UNIVERSITY OF CAMBRIDGE

Managing cyber risk in the Fourth Industrial Revolution:

Characterising cyber threats, vunerabilities and potential losses

A briefing paper commissioned by Policy Links (Institute for Manufacturing – University of Cambridge) on behalf of the Global Manufacturing & Industrialisation Summit (GMIS) and Lloyd's Register Foundation (LRF)

Jennifer Copic and Éireann Leverett
Cambridge Centre for Risk Studies
University of Cambridge Judge Business School

July 2019

Lloyd's Register Foundation

GMIS Global Manufacturing & Industrialisation Summit

About the Briefing Paper

This is one of two briefing papers developed under the project "The safety and security dimensions of Industry 4.0", commissioned to the University of Cambridge (Policy Links – Institute for Manufacturing) by the Global Manufacturing & Industrialisation Summit (GMIS) and Lloyd's Register Foundation (LRF).

The briefing papers constitute the first stage within an open, multi-stakeholder project that aims to bridge the safety and security knowledge gaps in the deployment of 4th Industrial Revolution (4IR) technologies in manufacturing. The intention of the briefing papers is not to be prescriptive, but to provide an in-depth analysis of selected themes related to emerging safety and security risks and requirements for manufacturing, in the context of 4IR.

This briefing paper has been produced without formal GMIS or LRF editing. The views expressed here do not imply the expression of any opinion on the part of GMIS or LRF. Mention of firm names or commercial products does not constitute an endorsement by the authors, GMIS or LRF.

Acknowledgements

The authors would like to thank the Cambridge Centre for Risk Studies staff for their contributions to the research summarised in this report: Dr Andrew Coburn, Dr Jennifer Daffron, Kayla Strong, Andrew Smith, Kelly Quantrill, Philip Cameron, Timothy Douglas, James Bourdeau, Tamara Evan, Dr Edward Oughton, Simon Ruffle, Dr Andrew Skelton, Dr Michelle Tuveson and Professor Daniel Ralph.

GMIS Global Manufacturing & Industrialisation Summit

The Global Manufacturing and Industrialisation Summit (GMIS) was established in 2015 as an industry association to build bridges between manufacturers, governments & NGOs, technologists, and investors in harnessing the Fourth Industrial Revolution's transformation of manufacturing to the regeneration of the global economy. A joint initiative by the United Arab Emirates and the United Nations Industrial Development Organization (UNIDO), GMIS is a platform that presents the manufacturing sector with an opportunity to contribute towards global good, working to the benefit of all.

LR Lloyd's Register Foundation

The Lloyd's Register Foundation is a UK charity established in 2012. With our mission to protect the safety of life and property, and to advance transport and engineering education and research, the Foundation has an important role to play in meeting the challenges of today and the future. Our vision is to be known worldwide as a leading supporter of engineering-related research, training and education that makes a real difference in improving the safety of the critical infrastructure on which modern society relies. In support of this, we promote scientific excellence and act as a catalyst working with others to achieve maximum impact.

Key messages

With the advancement of the 4th Industrial Revolution (4IR), manufacturers are exposing themselves to more and more vulnerabilities as they deploy new technologies, which are increasingly Internet-connected. The increased risk can come from the new technologies themselves or from the interactions between new and legacy systems. Cyber attacks are now a growing concern for the manufacturing sector, whether the attacks target safety instrumentation systems, industrial control systems or enterprise systems. A 2018 study by Make UK and AIG found that 48 per cent of UK manufacturers have experienced a cyber attack, with a quarter of the attacks resulting in a financial impact.[1] Intellectual property (IP) is the most commonly cited motivation for attacks on the manufacturing sector, although we note that the motivation is not commonly known in most cyber incidents. This paper will outline the cyber threats and vulnerabilities to the industrial sectors, categorise the losses the sector might experience during an attack and review risk transfer mechanisms, highlighting an innovative application approach enabling an improvement culture within corporates. It will also detail why a particular focus should be created by researchers and policy-makers on issues of integrity and safety, before, during or after a cyber attack. Current approaches are pragmatic throughout the organisation, from board to shop floor. A new paradigm is needed to ensure cyber security and safety in the manufacturing sector, as 4IR technologies require a dedicated focus on safe adoption and integration into existing systems.

[1] Make UK and AIG. (2018) Cyber Security for Manufacturing.

List of acronyms

AIC	Availability, Integrity and Confidentiality
AIG	American International Group
ARC	Additions Recruitment Consultants
BI	Business Interruption
CBI	Contingent Business Interruption
CIA	Confidentiality, Integrity and Availability
CRM	Client Relationship Management
DCS	Distributed Control Systems
EMS	Energy Management Systems
ERP	Enterprise Resource Planning
FLEXA	Fire, Lightning, Explosion and Aircraft Impact
HMI	Human Machine Interface
HPR	Highly-Protected Risk
ICS	Industrial Controls Systems
IIoT	Industrial Internet of Things
IoT	Internet of Things
IP	Intellectual Property
IT	Informational Technology
OT	Operational Technology
PLCs	Programmable Logic Controllers
SCADA	Supervisory Control and Data Acquisition
SIS	Safety Instrumented Systems
TTPs	Tactics, Techniques and Procedures

1. Classifications of cyber security threats and vulnerabilities

The 4th Industrial Revolution (4IR) is introducing ground-breaking productivity improvements within the manufacturing sector, driven by Internet connectivity. Intelligent factories have all the machines, components, sensors, actuators, as well as the products being produced, connected to the Internet to enable communication as the Industrial Internet of Things (IIoT). This expands to the deployment of machine learning to do root-cause analysis on faulty equipment and to predict likely failure points, and to the integration of smart whiteboards displaying real-time production metrics.[2] These technological advancements enable a truly cyber-physical space that increases the risk potential, because with increased connectivity must come more rapid patch cadence, and change-management practices must adapt accordingly.

Distinguishing between the types of system present in a manufacturing environment is helpful in aiding threat classification. Informational technology (IT) systems and operational technology (OT) systems face different inherent threats and vulnerabilities. IT systems are traditional PCs, servers, cloud storage, enterprise networks, smartphones, tablets, and so on, while OT systems are industrial controls systems (ICS),[3] safety instrumented systems (SIS), IIoT, energy management systems (EMS), and so on. In addition to the IT risks inherent in all organisations, the OT risks add a layer of complexity that is unique to the manufacturing sector, as it introduces the potential for cyber-physical consequences, which include damage to employees, facilities, products, machinery or, potentially, customers. For example, a robotic arm that was in standby mode was rotated 180 degrees during a ping sweep, which could have caused bodily injury if an employee had been standing nearby.[4] The potential for harm warrants a deeper understanding of the threats and vulnerabilities, and the operational or capital expenses that it incurs to protect employees, customers and facilities.

Broad taxonomy of cyber security threats

There are three main components to consider when creating a taxonomy of threats on OT systems within the manufacturing sector: adversarial attack techniques, target OT assets and vulnerable systems.

[2] E. de Boer, D. Hernandex Diaz and H. Leurent (2018). The Fourth Industrial Revolution and the Factories of the Future. McKinsey & Company. Accessed 22 April 2019.

[3] Examples of industrial control systems (ICS) include: supervisory control and data acquisition (SCADA), distributed control systems (DCS) and programmable logic controllers (PLCs).

[4] RISI – The Repository of Industrial Security Incidents (1998). Ping Sweep Causes Inappropriate Control of a 9 Foot Robotic Arm.

THE GOAL OF CYBER ATTACKS ON MANUFACTURING OPERATIONAL TECHNOLOGIES (OT) IS TO COMPROMISE:

AVAILABILITY	INTEGRITY	CONFIDENTIALITY
Adversarial Attack Techniques • Spearphising Attachment • Scheduled Task • Automated Exfiltration • Network Sniffing • ARP Spoofing • Physical Access • Social Engineering • Distributed Denial of Service (DDos) • Compromised USB • Etc., see MITRE ATT&CK™ Matrix for more TTPs	Target OT Assets • Sensors • Actuators • Data Stores • Communication Network • Decision Logic • Safety Systems • External Dependencies	Vulnerable Systems OT Related • Industrial Controls Systems (ICS) • Safety Instrumented Systems (SIS) • Industrial Internet of Things (IIoT) • Energy Management Systems (EMS) • Etc. IT Related • Operating Systems (OS) • Enterprise Resource Planning (ERP) • Client Relationship Management (CRM) • Etc.

Table 1 - Theoretical Cyber OT Attack Framework for an Individual Company (Source: Cambridge Centre for Risk Studies)[5,6]

Adversaries have several tactics, techniques and procedures (TTPs) that they utilise in order to compromise a system and achieve their end goal. For example, the attacker could use a spearphising attachment in an email to gain initial access and then escalate privilege through a scheduled task technique to gain access to sensitive data and finally exfiltrate the data through an automated exfiltration technique. As this illustration shows, adversaries may use a combination of TTPs to perform an attack. In 2015 the MITRE ATT&CK™ Matrix was published, which summarises the TTPs that adversaries use during cyber attacks on Windows, Mac and Linux-based operating systems, as well as mobile devices (see footnote 6). The TTPs described in the MITRE ATT&CK™ Matrix are usually transferable to OT systems.

These TTPs are used to target key assets within an industrial environment such as sensors, actuators, data stores, communication networks, decision logic, safety systems and external dependencies. The first six assets are described in the recent cyber book published by members of the Cambridge Centre for Risk Studies: Solving Cyber Risk (2018), while for the purposes of this paper, external dependencies have been added to add clarity of impacts. The addition of external dependencies is key for individual companies to monitor and mitigate their potential risk as it captures potential third-party cyber exposures. For example, almost all industrial sites are dependent on the national power grid supplying power to their facility. If a cyber attack were executed on the power network, resulting in a power outage, this could potentially limit production capabilities at all dependent industrial sites. In a sentence: Could a cyber attack on one of your upstream suppliers halt production in your business?

A 2019 Ponemon Institute survey of security professionals in the US, UK, Germany, Australia, Mexico and Japan critical infrastructure sectors found that 90 per cent had been hit by at least one successful

[5] The Theoretical OT Attack Targets were originally published in A. Coburn, E. Leverett, and G. Woo (2018). Solving Cyber Risk: Protecting Your Company and Society. Hoboken, New Jersey: John Wiley & Sons. and are expanded for the purposes of this paper.

[6] The Adversarial Attack Techniques are taken from B. Strom (2018). ATT&CK 101 MITRE ATT&CKTM (blog).

cyber attack in the last two years.[7] This highlights the idea that critical infrastructure defined as "utilities, energy, health and transport sectors" are equally, if not more, targeted than the manufacturing sector, thus representing a major concern for the continuity of operations in the manufacturing sector.

An adversary's goal when targeting these critical infrastructure assets is to limit or eliminate their availability, compromise their integrity or reduce confidentiality of data. This is called the CIA triad, also called the AIC triad when discussing OT systems. The ordering was changed to reflect the difference in prioritisation that is more relevant to OT systems. Availability in an OT sense means ensuring that key systems and assets are operating effectively and reliably. Integrity means "guarding against improper information modification or destruction, and includes ensuring information…authenticity"[8] The aim of confidentiality in an OT environment is to prevent the release of information. Availability is listed first when discussing OT systems, as it is a critical component: if the system isn't available then the process is either not operating in its entirety or not operating at full capacity. Without available systems, integrity and confidentiality do not matter. Potentially, because of this ordering, more emphasis has been placed within the academic community, as well as industry, on ensuring availability, with sustainably less focus on integrity or confidentiality.

Finally, these TTPs targeting key OT assets exploit vulnerabilities in IT or OT systems such as the ICS, SIS, IIoT, operating system (OS), enterprise resource planning systems (ERP) or client relationship management systems (CRM), to name a few. Adversaries use TTPs within these vulnerable systems to target key OT assets.

Integrity is key

Throughout this paper, we will continue to refer to integrity as a key concept for understanding the vulnerability and impact associated with cyber attacks. It is worth defining what we mean and how it is useful from either a micro- or macro-level view. An organisation should have the capability to verify the integrity of code, data, contracts, transactions, messages and authorisations, among other things. It is useful before a cyber attack to be confident that back-ups are legitimate, have not been altered and are fit for purpose. It is useful during an attack to know which data has veracity and integrity, and which sources of data may or may not be giving you the truth about the cyber incident. Useful questions to pose are: Has this data been altered during the cyber attack, what can be relied on with certainty and what is known to be an unreliable source of information? After an incident, the ability to verify the integrity of back-ups as they are restored is crucial, as are the log files of the incident. Thus, verification of integrity is a useful property at almost any point in time, and almost any tier of the business.

At micro or site level we can verify the integrity of network traffic and firmware files with cryptography or check that intellectual property has not been altered and site plans remain intact. At a macro or enterprise level we must be able to demonstrate that board members have not had their emails altered when they make decisions about how to run the company. Integrity can also be framed to ensure service level agreements are adhered to, verifying supplier's contracts to ensure that promises

[7] D. Simmons (2019). Hack Attacks 'damage' Key Infrastructure. BBC News, sec. Technology.

[8] W. A. Conklin (2016). IT vs. OT Security: A Time to Consider a Change in CIA to Include Resilience. 2016 49th Hawaii International Conference on System Sciences (HICSS): 2642–2647.

are met. In short, integrity and verification are an ideal opportunity for anyone interested in how to improve the cyber security of industrial systems and businesses. Building capability to verify integrity at any point in time, and at any level of a company's structure, will pay off immensely during a cyber crisis. Consider the vulnerabilities below, and how the inability to "know with certainty" or verify the integrity of various things or processes is at the root of the problems we face in ICS security.

Cyber security vulnerabilities

OT systems are built around physical devices or machines controlled by ICS that are often connected to the Internet in order to enable real-time monitoring, analytics, control and predictive maintenance. Legacy systems left security problems to the customer, suggesting that they "just not connect to the Internet", while the increased use of smart devices, sensors and IIoT increases the connectivity of manufacturing floors, thus changing the cyber attack landscape for OT systems. The ARC Group estimates that companies will spend $42 billion this year connecting industrial equipment to the Internet.[9] The following is a list of the potential vulnerabilities found in OT systems and published by the Centre for Risk Studies in 2018.[10,11]

- ICS lifetime versus IT system lifetime – engineering systems are generally designed to last five times longer than the underlying IT systems.[12] This is important because cyber threats are co-adaptive, developing new techniques over the lifetime of a product. Continual verification of the device's integrity over a long lifespan is crucial and extremely challenging for legacy systems.

- Poor patching cadence – given the complexities of these OT systems, it is challenging to patch operating systems and software to ensure the functionality of the entire system. A study by Wang et al. of 100,000+ Internet-connected ICS devices found that they were patched within 60 days of vulnerability disclosure.[13] However, a study by the Zero Day Initiative determined that in 2016 it took 143 days for human machine interface (HMI) vulnerabilities to have a patch released by the vendor.[14] Note that this suggests it takes 143 days to produce the patch, and another 60 before it is deployed, meaning that 203 days would pass before the average system were patched. Not only is patching cadence within an organisation a concern but patch releases from vendors are also subject to lengthy delays. There is little point in having a patch cadence that is 10x faster than your vendors. Verifying the integrity of patches, that they will not disrupt the business, and that vendors will produce them in a timely manner, is the goal.

- Poor password security and unencrypted protocols – default passwords on ICS devices are not regularly changed (see footnote 14). Although the recent Mirai Botnet cyber attack was not related to ICS, it highlights these security issues. The Mirai Botnet was created as a result of Internet of Things (IoT)

[9] M. Giles (2019). Triton Is the World's Most Murderous Malware, and It's Spreading. MIT Technology Review.

[10] The following list has been adapted and significantly expanded from the original version published in S. Ruffle et al. (2018). Submission to UK Parliamentary Joint Committee on the National Security Strategy: Cyber Security: Critical National Infrastructure Inquiry. Cambridge Centre for Risk Studies.

[11] For further information on the technical side of these vulnerabilities, see ICS-CERT (2018). Overview of Cyber Vulnerabilities. Accessed 6 April 2018.

[12] SecurityZap (2015). Vulnerabilities in Industrial Control Systems – SCADA. Security Zap.

[13] B. Wang et al. (2017). Characterizing and Modeling Patching Practices of Industrial Control Systems. Proceedings of the ACM on Measurement and Analysis of Computing Systems 1, no. 1: 1–23.

[14] B. Gorenc and Fritz Sands (2017). Hacker Machine Interface: The State of SCADA HMI Vulnerabilities. Trend Micro Zero Day Initiative Team.

devices being sold with easily hackable passwords and using unencrypted protocols – the languages used to communicate with devices – that can easily be monitored and intercepted by malicious actors.[15] This situation is gradually improving but many older systems are still in use and vulnerable to cyber attack. "How do I know this password has not been used by someone else, maliciously?" is a question of integrity verification in this space, but many others exist. How do I reset the password when something goes wrong, and will that break all my integrations? Does the vendor provide any documentation about changing passwords, keys or certificates, and how to recover a device from a hostile condition (infected or compromised firmware).

- Increasing use of IIoT – insecure remote connectivity of smart devices and IIoT enables unrestricted outbound Internet access. IIoT devices enable machine and sensor monitoring and predictive performance estimates, while smart products – that is, products that know when they were made, by whom, what ingredients they include, and so on – can improve quality control. Yet, it can be challenging to convince oneself of the integrity of IIoT devices after exposing them to the Internet. "Further research is required to develop and design appropriate [Industrial] IoT security mechanisms, including novel isolation primitives that are resilient to run-time attacks, minimal trust anchors for cyber-physical systems, and scalable security protocols."[16]

- Third-party vendor access – outside vendors are often employed to aid in various engineering support activities such as system improvement, training and predictive maintenance. This poses a further risk should the vendor (or its client organisation) not adhere to a rigorous cyber security culture. The integrity of the vendor's cyber security practice should be subject to audit and penalties for not adhering to contractual requirements around cyber security.

- Enterprise management systems – to enable real-time monitoring of production processes, a corporate office will have an uptime/downtime and production count reporting system; these systems are a potential entry point for attackers who are trying to pivot (move from one network segment to another) from a corporate environment into the control system. The integrity of the network after the addition of new devices and systems at the border is critical, and the business should have methods of continually verifying the integrity of IIoT devices, or consider buying other devices that provide integrity verification in an easy-to-use manner.

- Network architecture – the use of firewalls, intrusion detection systems and user privileges can increase or decrease an OT system's security depending on how they are deployed. Once again, integrity plays a role, in this case maintaining and verifying the network, and what devices people have access to.

- Testing costs – the security of many commercially successful off-the-shelf products has steadily improved over time as a result of mutually beneficial security testing by independent security professionals. The popularity of a product, such as a smartphone or a virtual assistant, and its level of availability, may inspire a penetration tester to interrogate that product for system weaknesses, leading to a growth in the tester's reputation and a boon for the product vendor. The reverse is true of OT equipment, as widely used systems rarely have any brand recognition outside industrial engineering circles, and equipment is expensive or cumbersome for a researcher to acquire for testing purposes. Many OT products are therefore under-examined because there

[15] J. Fruhlinger (2018). The Mirai Botnet Explained: How IoT Devices Almost Brought down the Internet. CSO Online.

[16] A. Sadeghi, C. Wachsmann, and M. Waidner (2015). Security and Privacy Challenges in Industrial Internet of Things. 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), 1–6.

is too little impetus for independent security testing. A further difficulty in adequately testing OT systems is that they are often inconveniently located in remote buildings, oil platforms or top-secret locations; access may require special authorisation and trained personnel. This contributes to extra cost and potential delays in the identification and subsequent resolution of problems. Add to this the management principle of “if it ain’t broke, don’t fix it” and the differences between IT system maintenance, renewal and security landscape and OT systems become evident. These differences must be recognised if effective mitigation strategies are to develop.

- Potential for physical consequence – it is possible to cause physical effects, even to damage expensive and logistically difficult-to-replace equipment by exploiting OT systems. The integrity of our safety systems in the presence of an adversary is a crucial goal for society and a huge opportunity for research in industrial systems. Safety protects us from murphy, and security from malice, but the two are developed in intellectual isolation and yet must work hand in glove for the future.

Cyber threat case studies

Automotive manufacturing plant goes offline because of Internet worm (2005)

In 2005 an Internet worm called Zotob infected the Windows 2000 operating systems at several automobile manufacturing plants, taking 13 of them offline for up to 50 minutes.[17] The worm made its way from the company network into the control network and was then able to travel from plant to plant. The impact was minimal, at only $14 million, as a patch was readily available to remedy the situation.[18] This case study highlights the risks of poor network segmentation between the front-office IT systems and the manufacturing-floor OT systems, and further illustrates what we said earlier about maintaining the integrity of the network in the presence of a problem.

Cyber-physical attacks affecting upstream service providers (2015 and 2016)

On 23 December 2015 a power outage occurred affecting three regional electricity distribution companies and interrupting service to an estimated 225,000 customers.[19] The Computer Emergency Response Team confirmed that the outage occurred and identified the malware as being from the BlackEnergy campaign.[20] This was the first known instance of a cyber attack causing a blackout. The malware was delivered via a phishing attack gaining access to the companies’ computers and remotely controlling the ICS systems to disconnect the substation breakers, disabling the power supply. At least thirty substations were disconnected for up to three hours.[21]

[17] P. F. Roberts (2005). Zotob, PnP Worms Slam 13 DaimlerChrysler Plants. eWEEK.

[18] Tofino (2009). Daimler Chrysler-Cyber Security Incident Case Profile.

[19] ICS-CERT (2016). Cyber-Attack Against Ukrainian Critical Infrastructure Alert (IR-ALERT-H-16-056-01).

[20] A. Cherepanov (2016). BlackEnergy by the SSHBearDoor: Attacks against Ukrainian News Media and Electric Industry. WeLiveSecurity.; F-Secure Labs Security Response (n.d.). BlackEnergy & Quedagh: The Convergence of Crimeware and APT Attacks. TLP: White.

[21] R. M. Lee, M. Assante and T. Conway (2016). Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case. TLP: White. Washington,

DC: SANS ICS and E-ISAC.

The following December 2016 saw another cyber-induced power outage. This outage only lasted approximately one hour. The malware responsible for the 2016 power outage was named “Industroyer” or “Crash Override”, which has the potential to automate blackouts, a capability not yet seen in practice.[22]

Cyber-physical attacks on upstream businesses that you depend upon can be as disruptive as attacks to your own systems. The insurance industry offers coverage for this exposure as contingent business interruption service provider interruption; yet in order for coverage to activate, physical damage must occur at the service provider’s facility. The definition of physical damage is still being tested in the US in relation to power outages and CBI. Furthermore, this case study is an example of external dependencies, a potential cyber risk for manufacturers.

Safety system attacks at petrochemical facilities (2017)

In late 2017 a destructive malware, termed Triton or Trisis, targeted a single petrochemical facility. Triton was designed to undermine ICS safety instrumented systems (SIS) and under the right circumstances could result in physical destruction.[23] The malware enabled attackers to remotely control the SIS targeting the Triconex safety controller by Schneider Electric. Reports indicate that the plant shut down initially in June 2017 and again in August 2017, and it is believed that the attackers were in the system long before the shut-down. Schneider Electric has released a patch to address the zero-day vulnerability used in the attack. This is the first known incident of a cyber attack violating safety instrumented systems, and it provides us with a key example of why we must focus on integrity. If it were easier to verify the integrity of the firmware of the SIS, it might have been quicker to detect and thwart these attacks.

Aluminium manufacturer shuts down production because of malware (2019)

LockerGoga malware began attacking the corporate network on 10 March 2019, affecting 40 locations globally.[24] LockerGoga variants were reported to change the password of all user accounts on the infected Windows workstation to “HuHuHUHoHo283283@dJDâ€”, including the local admin account password, thus restricting access to the key systems needed to operate their aluminium manufacturing facilities. They were operating in manual mode at 100 per cent of normal production within one week of the attack, except for the one division that was the most impacted, which was still only at 85–90 per cent capacity, with an entire unit at a standstill as of 12 April 2019, nearly five weeks after the attack.[25] The attack was reported to the national government and security agency, highlighting how seriously governments can take attacks on the manufacturing sector. The aluminium manufacturer, “which likely had a reasonable security stack…got wiped out anyway”.[26]

[22] A. Greenburg (2017). Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid. WIRED.

[23] B. Johnson et al. (2017). Attackers Deploy New ICS Attack Framework ‘TRITON’ and Cause Operational Disruption to Critical Infrastructure. FireEye.; Dragos (2017). TRISIS Malware - Analysis of the Safety System Targeted Malware. TLP: White.

[24] Norsk Hydro (2019). Norsk Hydro ASA Webcast 1. (19-3-2019); Norsk Hydro (2019). Norsk Hydro ASA Webcast 2 (20-3-2019); K. Beaumont (2019). How LockerGoga Took down Hydro — Ransomware Used in Targeted Attacks Aimed at Big Business. DoublePulsar.

[25] Norsk Hydro (2019). Update on Cyber Attack March 26; Norsk Hydro (2019). Update on Cyber Attack April 12.

[26] K. Beaumont (2019). How LockerGoga Took down Hydro — Ransomware Used in Targeted Attacks Aimed at Big Business. DoublePulsar.

Although unconfirmed, some have speculated that the ransomware could really be a wiper, intended to obfuscate attribution by destroying evidence of the threat actors' true target within the network. Cisco Talos highlighted that the command and control infrastructure that is often found in ransomware was not in place, as it asks for emails to be sent for payment instructions instead of leaving the customary ransom note, and does not include bitcoin wallet addresses, which could strengthen the wiper argument. LockerGoga does not contain the ability to self-propagate on networks once an initial infection occurs. At least five variant samples are known to be in existence according to ongoing independent research by one of the co-authors.

An engineering consulting company was also hit by LockerGoga in January, yet anti-malware detection systems were still not detecting LockerGoga at the time of the aluminium manufacturing attack (see footnote 26). This case study is a good example of malware that targeted Windows OS systems yet still affected manufacturing operations; it is also a good example of malware that was known prior to the attack and yet not detected by anti-malware systems.

2. Categories of cyber security losses for manufacturers

Taxonomy of cyber losses

In order to understand how the threats described in the previous section might impact a company, a taxonomy of losses is needed. The Cambridge Centre for Risk Studies developed the following taxonomy in 2016 after interviewing numerous cyber security specialists and primary cyber insurers. Utilising a taxonomy such as this can be helpful in estimating the losses experienced from a cyber attack during scenario-planning exercises.

Table 2 - Cyber Loss Taxonomy (Source: Cambridge Centre for Risk Studies)[27]

V1.0 CODE	CYBER LOSS COVERAGE – PRIMARY CATEGORY	DESCRIPTION
1	Breach of privacy event	The cost of responding to an event involving the release of information that causes a privacy breach, including notification, compensation, credit-watch services and other third party liabilities to affected data subjects, IT forensics, external services, and internal response costs, legal costs.
2	Data and software loss	The cost of reconstituting data or software that have been deleted or corrupted.
3	Network service failure liabilities	Third-party liabilities arising from security events occurring within the organisation's IT network or passing through it in order to attack a third-party.
4	Business Interruption	Lost profits or extra expenses incurred due to the unavailability of IT systems or data as a results of cyber attacks or other non-malicious IT failures.
5	Contingent Business Interruption	Business interruption resulting from the IT failure of a third party, such as a supplier, critical vendor, utility, or external IT services provider.
6	Incident response costs	Direct costs incurred to investigate and close the incident to minimise post-incident losses. Applies to all the other categories/events.
7	Regulatory and defence coverage	Covers the legal, technical or forensic services necessary to assist the policyholder in responding to governmental inquiries relating to a cyber attack, and provides coverage for fines, penalties, defence costs, investigations or other regulatory actions where in violation of privacy law, and other costs of compliance with regulators and industry associations. Insurance recoveries are provided where it is permissible to do so.
8	Liability – Product and Operations	Third party liabilities arising in relation to product liability and defective operations.
9	Liability – Technology Errors & Omissions	Coverage for third party claims relating to failure to provide adequate technical service or technical products including legal costs and expenses of allegations resulting from a cyber attack or IT failure.
10	Liability – Professional Services Errors & Omissions	Coverage for third party claims relating to failure to provide adequate professional services or products (excluding technical services and products) including legal costs and expenses of allegations resulting from a cyber attack or IT failure.
11	Liability – Directors & Officers	Costs of compensation claims made against the individual officers of the business, including for breach of trust or breach of duty resulting from cyber-related incidents and can result from alleged misconduct, or failure to act in the best interests of the company, its employees, and its shareholders.
12	Multi-media liabilities (defamation and disparagement)	Cost for investigation, defence cost and civil damages arising from defamation, libel, slander, copyright / trademark infringement, negligence in publication of any content in electronic or print media, as well as infringement of the intellectual property of a third party.
13	Financial theft & fraud	The direct financial loss suffered by an organisation arising from the use of computers to commit fraud or theft of money, securities, or other property.
14	Reputational damage	Loss of revenues arising from an increase in customer churn or reduced transaction volumes, which can be directly attributed to the publication of a defined security breach event.
15	Cyber extortion	The cost of expert handling for an extortion incident, combined with the amount of the ransom payment.
16	Intellectual property (IP) theft	Loss of value of an IP asset, expressed in terms of loss of revenue as a result of reduced market share.
17	Environmental damage	Cover for costs of clean up, recovery and liabilities associated with a cyber induced environmental spill or release.
18	Physical asset damage	First-party loss due to the destruction of physical property resulting from cyber attacks.
19	Death and bodily injury	Third-party liability for death and bodily injuries resulting from cyber attacks.

[27] The table has been reprinted from Cambridge Centre for Risk Studies (2016). Cyber Exposure Data Schema. Cyber Accumulation Risk Management.

For cyber attacks causing physical damage, the loss categories of most concern are: Physical Asset Damage, Death and Bodily Injury, Environmental Damage and Business Interruption. A potential attack targeting a chemical manufacturer that spoofs sensory data for a pressure vessel, violating the integrity of sensor readings, could result in an explosion causing physical asset damage, as well as injury or death to employees.[28] This is the fundamental concern when it comes to OT cyber attacks, namely, the potential to cause physical harm, and it highlights the interconnectedness of physical safety and cyber security.

Traditionally, security research has dealt primarily with threats to confidentiality and virtual harm such as data breaches. Safety has focused on redundancy as a method to prevent harm, but once a safety system is in place corporates have had no reason to doubt its integrity. A new paradigm must emerge where safety and security systems do not allow unsafe operations, but safety systems can guarantee their integrity, and not be abused into a method of bypassing security, or causing greater harm than they should prevent. As safety starts to require security, compliance needs to be supplemented with adversarial thinking. A key implication of Industry 4.0 is, therefore, the need to "unify" safety and security over the coming years for successful implementation.

Cyber loss case studies

Business interruption from malware at a pharmaceutical manufacturer (2017)

A global pharmaceutical manufacturer was hit with the NotPetya, a very infectious malware seen in June 2017. This malware, deployed in an update for MEDoc, an accounting software, affected 16,500 computers globally and combined ransomware and wiper capabilities into one dangerous cyber weapon targeting Windows systems.[29] The cyber attack caused temporary production delays at a facility making a key vaccination, resulting in the company borrowing from the US Center for Disease Control (CDC) stockpile to meet demand.[30] In their 2018 annual report, they estimated a total of $915 million in losses driven by lost sales in 2017 and again in 2018 (see footnote 30). Additional costs include excess production costs, remediation costs within marketing and R&D and the costs of purchasing vaccines from the CDC. All these losses fall into one of two categories from the taxonomy above: Business Interruption and Incident Response Costs. Although not explicitly reported, there is potential that the aggregate loss estimated provided could also include Data and Software Loss.

Physical asset damage from malware at candy manufacturer (2017)

A candy manufacturer reported $187.6 million in losses from NotPetya as a result of damage caused to its hardware and operational software systems, affecting sales, distribution and other financial systems.[31] It lost 1,700 servers and 24,000 laptops because of the malware.[32]

[28] This attack method was proven and discussed in the following presentation by J. Larsen (2015). Remote Physical Damage 101 - Bread And Butter Attacks. Black Hat.

[29] D. Palmer (2017). Petya Ransomware Attack: How Many Victims Are There Really? ZDNet, Accessed 12 May 2019.

[30] Merck & Co. (2018). Merck & Co., Inc. Form 10-K. SEC.gov.

[31] E. Rosen (2018). Manufacturers Remain Slow to Recognize Cybersecurity Risks. The New York Times, sec. Business.

[32] K. McCarthy (2019). Cyber-Insurance Shock: Zurich Refuses to Foot NotPetya Ransomware Clean-up Bill – and Claims It's 'an Act of War'. The Register.

The manufacturer is claiming physical asset damage as the result of a clause in its property insurance that states: "Physical loss or damage to electronic data, programs, or software, including physical loss or damage caused by the malicious introduction of a machine code or instruction".[33] The losses experienced fall into the following categories: Physical Asset Damage, Business Interruption and Incident Response Costs.

Incident response costs high for aluminium manufacturer following cyber attack (2019)

Revisiting the aluminium manufacturer cyber attack discussed above, we now focus on the loss implications of the March 2019 attack affecting 60 locations globally. The event impacted production, resulting in several plants having to operate in manual operation, with some only able to perform limited operations. An April 2019 update states that the administration and financial systems are still impacted and thus the company has delayed its quarterly reporting.[34] The first week of the attack cost an estimated 300–350 million NOK, with no immediate impact to its stock price following the event (see footnote 26). This case study sees losses from Incident Response Costs, Data and Software Loss and some Business Interruption.

[33] R. Armstrong and O. Ralph (2019). Mondelez Sues Zurich in Test for Cyber Hack Insurance. Financial Times.

[34] Norsk Hydro (2019). Update on Cyber Attack April 12.

3. Cybersecurity mitigation approaches

The four main strategies in risk management are to avoid, transfer, mitigate or accept the risks. Several options exist to try to avoid or mitigate the risk exposure for corporates. Below is just a sampling of these options.

- Patch or replace legacy systems
- Remove Default passwords, encryption keys, and certificates before device deployment
- Use strong passwords when possible
- Minimise third party network access, and log access when they do occur
- Continuously verify device, IIoT and network integrity
- Segregate networks, and use anti-virus products where possible
- Maintain logs for investigation, ideally in a remote backup
- Encourage cross communication between internal IT and OT specialists
- Adopt relevant cyber security standards
- Utilise cyber stress test scenarios to estimate potential losses and to test crisis management plans

Cyber scenario stress-test development

Using scenario planning can help prioritise key cyber investments as well as better understand the loss estimation should cyber attacks occur. This is useful for risk mitigation (reducing the exposure of a company prior to the event), loss management (improving the predictive power of potential loss estimation) and for crisis response (mapping the capabilities and needs during a cyber crisis).

The high-level scenario development process includes writing a scenario narrative and estimating losses. Developing the scenario narrative includes conducting background research, interviewing subject-matter experts, creating an event timeline, specifying the footprint and determining the relevant scenario parameters. Meanwhile, estimating the losses can include social, macroeconomic, organisational, investment portfolio and optional insurance losses.

Cyber loss stress tests

The Cambridge Centre for Risk Studies has developed a number of cyber-related stress-test scenarios, which provide a detailed narrative and timeline of events of plausible cyber attacks that corporates could face: a key software failure, cyber-induced power outages and a very contagious malware event. Each of these scenarios could enable internal company conversations about how prepared the organisation is should this event occur. The detailing of the macro and microeconomic losses aids this conversation. The following table provides an overview of each scenario and a summary of the macroeconomic losses.

Table 3 - Cyber Stress-Test Scenarios by Macroeconomic Impact (Source: Cambridge Centre for Risk Studies)

CYBER STRESS-TEST SCENARIO NAME	BRIEF SCENARIO DESCRIPTION	MACROECONOMIC LOSSES IN THE STANDARD SCENARIO VARIANT (FIVE-YEAR GDP@RISK)
Sybil Logic Bomb, 2014	This scenario imagines that a logic bomb is deployed in a key relational database software that is key to the operations of most global corporations. An "information malaise", meaning a distrust of data, affects the global economy in the long term.	$4.5 trillion
US Blackout, 2015	In this scenario, attackers target electricity generators, eventually causing physical damage and an extended power outage for much of the Northeastern US. The direct impacts for manufacturers include the lack of power to continue operations, while the indirect impacts include the potential of limited supplier interactions resulting from third-party failures.	$243 billion
UK Blackout, 2016	A series of cascading power outages caused by a cyber attack affecting an electricity distribution network. Outages impact other sectors such as rail, shipping and communications, and other primary utilities such as water, all of which could have an indirect impact on the manufacturing sector.	£49 billion
Bashe Contagious Malware, 2019	Similar to the NotPetya and WannaCry attacks of 2017, this scenario imagines a malware with much greater reach infecting 30 million devices globally. Manufacturing is the third most impacted sector following retail and health care.	$85 billion

Sources: Cambridge Centre for Risk Studies (2014). Sybil Logic Bomb Cyber Catastrophe Stress Test Scenario. Cyber Stress Test: Catastrophe Scenario; Cambridge Centre for Risk Studies (2015). Lloyd's Business Blackout Scenario. Emerging Risk Report. Lloyd's of London; Cambridge Centre for Risk Studies (2016). Integrated Infrastructure: Cyber Resiliency in Society. Cambridge Risk Framework for Critical Infrastructure Threat Scenario; Cambridge Centre for Risk Studies (2019). Bashe Attack: Global Infection by Contagious Malware. CyRiM Report 2019.

4. Risk transfer mechanisms

When considering risk transfer the most common form is through insurance products, with contracts being an additional option. Of course, risk transfer itself could be accomplished through a variety of means, such as self insuring, or through an insurance captive.[35] This section will summarise the current state of the for profit cyber insurance market, though will generally apply to self insurance and the use of captives as well.

Current state of cyber insurance market for OT systems

It is estimated that the current affirmative cyber insurance market is $6.4 billion in premiums.[36] Cyber insurance coverage offered can either be affirmative, meaning it explicitly covers cyber risk, or non-affirmative or silent, meaning it is not explicit in its coverage. The following definitions are used when discussing these types of policy. [37]

- Affirmative Standalone Cyber Cover – specific standalone policies for data breach, liabilities, property damage and other losses resulting from information technology failures, either accidental or malicious.
- Affirmative Cyber Endorsements – cyber endorsements that extend the coverage of a traditional insurance product, such as commercial general liability.
- Non-affirmative Cyber Exposure: Gaps in Explicit Cyber Exclusions – there are a range of traditional policies, such as commercial property insurance, that have exclusion clauses for malicious cyber attacks caused by nominated perils such as: Fire, Lightning, Explosion and Aircraft Impact (FLEXA).
- Non-affirmative Cyber Exposure: Policies without Cyber Exclusions – many insurance lines of business incorporate "All Risks" policies without explicit exclusions or endorsements for losses that might occur via cyber attacks.

Using the taxonomy of cyber losses provided in Table 2, the Centre reviewed 32 affirmative standalone cyber insurance products in late 2017 to determine the spread of coverage available (see Table 4). The review highlighted that Breach of Privacy, Data and Software Loss and Business Interruption were the top three types of coverage available, with Physical Damage and Death and Bodily Injury towards the bottom of the ranking. An Aon Benfield review found that 140 US insurers and 77 out of 105 Lloyd's Syndicates and Managing Agents are selling cyber insurance.[38] There is limited uptake of cyber insurance beyond the US, where 90 per cent of cyber premiums are written, 4 per cent in Europe and 6 per cent in the rest of the

[35] Captive insurance is a collective of companies looking to specific risks for the group. For more information on captives see PwC. (2017) Captive Insurance. Accessed 29 April 2019.

[36] Estimated by Centre for Risk Studies based on data points provided in O. Ralph (2017). Cyber Insurance Market Expected to Grow after WannaCry Attack. Financial Times.

[37] The following list has been reprinted from Footnote 38.

[38] Aon Benfield (2017). Cyber Update: 2016 Cyber Insurance Profits and Performance; Lloyd's (2017). Cyber Products at Lloyd's.

world.[39] The fastest uptake is seen in health care, professional service and IT sectors, with energy utilities and manufacturing sectors lagging behind.[40]

Table 4 - Cyber Loss Insurance Coverage Categories by % of Primary Insurer Product Offering, 2017 (Source: Cambridge Centre for Risk Studies)[41]

V1.0 CODE	CYBER LOSS COVERAGE CATEGORY	% OF PRODUCTS OFFERING THIS COVER (SAMPLE OF 32)
1	Breach of privacy event	94%
2	Data and software loss	84%
4	Business interruption	78%
15	Cyber extortion	78%
6	Incident response costs	75%
12	Multimedia liabilities (defamation and disparagement)	72%
7	Regulatory and defence coverage	69%
3	Network service failure liabilities	53%
14	Reputational damage	50%
13	Financial theft and fraud	28%
9	Liability – technology errors and omissions	22%
10	Liability – professional services errors and omissions	19%
16	Intellectual property (IP) theft	19%
18	Physical asset damage	19%
19	Death and bodily injury	13%
20a	Cyber terrorism	9%
5	Contingent business interruption	3%
11	Liability – directors and officers	3%
17	Environmental damage	3%
8	Liability – product and operations	0%

Cyber insurance application process[42]

The insurance industry is an advantageous position to encourage manufacturers (and safety assurance practitioners) to improve their cyber security practices as a means of securing insurance coverage. We are already seeing this happen on the IT side as insurers transition from an application-based approach for assessing risk to a highly-protected risk (HPR) approach. An application approach uses lengthy questionnaire forms in combination with underwriting judgement in order to determine risk exposure, while the HPR approach uses an engineering tactic, applying additional diagnostic/risk assessment tools and advisory consulting to determine an organisation's risk exposure, proactively address any areas of concern, and accurately select the best insurance policies. Given the ever-changing cyber

[39] W. Hedrich, G. Wong and J. Yeo (2017). Cyber Risk in Asia-Pacific: The Case for Greater Transparency. Marsh & McLennan.

[40] Advisen and PartnerRe (2017). 2017 Survey of Cyber Insurance Market Trends.

[41] S. Ruffle et al. (2018). Submission to UK Parliamentary Joint Committee on the National Security Strategy: Cyber Security: Critical National Infrastructure Inquiry. Cambridge Centre for Risk Studies.

[42] This entire section has been adapted from the following report Footnote 45.

threat landscape, it is vital to use an HPR approach to accurately evaluate the cyber risk profile of a corporation and to continuous monitor risk exposure.[43] This exposure assessment is typically conducted by third-party cyber security risk mitigation firms with in-house technical knowledge.

This is an interesting trend to watch as it highlights the fact that the traditional application approach to risk assessment is insufficient in capturing the dynamic nature of cyber risk, specifically for OT Systems. An added benefit of the HPR approach is that it encourages a culture of improvement, given that the insurer can ask the client and safety assurance practitioners to implement suggested updates from the detailed cyber security assessment completed by the specialist vendors. It is encouraging that we are seeing this progress on the IT side of risk, but only a small number of insurers are explicitly offering standalone physical damage cyber policies for OT risks. We have not yet seen the insurance industry driving the change required in security culture for OT systems.

Cyber Business Interruption coverage advances and gaps

As cyber risks have advanced so too has Cyber Affirmative BI policies, with some policies covering a selection of the event triggers such as malicious threat actor, unplanned system outage due to negligence and unplanned IT supply chain disruption.[44] Further, it is important to review any exclusions on cyber BI policies that may limit cover. "Many insurers have "failure to patch" exclusions, which exclude any and all coverage for any and all damages in the event that the vulnerability had been previously identified and not patched."[45]

Some degree of insurance cover is provided against OT attacks as part of silent cyber insurance. "Silent" meaning non-cyber policies such as property insurance, that does not exclude a cyber incident under certain cases. Here, nominated perils such as Fire, Lightning, Explosion and Aircraft Impact (FLEXA) will be covered by traditional property insurance policies, even if caused by a cyber attack (unless this cause is specifically excluded in the contract, a practice that is not common at the time of writing). Claims which trigger FLEXA policies will therefore be payable for any physical damage, business interruption and liability. Once aggregated, these costs may be much larger than the original physical loss.

[43] M. Gnatek and Karen Miller. (2016) Changing the Game: An HPR Approach to Cyber.

[44] G. Buck. (2018) Expanding Cyber BI. Risk & Insurance.; JLT. 2018. Cyber Drives Business Interruption Concerns.

[45] Aon Risk Solutions. (n.d.) Client Alert: WannaCry Cyber Attack.

5. Key areas of action for the safe adoption of 4IR technologies in manufacturing

With the advancement of new technologies delivered through the 4th Industrial Revolution, the manufacturing sector needs to review safer ways to adopt these technologies, focusing on cyber security. If integrity cannot be verified within a business, it will be difficult for that business either to verify third parties or justify to their customers that they are safe. Cyber risk seems simple, until you face it daily; thus, in order to truly tackle this issue, a joint effort is needed between industry, policy-makers and researchers across the security and safety communities.

Cyber threat and loss taxonomies

A cyber threat taxonomy detailing the adversary techniques, OT target assets and vulnerable systems with overarching adversary goals provides a common framework for all levels within an organisation to use in order to communicate risks (including those related to safety). This taxonomy can be used by corporates as a checklist of cyber attacks to safeguard against allowing for interesting dialogue around threats currently without mitigation.

Furthermore, the loss taxonomy provided aids in categorising the consequences to the organisation and its balance sheet from cyber attacks, allowing for comprehensive comparisons of which scenarios impact the business most. Again, the loss taxonomy can be used as a checklist when developing internal scenarios or estimating losses from external scenarios.

Cyber scenario stress-test development

The Cambridge Centre for Risk Studies will soon publish its guidelines for developing stress test scenarios, so please watch this space. Using scenario planning can help prioritise key cyber investments as well as better understand the loss estimation should cyber attacks occur. This is useful for risk mitigation (reducing the exposure of a company prior to the event), loss management (improving the predictive power of potential loss estimation) and for crisis response (mapping the capabilities and needs during a cyber crisis). This paper summarises how to develop stress test scenarios and highlights macroeconomic loss estimates for various scenarios developed at the Centre. These losses range from £49 billion for a UK based power outage up to $4.5 trillion for a systemic failure of a key relational database software used extensively by corporates.

One recommended action is to initiate an internal multi-phased scenario. Phase 1 of the project would be to comply relevant external cyber scenarios to your business and, using the loss taxonomy provided, estimate losses. Phase 2 of this project would be to develop company specific cyber scenarios with impacts estimated. Finally, in Phase 3 you would take the most impactful scenarios and schedule a role playing exercise within your corporation where staff members have to go through the motions of the cyber attack from beginning until complete resolution. This is becoming a common practice with the US Pentagon even organising a 6 day event with electricity grid operators to role play a cyber attack on the electricity grid.[46]

Cyber insurance

The current cyber insurance market is small but growing and thus ripe for potential confusion for corporates when trying to assess what coverage to purchase. Some insurers offer an innovative application process, called HPR to accurately evaluate the cyber risk profile of a corporation and to continuously monitor risk exposure, thus limiting the risk for both parties by encouraging security risk mitigation and driving an improvement culture within corporates.

Cyber insurance coverage can be provided via silent policies, traditional property or liability policies that don't explicitly exclude cyber perils and cyber affirmative policies. Affirmative standalone cyber insurance currently focuses on Breach of Privacy, Data and Software Loss and Business Interruption, while the potentially costlier safety exposures manufacturers face of Physical Asset Damage and Bodily Injury and Death are towards the lower end of coverage offerings. Only a few companies offer industrial system specific products, but this is growing. Corporates should review their cyber insurance policies to ensure that the coverage provided is adequate to meet potential exposure to cyber security induced safety incidents.

Conclusions

The academic community needs to focus on research into safety and security cultures. Traditionally, security research has dealt primarily with threats to confidentiality and virtual harm such as data breaches. Safety has focused on redundancy as a method to prevent harm, but once a safety system is in place corporates have had no reason to doubt its integrity. A new paradigm must emerge where safety and security systems do not allow unsafe operations, but safety systems can guarantee their integrity, and not be abused into a method of bypassing security, or causing greater harm than they should prevent. Funding or supporting cyber-related research, either internally or externally, should be a key goal.

Understanding the cyber risks inherent in industrial systems operations, and subsequently the potential losses from events, is key to managing these exposures. The threat and loss taxonomies provided in this paper enable a common language, while scenario stress testing can facilitate conversations that are vital for industry, policy-makers and researchers to have across security and safety communities, encouraging better risk avoidance, mitigation and crisis management. Developing an adequate cyber crisis response is more productive than limiting the scope of potential scenarios to those likely to occur; in other words, expect the unexpected. There is no reason why you cannot rehearse cyber incidents long before they occur!

[46] J. Marks. (2018) Pentagon Researchers Test 'Worst-Case Scenario' Attack on U.S. Power Grid. Nextgov.com. November 13, 2018.

Suggested resources

The following list is a selection of key cyber-related resources for manufacturers with a specific focus on OT systems and components, although one guide on securing IT-related systems has been included in the summary below.

- Consequence-driven cyber-informed engineering – a step-by-step guide developed by Idaho National Laboratories on how to review your "own environments for high-impact events/ risks; identify implementation of key devices and components that facilitate that risk; illuminate specific, plausible cyber attack paths to manipulate these devices; and develop concrete mitigations, protections, and tripwires to address the high-consequence risk". [47]
- Guide to Industrial Control Systems (ICS) Security – the National Institute of Standards and Technology (NIST) has published a detailed guide on how to secure ICS, SCADA, DCS and PLC, or what we have defined as OT technology.[48]
- Critical Manufacturing Sector Cyber Security Framework – the US Department of Homeland Security published a framework on how to identify, mitigate and manage cyber threats to manufacturers.[49]
- 10 steps to cyber security - the UK's National Cyber Security Centre (NCSC) has provided an overview of 10 mitigation techniques that corporates can utilise to limit impacts. Although these mitigation methods focus on IT related vulnerabilities, they are still relevant to the manufacturing sector as two of the case studies have highlighted previously in this paper.[50]
- Industry 4.0: Cybersecurity Challenges and Recommendations – the European Union Agency for Network and Information Security (ENISA) have just released a short guide providing recommendations on 4IR technology challenges including insight into OT huddles.[51]

About the authors

Jennifer Copic leads the University of Cambridge Centre for Risk Studies' research track on multi-threat analysis. Her research interests include scenario stress-test development, regulatory risk and reporting, cyber security loss estimations, emerging risks and insurance-related analysis. Jennifer leads the application framework specification activities for risk dashboards and other visualisation projects for complex data sets to enable organisations to make data-driven decisions.

She holds a BS in Chemical Engineering from the University of Louisville and an MS in Industrial and Operations Engineering from the University of Michigan. Prior to joining the Centre for Risk Studies, Jennifer worked as a systems engineer for General Mills at a manufacturing plant.

Éireann Leverett is a Senior Risk Researcher at the Centre for Risk Studies, where his research focuses on technological disasters and the economic impacts of computer security failures or accidents. He is interested in computer security at scale, security economics, systems security, incident response, critical infrastructure protection, safety, firmware signing, exploit markets, vulnerability management, quality assurance, indicators of compromise, modelling, networks, risk, visualisations and zero knowledge proofs.

He holds a Master of Philosophy degree in Advanced Computer Science from the University of Cambridge and a Bachelor degree in Engineering from Edinburgh University. Prior to work at the Centre for Risk Studies he worked for 3.5 years as an ethical hacker in the industrial system practice of IOActive. He also runs his own company dedicated to cyber risk research and management: Concinnity Risks.

[47] S. G. Freeman, C. St Michel, R. Smith, and M. Assante (2016). Consequence-Driven Cyber-Informed Engineering (CCE). Idaho National Lab. (INL), Idaho Falls, ID (United States), 18 October 2016.

[48] K. A. Stouffer, V. Y. Pillitteri, S. Lightman, M. Abrams and A. Hahn (2015). Guide to Industrial Control Systems (ICS) Security. Special Publication (NIST SP) – 800-82 Rev 2, 3 June 2015.

[49] DHS. (2015). Critical Manufacturing Sector Cyber Security Framework Implementation Guidance.

[50] NCSC (2018) 10 Steps to Cyber Security.

[51] ENISA (2019) Industry 4.0 - Cybersecurity Challenges and Recommendations. Report/Study.

About Policy Links

Policy Links is the knowledge exchange unit of the Centre for Science, Technology & Innovation Policy (CSTI), University of Cambridge. It aims to provide professional advice and education services grounded in the latest academic research to address the needs of policy officials and civil servants working in the areas of technology, manufacturing and innovation policy.

Policy Links is part of IfM ECS, a wholly owned subsidiary of the University of Cambridge. IfM ECS is embedded within the Institute for Manufacturing (IfM), a division of the University of Cambridge Engineering Department.

Policy Links | IfM Education & Consultancy Services | University of Cambridge | 17 Charles Babbage Road | Cambridge CB3 0FS

+44(0)1223 766141 | www.ifm.eng.cam.ac.uk/services/policy-links