WALLIX
CYBERSECURITY SIMPLIFIED

Securing Industry 4.0

The Convergence of IT and OT

Securing Industry 4.0

The Convergence of IT and OT

TABLE OF CONTENTS

INTRODUCTION 2
THE CONVERGENCE OF IT AND OT 5
ICS & SCADA 5
COMPLIANCE 7
CONTROLLING ACCESS 9
CONCLUSION 10

The world is more connected than ever. With the rise of increasingly sophisticated technologies, we are entering what many are hailing as the 'Fourth Industrial Revolution' – Industry 4.0. Manufacturing, Utilities, Energy and even Transportation are all being transformed by the increased connectivity this new age has to offer.

However, along with the vast benefits to be enjoyed from a truly connected world, there is also a rising tide of security threats which, if not properly addressed, could spell disaster, not just for industry, but for civilization at large. It is now widely accepted that the wars of the future will take place less on the battlefield, and more in cyberspace.

Instances of nation-state attacks have already been reported. Likewise, criminal attacks by individuals and small groups also take place on a regular basis. Events such as the 2017 WannaCry ransomware attack, the 2016 attacks on US water utilities, and the 2015 attack on Ukraine's power grid clearly highlight the impact that cyber incidents can have. It's safe to say that it's only a matter of time before an even larger-scale attack is attempted. Are we ready?

CONSEQUENCES OF DIGITAL INSECURITY

Every organization, of any size or shape, is under constant threat of attack. And the ramifications can be highly damaging even to the smallest of businesses. For example, a breach in data security can put an organization at significant legal risk. Where the organization is found to be failing to meet compliance requirements, beyond penalizing fines there is even risk to the business itself, whose license to operate can be revoked in severe cases, and individuals responsible for the breach facing jail time.

For the industrial sector (i.e. manufacturing, utilities, energy, and transportation), breaches can also result in physical harm, either to employees injured by a malfunctioning production line or to the public put at risk by system outages. As the Industrial Internet of Things (IIoT) expands, industrial equipment is increasingly connected to digital systems and needs to be protected from new digital threats.

Without proper security in place, there is potential for such equipment to be manipulated by hackers and terrorists, or simply left exposed by negligence. This can result in anything from breakage (costly) to explosions (deadly), and much in between.

Disruption to energy networks, the delivery of utilities such as gas and water, and to transportation networks, can threaten the safety of the public. Without utilities, without electricity, individuals become susceptible to crime, cold, drought and accidents. In the event of an attack on transport networks, threat to life from accidents, collisions or power surges are a real possibility.

So what can we learn from failures of the past? How can this inform our approach in the present and build a safe and sustainable industrial infrastructure for the connected future?

“Without proper security in place, there is potential for such equipment to be manipulated by hackers and terrorists, or simply left exposed by negligence.”

The Convergence of IT and OT: The Industrial Internet of Things (IIoT)

While IT (Information Technology) comprises the use of software, networking devices and, of course, computers to process, store, secure, and share electronic data, OT (Operational Technology) monitors events, devices and processes in manufacturing and industrial environments.

OT	IT
Closed Environment	Open Environment
Rare updates & replacements	Regular updates
Limited patching	Frequent patching, as needed
Physical systems	Digital by nature

In the past, OT took place within a closed environment, completely separated from the IT department.

With the advent of new levels of connectivity, digital has come to the realms of OT, bringing it together with IT into a symbiotic relationship: connecting the physical with the digital.

Connected tools now allow OT functions to be scrutinized and operational performance quantified with more accuracy and regular attention than before. Big data and analytics mean that performance and events can be monitored carefully, in real-time, remotely. Operations can be optimized with precision, costs of production reduced, and third-party service providers can be enlisted to build on efficiency, productivity and performance across the organization.

Clearly, the convergence of IT and OT has introduced a great range of benefits across all industries that it has touched. But as with most big developments, these benefits have come at a price.

Poorly secured OT can provide an all-too convenient entry point for threats to infiltrate the network, giving potential attackers free reign over highly-sensitive assets (both physical and digital).

ICS & SCADA

Industrial Control Systems and SCADA have been in use for years now, pre-dating the new hyper-connected era in which we find ourselves today. Industrial systems, particularly those in fields delivering essential services, are high-profile targets for cyberattack, a fact that has gone unacknowledged for too long. Indeed, the issue of cybersecurity for these systems has only come to greater attention after they have already been connected, and even threatened.

The fact is that both SCADA and ICS remain vulnerable, with a number of security challenges to be addressed as a matter of urgency. ICS and SCADA face particular vulnerabilities, many of which can be eased with robust solutions including Privileged Access Management (PAM) while ensuring Industry 4.0 organizations meet increasingly stringent compliance requirements.

ICS: Industrial Control Systems

Industrial Control Systems are used to operate or automate industrial processes, comprising devices, software and networks working in tandem.

In the earlier days of large industrial plants, control panels were localized to each process. People were required to man each of these panels, and there was no way to view how the process was performing, certainly not within the context of the plant overall. To solve this, all plant measurements were transmitted to a central control room, from which each process could be monitored and assessed. Eventually, controller-based algorithms were developed, leading to what we now know as 'distributed control systems' (DCS).

ICS have been designed to operate similarly to other mechanical systems within the plant, being easy to use, configure and manage and to last years without any major modifications. They were also isolated from other elements of the corporate infrastructure (i.e. IT systems).

Over time, processes became increasingly centralized and automated, and until fairly recently, 'air locks' were considered a sufficient barrier against attacks. Disconnecting ICS from the business network prevented attackers from reaching it. However, this is no longer feasible in the connected era of the IoT.

Major ICS vulnerabilities are identified every year. In fact, many of these vulnerabilities may have existed for years without having been detected. This is partially due to ICS engineers' reluctance to prioritize security over network stability, as the patching and replacement of legacy systems and controllers often necessitates disruption and downtime. Considering the potential ramifications of a breach caused by vulnerable ICS, this is particularly problematic.

SCADA: Supervisory Control and Data Acquisition

Developed as a means of providing remote universal access to OT systems, SCADA systems are a kind of central nervous system for industrial plants. Supervisory computers and sensors from PLCs (Programmable Logic Controllers) and RTUs (Remote Terminal Units) feed data back to the SCADA system which monitors and controls the processes of these devices, visualizing behavior and performance for human attention.

Because SCADA systems have been essentially 'air-locked' from the outside world for so long, with hardware (i.e. RTUs and PLCs) communicating with the system independently from any external internet connection, little attention has been paid to ensuring their security. SCADA systems are now perhaps the most widely used types of ICS, and are consequently perhaps more vulnerable to cyber-attack than other connected devices and systems, as a result of their need for security being overlooked for so long.

As these traditionally isolated systems have become connected and IP-enabled, risk exposure has increased dramatically. Potential attackers can target the PLCs and RTUs, as well as the SCADA system itself. Back in 2010, the discovery of the Stuxnet worm targeting PLCs in an Iranian nuclear facility made it very clear that securing industrial networks now includes paying close attention to those devices that were once considered invulnerable. In order to secure SCADA systems, it is now highly recommended that stringent access management systems are put in place to avoid potentially deadly attacks.

The Consequences of Weak Security

A weak security system puts organizations, workers and the general public at risk from a number of angles. These dangers can include physical risk to life and health, ramifications that transcend the organization itself.

Employees can be put in immediate danger in the event of a malign attack on the physical infrastructure of the organization (e.g. on the production line) by a cybersecurity breach that infiltrates the RTUs or PLCs. Malfunctioning machinery and disrupted processes can be extremely hazardous, with explosions, power surges and sudden changes in machine activity among the many dangers such a breach may cause.

One of the biggest potential results of a cyber breach is a full production shutdown. One of the many ways that attackers seek to hurt an organization, a severe breach can cause serious disruption and may result in production shutdown if not caught in time. Not only is this financially detrimental, but can have major reputational and public safety consequences as well. Disruption to rail networks and traffic signals can cause damage to normal functioning of integral aspects of our built environment, as well as physical risk. A power grid shutdown, for example – such as the infamous attack in the Ukraine in 2015 – can have extreme impacts. Without gas, electricity or water, the consequences could be fatal.

For the organization itself, the financial cost of a cyber breach or attack is just the tip of the iceberg. Data leaks are hugely disruptive, and put the organization under great pressure from additional repercussions:

- Scrutiny for failing to meet compliance requirements
- Loss of reputation from exposing customer data
- Lost business
- Potential lawsuits and legal action

Whether from consumers or regulatory bodies, the legal fallout of a serious incident is likely to be crippling from both a financial and reputational perspective, with everything from firings and jail time for responsible individuals to sanctions or ultimate closing of the organization itself.

Compliance

Whether from consumers or regulatory bodies, the legal fallout of a serious incident is likely to be crippling from both a financial and reputational perspective, with everything from firings and jail

time for responsible individuals to sanctions or ultimate closing of the organization itself.

NIS Directive

The EU's NIS Directive aims to raise levels of security and resilience of network and information systems, and applies to both operators of essential services (OES) such as energy and transportation organizations and digital service operators (DSO).

To ensure compliance, organizations implicated in the Directive must

- Define a reliable and consistent security policy
- Implement robust security measures to protect IT systems
- Monitor, audit and report on security measures
- Comply with international standards & regulations

The NIS Directive therefore covers a broad scope in order to ensure a 360° approach to security, accounting for prevention and reactivity in the face of detecting and managing security incidents.

GDPR (General Data Protection Regulations)

GDPR addresses the security of and incidents related to personal data of European citizens and how it is processed, covering both digital and 'manual' data. Any organization, regardless of industry, which handles the personal data of private individuals in the EU must comply with GDPR.

Some key points to ensure GDPR compliance:

- Apply data protection by design/default
- Identify any potential 'gaps' in security and take adequate steps to correct them
- Conduct a thorough data inventory and audit of data flow (including access management)

Failure to comply with GDPR may result in a fine of up to 4% of a company's annual turnover. It's also worth noting that the potential legal ramifications of breaching the integrity of personal data, not to mention PR disasters leading to loss of business and thus further financial impact.

NERC: North American Electric Reliability Corporation

The mission of NERC is "to assure the effective and efficient reduction of risks to the reliability and security of the grid". Covering the protection of critical cyber assets and security management, as well as disaster recovery planning, all bulk power system owners and operators are required to comply with NERC-approved Reliability Standards.

Requirements for NERC CIP compliance:

- Identification of critical assets and regular performance of asset risk analysis
- Definition and implementation of policies regarding monitoring and changing of critical asset configuration
- Definition and implementation of asset access management policies
- Deployment of systems for monitoring security events

- Comprehensive contingency plans for cyber attacks and other unplanned events

NIST Cybersecurity Framework

Endorsed by the US government, NIST produces standards and guidelines to assist industrial corporations and organizations in meeting best practice data security protocols. It is closely aligned with compliance for other regulatory bodies, including HIPAA, FISMA and SOX.

The NIST Framework outlines the major themes of security procedure:

- Identify organizational vulnerabilities and security risk
- Protect critical infrastructure with appropriate security measures and tools
- Detect incidents quickly and uncover all relevant information
- Respond rapidly to ensure quick containment of an incident
- Recover and return to normal operations as quickly as possible

Ultimately, what these regulations – among many others – have in common is an insistence upon control over who has access to critical systems, when, and how they are permitted to use them. Equally, they hold organizations accountable for tracing all actions that take place and maintaining visibility on each user. The bottom line is that all regulatory bodies recommend, whether overtly or through suggestion, that all organizations operate with an effective PAM system in place.

Controlling Access

An organization that takes active control over access to systems, networks and processes significantly reduces ICS vulnerabilities, thus securing its assets and ensuring that it is fully compliant with all laws and regulations.

In order to comply with all regulations and guidelines and to secure your organization, managing who has access to which parts of the network should be considered a priority. While most attention is paid to the threat of attacks from outside sources, it is equally as important to secure the organization from the inside. External attackers can piggyback on credentials from those within the organization to execute their attack, a move that can be avoided, or at least mitigated, by having proper access management in place. Likewise, increasing reports of insider attacks highlight the need to minimize access to the least privilege principle.

- **Access Control** - Streamline all administrative access – granting and revoking privileges – through a single console. Limit a user's access to only those resources necessary to do his or her job, as and when needed

- **Session Monitoring** - All activity in privileged user sessions is monitored and can be audited for review and compliance. Automatically identify, alert, and terminate suspicious actions on sensitive resources.

- **Password Management** - Eliminate the need for shared passwords and enforce credential complexity. All access is routed through the Bastion, and passwords rotate to ensure complete security.

Conclusion

In a world where connectivity across devices and systems is now ubiquitous, the necessity for organizations to arm themselves adequately against the growing tide of cyber threats is absolutely crucial. As the use of IoT grows across the industrial sector, the pressing need to secure all operational collateral, both physical and digital, cannot be underestimated.

Privileged Access Management plays a central role in securing these systems. Without effective controls over access to critical systems and data, the dangers to organizational performance, compliance, profitability and reputation are immense. Furthermore, any breach that threatens the safety of workers and the general public is inexcusable. It is time we took the security of Industry 4.0 seriously. There is too much at stake not to.

WALLIX Bastion's Privileged Access Management (PAM) solution can deftly handle the largest and most complex network infrastructures, connecting digital and legacy systems to secure the most important services upon which our world relies. To find out more about how we can help to optimize your organization's security, get in touch with WALLIX today.

about WALLIX

WALLIX Group is a cybersecurity software vendor dedicated to defending and fostering organizations' success and renown against the cyberthreats they are facing. For over a decade, WALLIX has strived to protect companies, public organizations, as well as service providers' most critical IT and strategic assets against data breaches, making it the European expert in Privileged Access Management.

WWW.WALLIX.COM

WALLIX
CYBERSECURITY SIMPLIFIED