Security in the era of Industry 4.0

The manufacturing sector is in the midst of the fourth industrial revolution. Smart, connected technologies are bringing together the digital, physical and biological spheres.

What is commonly referred to as Industry 4.0 is being driven by increased interconnectivity and digitization of production technologies and processes. The possibilities emerging for manufacturers to connect people, machines, factories and digital workspaces are endless.

This Industry 4.0 transformation process promises huge productivity benefits – but also poses a new wave of security threats.

"The fourth industrial revolution represents an unprecedented opportunity through interconnectivity," says Stephen Phipson CBE, Chief Executive, Engineering Employers' Federation. "But that very openness brings with it increased risk. Cyber-vulnerability is a major barrier to business and growth; threatening loss of data, theft of capital and intellectual property, disruption to business, and impact on trading reputation."[1]

"The fourth industrial revolution represents an unprecedented opportunity through interconnectivity"

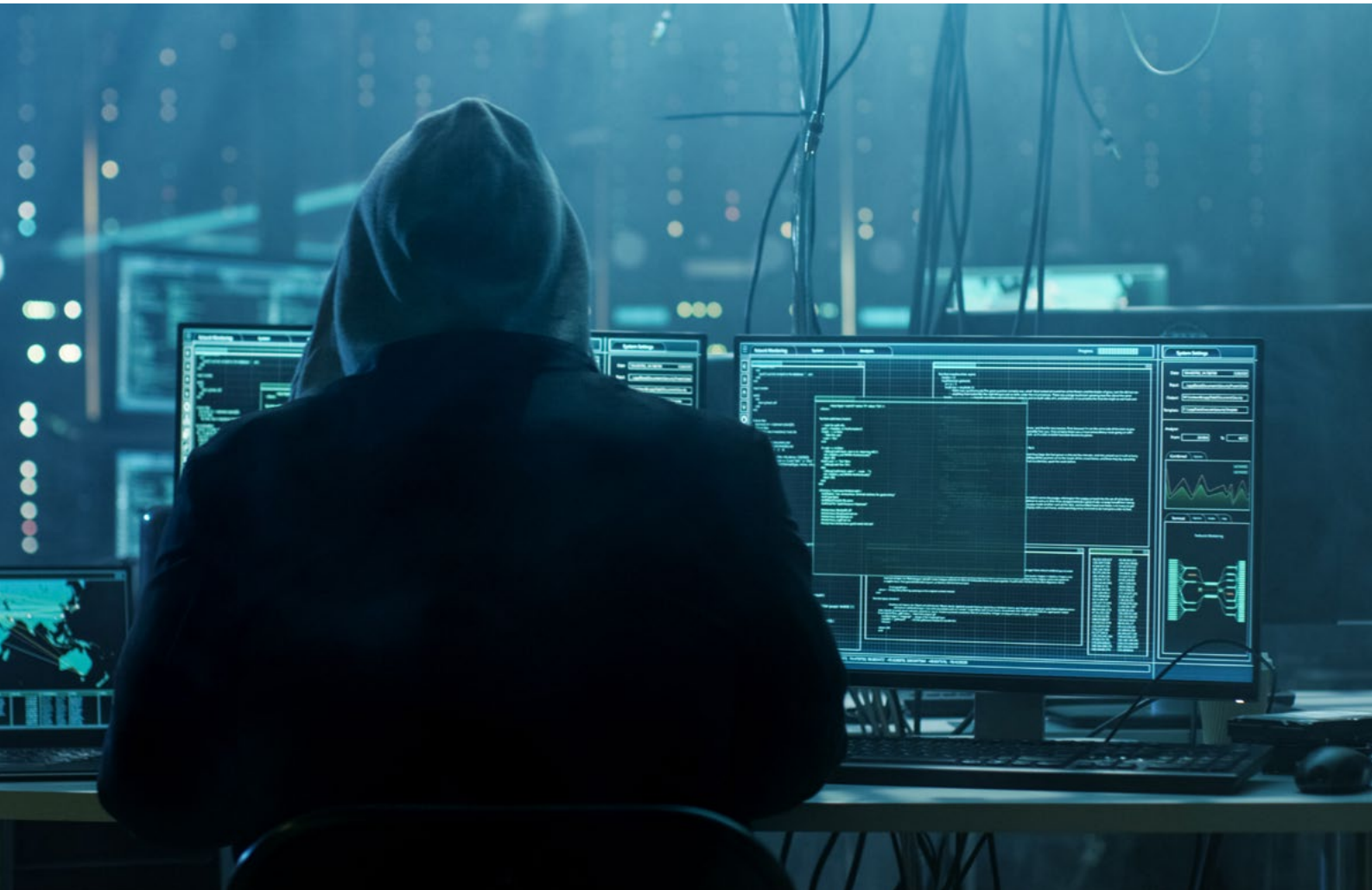
Manufacturing attacks

Today's manufacturing industry is increasingly a target for sophisticated cyber-criminals. Barely a month goes by without a targeted cyber-attack on a large manufacturing business hitting the headlines.

In March 2019, for example, one of America's largest beverage manufacturers was the victim of a ransomware attack that knocked out more than 200 of its servers and networked computers.[2] On that occasion, Arizona Beverages was forced to bring in an external security consultant at a cost of "hundreds of thousands of dollars", following profit-sapping weeks of downtime.

In April 2019, Aebi Schmidt, a Swiss airport maintenance manufacturer with operations worldwide was hit by a similar ransomware attack, in which the company's Windows network had been compromised by a virus, resulting in various systems having to be shut down and numerous employees sent home.[3]

These and other recent high-profile cases of cyber-attacks on smart factories are just the tip of the iceberg as many victims choose to never go public.[4] Each attack presents its own unique range of security issues and challenges. This is why it is increasingly vital that modern manufacturers are both educated and aware of security best practice for Industry 4.0.



Security laggards

A recent research report by digital security analyst Trend Micro warns that manufacturing is "significantly behind" others and thus particularly vulnerable to cyber-attacks.[5]

The shift to Industry 4.0 encourages a closer relationship between information technology (IT) and operational technology (OT).

An increasingly symbiotic connection between management and production ushers in a number of sector-specific security challenges. These include support for older equipment, aging technologies and regular software patching.

As such, today's manufacturing industry is a security laggard – and therefore a prime target. The sector is over-reliant on out-of-date operating systems and old technologies for transferring data. Plus, valuable digital IP content is at a high risk of theft from a multitude of malicious files.

The human factor

Human-machine interfaces are still the most popular way for hackers to find their way into a manufacturer, which might involve staff receiving and clicking on unsolicited emails or browsing phishing sites on the web. This approach accounts for 60%[5] of equipment exploits and shows critical processes can be tampered with.

The prevalence of these types of security vulnerabilities in the manufacturing sector are the reason why the industry is such a major target for cyber-criminals looking to steal IP, extort cash or simply cause mayhem.

This cybersecurity problem is compounded by a widely perceived lack of cybersecurity expertise from professionals on the inside.[6]

So, for example, according to a recent report by AIG and Make UK, 41%[6] of manufacturers don't believe they have enough relevant security information to even assess their true cyber risk, while 45%[6] feel they don't have access to the right tools to properly protect themselves.

Over a third (35%)[1] of those manufacturers surveyed say cyber threats are holding them back from fully investing in new digital technologies in readiness for Industry 4.0. While 12%[1] of companies admit to having no technical or managerial processes in place to even start assessing the real cybersecurity risk they face.

Remaining secure

It is imperative that manufacturers follow industry best practice digital security tips to remain secure:

1. Secure networks with up-to-date firewall protection.
2. Choose hardware designed with built-in security, to help protect devices, detect intrusion, and have the ability to recover from breach.
3. Check new peripherals and add-on technologies are integrated into security protocols.
4. Disable all unnecessary ports and network services, and set all devices and software to secure settings.
5. Properly police access to devices and services.
6. Segment your network and implement access controls across domains and subnetworks.
7. Use antimalware solutions, download from manufacturer-approved stores and run apps and programs in an isolated environment.
8. Consistently check that operating systems, software and firmware are up-to-date and running the latest security patches.
9. Regularly audit employees, devices, and software in your infrastructure.
10. Educate employees on practising good cyber security behaviour, including password management and reporting of suspicious phishing emails or any other activity.

How HP can help

Cybersecurity is a critical technological challenge for manufacturers in the age of Industry 4.0. With over 25 years of experience in reinventing and continuously innovating in endpoint security, HP can help manufacturers protect valuable data, documents and devices from the most sophisticated cyber-criminals. Across HP's portfolio, we address security from the very early design phases of our hardware, solutions and services offering, to help customers stay ahead of a degrading threat landscape.

In addition to how we address security in our offering, HP continues to invest in longer-term research at HP Labs, with our Security Lab working closely with HP businesses and external partners to continuously analyse emerging threats, and create the cybersecurity innovations that will help our manufacturing customers safely capitalize on the productivity opportunities of Industry 4.0, securely and affordably.

1. AIG and Make UK report, 2018: https://www.makeuk.org/Insights/Reports/2019/02/11/Cyber-Security-for-Manufacturing
2. Washington Times, Arizona Beverages, April 2019: https://www.washingtontimes.com/news/2019/apr/2/arizona-beverages-hacked-in-targeted-ransomware-at/
3. TechCrunch, Aebi Schmidt, April 2019: https://techcrunch.com/2019/04/23/aebi-schmidt-ransomware/
4. Smart Machines and Factories, May 2019: https://m.smartmachinesandfactories.com/news/fullstory.php/aid/459/Cyber-attacks_on_smart_factories_are_on_the_rise.html
5. Trend Micro research, April 19: https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/security-in-the-era-of-industry-4-dealing-with-threats-to-smart-manufacturing-environments?ClickID=c4nnnv7sz74wlvvz7akweq4xfskpansqskz. Direct white paper link: https://documents.trendmicro.com/assets/white_papers/wp-threats-to-manufacturing-environments-in-the-era-of-industry-4.pdf
6. AIG and Make UK report, 2018: https://www.makeuk.org/Insights/Reports/2019/02/11/Cyber-Security-for-Manufacturing

c-06429786, August 2019