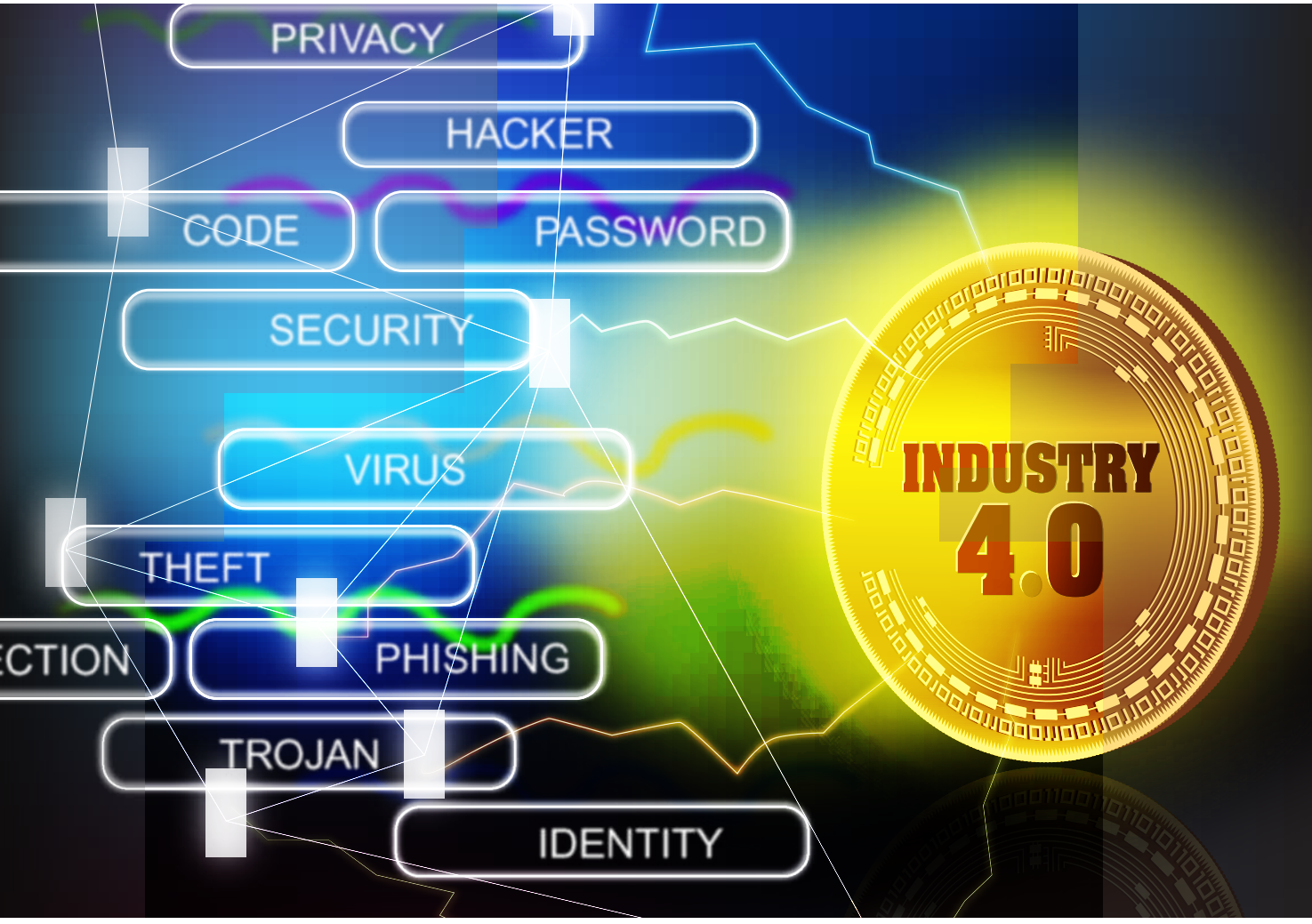


FLIP SIDE OF THE COIN

The industry 4.0 revolution has brought about unprecedented levels of efficiency in manufacturing. But it also comes with its own set of challenges, the biggest one being cybersecurity and the protection of data

By Kruti Bharadva

When Torstein Gimnes Are's phone rang at 4 am in Oslo, Norway, he knew it wouldn't be good news.

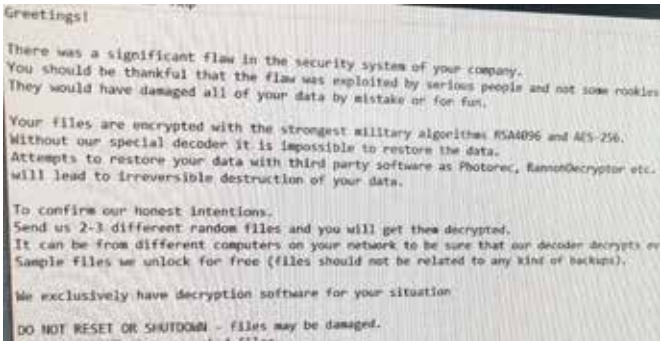
"We may be under attack," were the words from the other end, from Gimnes's IT colleague at Norsk Hydro, one of the world's largest aluminium companies. Production lines had stopped at some of its 170 plants. Other facilities were switching from computer to manual operations.

The breach would ultimately affect all 35,000 Norsk Hydro employees across 40 countries, locking the files on thousands of servers and PCs. The financial impact would eventually approach $71 million. All this damage had been set in motion three months earlier when one employee unknowingly opened an infected email from a trusted customer and allowed hackers to invade the IT infrastructure and covertly plant their virus.

The cyberattack on Norsk Hydro is perhaps one of the most well-known, and certainly the most well documented as the company made a swift and unshakeable decision in face of the ransom demands – Transparency. We shall circle back to this vital point, but first a look down to the very roots of cyber security in manufacturing.

THE ROLE OF INDUSTRY 4.0

McKinsey defines Industry 4.0 as 'the next phase in the digitisation of the manufacturing sector, driven by four disruptions: The astonishing rise in data volumes, computational power, and connectivity, especially new low-power wide-area networks; the emergence of analytics and business intelligence capabilities (BI); new forms of human-machine interaction such as touch interfaces and augmented-reality systems; and improve-



Ransomware note at the Norsk-Hydro attack

ments in transferring digital instructions to the physical world, such as advanced robotics and 3-D printing.'

Industry 4.0 is followed by 'the smart factory.' More than just the latest buzzword, the smart factory is a confluence of trends and technologies that are reshaping the way things are made and revolutionising the way factories function. Industrial control systems (ICS), supervisory control and data acquisition (SCADA) systems, big data, the Internet of Things (IoT), the Industrial Internet of Things (IIoT), smart and self-learning machines, advanced analytics, robotics, and cognitive computing all fall under the Industry 4.0 umbrella.

There's a lot to be gained by adopting Industry 4.0 technologies, and Indian manufacturing seems to be at the forefront of 'talking' about doing so. Why then, has the adoption of industry 4.0 not kept pace with expectations? The answer is simple: Security.

As it continues to adopt Industry 4.0, the manufacturing industry becomes an increasingly appealing target for attackers, who have the opportunity to move laterally across a manufacturing network, jumping across IT and OT systems for their malicious activities. Without strong protections in place, bad actors can take advantage of systems for industrial espionage, intellectual property theft, IP leakage, or even production sabotage.

THE SITUATION IN INDIA

According to the annual IBM X-Force Threat Intelligence Index, India reported the second-highest number of cyber-attacks after Japan in the Asia-Pacific region in 2020. The report additionally states that India accounted for 7 per cent of all cyber-attacks observed in Asia in 2020 and that finance and insurance were the top attacked industry in India (60 per cent), followed by manufacturing and professional services.

The 2020 threat landscape in India was largely shaped by the pandemic. As the pandemic's timeline of events and progress unfolded, so did attack trends shift. Ransomware was the top attack type in India with a 40 per cent share in the overall threat landscape. Further, digital currency mining and server access attacks hit Indian companies last year. We also witnessed cybercriminals using relief efforts and public health information as spam lures including targeted attacks on critical components of the vaccine supply chain.

In essence, the pandemic reshaped what is considered critical infrastructure today, and cyber attackers took note. Many organisations were pushed to the front lines of response efforts for the first time – whether to support Covid-19 research, uphold vaccine and food supply chains, or produce personal protective equipment. Cyberattacks on healthcare, manufacturing, and energy doubled from the year prior, with threat actors targeting organisations that could not afford downtime due to risks of disrupting medical efforts or critical supply chains. Attackers took advantage of the nearly 50 per cent increase in vulnerabilities in industrial control systems (ICS) – on which manufacturing and energy greatly depend.

INDUSTRY 4.0 CYBERSECURITY CHALLENGES

Manufacturing is the second-most attacked industry, yet the manufacturing sector lags when it comes to security. Smart factories can be subject to the same vulnerability exploitation, malware, denial of service (DoS), device hacking, and other common attack methods that other networks face. And the smart factory's expanded attack surface makes it extra difficult for manufacturers to detect and defend against cyberattacks. These threats now work on an entirely new level with the dawn of the IoT, and they can result in serious physical consequences, especially in the realm of the IIoT.

Here are a few new security challenges that organizations face in the age of Industry 4.0:

- Every connected device represents a potential risk
- Manufacturing systems such as Industrial Control Systems (ICS) have unique vulnerabilities that

make them particularly susceptible to cyberattacks

- Industry 4.0 connects previously isolated systems, which increases the attack surface
- Upgrades are often installed piecemeal since the systems are very complex
- Manufacturing has many fewer regulated compliance standards than other sectors
- Visibility is poor across separate systems and isolated environments

Also, note that the battle is decidedly unbalanced. While organizations must protect a wide swathe of technology over a very large attack surface, attackers need only pinpoint the weakest link.

TOP 5 MANUFACTURING CYBERSECURITY THREATS

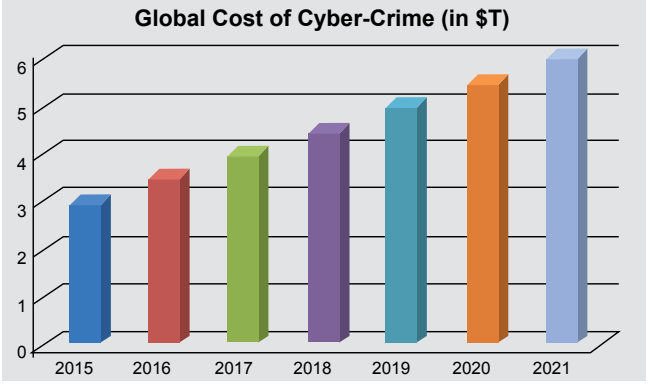
The evolution of cybercrime is constant. If you are a manufacturer, it's imperative to understand the biggest dangers you are facing so that you can brace for them. We've rounded up five of the most common cybersecurity threats manufacturing companies come up against:

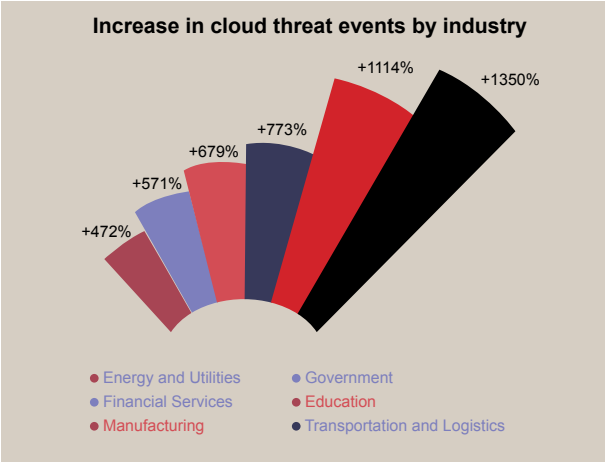
1. **Intellectual Property Theft**
   The technology-driven world in which we live has made IP theft easier. Unfortunately, it's often overlooked in favour of other types of cyber-attacks. For manufacturing firms, where IP- through innovation and creativity- is often a driving force behind their success, this is a critical risk area.
2. **Phishing**
   No matter what industry your business operates in, phishing is a constant threat. It's also one of the oldest threats and it continues to be one of the most widespread forms of attack.

   To carry out deadly phishing attacks, hackers utilise a tool that workers are on and checking multiple times a day — email. And while certain tools can help prevent phishing, it's ultimately an attack on humans, not systems or networks. It all starts with a malicious email that's disguised as a trustworthy one. The goal is for targets to believe the email is reliable, leading them to click a link or download an attachment.

   What's especially alarming about phishing attacks in 2020 is how sophisticated and convincing they are getting. Many individuals assume they can easily spot phishing emails. However, criminals are getting extremely good at imitating emails from authoritative and trustworthy sources, making it much easier than people think to fall for a phishing scam.
3. **IoT Attacks**
   IoT solutions can decrease supply-chain risk, ensure high-quality products, and increase efficiency. However, connected IoT systems come with an inherent downside. They can enable deadly cyber-attacks that allow a criminal to infiltrate your network through your devices. Often, organizations pay less attention to securing IoT devices than other aspects of their network. And because these devices connect to the internet, they can open a doorway for hackers if left unprotected. When these devices affect critical systems, one successful IoT attack can halt the entire manufacturing process. And we all know that with downtime, come costs.
4. **Supply Chain Attacks**
   Now more than ever, manufacturing firms receive and supply sensitive information to many different enterprises. From vendors to partners, these digital touchpoints allow for more efficient and effective operations. In a supply chain attack, a hacker will gain access to a partner or provider that has access to your systems and data. Through this relationship, the criminal can enter your network, steal your data, and cause significant harm to your company. To manage this third-party risk, manufacturers need to be extremely aware of who they are sharing information with and what cybersecurity measures these partners have in place. It's no longer enough to worry about your own company's safeguards. You need to protect your data and systems from every point.
5. **Ransomware**
   Ransomware is an increasingly dangerous threat and, unfortunately, all too common. Every business is in fear of a ransomware attack, but for manufacturers especially, it can cost them everything.

   This deadly malware variant usually infects your systems when an unsuspecting employee accidentally clicks on a malicious link or attachment in a phishing email. And once someone opens this door for ransomware to creep in, it encrypts an organisation's data, possibly spreading throughout the entire network. To regain access to their information, companies must pay the requested ran-





som, which is often enormous. Not to mention, the cost of downtime.

THE ISSUE OF TRANSPARENCY

In November 2019, The Nuclear Power Corporation of India Limited (NPCIL) confirmed that there had been a cyberattack on the Kudankulam Nuclear Power Plant (KKNPP) in Tamil Nadu, India, in September. The nuclear power plant's administrative network was breached in the attack but did not cause any critical damage. KKNPP plant officials had initially denied suffering an attack and officially stated that KKNPP "and other Indian Nuclear Power Plants Control Systems are stand-alone and not connected to outside cyber network and Internet- and any Cyber-attack on the Nuclear Power Plant Control System was not possible." This statement brings forward the issue of transparency, something lagging quite behind in the Indian manufacturing sector.

Back to Norsk Hydro, their decision to be 'transparent' gained accolades from security experts around the world because it bucked the usually secretive responses many organizations employ after getting hacked. Senior staff hosted daily webcasts and answered audience questions. Executives held daily press conferences at their Oslo headquarters posted updates to Facebook, welcomed journalists into their operations control rooms – and even launched a new company website during the attack's first week.

In India, an organisation which is working towards bringing about change is the Data Security Council of India (DSCI) - a not-for-profit, industry body on data protection in India, set up by NASSCOM®, committed to making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cybersecurity and privacy. To further its objectives, DSCI engages with governments and their agencies, regulators, industry sectors, industry associations and think tanks for policy advocacy, thought leadership, capacity building and outreach activities.

DSCI also endeavours to increase India's share in the global security product and services market through global trade development initiatives. These aim to strengthen the security and privacy culture in India.

EMERGING INDUSTRY 4.0 BEST PRACTICES FOR ENHANCED SECURITY

As more connected systems are deployed and the opportunities for an attack against intellectual property increase, protecting against evolving threats is becoming a full-time task.

The manufacturing sector needs to:

- Adopt a risk-based security mindset (tying business criticality to defence strategies)
- Keep an accurate inventory of all OT assets in real-time
- Marry the best of IT and OT as an integrated defence strategy across all attack surfaces
- Identify and fix outdated systems, unpatched vulnerabilities and poorly secured files
- Take a security-first approach to the deployment of new connected systems
- Remain ever vigilant to spot potential threats with real-time vulnerability assessments and risk-based prioritisations
- Ensure that technology suppliers and connected equipment manufacturers commit to regular security and software patches and audits
- Threat intelligence, including monitoring of the dark web, can also act as an early warning system to uncover planned attacks. Thus, the organisation can pre-empt a breach and take immediate action to protect its digital corporate assets and physical infrastructure

TAKING BACK CONTROL

The combination of elevated security processes, enhanced training and manufacturing industry-specific security solutions is helping progressive organisations to reduce the risk of cyber-attacks.

This approach is also allowing breaches to be discovered more quickly while mitigating damage. There is still no "magic bullet" that will guarantee complete protection but the journey towards better security often starts with a security assessment. Typically, the assessment would start with non-intrusive network traffic recording, with no interruption to ongoing production (OT) operations. This would be used to create a clear, drill-down visualization of the OT network topology including all connected assets along with detection of all known vulnerabilities and analysis of the risks to the customer network with a prioritized risk-mitigation plan.

In the end, cybersecurity best practices will certainly be key to the success of Industry 4.0.