FROST & SULLIVAN

Cybersecurity for Industrial Automation & Control Environments

Protection and Prevention Strategies in the Face of Growing Threats

A Frost & Sullivan White Paper in Partnership with Schneider Electric

Prepared by Ivan Fernandez, Industry Director, Industry Practice

Table of Contents

The Paper was completed in April 2013.

Executive Summary

The **proliferation of cyber threats** [1] has prompted asset owners in industrial environments to search for security solutions that can protect their assets and prevent potentially significant monetary loss and brand erosion.

While some industries have made progress in minimizing the risk of cyber attacks, the **barriers to improving cybersecurity remain high**. More **open and collaborative networks** have made systems more vulnerable to attack. **End user awareness** and appreciation of the level of risk is inadequate across most industries outside critical infrastructure environments. The **uncertainty in the regulatory landscape** also remains a significant restraint. With the **increased use of commercial off-the-shelf IT solutions** in industrial environments, control system availability is vulnerable to malware targeted at commercial systems. **Inadequate expertise in industrial IT networks** is a sector-wide challenge.

Against this background, organizations need to partner with a solutions provider who understands the unique characteristics of the industrial environment and is committed to security. One such solutions provider, **Schneider Electric** helps its customers adopt the multi-layered **Defense-in-Depth approach** through a holistic, step-by-step plan to mitigate risk. This includes **improved security features** on current and upcoming solutions, the use of the **Automation Systems Manager** (ASM) to monitor, manage and protect assets, and a **comprehensive suite of services** to support customers. With this expertise from Schneider Electric, a trusted global solutions provider, organizations can move from reactive and adhoc responses, to a proactive, planned and holistic approach to security.

---

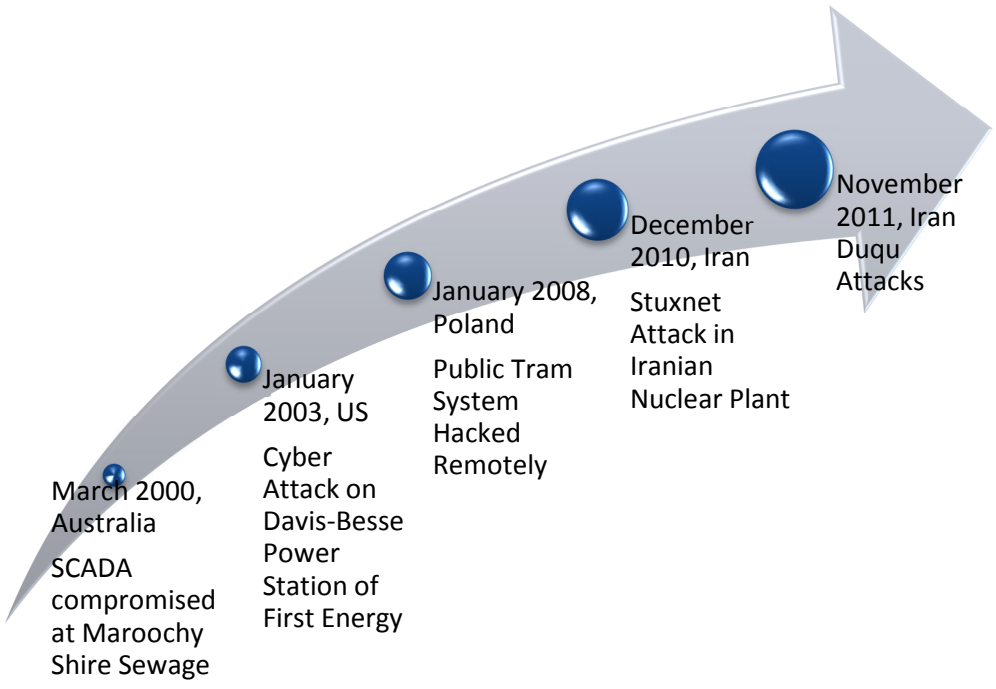
[3] Cyber threats are broadly defined as intentional or unintentional acts that compromise or disrupt computers and/or networks.

The Exponential Increase in Cyber Threat Levels

Over the last decade, the rise in cyber attacks on critical infrastructure has resulted in cyber security 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[2] or social gain, or even as a result of a personal grievance.

Cyber threats are primarily aimed at industrial control systems such as distributed control systems (DCS), programmable logic controllers (PLC), supervisory control and data acquisition (SCADA) systems and human machine interfaces (HMI) through loopholes which can range from unsecured remote access, to inadequate firewalls, to a lack of network segmentation.

Such threats are not a new phenomenon. However, a spate of high-profile attacks over the last decade has brought this issue to centre stage.



The Stuxnet worm gained global attention in December 2010, when an Iranian nuclear plant was sabotaged and the plant's operation was compromised.

There have been numerous theories about this high-profile attack, with industry and media circles providing multiple viewpoints.

While the Stuxnet story might still be subject to popular debate, its impact on the domain of industrial cyber security has been unprecedented.

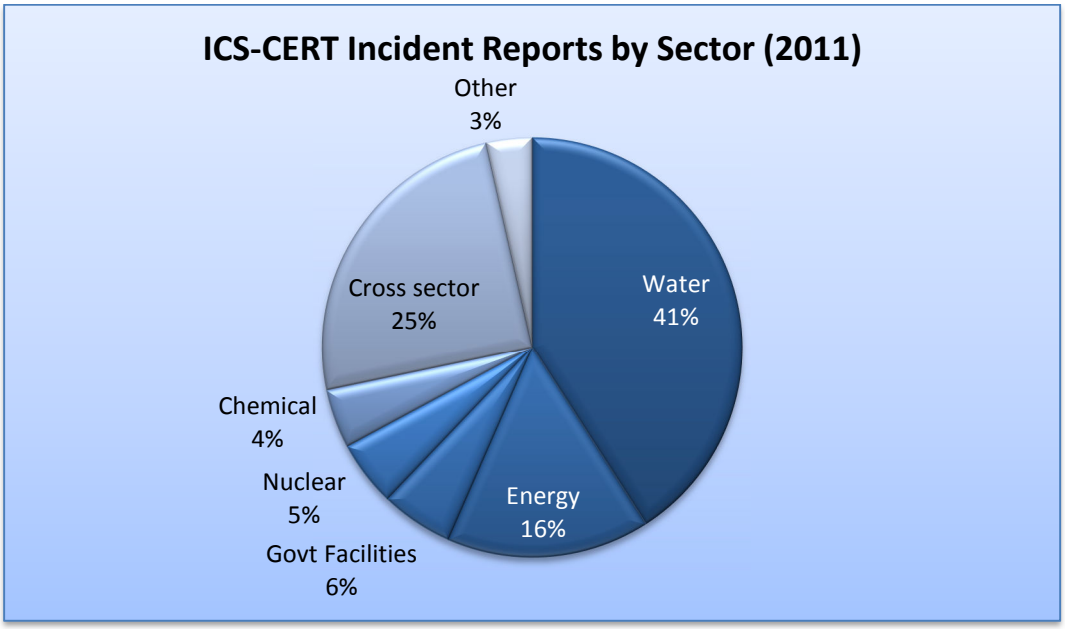
[4] Some politically-driven cyber attacks are the result of hactivism; illegal cyber intrusions as a means of political protest.

Source: Frost & Sullivan

om 2006 to 2012, the number of cyber security incidents reported by federal agencies to the U.S. Computer Emergency Readiness Team (CERT) has increased by 782%[3]. For a variety of reasons, many attacks remain unreported[4]; thus implying that the scale of the problem is larger than evident from reported statistics.

From 2006 to 2012, the number of cyber security incidents reported by federal agencies to the U.S. Computer Emergency Readiness Team (CERT) has increased by 782%.

In 2011, Industrial Control Systems CERT (ICS-CERT) registered 198 reported incidents, with the sector split as shown in the exhibit below:

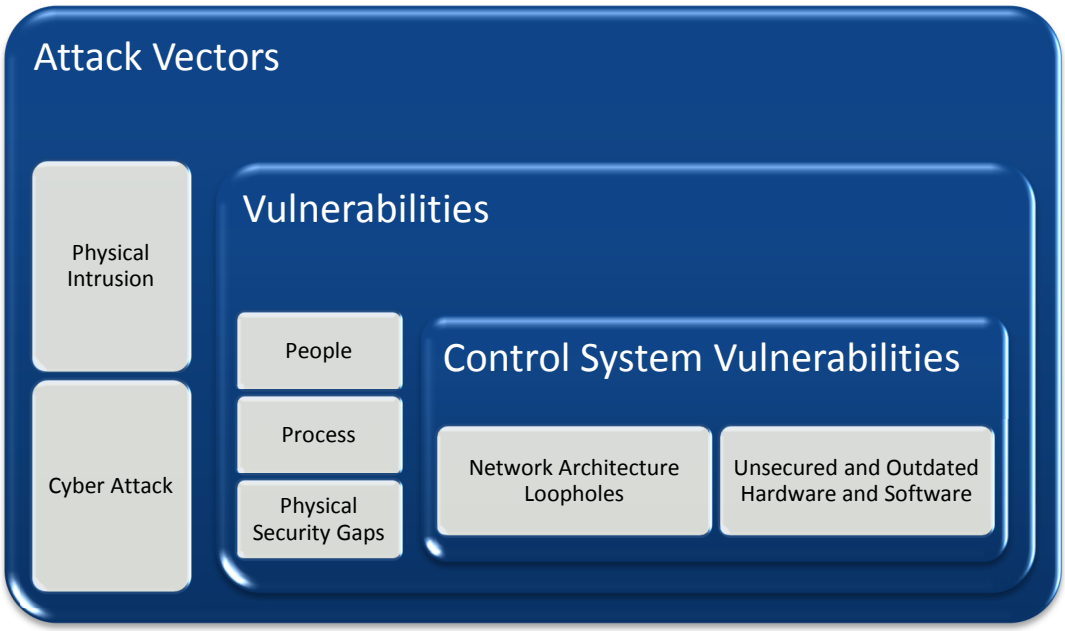


Source: ICS-CERT

[5] US Government Accountability Office, *"Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented",* February 2013

Reasons for not reporting a cyber attack could be fear of negative publicity or penalty for non-compliance, uncertainty about what could actually be done post-incident or even the uncertainty over whether the attackers could be located and brought to justice.

While motivations for intentional attacks vary, the key attack vectors for any cyber threat are typically as follows:



Source: Frost & Sullivan

Physical intrusion or a **cyber attack** is typically driven by economic, competitive, political or social agendas. These are obviously beyond the control of the enterprise seeking to protect itself. However, some aspects that are generally well within the control of an organization, are often overlooked, such as people, process and physical vulnerabilities .

In terms of a site's **physical security**; unsecured gates and inadquate physical access control are obvious, but common gaps.

People or human factors could include a number of factors such as designer/installer error in configuring/installing the system, operator error in running processes and systems, inadequacy of maintainance and upgrade plans, inadequate skill levels etc. However, errors and accidents are not the only internal threat sources from a human factor perspective. Malicious attacks from internal sources are also a possibility, especially from disgruntled employees or contractors. It must also be noted that human factors do not only imply individual-specific risks. An overall **process** culture that does

Malicious attacks from internal sources are also a possibility to be reckoned with; especially from disgruntled employees or contractors.

not understand or appreciate the key risks, that does not manage operations in a secure manner (including basic password management or changeover management). Or an environment that does not audit and enforce consistently and effectively, and that underutilizes available supervision and detection tools, exposes itself to an unacceptable level of risk. In such a process culture, the priorities of the IT department and industrial control department are often not aligned.

In terms of control system vulnerabilities, **network** loopholes[5] can range from unsecured remote access to inadequate firewalls to lack of network segmentation, while **hardware and software** issues could include unsecured remote terminal units (RTUs), PCs, USBs, mobile devices, peripherals and specific HMI, as well as all manner of control software.

A cyber attack can result in significant monetary loss through production / process downtime or disruption, damage to equipment and infrastructure, as well as potential non-compliance with regulation that can result in large penalties. It can also result in brand erosion, loss of confidential/proprietary information and quality compromises. In fact, in the near future, implementation of security strategies in factories and all critical infrastructure sites[6] will become mandatory for regulatory compliance. Despite the emergence of integrated product-specific safety features, an industrial network strategy will be necessary to address the challenges posed by cyber threats in coming years.

Implementation of security strategies in factories and all critical infrastructure sites will become mandatory for regulatory compliance. An industrial network strategy will be necessary to address the challenges posed by cyber threats in the coming years.

Minimizing Risk: The Industry's Response

Some industries have been more proactive than others in minimizing the risk of cyber attacks. Most end users have taken a few obvious steps in plugging certain gaps. For example, according to the Repository for Industrial Security Incidents (RISI) database,

---

[7] Given the flat structure of organizations today, loopholes in the corporate IT networks could also result in compromising the industrial control system.

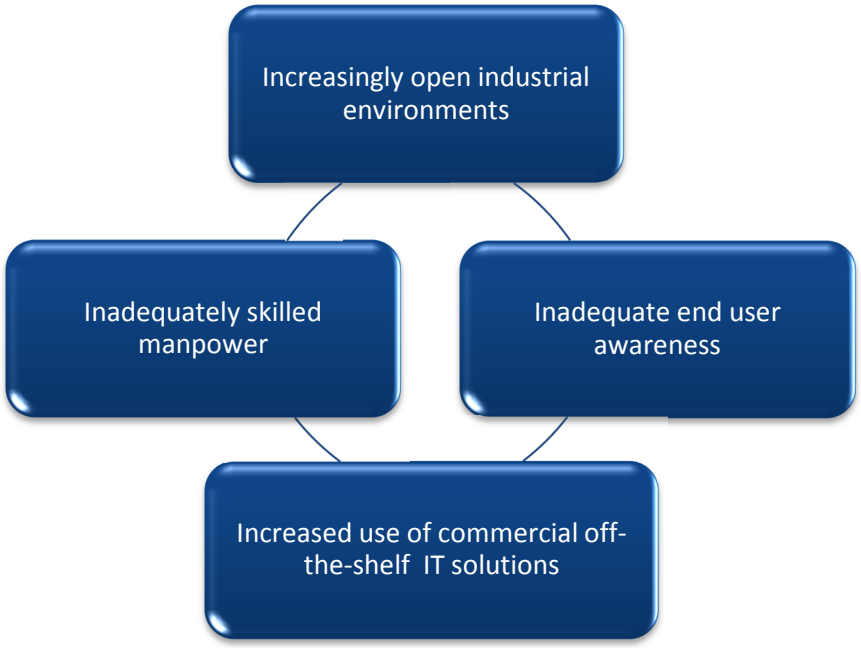
For example, the North American bulk power sector is now required to comply with Critical Infrastructure Protection (CIP) standards relating to cyber security - North American Electric Reliability Corporation (NERC) Standards CIP-002-3 through CIP-009-3 - Critical Cyber Asset Identification

more than 60% of facilities had implemented patch and anti-malware management programs in 2011[7]. However, the significant change to identify and eliminate the biggest vulnerabilities involves a higher level of engagement that few organizations have initiated. This is because there are various hurdles to implementing cyber security initiatives.

Although open and collaborative systems have raised productivity and profitability, they have also made the system more vulnerable to attack.

Barriers to Improving Cyber Security

The exhibit below lists the key barriers to improving cyber security in industrial environments:



Increasingly open and collaborative nature of industrial environments: In the past, industrial networks were primarily isolated systems, running proprietary control protocols, using specialized hardware and software. However, industrial architecture has transformed over time, with collaborative mechanisms that involve internal and

[8] Repository for Industrial Security Incidents (RISI), "*Annual Report on Cyber Security Incidents and Trends Affecting Industrial Control Systems",* 2011

external integration. Senior management now requires real-time data access for analysis, decision-making and reporting. Therefore, the degree of isolation of industrial control systems has decreased significantly over the last few decades as the use of IP-based, wireless and mobile devices in industrial environments has increased. In addition, legacy control systems were not designed to contend with current threat levels. Although open and collaborative systems have raised productivity and profitability, they have also made systems more vulnerable to attack. According to the RISI database, approximately 35% of industrial control system security incidents in 2011 were initiated through remote access[8]. This is not surprising when another finding from the same report indicates that close to 65% of facilities allow remote access to their control systems.

According to the RISI database, approximately 35% of industrial control system security incidents in 2011 were initiated through remote access.

Inadequate end user awareness and end user inertia: End users in certain industries (notably in critical infrastructure environments such as power, oil & gas, water & wastewater and nuclear facilities) show a high level of awareness and appreciation of the need for a comprehensive security strategy. They tend to have detailed cyber security plans and procedures in place. Their concern is real. Their investment of time and capital in protecting their assets is considerable.

However, many end users in other industries (including manufacturing) are either unaware of the risk of cyber attacks or reluctant to implement security strategies in their enterprises, as investments in cyber security do not appear to have a tangible return-on-investment (ROI). This leads to a complacent 'wait and watch' approach that only mandatory regulation or the unfortunate instance of a cyber attack may change. Given the uncertainty of the regulatory landscape today, this mindset may persist. Another reason for low uptake of security planning and implementation amongst some industries is the fact that the task appears too daunting and sizable; analysis does not lead to action and the vision of a total system overhaul remains just that – a vision. Finally, in the customized control environment of an industrial site, it is difficult to predict how a newly introduced patch will impact the functioning of the control system;

---

[9] Repository for Industrial Security Incidents (RISI), *"Annual Report on Cyber Security Incidents and Trends Affecting Industrial Control Systems"*, 2011

especially if the patch is not tested rigorously. This increases the organization's reluctance to act on potential threats.

Increased use of commercial off-the-shelf IT solutions in industrial environments: While the gradual shift toward IT-based solutions in the industrial space was made for commercial benefits, ease-of-operability and integration, it has also resulted in control systems having to face increased exposure to malware and security threats that are targeted at commercial systems. This increases the risk to control system availability.

Inadequate skilled manpower: While the industrial sector prides itself on a highly skilled workforce focused on automation systems, such product-specific expertise does not always translate into adequate expertise in industrial IT networks. This gap weakens an organization's ability to develop comprehensive protection and prevention strategies.

Partnering with the Right Solutions Provider

To help address these barriers, organizations would be best served by partnering with solutions providers who understand the unique characteristics of the industrial environment and are committed to security. One such end-to-end solutions provider, Schneider Electric is seeking to 'build in' security for its new solutions and services across the entire lifecycle, as well as improve security capabilities in existing solutions.

Given the complex nature of the challenge, Schneider Electric is approaching the problem from different angles:

The Defense-in-Depth Approach

Schneider Electric recommends a Defense-in-Depth[9] approach to cyber security for its 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.

Schneider Electric, with operations in over 100 countries, offers integrated solutions across multiple industries, with the focus on making energy safe, reliable, efficient, productive and green.

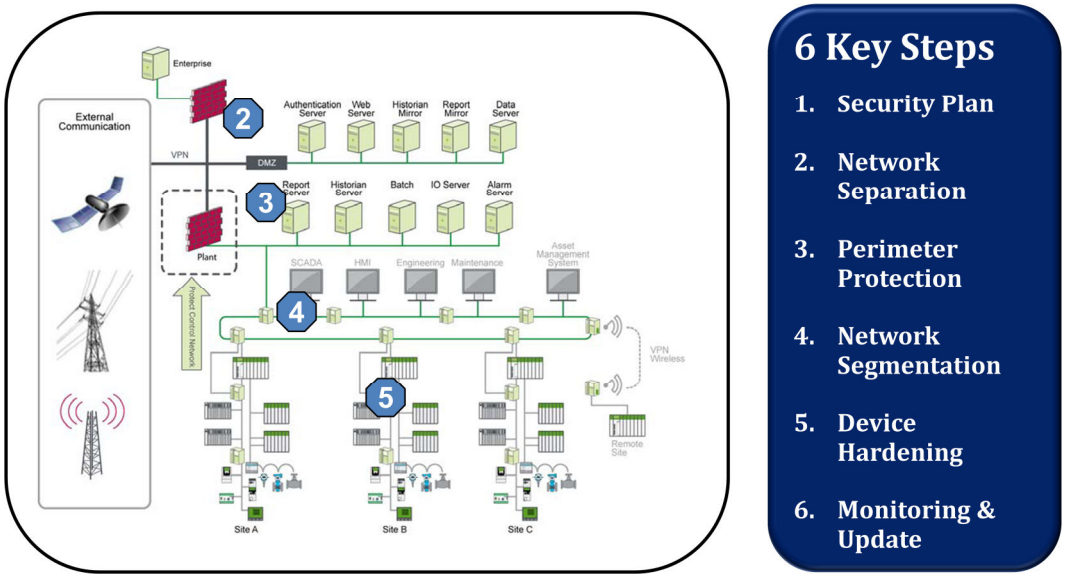
www.schneider-electric.com

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.

---

[10] Originally a military strategy, Defense-in-Depth was developed by the U.S. Department of Defense's National Security Agency (NSA).

The Defense-in-Depth Approach in the Industrial Environment



6 Key Steps

1. **Security Plan**
2. **Network Separation**
3. **Perimeter Protection**
4. **Network Segmentation**
5. **Device Hardening**
6. **Monitoring & Update**

Source: Schneider Electric

The 6 key steps used in the Defense-in-Depth approach are:

Security Plan: Policies and procedures that cover risk assessment, risk mitigation and methods to recover from disaster.

Network Separation: Separating the industrial automation and control system from other networks by creating demilitarized zones (DMZ) to protect the industrial system from enterprise network requests and messages.

Perimeter Protection: Firewalls, authentication, authorizations, VPN (IPsec) and anti-virus software to prevent unauthorized access.

Network Segmentation: Containment of a potential security breach to only the affected segment by using switches and VLANs to divide the network into sub-networks and by restricting traffic between segments. This helps contain malware impact to one network segment; thus limiting damage to the entire network.

Device Hardening: Password management, user profile definition and deactivation of unused services to strengthen security on devices.

Monitoring & Update: Surveillance of operator activity and network communications. Regular updates of software and firmware.

While the Defense-in-Depth approach encourages the creation and implementation of a comprehensive plan, a common misconception amongst organizations is that this equates to an “all-or-nothing” approach. This is where Schneider Electric’s step-by-step approach can help clarify what could be the ideal way forward for organizations.

Implementing a Step-wise Plan

According to the Pareto Principle, approximately 80% of impacts arise from 20% of causes. Recognizing that the reason for inaction can sometimes be the sheer enormity of the task, Schneider Electric’s recommendation to clients is generally to adopt a step-by-step plan. This means:

1. Identifying the biggest impact to the organization in terms of a security breach
2. Zoning in on which specific area of plant operations is linked to that impact
3. Outlining what the biggest vulnerabilities are in relation to that area of operation
4. Minimizing or eliminating those vulnerabilities

Once complete, the organization can move on to the next impact-area-vulnerability issue. Rather than revamping an entire system at once and falling victim to "analysis paralysis", a focused step-by-step approach not only ensures that the significant changes with the highest impact are effected immediately, but also the organization does not spread itself too thin and therefore, realizes the best value for dollars invested.

However, a step-at-a-time tactic should not tempt organizations into losing sight of the ‘big picture’. This is where security beyond the cyber threat needs to be considered as well.

Security; not just Cybersecurity

Best practice cybersecurity planning, in effect, addresses total security requirements in a unified manner; not just that of cyber security. With Schneider Electric’s

Best practice cyber security planning, in effect, addresses total security requirements in a unified manner; not just that of cyber security.

comprehensive suite of industrial control solutions (from I/O level through to PLCs, SCADA and enterprise level solutions such as Ampla), building access control, data center solutions, electrical distribution products, as well as security systems (including video surveillance, access control, fire & life safety and intrusion detection systems), organizations are reassured that any plan to mitigate vulnerability will be holistic. This is possible not only because of the diverse offerings available, but also because a single view of total operations is made possible.

Through the strategic partnership with industrial security software solutions provider, Industrial Defender, Schneider Electric now offers Industrial Defender's unified platform for security, compliance and change management.

Strategic Partner – Industrial Defender

Through the strategic partnership with industrial security software solutions provider, Industrial Defender, Schneider Electric now offers their unified platform for security, compliance and change management. This enables Schneider Electric's customers to monitor, manage and protect their assets through a suite of software solutions that form the Automation Systems Manager (ASM) platform.

Organizations will now be able to identify changes to the system, who made them and why. The whitelisting[10] option, which allows only approved applications to run on the system, ensures that potential threats are blocked. The generation of periodic reports helps improve the efficiency of compliance reporting.

Beyond the use of such a security platform, organizations also need to consider security-specific capability improvements in their actual control system software and hardware.

Cybersecurity Enablers

In terms of specific cybersecurity enablers, Schneider Electric's offer includes:

- ConneXium Industrial Firewalls for improved control network perimeter security
- ConneXium Tofino Firewall to secure communication zones within the control network

---

[13] NERC CIP specifically includes whitelisting solutions as a method to prevent malicious code. Also, Whitelisting has been ranked the number 1 strategy to mitigate targeted cyber intrusions by the Australian Defence Signals Directorate (DSD (Australian Department of Defence, Oct 2012)

- Core offerings such as PACs, SCADA, HMI devices, and Ethernet modules hardened with password protection, access control, and the ability to turn off unneeded / unused services.

These features apart, added assurance comes when all offerings are brought to the appropriate level of relevant security standards.

Standards

Since most industrial environments work on hardware and software from a number of vendors, security is an industry-wide challenge; requiring some level of consensus across suppliers and service providers in relation to terminology, documentation and definitions around what is 'compliant'.

While there is currently no industry-wide standard for industrial security, one that is likely to become the default standard is IEC 62443.

While there is currently no industry-wide standard for industrial security, one that is likely to become the default standard is IEC 62443[11]. Schneider Electric is working to ensure that all legacy and new products are brought to the appropriate IEC 62443 level. Schneider Electric is also an accredited test center for Achilles[12] robustness certification.

Software and hardware aside, customers are also looking for consistent support across the entire lifecycle.

Services

Since desired security outcomes are a moving target, Schneider Electric recognizes the criticality of a comprehensive suite of services for organizations seeking to improve their preparedness. These include:

---

[14] International Electrotechnical Commission (IEC) Standard for Industrial Communication Networks - Network and system security.

Achilles certifications from software solutions provider, Wurldtech, are internationally recognized, independent, best practice certifications for the secure development of applications, devices and systems found in critical infrastructure.

- **Assessment and Design** services that help clients identify biggest risks, areas to focus on to mitigate the biggest risks and security hardware, software and network design elements that will be required to improve the system.
- Ongoing support in **monitoring, managing and protecting** the system so that issues are contained, the appropriate personnel are notified of incidents, updates and information on new patches are passed on regularly to registered customers via the web portal, etc.
- **Recommendations** in the form of Tested Validated Documented Architecture (TVDA[13]) which helps clients apply the Defense-in-Depth approach across their systems.

With this suite of services, customers can address total cost of ownership concerns with greater confidence.

Being energy-solutions-focused helps Schneider Electric to apply its site-wide diagnostics capabilities to ensure security outcomes are met without slowing operations or impacting profitability.

Total Cost of Ownership focus

Being energy-solutions-focused helps Schneider Electric to apply its site-wide diagnostics capabilities to ensure security outcomes are met without slowing operations or impacting profitability. The suite of automated tools and reports and managed services can help organizations reach their energy efficiency goals in a more secure and reliable manner. This is enabled by higher system reliability and availability, as well as the ability that the organization then has to better leverage internal resources for other core functions.

Secure Development Lifecycle

To help deliver all of these benefits to clients, Schneider Electric is internally implementing a secure development lifecycle for its products. This approach involves:

- Identifying what security features are needed in each product
- Threat modelling and risk analysis

---

[15] The TVDA based on Schneider Electric's PlantStruxure solution acts as a reliable guide to system integrators and project engineers during design and implementation of a project.

- Attack surface reduction (securing software by reducing potential access to unvalidated users and providing a 'turn-off option for services not frequently used)
- Secure coding (that seeks to eliminate coding defects)
- Inhouse testing of security features
- Independent testing of penetration risk
- Strengthening documentation of security-related data for customers (including recommendations for how products can be best installed and the security profile of products)
- Outlining the appropriate incident response steps for customers

Conclusion

The implications of cyber security and the need for a comprehensive security strategy are now being acknowledged by more sections of the industry. This is because the increased number of cyber attacks and the potential disruption they can cause have made security risks now very much part of operational risk. However, apart from uncertainty in the regulatory landscape, the main roadblock is the lack of a clear management policy on cybersecurity within organizations. One reason that is used to explain this gap is the perception of low ROI on cybersecurity investments. However, it is becoming clearer that as cyber threats become more sophisticated, the impact of a cyber attack can be catastrophic for organizations, governments and the public. Potential monetary losses for industry are considerable. In the case of critical infrastructure, non-compliance (with increasingly stringent regulation on security) is unlikely to remain an option.

In this context, organizations will be able to make the successful shift toward securing their operations by relying on industrial control solutions providers that treat security as core to their offerings. Of course, it is vital that organizations realize that this is a joint process where vendors and clients need to work together to achieve agreed objectives. That is why one of the critical success factors in raising the bar for cybersecurity in an

Organizations will be able to make the successful shift toward securing their operations by relying on industrial control solutions providers that treat security as core to their offerings.

organization is the level of trust it has in its solutions provider. After all, security is never a one-time project and the process of learning and adapting is ongoing.

However, once the need is acknowledged, an actionable plan is required to identify the biggest impact to the organization in terms of a security breach, locating which specific area of plant operations is linked to that impact, and minimizing or eliminating the main vulnerabilities related to that operation. This process can then help kickstart the much wider review of operations towards implementing a holistic Defense-in-Depth approach to cybersecurity.