OPERATIONAL TECHNOLOGIES

Cybersecurity

As utilities continue to modernize their critical infrastructure, related OT networks are becoming ever-more connected to IT, increasing the potential for security breaches. PSC offers a variety of cybersecurity services to help increase your network's resilience and to achieve full compliance with cybersecurity regulations.

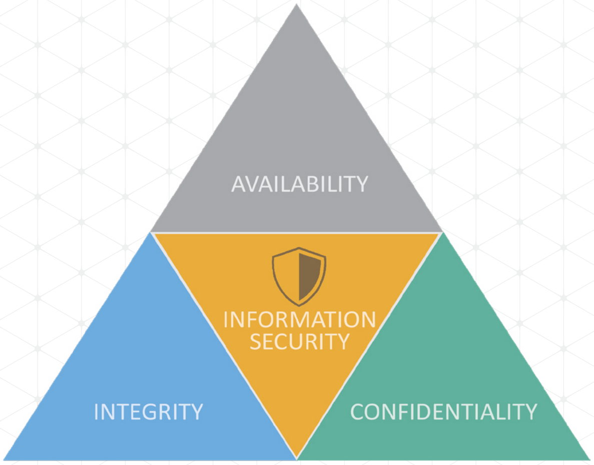
Cybersecurity - information security and operational security - ensures the integrity, confidentiality, and availability of digital systems. This is achieved by evolving risk management approaches, appropriate security governance, mitigation technologies and best practice IT/OT processes that are designed to protect systems and information from disruption, damage and unauthorized access.

Overview

PSC's global specialists understand the electric utility and energy markets businesses, and the technical challenges utilities face in securing their digital assets. We combine our in-house IT security expertise with our deep electricity utility OT domain experience to help our clients minimize their risk. Simply put, our experts help utilities assess their vulnerabilities and threats and implement solutions that improve cybersecurity, while complying with all regulatory standards.

PSC can help preserve the confidentiality, integrity and availability of utilities' mission-critical networks by bringing lessons learned from cybersecurity projects around the world. Our experts can assist in developing business cases and recommendations; evaluating and procuring new cybersecurity solutions; and implementing and supporting cybersecurity projects.

We are vendor-neutral and independent; our sole focus is providing recommendations and services that best meet our clients' individual needs.



Cybersecurity aims to preserve the confidentiality, integrity and availability of computer systems and is the cornerstone of all cybersecurity endeavors, referred to as the CIA Triad

Security management

- Assessing the overall cybersecurity function or practice and making recommendations for improvements
- Assessing existing cybersecurity governance structures and recommending improvements
- Assessing software and infrastructure for security risks and recommending and implementing enhancements
- Defining requirements for security improvement and mitigation
- Define high-level and detailed security specifications either to be implemented as stand-alone systems or as intricately integrated parts of bigger solutions
- Developing project budgets and timelines for system upgrades
- The build, test and implementation of security systems and mechanisms to reduce and mitigate cybersecurity risk
- Conducting regular system tests and ensuring continuous monitoring of network and systems security
- Ensuring all personnel that have access to the system are limited by need and role
- The development of IT / OT business resiliency plans i.e. both business continuity and disaster recovery planning related to business-critical systems
- Promptly responding to all security incidents and providing thorough post-event analyses and recommendations for both administrative and logical improvements
- Ultimately taking responsibility for improving client's overall security and resilience postures

Risk management

- Regulation and compliance
- Quantitative risk analysis and mitigation
- Governance
- Technical controls
- Policy, Guidelines, Standards

Asset security

- Identifying ownership
- Classifying and Labeling
- Threat Modeling
- Asset control - Identify and Access Management

Security design

- Enterprise Security Architecture and Solutions Architecture
- Pervasive Security – Monolithic infrastructure redesign to defend in depth
- Zone design
- Countermeasure design
- Continuity planning and disaster recovery

Security implementation and operations

- Security Orchestration
- Setup and manage Information Security Management System (ISMS)
- Implement and operate cybersecurity tools and technologies
- Security Incident and Event Management
- Automated vulnerability testing

PSC projects

The following selection provides a sample of Cybersecurity projects completed by PSC.

SCADA Security Review
PSC assisted in the review and gap analysis of a client's SCADA environment based on the ISO27001 and NIST frameworks. This work has resulted in a plan that addressed the critical areas in the strategy of their SCADA environment.

Substation Firewall Design and Selection Tests
Being vendor-neutral and experienced in control systems network security design and implementation, PSC provided advice in the selection of three candidate firewalls to be used in a substation environment. Using firewall and security device test methodology, based on industry standards, a fit-for-purpose firewall was selected and integrated into the Substation Security design.

Control Network Infrastructure and Security Review
PSC performed a network review based on the client's security policy and industry standards, including NIST publications, ANSI ISA99, and IEC 27000 series. Recommendations and options for remediation were also provided.

SCADA Remote Access Design
PSC delivered a secure design for remote access for a customer in its Water and Sewerage SCADA system. The proposed fit-for-purpose solution met the customer's security policy requirements, budget and was in line with security best practices.

SCADA Network Upgrade
PSC delivered a network design and implementation for an upgrade of a SCADA network consisting of three control sites. The design incorporated best practices in SCADA high availability, security and performance features for a highly resilient network. This includes QoS and service definitions, LAN and WAN security safeguards, path protection and physical redundancies.

SCADA Perimeter Security Design & Implementation
PSC designed and implemented a perimeter security solution for a SCADA network. The design involved Checkpoint firewalls and RSA 2-factor authentication.

SCADA Virtualization Design, Australia
PSC designed and implemented a VMware vSphere solution for a Transmission Utility for its SCADA environment. The solution included a highly available iSCSI SAN, sized according to the client requirements.

SCADA Security Review
PSC assisted in a security review and the approach taken was to standardize with a focus on critical infrastructure. PSC performed the network review based on the client's security policy and industry standards and security frameworks, including ISO 27001:2013, NIST publications, ANSI/ISA-62443, Australian DSD and TISN recommendations.

Network and Security Enhancements
PSC developed the design and implementation of network and security enhancements for the utility. The design takes the approach of defence-in-depth and consistency with control systems security best practices. The layers of defence include the optimal placement of suitable security controls, with the need of balance between ease of operation, which affects availability, confidentiality and integrity.

Security Monitoring Solution
PSC delivered a security monitoring design for a Utility based on the defence-in-depth approach. A combination of technologies were used to gain better visibility of the network - providing both the bird's eye view and the detailed level view on-demand. This approach has reduced the effort required to monitor and respond to security events on the network, delivering operational cost efficiency.

Substation Security Architecture
PSC delivered a substation security architecture based on the client requirements, standards and frameworks including NIST 800-82, ISO 27000 series, and ISA99. Included in the architecture were the classification of substations according to their risk profiles, and recommendations of appropriate security controls and security technologies to be applied.

Control Systems Data Storage Review
PSC reviewed the existing data handling procedures and technology that were in place for a Utility in Australia. Based on the client's disaster recovery requirements, the RTO (Recovery Time Objectives), RPO (Recovery Point Objective), data compliance retention requirements and on-site data gathering, PSC identified areas for improvement and recommended changes to the processes and tools used for data storage backup efficiency and confidence in data protection.

PSC

Specialist Consultants
to the Electricity Industry
pscconsulting.com

New Zealand	Australia	North America	Europe	Asia
Wellington	Fortitude Valley, QLD	Kirkland, WA	Warwick, UK	Singapore
+64 4 232 7680	+61 1300 933 632	+1 425 822 8489	+44 1926 675 851	+65 (800) 616 3283

CONTACT US