Cyber Security

Electrical power transmission and distribution grids are controlled using the information that is constantly hauled to and from the many power lines, substations and national and regional control centres to efficiently deliver electric power to consumers.

The management of this information takes place through data collected and transmitted via a traditional Time Division Multiplex (TDM) telecommunications network or a modern Internet Protocol Network (IP). Alternatively, a combination of TDM and IP networks that are layered on top of the power network often referred to as the nerve system of the electricity grid.

SMARTENING THE GRID OPENS THE NETWORK TO CYBER ATTACKS

However, with the advent of smartening the grid's nerve system, many automation and power control systems have been integrated into the energy network and therefore those aspects relating to cyber security and information sharing need to be taken into consideration.

There are several matters that need to be addressed in the area of cyber security, especially with major initiatives in South Africa and across the globe moving towards cleaner energy sources. Renewable energy resources are on the whole owned and/or operated by Independent Power Producers that connect to the national grid, thereby increasing the possibility of cyber related risks.

Cyber Infrastructure refers to ICT systems and services, consisting of all hardware and software, that process, store, and communicate information, or any combination of all of these elements. The development of smart grids replacing the conventional power grids is envisioned as being a great step moving towards cleaner energy sources. Smart grids use an intelligent two-way digital communication for monitoring and controlling the devices.

The smart grids therefore will play an important role in responding to many conditions in supply and smart energy demand and can save governments billions of dollars over the next 20 years.

SECURITY-CONSCIOUS RELATIONSHIPS

The ICT systems allow utilities to remotely control and monitor power generation devices and substations over phone lines, radio links and, IP networks.

During the rollout of Smart Grids it is very important to articulate mutual expectations and responsibilities for managing the security risks that arise when:

- Sharing information and resources among acquirers and suppliers: people, services, infrastructures, information, and facilities;
- Integrating information and communication technology (ICT) components provided by suppliers into existing infrastructures depending on products that will be operational for years to come; and
- The increased use of outsourced services, such as public telecom operators and cloud services.

Integrating security considerations into supplier relationships is a joint responsibility for acquirers and suppliers. It is critical that utilities organise their own processes and activities in such way that they are conducive to building productive and security-conscious relationships with suppliers.

The UTC acknowledges that many of the practices addressed here already exist in numerous acquirer and supplier organisations. However, these practices may not have been the subject of discussion among acquirers and suppliers in the utility sector. UTC therefore proposes ten basic practices that will help utilities begin to organise relationships with their suppliers in a productive way.

The ten basic practices are based on global and industry-based standards and best practices:

1. **Identify critical assets, systems, and processes, and prioritise them:** Due to resource constraints, it is impossible to protect everything equally, therefore start by making choices on which assets are most critical and which suppliers support these critical assets. This will offer a clear understanding of the security risks associated with those supplier relationships.

2. **Identify critical data/information about your business and customers:** The utility and supplier should discuss what data will be shared, and decide what is necessary to be shared and how this data should be protected. Data examples include customer records, electricity or water usage data, engineering drawings and network configurations, wiring maps, lists of executives and their salaries, security vulnerabilities, and numerous other types of business-specific information. The party that receives such data has a responsibility to protect it from unauthorised access and release, both intentional and unintentional.

3. **Identify your suppliers:** Suppliers need to be identified in the supply chain. Depending on the criticality of the asset/supplier and the level of integration between utility and supplier staff and systems, utilities can ask these suppliers to identify their primary sub-suppliers. If that is not practical, utilities can ask their suppliers to ascertain or demonstrate that they have a robust supplier management program themselves and that they are managing supply chain risks as required. This can include explicit processes to purchase parts from authorised resellers, having standardised contractual language that addresses security risks, and propagating those security requirements down the supply chain.

Considerations for Power Networks

4. **Assess supplier risk and prioritise suppliers:**
   Below are the criteria that you should consider when assessing risks that are associated with your suppliers. At a minimum, utilities should look at the following:
   - Are your and your suppliers' systems accessing each other?
   - Do your suppliers' employees have access to your facilities and systems?
   - How long do you expect this relationship to last (one-time, short-term, mid-term, long term)?
   - How important/critical is the function/system/capability provided by the supplier to you?

5. **Establish general security requirements by priority:**
   Security requirements provide a language for utilities to communicate their expectations to suppliers. The level of rigour in these requirements should depend on the criticality of suppliers to the utilities' operations. These should be high-level requirements that articulate the outcome rather than specific ways to do things or specific technologies. Getting into too much detail may limit innovation and potentially security. What if a supplier has a better way of getting to the acquirer's desired outcome than the way the acquirer specifies?

6. **Establish how you will want to share information with suppliers on vulnerabilities and incidents:**
   Incidents happen in even the best-managed environments. Developing vulnerability-free code, for example, is impossible, so vulnerabilities will be discovered after installation in the acquirer's environment. When an event happens, how will the utility and supplier communicate with each other and with the outside world? Whose responsibility will it be to address the problem? How will the two parties continue after the problem is addressed? Discussion about common communication strategies and shared responsibilities in addressing incidents and vulnerabilities is critical.

7. **Establish how you will want to monitor supplier adherence to requirements:**
   The work you have just completed to figure out what is important and to develop security requirements for that set of important assets and relationships will not be productive unless the results are monitored. However, this monitoring cannot be decided in a vacuum. While utilities may want to ask all kinds of questions and see all kinds of information, they need to be productive and efficient in their monitoring approaches. Utilities will need to figure out how they would like to monitor whether their suppliers are implementing the security as defined, discuss those methods with suppliers, and negotiate a monitoring approach that makes sense for both organisations.

8. **Ensure your employees have the relevant information and are kept up to speed:**
   Lots of people touch products and services as they traverse an enterprise throughout the lifecycle of a supplier relationship. The roles of these people span the entire lifecycle of the acquired (or supplied) product and service and include acquisition/procurement, legal, information technology, supply chain, engineering, software and system development, delivery, shipping and receiving, human resources, information/cyber security, physical security, network operations, facilities, and potentially many others. All these people need to understand their role in managing security risks associated with supplier relationships.

9. **Make arrangements for contingencies:**
   The life of a system does not end when it goes into production. Generally, utilities keep their Operations Technology systems for a long time, a lot longer than IT systems. Suppliers who put those systems together may experience changes during the system's lifetime that will impact the utility who had acquired that system. Supplier eventualities need to be evaluated and mitigations for the associated risks should be developed.

10. **Conclude supplier relationships in a risk-conscious manner:**
    Lastly, supplier relationships sometimes end and utilities need to protect their operations, systems, and information in the process of terminating such relationships. The extent of what needs to be done depends on the same risk factors as assessing potential risks associated with supplier relationships. These eventualities need to be identified and dealt with as early as during the procurement process. ESI

African Utilities Telecom Council (AUTC) is a regular feature in ESI Africa, delivering information for the utilities and private sector on telecommunication challenges and solutions.

ABOUT THE AUTHORS:

Corrie Vermeulen is the Director for AUTC. He has a National Diploma and GCC in Electrical Engineering, and an Executive Management Certificate from the University of Cape Town. He has more than 30 years' utility experience in Electrical Engineering that includes Protection Systems and Telecommunications Networks and spent most of his career with Eskom.

Nadya Bartol is Vice President of Industry Affairs and Cybersecurity Stategies at UTC. She leads UTC cyber security innitiatives world-wide driving strategic solutions to long term utility cyber security challenges including workforce development, utility modernization and IT/OT convergence.