Reassuring the Reshoring: a Cyber Risk Management Proposal

by

Tom Finan

The reshoring of manufacturing to the U.S. and other advanced economies has been a slow but steady phenomenon for many years. A combination of government action spurred by COVID-19, changing economics, and increased automation promises to accelerate this trend. Wherever manufacturers locate, however, the sector is one with significant cyber risk for which most companies are unprepared. Reshoring presents the insurance industry with a unique opportunity to help.

Brokers, underwriters and reinsurers should collaborate with manufacturers to develop cybersecurity best practices for reshorers. Companies that implement those best practices successfully should qualify for customized cyber insurance coverage tailored to their specific needs. This "test bed" approach would help create a virtuous cycle of cybersecurity improvement among this small but growing population of companies. Incorporating lessons learned, similar coverage eventually could be extended beyond reshorers to all organizations contending with cyber risk due to converging information technology (IT) and operational technology (OT) systems.

This initiative could have positive impacts in the near and long term. With vetted best practices to guide them, IT- and OT-dependent companies could advance their cybersecurity maturity considerably. As insurance industry confidence in those practices builds over time, the cyber insurance market's capacity to cover related losses would likely expand accordingly. In the process, the cyber resilience of countries worldwide would be immeasurably enhanced.

Reshoring momentum

Government Action

In the ongoing wake of COVID-19, leaders across the U.S. Federal Government have responded with a wave of executive actions, legislative proposals, and other public policy initiatives designed to encourage the reshoring of American manufacturing.[1] Each of these efforts represents increasing bipartisan consensus about the future of global supply chains.[2] Simply put, overreliance on one geographic region to source goods and materials essential to everyday life poses an unacceptable risk to both economic and national security.[3]

In Congress alone, Members have drafted a series of bills establishing tax, grant, and other incentives to encourage the domestic production of personal protective equipment (PPE), medical devices, and pharmaceuticals.[4] Similar legislation seeks the repatriation of 5G network manufacturing, semiconductor assembly, and the provisioning of defense materiel.[5] Other strategically important items for reshoring consideration include the production of industrial magnets, industrial molds, and lithium and lithium-ion batteries as well as the mining of rare earth metals.[6]

Momentum is growing for additional government action. Surging public sentiment favoring domestic re-industrialization is now coinciding with newfound business appreciation of how well local supply chains have performed during the pandemic compared to their less dependable international counterparts.[7] This awakening has led several experts to call for more tax incentives, deregulation, and targeted research and development investment to facilitate the reshoring shift.[8]

Political support for this trend is by no means limited to the U.S. In response to COVID-19, French President Emanuel Macron has said that supply chains will "need to become more French."[9] Germany's health minister likewise wants to minimize "one-sided dependencies [with supply chains] in order to win back national sovereignty."[10] For its part, Japan's national bank has allocated upwards of $2 billion dollars to help its domestic manufacturers reshore from overseas.[11] Australia and South Korea are considering similar moves.[12] The conclusion is clear: the pandemic has initiated a global rethinking of what manufacturing should be conducted and where in order to promote greater resiliency against pandemics and other large scale disasters.

Cost

For their part, American manufacturers had been warming to the idea of reshoring their operations even prior to COVID-19 given rising labor costs and other overseas business challenges.[13] In China, for example, wages for manufacturing jobs tripled between 2005 and 2016.[14] Shipping and logistics costs associated with global supply chains also were increasing.[15] Manufacturer frustration likewise was mounting with Asia-based factories that used unapproved suppliers and components, foreign finished goods that differed from samples, inconsistent product quality, and intellectual property (IP) theft.[16]

Despite these issues, a March 2020 survey revealed that only 10% of American manufacturers had an active interest in reshoring.[17] The pandemic changed everything. Just two months later, in May 2020, a follow-up survey found that that figure had leapt to 64%.[18] In short, the widespread disruption of global supply chains caused by the pandemic quickly transformed what had been a tentative exploration of moving manufacturing homeward into a full-on embrace.[19]

This momentum likely will continue as manufacturers begin to reassess the economics of domestic production. Historically, manufacturers chose to offshore based on a product's final price at the factory door – in other words, the price to actually make it.[20] Given much lower overseas labor costs, that price regularly justified locating factories out of the U.S.[21] Organizations such as the Reshoring Institute, however, argue that manufacturers should use a more comprehensive and revealing metric to inform decisions about where to locate: a product's total cost.[22]

Total cost considers not only the price of labor but also dozens of hidden expenses incurred at every stage of the manufacturing process.[23] The Reshoring Institute's total cost calculator tool accordingly builds in items such as duties and freight rates, travel expenses, inventory carrying costs, warranty expenses, IP loss, impacts on product innovation caused by locating production far from engineering teams, losses related to long delivery times, political instability, and – of particular relevance to the COVID-19 situation – supply chain shocks.[24] These frequently overlooked expenses typically reveal a 20-30% understatement of offshoring costs.[25]

What does this mean for manufacturers considering a return of operations to the U.S. and other advanced economies? The American case is illustrative. If looking just at the historic metric – the price of making something – rising overseas labor costs alone justify reshoring approximately eight percent of overseas manufacturing.[26] Taking a product's total cost into account, however, boosts that percentage to 32%.[27] Subjecting foreign-made products to a 15% tariff, which already is in place against $112 billion in Chinese-made goods, raises the percentage even higher to 46%.[28] Taken together, a strong business case exists today for reshoring almost half of American overseas manufacturing.

Automation

While it predated COVID-19, another key factor accelerating the reshoring trend is the advent of robots and other automation technologies. As a recent report by the Information Technology and Innovation Foundation noted:

> While both developed and developing economies stand to benefit from the next production system . . . higher-wage nations will get more of a productivity boost from these technologies than lower-wage ones. Lower labor costs in developing economies provide less incentive to adopt automation equipment like robotics, and the new production systems enable shorter production runs, smaller factories, and higher productivity – all of which will work in the direction of reshoring to higher-wage nations.[29]

Research by the World Economic Forum confirms this shift, showing a direct correlation between increasing automation and increasing reshoring of production to developed industrialized countries.[30] The Reshoring Institute 2019 Survey of Global Manufacturing demonstrates the same correlation.[31] It found that more than half of manufacturing executives were planning or considering reshoring activities within the next five years.[32] It likewise found that 70% of those executives are considering investments in robotics to improve production efficiencies.[33]

COVID-19 is only speeding this change.[34] As the pandemic continues to reveal global supply chain risks, increasing numbers of manufacturers are investing in automation as a hedge against future disruption shocks.[35] The low cost of robots, in turn, directly incentivizes reshoring by reducing the margin companies can save on labor by offshoring.[36]

Manufacturing at risk

In the Crosshairs

Wherever they do business, manufacturers are a major target of malevolent nation states, cybercriminals, and hacktivists.[37] These cyber-skilled threat actors want to steal their money, IP, and other sensitive data.[38] They see manufacturers as easy marks. The sector is the third most commonly breached industry among the 20 tracked in the latest Verizon Data Breach Investigations Report, ranking just behind financial services and healthcare.[39] Nearly half of all manufacturers report experiencing a data breach or other cyber incident in the last twelve months.[40] Sixty-four percent of industry leaders believe cyber attacks against their companies will increase in the years ahead,[41] and 77% rank cybersecurity as a major priority for their companies going forward.[42] Notably, 89% anticipate that cyber attacks on OT environments will grow in sophistication in the near future.[43]

On this last point especially, manufacturers are right to worry. Among their latest tactics, threat actors are increasingly exploiting cybersecurity gaps caused by the convergence of IT and OT networks.[44] Growing numbers are successfully penetrating Supervisory Control and Data Acquisition (SCADA) and other industrial control systems (ICS), shutting them down, and holding production lines hostage until victims make hefty ransom payments.[45] This and other financially-motivated cybercrimes motivate 73% of all manufacturing sector breaches today.[46]

The secret to this cybercriminal success is straightforward. While IT and OT convergence provides tremendous benefits when it comes to efficiency and productivity, it also exposes manufacturers to much greater vulnerability.[47] Most decades-old SCADA and other ICS that comprise OT networks – now linked to the Internet for the very first time – were not built with cybersecurity in mind.[48] These technologies, moreover, are typically managed by operational specialists who, unlike their IT counterparts, focus more on performance and safety than on security.[49] Many manufacturers accordingly experience a culture clash between their IT and OT teams about how to best prioritize cyber risk, who has final authority to address it, and how.[50] Unresolved friction between the two camps can make it difficult to effect change.

Enterprising threat actors know this and see the infiltration of IT and OT networks as an easy path to cause all manner of mayhem. That mayhem may include Distributed Denial of Service (DDoS) attacks and outright takeovers of unprotected systems that bring production processes to a standstill.[51] Threat actors likewise can remotely manipulate Industrial Internet of Things (IIoT) technologies to cause equipment malfunctions that result in serious property damage, bodily harm, and even environmental pollution.[52] What makes each of these scenarios so pernicious is that they often need only threaten harm in order to successfully extort money from target companies.

These threats work because the potential loss consequences are so high. Manufacturers use key performance indicators – KPIs – to monitor, analyze, and optimize production processes in order to meet business goals.[53] One core KPI is "equipment availability."[54] An equipment availability score of 100%, for example, means that a process is always running during planned production time.[55] The financial impact of unplanned downtime – when equipment is unavailable – can be enormous, with some experts estimating a revenue loss rate as high as $2 million, on average, per four-hour incident.[56] This exerts tremendous pressure on manufacturers. In addition to no revenue being generated during these outage periods, overhead costs continue to mount as production backups multiply.[57]

Making matters worse, a large percentage of manufacturers don't maintain complete and/or recent data and network backups that could be used to reconstitute compromised operations.[58] Initial recovery efforts consequently can involve complex manual processes and out-of-band communications that slow restoration efforts.[59] Many manufacturers likewise lack formalized cyber incident response and recovery plans.[60] Without such plans, it can take days or weeks to get equipment up and running to pre-attack levels.[61] The resulting lost profits, cost of needed repairs and clean-up, contractual payouts, and stock price impacts all combine into huge potential incident expense.[62]

The math for threat actors therefore is easy. They simply measure the anticipated cost of downtime to a particular company against the cost of an extortion or ransomware demand.[63] Having researched their target, threat actors calibrate that demand to a level they believe has a reasonable chance of being paid out of sheer business necessity.[64]

Finally, manufacturers are just as exposed as companies in other sectors when it comes to ransomware attacks on IT systems.[65] These more traditional attacks typically encrypt critical business, customer, and other data that's essential to executing billing, order processing, and other day-to-day client transactions.[66] In response, many manufacturers feel compelled to pay in order to stop a threatened harm from happening or to cut their losses once deployed ransomware begins to corrupt enterprise systems.[67]

Under these circumstances, it's unsurprising that manufacturers recently experienced the steepest increase in ransomware incidents – up 156% between Q4 2019 and Q1 2020 – compared to the all industry average increase of 25% over the same period.[68] It's equally unsurprising that of the 143 ransomware cases that just one consulting firm handled in 2019, manufacturers spent more than any other sector on ransom demands.[69] Specifically, they paid 62% of the $11+ million the firm transferred to threat actors despite their being involved in only 18% of the firm's paid ransom cases.[70]

The risks to manufacturers do not end there. On the IP side of the equation, threat actors regularly conduct cyber attacks to obtain blueprints, confidential business information, design/specification information, distribution strategies, schematics, secret formulas, supply chain data, and details about unique assembly processes.[71] Commercial competitors seeking to avoid the high cost of designing and developing this IP on their own often are eager buyers of these stolen assets.[72] Cyber espionage accordingly motivates 27% of all known manufacturing sector breaches today.[73] Hackers also target manufacturers through "plain old vanilla" cyber intrusions in order to access client and employee personal data that they then use to commit lucrative identity theft and related crimes.[74]

Willis Towers Watson has tracked these trends through an increasing volume of cyber insurance claims filed by clients. According to that data, the average cost of a manufacturing sector cyber event is $2.4 million. Data breaches are the most frequently reported losses and have the largest total amount of associated costs. While less commonly reported, business disruption and ransomware events have a high average severity. The number of claims notifications related to ransomware and phishing attacks have increased significantly in the last year:

- Cybercriminals launched a Ryuk ransomware attack against a large action sports and lifestyle design and manufacturing company. After encrypting the company's network, the attackers made an eight-figure dollar demand to restore access to impacted data and systems. Because its backups were not impacted, the company did not pay. It instead opted to use restoration efforts to return to service. The client nevertheless incurred sizable incident response costs associated with retaining breach counsel, a forensic investigator, a public relations firm, and other vendors assisting with the investigation. The company's cyber and kidnap and ransom (K&R) insurance policies are covering those costs. The client also has submitted a business interruption claim under its cyber insurance policy. In total, it sustained a seven-figure dollar loss.

- Threat actors launched a ransomware attack against a large supply chain management company that encrypted its network. The client's cyber insurance policy included incident response coverage that is paying for its incident response expenses. The policy's third-party liability coverage likewise is paying the client's defense costs related to claims made by several customers alleging violations of the company's Master Services Agreement. The client also will be submitting a business interruption claim under the policy. In total, it sustained a seven-figure dollar loss.

- An employee at a large clothing manufacturer fell victim to a phishing attack which led to the compromise of their email account. The account was used to send emails to other employees as well as outside customers and contacts. Ultimately, a total of six employee email accounts were compromised. The manufacturer's cyber insurance policy covered the client's incident response costs which represented a six-figure dollar loss.

A sector unprepared

While the manufacturing sector's growing commitment to addressing these challenges is a positive development, many companies continue to face systemic challenges that blunt their cyber risk management progress. First and foremost among them is culture. Engineers who have advanced during their careers into key manufacturing leadership roles now drive digital transformation strategies across the industry.[75] As part of that work, they naturally prioritize what they know and value most: the efficiency and productivity of factory operations.[76] While many manufacturers have adopted IT/OT convergence strategies with both goals in mind, they often neglect cybersecurity.[77] This blind spot leaves SCADA and other ICS vulnerable.[78] It also frequently extends to the factory floor. In many organizations, operations managers still do not recognize cyber risk as a potential cause of downtime and business interruption.[79]

Compounding this problem is the fact that manufacturers historically considered themselves to be too "low profile" to merit much attention from threat actors.[80] For this reason, they dismissed cyber risk management as a cost burden that brought little value to daily operations and overall profits.[81] This misperception has its roots in longtime, wall-to-wall media coverage of cyber incidents that involved mainly financial, healthcare, and retail companies.[82] For those sectors, the negative publicity spurred customer demand for increased cybersecurity, a healthy reaction that unfortunately has yet to materialize in manufacturing. [83]

Without this forcing function, many manufacturers continue to discount the value of their data.[84] They likewise have been slow to fully appreciate the potential losses that could arise from threat actors infiltrating their OT systems and leveraging that access for financial gain.[85] This apathy has resulted in a harmful lack of vigilance that has prevented many manufacturers from making cyber risk management the top priority it should be.[86]

The good news is that this dynamic is changing. Industry leaders are now discovering the numerous cybersecurity issues they must address in order to better protect themselves, their customers, and the bottom line:

- The manufacturing sector today lacks a set of agreed-upon cybersecurity best practices.[87] Without them, two-thirds of manufacturers spend the bulk of their time on cyber incident prevention when they should be focusing equally on incident response planning.[88] Without that balance, they're missing a major opportunity to minimize cyber event losses.[89]

- Manufacturing typically runs on operating systems that depend on decades-old software that no longer receives security updates – a major vulnerability that can enable DDoS attacks and total system takeovers.[90] The sector also relies on legacy infrastructure applications that require unsupported platforms for continued operations.[91] Without up-to-date support, manufacturers struggle to develop effective cybersecurity strategies and controls.[92]

- Many sector companies own factories throughout the world.[93] This geographic diversity, while traditionally viewed as a cost-saving strength, makes mapping the attack surface of an entire organization difficult.[94] This complicates manufacturer efforts to prioritize and address cyber risk comprehensively.[95]

- Manufacturers often have little insight into the cybersecurity of their supply chain partners and lack the centrally-managed cybersecurity control over them that's common in other sectors.[96] This makes these third parties prime targets for threat actors seeking to leverage their remote access into manufacturer systems in order to damage, steal, and otherwise threaten harm.[97]

- Cybersecurity education across the sector must mature considerably before it can help drive needed cultural change.[98] Many manufacturers – most of which are small or medium-sized businesses – lack the funds to develop and execute next generation training and other strategic initiatives.[99]

The Wall Street Journal recently surveyed companies across multiple industry sectors about cybersecurity and highlighted several areas where manufacturers lag their peers.[100] Among other shortcomings, less than two-thirds of manufacturers have instituted in-house cybersecurity programs.[101] By contrast, 83% of both professional/business services companies and government/public sector entities have done so.[102] Similarly, only 56% percent of manufacturers have a dedicated budget for cybersecurity compared to 81% of their professional/business service company counterparts.[103] Moreover, less than half of manufacturers employ cybersecurity professionals while 75% of government/public sector organizations have made such hires.[104] When it comes to cyber incident response planning, manufacturers rank dead last.[105]

Cyber resilience through cyber insurance

Despite these cybersecurity deficiencies, cyber insurance can help put manufacturers on a solid improvement track. To this end, the Wall Street Journal further observed that companies that purchase policies typically are more cyber secure than peers, particularly when it comes to cyber preparedness.[106] "Simply having insurance suggests businesses have assessed their risk, understand their critical data assets and are aware of the potential for disruption if attacked," the paper noted.[107] "The businesses may also be making efforts to decrease their insurance premium by taking risk-reduction measures.[108] More and more companies are purchasing coverage in order to avail themselves of generous pre- and post-breach services that can advance a company's cyber risk management position.

To be clear, coverage alone does not make a company more secure. Instead, it creates an invaluable opportunity for cybersecurity collaboration. Specifically, the application, underwriting, and renewal *process* can help open up needed conversation among an organization's key leaders about how to best mitigate cyber vulnerabilities. This process – which involves questions, advice, and input from a company's broker and underwriter(s) – quickly highlights critical cyber gaps. In so doing, it helps make the business case for responsive cybersecurity investments that reduce potential loss. Those investments, once implemented, boost not only a company's cyber resilience but also the likelihood that it will obtain coverage on the most favorable terms possible. In short, the insurance process can catalyze a virtuous cycle of cybersecurity improvement, one where companies constantly enhance their cyber risk postures in return for continued access to quality coverage.

Given these clear cyber risk management benefits, the Wall Street Journal found that 67% of health care companies currently purchase cyber insurance.[109] Other analyses show the education sector close behind with a 66% uptake rate,[110] with hospitality and gaming companies at 61%.[111] Just over half of communications and technology firms buy the coverage.[112] By contrast, only 30% of surveyed manufacturers have purchased a policy.[113]

We must do better. The insurance industry should partner with the manufacturing sector to develop a strategy that makes improving the cybersecurity of sector companies its centerpiece. Starting with reshorers, the strategy – comprised of both consensus-based best practices and tailored cyber insurance coverage – could radically improve both the cyber risk management position of individual manufacturers and resilience globally.

Core coverage

The good news is that the building blocks for such a strategy already exist. Cyber insurance for manufacturers is available and expanding as property and other traditional policies increasingly exclude cyber losses. While cyber coverage categories continue to evolve, the following dozen – which typically are covered but can vary – respond directly to losses of particular relevance to reshorers as well as the broader manufacturing base:

- Business Interruption and Extra Expense. Covers a manufacturer's lost income and extra expense associated with its inability to prevent a disruption to its OT and/or IT network(s) caused by a cyber attack or programming or software failure either (1) on its network(s); or (2) at a third party provider hosting the manufacturer's application. Contingent Business Interruption and Extra Expense extends the same coverage to situations where a manufacturer's business is interrupted because of a disruption to a third party provider's OT and/or IT network(s).

- Cyber Extortion/Ransomware. Pays credible extortion/ransomware demands and related response costs in response to cybercriminal threats to release or destroy a manufacturer's private information and/or to take down its network/operations. Coverage also provides access to ransom negotiator services.

- System Failure. Covers a manufacturer's lost income and extra expense associated with unintentional and unplanned outages of its OT and/or IT network(s), including but not limited to administrative or programming errors, that are not part of or caused by a security breach. Contingent System Failure extends the same coverage to situations where a manufacturer's business is interrupted because of a disruption to a third-party provider's network(s) associated with an unintentional and unplanned outage that is not part of or caused by a security breach.

- Cyber Property Damage. Pays for the physical loss or damage to a manufacturer's tangible real and personal property, excluding data, that occurs as a result of a failure or violation of the security of the manufacturer's computer system, including OT, SCADA, and other ICS. Cyber property damage covers the loss of use of electronic equipment due to the introduction of code which reprograms software, including the firmware of such equipment, rendering it useless for its intended purpose.

- Cyber Bodily Injury. Covers damages and claim expenses arising from a bodily injury claim against a manufacturer alleging the failure or violation of the security of the manufacturer's computer system, including OT, SCADA, and other ICS.

- Regulatory Shutdown. Pays a manufacturer for its income loss and extra expenses arising from the regulatory shutdown of its computer system, including OT, SCADA, and other ICS. A

regulatory shutdown means a total or partial shutdown of such system(s) necessary to comply with an enforceable legal or regulatory order from a governmental agency or authorized data protection authority resulting from an actual or suspected failure or violation of the security of that/those system(s).

- Voluntary Shutdown. Covers a manufacturer's lost income and extra expenses arising from the voluntary shutdown of its computer system, including OT, SCADA, and other ICS. A voluntary shutdown means an intentional and discretionary total or partial shutdown of such system(s) done with the reasonable belief by a member of the manufacturer's "control group" that such shutdown is likely to mitigate, minimize, or avoid the loss that would otherwise be incurred as a result of a potential failure or violation of the security of that/those system(s). Control group members include the manufacturer's Chief Executive Officer, Chief Financial Officer, Chief Information Officer, Chief Privacy Officer, Chief Security Officer, Chief Information Security Officer, Data Protection Officer, Chief Technology Officer, Risk Manager, Insurance Manager, General Counsel, or their functional equivalent(s).

- IP Theft/Loss. Provides manufacturers with agreed value, first-party coverage for the theft, disclosure, and/or misappropriation of its trade secrets.

- Cyber Incident Response Expenses. Covers a manufacturer's direct first-party expenses – usually on a reimbursement basis – to mitigate a security or privacy incident. Those expenses may include forensic costs (to understand the scope and extent of the incident), legal costs, public relations, notifications to impacted individuals, credit and identity monitoring services, and call center expenses.

- Privacy Injury Liability. Pays losses associated with a manufacturer's inability to protect third party personally identifiable information (PII) or corporate confidential information. Such information can be in any format (online or offline) and breached intentionally or negligently by any person, including third-party service providers to which the manufacturer has outsourced information. Subject to terms and conditions, the policy will defend the manufacturer and pay on its behalf to settle the action or the resulting damages.

- Network Security Liability. Pays losses associated with a manufacturer's inability to use or access its network on which a third party's business relies; the infection of networks of others via a manufacturer's network; information damage to other networks via a manufacturer's network; and/or the inability of others to rely upon the accuracy, validity, or integrity of their information residing on that network. Subject to terms and conditions, the policy will defend the manufacturer and pay on its behalf to settle the action or the resulting damages.

Clarifying confusion

Last year, the media reported extensively on an insurer's refusal to pay for losses stemming from the NotPetya cyber attacks of 2017.[114] The malware – a military-grade worm that spread uncontrollably after initially attacking targets in Ukraine – caused an estimated $10 billion dollars in damages to construction firms, energy and transportation companies, hospitals, and manufacturers.[115] Sensational press reports implied that cyber insurance would not cover these losses given suspected state actor involvement, leaving companies exposed to an alarming new threat.[116] That implication was wrong.

As an initial matter, the policy in question was a traditional property policy, not a cyber policy.[117] Property underwriters never intended their forms to cover the full range of cyber losses that companies have incurred in recent years and therefore did not design limits, premiums, or retentions to capture them.[118] By contrast, cyber insurance policies squarely address those losses by design.[119] Moreover, the insurer in question denied coverage under the property policy's war exclusion, a standard provision that applies to hostile or warlike actions by a government or other sovereign power, a military force, or agent(s) of same.[120] While cyber insurance policies include similar provisions, most insurers would be loath to invoke them.[121] Doing so would devalue the policies to such an extent that they'd no longer remain commercially viable products.[122] To Willis Towers Watson's knowledge, no underwriter to date has denied coverage under a cyber insurance policy's war exclusion.

For added measure, cyber insurance policies often include "carve-backs" for cyberterrorism activity.[123] These provisions cover losses arising from actual or threatened cyber attacks conducted on behalf of, or in connection with, a government to – among other things – cause destruction or harm to critical infrastructure or data in order to further some financial, ideological, political, social, or religious objective.[124] A cyber insurance policy with such a carve-back, had it been in place, may well have avoided the NotPetya coverage dispute.

What does this mean for reshorers? An enterprising broker certainly could engage multiple underwriters to build a bespoke cyber insurance policy for a single company that includes all twelve of the aforementioned coverage categories along with a clarifying cyberterrorism carve-back. The accelerating reshoring phenomenon, however, presents a unique opportunity to forge something new for the greater good. That "something" is a unified package policy that directly links the award of meaningful cyber coverage for these companies to demonstrated cybersecurity improvement.

Building best practices: a partnership proposal

Manufacturers today need a roadmap for better and more cost-effective cybersecurity. As a first step, the insurance industry and sector representatives should establish a working group to develop a series of consensus-based cybersecurity best practices for reshorers. The group – Partnering Reshorers and Insurance for Manufacturing Excellence in Cybersecurity (PRIME-C) – should collaborate to incorporate those practices into a unified package policy designed to meet the risk transfer needs of that distinct subset of companies. Reshorers thus could serve as a test bed to achieve one of the insurance industry's longest standing goals: reward companies that manage cyber risk well with more coverage at lower premiums. Reshorers that implement the best practices, and demonstrate cybersecurity improvement over time, should be so rewarded. Once specific controls emerge as "best in class," underwriters could then extend the policy to all IT- and OT-dependent companies.

This initiative could help reshorers "leapfrog" across the cybersecurity maturity continuum, enabling them not only to catch up to but also surpass their peers in other sectors. As noted previously, however, while reshoring costs are not nearly as high as conventional wisdom would assume, manufacturers do not have unlimited resources. To justify cybersecurity investment, they must maximize their risk management return on every cybersecurity dollar they spend. The development of best practices therefore must be pursued with three overarching priorities in mind:

- Identify cyber threats especially relevant to reshorers based on known threat actor tactics, techniques, and procedures;

- Prioritize immediate, mid-term, and longer-terms plans of action to mitigate corresponding cyber vulnerabilities; and
- Align investment designed to tackle those threats and vulnerabilities in ways that support the successful accomplishment of business goals and objectives.

Cyber threat agenda

The PRIME-C group should start by focusing its attention on the portions of the cyber "kill chain" where well-positioned controls could stop threat actors in their tracks.[125] To do so, the group's agenda should include a laser-like focus on tactics, techniques, and procedures (TTPs), the means by which known threat actors conduct their nefarious activities. Because TTPs are hard to change, they tend to remain constant over time.[126] That constancy is a bonus for cyber risk management. It enables greater predictability about how certain threat actors will likely advance an attack. That predictability, in turn, supports the business case for investing in the controls most likely to thwart threat actor behavior.

To aid its efforts, the PRIME-C group should consider incorporating the MITRE Corporation's (MITRE) Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework into its cyber threat discussion.[127] ATT&CK defines threat actor groups and incorporates TTP input about them from private and public sector contributors worldwide, creating a one-of-its-kind database available to all.[128] Once focused exclusively on data privacy events, MITRE recently expanded the ATT&CK database to include OT-related cyber incidents.[129] Given the richness of this data, the PRIME-C group should further consider engaging MITRE to develop threat analyses tailored specifically to reshorer needs. Such analyses should clarify which threat actors are most likely to attack and what responsive controls would provide the greatest cybersecurity benefit over time. Armed with this insight, underwriters could then require those controls as a condition for coverage under a unified package policy.

As a further potential best practice, the PRIME-C group should consider encouraging reshorer adoption of STIX/TAXII-supported cyber threat intelligence platforms to help their security teams assess, analyze, and respond to rapidly developing cyber attack situations. The STIX-TAXII standards, created by MITRE and the U.S. Department of Homeland Security, provide a common cyber threat intelligence language and transport method so contributors can share up-to-the-minute threat information at machine speed.[130] Companies can use this continuously updated information to detect threat actors early in the attack cycle – e.g., at the reconnaissance, planning, and scanning stages – before they gain access to internal networks and deploy their exploits.[131]

Finally, the PRIME-C group should explore the possibility of obtaining threat information through a partnership with the Global Manufacturing Information Sharing and Analysis Organization (GM-ISAO). The GM-ISAO is a non-profit, member-led organization that collaborates with Federal, State, local, and tribal governments on cyber resilience issues.[132] The PRIME-C group could engage the organization on opportunities to promote cyber risk information sharing that's particularly relevant to reshorers. [133] It likewise could explore the GM-ISAO's interest in developing risk analyses that inform the cybersecurity investment strategies of those companies.[134]

Cyber vulnerability agenda

On the vulnerability front, the PRIME-C group should place particular emphasis on bridging the IT and OT system divide. To help set investment priorities, the group should review the International Society of Automation's (ISA) 62443 standards – the only international standards for Industrial Automation and

Control Systems (IACS) cybersecurity – as a potential source for best practices development.[135] Taking a truly holistic approach, the standards speak not only to controls system technology (i.e., SCADA and other ICS) but also to the people and work processes needed to ensure its safety, integrity, and reliability.[136] As ISA guidance notes, "Without people who are sufficiently trained, risk-appropriate technologies and countermeasures, and work processes throughout the security lifecycle, an IACS could be vulnerable to cyber attack."[137]

The ISA 62443 standards have been adopted by the International Electrotechnical Commission (IEC) and are recognized internationally by both government regulators and the commercial sector.[138] They've also been included as reference standards in such works as the National Institute of Standards and Technology (NIST) Cybersecurity Framework (NIST CSF), ENISA, and the United Nations Economic Commission for Europe (UNECE) Common Regulatory Framework on Cybersecurity.[139] Given the standard's NIST CSF connection, the PRIME-C group also should pay special attention to NIST's recently updated "Cybersecurity Framework Manufacturing Profile" as a further source for developing the best practices.[140] The Profile provides detailed guidance on how manufacturers can implement the NIST CSF and cites the ISA 62443 standards extensively.[141]

As a further resource for its vulnerability discussions, the PRIME-C group should assess how reshorers could best avail themselves of the National Vulnerability Database (NVD). The NVD is the most comprehensive database of reported known software vulnerabilities that have or could be exploited by threat actors.[142] Operated by NIST, it provides an easily searchable interface and data feeds that companies can use to learn about the hundreds of new vulnerabilities submitted every month by government agencies, private companies, and the public.[143] To prioritize vulnerabilities for remediation, manufacturer security teams can integrate NVD data with additional information such as threat intelligence feeds, cyber risk trend information, and third party vendor-reported information.[144]

In addition, the PRIME-C group should consider discussing how to promote more robust cyber risk cultures within reshorer companies. The human element of cyber risk is a growing concern. Willis Towers Watson cyber claims data shows that an organization's employees are the direct cause of 63% of all cyber incidents – through accidental disclosure, social engineering scams, inadvertent ransomware infection, and even malicious intentional behavior. Given the vulnerability that employees represent, manufacturers need to assess and analyze the elements of their workplace cultures that shape both positive and negative cyber attitudes and behaviors.

To that end, Willis Towers Watson researchers are well-versed in this area. Each year, they conduct employee engagement surveys for over 700 companies worldwide that include about seven million people. After exhaustive study and analysis, they've identified four cultural indicators of higher-than-average cyber risk: lack of customer focus, poor adaptability, low empowerment and inadequate training and compensation.[145] The criticality of these four aspects of employee experience makes clear that cybersecurity – for IT and OT networks – should not remain the exclusive domain of CISOs, CSOs, and other technical professionals. On the contrary, HR leaders are the experts in workplace culture and must join the fight.

The PRIME-C group therefore should invite HR leaders into the best practices development process to help address these employee experience areas. HR leaders should bring their expertise to bear on the IT/OT culture divide and define governance and other human capital-based approaches to promote collaboration on the factory floor. Those approaches could include creating an IT/OT security integration body to identify key cyber risks, aligning IT and OT teams through cross-training about each other's

disciplines, and developing an integrated policy framework that gets IT and OT teams using the same language and collaborating on projects.[146]

Investment agenda

Lastly, the PRIME-C group should develop best practices that encourage reshorer adoption of enterprise risk management (ERM) approaches to cybersecurity. Executives have increasingly realized that the central goal of a truly effective cyber risk management program should be to ensure it supports the successful accomplishment of their organizations' key business goals and objectives. ERM enables them to put cyber risk into that business context.

To attain that assurance, the PRIME-C group should establish a cross-functional approach that engages key leaders across an enterprise, including but not limited to the Chief Security Officer, the Chief Information Security Officer, the Chief Information Officer, the Chief Risk Officer, the Chief Human Resources Officer, the General Counsel, and the Chief Financial Officer. Each will have a unique take on their company's mission critical functions that must perform without interruption, sensitive data that must be prioritized for protection, and the potential losses that a serious cyber incident could cause. Each also will know what cyber risks keep them up at night, which can be tolerated, and which intolerable risks should be prioritized for action.

When building the best practices, the PRIME-C group should determine how to best engage these leaders – through surveys, interviews, and otherwise – in order to identify areas of agreement and disagreement. The group likewise should include recommendations for reshorers on how to convene and structure conversations that drive toward consensus around IT and OT cybersecurity priorities and related investment strategies.

Conclusion

Manufacturing long avoided the kinds of damaging cyber attacks suffered by most other industry sectors. That has changed. Increasing threat actor awareness about the vulnerabilities that accompany IT and OT convergence – and how to exploit them – now places sector companies in serious jeopardy of financial loss. Threat actor appreciation of the value of manufacturer IP and other sensitive data likewise has spurred a surge of damaging cyber-enabled thefts that put companies at further risk.

By engaging manufacturers through a resilience-focused cyber insurance initiative, focused first on reshorers, the insurance industry could help the sector improve its cyber risk management game in a comprehensive and cost-effective manner. Linking the successful implementation of a new set of best practices to meaningful coverage would create a virtuous cycle of cybersecurity improvement that will make everyone safer. The conversation should begin now. A more cyber secure world awaits!

---

[1]Wiley.law. 2020. *Summary Of Recently Proposed Reshoring, Manufacturing, And Buy America Initiatives*. [online] Available at: https://www.wiley.law/assets/htmldocuments/summary-of-recently-proposed-reshoring-manufacturing-and-buy-america-initiatives.pdf; [Accessed 8 July 2020]; Pamuk, H. and Shalal, A., 2020. *Trump Administration Pushing To Rip Global Supply Chains From China: Officials*. [online] Reuters. Available at: https://www.reuters.com/article/us-health-coronavirus-usa-china/trump-administration-pushing-to-rip-global-supply-chains-from-china-officials-idUSKBN22G0BZ.

[2] Wiley.law. 2020. *Summary Of Recently Proposed Reshoring, Manufacturing, And Buy America Initiative*; Shalal, A., Alper, A. and Zengerle, P., 2020. *U.S. Mulls Paying Companies, Tax Breaks To Pull Supply Chains From China*. [online] Reuters. Available at: https://www.reuters.com/article/us-usa-china-supply-chains-idUSKBN22U0FH; Sparrow, N., 2020. *US Agency Puts Resources Into Reshoring Medical Manufacturing*. [online] plasticstoday.com.

Available at: https://www.plasticstoday.com/medical/us-agency-puts-resources-reshoring-medical-manufacturing/111652449263250.

[3] Adler, D. and Breznitz, D., 2020. *A Lesson From The Pandemic: It's Time To Reindustrialize The United States*. [online] Barrons.com. Available at: https://www.barrons.com/articles/a-lesson-from-the-pandemic-its-time-to-reindustrialize-the-united-states-51592352083?mod=hp_LATEST; Ferry, J., 2020. *Reshoring Pharmaceutical And Medical Device Manufacturing Would Save Lives, Create Jobs*. [online] MarketWatch. Available at: https://www.marketwatch.com/story/reshoring-pharmaceutical-and-medical-device-manufacturing-would-save-lives-create-jobs-2020-03-30; Sobey, R., 2020. *Coronavirus Fallout: Reshoring Manufacturing Is Key For Economy And National Security, Experts Say*. [online] Bostonherald.com. Available at: https://www.bostonherald.com/2020/04/19/coronavirus-fallout-reshoring-manufacturing-is-key-for-economy-and-national-security-experts-say/.

[4] Thom Tillis U.S. Senator for North Carolina, 2020. *Tillis, Bennet & Hyde-Smith Introduce Bipartisan Legislation To Rebuild The Strategic National Stockpile And Strengthen Domestic PPE Manufacturing*. [online] Available at: https://www.tillis.senate.gov/2020/5/tillis-bennet-hyde-smith-introduce-bipartisan-legislation-to-rebuild-the-strategic-national-stockpile-and-strengthen-domestic-ppe-manufacturing; Lairo, J., 2020. *COVID-19 Crisis Exposes U.S. Vulnerabilities In Its Supply Chain*. [online] Kas.de. Available at: https://www.kas.de/documents/283221/283270/COVID-19+crisis+exposes+U.S.+vulnerabilities+in+its+supply+chain.pdf/22c3b078-8edf-5be6-b95b-463bfefc17ea?version=1.0&t=1591342731401; Williams, A., 2020. *US Lawmakers Push To Reclaim Medical Supply Chains From China*. [online] Ft.com. Available at: https://www.ft.com/content/d71c01db-5333-470b-abcd-0df126864447; Shalal, A., Alper, A. and Zengerle, P., *U.S. Mulls Paying Companies, Tax Breaks To Pull Supply Chains From China*; Sparrow, N., *US Agency Puts Resources Into Reshoring Medical Manufacturing*; Adler, D. and Breznitz, D., *A Lesson From The Pandemic: It's Time To Reindustrialize The United States*.

[5] Palmer, D. and Rodriguez, S., 2020. *Lawmakers Unveil Bill To Boost Semiconductor Production*. [online] POLITICO. Available at: https://www.politico.com/newsletters/morning-trade/2020/06/11/lawmakers-unveil-bill-to-boost-semiconductor-production-788432; Swanson, A. and Clark, D., 2020. *Lawmakers Push To Invest Billions In Semiconductor Industry To Counter China*. [online] Nytimes.com. Available at: https://www.nytimes.com/2020/06/11/business/economy/semiconductors-chips-congress-china.html; Benton Institute for Broadband & Society, 2020. *House Commerce Leaders Applaud Signing Of 5G Security And Broadband Mapping Legislation*. [online] Available at: https://www.benton.org/headlines/house-commerce-leaders-applaud-signing-5g-security-and-broadband-mapping-legislation; Miller, M., 2020. *Lawmakers Introduce Legislation To Boost American 5G Efforts*. [online] The Hill. Available at: https://thehill.com/policy/cybersecurity/494522-lawmakers-introduce-legislation-to-boost-american-5g-efforts; Sparrow, N., 2020. *US Agency Puts Resources Into Reshoring Medical Manufacturing*; Thom Tillis U.S. Senator for North Carolina, *Tillis, Bennet & Hyde-Smith Introduce Bipartisan Legislation To Rebuild The Strategic National Stockpile And Strengthen Domestic PPE Manufacturing*; Adler, D. and Breznitz, D., *A Lesson From The Pandemic: It's Time To Reindustrialize The United States*; Shalal, A., Alper, A. and Zengerle, P., 2020. *U.S. Mulls Paying Companies, Tax Breaks To Pull Supply Chains From China*.

[6] Rubio, M., 2020. *America's Security Needs A Cooperative Rebuilding Of Rare-Earth Supply Chains*. [online] Foreign Policy. Available at: https://foreignpolicy.com/2020/06/17/marco-rubio-rare-earth-minerals-china/; Magnier, M., 2020. *Digging In On Rare Earth, The Next Front In The US Supply Chain War With China*. [online] Sg.news.yahoo.com. Available at: https://sg.news.yahoo.com/digging-rare-earth-next-front-151838481.html: McCafferty, R., 2020. *Manufacturers Think Pandemic Could Lead To More U.S. Work*. [online] Crain's Cleveland Business. Available at: https://www.crainscleveland.com/manufacturing/manufacturers-think-pandemic-could-lead-more-us-work; Rooney, J., 2020. *Could COVID-19 Move More EV Battery Manufacturing To The U.S.?*. [online] Inside EVs. Available at: https://insideevs.com/news/410044/covid-19-ev-battery-production-future/; Vinoski, J., 2020. *Urban Mining Company's Rare Earths Recycling Helps Us Tackle Chinese Dominance*. [online] Forbes. Available at: https://www.forbes.com/sites/jimvinoski/2020/06/11/urban-mining-companys-rare-earths-recycling-helps-us-tackle-chinese-dominance/#5f25212725ea; Webb, S., Shumaker, L. and Oatis, J., 2019. *U.S. Dependence On China's Rare Earth: Trade War Vulnerability*. [online] Reuters. Available at: https://www.reuters.com/article/us-usa-trade-china-rareearth-explainer/u-s-dependence-on-chinas-rare-earth-trade-war-vulnerability-

idUSKCN1TS3AQ; Clad, J., 2020. *The Case For American-Based Resilient Supply Chains*. [online] The National Interest. Available at: https://nationalinterest.org/feature/case-american-based-resilient-supply-chains-163531; Rathke, S. and O'Connell, J., 2020. *Global Supply Chains In The Wake Of COVID-19 In Socially Critical Industries – Is It Time To Reshore?*. [online] The National Law Review. Available at: https://www.natlawreview.com/article/global-supply-chains-wake-covid-19-socially-critical-industries-it-time-to-reshore; Coates, R., 2019. *4 Considerations For Western Companies That Want To Leave China*. [online] Robotics Business Review. Available at: https://www.roboticsbusinessreview.com/manufacturing/china-departure-considerations-reshoring/; Thom Tillis U.S. Senator for North Carolina, *Tillis, Bennet & Hyde-Smith Introduce Bipartisan Legislation To Rebuild The Strategic National Stockpile And Strengthen Domestic PPE Manufacturing*; Shalal, A., Alper, A. and Zengerle, P., 2020. *U.S. Mulls Paying Companies, Tax Breaks To Pull Supply Chains From China*; Sparrow, N., *US Agency Puts Resources Into Reshoring Medical Manufacturing.*

[7] Haley, N. and Simon, B., 2020. *Nikki Haley And Former Walmart U.S. President Bill Simon: Coronavirus Makes The Case For Bringing Manufacturing Back To America*. [online] Fortune. Available at: https://fortune.com/2020/07/18/ppe-manufacturing-jobs-companies-us/; Moser, H., 2020. *COVID-19 Factors Accelerating Reshoring | Modern Casting*. [online] Moderncasting.com. Available at: https://www.moderncasting.com/articles/2020/06/09/covid-19-factors-accelerating-reshoring; Schwaerzler, C., Henderson, G., Patel, J., Manetti, M., Chin, V., Rathore, M., Mahmoudi, M. and Osman, D., 2020. *How Governments Can Galvanize Their Nations For The Rebound*. [online] BCG. Available at: https://www.bcg.com/en-us/publications/2020/three-government-priorities-for-rebuilding-post-covid.aspx; Reynolds, S., 2020. *COVID-19 Pandemic Accelerating 'Re-Shoring'*. [online] Wccftech. Available at: https://wccftech.com/covid-19-pandemic-accelerating-re-shoring/; Adler, D. and Breznitz, D., *A Lesson From The Pandemic: It's Time To Reindustrialize The United States.*

[8] Herman, A., 2020. *Opinion | Bringing The Factories Home*. [online] WSJ. Available at: https://www.wsj.com/articles/bringing-the-factories-home-11595180872.

[9] Belton, K., 2020. *COVID-19 Makes The Case For Resilient Manufacturing*. [online] IndustryWeek. Available at: https://www.industryweek.com/the-economy/public-policy/article/21129255/covid19-makes-the-case-for-resilient-manufacturing; Rathke, S. and O'Connell, J., *Global Supply Chains In The Wake Of COVID-19 In Socially Critical Industries – Is It Time To Reshore?*

[10] Meffert, J., Mohr, N. and Richter, G., 2020. *How The German Mittelstand Is Mastering The COVID-19 Crisis*. [online] McKinsey.com. Available at: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/how-the-german-mittelstand-is-mastering-the-covid-19-crisis#; Belton, K. *COVID-19 Makes The Case For Resilient Manufacturing*.

[11] Rapoza, K., 2020. *Japan Ditches China In Multi-Billion Dollar Coronavirus Shakeout*. [online] Forbes. Available at: https://www.forbes.com/sites/kenrapoza/2020/04/09/japan-ditches-china-in-multi-billion-dollar-coronavirus-shakeout/#64128ab53410; Belton, K. *COVID-19 Makes The Case For Resilient Manufacturing*.

[12] Ibisworld.com. 2020. *Short Supply: COVID-19 Implications For Australian Supply Chains | Ibisworld Industry Insider*. [online] Available at: https://www.ibisworld.com/industry-insider/analyst-insights/short-supply-covid-19-will-have-long-term-implications-for-australian-supply-chains/; Koreaherald.com. 2020. *[Editorial] Unexpected Opportunity*. [online] Available at: http://www.koreaherald.com/view.php?ud=20200506000615; Belton, K. *COVID-19 Makes The Case For Resilient Manufacturing*.

[13] Kapadia, S., 2020. *The 5 Ws Of Reshoring Supply Chains*. [online] Supply Chain Dive. Available at: https://www.supplychaindive.com/news/5-ws-reshoring-supply-chains-diversify-localization/579943/; NWIRC. 2014. *10 Most Commonly Cited Reasons For Reshoring - NWIRC*. [online] Available at: https://www.nwirc.org/most-common-reasons-for-reshoring/.

[14] Buchanan, L., 2020. *Why U.S. Manufacturers Are Turning Their Attention To 'Reshoring'*. [online] Inc.com. Available at: https://www.inc.com/leigh-buchanan/how-american-manufacturers-are-reshoring.html.

[15] Boerner, D., 2020. *Two-Thirds Of North American Manufacturers Say They Want To Reshore Operations. Here's Why.*. [online] Bisnow. Available at: https://www.bisnow.com/national/news/industrial/manufacturers-looking-to-the-us-could-further-boost-industrial-cre-104369; *PLS Logistics Services*, 2016. The State of Reshoring: What Supply Chains Need to Know. Available at: https://www.plslogistics.com/blog/the-state-of-reshoring-what-supply-chains-need-to-know/.

[16] Nash-Hoff, M., 2016. *What Could Be Done About China's Theft Of Intellectual Property?*. [online] IndustryWeek. Available at: https://www.industryweek.com/innovation/intellectual-property/article/22008111/what-could-be-done-about-chinas-theft-of-intellectual-property; Buchanan, L., *Why U.S. Manufacturers Are Turning Their Attention To 'Reshoring'*; *PLS Logistics Services*, The State of Reshoring: What Supply Chains Need to Know.
[17] Boerner, D., *Two-Thirds Of North American Manufacturers Say They Want To Reshore Operations. Here's Why.*
[18] Ma, C., 2020. *Manufacturer Interest In Reshoring, Hiring, And Apprenticeships Increasing During COVID-19 Pandemic [Report]*. [online] Thomasnet.com. Available at: https://www.thomasnet.com/insights/manufacturer-interest-in-reshoring-hiring-and-apprenticeships-increasing-during-covid-19-pandemic-report/ [69%]; Boerner, D., *Two-Thirds Of North American Manufacturers Say They Want To Reshore Operations. Here's Why.*
[19] Rustici, C., 2020. *In The US, Businesses Are Starting To Reshore Their Manufacturing - DirectIndustry E-Magazine*. [online] DirectIndustry e-Magazine. Available at: http://emag.directindustry.com/in-the-us-businesses-are-starting-to-reshore-their-manufacturing-reshoring-nearshoring/.
[20] Gray.com. 2020. *Reshoring In The COVID-19 Storm*. [online] Available at: https://www.gray.com/insights/reshoring-in-the-covid-19-storm/.
[21]Moser, H., 2019. *How TCO Calculations Can Help You Better Assess Your Offshoring vs. Reshoring Options*. [online] Thomasnet.com. Available at: https://www.thomasnet.com/insights/better-assess-costs-risks-of-offshoring-vs-reshoring-by-calculating-total-cost-of-ownership/; Gray.com, *Reshoring In The COVID-19 Storm*.
[22] Martin, H., 2020. *Q&A With Harry Moser, Founder And CEO Of The Reshoring Initiative*. [online] MSCDirect.com. Available at: https://www.mscdirect.com/betterMRO/metalworking/qa-harry-moser-founder-and-ceo-reshoring-initiative; Moser, H., *How TCO Calculations Can Help You Better Assess Your Offshoring vs. Reshoring Option*; Gray.com, *Reshoring In The COVID-19 Storm*.
[23] Moser, H., *How TCO Calculations Can Help You Better Assess Your Offshoring vs. Reshoring Option*.
[24] Gray.com. 2020. *Reshoring In The COVID-19 Storm*; Moser, H., *How TCO Calculations Can Help You Better Assess Your Offshoring vs. Reshoring Option.*
[25] Moser, H., How TCO Calculations Can Help You Better Assess Your Offshoring vs. Reshoring Option.
[26] Gray.com. 2020. *Reshoring In The COVID-19 Storm*.
[27] Ibid.
[28] CNBC.com. 2019. *Trump's 15% Tariffs On $112 Billion In Chinese Goods Take Effect*. [online] Available at: https://www.cnbc.com/2019/09/01/trumps-15percent-tariffs-on-112-billion-in-chinese-goods-take-effect.html; Gray.com. 2020. *Reshoring In The COVID-19 Storm*.
[29] Francis, S., 2019. *Robotics Poised To Increase Productivity And Reshore Manufacturing, Says New Report*. [online] Robotics & Automation News. Available at: https://roboticsandautomationnews.com/2019/10/15/robotics-poised-to-increase-productivity-and-reshore-manufacturing-says-new-report/26295/; Bharadwaj, A. and Dvorkin, M., 2019. *The Rise Of Automation: How Robots May Impact The U.S. Labor Market | St. Louis Fed*. [online] Stlouisfed.org. Available at: https://www.stlouisfed.org/publications/regional-economist/second-quarter-2019/rise-automation-robots.
[30] Krenz, A., Prettner, K. and Strulik, H., 2019. *Industrial Robots Are Bringing Jobs Back Home, But Not For Low-Skilled Workers*. [online] World Economic Forum. Available at: https://www.weforum.org/agenda/2019/06/industrial-robots-are-bringing-jobs-back-home-but-not-for-low-skilled-workers; Petersen, T., 2019. *What Is The Impact Of Reshoring?*. [online] Available at: https://ged-project.de/trade-and-investment/what-is-the-impact-of-reshoring/.
[31] Coates, R., Hobson, D., Levy, A. and Afshar, J., 2019. *Reshoring Institute 2019 Survey Of Global Manufacturing: The Changing Trends Of Reshoring In The United States*. [online] Reshoringinstitute.org. Available at: https://reshoringinstitute.org/wp-content/uploads/2019/05/2019-Survey-of-Global-Mfg.pdf.
[32] Ibid.
[33] Ibid.
[34] Marin, D., 2020. *How COVID-19 Is Transforming Manufacturing | By Dalia Marin - Project Syndicate*. [online] Project Syndicate. Available at: https://www.project-syndicate.org/commentary/covid19-and-robots-drive-manufacturing-reshoring-by-dalia-marin-2020-04.

[35] Guillot, C., 2020. *Coronavirus-Driven Robotics Adoption Could Become A Fixture*. [online] Supply Chain Dive. Available at: https://www.supplychaindive.com/news/coronavirus-robots-robotics-automation-manufacturing-operations/576743/; Marin, D., *How COVID-19 Is Transforming Manufacturing.*

[36] Everett, G., 2020. *BANK OF AMERICA: Here's How Investors Can Position For A 'Tectonic Shift' In Global Manufacturing That Brings More Jobs Home From Abroad | Markets Insider*. [online] markets.businessinsider.com. Available at: https://markets.businessinsider.com/news/stocks/investors-prepare-reshore-global-supply-chains-position-manufacturing-bank-america-2020-2-1028889832#; Aeppel, T., 2019. *U.S. Companies Put Record Number Of Robots To Work In 2018*. [online] Reuters. Available at: https://www.reuters.com/article/us-usa-economy-robots/u-s-companies-put-record-number-of-robots-to-work-in-2018-idUSKCN1QH0K0; Marin, D., *How COVID-19 Is Transforming Manufacturing.*

[37] Garrett, G., 2018. *Cyber Safety: How To Protect Your Company From Cyberattacks In 2019*. [online] EHS Today. Available at: https://www.ehstoday.com/safety-leadership/article/21919933/cyber-safety-how-to-protect-your-company-from-cyberattacks-in-2019.

[38] Verizon. 2020. *2020 Data Breach Statistics By Industry*. [online] Available at: https://enterprise.verizon.com/resources/reports/dbir/2020/data-breach-statistics-by-industry/; SSI Staff., 2017. *Hackers Are Taking Dead Aim At Manufacturers As Cyber Attacks Rise Globally*. [online] Security Sales & Integration. Available at:<https://www.securitysales.com/emerging-tech/cybersecurity-tech/hackers-manufacturers-cyber-attacks/; Hosn, H., 2019. *Why Manufacturing Is One Of The Most Attractive Industries For Cyberattacks*. [online] Manufacturingglobal.com. Available at: https://www.manufacturingglobal.com/technology/why-manufacturing-one-most-attractive-industries-cyberattacks; Mendoza, N.F., 2020. *Cybersecurity Risks In A Possible US Manufacturing Resurgence*. [online] TechRepublic. Available at: https://www.techrepublic.com/article/cybersecurity-risks-in-a-possible-us-manufacturing-resurgence/.

[39] Verizon, *2020 Data Breach Statistics By Industry*.

[40] Presti, K., 2020. *Supply Chain Pivots Need To Start With Cybersecurity*. [online] Manufacturing Business Technology. Available at: https://www.mbtmag.com/security/blog/21138223/supply-chain-pivots-need-to-start-with-cybersecurity.

[41] Tate, P., 2018. *Cyber Risk: The M4.0 Dilemma - Manufacturing Leadership Council*. [online] Manufacturing Leadership Council. Available at: https://www.manufacturingleadershipcouncil.com/2018/12/07/cyber-risk-the-m4-0-dilemma/.

[42] Kurtz, J., 2020. *20 Cybersecurity Statistics Manufacturers Can't Ignore*. [online] NIST Manufacturing Innovation Blog. Available at: https://www.nist.gov/blogs/manufacturing-innovation-blog/20-cybersecurity-statistics-manufacturers-cant-ignore.

[43] MAPI, 2020. *Securing Critical Operational Technology In Manufacturing*. [online] MAPI. Available at: https://www.mapi.net/sites/default/files/Securing%20Critical%20Operational%20Technology%20in%20Manufacturing.pdf.

[44] Low, J., 2020. *Industrial Robots Are Dominating — But Are They Safe From Cyber-Attacks?* [online] TechHQ. Available at: https://techhq.com/2020/08/industrial-robots-are-dominating-but-are-they-safe-from-cyber-attacks/; Thryft, A., 2020. *Critical Infrastructure Cyber-Attacks On The Rise - EE Times Asia*. [online] EE Times Asia. Available at: https://www.eetasia.com/critical-infrastructure-cyber-attacks-on-the-rise/; IT Supply Chain. 2020. *As Cyber Criminals Shift Their Attack Focus, Are Manufacturing Supply Chains At Greater Risk?*. [online] Available at: https://itsupplychain.com/as-cyber-criminals-shift-their-attack-focus-are-manufacturing-supply-chains-at-greater-risk/.

[45] Williamson, J., 2020. *Why Manufacturers Are A Particularly Juicy Target For Cyberattack*. [online] The Manufacturer. Available at: https://www.themanufacturer.com/articles/why-manufacturers-are-a-particularly-juicy-target-for-cyberattack/; Ashford, W., 2017. *Manufacturing A Key Target For Cyber Attacks*. [online] ComputerWeekly.com. Available at: https://www.computerweekly.com/news/450424302/Manufacturing-a-key-target-for-cyber-attacks; Deloitte. 2020. *Manufacturing - Cyber Executive Briefing | Case Studies*. [online] Available at: https://www2.deloitte.com/global/en/pages/risk/articles/Manufacturing.html; Virani, R., 2020. *Manufacturers Industry Targeted: 156% Increase In Cyberattacks In Q1*. [online] Alliant Cybersecurity. Available at: https://www.alliantcybersecurity.com/manufacturers-industry-targeted-156-increase-in-cyberattacks-in-q1/.

[46] Verizon, *2020 Data Breach Statistics By Industry*.
[47] Forde, M., 2019. *71% Of Manufacturers Employ IoT Despite Cyber Risks: PwC*. [online] Supply Chain Dive. Available at: https://www.supplychaindive.com/news/manufacturers-iot-tech-projects-cyber-risk/567658/; Presti, K., *Supply Chain Pivots Need To Start With Cybersecurity*.
[48] Saunders, H., 2017. *5 Steps To Protect Your Factory From A Ransomware Attack*. [online] Gblogs.cisco.com. Available at: https://gblogs.cisco.com/uki/5-steps-to-protect-your-factory-from-a-ransomware-attack/; Ashford, W., *Manufacturing A Key Target For Cyber Attacks*; Presti, K., *Supply Chain Pivots Need To Start With Cybersecurity*.
[49] Geyer, G., 2020. *Fostering Cooperation Between IT Security Teams And OT Personnel*. [online] Blog.claroty.com. Available at: https://blog.claroty.com/fostering-cooperation-between-it-security-teams-and-ot-personnel; Grzadkowska, A., 2019. *Manufacturers' Cyber Risk Is About Far More Than Data Breach*. [online] Insurancebusinessmag.com. Available at: https://www.insurancebusinessmag.com/us/news/cyber/manufacturers-cyber-risk-is-about-far-more-than-data-breach-165097.aspx.
[50] Cappelli, D., 2019. *Integrate Your IT-OT Security Efforts To Protect Against Cybersecurity Threats*. [online] Plantservices.com. Available at: https://www.plantservices.com/articles/2019/automation-zone-integrate-your-it-ot-security-efforts/; Krewson, K. and Carhart, L., 2019. *5 Tips For A Happy Marriage Between IT And OT*. [online] Crowdstrike.com. Available at: https://www.crowdstrike.com/blog/5-tips-for-building-cooperation-between-it-cybersecurity-and-operational-technology-teams/;Geyer, G., 2020. *Fostering Cooperation Between IT Security Teams And OT Personnel*.
[51] Presti, K., *Supply Chain Pivots Need To Start With Cybersecurity*; Grzadkowska, A., *Manufacturers' Cyber Risk Is About Far More Than Data Breach*.
[52] Grzadkowska, A., 2019. *Manufacturers' Cyber Risk Is About Far More Than Data Breach*.
[53] Datapine.com. 2020. *Manufacturing KPIs & Metrics - Explore The Best KPI Examples*. [online] Available at: https://www.datapine.com/kpi-examples-and-templates/manufacturing.
[54] Newton, M., 2017. *KPIs For Industrial Automation And Process Control*. [online] Blog.opto22.com. Available at: https://blog.opto22.com/optoblog/kpis-for-industrial-automation-and-process-control;UpKeep. 2020. *What Are The Best Metrics And KPIs For Manufacturing Companies?*. [online] Available at: https://www.onupkeep.com/answers/asset-management/what-are-the-best-metrics-and-kpis-for-manufacturing-companies/.
[55] Newton, M., *KPIs For Industrial Automation And Process Control*.
[56] Brand, P., 2020. *Downtime In Manufacturing: What's The True Cost?*. [online] Oden Technologies. Available at: https://oden.io/blog/downtime-in-manufacturing-the-true-cost/; Sheridan, K., 2020. *ICS Threat Snake Ransomware Suspected In Honda Attack*. [online] Dark Reading. Available at: https://www.darkreading.com/attacks-breaches/ics-threat-snake-ransomware-suspected-in-honda-attack/d/d-id/1338075.
[57] Immerman, G., 2018. *The Real Cost Of Downtime In Manufacturing*. [online] Machinemetrics.com. Available at: https://www.machinemetrics.com/blog/the-real-cost-of-downtime-in-manufacturing; Brand, P., *Downtime In Manufacturing: What's The True Cost?*.
[58] Slaby, J., 2019. *Ransomware Crushes Another Manufacturing Industry Target*. [online] Acronis.com. Available at: https://www.acronis.com/en-us/blog/posts/ransomware-crushes-another-manufacturing-industry-target.
[59] Sheridan, K., *ICS Threat Snake Ransomware Suspected In Honda Attack*; Slaby, J., *Ransomware Crushes Another Manufacturing Industry Target*.
[60] Sheridan, K., *ICS Threat Snake Ransomware Suspected In Honda Attack*; Saunders, H., *5 Steps To Protect Your Factory From A Ransomware Attack*.
[61] Sheridan, K., *ICS Threat Snake Ransomware Suspected In Honda Attack*; Saunders, H., *5 Steps To Protect Your Factory From A Ransomware Attack*.
[62] Slaby, J., *Ransomware Crushes Another Manufacturing Industry Target*..
[63] Sheridan, K., *ICS Threat Snake Ransomware Suspected In Honda Attack*.
[64] Zafra, D., Lunden, K., Brubaker, N. and Kennelly, J., 2020. *Ransomware Against The Machine: How Adversaries Are Learning To Disrupt Industrial Production By Targeting IT And OT*. [online] FireEye. Available at:

https://www.fireeye.com/blog/threat-research/2020/02/ransomware-against-machine-learning-to-disrupt-industrial-production.html; Sheridan, K., *ICS Threat Snake Ransomware Suspected In Honda Attack*.

[65] Elworthy, R., 2020. *Ransomware And The Manufacturing Industry*. [online] Nuspire. Available at: https://www.nuspire.com/blog/ransomware-and-the-manufacturing-industry/; Higgins, K., 2019. *How A Manufacturing Firm Recovered From A Devastating Ransomware Attack*. [online] Dark Reading. Available at: https://www.darkreading.com/attacks-breaches/how-a-manufacturing-firm-recovered-from-a-devastating-ransomware-attack/d/d-id/1334760.

[66] Elworthy, R., 2020. *Ransomware And The Manufacturing Industry*; Higgins, K., *How A Manufacturing Firm Recovered From A Devastating Ransomware Attack*.

[67] Janofsky, A., 2020. *Which Industries Are Most Likely To Pay Ransomware?*. [online] WSJ. Available at: https://www.wsj.com/articles/which-industries-are-most-likely-to-pay-ransomware-11592606176; Climer, S., 2018. *Why Cybersecurity In Manufacturing Matters: New Tech, New Target*. [online] Mindsight. Available at: https://gomindsight.com/insights/blog/cybersecurity-in-manufacturing-risk/; Virani, R. *Manufacturers Industry Targeted: 156% Increase In Cyberattacks In Q1*.

[68] Beazley.com. 2020. *The Enduring Threat Of Ransomware*. [online] Available at: https://www.beazley.com/news/2020/beazley_breach_insights_june_2020.html.

[69] Coker, J., 2020. *Manufacturing Sector Paid Out 62% Of Total Ransomware Payments In 2019*. [online] Infosecurity Magazine. Available at: https://www.infosecurity-magazine.com/news/manufacturing-ransomware-payments/.

[70] Ibid.

[71] Manganello, K., 2019. *How To Protect Your Manufacturing Assets Against The Growing Threat Of Cybercrime*. [online] Thomasnet.com. Available at: https://www.thomasnet.com/insights/how-to-protect-your-manufacturing-assets-against-the-growing-threat-of-cybercrime/; Hulme, G., 2019. *It's Time Manufacturers Assemble A Sound Cybersecurity Effort*. [online] Security Boulevard. Available at: https://securityboulevard.com/2019/03/its-time-manufacturers-assemble-a-sound-cybersecurity-effort/; Messenger, A., 2018. *Why Cyber Criminals Target The Manufacturing Industry*. [online] Corvid.co.uk. Available at: https://www.corvid.co.uk/blog/why-cyber-criminals-target-the-manufacturing-industry; Verizon, *2020 Data Breach Statistics By Industry*. Ashford, W., *Manufacturing A Key Target For Cyber Attacks*; Hosn, H., *Why Manufacturing Is One Of The Most Attractive Industries For Cyberattacks*; Deloitte, *Manufacturing - Cyber Executive Briefing | Case Studies*; Mendoza, N.F., *Cybersecurity Risks In A Possible US Manufacturing Resurgence*.

[72] Manganello, K., *How To Protect Your Manufacturing Assets Against The Growing Threat Of Cybercrime*; Hulme, G., *It's Time Manufacturers Assemble A Sound Cybersecurity Effort*; Messenger, A., *Why Cyber Criminals Target The Manufacturing Industry*; Verizon, *2020 Data Breach Statistics By Industry*. Ashford, W., *Manufacturing A Key Target For Cyber Attacks*; Hosn, H., *Why Manufacturing Is One Of The Most Attractive Industries For Cyberattacks*; Deloitte, *Manufacturing - Cyber Executive Briefing | Case Studies*; Mendoza, N.F., *Cybersecurity Risks In A Possible US Manufacturing Resurgence*.

[73] Verizon, *2020 Data Breach Statistics By Industry*.

[74] Forsyth, E., 2019. *The 5 Most Common Cybersecurity Threats To Manufacturers*. [online] NIST. Available at: https://www.nist.gov/blogs/manufacturing-innovation-blog/5-most-common-cybersecurity-threats-manufacturers; Manganello, K., 2019. *How To Protect Your Manufacturing Assets Against The Growing Threat Of Cybercrime*.

[75] Hannigan, R., 2019. *Why The Manufacturing Sector Finds Cybersecurity Challenging*. [online] Manufacturing Business Technology. Available at: https://www.mbtmag.com/security/blog/13249322/why-the-manufacturing-sector-finds-cybersecurity-challenging.

[76] Ibid.

[77] Lydecker, D., 2019. *Manufacturers Can't Afford The Cyber Risks They're Overlooking*. [online] Manufacturing Business Technology. Available at: https://www.mbtmag.com/security/article/13251738/manufacturers-cant-afford-the-cyber-risks-theyre-overlooking; Williams, G., 2018. *(Cyber)Securing Manufacturing's Future*. [online] New Equipment Digest. Available at: https://www.newequipment.com/plant-operations/article/22059955/cybersecuring-manufacturings-future.

[78] Tollefson, R., 2020. *ICS/SCADA Malware Threats*. [online] Security Boulevard. Available at: https://securityboulevard.com/2020/04/ics-scada-malware-threats/; Narayanan, S. and Coxon, M., 2018. *It's The Last IT/OT Mile That Matters In Avoiding Industry 4.0'S Pilot Purgatory*. [online] McKinsey.com. Available at: https://www.mckinsey.com/business-functions/operations/our-insights/operations-blog/its-the-last-it-ot-mile-that-matters-in-avoiding-industry-40s-pilot-purgatory; Weiss, J. and Ku, R., 2017. *Industrial Cyber Security: Why IT & OT Collaboration Is No Longer An Option But A Necessity*. [online] IIOT-World.com. Available at: https://iiot-world.com/ics-security/cybersecurity/industrial-cyber-security-why-it-ot-collaboration-is-no-longer-an-option-but-a-necessity/; Brocklehurst, K., 2017. *IT-OT Convergence: Who Owns OT Security?*. [online] Belden.com. Available at: https://www.belden.com/blog/industrial-security/it-ot-convergence-and-conflict-who-owns-ics-security.

[79] Hannigan, R., *Why The Manufacturing Sector Finds Cybersecurity Challenging*.

[80] Neveux, E., 2020. *Five Ways Cyberattacks Put Manufacturing Systems At Risk*. [online] Security Boulevard. Available at: https://securityboulevard.com/2020/03/five-ways-cyberattacks-put-manufacturing-systems-at-risk/; SSI-net.com. 2019. *Why Cyber Security Practices In Manufacturing Needs An Update. Systems Solution, Inc. (SSI)*. [online] Available at: https://www.ssi-net.com/why-cyber-security-practices-in-manufacturing-needs-an-update/; Seqrite Blog. 2019. *The Manufacturing Industry's Major Cybersecurity Challenges*. [online] Available at: https://www.seqrite.com/blog/manufacturing-cybersecurity-challenges/; Lydecker, D., 2019. *Manufacturers Can't Afford The Cyber Risks They're Overlooking*.

[81] Souza, C., 2019. *Manufacturing And Cybersecurity: Know The Essentials*. [online] Nationaldefensemagazine.org. Available at: https://www.nationaldefensemagazine.org/articles/2019/6/14/viewpoint-manufacturing-and-cybersecurity---know-the-essentials.

[82] Bayern, M., 2019. *How US Retailers Can Protect Themselves From Targeted Cyberattacks*. [online] TechRepublic. Available at: https://www.techrepublic.com/article/how-us-retailers-can-protect-themselves-from-targeted-cyberattacks/; Sidel, R., 2014. *Home Depot's 56 Million Card Breach Bigger Than Target's*. [online] WSJ. Available at: https://www.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571; SSI-net.com. 2019. *Why Cyber Security Practices In Manufacturing Needs An Update;* Seqrite Blog. 2019. *The Manufacturing Industry's Major Cybersecurity Challenges*; Lydecker, D., *Manufacturers Can't Afford The Cyber Risks They're Overlooking*.

[83] Climer, S., *Why Cybersecurity In Manufacturing Matters: New Tech, New Target*; Messenger, A., *Why Cyber Criminals Target The Manufacturing Industry*.

[84] Climer, S., *Why Cybersecurity In Manufacturing Matters: New Tech, New Target*; Messenger, A., *Why Cyber Criminals Target The Manufacturing Industry*.

[85] Robinson, P., 2020. *Protecting Manufacturing From Cyber Breaches*. [online] TechRadar. Available at: https://www.techradar.com/news/protecting-manufacturing-from-cyber-breaches.

[86] Imagine IT, Inc. 2020. *The Top 4 Technology Challenges For Small To Midsized Manufacturers In 2020.* Imagine IT, Inc. [online] Available at: https://www.imagineiti.com/the-top-4-technology-challenges-for-small-to-midsized-manufacturers-in-2020/; Weston, B., 2019. *How Small Manufacturing Businesses Drive The U.S. Economy*. [online] Score.org. Available at: https://www.score.org/blog/how-small-manufacturing-businesses-drive-us-economy; Henneberry, B., 2020. *Top Manufacturing Companies In The USA*. [online] Thomasnet.com. Available at: https://www.thomasnet.com/articles/top-suppliers/manufacturing-companies/; SBECouncil.org. 2018. *Facts & Data On Small Business And Entrepreneurship*. [online] Available at: https://SBECouncil.org/about-us/facts-and-data/; Manganello, K., *How To Protect Your Manufacturing Assets Against The Growing Threat Of Cybercrime*.

[87] Climer, S., *Why Cybersecurity In Manufacturing Matters.*

[88] Sloan, R., 2020. *Which Industries Aren't Ready For A Cyberattack?*. [online] WSJ. Available at: https://www.wsj.com/articles/the-industries-most-vulnerable-to-cyberattacksand-why-11592786160; Gold, S., 2020. *With Opportunity Comes Vulnerability*. [online] IndustryWeek. Available at: https://www.industryweek.com/technology-and-iiot/cybersecurity/article/21127200/with-opportunity-comes-vulnerability; Short, T., 2018. *How To Avoid The Worst Manufacturing Cyber Security Risks*. [online] Software Advice. Available at: https://www.softwareadvice.com/resources/avoid-worst-manufacturing-cyber-security-risks/.

[89] Sloan, R., *Which Industries Aren't Ready For A Cyberattack?*;Gold, S., *With Opportunity Comes Vulnerability*; Short, T., *How To Avoid The Worst Manufacturing Cyber Security Risks*..

[90] Kaplan, D., 2020. *From Legacy Systems To Connected Tech, Manufacturers Face Cyber Risks*. [online] Supply Chain Dive. Available at: https://www.supplychaindive.com/news/legacy-systems-connected-technology-manufacturers-cyber-risks/572938/; Pollack, B., 2018. *The Cost Of Aging, Obsolete Systems*. [online] Automation World. Available at: https://www.automationworld.com/factory/oee/blog/13319075/the-cost-of-aging-obsolete-systems; Warren Averett CPAs & Advisors. 2018. *Cybersecurity For The Manufacturing Industry*. [online] Available at: https://warrenaverett.com/insights/cyber-security-manufacturing-industry/; Field, K., 2016. *The Urgent Need To Improve Industrial Internet Security*. [online] IndustryWeek. Available at: https://www.industryweek.com/technology-and-iiot/article/21978359/the-urgent-need-to-improve-industrial-internet-security; Sloan, R., 2020. *Which Industries Aren't Ready For A Cyberattack?*; Presti, K., *Supply Chain Pivots Need To Start With Cybersecurity*.

[91] Vavra, C., 2019. *Upgrading Your Hardware, Software Systems*. [online] Control Engineering. Available at: https://www.controleng.com/articles/upgrading-your-hardware-software-systems/; Lorincz, J., 2018. *Cyber Secure Manufacturing Is Smart Manufacturing*. [online] Sme.org. Available at: https://www.sme.org/cyber-secure-smart-manufacturing; Vickers, D., 2016. *Solving The Legacy Platform Problem*. [online] IT Today. Available at: http://www.ittoday.info/Articles/Solving-Legacy-Platform-Problem.htm; Kaplan, D., *From Legacy Systems To Connected Tech, Manufacturers Face Cyber Risks*; Sloan, R., *Which Industries Aren't Ready For A Cyberattack?*

[92] Sloan, R., *Which Industries Aren't Ready For A Cyberattack?*

[93] Trend Micro. 2019. *The IIOT Attack Surface: Threats And Security Solutions*. [online] Available at: https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/-the-iiot-attack-surface-threats-and-security-solutions; Hannigan, R., *Why The Manufacturing Sector Finds Cybersecurity Challenging*.

[94] Trend Micro. 2019. *The IIOT Attack Surface: Threats And Security Solutions*. [online] Available at: https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/-the-iiot-attack-surface-threats-and-security-solutions; Hannigan, R., *Why The Manufacturing Sector Finds Cybersecurity Challenging*; Hosn, H., *Why Manufacturing Is One Of The Most Attractive Industries For Cyberattacks*.

[95] Trend Micro. *The IIOT Attack Surface: Threats And Security Solutions*; Hannigan, R., *Why The Manufacturing Sector Finds Cybersecurity Challenging*.

[96] Hannigan, R., *Why The Manufacturing Sector Finds Cybersecurity Challenging.*

[97] Korolov, M., 2019. *What Is A Supply Chain Attack? Why You Should Be Wary Of Third-Party Providers*. [online] CSO Online. Available at: https://www.csoonline.com/article/3191947/what-is-a-supply-chain-attack-why-you-should-be-wary-of-third-party-providers.html; Maley, B., 2019. *National Supply Chain Integrity Month: Understanding Third-Party Cyber Risk*. [online] Security Boulevard. Available at: https://securityboulevard.com/2019/04/national-supply-chain-integrity-month-understanding-third-party-cyber-risk/; Ghosh, S. and Kommareddy, S., 2018. *Is Cybersecurity The Weakest Link In Your Supply Chain?*. [online] Manufacturing Leadership Council. Available at: https://www.manufacturingleadershipcouncil.com/2018/12/04/is-cybersecurity-the-weakest-link-in-your-supply-chain/; *Configuring And Managing Remote Access For Industrial Control Systems*. [online] U.S. Department of Homeland Security. Available at: https://us-cert.cisa.gov/sites/default/files/recommended_practices/RP_Managing_Remote_Access_S508NC.pdf; Sloan, R., 2020. *Which Industries Aren't Ready For A Cyberattack?;* Hannigan, R., *Why The Manufacturing Sector Finds Cybersecurity Challenging.*

[98] 2017. *Cybersecurity For Manufacturers: Securing The Digitized And Connected Factory*. [online] Alliance for Manufacturing Foresight and Computing Community Consortium. Available at: http://acemetal.com/wp-content/uploads/2018/04/MForesight-Cybersecurity-Report.pdf; Manganello, K., *How To Protect Your Manufacturing Assets Against The Growing Threat Of Cybercrime*.

[99] Imagine IT, Inc., *The Top 4 Technology Challenges For Small To Midsized Manufacturers In 2020*;Henneberry, B., *Top Manufacturing Companies In The USA*; Weston, B., *How Small Manufacturing Businesses Drive The U.S. Economy*; Climer, S., *Why Cybersecurity In Manufacturing Matters: New Tech, New Target*; SBECouncil.org, *Facts & Data On Small Business And Entrepreneurship*.

[100] Sloan, R., *Which Industries Aren't Ready For A Cyberattack?*

[101] Ibid.

[102] Ibid.

[103] Ibid.
[104] Ibid.
[105] Ibid.
[106] Ibid.
[107] Ibid.
[108] Ibid.
[109] Ibid.
[110] Granato, A. and Polacek, A., 2019. *The Growth And Challenges Of Cyber Insurance – Federal Reserve Bank of Chicago*. [online] Chicagofed.org. Available at: https://www.chicagofed.org/publications/chicago-fed-letter/2019/426.
[111] Insurance Journal. 2020. *Cyber Insurance Sales To U.S. Businesses Picking Up: Marsh*. [online] Available at: https://www.insurancejournal.com/news/national/2020/03/26/562458.htm.
[112] Granato, A. and Polacek, A., *The Growth And Challenges Of Cyber Insurance – Federal Reserve Bank of Chicago*.
[113] Ibid.
[114] Satariano, A. and Perlroth, N., 2019. *Big Companies Thought Insurance Covered A Cyberattack. They May Be Wrong.*. [online] Nytimes.com. Available at: https://www.nytimes.com/2019/04/15/technology/cyberinsurance-notpetya-attack.html; Corcoran, B., 2019. *What Mondelez V. Zurich May Reveal About Cyber Insurance In The Age Of Digital Conflict*. [online] Lawfare. Available at: https://www.lawfareblog.com/what-mondelez-v-zurich-may-reveal-about-cyber-insurance-age-digital-conflict; Osborne, C., 2019. *NotPetya An 'Act Of War,' Cyber Insurance Firm Taken To Task For Refusing To Pay Out | Zdnet*. [online] ZDNet. Available at: https://www.zdnet.com/article/notpetya-an-act-of-war-cyber-insurance-firm-taken-to-task-for-refusing-to-pay-out/.
[115] Brennan, N. and Voses, M., 2020. *The Coming Cyber Pandemic: Part II*. [online] The National Law Review. Available at: https://www.natlawreview.com/article/coming-cyber-pandemic-part-ii; Nash, K., Castellanos, S. and Janofsky, A., 2018. *One Year After NotPetya Cyberattack, Firms Wrestle With Recovery Costs*. [online] WSJ. Available at: https://www.wsj.com/articles/one-year-after-notpetya-companies-still-wrestle-with-financial-impacts-1530095906.
[116] Kisch, M., 2017. *What Do Recent Attacks Mean For OT Network Security?*. [online] Security Intelligence. Available at: https://securityintelligence.com/what-do-recent-attacks-mean-for-ot-network-security/; Brennan, N. and Voses, M., *The Coming Cyber Pandemic: Part II*; Nash, K., Castellanos, S. and Janofsky, A., *One Year After NotPetya Cyberattack, Firms Wrestle With Recovery Costs*.
[117] OECD.org. 2020. *Encouraging Clarity In Cyber Insurance Coverage: The Role Of Public Policy And Regulation - Organization For Economic Co-Operation And Development*. [online] Available at: https://www.oecd.org/finance/insurance/Encouraging-Clarity-in-Cyber-Insurance-Coverage.pdf; Aburish, N., Hsieh, M. and Fixler, A., 2019. *The Role Of Cyber Insurance In Securing The Private Sector - Foundation For The Defense Of Democracies*. [online] FDD. Available at: https://www.fdd.org/analysis/2019/09/11/cyber-insurance/; Gul, S. and Slipsky, M., 2018. *The Art Of (Cyber) War, Or How A Little Known Policy Exclusion Can Nullify Your Insurance Coverage*. [online] Poyner Spruill LLP. Available at: https://www.poynerspruill.com/thought-leadership/the-art-of-cyber-war-or-how-a-little-known-policy-exclusion-can-nullify-your-insurance-coverage/.
[118] Synott, M., 2020. *The Problem Of Silent Cyber Risk Accumulation*. [online] Willis Towers Watson. Available at: https://www.willistowerswatson.com/en-US/Insights/2020/02/the-problem-of-silent-cyber-risk-accumulation.
[119] Krauss, J., 2019. *Cyberinsurance 2.0: The New Wave Of Cyberinsurance*. [online] Willis Towers Watson. Available at: https://www.willistowerswatson.com/en-US/Insights/2019/07/decode-cyber-brief-cyberinsurance-the-new-wave-of-cyberinsurance.
[120] Hsieh, M. and Fixler, A., *The Role Of Cyber Insurance In Securing The Private Sector - Foundation For The Defense Of Democracies*; Gul, S. and Slipsky, M., *The Art Of (Cyber) War, Or How A Little Known Policy Exclusion Can Nullify Your Insurance Coverage*.
[121] Rundle, J., 2019. *Cyberattacks Complicate War Exclusions For Insurers*. [online] WSJ. Available at: https://www.wsj.com/articles/cyberattacks-complicate-war-exclusions-for-insurers-11575628201.
[122] Ibid.

[123] Hill, A., 2020. *Cyber Risk Poses Ongoing Challenge For First-Party Property Damage Lines Of Business*. [online] Willis Towers Watson. Available at: https://www.willistowerswatson.com/en-US/Insights/2020/01/cyber-risk-poses-ongoing-challenge-for-first-party-property-damage-lines-of-business; Ahmed, M. and Dyson, B., 2020. *Cyber Insurers Wrestle With War Exclusions As State-Sponsored Attack Fears Grow*. [online] S&P Global Market Intelligence. Available at: https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/cyber-insurers-wrestle-with-war-exclusions-as-state-sponsored-attack-fears-grow-56743302; Bantham, R., 2019. *Cyber Coverage Confusion*. [online] Risk Management. Available at: http://www.rmmagazine.com/2019/10/01/cyber-coverage-confusion/; Del Prete, C., 2019. *Common Exclusions Invoked By Cyber Carriers To Deny Coverage*. [online] Tech Risk Report. Available at: https://www.techriskreport.com/2019/02/common-exclusions-invoked-cyber-carriers-deny-coverage/.

[124] Smith, K., 2019. *Going Dark*. [online] Best's Review. Available at: http://news.ambest.com/ArticleContent.aspx?pc=1009&altsrc=158&refnum=285596; Smith, K., 2019. *An Act Of War?*. [online] Best's Review. Available at: http://news.ambest.com/articlecontent.aspx?refnum=288755&altsrc=123.

[125] Center for Internet Security. 2020. *EI-ISAC Cybersecurity Spotlight – Cyber Kill Chain®*. [online] Available at: https://www.cisecurity.org/spotlight/ei-isac-cybersecurity-spotlight-cyber-kill-chain/; Korolov, M. and Myers, L., 2018. *What Is The Cyber Kill Chain? Why It's Not Always The Right Approach To Cyber Attacks*. [online] CSO Online. Available at: https://www.csoonline.com/article/2134037/strategic-planning-erm-the-practicality-of-the-cyber-kill-chain-approach-to-security.html.

[126] 2018. *A Guide To Cyber Attribution*. [online] Office of the Director of National Intelligence. Available at: https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf; Bianco, D., 2013. *The Pyramid Of Pain*. [online] Enterprise Detection and Response. Available at: https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html.

[127] Strom, B., 2018. *ATT&CK 101*. [online] Medium. Available at: https://medium.com/mitre-attack/att-ck-101-17074d3bc62.

[128] MITRE | ATT&CK. 2020. *Contribute | MITRE ATT&CK®*. [online] Available at: https://attack.mitre.org/resources/contribute/.

[129] Smith, T., 2020. *ICS ATT&CK: Designed To Help Protect From Cyber Attacks*. [online] POWER Magazine. Available at: https://www.powermag.com/ics-attck-designed-to-help-protect-from-cyber-attacks/; MITRE, 2020. *MITRE Releases Framework For Cyber Attacks On Industrial Control Systems*. [online] Available at: https://www.businesswire.com/news/home/20200107006064/en/MITRE-Releases-Framework-Cyber-Attacks-Industrial-Control.

[130] Rockwell, M., 2017. *Cyber Threat Info Sharing Made Easier*. [online] GCN. Available at: https://gcn.com/articles/2017/04/17/stix-threat-info-sharing.aspx; Miller, J., 2015. *DHS To Launch STIX, TAXII Service For Cyber*. [online] Federal News Network. Available at: https://federalnewsnetwork.com/technology-main/2015/05/dhs-to-launch-stix-taxii-service-for-cyber/; Van Impe, K., 2015. *How STIX, TAXII And Cybox Can Help With Standardizing Threat Information*. [online] Security Intelligence. Available at: https://securityintelligence.com/how-stix-taxii-and-cybox-can-help-with-standardizing-threat-information/.

[131] Toussain, M., 2014. *Home Field Advantage - Using Indicators Of Compromise To Hunt Down The Advanced Persistent Threat*. [online] SANS Institute. Available at: https://www.sans.org/reading-room/whitepapers/detection/home-field-advantage-indicators-compromise-hunt-down-advanced-persistent-threat-35462; Van Impe, K., *How STIX, TAXII And Cybox Can Help With Standardizing Threat Information*.

[132] GMISAO org. 2020. *GM-ISAO – Global Manufacturing Cyber Security Resilience*. [online] Available at: http://gmisao.org/gm-isao; CISA.gov. 2019. *Information Sharing And Analysis Organizations (ISAOs)*. [online] Available at: https://www.cisa.gov/information-sharing-and-analysis-organizations-isaos.

[133] GMISAO org., *GM-ISAO – Global Manufacturing Cyber Security Resilience*; CISA.gov. *Information Sharing And Analysis Organizations (ISAOs).*

[134] GMISAO org., *GM-ISAO – Global Manufacturing Cyber Security Resilience*; CISA.gov. *Information Sharing And Analysis Organizations (ISAOs).*

[135] International Society of Automation. 2020. *ISA99, Industrial Automation & Control Systems Security*. [online] Available at: https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa99.

[136] Ibid.
[137] Ibid.
[138] Ibid.
[139] International Society of Automation. 2020. *UN To Integrate ISA/IEC 62443 Into Cyber Framework*. [online] Available at: https://www.isa.org/intech-home/2019/january-february/departments/united-nations-commission-to-integrate-isa-iec-624.
[140] Stouffer, K., Zimmerman, T., Tang, C., Lubell, J., Cichonski, J. and McCarthy, J., 2019. *Cybersecurity Framework Manufacturing Profile*. [online] NIST. Available at: https://www.nist.gov/publications/cybersecurity-framework-manufacturing-profile-0.
[141] Ibid.
[142] Nvd.nist.gov. 2020. *National Vulnerability Database - NIST*. [online] Available at: https://nvd.nist.gov/; Sass, R., 2019. *Not All National Vulnerability Databases Are Created Equal*. [online] ITProPortal. Available at: https://www.itproportal.com/features/not-all-national-vulnerability-databases-are-created-equal/; Avner, G., 2018. *The National Vulnerability Database Explained*. [online] Blog - WhiteSource. Available at: https://resources.whitesourcesoftware.com/blog-whitesource/the-national-vulnerability-database-explained.
[143] Hightower, C., 2019. *Thinking Outside The National Vulnerability Database Box*. [online] Infosecurity Magazine. Available at: https://www.infosecurity-magazine.com/opinions/national-vulnerability-database/; CCCure. n.d. *The National Vulnerability Database (NVD)*. [online] Available at: https://cccure.training/m/articles/view/The-National-Vulnerability-Database-NVD.
[144] Mell, P., Scarfone, K. and Romanosky, S., 2007. *The Common Vulnerability Scoring System (CVSS) And Its Applicability To Federal Agency Systems*. [online] NIST. Available at: https://csrc.nist.rip/library/NIST%20IR%207435.pdf; Hightower, C., *Thinking Outside The National Vulnerability Database Box*; CCCure, *The National Vulnerability Database (NVD)*.
[145] Kulesa, P., 2019. *Diagnosing company culture to mitigate risk.* [online] Willis Towers Watson. Available at: https://www.willistowerswatson.com/en-US/Solutions/products/cyber-risk-culture-survey.
[146] Kennedy, T., n.d. *Manufacturing Cybersecurity*. [online] ChiefExecutive.net. Available at: https://chiefexecutive.net/manufacturing-cybersecurity/amp/.