Security in a Converging IT/OT World

Introduction

Around the winter solstice, darkness comes early to the citizens of Ukraine. On December 23, 2015, it came a little earlier than normal. In mid-afternoon, a worker at a Ukraine power plant sat in disbelief as an invisible outside force took control of his computer and began to shut off power to a vast part of the country, putting nearly a quarter of a million people in the dark and without heat...in the dead of winter.[1]

This high-profile case of cyber crime against critical infrastructure illustrates an important point. As more industrial machines and assets connect to the Industrial Internet to benefit from greater efficiencies and lower costs, it increases the risk of cyber attack.

Not surprisingly, a SANS Institute survey revealed that two-thirds (66.7%) of respondents believe that threats to the security of control systems are severe/critical or high. Another 2016 global research study showed that IT security was the top investment by leaders from industrial organizations. However, security for industrial control systems (ICS) was on the bottom of the list.[2]

52% of the respondents expect a cyber attack on their operational technology (OT) systems in the next 12 months.

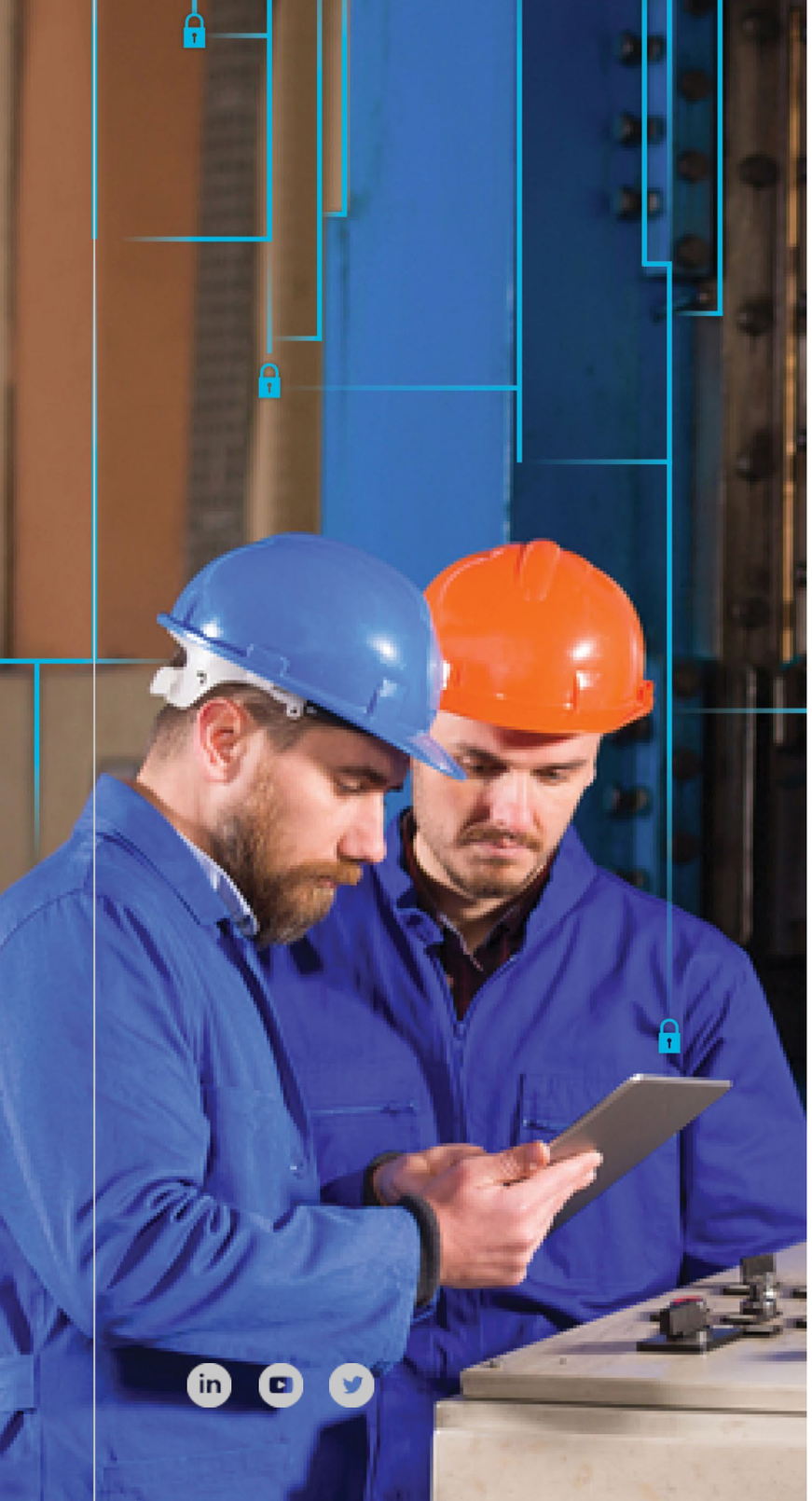
Ironically, this same study—commissioned by GE Digital (formally Wurldtech)—revealed that more than half (52%) of the respondents expect a cyber attack on their operational technology (OT) systems in the next 12 months. And, nearly three-fourths of respondents (71%) said the majority of OT-specific attacks went undetected for more than three months.

Low investment, increased attacks, more maleficence expected. Troubling news indeed. So what's to be done?

GE Digital commissioned SANS Institute, which trains over 12,000 security professionals each year, to address the unique challenges in securing ICS environments and provide recommendations for effective ICS security.

1. *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid, Wired, March 3, 2016*

2 *SANS: Security in a Converging IT/OT World, December 2016*



A little review

Operational technology (OT) is a relatively new field for cyber security. Historically, OT environments were isolated from other networks via air gapping, which protects ICS environments by walling them off from the cyber world beyond. But digital investments to automate systems and data analytics to predict machine performance have increased levels of vulnerability, rendering air gaps useless.

IT and OT are both essential to a holistic and hardened cyber security posture. But where IT security is focused on managing and protecting data, OT cyber security focuses on protecting specific processes and commands. These commands are what operate oil rigs, power plants, manufacturing facilities, and more.

And now, for the bad news—SANS believes OT security is roughly a decade behind IT security in many ways, including organizational development, funding tools, and skilled resources. This is particularly disconcerting when you consider that cyber crime sophistication and success at penetrating vulnerable systems has risen dramatically over the past decade.

The Industrial Internet opportunity cannot be denied, but neither can the risks. The stakes are high, as nation states and bad actors seek to disrupt society or, worse, cause harm to production, people, and/or the environment.

Investing in OT cyber security—not so fast

SANS Institute reports that funding for IT security has typically ranged from 5-10% of the total IT budget. Unfortunately, OT security hasn't had a line-item in budget planning because historically there was no need. Awareness of the risk of an attack on ICS systems is increasing, but justification for ICS funding remains a challenge. Data on ICS security breaches is difficult to come by, and unless a company has experienced an incident, making a case for new spend can be a hard sell.

Today, the question of "who pays?" prevails. Should IT departments fund OT cyber security? Or should it fall to OT business units? Which should clearly understand the risk associated with service interruptions and security risks?

Most corporations that depend on OT have plans in place to manage the physical and environmental risks to safety and operational performance. SANS believes these plans, which define the acceptable levels of risk, must be expanded to include network-based threats to systems. Companies must understand that ICS threats, and the reality of cyber attacks, have the potential to nullify the promise of the Industrial Internet.

Unique challenges

There are real differences between OT and IT environments. ICS equipment suppliers often include remote access to devices for service level agreements. Additionally, safety regulations may prevent modifications to equipment, and operators may be required to provide data to third parties, establishing multiple targets for malicious forces seeking proprietary information.

Add to these issues legacy equipment, limited device virtualization options, and the high cost of industrial equipment, and it becomes exceptionally challenging to test and implement security changes.

And now for the good news. Networks can be secured without disrupting operations by implementing a coordinated program that allows visibility into control network traffic and establishes policies to protect it.

Continuing developments in technology will continue to create and uncover new vulnerabilities, exposing ICS networks to intentional and accidental dangers. But these real-world steps outlined by SANS can help industrial organizations improve their security posture today.

It's important to recognize that establishing a successful, sustainable security program is a complex and long-term effort. But an effective OT security strategy will greatly reduce security incidents and help protect your people, processes, and profits.

Learn more from the SANS Institute report

CLICK HERE

SANS Institute recommends these important capabilities for securing ICS environments:

Network segmentation
Document physical, logical and application network maps, and maintain their accuracy as systems and software change.

Deep protocol inspection and intrusion detection
Procure new monitoring tools to help monitor, collect, and analyze ICS network traffic without negative impact to operations.

Cyber security assessment and audit plan
Know what to do in the event of an incident to lessen the impact and prevent further disruption. Assessments are necessary to gain insight into the effectiveness of current security practices and inform decision-making on potential improvements.Procurement security policies: Enact security controls with vendors, and work with your suppliers to improve the security design of current and future products and processes.

Access control and credentials management
Establish a credential security program, capturing details of existing user roles and align credentials with the new controls.

Incident response
Implement tools to identify and notify security analysts to suspect traffic, with clear response processes.

Vulnerability and patch management
Regularly review and patch known vulnerabilities to help limit negative events.

Security awareness program
The growing numbers of breaches that began with phishing and social engineering have necessitated training to optimize safety efforts. The importance of this step should not be overlooked.

About GE

GE (NYSE: GE) is the world's Digital Industrial Company, transforming industry with software-defined machines and solutions that are connected, responsive and predictive. GE is organized around a global exchange of knowledge, the "GE Store," through which each business shares and accesses the same technology, markets, structure and intellect. Each invention further fuels innovation and application across our industrial sectors. With people, services, technology and scale, GE delivers better outcomes for customers by speaking the language of industry.

Contact Information

Americas: 1-855-YOUR1GE (1-855-968-7143)
gedigital@ge.com

www.ge.com/digital