On the impact of Cyber-attacks on Industrial Control System Environment (ICSE) and Operational Technology (OT) Networks in the Manufacturing sector

Author: Vishnu Palassery

secolve
OT SECURITY SOLVED

Head Office Address: Level 2, 11 York Street, Sydney, NSW 2000
Contact: info@secolve.com
1800 SECOLVE (732 658)

INTRODUCTION

Industrial Control Systems (ICS) and Operational Technology (OT) are integral aspects of the manufacturing sector. They are key to the operation, monitoring and control of manufacturing machinery in plant and other important assets within the sector (Knapp and Langill, 2015) (i-SCOOP, n.d.). The cybersecurity of ICS, OT and other affiliated systems and networks is therefore of vital importance. Unlike cyber-attacks against traditional systems, attacks against ICS and OT affect not only vital business operations but also processes of physical manufacturing machinery (Kondo et al., 2018) (i-SCOOP, n.d.). In addition to crippling normal machine operations by stopping or slowing important manufacturing processes, attacks can also cause physical damage to machinery. Many of these attacks are capable of directing the ICS of machinery to operate outside of normal parameters, causing dangerous malfunctions which can endanger the lives of people close by (Knapp and Langill, 2015) (Kondo et al., 2018).

Manufacturing is a staple sector. It contributes greatly to a nation's economy, as is the case with Australia, where manufacturing is estimated to be responsible for six percent of the nation's total Gross Domestic Product (GDP) (Economic importance of manufacturing, 2020). The industry is responsible not only for the production of non-essential consumer products, but also for the manufacturing of products, equipment, parts, and materials for important industries such as mining, oil, agriculture, food processing, pharmaceutical production and chemical manufacturing. In fact, these important industries can be seen as aspects of the manufacturing sector itself (Chilingar, Mourhatch and Al-Qahtani, 2009).

The manufacturing industry especially proved its worth to the health sector in 2020 due to the COVID-19 pandemic, as the industry has produced much needed essential medical equipment such as Personal Protective Equipment (PPE) to health care workers and facilities (Economic importance of manufacturing, 2020). Cybersecurity within this sector is critical as any damage to infrastructure and disruption to operations could result in disastrous consequences to the sector and to people and other critical sectors reliant on it.

The purpose of this paper is to showcase 34 cybersecurity incidents in the manufacturing sector in the last 20 years. It aims to raise awareness of cybersecurity in the manufacturing sector especially in regard to ICS and OT environments and to highlight how many of these incidents overlap in similarity.

"Unlike cyber-attacks against traditional systems, attacks against ICS and OT affect not only vital business operations but also processes of physical manufacturing machinery. In addition to crippling normal machine operations…attacks can also cause physical damage to machinery."

Identified cyber-incidents in the Manufacturing sector

Attack – 1	2020 - Honda, Global
What happened	Multinational car manufacturer Honda was the victim of a ransomware attack aimed at the company's global operations, affecting both internal networks and production systems of manufacturing plants in multiple countries (Whittaker, 2020)(Tidy, 2020).The culprit managed to gain unauthorised access to the SCADA system and subsequently acquired control over the pumping stations by taking advantage of the then insecure and often improperly configured radio communications utilised in SCADA systems. The attacker did this using a standard laptop and a radio transmitter. This, as well as the inherent vulnerability of the legacy system, was the major contributing factor for the success of the attack (Hemsley & E. Fisher, 2018).
How did it happen and was it successful?	The attack was successful. According to security analysts, the attackers are presumed to have predominantly used Snake ransomware alongside other attack tools favoured by state actors. The virus managed to infect an internal server of the company, then proceeded to spread throughout other systems. The tools used are known to have been designed to compromise ICS networks, which is demonstrated through some of the damage caused by the attack (Whittaker, 2020) (Tidy, 2020) (Virani, 2020) (Winder, 2020) (Dooley and Ueno, 2020). Security analysts have also hypothesised that the attackers may have taken advantage of Covid-19 related panic and the vulnerabilities attached to remote working protocols. (Tidy, 2020) (Winder, 2020).
Impact	The attack resulted in severe slowing of global operations, to the extent of complete stoppage in some cases. The attack also compromised the production systems of manufacturing plants in a number of countries, predominantly Brazil, Japan, India, Italy, North America and Turkey. This resulted in the production of affected factories being halted for some time (Whittaker, 2020) (Tidy, 2020) (Virani, 2020) (Winder, 2020) (Dooley and Ueno, 2020).

Attack – 2	2020 - BlueScope Steel, Australia
What happened	The Australian steel product manufacturer, BlueScope Steel, was victim to a ransomware attack, which was initially identified in the IT systems of one of the company's US facilities (Clifford, 2020) (Crozier, 2020) (CISOMAG, 2020).
How did it happen and was it successful?	The attack was successful, however the company itself have not disclosed the nature of the attack. Some cyber security specialists have stated that phishing schemes were most likely used to deliver ransomware into company systems, but this has not been confirmed (Clifford, 2020) (Crozier, 2020) (CISOMAG, 2020).
Impact	The attack affected companywide operations and production systems in many of BlueScope's manufacturing plants, thus forcing them to switch to manual operations in many instances. One example: a furnace in the company's Port Kembla plant was forced to switch to manual operation (Clifford, 2020) (Crozier, 2020) (CISOMAG, 2020).

Attack – 3	2020 – Tower Semiconductor, Israel
What happened	Tower Semiconductor, the Israel based integrated circuit manufacturer, was victim to a cyber-attack which affected many of its operations (Hacker News, 2020) (Staff, 2020).
How did it happen and was it successful?	The attack was a success but its nature has not been confirmed by the company. The attack is, however, suspected of being ransomware based. It is also suspected that the infrastructure was specifically targeted for the purpose of industrial espionage, similar to some Stuxnet based attacks in the 2010s that were used to both spy on and sabotage targets (Goud, 2020) (Leyden, 2020) (CISOMAG, 2020) (McMillan, 2010).
Impact	The attack resulted in many of the company's critical operations, including manufacturing, to be halted until the situation rectified and the risk of resuming operations was eased to a safe level. Any future damages caused by this incident were not disclosed by the company (Hacker News, 2020) (Staff, 2020) (Goud, 2020) (Leyden, 2020) (CISOMAG, 2020).

Attack – 4	2020 - Lion (Attack 1), Australia
What happened	The Australian beverage manufacturer on June 9th was victim to a ransomware attack targeted at the company's internal IT systems. The attackers demanded a payment of USD 800, 000 to decrypt the encrypted data (Hacker News, 2020) (Grubb, 2020) (Lion, 2020) (Varghese, 2020) (Grubb, 2020).
How did it happen and was it successful?	The attack was successful. The attackers utilised the REVil ransomware attack which is designed to exploit vulnerabilities present in devices running Windows operating systems, enabling instantaneous extraction and encryption of data and files (Hacker News, 2020) (Grubb, 2020) (Lion, 2020) (Varghese, 2020) (Grubb, 2020).
Impact	The attack resulted in the shutdown of several company systems and networks, resulting in the company having limited visibility of the products in their systems. Furthermore, the attack negatively affected a number of company breweries, causing both supply and manufacturing issues. These issues were further exasperated due to COVID-19 related complications (Hacker News, 2020) (Grubb, 2020) (Lion, 2020) (Varghese, 2020) (Grubb, 2020).

Attack – 5	2020 - Lion (Attack 2), Australia
What happened	After the initial attack, whilst recovering, the beverage manufacturer was subjected to a second ransomware attack with a new demand of $1 million (Grubb, 2020) (Berry, 2020).
How did it happen and was it successful?	Taking advantage of the company's slow recovery from the first attack and COVID-19 related complications, the attackers launched a successful second ransomware attack to cause further damage to the company's manufacturing and supplies. (Grubb, 2020) (Berry, 2020).
Impact	The second attack resulted in delaying the recovery efforts of the damages caused by the previous attack, as well as causing additional damage to the company's it systems (Grubb, 2020) (Berry, 2020).

Attack – 6	2020 – Tesla, United States
What happened	The Nevada factory of world leading electric car manufacturer Tesla was the target of a potentially state-sponsored cyber-attack (Hacker News, 2020) (Staff, 2020) (Alvarez, 2020) (Zachariah, 2020).
How did it happen and was it successful?	The Russian sponsor behind the attack approached an unnamed Russian-speaking non-citizen employee of the company in an attempt to recruit them with an offer of USD1 million to intentionally sabotage the systems and networks of the factory with provided malware, which would encrypt data and files and be held for ransom. This would then be followed by a Distributed Denial of Service Attack (DDoS). This attempted attack was thwarted with the help of the said employee, who reported the incident to the company and the Federal Bureau of Investigation (FBI). A sting operation was commenced to apprehend the person behind the attack, which resulted in the arrest of a Russian national (Hacker News, 2020) (Staff, 2020) (Alvarez, 2020) (Zachariah, 2020) (Writer, 2020).
Impact	Due to the attack being thwarted, there was no significant impact to the company's operations. However, had the conspirators succeeded in their attempt, the attack would have resulted in not only a serious data breach but also potentially serious damage to the company's systems. The planned DDoS attack in particular would have likely crippled the critical operations of the factory, causing production to halt (Staff, 2020) (Alvarez, 2020) (Zachariah, 2020).

Attack – 7	2020 – Unidentified small manufacturing company, United States
What happened	An unidentified manufacturing company from Kentucky was the target and victim of a ransomware attack (Roby, 2020).
How did it happen and was it successful?	The attack was successful. An employee of the company clicked on a phishing link that allowed the attackers to infect the company's systems with malware (Roby, 2020).
Impact	The attack resulted in staff being locked out of company systems and networks, including the systems responsible for operational control of manufacturing machinery. The company also acquiesced to attackers' demands and paid a ransom of USD150, 000, which was decreased from an initial USD400, 000 ransom demand (Roby, 2020).

Attack – 8	2020 - Fisher & Paykel Appliances, New Zealand
What happened	Whitegoods manufacturer Fisher & Paykel was the victim to a ransomware attack targeting their systems and networks (Saarinen, 2020) (Tonkin, 2020) (Strecker, 2020).
How did it happen and was it successful?	The hackers were successful in their attack. They used the relatively recent Nefilim ransomware package for their attack. The ransomware infected the systems and networks of the company. The malware encrypted and extracted important files and data, which were then used to extort a ransom from the company (Saarinen, 2020) (Tonkin, 2020) (Strecker, 2020).
Impact	The attack forced the company to shut down its IT systems and networks for certain duration. This resulted in the company halting operations, which lead to a negative impact in manufacturing and distribution operations (Saarinen, 2020) (Tonkin, 2020) (Strecker, 2020).

Attack – 9	2019 – ASCO, Belgium, Germany, Canada, and the United States
What happened	The world leading aircraft parts manufacturer ASCO was the victim of a ransomware attack that affected the operations of company facilities in Belgium, Germany, Canada and the United States (Hacker News, 2019) (Goud, 2019) (Computer Weekly, 2019).
How did it happen and was it successful?	The perpetrators were successful in their attack. The company, in their statement disclosing the attack, did not provide the type of the ransomware used or how the company's system was initially infected. The company did say that it was a large-scale attack aimed to compromise as many systems and networks of the company as possible (Hacker News, 2019) (Goud, 2019) (Computer Weekly, 2019).
Impact	The attack resulted in the temporary unemployment of 1,000 workers, disruption ASCO's communications systems and the halting of production in the company's factories in Belgium, Germany, Canada and the United States (Hacker News, 2019) (Goud, 2019) (Computer Weekly, 2019).

Attack – 10	2019 - Aebi Schmidt, Switzerland
What happened	The Switzerland based special purpose vehicle manufacturer was the victim of a ransomware attack against their international systems and networks (Hacker News, 2019) (Goud, 2019) (Whittaker, 2019).
How did it happen and was it successful?	The attack was successful, but the nature of the ransomware used by the attackers was not revealed. What is known about the virus is that it affected the company's Windows network, indicating that the malware was designed to exploit vulnerabilities present in Windows systems at the time. The method used to conduct the attack was through phishing email attacks which deceived an employee or someone with legitimate access to company's systems to infect it by accessing the fraudulent email (Hacker News, 2019) (Goud, 2019) (Whittaker, 2019).
Impact	The attack affected many systems responsible for global operations, such as sales and email services, and it left a number of employees temporally unemployed without pay. The attack also affected manufacturing operations specifically in the company's European locations (Hacker News, 2019) (Goud, 2019) (Whittaker, 2019).

Attack – 11	2019 – Defence contractor Rheinmetall, Brazil, Mexico, United States
What happened	The Rheinmetall manufacturing plants in Brazil, Mexico and the United States were the victim of a malware-based attack aimed at causing disruption to the company's operations (Cimpanu, 2019) (Lyngaas, 2019) (Paganini, 2019).
How did it happen and was it successful?	The attack was successful, but neither the infection method used by the attackers, nor the malware used, were disclosed by the company. However, it is theorised that the attack is similar in nature to several ransomware attacks that happened in the same year, such as the above mentioned Aebi Schmidt attack (Cimpanu, 2019) (Lyngaas, 2019) (Paganini, 2019).
Impact	The attack caused significant disruptions to the operations of the company, in particular the production operations of the company's manufacturing plants in Brazil, Mexico and the United States. The attack also took a toll on the company's financials, with a loss of three to four million euros each week as they recovered (Cimpanu, 2019) (Lyngaas, 2019) (Paganini, 2019).

Attack – 12	2019 – Pilz, Germany
What happened	German-based automation tools manufacturer Pilz was the victim of a ransomware attack that affected much of its global operations (Cimpanu, 2019) (Truta, 2019).
How did it happen and was it successful?	The attack was not necessarily successful in affecting production systems in particular. The method used by the attackers to infect the company's systems is believed to be spear phishing email campaigns. The ransomware package used was the BitPaymer ransomware, which is delivered through the Dridex trojan, which exploits vulnerabilities in Windows systems to conduct attacks (Cimpanu, 2019) (Truta, 2019).
Impact	The attack heavily disrupted worldwide company operations, crippling communication networks, several servers and workstations in all of the company's business locations, causing them to be disconnected from the company's main network. As a result of this attack, many services required for the company's global operations were forced to halt or were severely impacted, thus slowing down the production operations. That being said, the malware itself did not manage to compromise actual production capabilities but it certainly had the potential for more extensive damage, as can be seen in other prominent ransomware attacks such as the Aebi Schmidt attack (Cimpanu, 2019) (Truta, 2019).

Attack – 13	2019 – Norsk Hydro, Norway
What happened	The worldwide networks of the globally leading Norsk Hydro aluminium producer was the victim of a ransomware attack, which negatively affected the company's global operations (Greenberg, 2019) (Goodin, 2019).
How did it happen and was it successful?	The attack was successful; the ransomware used was the LockerGoga malware. According to analysis from security experts who conducted the investigation on the attack, the attackers most likely acquired initial access to company systems through phishing attacks. With this foothold, they then acquired domain administrator rights to systems. This can be done by using common intrusion tools such a Minimax, which can extract passwords present in the memory cache of Windows systems. With this privileged access, the attackers were then able to infect the desired systems with the ransomware package through the functions provided by Windows Active Directory management tools (Greenberg, 2019) (Beaumont, 2019).
Impact	The attack caused worldwide disruptions to many of the company's operations. A number of the company's manufacturing plants were forced to switch to manual operations due to system compromise, and some had to be stopped entirely. The slowdown of production due to this attack resulted in the company incurring a substantial drop in its profits. (Greenberg, 2019) (Goodin, 2019).

Attack – 14	2019 – Demant, Denmark, Poland, France, and Mexico
What happened	The systems and networks of hearing aid manufacturer, Demant, was the victim of a ransomware based cyberattack (Cimpanu, 2019) (Zorz, 2019).
How did it happen and was it successful?	The attack was successful; however, the company has not disclosed the complete details of the attack, so much remains unknown. The Danish media has reported it to be a ransomware-based attack which came from outside, indicating that internal sabotage was not the cause (Cimpanu, 2019) (Zorz, 2019).
Impact	The company's infrastructure was heavily impacted by the attack due to their IT network shutting down when the attack was identified. Furthermore, the systems and networks of the company's production plants in Denmark, Poland, France, and Mexico were also compromised, thereby negatively impacting the company's production and distribution output. The attack also resulted in many of the company's hearing clinics being unable to serve the needs of their customers. This all resulted in massive reductions in company profits, to the tune of $90 million, and the company's growth was drastically affected for the immediate future (Cimpanu, 2019) (Zorz, 2019).

Attack – 15	2018 - Taiwan Semiconductor Manufacturing Company (TSMC), Taiwan
What happened	The world's largest contracted chip manufacturer, TSMC, with prominent customers such as Apple, was the victim of a ransomware attack targeting their manufacturing processes. However, despite the malware used being ransomware, there was no ransom demand, indicating that the attacker's primary objective was to cause damage (Staff, 2018) (Security, 2018) (Update, 2019) (team, 2018).
How did it happen and was it successful?	The attack was successful, utilising WannaCry ransomware. This malware managed to infect the affected systems, due to a supplier of the company directly installing software infected with the malware into some of the systems in the factory. The production system that was initially infected was isolated from the internet, and thereby the company's main network, at the time, rendering some important safeguards became ineffective. This, along with the outdated and unpatched Windows system at the time, enabled the malware to spread faster once the affected systems were reconnected to the company's main network (Security, 2018) (team, 2018) (Staff, 2018).
Impact	The attack affected 10,000 computer systems and manufacturing tools, encompassing the majority of the company's manufacturing plants in Taiwan. The affected systems and tools were shut down for recovery. This resulted in an entire day's worth of production being lost, causing a slowdown in the delivery of product to customers. This attack in total cost the company USD170 million (Staff, 2018) (Security, 2018) (Update, 2019) (team, 2018).

Attack – 16	2018 – Boeing, United States
What happened	The US based facility of the leading aircraft manufacturer was victim to a ransomware attack. The initial reports claimed that the attack caused significant damage to company's production systems; it was later proven that these reports were not true (Gates, 2018) (Goud, 2018) (Muncaster, 2018).
How did it happen and was it successful?	The attack was successful but perhaps not to the extent the hackers desired. The malware used in the attack was WannaCry ransomware - the same malware used in the previous attack in this list. WannaCry was designed to exploit vulnerabilities in Windows operating systems at the time, to spread through the network of the infected system (Gates, 2018) (Goud, 2018) (Muncaster, 2018).
Impact	While some systems were affected to a degree, it wasn't to the crippling degree initially reported, but was negligible to the company's production output. The attack did, however, have the potential to do significant damage to manufacturing system, as it is similar to the previous attack in this paper (Gates, 2018) (Goud, 2018) (Muncaster, 2018).

Attack – 17	2017- Nissan-Renault, Global
What happened	Partner car manufacturers Nissan and Renault were the victim of a global Ransomware attack campaign with the aim to compromise both companys' systems and networks (Frost and Tajitsu, 2017) (Staff, 2017) (Eisenstein, 2017).
How did it happen and was it successful?	The attack was a success and the ransomware used was the WannaCry malware, the same used in the previous two entries on this report. Similar those entries, the rapid spread of the malware through Renault –Nissan's systems and network can likely be attributed to the malware exploiting the vulnerabilities in outdated Windows systems and networks. (Frost and Tajitsu, 2017) (Staff, 2017) (Eisenstein, 2017).
Impact	The attack negatively impacted the operations of the auto group, including the production of six of the auto group's factories - four catering solely to Renault, one catering to both, and one exclusively Nissan plant (Frost and Tajitsu, 2017) (Staff, 2017).

Attack – 18	2017 – Honda, Japan
What happened	A Honda plant in Japan was the victim to a ransomware attack of WannaCry - the same variant as the previously described three attacks in this paper (Lyon, 2017) (Staff, 2017).
How did it happen and was it successful?	This attack, like the previous three attacks in this paper, was successful, the ransomware package being WannaCry malware, which exploited the vulnerabilities present in Honda's outdated Windows based systems and networks (Lyon, 2017) (Staff, 2017).
Impact	The attack compromised Honda's networks and systems not only in Japan but spread to their networks in Europe, North America and China. However, in regard to the impact on manufacturing, only the production systems of the company's Japan based factory was affected by the attack, causing said plant to shut down for some time (Lyon, 2017) (Staff, 2017).

Attack – 19	2017 - Russian Government Dragonfly campaign, United States
What happened	The Dragonfly campaign was a Russian sponsored cyber-attack campaign targeting Industrial Control Systems (ICS) of critical US sectors which include nuclear, water, commercial, aviation and - most relevant to this paper - critical manufacturing (Cybersecurity and Infrastructure Security Agency, 2018) (CATAPULT, n.d.).
How did it happen and was it successful?	The attack was a success as it did cause damage, but no long-lasting crippling damage was inflicted. The attacks in this campaign were conducted in stages. Spear phishing attacks were used at first to launch malware-based intrusions and to acquire credentials to gain remote access to systems and networks. With this access, the attackers searched for information regarding vulnerable ICSs to compromise. This stage of the attack was conducted against trusted third-party organisations affiliated with the intended targets, which had less secure networks. These less secure networks were used as stage points to launch the real attacks when third-party networks converge with the networks of the intended target (Cybersecurity and Infrastructure Security Agency, 2018) (CATAPULT, n.d.).
Impact	The attack managed to compromise systems of several critical infrastructure entities, including manufacturing (Cybersecurity and Infrastructure Security Agency, 2018).

Attack – 20	2017- Pharmaceutical company Merck & Co
What happened	The pharmaceutical manufacturer was the victim to a misleading ransomware attack targeting the company's worldwide operations. Unlike traditional ransomware attacks which aim to extort money, the aim of this attack was to sabotage the company's systems (Erman and Finkle, 2017) (Paganini, 2017) (Vijayan, 2017).
How did it happen and was it successful?	The attack was successful and the disguised ransomware package used was the NotPetya malware. The malware is designed to appear as a traditional ransomware, but instead it is the wiper variant of malware designed to sabotage systems networks by quickly and destructively spreading through them, crippling them in the process. The attackers also sent a false ransom demand to continue the ruse of ransomware attack, as they aimed to take advantage of the media coverage of then recent numerous reports of WannaCry ransomware for this purpose. This was made possible because the structure of NotPetya malware was very similar to WannaCry, but was more sophisticated (Erman and Finkle, 2017) (Paganini, 2017).
Impact	The attack resulted in company's worldwide operations being disrupted - the company's manufacturing operations in particular. This led to the slowdown of drug production and the shipment of products to customers. This resulted in the company having lower profits than expected for that year (Erman and Finkle, 2017) (Paganini, 2017) (Vijayan, 2017).

Attack – 21	2017- Petrochemical company – Saudi Arabia
What happened	The petrochemical plant was the victim to a cyber-attack. The attack is believed to be state sponsored. The aim was to compromise the safety controls of the systems responsible for the operation of machinery in the plant, in order to induce an explosion due to safety failures (Bedwell, 2020) (Sutton, 2018) (Perlroth, 2018).
How did it happen and was it successful?	While the attack did have a negative impact on the operations of the plant, the real goal of disrupting the plant's safety controls was unsuccessful due to a flaw in the malware's code. The malware used was Triton. This malware is designed to cause a malfunction in the plant's Safety Instrumented System (SIS) responsible for ensuring the machinery of the plant operates within normal safe parameters. How the plant's systems got infected has not been disclosed (Bedwell, 2020) (Sutton, 2018) (Perlroth, 2018).
Impact	The attack resulted in plant machinery and overall production systems of the plant to randomly malfunction and shutdown. This was due to the error in Triton's code as this was not the attack's intended effect. Once this was noticed, the entire plant had to be shutdown to deal with the issue. The consequences of this attack if not for the flaw in the malware's programming had the potential to be much more catastrophic and tragic if the real goal of triggering an explosion had been achieved. This attack was the first of its kind in specifically targeting a plant SIS (Bedwell, 2020) (Sutton, 2018) (Perlroth, 2018).

Attack – 22	2014 - Steel mill, Germany
What happened	An unidentified German steel mill was the victim to a damaging cyber intrusion by attackers who had an advanced understanding of Industrial Control System Environments (ICSE) (Federal Office for Information Security, 2014) (BBC, 2014).
How did it happen and was it successful?	The attackers were successful in achieving their purpose. To conduct the attack, the attackers used social engineering tactics - predominantly spear phishing campaigns aimed at specific individuals working at the mill - to get log in credentials to obtain initial access to the mill's systems. This access, along with attackers' in-depth knowledge in ICSEs, allowed them to progressively work their way through the plant's corporate network to its production systems and networks (Federal Office for Information Security, 2014) (BBC, 2014).
Impact	The intrusion resulted in the disruption of control components of the plant's production systems. This eventually led to the failure of the plant's production capabilities, resulting in the malfunction and breakdown of an important blast furnace because of its improper shutdown, causing significant damage (Federal Office for Information Security, 2014) (BBC, 2014).

Attack – 23	2011 – Steel Plant, Brazil
What happened	The control and automation systems and networks of the unidentified steel plant was the victim of malware infection (RISI, n.d.) (178, n.d.).
How did it happen and was it successful?	The attack was successful; the malware at the source of the infection was the Conficker worm. The malware exploits the vulnerabilities present at Windows based systems and networks to successfully infect the target. In this attack, once the plant's control systems were infected, the worm proceeded to spread through the automation systems of the plant where the virus induced a period of instability in the communications between the steel plant's programmable logic controllers (PLC) and supervisory stations (RISI, n.d.) (178, n.d.).
Impact	The instability in communication between the steel plant's PLCs and supervisory stations resulted in the disruption and shutdown of the majority of the plant's supervisory systems (RISI, n.d.) (178, n.d.).

Attack – 24	2010 – Shutdown of Milling Factory - Iran
What happened	The systems of an unidentified multipurpose milling factory were the victim to a virus infection (RISI, n.d.) (167, n.d.).
How did it happen and was it successful?	The attack was successful and the virus behind the infection was the Stuxnet worm. Stuxnet at the time exploited zero-day vulnerabilities present in Windows systems to successfully infect them. Once infected, it rapidly spread through plant networks and altered the programmable logic controllers responsible for the operation of machinery. This resulted in making them operate outside of safe operating parameters, causing them to malfunction (RISI, n.d.) (167, n.d.) (Fruhlinger, 2017).
Impact	The attack resulted in the total shutdown of all operations of the milling plant (RISI, n.d.) (167, n.d.).

Attack – 25	2008 – Steel Plant, Brazil
What happened	An unidentified steel plant in Brazil was the victim to a malware infection which targeted the plant's automation network (RISI, n.d.) (131, n.d.).
How did it happen and was it successful?	The attack was successful and the malware used in the attack was the Ahack. The Ahack worm exploited vulnerabilities at the time in the plant's Windows-based systems network to succeed in the infection. Once successful, the worm rapidly spread through the plant's systems and networks and disrupted the communications between the steel plant's programmable logic (PLC) controllers and supervision stations by overwhelming them with a flood of miscellaneous packets (RISI, n.d.) (131, n.d.).
Impact	The attack resulted in the periodic stopping and restarting of the plant's production systems, resulting in a drastic reduction of the plant's production output during this period (RISI, n.d.) (131, n.d.).

Attack – 26	2006 – General manufacturer, Russia
What happened	The SCADA systems of the unidentified Russian general manufacturing plant was compromised due to a cyber intrusion (RISI, n.d.) (109, n.d.).
How did it happen and was it successful?	The attack was successful and was the result of a Trojan backdoor installed in one of the machines connected to the plant's SCADA system. After the Trojan was identified, all machines and devices that had contact with the SCADA systems were tested. The machines were cleared, but an identical copy of the Trojan backdoor was found in an external USB device used to take hard disk images, indicating that it was the source of initial infection (RISI, n.d.) (109, n.d.).
Impact	The attack resulted in the communications between multiple SCADA servers of the plant being disrupted, thereby slowing down the manufacturing plant's operations. Recovery efforts and security procedures after the identification of the Trojan backdoor most likely added to the disruption of normal plant operation (RISI, n.d.) (109, n.d.).

Attack – 27	2005 – DaimlerChrysler, United States
What happened	The DaimlerChrysler auto manufacturer group was the victim to a series of computer worm infections targeting the systems of 13 of their plants (RISI, n.d.) (Roberts, 2005).
How did it happen and was it successful?	The attack was successful because the unpatched Windows-based systems had critical vulnerabilities. The malware packages used were the Zotob, RBot and IRCBot computer worms, which exploited the vulnerabilities in the affected plants' systems and networks to infect them (Roberts, 2005) (Roberts, 2005).
Impact	The attack resulted in all 13 manufacturing plants shutting down to update outdated systems and networks, resulting in total vehicle production to cease for 50 minutes. This also resulted in the temporary unemployment of 50,000 employees during the day of shutdown (Roberts, 2005) (Roberts, 2005).

Attack – 28	2004 – Electronic manufacturing lab
What happened	The systems of the unidentified manufacturing lab from an unknown location were the victim of a complex malware based attack affecting a wide area of the systems and networks of the lab (RISI, n.d.).
How did it happen and was it successful?	The attack was successful and was the result of a backdoor Trojan. Before the Trojan was identified by the antivirus installed in the infected systems, the Trojan managed to collate a txt file with a list of user login credentials and IP addresses of the entire lab's machines and send them through the internet to an unknown source. Following this, more systems and networks of lab machines were identified as being similarly infected and quickly spread throughout the lab's network (RISI, n.d.).
Impact	The lab resorted to shutting down the infected machines, which amounted to half of the operating machines of the lab. This resulted in the slowdown of production. But as more and more systems and machines were shown as being affected and with no appropriate solution found, the lab engineers resorted to resetting the test beds, hubs and systems connected the lab machines, as well as the switches that ensured their connectivity. This all resulted in the loss of a total three weeks of development time (RISI, n.d.).

Attack – 29	2004 – Paper mill, United States
What happened	The systems of an unidentified paper mill were the victim of a virus infection (RISI, n.d.).
How did it happen and was it successful?	The attack was successful but the name of the virus is unknown. The virus was able to infect the systems of the paper mill due to a contractor affiliated with the mill providing an access point for the infection. At the time of the attack, the mill and the contractor were connecting through an unsecure and remote dial-up internet connection to access the Human Machine Interface (HMI) which provided the operational controls of the manufacturing press (RISI, n.d.).
Impact	The virus, through the manufacturing press's HMI, threatened its operational controls (RISI, n.d.).

Attack – 30	2004 – Food and beverage manufacturer, United Kingdom
What happened	The SCADA systems of a pilot plant of an unidentified food and beverage manufacture was the victim of a virus infection (RISI, n.d.).
How did it happen and was it successful?	The attack was successful and is widely attributed to the lack of antivirus software and other security measures in the plant's systems, resulting in the systems having negligible defence when a contracting company connected an infected laptop to the plant's SCADA systems. Furthermore, once the systems were scanned and the infection was identified, the results showed that the systems were infected with numerous separate malware and viruses. This is believed to be the result of both the lack of security features in the systems, employees and others affiliated people of the plant accessing infected emails and connecting infected external devices to the systems (RISI, n.d.).
Impact	The attack resulted in the total shutdown of the plant's operations until all identified issues at the time were rectified (RISI, n.d.).

Attack – 31	2003 – Metal industry manufacturer, Canada
What happened	The Human Machine Interface of the systems responsible for the control operation of smelting stations in an unidentified metal manufacturing plant was the victim of a computer worm infection (RISI, n.d.) (72, n.d.).
How did it happen and was it successful?	The attack was successful and the computer worm behind the infection was the Blaster worm (RISI, n.d.) (72, n.d.). The Blaster worm infects its targeted systems by exploiting vulnerabilities present in Windows-based systems and networks at the time (Dotan, 2017).
Impact	The attack resulted in the significant slowdown of the HMI input being processed to dictate operations of smelting machines. The effects persisted for several weeks while recovery was underway (RISI, n.d.) (72, n.d.).

Attack -32	2003 - Sappi Fine Paper, United States
What happened	The control systems of the Sappi Fine Paper paper manufacturer, like the previous attack in this paper, were infected by the Blaster computer worm (RISI, n.d.) (71, n.d.).
How did it happen and was it successful?	The attack was successful due to numerous vulnerabilities reported in the paper company's control systems, with an individual machine itself being identified as having up to 40 vulnerabilities that could be exploited by the worm. Even after numerous patches, new vulnerabilities in the company's control systems were still reported (RISI, n.d.) (71, n.d.).
Impact	The process control systems of the company were compromised, which likely had a significant negative impact in their operations (RISI, n.d.) (71, n.d.).

Attack – 33	2002 - Semiconductor manufacturing plant, United States
What happened	In an unidentified semiconductor manufacturing plant, a Programmable Logic Controller (PLC) responsible for the operations of a water purification system was the victim of cyber-attack (RISI, n.d.).
How did it happen and was it successful?	The attack was successful, but the method used by the attackers is unknown. The attacks success, however, is attributed to the PLC being connected to an unsecured LAN with internet connectivity (RISI, n.d.).
Impact	The attack disabled the targeted systems, leaving them inoperable for several hours (RISI, n.d.).

Attack – 34	2001 – Major food and beverage manufacturer, United States
What happened	The production systems in a manufacturing plant of an unidentified food and beverage manufacturer was the victim to a virus infection (RISI, n.d.).
How did it happen and was it successful?	The attack was successful, and the virus used was the Nimda computer worm. The virus operates by sending itself through infected emails to potential targets and, when accessed, it exploits the vulnerabilities in outdated Windows servers in order to infect files in local and remote systems (NortonLifeLock, n.d.). In this case, however, the production systems of the plant were infected by an employee. They, through their infected personal computer, remotely accessed the process control servers of the plant, which did not have the appropriate security measures in place to combat the infection. Once infected, the virus quickly spread through the systems and networks of the production plant (RISI, n.d.).
Impact	Through great effort, the employees of the plant prevented the worst-case scenario of total production shutdown. However, the attack still caused the company thousands of dollars for the time needed for repair and recovery (RISI, n.d.).

CONCLUSION

This paper highlights 34 cyber-attacks in the manufacturing sector. It provides an overview of the details that facilitated the attacks and the impact they had on the attacked entity in the sector. Many of the vulnerabilities and factors that led to an attack and the type of attack are the same or similar across many of the attacks in this paper. Examples of this are the number of ransomware attacks, exploitable vulnerabilities due to outdated systems networks, successful phishing scams and the connection of infected external devices to production systems.

The consistency in the similarity of factors that led to the respective attacks in this paper, even in the recent past, indicates that there is a serious lack in cyber awareness in this sector, and appropriate effort to ensure adequate cybersecurity among many entities in manufacturing is missing. This is a matter of serious concern. The details of the pool of attacks in this paper indicate that cybersecurity in the sector within the last 20 years has not only been underestimated, but in some instances undervalued.

The manufacturing sector is a critical infrastructure. It is integral to the operations of many other important industries, and it not only caters to the wants of the current consumerist society but also to the needs of the society both economic and material (Chilingar, Mourhatch and Al-Qahtani, 2009) (Economic importance of manufacturing, 2020). The cybersecurity in the manufacturing sector is critical, especially in regards to environments pertaining to ICSs and OT..

"The consistency in the similarity of factors…even in the recent past, indicates that there is a serious lack in cyber awareness in this sector, and appropriate effort to ensure adequate cybersecurity among many entities in manufacturing is missing."

REFERENCES

Alvarez, S., 2020. Tesla Employee Foregoes $1M Payment, Works With FBI To Thwart Cybersecurity Attack. [online] www.teslarati.com. Available at: <https://www.teslarati.com/tesla-employee-fbi-thwarts-russian-cybersecurity-attack/> [Accessed 22 October 2020].

Australian Government - Department of Industry Science, Energy and Resources. 2020. Economic Importance Of Manufacturing. [online] Available at: <https://www.industry.gov.au/data-and-publications/make-it-happen-the-australian-governments-modern-manufacturing-strategy/economic-importance-of-manufacturing> [Accessed 25 November 2020].

BBC, 2014. Hack Attack Causes 'Massive Damage' At Steel Works. [online] www.bbc.com. Available at: <https://www.bbc.com/news/technology-30575104> [Accessed 24 October 2020].

Beaumont, K., 2019. How Lockergoga Took Down Hydro—Ransomware Used In Targeted Attacks Aimed At Big Business. [online] doublepulsar.com. Available at: <https://doublepulsar.com/how-lockergoga-took-down-hydro-ransomware-used-in-targeted-attacks-aimed-at-big-business-c666551f5880> [Accessed 19 October 2020].

Bedwell, P., 2020. Surge In Cyberattacks Puts Manufacturing OT Systems At Risk. [online] securityboulevard.com. Available at: <https://securityboulevard.com/2020/09/surge-in-cyberattacks-puts-manufacturing-ot-systems-at-risk/> [Accessed 24 October 2020].

Berry, K., 2020. Lion Struck By Second Cyber Attack. [online] Foodanddrinkbusiness.com.au. Available at: <https://www.foodanddrinkbusiness.com.au/news/lion-struck-by-second-cyber-attack> [Accessed 22 October 2020].

CATAPULT, n.d. Dragonfly ICS Cyber Attack | News & Information. [online] Catapultsoftware.com. Available at: <https://www.catapultsoftware.com/news/dragonfly-ics-cyber-attack.html> [Accessed 17 October 2020].

Chilingar, G., Mourhatch, R. and Al-Qahtani, G., 2009. The Fundamentals Of Corrosion And Scaling For Petroleum & Environmental Engineers. Houston: Gulf Publishing Company, p.214.

REFERENCES

Cimpanu, C., 2019. Major German Manufacturer Still Down A Week After Getting Hit By Ransomware. [online] www.zdnet.com. Available at: <https://www.zdnet.com/article/major-german-manufacturer-still-down-a-week-after-getting-hit-by-ransomware/> [Accessed 19 October 2020].

Cimpanu, C., 2019. Malware Infection Disrupts Production At Defence Contractor Plants In Three Countries. [online] www.zdnet.com. Available at: <https://www.zdnet.com/article/malware-infection-disrupts-production-at-defence-contractor-plants-in-three-countries/> [Accessed 20 October 2020].

Cimpanu, C., 2019. Ransomware Incident To Cost Danish Company A Whopping $95 Million. [online] www.zdnet.com. Available at: <https://www.zdnet.com/article/ransomware-incident-to-cost-danish-company-a-whopping-95-million/> [Accessed 13 November 2020].

CISOMAG, C., 2020. Bluescope Cyber Incident Derails Its Australia Operations. [online] CISO MAG | Cyber Security Magazine. Available at: <https://cisomag.eccouncil.org/bluescope-cyber-incident/> [Accessed 7 November 2020].

CISOMAG, C., 2020. Israel's Tower Semiconductor Hit By A Cyberattack. [online] CISO MAG | Cyber Security Magazine. Available at: <https://cisomag.eccouncil.org/tower-semiconductor-cyberattack/> [Accessed 23 October 2020].

Clifford, J., 2020. Bluescope Steel Hit By Cyber Attack Causing Worldwide System Shutdown Of Operations. [online] Abc.net.au. Available at: <https://www.abc.net.au/news/2020-05-15/bluescope-steel-cyber-attack-shut-down-kembla-ransomware/12251316> [Accessed 7 November 2020].

Computer Weekly, 2019. Asco Breaks Silence On Ransomware Attack. [online] www.computerweekly.com. Available at: <https://www.computerweekly.com/news/252465178/Asco-breaks-silence-on-ransomware-attack> [Accessed 21 October 2020].

Crozier, R., 2020. Bluescope IT 'Disruption' Feared To Be Ransomware Attack. [online] iTnews. Available at: <https://www.itnews.com.au/news/bluescope-it-disruption-feared-to-be-ransomware-attack-548127> [Accessed 7 November 2020].

REFERENCES

Cybersecurity and Infrastructure Security Agency, 2018. Alert (TA18-074A). [online] Available at: <https://us-cert.cisa.gov/ncas/alerts/TA18-074A> [Accessed 17 October 2020].

Dooley, B. and Ueno, H., 2020. Honda Hackers May Have Used Tools Favored By Countries. [online] Nytimes.com. Available at: <https://www.nytimes.com/2020/06/12/business/ransomware-honda-hacking-factories.html> [Accessed 7 November 2020].

Dotan, L., 2017. What Is The Blaster Worm. [online] www.cybereason.com. Available at: <https://www.cybereason.com/blog/what-is-the-blaster-worm> [Accessed 16 November 2020].

Eisenstein, P., 2017. European Car Plants Halted By WannaCry Ransomware Attack. [online] www.nbcnews.com. Available at: <https://www.nbcnews.com/business/autos/european-car-plants-halted-wannacry-ransomware-attack-n759496> [Accessed 18 October 2020].

Erman, M. and Finkle, J., 2017. Merck Says Cyber Attack Halted Production, Will Hurt Profits. [online] www.reuters.com. Available at: <https://www.reuters.com/article/us-merck-co-results-idUSKBN1AD1AO> [Accessed 24 October 2020].

Federal Office for Information Security, 2014. The State Of IT Security In Germany 2014. Bonn: Federal Office for Information Security, p.31.

Frost, L. and Tajitsu, N., 2017. Renault-Nissan Is Resuming Production After A Global Cyberattack Caused Stoppages At 5 Plants. [online] www.businessinsider.com. Available at: <https://www.businessinsider.com/renault-nissan-production-halt-wannacry-ransomeware-attack-2017-5?IR=T> [Accessed 18 October 2020].

Fruhlinger, J., 2017. What Is Stuxnet, Who Created It And How Does It Work?. [online] www.csoonline.com. Available at: <https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html> [Accessed 25 October 2020].

Gates, D., 2018. Boeing Hit By WannaCry Virus, But Says Attack Caused Little Damage. [online] www.seattletimes.com. Available at: <https://www.seattletimes.com/business/boeing-aerospace/boeing-hit-by-wannacry-virus-fears-it-could-cripple-some-jet-production/> [Accessed 18 October 2020].

REFERENCES

Goodin, D., 2019. “Severe” Ransomware Attack Cripples Big Aluminum Producer. [online] arstechnica.com. Available at: <https://arstechnica.com/information-technology/2019/03/severe-ransomware-attack-cripples-big-aluminum-producer/> [Accessed 19 October 2020].

Goud, N., 2019. Aircraft Parts Manufacturer Asco Hit By A Ransomware Attack - Cybersecurity Insiders. [online] www.cybersecurity-insiders.com. Available at: <https://www.cybersecurity-insiders.com/aircraft-parts-manufacturer-asco-hit-by-a-ransomware-attack/> [Accessed 21 October 2020].

Goud, N., 2020. Cyber Attack On Tower Semiconductor - Cybersecurity Insiders. [online] Cybersecurity Insiders. Available at: <https://www.cybersecurity-insiders.com/cyber-attack-on-tower-semiconductor/> [Accessed 23 October 2020].

Goud, N., 2018. Details About WannaCry Ransomware Attack On Boeing Company. [online] www.cybersecurity-insiders.com. Available at: <https://www.cybersecurity-insiders.com/details-about-wannacry-ransomware-attack-on-boeing-company/> [Accessed 18 October 2020].

Goud, N., 2019. Ransomware Attack On Aebi Schmidt. [online] www.cybersecurity-insiders.com. Available at: <https://www.cybersecurity-insiders.com/ransomware-attack-on-aebi-schmidt/> [Accessed 20 October 2020].

Greenberg, A., 2019. A Guide To Lockergoga, The Ransomware Crippling Industrial Firms. [online] www.wired.com. Available at: <https://www.wired.com/story/lockergoga-ransomware-crippling-industrial-firms/> [Accessed 19 October 2020].

Grubb, B., 2020. 'Cyber Crisis' Deepens At Lion As Second Attack Bites Beer Giant. [online] The Sydney Morning Herald. Available at: <https://www.smh.com.au/technology/cyber-crisis-deepens-at-lion-as-second-attack-bites-beer-giant-20200618-p5540c.html> [Accessed 22 October 2020].

Grubb, B., 2020. Drinks Giant Lion Hit By Cyber Attack As Hackers Target Corporate Australia. [online] The Sydney Morning Herald. Available at: <https://www.smh.com.au/technology/drinks-giant-lion-hit-by-cyber-attack-as-hackers-target-corporate-australia-20200609-p550pu.html> [Accessed 22 October 2020].

REFERENCES

Hacker News, C., 2020. Cyberattacks In Manufacturing Sector - A Clear And Present Danger. [online] cyware.com. Available at: <https://cyware.com/news/cyberattacks-in-manufacturing-sector-a-clear-and-present-danger-b11f72c4> [Accessed 23 October 2020].

Hacker News, C., 2019. Major Airplane Parts Manufacturer ASCO Hit With Ransomware Attack. [online] cyware.com. Available at: <https://cyware.com/news/major-airplane-parts-manufacturer-asco-hit-with-ransomware-attack-a549478c> [Accessed 21 October 2020].

Hacker News, C., 2019. Unknown Ransomware Cripples Computer Systems Of Aebi Schmidt. [online] cyware.com. Available at: <https://cyware.com/news/unknown-ransomware-cripples-computer-systems-of-aebi-schmidt-ffa880fb> [Accessed 20 October 2020].

i-SCOOP, i., n.d. Operational Technology (OT) – Definitions And Differences With IT. [online] i-SCOOP. Available at: <https://www.i-scoop.eu/industry-4-0/operational-technology-ot/> [Accessed 28 November 2020].

Knapp, E. and Langill, J., 2015. Industrial Network Security. 2nd ed. Massachusetts: Syngress, pp.9-40 ,171-207.

Kondo, S., Sakashita, H., Sato, S., Hamaguchi, T. and Hashimoto, Y., 2018. An application of STAMP to safety and cyber security for ICS. 13th International Symposium on Process Systems Engineering (PSE 2018), [online] 44, pp.2335-2340. Available at: <https://www.sciencedirect.com/science/article/pii/B9780444642417503840> [Accessed 17 November 2020].

Leyden, J., 2020. Chipmaker Tower Semiconductor Recovers From Mystery Cyber-Attack. [online] The Daily Swig | Cybersecurity news and views. Available at: <https://portswigger.net/daily-swig/chipmaker-tower-semiconductor-recovers-from-mystery-cyber-attack> [Accessed 23 October 2020].

Lion, 2020. Lion Cyber Incident Update 26 June 2020. [online] Available at: <https://www.lionco.com/media-centre/lion-update-re-cyber-issue> [Accessed 22 October 2020].

REFERENCES

Lyngaas, S., 2019. German Manufacturer Says Malware Has Caused 'Significant Disruption' To Plants In Three Countries. [online] www.cyberscoop.com. Available at: <https://www.cyberscoop.com/rheinmetall-malware-disruption-manufacturing/> [Accessed 20 October 2020].

Lyon, P., 2017. Cyber Attack At Honda Stops Production After WannaCry Worm Strikes. [online] www.forbes.com. Available at: <https://www.forbes.com/sites/peterlyon/2017/06/22/cyber-attack-at-honda-stops-production-after-wannacry-worm-strikes/?sh=6c2522a15e2b> [Accessed 17 October 2020].

McMillan, R., 2010. Siemens: Stuxnet Worm Hit Industrial Systems. [online] Computerworld. Available at: <https://www.computerworld.com/article/2515570/siemens--stuxnet-worm-hit-industrial-systems.html> [Accessed 23 October 2020].

Muncaster, P., 2018. Boeing Computers Hit By WannaCry. [online] www.infosecurity-magazine.com. Available at: <https://www.infosecurity-magazine.com/news/boeing-computers-hit-by-wannacry/> [Accessed 18 October 2020].

NortonLifeLock, n.d. Virus Information - Nimda. [online] www.nortonsecurityonline.com. Available at: <https://www.nortonsecurityonline.com/security-center/virus-information/nimda.html> [Accessed 8 November 2020].

109, n.d. Trojan Found On SCADA Server. [online] Hub.tisafe.com. Available at: <https://hub.tisafe.com/> [Accessed 16 November 2020].

131, n.d. Steel Plant Infection With Ahack Worm. [online] Hub.tisafe.com. Available at: <https://hub.tisafe.com/> [Accessed 26 October 2020].

167, n.d. Malware Shuts Down Milling Factory. [online] Hub.tisafe.com. Available at: <https://hub.tisafe.com/> [Accessed 25 October 2020].

178, n.d. Steel Plant Infected With Conficker. [online] hub.tisafe.com. Available at: <https://hub.tisafe.com/> [Accessed 25 October 2020].

REFERENCES

Paganini, P., 2019. Malware-Based Attacks Disrupted Operations Of Rheinmetall AG And Defence Construction Canada. [online] securityaffairs.co. Available at: <https://securityaffairs.co/wordpress/91813/malware/rheinmetall-dcc-malware-attacks.html> [Accessed 20 October 2020].

Paganini, P., 2017. Pharmaceutical Giant Merck Confirmed Notpetya Attack Disrupted Operations Worldwide. [online] securityaffairs.co. Available at: <https://securityaffairs.co/wordpress/61580/malware/notpetya-disrupted-merck-operations.html> [Accessed 24 December 2020].

Perlroth, N., 2018. A Cyberattack In Saudi Arabia Had A Deadly Goal. Experts Fear Another Try.. [online] www.nytimes.com. Available at: <https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html> [Accessed 24 October 2020].

RISI, n.d. Backdoor Trojan Attack On Manufacturing Lab. [online] Risidata.com. Available at: <https://www.risidata.com/Database/Detail/backdoor-trojan-attack-on-manufacturing-lab> [Accessed 4 November 2020].

RISI, n.d. Blaster Impacts HMI Stations In Smelter. [online] www.risidata.com. Available at: <https://www.risidata.com/Database/Detail/blaster-impacts-hmi-stations-in-smelter> [Accessed 16 November 2020].

RISI, n.d. Infected Laptop Infects SCADA Network. [online] www.risidata.com. Available at: <https://www.risidata.com/Database/Detail/Infected_Laptop_Infects_SCADA_Network> [Accessed 6 November 2020].

RISI, n.d. Malware Shuts Down Milling Factory. [online] www.risidata.com. Available at: <https://www.risidata.com/Database/Detail/malware-shuts-down-milling-factory> [Accessed 25 October 2020].

RISI, n.d. Nimda Impact On Manufacturing System. [online] Risidata.com. Available at: <https://www.risidata.com/Database/Detail/nimda-impact-on-manufacturing-system> [Accessed 8 November 2020].

REFERENCES

RISI, n.d. Paper Company Control System Hit By Blaster. [online] www.risidata.com. Available at: <https://www.risidata.com/Database/Detail/paper-company-control-system-hit-by-blaster> [Accessed 15 November 2020].

RISI, n.d. Reverse Osmosis System PLC Attacked. [online] www.risidata.com. Available at: <https://www.risidata.com/Database/Detail/reverse-osmosis-system-plc-attacked> [Accessed 8 November 2020].

RISI, n.d. Trojan Found On SCADA Server. [online] www.risidata.com. Available at: <https://www.risidata.com/Database/Detail/trojan_found_on_scada_server> [Accessed 14 November 2020].

RISI, n.d. Steel Plant Infection With Ahack Worm. [online] www.risidata.com. Available at: <https://www.risidata.com/Database/Detail/steel_plant_infection_with_ahack_worm> [Accessed 26 October 2020].

RISI, n.d. Steel Plant Infected With Conficker. [online] Risidata.com. Available at: <http://www.risidata.com/Database/Detail/steel_plant_infected_with_conifcker> [Accessed 25 October 2020].

RISI, n.d. Virus Impacts Paper Machine HMI. [online] www.risidata.com. Available at: <https://www.risidata.com/Database/Detail/virus-impacts-paper-machine-hmi> [Accessed 5 October 2020].

RISI, n.d. Zotob, Pnp Worms Hit 13 Automotive Manufacturing Plants. [online] www.risidata.com. Available at: <https://www.risidata.com/Database/Detail/zotob_pnp_worms_hit_13_automotive_manufacturing_plants> [Accessed 27 October 2020].

Roberts, P., 2005. Zotob, Pnp Worms Slam 13 Daimlerchrysler Plants. [online] www.eweek.com. Available at: <https://www.eweek.com/security/zotob-pnp-worms-slam-13-daimlerchrysler-plants> [Accessed 27 October 2020].

Roby, K., 2020. Ransomware Attack: Why A Small Business Paid The $150,000 Ransom. [online] www.techrepublic.com. Available at:

REFERENCES

<https://www.techrepublic.com/article/ransomware-attack-why-a-small-business-paid-the-150000-ransom/> [Accessed 22 October 2020].

Saarinen, J., 2020. Fisher & Paykel Appliances Struck By Nefilim Ransomware. [online] www.itnews.com.au. Available at: <https://www.itnews.com.au/news/fisher-paykel-appliances-struck-by-nefilim-ransomware-549102> [Accessed 21 October 2020].

Security, S., 2018. TSMC WannaCry Hits OT Plants With A Hefty Price Tag. [online] medium.com. Available at: <https://medium.com/@SkyboxSecurity/tsmc-wannacry-hits-ot-plants-with-a-hefty-price-tag-5761cf8c8910> [Accessed 19 October 2020].

71, n.d. Paper Company Control System Hit By Blaster. [online] Hub.tisafe.com. Available at: <https://hub.tisafe.com/> [Accessed 15 November 2020].

72, n.d. Blaster Impacts HMI Stations In Smelter. [online] Hub.tisafe.com. Available at: <https://hub.tisafe.com/> [Accessed 16 November 2020].

Staff, R., 2018. Apple Chip Supplier TSMC Resumes Production After WannaCry Attack. [online] in.reuters.com. Available at: <https://in.reuters.com/article/taiwan-tsmc-virus-idINKBN1KR0B9> [Accessed 19 October 2020].

Staff, R., 2020. Israel's Tower Semi Halts Some Operations After Cyber Attack. [online] U.S. Available at: <https://www.reuters.com/article/us-towerjazz-cyber/israels-tower-semi-halts-some-operations-after-cyber-attack-idUSKBN25X07T\> [Accessed 23 October 2020].

Staff, R., 2017. Honda Halts Japan Car Plant After WannaCry Virus Hits Computer Network. [online] www.reuters.com. Available at: <https://www.reuters.com/article/us-honda-cyberattack-idUSKBN19C0EI> [Accessed 17 October 2020].

Staff, R., 2020. Musk Confirms Tesla Nevada Factory Was Target Of 'Serious' Cyberattack. [online] www.reuters.com. Available at: <https://www.reuters.com/article/us-tesla-cyber/musk-confirms-tesla-nevada-factory-was-target-of-serious-cyberattack-idUSKBN25O07K> [Accessed 22 October 2020].

REFERENCES

Staff, R., 2017. Renault-Nissan Resumes Nearly All Production After Cyber Attack. [online] www.reuters.com. Available at: <https://www.reuters.com/article/us-cyber-attack-renault-idUSKCN18B0S5> [Accessed 18 October 2020].

Strecker, T., 2020. Fisher & Paykel Appliances A Victim Of Ransomware Scourge. [online] www.stuff.co.nz. Available at: <https://www.stuff.co.nz/business/121798667/fisher--paykel-appliances-a-victim-of-ransomware-scourge> [Accessed 21 October 2020].

Sutton, M., 2018. Cyber Attack On Saudi Plant Designed To Cause Explosion. [online] www.itp.net. Available at: <https://www.itp.net/616795-cyber-attack-on-saudi-plant-designed-to-cause-explosion> [Accessed 24 October 2020].

team, I., 2018. TSMC Cyber Attack Was Apparently Caused By WannaCry. [online] Itpro.co.uk. Available at: <https://www.itpro.co.uk/security/31629/tsmc-cyber-attack-was-apparently-caused-by-wannacry> [Accessed 19 October 2020].

Tonkin, C., 2020. Fisher And Paykel Hit By Ransomware. [online] ia.acs.org.au. Available at: <https://ia.acs.org.au/article/2020/fisher-and-paykel-hit-by-ransomware.html> [Accessed 21 October 2020].

Tidy, J., 2020. Honda's Global Operations Hit By Cyber-Attack. [online] BBC News. Available at: <https://www.bbc.com/news/technology-52982427?xtor=AL-72-%5Bpartner%5D-%5Bbbc.news.twitter%5D-%5Bheadline%5D-%5Bnews%5D-%5Bbizdev%5D-%5Bisapi%5D&at_medium=custom7&at_custom1=%5Bpost+type%5D&at_custom3=%40BBCTech&at_custom2=twitter&at_custom4=FFF504CC-AA52-11EA-B622-1CC34744363C&at_campaign=64> [Accessed 7 November 2020].

Truta, F., 2019. Automation Giant Pilz Halts Operations For A Week After Ransomware Infection. [online] securityboulevard.com. Available at: <https://securityboulevard.com/2019/10/automation-giant-pilz-halts-operations-for-a-week-after-ransomware-infection/> [Accessed 19 October 2020].

Update, I., 2019. MANUFACTURING DISRUPTION HIGHLIGHTS THE NEED TO TAKE OT CYBERSECURITY SERIOUSLY. [online] www.industryupdate.com.au. Available at: <https://www.industryupdate.com.au/article/manufacturing-disruption-highlights-need-take-ot-cybersecurity-seriously> [Accessed 19 October 2020].

REFERENCES

Varghese, S., 2020. Attackers Give Lion Deadline For Paying Ransom Of US$800,000. [online] Itwire.com. Available at: <https://www.itwire.com/security/attackers-give-lion-deadline-for-paying-ransom-of-us%24800,000.html> [Accessed 22 October 2020].

Vijayan, J., 2017. Ransomware Attack On Merck Caused Widespread Disruption To Operations. [online] www.darkreading.com. Available at: <https://www.darkreading.com/attacks-breaches/ransomware-attack-on-merck-caused-widespread-disruption-to-operations/d/d-id/1329503> [Accessed 24 October 2020].

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/> [Accessed 7 November 2020].

Whittaker, Z., 2019. Manufacturing Giant Aebi Schmidt Hit By Ransomware. [online] Techcrunch.com. Available at: <https://techcrunch.com/2019/04/23/aebi-schmidt-ransomware/> [Accessed 20 October 2020].

Whittaker, Z., 2020. Techcrunch Is Now A Part Of Verizon Media. [online] Techcrunch.com. Available at: <https://techcrunch.com/2020/06/09/honda-ransomware-snake/> [Accessed 7 November 2020].

Winder, D., 2020. Honda Hacked: Japanese Car Giant Confirms Cyber Attack On Global Operations. [online] Forbes. Available at: <https://www.forbes.com/sites/daveywinder/2020/06/10/honda-hacked-japanese-car-giant-confirms-cyber-attack-on-global-operations-snake-ransomware/?sh=69b3b6c453ad> [Accessed 7 December 2020].

Writer, S., 2020. Tesla's Nevada Factory Was Target Of 'Serious' Cyber Attack. [online] www.itnews.com.au. Available at: <https://www.itnews.com.au/news/teslas-nevada-factory-was-target-of-serious-cyber-attack-552585> [Accessed 22 October 2020].

Zachariah, B., 2020. Russian Citizen Arrested For Tesla Factory Cyber Attack Plot – Report. [online] CarAdvice.com. Available at: <https://www.caradvice.com.au/878712/russian-citizen-arrested-for-tesla-factory-cyber-attack-plot-report/> [Accessed 22 October 2020].

REFERENCES

Zorz, Z., 2019. Danish Company Demant Expects To Suffer Huge Losses Due To Cyber Attack - Help Net Security. [online] www.helpnetsecurity.com. Available at: <https://www.helpnetsecurity.com/2019/10/01/demant-cyber-attack/> [Accessed 13 November 2020].

secolve

OT SECURITY SOLVED

Head Office Address: Level 2, 11 York Street, Sydney, NSW 2000

Contact: info@secolve.com

1800 SECOLVE (732 658)