OT Security Specialists – The Digital Shepherds of Our Critical Infrastructures

Written by Joshua Bucheli, AI Ethics Researcher and Fellow at the ForHumanity Center, in Collaboration with Swantje Westpfahl, Acting Director of the ISS, Christian Fichtner, Senior Cyber Security Architect at DB, Stefan Schillings, Information Security Officer and Cloud Architect at SBB, and Peter Kosel, Founder of cyberunity

10 years ago the infamous PSN hack and outage prevented millions from gaming online for close to a month, costing Sony over $170 million, compromising sensitive data of close to 80 million accounts, and outraging gamers the world over.

While typical of the kind of costly inconvenience that cybersecurity breaches in IT can cause, such incidences pale in comparison to what lies on the horizon if our key infrastructures become vulnerable to similar attacks.

IT is often in the limelight, but it is not the only dimension of cybersecurity. Indeed, securing Operational Technologies (OT) – the hardware and software that monitors and controls physical devices and processes in an infrastructure – is just as, if not even more important.

"In contrast to the beginnings of OT, which were designed more for a single purpose than for interoperability with IT, OT structures in the 'Industrie 4.0 environment' are becoming more intelligent and are communicating far beyond their physical boundaries. However, this is countered by proprietary protocols that have implemented security in a rather rudimentary way and that are many times more vulnerable than the protocols that currently exist in IT environments," says Christian Fichtner, Senior Cyber Security Architect at the Deutsche Bahn.

Think control panels in factories or switches in railway networks. Think power grids and the systems that operate traffic lights, industrial machinery, and the rods in nuclear reactors. Although slightly behind IT, these OT legacy (outdated but functional) systems are entering the digital age – our critical infrastructures are 'going online'.

Where Does Operational Technology Stand Today?

According to Swantje Westpfahl, acting Director of the Institute for Safety and Security, digitisation is the name of the game:

"The OT sector is fully immersed in the digitisation process and as soon as these systems are connected to the network, they are at risk. Everyone wants to be more connected because it makes things easier. But it is precisely this ease that also brings risks – both obvious and obscure. The fact that things are developing in the direction of automation *and* remote management makes the situation all the more volatile."

Perhaps the most pressing issue facing OT today is the growing awareness gap when it comes to the nature and scope of cyber-threats:

"People stand next to control panels and think they have everything under control. But as legacy systems go online, these individuals are often not aware of how easy it is to hack such systems – this represents potentially life-threatening risks."

Consider Transmission System Operators (TSOs) that manage the distribution of electricity at the national and regional level. Once these go online and become hackable, breaches in security can mean catastrophic blackouts lasting for days or even weeks.

Take, for example, the power outages in Ukraine in 2015 and 2016, or the Stuxnet incident that occurred 10 years ago, in which centrifuges in Iran's uranium enrichment programme were sabotaged.

Even seemingly trivial OT can cost lives if left exposed to cyberattacks. Take the systems that regulate brewery and distillery equipment – if compromised, manipulation of these machines by nefarious parties could not only halt production, but even cause tragic explosions.

We need only look to the devastation caused by events like the 2014 sabotage of a German steel mill's blast furnace to imagine the potential havoc that maliciously orchestrated industrial disasters could bring.

The development of IoT technology, which will likely be hooked up to the same networks as future OT, will no doubt also play a decisive role in this whole equation, argues Swantje, as will the brute force threats posed by the emergence of quantum computers.

Some nations have already made concerted efforts to address these concerns:

Israel is ahead of the pack when it comes to integrating cybersecurity studies into public education systems. Estonia is almost completely digitised and has leveraged blockchain technology as a means to secure information infrastructures. Meanwhile, Japan is ahead of the curve in terms of addressing automotive security concerns, rapidly implementing regulations like the UN Norm R155 /R156 and treating automobiles first and foremost as IoT.

Nevertheless, there is still a long way to go - it is absolutely crucial that businesses, industry leaders, and policymakers recognise and embrace tools like the ICBC's Cyber Demonstrator in order to better acquaint themselves with these issues sooner rather than later:

"Ultimately, simple probability based risk calculations won't cut it. If we look at the uptick in cyber attacks in recent years, it becomes evident that they will become the norm rather than the exception -- and this is true for OT just as much as IT", warns Swantje.

OT Security-Specialists - Hard Skills and Qualifications:

When it comes to education, computer science degrees offering majors focused on IoT, SCADA, and other critical infrastructures will be a considerable asset to aspiring OT security specialists (see, for example, the Hochschule Luzern's Bachelor in Information & Cyber Security Major in Technology).

Certificates and training specific to industrial cybersecurity like those offered by the ISS' Capacity Building Center (ICBC) and Dragos, or the GIAC's GICSP, GRID, and GCIP will of course give candidates a particular edge. However, individuals with other security certifications like CEH, CISSP, and CISM will also stand out positively and degrees and certifications in engineering disciplines will also be a plus.

Regardless of formal qualifications, what the industry needs are individuals with the skills necessary to shepherd our critical infrastructures securely into the digital age. The battle for these infrastructures will be fought on many fronts, so the wider employers cast their nets in terms of IT-engineers and network specialists, the better they will be able to defend their OT.

"The larger and more interlinked the enterprise in question, the more important individuals with the ability to bring a holistic perspective to both IT- and OT security", advises Swantje.

"Aspiring OT security specialists should therefore ideally be able to bring together expertise and best practices from disparate fields like manufacturing, IT focused cybersecurity, and risk-management".

In terms of hard skills, this means the following: engineering know-how, expertise in the fields of network security, penetration testing, and establishing business-continuity models, and an understanding of the real-time application of these skillsets. Experience in securing physical systems, ICS, and a basic understanding of electrical or mechanical engineering will also be a huge plus.

Because OT is all around us, there are myriad points of entry to the OT security industry. Organisations that offer dedicated Industrial OT security solutions like Dragos, Fortinet, InfoGuard, Secunet, Cyberbit, or VINCI Energies' forthcoming international Security Operations Center hub in Basel are ideal places to start.

Nevertheless, industries in which these OT systems are manufactured and in which they have operated for decades must not be overlooked.

As Stefan Schillings, Information Security Officer and Cloud Architect at the SBB, points out, "The difficulty of operating and supporting OT systems over decades is huge. Supply chains need to be actively secured and audited - and changes to existing assets require very precise expertise, which is a real challenge in times of online patching!"

Railways like the SBB, the DB, and the EWS, manufacturers of industrial machinery like Caterpillar Inc, ABB Group, Cisco, and Linde AG, and other entities operating key infrastructures like energy companies and nuclear plants will all need the support of OT security specialists if they are to survive the transition into the digital age.

Beyond Hard-Skills:

"OT security specialists are leading the current leap in information security, which, as in IT, increasingly affects OT. They understand the business and mediate between OT and a much smaller IT world. They act as interpreters between engineers and IT professionals, represent OT relevant aspects of a converging IT/OT world, and develop security concepts based on greenfield, brownfield and darkfield approaches. After all, every OT environment is different and optimally adapted to its particular task," explains Christian.

As a result of these diverse responsibilities, it is absolutely essential that aspiring OT security specialists possess qualities that go beyond the aforementioned hard skills.

For example, communication skills are also vital. OT security specialists will not only need to be able to work dynamically within interdisciplinary teams to identify security requirements, they will need to be able to communicate and justify these requirements to managers and C-Suite executives throughout an enterprise (or at the very least the CISO).

Vigilance and strong analytical skills are also key, as individuals will have to spot and contend with ever-evolving threats on a daily basis.

"Making operational branches aware that their assets are not invulnerable requires imagination and tools like the Mitre-ICS ATT&CK Framework can help make these evolving threat scenarios more visible, giving SOC units a better understanding of potential targets and countermeasures," adds Stefan.

Also not to be overlooked, says Swantje, is perseverance:

“Security is inherently a prickly discipline that many still consider an annoyance. People would much rather assume that their firewalls will sufficiently protect their networks than deal with the complexities of issues like remote maintenance and access controls.”

To contend with this, OT security specialists will need a steadfast conviction that the work they are doing is vital to setting us on the right track for a secure future.

As Peter Kosel, Founder and Talent Community Manager of cyberunity AG, concludes, “the issue of OT security affects virtually everyone. Whether the digitisation of OT is looked back on as humanity’s most fatal faux pas or as one of its most fruitful innovations will depend in large part on whether or not employers establish forward-looking talent pools composed of qualified and capable OT specialists. If companies only tackle the issue of OT security recruitment after these systems have come under attack, then they will have great difficulty in attracting the right people on short notice.”

Peter emphasises how crucial it is for employers to move away from the traditional recruitment process, which only starts when a position urgently needs to be filled, if they want to ensure corporate success and sustainability. The KNOW YOUR TALENTS approach starts well before

a vacancy arises and relies on lively relationships with future high performers in order to be able to contact and win them over easily once they are needed.

Those interested in the **ICBC's' OT Security Training and Exercises** can find more information via the following link: **https://icbc.uniss.org**