In the wrong hands it's an open invitation

Life Is On Schneider Electric

If someone takes over your control system infrastructure it could prove fatal

Control systems are indispensable for a number of industrial processes and are lucrative targets for intruders, criminal groups, foreign intelligence, phishers, spammers, hactivists or terrorists.

Cyber-incidents affecting these control systems can have disastrous effects, not only on your operations, but also on a country's economy and on people's lives. Cyber-intrusions can cause power outages, paralyze transport systems and trigger ecological catastrophes.

The implications of cybersecurity and the need for a comprehensive security strategy is now being acknowledged by more sectors and is now very much part of standard operational risk management.

Without the right protection your secrets can be seen by anyone

In our modern, interconnected world, cyber-attacks are never far from the headlines as organizations report a surge in incidents with criminals and state actors seeking to steal commercial secrets on an unprecedented scale.

In 2015 a significant proportion of computer and organizational security professionals believed unintentional insider threat (UIT) to be the greatest cost to their enterprise[1]. More than 95% reported that these breaches involved operator errors[2].

With over 50% of organizations reporting that they have encountered an insider cyberattack[3], 43% of all data loss can be attributed to internal actors[4].

Intellectual property can represent years of effort and millions of dollars worth of investment, which can be stolen in the blink of an eye with litigation unlikely to fully restore the pre-attack position.

Businesses need to ensure that their intellectual property is appropriately protected to minimize its vulnerability and protect its future.

[1] www.securonix.com/insider-attacks-were-the-most-costly-breaches-of-2015
[2] www.virtru.com/blog/insider-threats-in-cyber-security
[3] www.computerworld.com/article/2691620/security0/insider-threats-how-they-affect-us-companies
[4] www.infosecurity-magazine.com/news/insider-threats-reponsible-for-43

Reduce the threats of a cyber-attack on your operations

The Schneider Electric™ Cybersecurity Services Team recommends a “Defense-in-Depth” approach to cybersecurity for our customers. Defense-in-Depth is a hybrid, multi-layered security strategy that provides holistic security throughout an industrial enterprise and is expected to become a security standard in factories of the future.

We do this by implementing our Cybersecurity Portfolio Lifecycle Methodology which is designed to support your business sustainability efforts and provide peace of mind across your entire operations.

Privacy and Data Security

Facility Security

Operational Safety

Cybersecurity Portfolio Lifecycle Methodology in Brief

Cybersecurity should be an on-going process. By adopting the lifecycle methodology, our Cybersecurity Services Team[5] ensures your proposed solution is network, control, and safety system agnostic and matches your business’ requirements appropriately.

1 Assess	We review the current network and system architectures, policy, procedure, and related compliance documentation as well as risk and threat reports to identify any potential problems or issues, and then recommend areas for improvement.	**Services:** Site and System Assessments, Policy and Procedure Assessments, Industry Compliance Assessments, Independent Verification and Validation, Gap Analysis, Risk / Threat Assessment, Protection / Security Assurance Level Formation, and Cybersecurity Program Development
2 Design	Using the various assessment and / or project planning documentation from Stage 1 as a guideline, we will identify documentation and solutions that should be created and / or implemented. An overall site and system architecture design will be developed that details all the necessary components required to satisfy the standards set by the customer and/or industry.	**Services:** Site and System Security Design, Security Policy Creation, Security Process and Procedure Creation, Virtual Control Effectiveness Validation, and Compliance Evaluation Criteria Establishment
3 Implement	Using the architecture and design documentation, our team will begin the process of implementing your upgraded cybersecurity solution from procurement and staging to system commissioning and end-user training.	**Services:** Hardware / Software Procurement, As–Designed Network and System Security Installation, Configuration, Hardening, Integration with Existing Business Processes and Applications, and Knowledge Transfer of Solutions
4 Maintain	Our Cybersecurity Services Team works closely with your designated security team to ensure proper solution management is understood. We also help to provide a mechanism by which continuous improvement and optimization are taking place that are adaptive to the ever-changing cybersecurity threat landscape.	**Services:** Periodic Security Patching, Solution Maintenance and Upgrades, Cybersecurity Lifecycle Roadmap Evaluations, Cybersecurity Awareness and Solution Training, Compliance and Control Effectiveness Assessments, Incident Response Exercises, Security Assurance Level Documentation, and Penetration Testing

[5] The Cybersecurity Services Team can ensure the proposed solution matches customers’ requirements appropriately as long as: a) All four of the services set out above are purchased from Schneider Electric; and b) The various procedures set out by the Cybersecurity Services Team are followed accordingly.

The exponential increase in cyber-threat levels

Over the last decade, the rise in cyber-attacks on critical infrastructure has resulted in cybersecurity becoming a central concern amongst industrial automation and control system users and vendors. These strategic attacks are aimed at disrupting industrial activity for monetary, competitive, political or social gain, or even as a result of a personal grievance.

Nuclear

Discovered in 2010, the Stuxnet virus remains one of the largest and most "successful" industrial attacks in cyber-history.

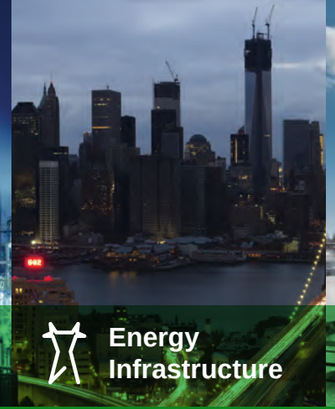
The Stuxnet worm targeted the PLC systems in Iran's nuclear program, causing centrifuges to spin out of control without triggering alarms.

Before it was caught, the attack was able to destroy up to 1/5 of the country's nuclear centrifuges and set its nuclear program back a decade.

Oil & Gas

In August 2012, a coordinated "spear-phishing" attack targeted the computer network of Saudi Arabia's state-owned oil firm, Aramco.

The attack infected as many as 30,000 computers and took two full weeks to beat, but it failed to completely shut down the flow of oil, which appears to have been its goal.



Energy Infrastructure

One of the biggest electrical blackouts in history, the 2003 First Energy blow out that left eight states in the dark for days may have been the result what is described as an "accidental cyber-attack."

A malicious worm designed to attack Windows and Unix systems of private users infected the system monitoring the grid.

Water & Wastewater

Hackers were able to change the levels of chemicals used to treat tap water at a water treatment plant. The attack focused on the outdated IT network of the plant, exploiting its web-accessible payments system and using it to access the company's web server.

Telecoms

A UK telecoms group's computer system was hacked in October 2015 in what was originally feared to be a mass raid on customers' personal data.

While not as successful as first believed, the attack lost the company 101,000 customers, suffering costs of £60m as a result.

Mining, Minerals & Metals

The hack of one of Canada's largest mining companies saw 14.8GB of uncompressed data from internal networks posted online. The leaked data included employee login IDs and passwords, salary and budget documents, and other sensitive corporate and personal information about the company and its employees.

Contact us today to learn more.

Schneider Electric Systems Inc.

Dubai
E Wing, Level 4, Silicon Oasis Headquarters,
P.O. Box 341057, Dubai,
United Arab Emirates
+971 4 7099333

Houston
10900 Equity Dr,
Houston, TX 77041,
United States
1-877-342-5173

Montréal
4 Rue Lake,
Dollard-des-Ormeaux,
QC H9B 3H9 Canada
1-800-565-6699

cybersecurity-services@schneider-electric.com

schneider-electric.com/process-automation

Life Is On | Schneider Electric