accenture

BUILDING GREATER CYBER RESILIENCE IN RENEWABLES

INTRODUCTION

In 2019, the renewable energy sector recorded its largest ever increase in installed capacity, with more than 200 GW added, outpacing net installations in fossil fuels and nuclear power combined.[1]

By year end, installed renewable energy capacity provide an estimated 27.3% of global electricity generation. In most countries, it is now more cost effective to produce electricity from wind and solar PV than from new coal-fired power plants, leading to record-low bids in tendering processes.[2]

The rapid growth in the deployment of renewables capacity has been accompanied by an evolution of business models, cost pressures and the regulatory landscape. Technology-wise, the industry is on course for an irreversible IT/OT convergence, driven by factors including:

Increased automation and digitalization of assets and operations.

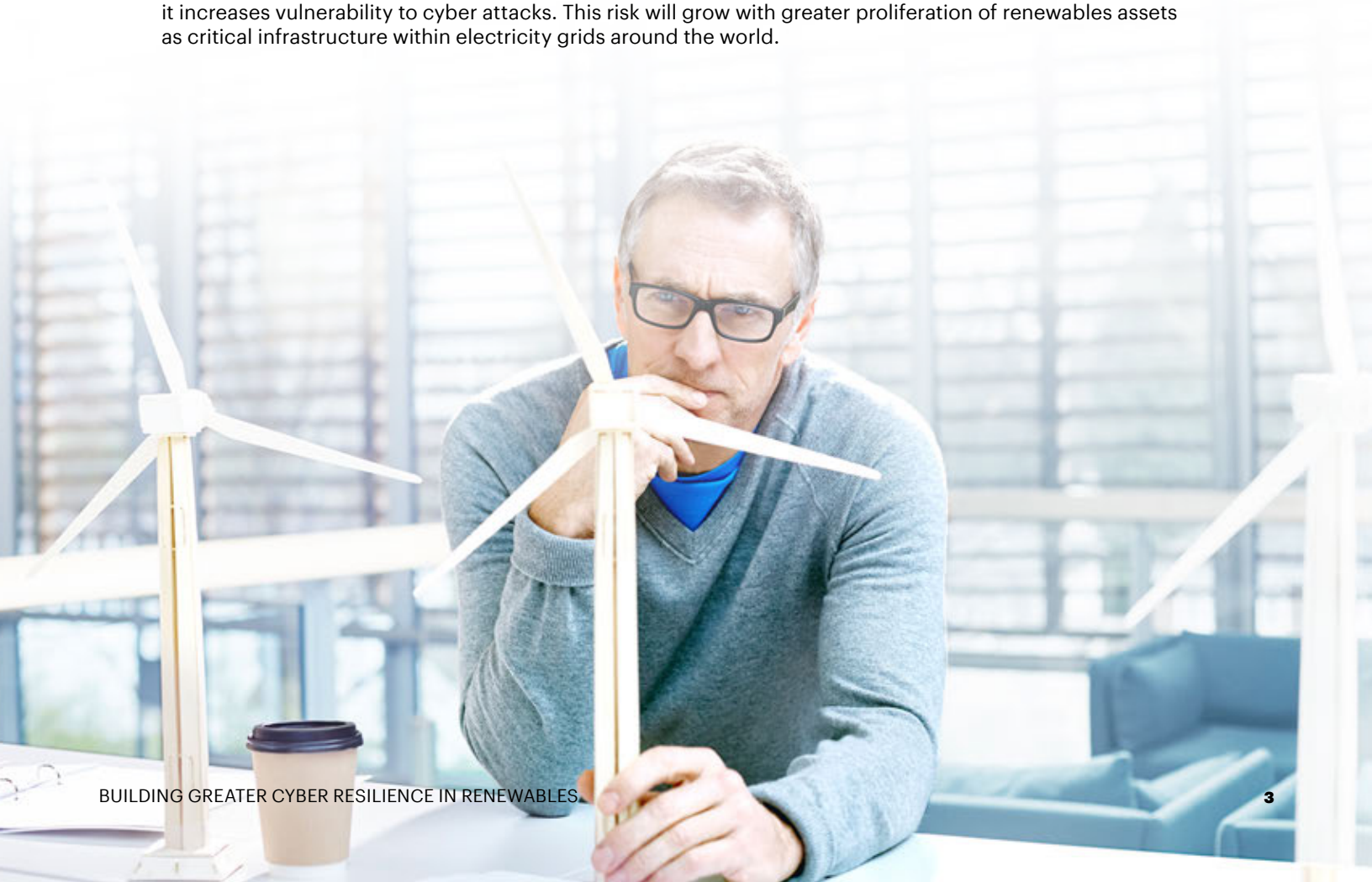
Growing use of intelligent connected devices.

Reduced maintenance cost to boost profits and shareholder return.

More demand for remote asset management.

Rising regulatory pressure across electricity and power generation.

While IT/OT convergence creates significant operational and financial benefit for renewables operators, it increases vulnerability to cyber attacks. This risk will grow with greater proliferation of renewables assets as critical infrastructure within electricity grids around the world.



Cybersecurity poses a serious challenge for renewables operators. Many of the systems currently in use were built prioritizing efficiency over security. Other risk factors include the ecosystem of original equipment manufacturers (OEMs) and third-party operations and maintenance (O&M) providers with access to their assets and networks and the manual processes used in onboarding these service providers and checking permits. Consequently, many renewables operators have significant technical, people and process security gaps; common gaps are illustrated in Figure 1.

Security gaps can be exploited across the entire renewables value chain by a variety of malicious actors, from nation states to hacktivists and cyber criminals to disgruntled employees. Gaps also create the risk of unintentional but damaging actions by company personnel and third parties.

These threats are constantly evolving and have potentially severe consequences such as:

- Loss of production and revenue.
- Damage to assets and infrastructure.
- Leakage of sensitive commercial information and reputational damage.
- Regulatory non-compliance and fines.
- Health, safety and environmental (HSE) risk.

To alleviate these risks, renewables operators need to develop a clear understanding of their cybersecurity gaps, apply mitigation steps, and evolve their approach to cybersecurity along with the cyber threat landscape.

Figure 1. Typical technical, people and process gaps.

Typical Technical Gaps

Without **VISIBILITY** into what devices and systems are on the network and how they communicate and operate, they cannot be easily or fully secured.

Renewables plants often include devices not designed for increased connectivity, so additional safeguards such as **NETWORK SEGMENTATION** should be considered.

Significant threat exposure from limited or no capabilities to **MONITOR ACCESS** to and from devices by authorized people and applications.

Lack of **AUTOMATION** to produce utilization reports, lifetime patch status, recall and other important capabilities.

Incomplete **SECURITY CONTROLS** to support inline, real-time prevention of cybersecurity threats without intrusive patching, downtime or service interruption.

Common People and Process Gaps

Accountability, **ROLES AND RESPONSIBILITIES** are often unclear.

GOVERNANCE is rarely well established, especially in areas of identity access management (IAM), change management, and patch management, and do not often involve security.

There are often **GENERATIONAL SUCCESSION** issues, coupled with staff that lack **SECURITY EXPERTISE** (limited pool).

Industrial device manufacturers' **PRODUCT DEVELOPMENT** processes often do not address or incorporate cybersecurity qualities or values.

Response plans do not **ADDRESS CYBER EVENTS**; focus is on maintenance and repair operations (MRO), but security is not directly addressed.

THE CURRENT STATE OF CYBERSECURITY

Given the severity of the associated risks and emerging compliance requirements, cybersecurity is increasingly becoming a high priority on the board and C-suite agenda for renewables operators and other utility companies.

Industry Trends

Renewables operators and the wider industry are realizing the criticality of cybersecurity in holistic asset resilience. Incident response and threat-hunting capabilities are being developed to safeguard business readiness for potential security events. Companies without in-house capabilities are also taking on managed security services to run their cybersecurity operations.

Research conducted by Accenture Security shows that, on average, utilities companies are improving on cybersecurity basics.[3] The companies surveyed—across all industries, including utilities—had an 11% reduction in direct attacks and a 27% reduction in security breaches over the past year. There has also been significant innovation investment, with 94% of utilities respondents spending more than 20% of their cybersecurity budgets on advanced technologies.

Common areas of investment include governance and management, asset management and inventory, network segmentation, remote access, backup and restore, cloud security and security monitoring.

While progress has been made, there is growing concern about the rise of indirect attacks targeting weak links in utilities' supply chains. These attacks accounted for 39% of the cybersecurity breaches in 2019.[3] Additionally, the cost of staying ahead of attackers is rising at unsustainable levels, and 77% of utilities say they do not see adequate return on their cybersecurity investments.[4]

Inadequate returns are evident in the low detection rates of breaches—only 56% are found by security teams, and in the long business impact, with only 12% of breaches having an impact lasting less than 24 hours.[5]

Challenges

While renewables operators are increasing commitment to and investment in cybersecurity, challenges remain that prevent security operations teams from keeping pace with the evolving cyber threat landscape.

Increase in electronic monitoring and control of utility-scale renewables and in the deployment of edge devices creates new entry points for cyber attacks on renewables assets. In solar, wider adoption of two-way communication smart inverters without strong communication standards introduces vulnerability. Likewise, weak cybersecurity controls on sensors and wind turbines leave wind power operators open to new cyber threats.

The rise of the industrial internet of things (IIoT) and hyper-connectivity means that the attack surface available to malicious actors is constantly growing, while asset discovery and cyber visibility is becoming more complex.

Renewables assets are geographically dispersed, mostly left unmanned, and have a workforce that often includes multiple third parties in remote locations. The large ecosystem of third-party service providers with network access poses a challenge as they, along with OEMs and suppliers, can introduce security weak links for attackers to exploit.

There are many security tools available that are not well integrated, are inflexible and become quickly outdated. These tools often have complex, labor-intensive installation and maintenance processes. They generate high volumes of data lacking in context and prioritization, requiring time-consuming investigation to extract useful intelligence.

Technical difficulties are exacerbated by the global talent shortage of operational technology (OT) security experts, due to simultaneous cross-industry investment in the area. This is further compounded by distrust and lack of communication between IT operations and the business, which can often lead to the information security team not being included when discussions begin on new operational initiatives.

Finally, increasing IT/OT convergence is exposing considerable disparity in the maturity levels of IT security and OT security in most companies. This is an area of concern as the automation of renewables infrastructure increases the stakes at play with potential security breaches.

CYBERSECURITY REGULATION IN RENEWABLES

Greater electricity generation from renewables around the world has resulted in renewables assets increasingly being classed as critical infrastructure. This development means that renewables operators are now required to comply with many new cybersecurity regulations implemented in response to the emergence of the IIOT.

Some regulations relevant to renewables operators include the NIS Directive on cybersecurity in the European Union, NERC CIP in the United States, a variety of national critical infrastructure protection regulations, ICS standards and leading cybersecurity practices such as ISA/IEC 62443, NIST 800-82, the NIST cybersecurity framework or ISO/IEC 27001.

While regulatory compliance is a good incentive and guideline for renewables operators, it should be the starting point and not the target state for cyber resilience. The major cybersecurity regulations apply across industries and are not tailored to the specific challenges of renewables operators. In addition, some operators at their current installed capacity do not yet meet the eligibility criteria for certain regulations that apply to the broader energy industry.

To shore up the cyber resilience of their operations, renewables operators will need to factor regulatory compliance requirements into their cybersecurity strategy, but also be proactive in developing additional layers of controls tailored to mitigate their specific challenges.

NIS DIRECTIVE

The first EU-wide legislation on cybersecurity providing legal impetus to boost overall level of cybersecurity in the EU.[6]

NERC-CIP

Standards defining the reliability requirements for planning and operating the North American bulk power system.[7]

ISA/IEC 62443

A flexible framework to address and mitigate current and future security vulnerabilities in industrial automation and control systems (IACSs).[8]

NIST 800-82

A guide for securing industrial control systems (ICS), including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations.[9]

NIST Cybersecurity Framework

A flexible framework providing voluntary guidance based on existing standards, guidelines and practices for organizations to better manage and reduce cybersecurity risk.[10]

ISO/IEC 27001

An internationally recognized standard that provides requirements for an information security management system (ISMS).[11]

RETHINKING CYBERSECURITY: A PARADIGM SHIFT

As renewables operators look to evaluate how they can boost cyber resilience, three key paradigm shifts are needed.

Bridging the maturity gap between IT security and OT security.

IT security extends from the cloud through to connected IT devices and is more mature than OT security. However, as the lines between IT and OT continue to blur, attempting to simply replicate security models from IT to OT should be avoided. Two key differences between IT and OT are impact and criticality, and these should be measured in both the digital and physical domains.

Bridging the security maturity gaps between operations, other functions such as business development and engineering, and third parties.

Renewables operators need to close security gaps within their organizations, in their supply chains and with their interfaces to OEMs/third party providers. Sealing these gaps is crucial, as malicious actors can exploit the weakest point in the network as a gateway to higher-value areas.

Building trust between IT operations and production operations.

Look to build synergy between IT and the business for greater collaboration, coordination and commitment. For successful threat mitigation, creating value and providing protection should be viewed as complementary rather than competing agendas.

CYBERSECURITY AND RENEWABLES DIGITAL TRANSFORMATION: BENEFITS

These three paradigm shifts could allow renewables operators not only to abate risks but also realize benefit for their wider digital transformation. There are strong incentives to improve cybersecurity, both for operators early in their digital transformation journey and those further along.

Security supports a nascent digital transformation

Improved cybersecurity capability is an enabler for operators early in the process of digitalizing their operations:

01 **Centralized data repository.** A strong cybersecurity framework allows the secure centralized collection of operations data to amass an asset history and facilitates development of predictive maintenance capabilities.

02 **OT network visibility.** OT network asset discovery, creation of network maps with communication flows and monitoring of the security of OT infrastructure can help safely increase OT network visibility. Greater OT network visibility can aid operational excellence through quicker identification of potential process disruption and asset failure scenarios.

03 **Enabling technologies.** Securing the OT network paves the way for architectural decisions on implementing enabling technologies such as assisted reality and industrial process optimization by making integrated real-time data safely available.

Security improves a delivered digital transformation

Improved cybersecurity capability also plays a key role for operators advanced in their digital transformation journey:

01 **Novel use cases:** Improved cybersecurity allows the business to trial new use cases and technologies by mitigating for the associated risk. This creates opportunities in risky but rewarding areas such as advanced process automation, which can improve safety, operations efficiency and production throughput.

02 **Enhanced situational awareness.** Improved cybersecurity allows for earlier incident detection, helping reduce unplanned outages and enhance production availability.

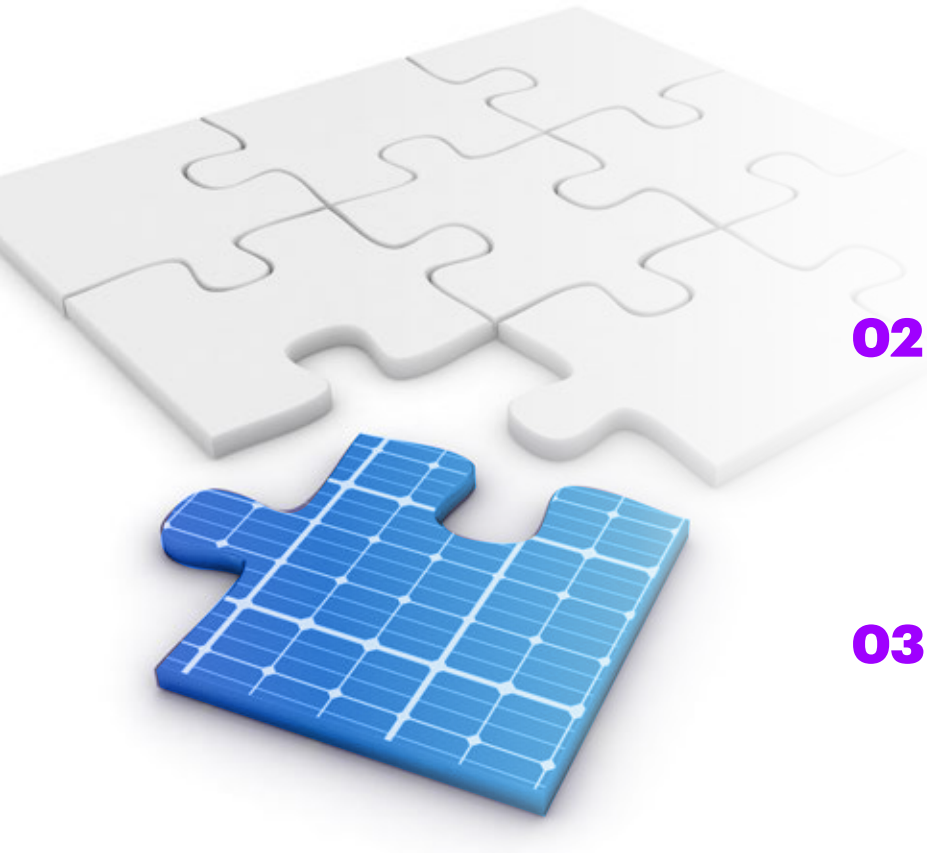
03 **Tightened access control.** Improved protection of systems and information from unauthorized access reduces the risk of sensitive information disclosure, network breaches and regulatory penalties.

RENEWABLES CYBERSECURITY PLAYBOOK: A WAY FORWARD

Digital transformation in renewables involves new and disruptive approaches, technologies and solutions, and will require new architectures, models and thinking around cybersecurity.

For sustained growth, operators should embed the security gene in the renewables DNA to strengthen the cyber resilience of their business, operations and infrastructure.

This vision of embedding the security gene requires creating a "cybersecurity playbook." The next two sections explore what this involves and how to apply it.



The "what" of the renewables cybersecurity playbook

Accenture's most recent Annual State of Cyber Resilience Report for Utilities identified an elite group of organizations outperforming in cybersecurity. These leaders are four-times better than the rest of the industry at stopping attacks. They are also better at finding breaches quickly, fixing breaches quickly and reducing breach impact (four-times, three-times and two-times better, respectively).

A deeper look into these cybersecurity leaders revealed three key differentiators that set them above the competition.

These differentiators provide guidance for renewables operators on what they should do to develop greater cyber resilience.

01 **Invest for operational speed:** Leaders prioritize speed of breach detection, recovery and response, and measure the success of their resiliency. They invest in advanced technologies such as a next-generation firewall, artificial intelligence (AI), and Security Orchestration, Automation and Response (SOAR). These technologies can help reduce the number of successful attacks and the impact and cost of breaches.

02 **Drive value from new investments:** Leaders scale their security technology investments: they are better at training their personnel and they collaborate more with internal and external ecosystem stakeholders. Consequently, they are better at discovering and defending attacks and aligning with regulatory requirements.

03 **Sustain what they have:** Leaders focus more budget on sustaining their existing core capabilities while the rest of the pack place a greater emphasis on piloting and scaling new capabilities. Leaders perform better on fundamental data protection practices, with a greater emphasis on data-centric security.

The "how" of the renewables cybersecurity playbook

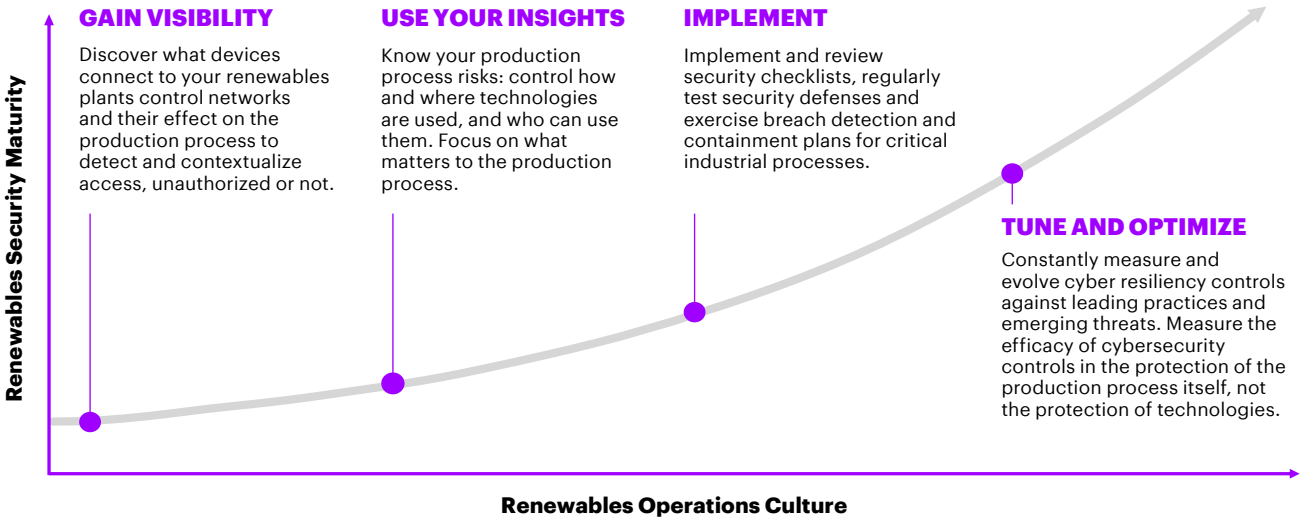
Building up cyber resilience requires direct action from renewables operators and collaboration with their ecosystem stakeholders. To effect change, two main approaches can be employed, but a simultaneous combination of both could yield the best results.

Security in renewables initiatives/projects.
Security must be assessed and prioritized at every stage of the project lifecycle and in all initiatives or business solutions. From the construction and commissioning of new plants to the adoption of emerging technologies like AI, machine learning and advanced analytics, security should be embedded in all of the processes.

Security initiatives/projects in renewables.
"Secure" is not an achievable state. Improving cyber resilience requires a program with an evolving playbook of people, process and technology initiatives coupled with constant vigilance.

Figure 2 illustrates key guidelines when considering cybersecurity initiatives to transform operations culture and increase security maturity.

Figure 2: Guidelines for increasing security maturity.

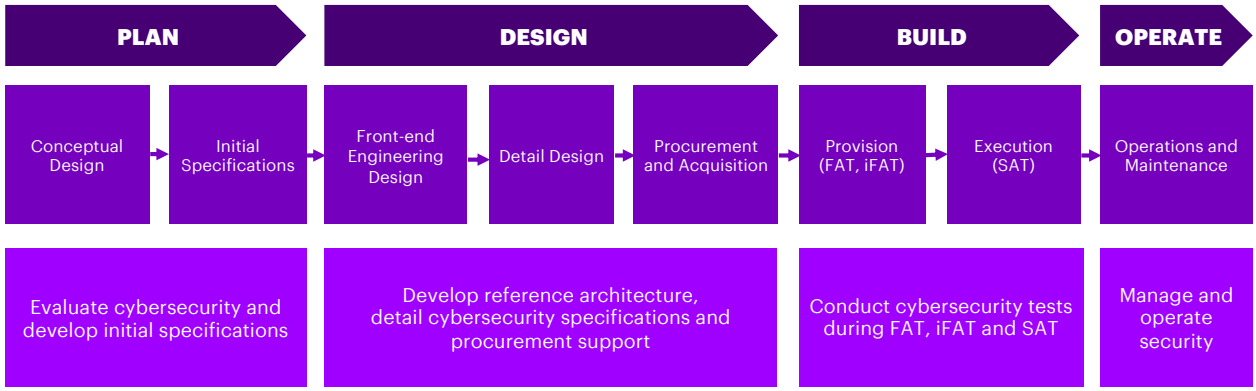


The considerations and approach to setting up a cybersecurity program will vary depending on the project scenario. In the following text, we illustrate three scenarios: constructing a new plant, operating existing plants, and completing mergers and acquisitions.

- **Constructing a new plant.**

  When constructing a new plant, cybersecurity needs be factored into the lifecycle of the project, assets and infrastructure. This begins with creating a reference model/architecture, security requirements and a procurement language in the planning phase. It involves security assessments during design, security evaluation during procurement and testing during construction and commissioning. Figure 3 demonstrates how to factor cybersecurity into a project.

Figure 3. Cybersecurity in the engineering, procurement and construction (EPC) project lifecycle.



- **Operating existing plants.**

  There are different considerations to factor in when creating a cybersecurity program for plants already in operation by a company, depending on the size and risk profile of the plant.

  Figure 4 details the approaches for relatively small plants with low financial and customer implications, compared to large plants with more severe implications or plants that are critical infrastructure.

Figure 4. Cybersecurity considerations for small and large plants.

SMALL PLANTS

Be brilliant at the basics, securing and remediating highest risks

- Establish baseline security
- Security activities for preventing and reducing attack impacts
- Security by design, embedded in operations
- Inventory and vulnerability assessment

LARGE PLANTS

Increase visibility, resilience and defense automation

- Inventory and business impact analysis
- Risk assessment and vulnerability assessment
- Security remediations plan/program
- Increase cybersecurity visibility

- **Completing mergers and acquisitions.**

  As many renewables operators look to scale and expand their portfolios, mergers and acquisitions are a common strategy of choice. It is crucial to embed cybersecurity due diligence in the deal process. Understanding the standard of cybersecurity controls of the business to be integrated is key for safeguarding network security and preventing the addition of potential points of failure.

  The main elements to carry out in this process include:

  - Develop a cybersecurity evaluation framework (including people, process and technology perspectives) comprehensively covering corporate, operations and regulatory cybersecurity requirements.
  - Conduct cybersecurity health assessments during the selling, merger or acquisition phases (including cyber-regulatory compliance assessments).
  - Conduct vulnerability assessment and penetration testing on identified critical processes and assets to identify overall security posture.

TIMELINE AND APPROACH OF A RENEWABLES CYBERSECURITY PROGRAM

Implementing a cybersecurity program is a key step for renewables operators looking to standardize and strengthen cybersecurity capabilities. It consists of three phases that tend to partially overlap each other: program development, OT security implementation and a transition to run.

Program development

The goal of this phase is to establish uniform, standardized cybersecurity governance and risk management frameworks. These frameworks should be backed up by an operational model and supporting organization to address the cyber threats identified across IT/OT and confirm business-driven operational resilience.

OT security implementation

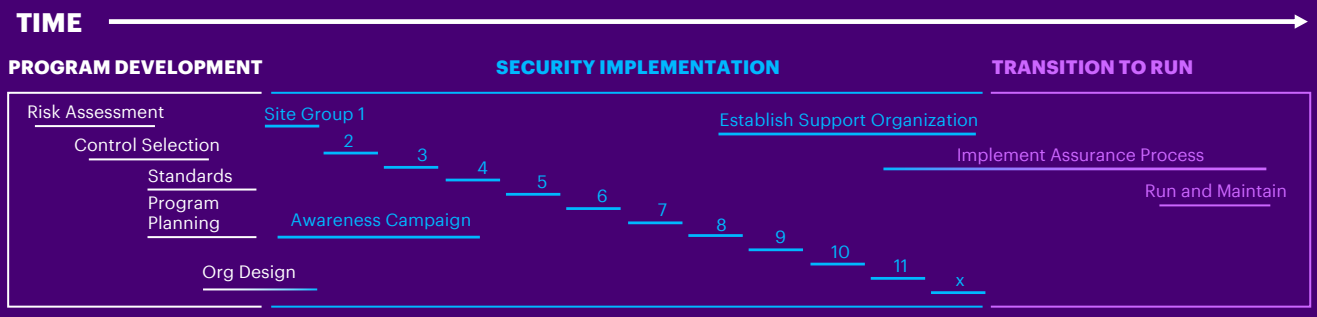
This phase includes assessing the security posture of plants, remediating identified risks and implementing the security controls developed in the initial phase.

Transition to run

While progressing through the OT security implementation, commence a transition from implementation to running and maintenance. This will confirm that change is sustainable, through validating efficacy of the implementation, compliance assurance and building a knowledge base.

Figure 5 illustrates a sample timeline of the activities involved in implementing a cybersecurity program, with further detail on the steps for each phase.

Figure 5. Timeline and approach of a renewables cybersecurity program.



PROGRAM DEVELOPMENT

- Conduct risk assessments to determine cyber risks with associated business impacts
- Develop cybersecurity governance and risk management frameworks; choose security controls based on risk reduction
- Develop EPC security requirements and security reference architecture
- Develop standards to implement the desired security controls
- Create a program to implement the chosen security controls in the business
- Establish an organization to support program implementation
- Manage supply chain security, establishing requirements with suppliers in cybersecurity procurement language

OT SECURITY IMPLEMENTATION

- Develop site procedures to enable compliance with the standard
- Implement baseline security controls to facilitate central visibility and management
- Based on the selected security controls, conduct site assessments to determine gaps against the desired baseline
- Based on the identified gaps, conduct a site-by-site remediation to bring into compliance with standard
- Run an awareness campaign to upskill personnel on security leading practice

TRANSITION TO RUN

- Transition from program controls implementation to run and maintain by company personnel
- Implement assurance process to confirm ongoing effectiveness and risk reduction of security controls
- Establish periodical maintenance windows to verify compliance with OT security standards
- Develop and maintain a knowledge base containing backlog of troubleshooting, processes and baseline creation history

CASE STUDY

CREATING A CYBERSECURITY PROGRAM AT A GLOBAL RENEWABLES OPERATOR

This major global diversified renewables company operates in dozens of countries across five continents. They worked with Accenture to set up a cybersecurity program for their global fleet of conventional and renewable assets.

In implementing this cybersecurity program, we used an IT/OT cybersecurity risk-based approach. The work was split across two phases, with the first involving:

Identifying impact areas by technology, regulation and business strategy.

Clustering plants based on impact areas.

Evaluating cybersecurity risk on IT/OT assets based on the clusters.

Technical OT assessment (networks, hosts and services).

Vulnerability analysis and a cybersecurity remediation plan.

The second phase of work on this program involved performing the necessary remediation activities on each plant to confirm compliance with security guidelines. Some of the actions taken included:

Patching: Implementing security patching on operating systems and software, uninstallation of unnecessary programs.

Account hardening: Removal of unnecessary user accounts and disabling unauthenticated network access.

Systems hardening: Disabling removable media drives such as USB ports and disabling the "autoplay" feature, among other measures.

End point security (antivirus and whitelisting): Installation of the company-approved antivirus and whitelisting agents on all systems.

CONCLUSION

Variable renewables currently make up more than 20% of electricity generation in many markets. By 2030, Europe expects variable renewables will account for 54% of the electricity mix and, combined with hydropower, almost 70%.[12] To support this transition, the power system is transforming to accommodate more variable generation, with plants that are fleets of intelligent, connected rotating and static equipment. Simultaneously, operators are undergoing a digital transformation, incorporating automation, robotics and hyper-connectivity in the construction and operation of wind and solar farms.

These ongoing infrastructural and digital transformations introduce new threats and complexities that call for a parallel transformation in cybersecurity to sustain renewables growth and protect future energy security. Cybersecurity should be considered as vital as data quality processes in plant design or health, safety and environment (HSE) and fault monitoring and analysis in operations. Cybersecurity should be embedded into renewables activities from design to decommissioning and into contracting with ecosystem partners. Regulations like the NIS directive requires operators to show cyber threat detection and remediation capabilities. However, operators will need to do more than the minimum necessary for compliance and be proactive in creating their own tailored cybersecurity roadmaps. The resiliency of renewables is more important than ever, and cybersecurity is at the core.

HOW ACCENTURE CAN HELP

Accenture brings deep expertise in renewables, IT and OT security, a broad market understanding, and industry knowledge to develop and provide secure solutions.

Highly experienced renewables cybersecurity team

The largest global team of OT and Industry X security professionals in the world. Our team has extensive OT security skills in utilities and renewables, leveraging a unique OT cybersecurity approach, methodology and assets.

Truly global partner

One cohesive team that can scale around the globe as the client requires and confirm consistency in the definition and execution of activities and deliverables across regions.

End-to-end cybersecurity player

More than 20 years of success in serving global organizations to assess, define, deploy, and manage their cybersecurity programs. We have global scalability to support security strategy, cyber defense, digital identity, applications security, and managed security services (MSS).

Cybersecurity technology ecosystem

Strong alliances, partnerships, and joint initiatives with a large pool of security, cloud and technology vendors as well as system integrators and OEMs, while always respecting a vendor-neutral position.

Innovative approach to cybersecurity

Significant, sustained investments in expertise and innovation centers, generating insights and assets to build forward-looking cybersecurity capabilities aligned with business strategy. We also participate in the entities framing and building the cybersecurity regulation space.

For our broader cybersecurity offering, please visit:
https://www.accenture.com/us-en/services/security-index

RENEWABLES CYBER RANGE: TEST, LEARN AND ASSESS IN A SAFE, REALISTIC AND BATTLE-PROVEN SETTING

A cyber range is a physical environment used for cyberwarfare training and cybertechnology development. It provides tools that help strengthen the stability, security and performance of cyber infrastructure and IT/OT systems used by governments and military agencies.

Cyber ranges provide a risk-free security stress-testing facility with much faster threat detection and response. They can help:

- Assimilate new tools without risk.
- Learn in a recognizable, scaled-down environment.
- Orchestrate diverse vendors and tools.
- Learn from external security experts.
- Improve anomaly and endpoint protection.
- Fine-tune event monitoring.
- Fuse intelligence and detection with response and remediation.
- Strengthen credentials management.
- Improve maintenance and upkeep.

Accenture has built a first of its kind renewables cyber range at our Innovation Center in Bilbao, Spain. It models a wide range of renewables infrastructure and processes including wind and solar farms, substations, energy storage, EV charging, office/headquarters simulation and a smart city.

The cyber range is equipped with a complete SCADA system to control the models and it tracks and visualizes all relevant parameters on a dashboard. It also has the leading-edge security architecture and cybersecurity protection systems to be used in stress-testing.

CONTACT

Samuel Linares
Managing Director
Global Industry X.0, Europe Industry X.0 and OT Security Lead

Marco Molinaro
Managing Director,
ICEG Security, Accenture Security

Kris Timmermans
Manager Director,
Europe Renewables Generation Lead
Accenture Strategy and Consulting

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services in strategy and consulting, interactive, technology and operations, with digital capabilities across all of these services. We combine unmatched experience and specialized capabilities across more than 40 industries – powered by the world's largest network of Advanced Technology and Intelligent Operations centers. With 513,000 people serving clients in more than 120 countries, Accenture brings continuous innovation to help clients improve their performance and create lasting value across their enterprises.

REFERENCES

1 REN21 GSR 2020 report - https://www.ren21.net.

2 Ibid.

3 Third Annual State of Cyber Resilience Report for Utilities, Accenture Security, 2020, www.accenture.com.

4 Ibid.

5 Ibid.

6 https://ec.europa.eu.

7 North American Electric Reliability Corporation (NERC), https://www.nerc.com.

8 ISA/IEC 62443, https://www.isa.org.

9 NIST Special Publication, https://nvlpubs.nist.gov.

10 https://www.nist.gov.

11 SO/IEC 27001, https://www.iso.org.

12 Renewable technologies in the EU electricity sector: trends and projections, European Commission, https://ec.europa.eu.