TOWARDS LASTING CYBER RESILIENCE IN MANUFACTURING

LOOKING BEYOND COVID-19 INDUCED RISE IN CYBER RISKS

JUN 2020

Coordinated cyber attacks on industrial infrastructure have risen by nearly 32 percent in the first four months of 2020 across the globe. Hackers are targeting everything from chemical and power plants to plants involved in processing food and metals. In this situation, employee safety and the environment are both threatened more than ever before.

THE INDUSTRIAL CONTROL SYSTEMS

Industrial control systems (ICS) and operational technology (OT) are being thrust into the future by enabling technologies and transformative waves of innovation such as industry 4.0, IIoT, and 5G, which promise to bring major benefits in the form of increased productivity, safety, and operational efficiency. Modern industrial corporations will need to evaluate the many technology benefits on offer and determine an acceptable risk posture for their company if and when they ride one or all of these transformative waves.

With each transformation comes cybersecurity risks, including an increase in the potential attack surface and a plethora of new attack vectors for cybercriminals to exploit. To counter them successfully, cybersecurity risk needs to be viewed end-to-end, not in operational silos.

> *An automotive giant was targeted through coordinated cyberattacks in June following which some plants were compromised and went offline. This attack was most likely a ransomware attack and fits into a larger pattern that Subex has seen in the last 95 days (from Feb 2020). Such attacks are likely to increase in the next few months and this rise is expected to continue for the next 6 months according to Subex's threat research team.*

Likewise, OT/IT security strategies and policies need to be understood and in sync across the entire industrial enterprise. Although OT and IT have diverse missions, business pressure will force a new emphasis on convergence or at the very least alignment between these two domains. The consensus within the OT cybersecurity industry is that the conventional wisdom surrounding air-gapped systems and the great divide between OT and IT is quickly becoming a thing of the past.

In one instance recorded at our ICS honeypot, Subex's threat researchers zeroed in on many multi-stage cyberattacks on simulated industrial control systems.

Using a variant of common ransomware, the hackers first tried to compromise admin credentials and then tried various methods to breach the system and gain control. The attacks on these systems across our honeypot networks increased by a whopping 69 percent in the first quarter of 2020. In most of these attempts, the hacker was trying to inject ransomware into the system.

CHALLENGES

OT cybersecurity has never been more important or more challenging. With plants and supply chains undergoing waves of transformation driven by new and emerging technologies and due to the emergence of a new breed of hackers chasing monetary gains by holding data to ransom, the risks associated with manufacturing are now growing at a fast pace. Many manufacturers have struggled to secure their endpoint assets and their connected environment because they couldn't detect nor the agility to mitigate these attacks on OT assets.

The problem is compounded by the addition of connected devices that cannot be patched or those that cannot host an agent-based cybersecurity solution. Cybercriminals see this as an opening for them to infiltrate a manufacturer's OT network and move laterally heading into the IT network and beyond. In this way, hackers can target multiple networks with one attack and go after various assets and data to increase their chances of monetizing the attack.

THE INDUSTRIAL CONTROL SYSTEMS

Geopolitical instability

Easy availability of OT equipment on e-commerce sites

Hackers can now order DDoS attacks and malware on-demand from the Darkweb

Hackers and groups are creating variants of existing malware faster to evade systems designed to detect malware

Convergence of IoT and OT is creating more surface area for cyberattacks

The biggest threat is employee activity. With hackers using targeted social engineering by targeting employees on social media and other sites, the chances of an employee falling for digital traps has increased exponentially in 2020. The prevailing environment of confusion and anxiety has added to the risk. It is only a matter of when rather than if.

PREPARING FOR THE 'NEW NORMAL'

Beyond everything you have heard, let us try and understand what the new normal is from a cybersecurity perspective. How much have risks increased for everyone in general and manufacturers in particular? And what does it translate into from a cyber resilience strategy perspective? Some characteristics of the new normal include:

- Increase in sophisticated cyberattacks
- Targeted cyberattacks launched on ICS and networks with high levels of persistence
- Use of botnets and other manipulated infrastructure globally to target supply chains and assembly lines
- Cyber insurance premiums to rise
- A major cyberattack will be just a click away
- Pilfered IP and other data will be siphoned off to locations where they cannot be traced easily
- Ransom demand and cost will increase enticing more hackers to join the fray and target manufacturers
- Unpatched systems or those parts of the infrastructure that were 'forgotten' during the Covid-19 pandemic will create problems for manufacturers especially those who are unable to discover assets or state of patching of devices
- The heightened reconnaissance activity detected by Subex's honeypot networks across 62 cities around the world points to hackers becoming more persistent and willing to wait for the right conditions to emerge before they strike
- Already, converged environments, representing a blend of IoT and OT systems have revealed new vulnerabilities that have already been exposed on the Dark web and other outlets, and many manufacturers are yet to address these chinks in the armor.

SECURING MANUFACTURING

To secure assets, data, and systems connected with manufacturing, a multi-pronged strategy must be adopted that includes:

- ✓ Building an enterprise risk model: look at security from an inside-outside perspective to understand the type of attacks, assets that could be targeted, weak points, employees who could be targeted and then link it with strategic decisions about infrastructure, technology, process modifications, and operations required to mitigate it.
- ✓ Evaluate supply chains linking with key processes and equipment to avoid supply chain poisoning
- ✓ Fortify your threat posture: regularly conduct ongoing rain checks on key measurement criteria and targets. Align them with the prevailing threat landscape and threat actor and malware behavior (extending point 1)
- ✓ Have regular conversations with all stakeholders and encourage employees and others to identify areas for improvement from a cybersecurity perspective
- ✓ Plan for the fallout of an attack: as part of the resilience strategy, put in place a comprehensive procedure for recovery. Document events, share the learnings with all stakeholders. This helps improve processes and planning thereby improving inputs for risk scenario modeling
- ✓ Digital risks cannot be handled in silos. As per a recent Gartner study, as less as 30% of all businesses are today taking enterprise-wide steps in a unified way to manage their digital risks. It is now time to treat cybersecurity as a strategic business driver and not a line item on an IT checklist

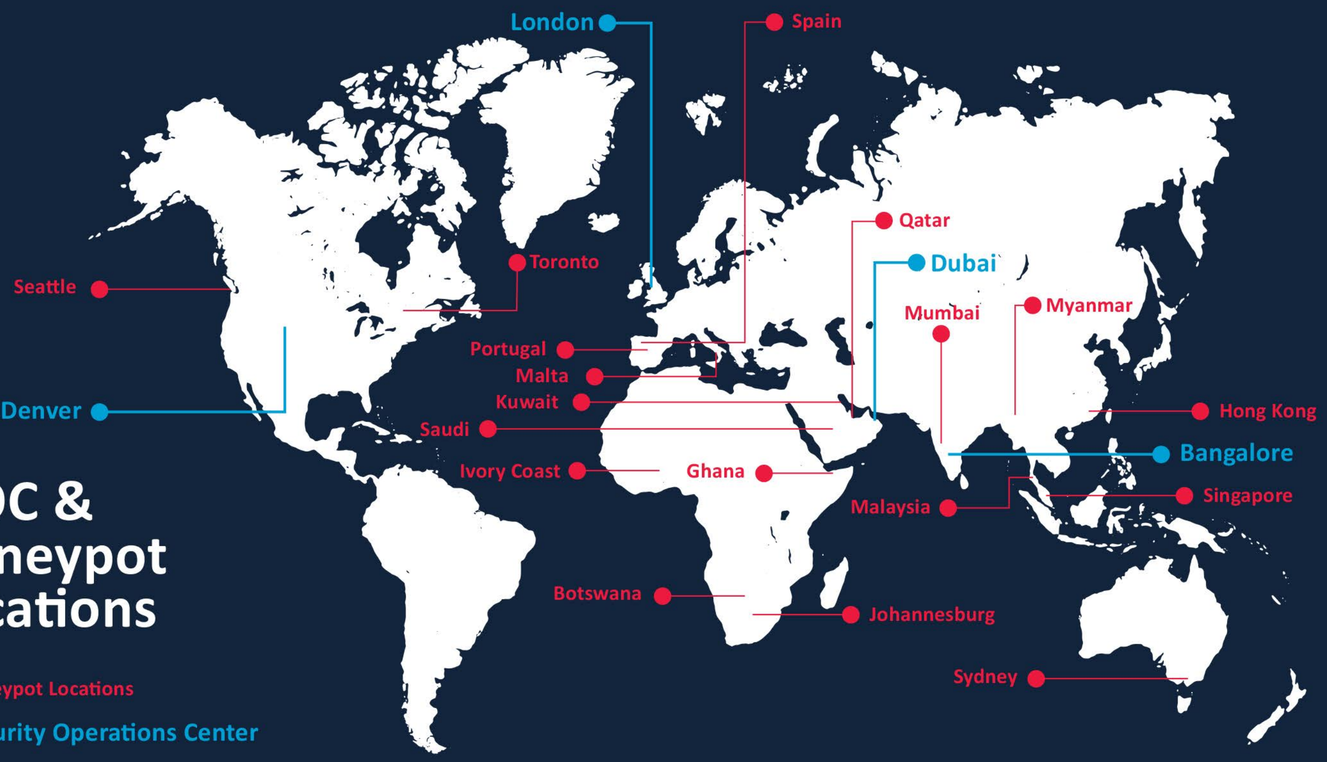
Subex is today helping manufacturers improve their cyber risk posture across the globe. For manufacturers we offer a robust cybersecurity solution that addresses potential cyber risks, detect critical exploits, monitor, identify and catalog threats in real-time in IoT, OT, and converged environments.

To continue this conversation, send us a line at info@subex.com. Don't forget to mention #covmfnsec to qualify for a special conversation.

About Subex

SUBEX

www.subex.com



ISOC & Honeypot Locations

● Honeypot Locations

● Security Operations Center

- Subex is the market leader in products Security and Fraud Management market, with over 180+ customers in total
- Awarded Pipeline Award at Nice 2016 for most innovative Security and Assurance Solution for IoT Security
- Subex is the Number 1 provider globally of Fraud Management and Security solutions in the Telecom Space, according to a Gartner report published in March 2016
- Subex runs the world's most comprehensive IoT and ICS focused honeypots of over 400 architectures in 32 locations around the world.
- +300 Installations around the world
- +700 Experts in Security/Fraud and other programs with assets, skills and innovative methods to ensure results for the operator
- Publicly listed in the National Stock Exchange (India) and Bombay Stock Exchange

Subex Limited

RMZ Ecoworld,
Devarabisanahalli,
Outer Ring Road,
Bangalore - 560103 India

Tel: +91 80 6659 8700
Fax: +91 80 6696 3333

Subex, Inc

12303 Airport Way,
Bldg. 1, Ste. 390,
Broomfield, CO 80021

Tel : +1 303 301 6200
Fax : +1 303 301 6201

Subex (UK) Ltd

1st Floor, Rama
17 St Ann's Road,
Harrow, Middlesex,
HA1 1JU

Tel: +44 0207 8265300
Fax: +44 0207 8265352

Subex (Asia Pacific) Pte. Limited

175A, Bencoolen Street,
#08-03 Burlington Square,
Singapore 189650

Tel: +65 6338 1218
Fax: +65 6338 1216

For more information write to info@subex.com

Regional offices: Dubai | Ipswich

Subex Limited. 2018. All rights reserved. Although every endeavour has been made to ensure that the information contained within this document is up to date and accurate, Subex Limited cannot be held responsible for any inaccuracy or error in the information contained within this document. 20062018.