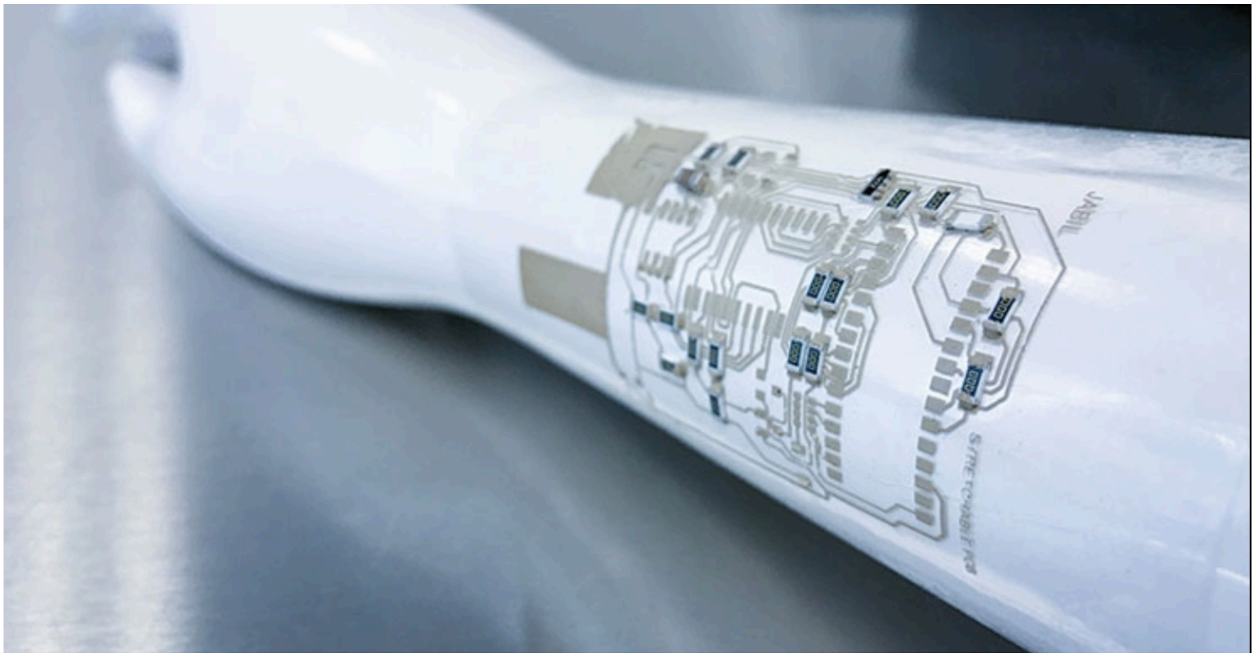

Cybersecurity Challenges for Flexible Hybrid Electronics Manufacturers

Executive Summary

Flexible Hybrid Electronics (FHE) manufacturing creates flexible, conformable devices with electronic capabilities. Combining both printed and advanced CMOS-based components on a flexible, plastic polymer film, FHE delivers a combination of flexibility with communication and processing capabilities that make it well-suited for Industrial Internet of Things (IIoT) devices, ranging from wearables and military applications to prosthetics and medical sensing. The FHE market, valued at just $95 million in 2019, is projected to grow to $3 billion by 2030. The FHE industry's membership organization NextFlex has invested $113 million to advance the commercialization of FHE.

Yet new data shows that the path forward could be a risky one for FHE manufacturers. The manufacturing sector is a growing target for cyberattacks, ranking second only to the finance sector in 2020. The electronics manufacturing industry—and FHE in particular—are at an even higher risk of cyberattack by malicious actors and a growing number of nation-states for several reasons: (1) FHE interconnectivity with IoT offers numerous access points; (2) the complexity of the manufacturing ecosystem offers a large attack surface for ransomware and corporate espionage; and (3) many FHE companies are small and medium-sized enterprises (SMEs), long considered to be low-hanging fruit by cybercriminals.

A recent report shows that more than 80 percent of electronics companies are implementing IIoT technologies in plants and assembly lines without thoroughly evaluating the risks or instituting standard security protocols. Regulatory compliance around FHE is growing, but compliance might not be enough. To ensure survival in this threat-laden environment—and to protect a burgeoning industry from malicious actors—manufacturers need to understand the looming threats that are customized to their unique processes. The call: to tackle threats quickly and decisively. When it comes to cyberattacks, it’s not a matter of if, but when.

Introduction

While flexible electronics manufacturing has existed for more than a decade, there was always a trade-off between flexibility and capability that limited its applications for smart technologies. Enter flexible hybrid electronics manufacturing (FHE), which prints rather than etches conductive interconnects, and the possibilities for new applications are seemingly endless. The flexibility, processing capability, and compatibility of FHE, combined with low-cost, high-volume manufacturing, make it suitable for many applications.

Customizable and environmentally friendly, FHE is fundamentally changing electronics manufacturing to open up a new generation of applications in Industrial Internet of Things (IIoT), from wearable healthcare monitoring and industrial/environmental monitoring to innovations in automotive and aeronautical.

That said, integration with Industrial Internet of Things (IIoT) solutions is also one of the many vulnerabilities of FHE regarding cybersecurity. It's no secret that manufacturing as a whole has been a prime target for malicious actors waging ransomware and acts of espionage. Add the complexity of the IIoT supply chain and the status of many FHE as small and medium-sized enterprises (SMEs), and the potential for a data breach or cyberattack is multiplied. As the nascent FHE evolves along with IIoT, the industry and its players must prioritize cybersecurity practices to ensure a robust, resilient manufacturing process. Here we will look at the cyber threats looming for small and medium-sized manufacturers in the U.S., many of which have already impacted larger and off-shore electronics manufacturers. Its distinct abilities in customization, form factor, signal, and robustness have made it highly adaptive to IIoT-type solutions, which, it turns out, is also one of the industry's vulnerabilities.

BACKGROUND

With great opportunity comes inherent threats. The more valuable FHE becomes, the more its processes will be coveted, disrupted, and stolen by bad actors. Here's a snapshot of the current threat landscape and the challenges it poses to manufacturing:

Because the technology is so cutting-edge, the desire to possess it is extremely high for both corporate competitors and foreign governments. As a result, the risk to the manufacturing sector is increasing, with cyberattacks impacting industrial processes, enabling information gathering, and increasing the theft of intellectual property (IP). Here are other key reasons for the increased threat of cyberattacks to FHE companies:

1. Cyberattacks are increasing in size and severity across all industries.
As cyber criminals worldwide become more sophisticated, cyber threats are worse for every industry across the board. In addition to the growing sophistication of cybercriminals, there is a shortage of skilled security personnel nationwide. Cyberattacks across five major U.S. industries have grown, in order:

- Government
- Manufacturing
- Services
- Education
- Healthcare

2. The manufacturing sector is especially vulnerable.
Manufacturing lags behind almost every other industry when it comes to implementing cybersecurity policies and protocols. A new study of manufacturing revealed that 50 percent of companies reported having experienced a data breach or cyber-attack within the previous 12 months.

3. SMEs are targeted at a higher rate than large enterprises.
Small and medium businesses typically lack resources (money and people) and industry protocols in a burgeoning field. And cyber-attacks are not only more likely for SMEs—they typically have greater consequences. The repercussions are fast and long-lasting for SMEs, and they can be the blow that finally brings a struggling company to its knees.

SIDEBAR
Sixty percent of SMEs that experience a data breach or cyberattack shutter their businesses within six months due to bankruptcy or inability to recover.

SMEs with under 50 employees rarely have a dedicated IT department. All it takes is one technician to disable software or skip a regular software update, and the gates are open to cybercriminals. Further, antivirus and anti-spam software used by SMEs rarely covers all forms of attack.

COVID-19: A PERFECT STORM

The COVID-19 pandemic created an unprecedented environment for bad actors:

1. **Remote work**

Throughout the pandemic, commercial IoT systems, which were made vulnerable by the shift to remote work and the ensuing lack of network control, saw a considerable increase in cyber-attacks, many of which were novel.

2. Budget cuts after COVID

Twenty-four percent of manufacturing companies were expected to cut their security budgets after the crisis.

3. COVID-19 information as a way into networks

Many bad actors used COVID as a theme for social engineering, a form of phishing that exploited manufacturing employees' safety and health concerns regarding the pandemic. These factors, coupled with the persisting tendency to treat IoT security as an afterthought, make post-crisis IIoT projects—or scaling-up of existing systems—a high-risk undertaking.

4. IIoT—helpful, but not

While IIoT development became instrumental in ensuring continuity and safety at production sites, it was a double-edged sword for manufacturers: production of IIoT can place a company's entire ecosystem at risk. A new study found that more than 80 percent of electronics companies are implementing IIoT technologies in plants and assembly lines without thoroughly evaluating the risks or implementing cybersecurity protocols.

Interconnectivity

Many electronics manufacturing companies don't adequately protect against cyberattacks when implementing Industrial Internet of Things (IIoT) sensors and technologies. Because of its interdependence on IIoT, the manufacturing supply chain is integrated, interconnected, and complex. Each point in the process is a potential access point for unauthorized entry.

The Cost of a Breach

Whether caused by cyber hackers, competing companies, foreign states engaged in corporate espionage, or even disgruntled employees, losses can mount quickly once under attack. The risks include equipment failure, loss of critical data, loss of reputation and market share—and even injury and loss of life. Add to that the consequences of non-compliance with growing regulatory issues, and the costs of a breach or attack can be incalculable.

Compliance & Consequences

Compliance regulations around cybersecurity are designed to protect you, the manufacturer, as well as the industry at large. Data in the wrong hands can threaten national security, fair trade, global economic competitiveness, and more.

Compliance requirements are increasing, particularly for FHE companies involved in the U.S. military supply chain. They will likely become more stringent as bad actors find new ways to infiltrate our nation's infrastructure. This pressure comes with the need for SMEs to keep costs down and remain competitive. Depending on who your customers are, your company will likely be subject to a growing list of regulatory agencies, each with their respective requirements and consequences for non-compliance. Compliance requirements that will affect many businesses in the Industrial IoT space include:

DFARS/SP 800-171

Any company doing with the federal government must meet standards outlined in NIST-800-171. The cost of non-compliance could be the loss of existing contracts. Once you become known for non-compliance, business partners will be required to stop working with you, and you may be barred from taking on federal contracts with federal agencies, including DoD and the General Services Administration (GSA).

Cybersecurity Maturity Model Certification (CMMC)

Any firm working as a contractor or sub-contractor for DoD needs to comply with the Cybersecurity Maturity Model Certification (CMMC). Announced in January 2021, the requirement won't be enforced until 2026. The cost of CMMC non-compliance is high for defense contracts and subcontractors of all sizes, as they will be barred from participating in DoD contracts in any capacity.

International Traffic in Arms Regulation (ITAR)

If your company sells to DoD or sells to a company that sells to DoD, you need to be ITAR-compliant. Non-compliant companies can face fines up to $500,000 per occurrence—and company executives can be fined and imprisoned.

The Big Picture for Compliance

Adding to the heightened vulnerability of manufacturing SMEs is the growing realization that the manufacturing industry holds essential and sensitive information, including intellectual property and customer data. The fallout of cybercrime reaches far and wide:

National Security

The negative impact on defense can be incalculable. People often associate national “threats” with matters of political upheaval or nuclear weapons. Concern about equally serious threats—hacking and malicious software—can seem almost negligible. But the threat to industrial electronics is real, and it can be a matter of life or death. In 2016, hackers managed to infiltrate a U.S. water treatment plant. Were it not for the timely detection of chemical mixture alterations, millions of people would have been poisoned.

Global Economic Power

Robotics, artificial intelligence, and sensor networks will continue to transform defense and commercial activities for years to come. If adequately protected, that progress will have a positive effect on the U.S. economy. As President Biden has pointed out, [if U.S. companies were better protected in the past], “many of the products that are being made abroad would be made here today.”

The Top Cybersecurity Threats

Phishing, malware, ransomware, and corporate espionage are the most common types of cyberattacks against SMEs because they are the most profitable to criminals.
And they’re effective because of SMEs' lack of preparedness to protect and defend against threats. Phishing isn't software but rather the process, usually in email form, of emails, of deceiving workers into volunteering confidential information or clicking on links containing malware.

Cyberattacks come in different forms, through several avenues, with ransomware leading the pack. How they line up:

1. Ransomware and malware (phishing is the most common avenue)
2. Nation-state espionage
3. Internal threats (both deliberate and unwittingly/through human error)

Phishing, malware, ransomware, and corporate espionage are the most common types of cyberattacks against SMEs because they are the most profitable to criminals. And they're effective because of SMEs' lack of preparedness to protect and defend against threats.

RANSOMWARE AND MALWARE

Ransomware is a type of malware that encrypts data on infected computers. It enables cybercriminals to extort money from victims while encrypting files that the host computer needs. Targeted ransomware is the new pervasive threat to manufacturing. The sudden convergence of interconnected enterprise and operations networks is contributing to the rapid increase in attacks, which increased by 40 percent to 199.7 million cases globally in the third quarter of 2020.

Malware, on the other hand, is any file or malicious code designed to damage a user's personal computer and network. Malware was behind the 2020 supply chain attack on SolarWinds' Orion IT management software. Bad actors were able to distribute malicious code via the software's automatic update mechanism. This single point of entry led to multiple downstream targets, and the average impact to each business was 11 percent of their respective annual revenue, an average of $12 million per company. Cleaning up the SolarWinds hack may cost as much as $100 billion as government agencies and corporations spend billions of dollars to root out the malicious Russian code.

PHISHING

A 2020 study revealed that the manufacturing industry was the most targeted by phishing attempts, with almost 40 percent of attacks aimed at the sector. Phishing is not a set of malicious code, but rather a means for extracting sensitive data from unsuspecting employees or installing ransomware and malware. Phishing typically arrives in the form of an email that appears to be from a reputable institution or individual.

During the COVID-19 pandemic, cybercriminals used workers' desire for the latest COVID-19 information to lure individuals into visiting malicious websites and sharing confidential data. Experts found more than 4,000 coronavirus-related domains have been registered since January 2020.

A particularly brutal phishing attacked occurred in 2016 against the accounting department of FACC AG, an Austrian airplane component manufacturer. The fraud started with a "whaling attack," which involves a cybercriminal sending an email that appears to be from a senior executive at the targeted firm. In this case, the email appeared to come from the company's CEO, and the email asked an FACC employee to send funds related to a fake acquisition. The total cost in damages and repairs was between $55.8 and $61 million.

CORPORATE ESPIONAGE

Adversaries from nation-states, cybercriminals, and malicious insiders target sensitive data for reasons including corporate spying, personal financial gain, and political advantage.

An industrial spy can be an insider, i.e., an employee who is there specifically to spy, or a disgruntled employee who trades information for personal gain or revenge. Spies may also use social engineering and phishing techniques to trick fellow employees into sharing privileged information.

Industrial espionage and intellectual property theft are major threats to manufacturing entities, primarily by state-sponsored adversaries and malicious insiders. Trade secrets related to process and automation functions can enable hostile governments—and corporate competitors—to fast-track their manufacturing processes or sabotage political systems and national security. It may not be possible for spies to replicate processes by merely accessing material specifications; instead, adversaries will likely try to steal algorithms, engineering designs, and programming specifications to reverse-engineer and replicate proprietary processes.

One high-profile use of corporate espionage involved research chemist Gary Min who in 2017 was found guilty of misappropriating intellectual property for his employer, DuPont. Upon his dismissal from the company, DuPont discovered that he had accessed 16,706 documents and downloaded 22,000 abstracts from the company's electronic data library, none of which were relevant to his job responsibilities or expertise. Instead, it involved DuPont's primary technologies and products, many of which were in the research and development phase. The cost DuPont was the market value of the technology that was accessed: $400 million-plus.

Summary

Many factors have conspired to land FHE manufacturers in the right place at the right time for rapid integration with IIoT. Unfortunately, as FEH manufacturers are poised for success, cybercriminals are positioned for attack. Bad actors are innovating as well, engineering new technologies to penetrate the unique, complex networks and workflows within the FHE manufacturing ecosystem. They're exploiting any weaknesses they can find in the FHE supply chain, from lack of employee threat awareness to easy network access that can happen when IT budgets shrink.

With numbers like this on the rise, it's never been more critical to build a security game plan for your organization. FHE is a new enough industry with few enough players that there are no incidents thus far. But as with all nascent and emerging industries, it's not a matter of IF there will be an attack, but when.

The cost of a data breach can be high—from penalties for non-compliance with regulatory agencies to crippling loss of data. Non-compliance with industry and government regulations can result in manufacturers losing accreditation or access to key government systems. In the most severe cases, non-compliance incurs criminal and civil penalties.

But there are solutions available in the form of managed cybersecurity services—and they don't have to break the bank or slow the speed of your FEH manufacturing protocols. Cloud-based solutions like Office 365 EMS (Enterprise Mobility + Security) deliver enterprise-level security to SMEs to assess security weaknesses, protect infrastructure, and detect threats.

1. ASSESS—A comprehensive **Risk Assessment** will identify risks to compliance and identify appropriate access levels for internal and external users.

2. PROTECT—Implement solutions for **Data Loss Prevention** and **Advanced Security Management.**

3. DETECT—**Ongoing monitoring** of your environment plus **Threat Detection** stops malicious links and attachments before they arrive via emails and other tools.

CloudFirst implements Microsoft Cloud Technologies to protect applications, computing, and network infrastructure with advanced security solutions that are fully managed 24/7.

—END—

References

1. In 2019, the FHE market was valued at $95 million. https://semiengineering.com/the-good-bad-and-unknowns-of-flexible-devices/

2. The total anticipated investment in advancing FHE since NextFlex's formation has been $113M. https://www.businesswire.com/news/home/20210215005035/en/NextFlex-Launches-14-Million-Funding-Round-for-Flexible-Hybrid-Electronics-Innovations-to-Address-Manufacturing-Challenges-and-Improve-Reliability

3. The manufacturing industry ranks second among the top five most targeted industries. https://www.forbes.com/sites/theyec/2021/01/19/what-businesses-are-the-most-vulnerable-to-cyberattacks/?sh=3ddab2e33534

4. 80 percent of electronics companies are implementing IIoT technologies in plants and assembly lines without thoroughly evaluating the risks. https://www.electronics-b2b.com/important-sectors/security-systems/the-importance-of-cyber-security-in-the-electronics-industry/

5. As cybercriminals worldwide become more sophisticated, cyber threats are worse for every industry across the board. https://www.forbes.com/sites/theyec/2021/01/19/what-businesses-are-the-most-vulnerable-to-cyberattacks/?sh=3ddab2e33534

6. In a 2019 survey of manufacturing companies, half of all respondents reported they had suffered a breach or cyberattack in the 12 months prior. https://www.thomasnet.com/insights/50-of-manufacturers-saw-data-breaches-in-past-year-survey/

7. Sixty percent of SMEs that experience a data breach or cyberattack shutter their businesses within six months due to bankruptcy or inability to recover. https://www.cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html

8. A recent report shows that more than 80 percent of electronics companies implement IIoT technologies in plants and assembly lines without thoroughly evaluating the risks or instituting standard security protocols. https://www.ibm.com/thought-leadership/institute-business-value/report/electronicsiiot

9. ITAR non-compliant companies can face fines up to $500,000 per occurrence. https://securityboulevard.com/2021/05/six-things-you-have-to-know-about-itar-compliance/

10. Ransomware increased by 40 percent to 199.7 million cases globally in the third quarter of 2020. https://www.business-standard.com/article/technology/ransomware-attacks-surge-40-to-199-7-million-globally-in-q3-report-120110200919_1.html

11. The average impact to each business impacted in the SolarWinds' Orion IT attack was 11 percent of their respective annual revenue, an average of $12 million per company. https://www.automationworld.com/Take5/video/21366548/take-five-with-awcyber-threats-expand-postcovid19