Convergence brings opportunity and risk
Protecting operational technology from cyber-attacks
Utility operators are under greater pressure than ever to protect their systems—both operational technology and information technology, but there is a huge difference when it comes to securing these distinct systems. Attempting to transfer security processes and tooling directly from one side to the other is not a viable approach. This paper examines recent drivers affecting security for utilities and offers a specific approach for addressing OT networks and facilities.
Introduction

Operational technology (OT), the industrial control systems (ICS) that help keep the power on and water and gas flowing, is becoming more prone to cyber-attack. Given that energy and water are essential requirements of society, any potential risk to this critical infrastructure also poses risk to society overall.

As utilities continue to seek greater operational efficiency and effectiveness, they are introducing internet connections to their existing OT networks. This positive convergence will improve performance and streamline ways of working by enabling capabilities such as off-site monitoring and remote maintenance. However, since much OT equipment dates from the 1980s and 1990s, it was developed with little idea it would be part of a connected society and, thus, with little thought to security.

Without careful planning and effective monitoring, exposing thousands of physically distributed OT facilities to information technology (IT) networks is creating serious security challenges for most utilities. Compounding these challenges is the growing number of bad actors prepared to exploit such vulnerabilities to disrupt the lives of citizens. As an example, stolen information and blueprints from nuclear and water companies could be used to cause widespread loss of power, grid tampering and water contamination, jeopardizing entire communities.

Alongside these developments is an increasingly formal regulatory structure for reporting breaches, the advance of the Internet of Things (IoT), and a highly vocal public ready to react when things go wrong.

The upshot is that utility operators are under greater pressure than ever to protect their systems—both OT and IT. But there is a huge difference when it comes to securing these distinct types of systems. Attempting to transfer security processes and tooling directly from the IT side to the OT is not viable.

As broader, more sophisticated cyber-attacks are carried out by a growing set of adversaries, utilities need to fully understand their risks. Since addressing all potential vulnerabilities at once is virtually impossible, mitigation actions must be prioritized based on potential impacts.

This white paper will examine these changes and offer steps senior leaders can take to secure the flow of essential services for their customers, and protect employees and citizens at large.

The current picture

NETWORKS UNDER ATTACK, COMMUNITIES AT RISK

Interconnectivity makes for an extremely vulnerable world, particularly when it comes to OT. As a result, utilities increasingly are turning their attention and resources to securing this domain.

Today’s cyber threats come from multiple sources: the IT hacking community, insiders enabling unauthorized access—both intentional (sabotage) and unintentional (scammed by phishing), and well-coordinated, well-funded groups determined to cause harm to people or property.

The wake-up-and-take-notice cyber event for utilities was the Stuxnet malware attack on Iranian nuclear facilities in 2008. Stuxnet proved that extensive harm was possible. It disrupted one-fifth of Iran’s facilities and is believed by some to have set back the country’s nuclear plans by as much as two years. Since this well-publicized event, other attacks have emerged and become more frequent.

While power companies and even nation states can fall victim to such attacks, the impact on the ordinary citizen can be far-reaching as well.

In 2015, around 230,000 Ukrainian residents suffered a power outage of up to 6 hours when almost 60 substations went offline due to a malware attack. Similar malware was found in the networks of at least two other utilities according to the Reuters news service.

By 2020, spending on OT security will double due to increasing attacks on critical industrial infrastructure and subsequent regulatory responses.

Indeed, such attacks have the potential to pose serious danger to an entire community. In 2016, an attack on a water treatment plant in the Asia-Pacific region enabled infiltrators to access not only the records of up to 2.5 million customers but also the system that controls the chemicals to treat the drinking water. Fortunately, the exposure was discovered and the attack thwarted before any damage could be done.

A HIGHLY TARGETED SECTOR

The energy industry is highly targeted for cyber-attacks. According to a 2016 survey on cybersecurity challenges in the energy industry by Dimensional Research for Tripwire, not only are attacks on the rise, but “energy organizations are experiencing a disproportionately large increase when compared to other industries.”

Even when a utility’s IT network has sophisticated cyber-defense in place, it is not always a given that connections to the OT network have the same rigors applied. The result: the door is left open to malicious elements.

In fact, some malware developers appear to be targeting OT because it never was designed to be protected on the internet.

LEGAL DEVELOPMENTS IN BREACH REPORTING

Regulatory requirements also are posing great challenges to utilities. Seventy percent of utility participants in the CGI Global 1000 outlook rated privacy and data protection laws as having a high or very high impact on their businesses.

Increasingly around the globe, legal frameworks have developed requiring utilities to report breaches and face financial and reputational consequences if they do not.

- In the U.S., the North American Electric Reliability Corporation (NERC) Reliability standards include mandatory critical infrastructure protection (CIP) standards which address the security of cyber assets essential to the reliable operation of the electric grid. CIP-008 ensures the identification, classification, response and reporting of cybersecurity incidents related to Critical Cyber Assets.

- In Canada, The Digital Privacy Act of 2015 created new legal obligations for companies that experience a security breach involving personal information. Further, each province also has privacy legislation, and often a Privacy Commissioner.

- In Europe, the European Network and Information Security Directive (NSID) text reached the final stages of ratification this year, making it mandatory for critical national infrastructure providers to report security breaches. Other nation states still have to ratify the legislation, but it is clear that utilities will be held to account for their security measures. The EU General Data Protection Regulation (GDPR), which requires companies to report breaches of consumer personal data, has been in place in the Netherlands since January 2016. When a recent utility data breach occurred (in the IT domain), GDPR required that it be reported in a timely and accurate way.

4. Personal Information Protection and Electronic Documents Act (PIPEDA)
Drivers of OT and IT network convergence

In the past, OT and IT systems had entirely separate jobs. There was no need to combine these networks because they did not report on the same operations. OT networks also had different priorities and infrastructure than IT. However, the paradigm has changed due to the growing need for data, technology advances, and an evolving regulatory framework.

The utilities industry recognizes the value of OT and IT convergence. Removing silos created by people, systems and data will allow smoother flow of information to support automatic control of the distributed network. Combining OT and IT technologies, along with other enterprise data sources, will enable truly agile and responsive organizations.

Also with convergence, data pulled from different sectors of the OT network could be analyzed in the IT network to help predict peaks and troughs in demand. Where budget pressures have resulted in fewer people onsite to monitor assets, equipment and service, OT connected to IT allows a power plant to be operated using less personnel.

In short, OT and IT convergence provides greater means of improving supply and demand.

EMERGING OT RISKS

Each element added to an OT network creates a new risk that can be exploited, exposing previously hidden infrastructure to potential attack. For example, many utilities are starting to use newer technology that embeds protocols and code to connect to the IT network. This means that an OT network could accidentally expose the system to the internet.

Lack of in-house security skills in operations is another risk. If departments running diesel generators or power plants do not have dedicated security architects because they are focused on operations and not IT, their designers may not be aware of current threats and points of vulnerability, and could be using old protocols or software without encryption.

The Internet of Things (IoT) also introduces new risk points. Monitoring devices, their connections to the cloud, and their access by users all need specific security implementations and to be integrated into a utility’s overall security framework.

In addition, many utilities have introduced mobile working to increase the productivity of onsite engineers. As a result, OT data is now flowing freely through IT and mobile applications and platforms.

In some cases, the required security measures to address these issues are well established, such as for data profiling and user permissions. In others, where legacy devices are being integrated, a careful assessment of risks is needed to ensure previously unconnected elements are made secure.

It is important to recognize that while breaches to IT systems raise financial and reputational risk, OT system breaches represent safety and operational risk.

Project SHINE (SHodan INtelligence Extraction) uncovered that over 1 million SCADA/ICS systems are connected to the internet with unique IPs, and this figure is growing by between 2000 and 8000 a day.

Utilities’ current state of preparedness

How prepared are utilities when it comes to mitigating security threats? The CGI Global 1000 outlook⁶, insights drawn from 1,000 in-person interviews with business and IT leaders, found that while most utility respondents said they are moderately prepared for cybersecurity threats, only 9% feel highly prepared. Many are falling short of the advanced capabilities needed to address rapidly emerging threats.

There is no question that utilities are under immense pressure, with numerous priorities competing for limited budgets. These priorities include regulatory compliance, aging workforce and infrastructure, pressure to become more customer-centric digital organizations, and, in Europe particularly, increased competition.

Utility responses in the CGI Global 1000 outlook indicated that keeping up with relentless risk and compliance requirements was the top barrier to evolving and investing in their cyber programs. Additionally, 67% said that initiatives related to digital transformation compete with budget for security programs.

“The worst case scenario is a critical infrastructure attack, and these organizations are ill prepared to deal with it.”

Dr. Larry Ponemon, founder of the Ponemon Institute

---

⁶ CGI Global 1000 outlook brings together the insights and CGI’s point of view on the strategic topics that emerged through face-to-face interviews conducted by CGI consultants with more than 1,000 business and IT leaders across 10 industries and 20 countries between January and April 2016.
Recommended actions

So what can utilities do to improve their OT and IT security postures? Utilities may be exceeding what’s required from a compliance perspective, but must do more to ensure cybersecurity is “baked in” to everything they do. A fragmented, business-as-usual approach no longer is viable, particularly for mission-critical systems. The high level of preparedness required to mitigate both internal and external threats requires a more holistic approach across the dimensions of people, process, technology and governance.

PEOPLE

1. Develop a culture of vigilance

Nobody is better placed to disrupt a utility than someone in the plant. In fact, most breaches come from inside an organization, so people who work onsite are the most important factor to consider when stepping up security measures. Gaps in security can be closed by ensuring all employees are vetted and their management access is controlled—particularly access to the business information model or any technical drawings of the plant. This level of supervision should extend beyond employees to those with occasional access to the premises, such as contractors or externally employed staff. Guests also need to be closely monitored as should any repairs to machinery performed by outsiders.

The mindset also needs to change. To mitigate insider threats, all employees need to view seemingly normal, everyday actions of employees through an insider threat lens. For example, when a staff member is found accessing a control system they would not normally access, it should be acceptable to ask what they are doing, and why.

Strict identity and access management protocols are needed to ensure employees can only access the information and physical sites required to do carry out their responsibilities.

This awareness must be embedded in company culture.

2. Improve education

While shoring up this first line of defense is an imperative, 68% of utilities in the CGI Global 1000 outlook said that providing effective security training is a challenge. Employee education must focus on safety and security, as well as the tradeoffs involved: All employees making safety and security decisions need to understand where OT meets IT, and what actions are needed at that intersection. For employees authorized to access OT and IT data remotely, or use field devices, thorough security training is needed to reduce the likelihood of an inside breach. These employees may not fully comprehend the consequences of adding a new Wi-Fi printer or creating a link from one system to another to get a seemingly non-critical piece of data for reporting, for example. Often, since they are not security practitioners, they do not understand that every door opened must be fully protected.

OT security must be integrated into existing safety programs to protect against a breach that can have a safety impact—for example, a USB stick carried by an employee could be accessed to trip the plant or throw off the electricity grid.

Nearly 40% of OT and IT executives in the CGI Global 1000 outlook indicated they struggle with how to effectively communicate to their top management and boards of directors the urgency related to rising threats. Both leaders and workers should be made aware of the threats to OT security and the risk of making connections between OT and the business network. While it can be a challenge to keep security “top of mind” for executives and employees, senior IT leaders need to continue to push the subject through information sharing and ongoing training across all levels of the organization.

PROCESS

1. Make a clear distinction between IT security and OT security, with safety paramount

When IT security is applied to the OT environment, accidents and safety issues are sure to happen. For example, an IT-driven decision could require that a door be left closed for confidentiality purposes, but an OT-driven decision would ensure that people are able to flee in an emergency. Trying to enforce IT security guidelines in the OT environment also is not viable. This is because the same measures and controls cannot be implemented, processes cannot be run and the vocabulary used by those who support these environments is not aligned.

This is because of the IT factors of confidentiality, integrity and availability (CIA) are inverted in the OT environment to availability, integrity and confidentiality (AIC). Utilities must place front and center the prioritization factors of the ISA/IEC 62443 Series of Standards on Industrial Automation and Control Systems (IACS) Security. The plant or energy transport network is concerned
with availability—“Can we control the physical process that produces or transports power and water, or generates power?” Even in manufacturing (e.g., steel production), while the process itself is of course a trade secret, the safety of the plant is more important.

2. Eliminate points of vulnerability

Utilities also need to ensure there is sufficient segregation between technologies and non-authorized users to guarantee security. Processes must control any flow of information, whether automated or manual. So whether a system needs a staff member to log on and upload data, or this is done automatically, each stage of the process must be fully documented. When maintenance is carried out, there should be an agreed timeline for access to the OT system, terminated automatically at the time agreed. This avoids a situation where a maintenance worker opens access to sensitive information by failing to reset a system correctly.

TECHNOLOGY

1. Prepare for the worst case

A proactive approach using threat intelligence will provide insight into the latest breaches that have occurred in the utilities sector or an adjacent sector, to help prepare for a similar threat. If one utility reports their control systems were attacked causing service downtime, other utilities should take precautions against a similar event happening to their own systems and test the updates against similar conditions. Security teams also should participate in threat intelligence consortia to understand changing threats specific to their industry, and integrate their own analytics with cross-industry data. This sharing enables proactive threat landscape assessments, monitoring, proactive response, and focused incident management-based solutions.

2. Create redundancy

Utilities are faced with unique security challenges. It simply is not possible to shut down OT completely for maintenance or software updates and patches, as is the case in an IT-only environment. Since the flow cannot be interrupted, a solution must be designed to contain the threat and hold it at bay until complete action can be taken. Systems can be designed with redundancy in mind, where each critical component has a redundant counterpart that can be taken off-line for updates, without shutting down service. This can also be achieved by swapping between redundant networks to keep the water or electricity flowing while devices are patched, and then swapping back afterwards.

3. Establish priorities

Utilities should identify the biggest risk for their primary process (e.g., power production, gas transport, water treatment and transport) and ensure security and safety personnel are on the same page and using the same vocabulary. Use of IEC-62264 and 62443 can help. They also need to identify which elements are linked to the most valuable assets and which are the most vulnerable, and then place more importance on securing those using segmentation. A multi-level approach to securing OT and IT can achieve the strongest defense. For example, at the lower end of the security stack, the focus might be on proper encryption and monitoring for abnormalities. Going up the stack, the priority might be connectivity, ensuring communications are properly encrypted and diagnostics updates are made. For cloud security, it could mean ensuring the right kind of enterprise grade security systems are in place. And with IoT, using a “start small and scale up” approach based on established IT security architectures may be in order. This provides the foundation on which to progress to increasingly complex business-critical solutions by adding new protocols and methodologies without undermining established security principles.

4. Monitor and test

In terms of spotting threats and preventing attacks, both OT and business systems need monitoring based on parameters for what is considered normal behavior. If those parameters start to be exceeded, even slightly, investigations are needed. Industrial control systems can identify an anomaly that strays from everyday behavior and send an alert to be actioned. For instance, if a remote terminal suddenly starts communicating with a device in a different substation, or the level of data being generated by an electronic device suddenly peaks, this should raise questions such as, “Has this situation arisen because someone has hacked into the system or is there a fault in the OT environment?” Continuous testing should also be part of the program. Responsibility for ensuring the security framework is tested regularly against different scenarios is another important role of the governance team. These tests should be conducted in an open, blame-free environment, where the focus is on “How can we improve?” and not “Who is at fault?” Lessons should be learned from every exercise conducted and
shared across different departments and, if relevant, with other utilities so collective knowledge can be built.

GOVERNANCE

1. Get the right people involved

In reviewing cybersecurity policies and processes, it is important to recognize that the OT network cannot be viewed in isolation, but rather must be viewed alongside the IT network. An engineer’s tablet or data link for a management information system could easily be what creates an opening for a bad actor, rather than an electronic device designed to monitor the OT network itself.

For this reason, the responsibility for cybersecurity cannot rest in OT or IT. It needs board-level support and then each stakeholder needs representation on the governance team. Stakeholders should include the OT and IT leads, of course, and may also include human resources, legal, commercial divisions and supply chain teams, to ensure an “it’s everyone’s responsibility” culture is developed to prevent breaches.

To be confident that good governance is in place, utilities should be able to answer the question, “Who owns cybersecurity in this department, and do they have the authority required to act quickly when an issue is identified?”

2. Determine what is OT and what is IT

As the possibilities of IoT blur the line between OT and IT, it is critical to view all systems handling real-time data and sending out signals to customers or field equipment through “OT eyes,” asking questions such as, “Will this system impact the physical process we run?” and, “What would happen if the system fails or makes an error?” This input should guide utilities in designing or redesigning and protecting the systems from intentional and unintentional compromises.
Conclusion

While utilities have numerous priorities competing for transformation budgets and attention, there is no greater risk to a utility and to citizens than a malicious and wide-spread cyber-attack. The solution is complex, and calls for a clear understanding of the risks that go hand in hand with converging OT and IT. It requires cultural and behavioral change as well as improved control and monitoring of operations. Only a holistic approach across people, process, technology and governance can provide the best defense against cyber breaches, to ensure essential services continue to flow, and employees and communities are kept safe.
About CGI

Founded in 1976, CGI is one of the largest IT and business process services providers in the world, delivering high-quality business consulting, systems integration and managed services. With a deep commitment to providing innovative services and solutions, CGI has an industry-leading track record of delivering 95% of projects on time and within budget, aligning our teams with clients’ business strategies to achieve top-to-bottom line results.

CGI and Utilities: CGI offers services and solutions across the utilities industry, including the electricity, downstream natural gas, and water and waste sectors. We have deep experience in both regulated and unregulated markets and have formed long-term client relationships with the world’s largest utilities. We partner with them to deliver innovative technologies that meet current and future requirements and help ensure long-term growth and success.

CGI and Cybersecurity: At CGI, security is part of everything we do. We take a business-focused approach at every level, from audit and compliance to policy and architecture. Our end-to-end offerings include consulting and training, integration and implementation and managed security services. Through our global network of Security Operations Centers, we have a 360-degree view of threats across sectors and geographies. Our security services teams continuously identify and deploy advanced solutions to maintain state-of-the-art infrastructure. Our global experience helps us predict and defend against new attacks, and our front-line capabilities reflect this knowledge.

Visit cgi.com or contact us at info@cgi.com for more information.

© 2016 CGI GROUP INC.