend #4: Distributed Energy Resources (DERs)

Hand in hand with the inevitable move away from carbon towards renewables, and the eventual phasing out of fossil fuel use, is the growth in consumer adoption of Decentralized Energy Resources, (DERs) which naturally include renewables. According to Bloomberg's New Energy Outlook, 'Consumer energy decisions such as rooftop solar and behind-the-meter batteries help shape an increasingly decentralized grid the world over.'

Distributed Energy Resources (DERs) implies the generation of renewable energy on a local level, which circumvents existing national (or even regional) infrastructure, and therefore depends to a large extent on the degree of deregulation within respective energy markets. Decentralization affects distribution as well as generation. It involves the establishment of a bi-directional energy flow, providing the framework by which ordinary consumers with, for example, solar panels on their houses, can feed any excess energy back into the grid, creating the new role of 'prosumer.' According to the EU, this is facilitated by the Smart Grid, which "open up the possibility for consumers who produce their own energy to respond to prices and sell excess to the grid."

The summer of 2021 G7 meeting stressed the importance of Distributed Energy Resources (DERs) for addressing security as well as climate challenges. DERs facilitate decarbonization by enabling renewables to be used – for example solar replacing fossils, (global solar power expanded by 138.2 GW of installation in 2020, an 18% year-on-year growth) and EVs replacing oil with electricity (global EV sales grew by 41% from 2019 and the global electric car sales share rose to a record 4,6% in 2020). Across the world, electrification solutions are proliferating with a fast-expanding supply of clean renewable electricity.

Bloomberg reports 'Australia and Japan are on track to develop the two most decentralized electric systems in the world.' The US is also fast decentralizing. In September 2020, the US Federal Energy Regulatory Commission (FERC) passed Order 2222 opening the door for a wholesale distributed energy resource (DER) market.

$96.7 billion

"The global market for heat pumps is forecast to grow from $60.4 billion in 2021 to $96.7 billion by 2026, at a compound annual growth rate (CAGR) of 9.9% for the period of 2021-2026."
Research and Markets

Another compelling advantage of DERs is, by enabling a range of efficient energy, localised demand solutions using battery and solar power, it offers empowerment (in both senses of the word) to populations in developing countries, allowing them to access, and even generate (as prosumers), energy on a local level, bypassing any shortcomings in national, regional or local infrastructure. The World Bank calculates 760 million people in the world don't have access to electricity in their homes, reduced from more than one billion a decade ago. 'Electrification through decentralized renewable-based solutions in particular gained momentum'. However distribution across countries is also woefully unequal. Only 6.7% of South Sudan citizens, 8.4% in Chad, 11.1% in Burundi, 11.2% in Malawi and 14.3% in Central African Republic have access to electricity.

DERs however underline the transition for traditional utility companies struggling to adapt from 20th century model of large, centralised, uni-directional generators connected to grids catering for stable demand and offering almost zero price flexibility. Bi-directional flow of power is a challenge that could result in an overflow of power line capacity. End-use devices represent an as yet unquantifiable burden on grids. Consumers all switching on heat pumps or charging EVs at the same time could cause unmanageable spikes in power use. Adapting to bi-directional flows is forcing utilities to invest significantly in updating grids.

Threat spotlight: the vulnerabilities of complex, automated multi-node networks

The power grid, and energy infrastructure in general, were not designed for bi-directional flow, and certainly not for flow between increasingly small loci of generation and distribution. Instead of the precise and tightly controlled unidirectional flow of energy from grid to home (or office), decentralization creates a highly complex interconnected web of end nodes, advanced controls, digital sensors, software and network architectures, with its own vulnerabilities and potential connection security concerns. Compounding this is the fact that such complex networks increasingly rely on automation in order to function – introducing further vulnerabilities related to the use of AI on legacy hardware and software.

Virtual power plants utilising smart grid infrastructure to connect small amounts of energy assets into a single generator empower consumers as suppliers (prosumers) channelling excess energy into the smart grid. The model is attractive and the energy industry forecasts a massive increase in decentralized digital devices funnelling distributed energy supply to virtual power plants. However dependency on smart grid infrastructure clearly increases cybersecurity risk. As widespread, decentralized energy sources are fed in by network-linked endpoints, the virtual power plant's centralised process is vulnerable to cyber criminals breaching the entire network via a single endpoint. For example an attacker could theoretically disrupt significant numbers of storage batteries or e-car chargers for payback. It is no coincidence that malware and ransomware targeting critical infrastructure services is on the rise. Conventional risk management is no longer sufficient. DERs clearly lessen the control and oversight utilities previously had over energy resources stored in their power grids.

Policing this new network is a complicated challenge, made worse by the immaturity of the decentralized sector. The current set up provides little transparency to utilities. The need for robust universal standards and regulation is clear. Questions around accountability for cybersecurity also loom large.

These risks make industry-specific vulnerability scans and emergency response retainers an absolute must for utilities companies. Prevention is better than cure and, if the worst happens (perhaps because of a vulnerability within a separate but connected architecture), acting promptly and appropriately, can stop disaster in its steps.

Trend #5: Regulatory challenges

Given the life-critical nature of utilities, the industry is among the most highly regulated on the planet; subject to a swathe of regulations, at international, national, regional and local level. A large proportion of these regulations relate to the fact that utilities companies are often natural monopolies, particularly in countries where private companies have secured tender for the sole supply of regional (or even national) utilities. However, monopoly regulations are only the beginning of the story. Utilities operators must navigate regulations covering an enormous range of concerns; including operations, distribution, maintenance, interconnection, billing/pricing, competition, procurement, data protection, and of course climate change mitigation. Noncompliance results in increasing system risk and sizeable financial penalties.

Unsurprisingly, cybersecurity and resilience in the utilities industry are tightly controlled. As an example, the US Federal Energy Regulatory Commission requires operators to give detailed answers to questions about their unique resilience risks, impact likelihood, identification of threats, incident planning, threat mitigation, analyses of past events, equipment, engineering and physical assets. In all cases, cyber risks are listed alongside natural events such as drought, since the Commission's January 2018 Order.

In 2021 governments around the world are urgently looking at measures to enforce cyber resilience in crucial utility companies. The May 6, 2021 attack on Colonial Pipeline, reportedly by a Russia-based cybercriminal group, shut down 5,500 miles of pipeline, transporting 45% of fuel supplies on the east coast of the US. A state of emergency was declared in four US states. For regulators this was a wake-up call. Was there a failure of compliance? Was this a preventable attack? The Department of Homeland Security rapidly laid out more stringent cybersecurity requirements 'to better identify, protect against, and respond to threats to critical companies in the pipeline sector'.

"As energy companies adapt their business models to fit today's fast-paced market environment, their legal and compliance functions must adapt as well. Digital enablement of energy regulatory and compliance monitoring processes can help address those problems and issues through a unified solution."
Deloitte

"CEOs report regulatory pressure on environmental, social, governance issues in survey." KPMG

Currently the EU is putting together a draft bill (replacing a 2018 law) to intensify cybersecurity requirements for electricity and energy suppliers. Taking a different approach the Federal Energy Regulatory Commission (FERC) is proposing a law change to offer federal subsidy incentives (deferred cost recovery) for electric companies implementing cybersecurity measures above standards of current regulations.

In addition, recently introduced regulations not pertaining to cybersecurity, nevertheless have a big impact on cybersecurity demands. A case in point is the US Federal Energy Regulatory Commission (FERC) Order 2222 potentially transforming the energy sector by liberalising the market for wholesale distributed energy resource (DER) providers.

In conclusion the cyber vulnerability of digitally integrated energy assets has yet to be fully tested. **A KPMG survey found that 48% of utilities CEOs believed that becoming the victim of a cyberattack was a question of 'when,' not 'if.'**

Threat spotlight: failure to comply with regulations leads to fatal outcomes

Failure to comply with regulations can lead to two fatal outcomes. Firstly, where regulations provide a guiding framework of cybersecurity standards, non-compliance could lead to a devastating breach. Secondly, on the governance side, failure to comply can lead to license loss. Both outcomes can bring a utilities operator to its knees.

2021's litany of cyberattacks on utilities across the globe shows the scale of the problem. Singling out just two: in August 2021 a breach at T-Mobile led to unauthorized access to more than 50 million people's personal details. In May 2021, Volue, Norwegian energy Technology Company was hit by a ransomware attack forcing it to switch off key water and water treatment facilities. The fallout from breaches like those above means regulators are compelled to continue tightening their rules.

The fines are getting tougher as well. In 2019 Duke Energy faced a record $10 million fine from federal authorities after exposure of extensive cybersecurity failures that allegedly "posed a serious risk" to grid security and reliability. China's newly signed Data Security Law (September 2021) contains detailed provisions regulating collection, usage and protection of data and stringent measures for failing to meet the provisions including potential suspension of business.

Compliance failure is not the only challenge when it comes to regulations. The dizzying array of regulations affecting utilities operators across the globe, in the context of drastic consequences for non-compliance, is exhausting, particularly for companies operating in multiple markets. This is further complicated by the constant emergence of new technologies, and uncertainties about the regulations that will emerge to govern them.

For utilities companies, being prepared for regulations means also adopting industry-appropriate cybersecurity.

Summary

The five trends outlined above highlight the huge opportunities and challenges that lie ahead for utility companies. The imperative is not just to embrace new technologies but also to secure them. Building a culture of cyber-immunity will empower utility companies to truly reap the benefits of high levels of connectivity and automation, minimize any negative impacts and maximize return on investment. In today's volatile and fast-changing environment, Kaspersky has perfectly engineered, tailored solutions and services – assisted by world-leading security intelligence – to protect data and business continuity 24/7 against advanced threats and targeted attacks – mitigating risks, detecting attacks earlier, neutralizing live attacks and fortifying future protection.

Kaspersky offers a **stage-by-stage cybersecurity approach** designed to clarify which level of security as well as which specific solutions suit your organization best. The stages provides a set of easily managed threat protection measures coordinating seamlessly with one another to meet the needs of each individual organization, and offer a cybersecurity roadmap assuring smooth transition from one IT security maturity level to another when the time comes.

Kaspersky's step-by-step cybersecurity approach

1

Kaspersky Security Foundations – essential core of cloud-based, automated protection for all devices, VDI and hybrid server infrastructures, before organizations advance seamlessly to ...

2

Kaspersky Optimum Security - for organizations requiring more specialized security against new and evasive threats, before effortlessly implementing ...

3

Kaspersky Expert Security – for organizations with established mature IT security teams combatting the most complex targeted attacks.

Cybersecurity maturity level	Solution
IT Smaller organizations without a specialized IT security team	**What** **Kaspersky Security Foundations** **How** Implement fundamental security for organizations of any size and infrastructure complexity, delivering cloud-managed automatic prevention of commodity cyberthreats on any devices, VDI and hybrid server infrastructures. ▸ **Endpoints:** Protect every endpoint in your organization with **Kaspersky Endpoint Security for Business; Kaspersky Embedded Systems Security** ▸ **Cloud:** Benefit from borderless security with **Kaspersky Hybrid Cloud Security** ▸ **Network:** Secure your perimeter with **Kaspersky Security for Mail Server; Kaspersky Security for Internet Gateway** ▸ **Data:** Safeguard valuable and sensitive data with **Kaspersky Security for Storage** ▸ **Security Management:** Access expertise with **Kaspersky Premium Support; Kaspersky Professional Services**
IT security Organizations in need of advanced defenses, but with limited specialist IT security resources	**What** **Kaspersky Optimum Security** **How** Combat evasive threats with effective endpoint detection and response and continuous security monitoring – but without prohibitive costs or complexity ▸ **Advanced detection:** Boost ML behavior analysis, sandboxing, threat intelligence and automated threat hunting* with **Kaspersky Sandbox, Kaspersky Threat Intelligence Portal and Kaspersky Managed Detection and Response Optimum** ▸ **Analysis and investigation:** Enhance threat visibility and simplified investigation process with **Kaspersky Endpoint Detection and Response Optimum** ▸ **Rapid response:** Deploy automated in-product response options, as well as guided and managed response scenarios* with **Kaspersky Endpoint Detection and Response Optimum and Kaspersky Managed Detection and Response Optimum** ▸ **Security awareness:** Equip employees with automated tools at all levels and develop key cybersecurity skills with **Kaspersky Security Awareness Training** *Supported by Kaspersky experts

Mature and fully formed IT security team and/or dedicated SOC

- Have a complex and distributed IT environment
- Are a highly likely target for complex and APT-like attacks
- Have a low risk appetite due to high costs of security incidents and data breaches
- Are concerned about regulatory compliance

What

Kaspersky Expert Security

How

Complete mastery over the most complex and targeted cyberattacks

- **Equipped:** Equip your in-house experts to address complex cybersecurity incidents. Benefit from a unified cybersecurity solution. **Kaspersky Anti Targeted Attack Platform with Kaspersky EDR** at its core empowers your team with XDR capabilities.

- **Informed:** Enrich your knowledge pool with threat intelligence and upskill your experts to deal with complex incidents:
  - Integrate actionable, immediate threat intelligence into your security program. **Kaspersky Threat Intelligence** gives you instant access to technical, tactical, operational and strategic threat Intelligence.
  - Develop your in-house team's practical skills, including working with digital evidence, analyzing and detecting malicious software, and adopting best practices for incident response, with **Kaspersky Cybersecurity Training**.

- **Reinforced:** Call upon external experts for security assessment, immediate support and back-up:
  - Take advantage of immediate support from the **Kaspersky Incident Response** team of highly experienced analysts and investigators to fully resolve your cyber-incident, fast and effectively.
  - Bring in a second opinion and managed threat hunting expertise from a trusted partner with **Kaspersky Managed Detection and Response**, so your in-house IT security experts have more time to spend reacting to the critical outcomes requiring their attention.
  - Understand just how effective your defenses would really be against potential cyberthreats, and whether you're already the unwitting target of a long-term stealth attack, through **Kaspersky Security Assessment**.

Targeted Solutions

What	How
Kaspersky Fraud Prevention	Advanced Authentication allows for frictionless and continuous authentication, cutting the costs of second factor processes for legitimate users, while keeping fraud detection rates high in real time. Automated Fraud Analytics thoroughly analyzes events that occur during the entire session, transforming them into valuable pieces of data. Protects the external perimeter of any organization, ensuring safety and protection for citizens/customers.
Kaspersky Industrial Cybersecurity	KICS offers a holistic approach to industrial cybersecurity, bringing value to any stage of the customer's OT security process – from cybersecurity assessments and training to advanced technologies and incident response. An ecosystem of integrated products and services allows to secure operational technology layers and elements of your organization - including SCADA servers, HMIs, engineering workstations, PLCs, network connections and even engineers - without impacting on operational continuity and the consistency of industrial process.
Kaspersky ICS Security Assessment	For organizations concerned about the potential operational impact of IT/OT security, Kaspersky provide a minimally invasive pre-installation cybersecurity assessment. A crucial first step in establishing security requirements within the context of operational needs, it can also provide significant insight into cybersecurity levels without any further deployment of protection technologies.

Cyberthreats News: www.securelist.com

IT Security News: www.kaspersky.com/blog

Threat Intelligence Portal: opentip.kaspersky.com

Technologies at a glance: www.kaspersky.com/TechnoWiki

Awards and recognitions: media.kaspersky.com/en/awards

Interactive Portfolio Tool: kaspersky.com/int_portfolio

kaspersky BRING ON THE FUTURE