IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Cybersecurity

Why Bridging Cultural Chasms is Key to Securing Operational Technology

Simon Hodgkinson

Simon Hodgkinson
Strategic Advisor
Semperis

Biography

Simon Hodgkinson is the former Chief Information Security Officer (CISO) at bp and Strategic Advisor at Semperis (https://www.semperis.com). At bp he was responsible for cybersecurity including strategy, governance, architecture, education, counter threat operations and incident response. He joined bp in 2002 and has held several senior IT leadership roles.

Prior to becoming CISO, he was the Vice President – Infrastructure, and Integration Services. During this time, he drove a significant improvement in IT operational integrity, led a transformation program and spearheaded the commitment to improve employees' IT experience. He led the CISO function in bp Supply & Trading, where he delivered a program to improve cyber-controls, many of which have been implemented across the bp group.

Before joining bp, Simon worked in IT for a dotcom, an investment bank and commercial software companies.

Keywords Operational Technology (OT), Operational resilience, Identity system, Identity security, Identity platform, OT security, Cyber security, Ransomware
Paper type Research

Abstract

Operational technology (OT) security is designed to meet the unique security needs of OT environments. This includes protecting system availability, understanding OT-specific protocols, and blocking attacks targeting the legacy systems commonly used in OT environments. As such, OT is becoming increasingly important. In this article, the author discusses how security practitioners bridge the cultural chasm with OT engineers where cyber security is often seen as just one risk among several.

Introduction

We have all heard about the importance of protecting information technology (IT) systems from attack, but what about the operational technology (OT)? This is the infrastructure that directly controls our factories, water treatment plants, and electrical grids. Securing it is critical to protecting the services that underpin our society, but those responsible for it are not the same people who secure our enterprise IT. Their focus is different, and so are their priorities.

Acknowledging and navigating these differences is a vital part of protecting your OT alongside your IT. That means rethinking fundamental concepts including risk and technology deployment.

Operational technology security is becoming increasingly important. The SANS ICS/OT Cybersecurity Survey[1] found almost seven in ten respondents consider cybersecurity threats against OT as high or critical. This number is increasing year-on-year.

Two cultural chasms

Cyber security teams must court specific stakeholders to get support in their quest for OT cyber security. The first group is OT engineers. These are the people tasked with ensuring that the sensors and physical controllers responsible for operating our oil well drills, manufacturing equipment, and water pumps continue to work properly.

IT cybersecurity professionals focus on IT security first. They want to protect information from theft, prevent unauthorized access to IT systems, and stop phishing attacks on their users. OT engineers are less concerned with these things. Instead, their focus is on controllers and sensors that affect physical processes and systems. As such, they're preoccupied with operational uptime, physical security and safety.

Cyber security staff must also build bridges with senior business executives. In many cases, this group is just now getting to grips with cybersecurity, driven by imperatives including regulation and the specter of personal liability and the realization that a major cyber-attack is an existential threat for many organizations. Now, they need help understanding the implications of OT security risk.

Practicality is key

Setting up relationships that allow you to report on OT security risks at board level is paramount. However, opening a channel of communication alone is not enough. Whether you are helping the board understand the need for OT cybersecurity investment or persuading engineers to let you near their programmable logic controllers, you must position cybersecurity risk in a broader context.

Cybersecurity is important, but as far as OT engineers are concerned it's just one risk among many that might well be sector-specific, such as safety, environmental and performance risk.

Similarly, for senior executives, cyber threats are part of a far broader set of business risks. These range from the financial cost to the legal risk or the effect of an outage of critical business operations on revenue.

All conversations with these stakeholder groups should be in their language. Talk to OT engineers about how a digital disturbance could take a PLC offline and what that might mean to the overall control infrastructure. Explain OT risk to senior executives in the context of business/operational resilience, not threats to your firewall, malware strains or threat actor names designed to create fear, uncertainty and doubt; cyber is just another business risk that should be considered as part of overall risk management discussions.

Show, don't tell

In my experience as CISO at bp, I found that the best tools for communicating cybersecurity risks to stakeholders in engineering and the C-suite were demonstrative. Red teaming – using offensive security exercises to identify paths to disrupt OT systems – can bring home the importance of securing industrial infrastructure.

The C-suite doesn't need to see things at that technical level, but business-focused demonstrations can win you valuable traction. Conduct a simulation that demonstrates how a compromise of key OT infrastructure could affect the organization's most important business outcomes. Then explain how likely such a compromise currently is, using the quantitative risk data at your disposal, and how you could drive it down with the right controls.

When you can't patch or replace, mitigate

Simulations like these can help make the case for the mitigating controls that organizations need to protect their OT systems. These controls are important for layering in security protections for infrastructure that might be decades old.

Cybersecurity controls in OT differ from those used in the enterprise IT infrastructure. For instance, deploying security patches is challenging in OT environments. Many OT vendors do not support deploying the latest security patches until they have been approved, which can take many weeks. Equally, the continuous running of the environment means the only downtime to perform patches is during maintenance windows, which could be months or even years away.

Therefore, one must consider mitigating controls; controls that reduce the likelihood of a vulnerability being exploited. This includes segmenting networks to reduce the ability for an adversary to laterally move from the IT networks into OT. This has traditionally been thought of as an "air gap" but in reality, network connectivity exists, and with the increasing digitalization of operational processes, more and more data passes between OT and IT which is used for things like optimization to improve performance or reduce cost. It is therefore critical to have defense-in-depth, including continuous monitoring for anomalous behavior.

Managing identity and access is a critical control. The SANS survey showed that compromised IT systems are the biggest attack vector in OT technology incidents, along with compromised engineering workstations. Secure user and equipment identities are important when enforcing strict access policies for people and equipment alike in IT and OT environments.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Identity information is valuable to attackers, who use it to access OT systems either directly or through connected IT infrastructure. Security teams must protect the underlying identity storage and management systems from compromise. For most companies, the identity system of choice is Active Directory. Organizations must protect their AD implementation from attack[2], both on-premises and in the cloud, especially given the increasing connection of OT systems to cloud infrastructure.

Time for a centre of excellence

One measure that will help to bridge the divide is a cross-disciplinary center of excellence for OT security. This brings together OT engineering and cyber teams, to deliver an achievable, pragmatic program of security improvements to reduce cyber risk, whilst maintaining the operation.

This center can be internally focused at the beginning, but there is plenty of opportunity for extending it to external stakeholders, including regulators and peers in your sector. Sharing information and best practices in OT security is a powerful step in getting ahead of attackers, and industry-specific ventures such as Information Sharing and Analysis Centers (ISACs) are an excellent place to begin.

Put identity at the centre of your security strategy

Companies using OT to run their businesses must pay attention to security now because the stakes are rising. While attacks on OT systems are still relatively rare, they do happen. For example Triton, first identified in 2017 as malware that disrupts safety shutdown procedures in energy plants, is still a threat, according to the FBI. The UK also worries about attacks on OT and has alerted[3] organizations of threats to infrastructure from state actors.

The identity management system is at the very heart of operational resilience. Put simply, for most organizations if your identity system is unavailable, you will not be able to continue to operate, and deliver business outcomes to your customers. To be operationally resilient, one must be able to withstand, or recover quickly from an adverse event like a ransomware attack.

Act now to fend off attacks that promise to grow in importance and reach over time. Getting it right could be the difference between keeping the lights on and stumbling in the dark.

Reference

[1] Pearson, D. (September 2023), SANS ICS/OT Cybersecurity Survey: 2023's Challenges and Tomorrow's Defenses (Se. Security Week. Available at: https://www.securityweek.com/wp-content/uploads/2023/09/sans-OT-survey.pdf

[2] Deuby, S. 'What is Active Directory Security?'. Semperis. Available at: https://www.semperis.com/blog/active-directory-security/what-is-active-directory-security/ . Available at: https://www.semperis.com/blog/active-directory-security/what-is-active-directory-security/

[3] (1 May 2024) *NCSC warns of emerging threat to critical national infrastructure*. National Cyber Security Centre. Available at: https://www.ncsc.gov.uk/news/ncsc-warns-of-emerging-threat-to-critical-national-infrastructure