RISE OF INDUSTRIAL 4.0: CRIPPLING A COUNTRY THROUGH CYBER ATTACKS IN MANUFACTURING
TABLE OF CONTENTS

1. ABSTRACT
2. HISTORY
3. EUROPEAN CYBER ATTACKS
4. IOT IN MANUFACTURING
5. INTELLIGENCE GATHERING AND ANALYSIS
6. CONCLUSION
Cyber Security in Industry 4.0: 
The Pitfalls of Having Hyperconnected Systems

MAURICE DAWSON
Assistant Professor, School of Applied Technology, Illinois Institute of Technology

Abstract

The fourth industrial revolution is referred to as Industry 4.0. The current trend with manufacturing is automation and unparalleled levels of data exchange. To bring this trend to realization requires integrating the Internet of Things, Internet of Everything cyber-physical systems, cloud computing technologies, and more into manufacturing. Industry 4.0 involves a hyperconnected system that includes the smarter use of robotics to effectively and efficiently move to manufacture to new heights. With the use of all these technological systems, it is imperative to ensure that cyber security plays a role during the rise of this digital industrial revolution. In the United Kingdom, more than eighty manufacturing plants were hit by cyber attacks while threats in this specific industry have risen. The pitfalls of having hyperconnected systems leave an entire industry even more vulnerable than the traditional enterprise system design.

Keywords:
cyber security, risk management, internet of things, hyperconnectivity
A LITTLE HISTORY

FIRST INDUSTRIAL REVOLUTION
Mechanization, water power, steam power

1750-1850

THIRD INDUSTRIAL REVOLUTION
Computer and automation

1870-1914

SECOND INDUSTRIAL REVOLUTION
Mass production, assembly line, electricity

1980s

FOURTH INDUSTRIAL REVOLUTION
Cyber Physical Systems

CURRENT
Manufacturing cyberattacks could cripple the UK

The potential for international cyberwarfare could put manufacturers in the firing line as hackers go after vital services and large-scale industrial facilities.

"Cyberspace is already an active battleground, with state and non-state actors continuously searching for adversaries' vulnerabilities, trying to obtain secret information, developing weapons and occasionally deploying them."
Estonia’s crisis was merely a taste of things to come. Another major incident occurred the following year. It was believed to have secretly launched Stuxnet, a malicious computer worm, to sabotage centrifuges at a uranium enrichment plant in Iran. The Iranian authorities didn’t even realise the nuclear plant had been under attack until two years later.
OUTBREAK: THE FIRST FIVE VICTIMS OF THE STUXNET WORM

The infamous Stuxnet worm was discovered in 2010, but had been active since at least 2009. The attack started by infecting five carefully selected organizations:

- Foolad Technic International Engineering Co, ICS vendor
- Behpajooh Co. Elec & Comp. Engineering, ICS vendor
- Neda Industrial Group, component supplier
- Control-Gostar Jahed Company, ICS vendor
- Kala Electric, Centrifuge developer
Nearly half of all UK manufacturers have experienced cyberattacks

And manufacturers could end up first in the firing line if a major cyberwar were to erupt. But nation states are far from being the most immediate threats or perpetrators. “Low-level non-state actors can still be reasonably well resourced and cause a lot of damage,” says Corey Milligan, one of the US Army’s first cyber-operations technicians and now a senior threat intelligence analyst at Armor Defense, a cloud security firm in Texas.

“These days cybercrime as a service is thriving. People can be hired through third parties to conduct espionage against rival companies to track disruptive technologies and uncover proprietary manufacturing processes to attempt to reduce their competitive advantages.”

As cybercrime reaches epidemic scales, manufacturers could find themselves sleepwalking into a disaster zone if they do not batten down the hatches.

Last April, a report by the UK manufacturers’ association Make UK and insurer AIG found that nearly half of UK manufacturers had been subject to cyberattacks. A quarter of these attacks resulted in financial and business losses. Yet 45 per cent were not confident they had the right tools to protect themselves.

Similarly in Germany, Europe’s largest economy, as many as two thirds of manufacturers said they were affected by cyberattacks over a two-year period, according to Bitkom, losing a total of $50 billion.
Manufacturers need to get wise or the country could suffer

Ironically, manufacturers are often a desirable target due to the sheer complexity of their processes. “Look at critical infrastructure for generation of electricity, water, services and so on. The challenge is in the uniqueness of the devices involved,” says Mr Milligan. “Just to evaluate the risks requires specialised training on how the individual devices work. You then need to go in and do the work of securing the systems. It’s a difficult, expensive and painstaking process.”

But he warns that unless manufacturers get on the case, they will face mounting costs from incoming government regulation; costs which some fear could put the brakes on the progress of the fourth industrial revolution.

But according to Professor Maurice Dawson, director of the Center for Cyber Security at the Illinois Institute of Technology, that could be the least of industry’s problems. In his view, the “hyperconnectivity” between smart robots and the cloud could leave entire sectors vulnerable to large-scale attacks with catastrophic cascading effects. At worse, these could take a chunk out of a country’s GDP.
Tampering with equipment in factories producing food, for instance, could lead to incorrect nutrient levels and unsafe items bypassing proper checks.

“Imagine a large organisation like Monsanto. A determined hacker has the ability to go in and change the makeup of the seed,” says Professor Dawson. “They could make the seed life shorter. If you’re planning for a harvest, the seeds fail. Now we have an issue of a food shortage. Or alternatively, the hacker can insert additives or ingredients to spark allergies or create reactions.”
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>R Language</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wireshark</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>KaliLinux</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Open Source Intelligence Techniques</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Python</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Metasploit</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Libre Writer</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Libre Impress</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Libre Calc</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pontoon (Translation Service)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Social Media</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>R Studio</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>KNIME</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LibreNMS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**FIGURE 6** Open Source Applications to Use During Intelligence Cycle
CONCLUSION

BASELINE
As this new industrial revolution is taking ground it will be key to establish what a baseline secure configuration would be for this manufacturing plants.

CERTIFICATION & ACCREDITATION
This will include a minimum set of security controls every organization will need to have before gaining an Approval to Operate (ATO).

TIGHTER REGULATIONS
This will include tighter regulatory polices, employee education, and hardened technology that is used within the boundaries of the network.