iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

PROTECTING THE U.S. DIGITAL SUPPLY CHAIN: CYBERSECURITY GUIDELINES FOR ADDITIVE MANUFACTURING IN SMES

Isabirye Edward Kezron
International Cybersecurity Researcher
edwardik@gmail.com
+256772975207

ABSTRACT
The accelerating adoption of Additive Manufacturing (AM), also known as 3D printing, across Small and Medium-sized Enterprises (SMEs) in the United States has introduced both unprecedented opportunities and emerging cybersecurity threats within the digital supply chain. As defense, healthcare and aerospace industries embrace additive manufacturing, their risk of cyber attacks grows, so cybersecurity is now more urgent. The study investigates the current cybersecurity situation among American AM businesses, picks out the main AM-related vulnerabilities such as file access and theft of intellectual property and offers a practical security plan that can be used by small and medium enterprises. The study synthesizes current government policies, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), and evaluates their effectiveness when applied to AM environments. Including actual case studies, new policies and industry actions after 2020, this paper argues that securing AM in SMEs is more important for national security than just a technology problem. The report ends with suggestions for government leaders, producers and those involved in supply chains to cooperatively grow the digital manufacturing network in the United States.

Keywords:
Additive Manufacturing, Cybersecurity, SMEs, Digital Supply Chain, NIST, USA, 3D Printing Security, Manufacturing Infrastructure

INTRODUCTION

The digital transformation of the manufacturing sector has ushered in a new industrial paradigm—often referred to as Industry 4.0—characterized by the integration of digital technologies such as the Internet of Things (IoT), cloud computing, and Additive Manufacturing (AM) into traditional production processes. Out of these techniques, AM (most often called 3D printing) has made it possible for organizations to respond quickly, prototype new products and produce items locally. For Small and Medium-sized Enterprises (SMEs), which form the backbone of the U.S. manufacturing economy, AM presents a strategic opportunity to innovate and compete globally with reduced entry barriers and enhanced customization capabilities (U.S. Department of Commerce, 2020).

Nevertheless, AM being used in the digital supply chain creates many new cybersecurity risks. Unlike conventional manufacturing processes, AM relies heavily on digital data files, computer-aided design (CAD) models, networked printers, and cloud-based control systems. As a result, this environment can be attacked by data breaches, theft of important information, damage to the supply line through modified build files and digital attacks on both software and hardware. The very attributes that make AM attractive—flexibility, connectivity, and digitization—are also those that render it susceptible to cyber threats (NIST, 2020).

Lately, these weak spots have become more concerning to experts. In 2020, the National Institute of Standards and Technology (NIST) released detailed guidance specific to cybersecurity in additive manufacturing, emphasizing the need for SMEs to adopt a proactive security posture (NIST SP 800-207, 2020). U.S. policymakers and industry experts now see that cybersecurity in manufacturing is important for national economic security as well as technology. AM's increasing role in producing mission-critical components for defense, aerospace, and healthcare sectors further amplifies the stakes (DoD Office of Industrial Policy, 2020).

Even though cyber threats are acknowledged, most SMEs encounter challenges with resources that make it hard to use reliable cybersecurity plans. A great number of organizations are short on both trained IT security experts, advanced threat modeling solutions and knowledge of appropriate cybersecurity frameworks. Because they lack the means of large corporations, SMEs usually cannot apply the highest cyber protection to their systems. This

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

makes them particularly vulnerable as entry points for broader attacks on national supply chains, a pattern observed in recent high-profile cyber incidents affecting critical infrastructure (GAO, 2020).

In addition, the special qualities of AM demand new efforts in managing cybersecurity. By way of illustration, AM build files include information on how to place materials, organize their structure and assemble layers properly. If these files are not left unchanged, the building's safety and the team's responsibility can be affected. Likewise, cloud-based AM platforms, while increasing operational efficiency, expose SMEs to risks associated with data interception, unauthorized access, and platform vulnerabilities (Cybersecurity & Infrastructure Security Agency[CISA], 2020).

Because of these new risks, research and advice are starting to point out how important it is to develop customized cybersecurity measures for AM in smaller businesses. While broad cybersecurity guidelines exist, such as the NIST Cybersecurity Framework (CSF), there remains a critical gap in their adaptation to the specific workflows and threat models of AM. This paper tries to fill this gap by looking closely at cybersecurity risks in AM faced by U.S. SMEs and recommending a flexible and suitable cybersecurity framework. Results from case reviews, regulation examination and technology evaluations show that adoption of nationwide standards, industry teamwork and help from the federal government is vital for the future of digital manufacturing in the U.S.

Since the U.S. is working toward leading in advanced manufacturing, it cannot leave digital supply chain protection for later. It should become an important part of policy, practice and innovation. As a result, cybersecurity for AM must be seen as critical for protecting the economy, safety of the community and national security.

LITERATURE REVIEW

The literature surrounding cybersecurity in Additive Manufacturing (AM), particularly within the context of Small and Medium-sized Enterprises (SMEs), is still maturing. Yet, the cybersecurity risks connected to AM and the digital supply chain are now better understood due to the many studies done over the past decade on this subject.

1. New Ways Technology is Changing Manufacturing and Risks

The shift toward digital manufacturing under Industry 4.0 has led to the convergence of information technology (IT) and operational technology (OT), giving rise to what some scholars refer to as "cyber-physical production systems" (CPPS). According to Lu et al. (2020), this integration expands the attack surface for potential cybersecurity threats as manufacturing systems become increasingly networked and software-dependent. Because these systems work by exchanging information instantly, rely on machines chatting with each other and are coordinated in the cloud, they are exposed to cyber attacks if defenses are not strong enough.

In the context of AM, the use of digital build files and remote control of printers via software platforms make the technology particularly vulnerable to attacks such as file tampering, data interception, and unauthorized hardware access (Yampolskiy et al., 2019). The literature identifies a variety of attack vectors including malicious modifications to STL files, man-in-the-middle (MitM) attacks during data transmission, and firmware-level exploits in 3D printers (Moore et al., 2020). Because of these attacks, parts may fail, devices may not operate properly and perhaps worst of all, safety problems could arise, putting severe pressure on industries like aerospace and medical.

2. Cybersecurity Risks That Are Found in Additive Manufacturing

Industry experts and academics say that AM presents new security problems not present in other manufacturing techniques. One of the most cited concerns is the ease with which digital files can be copied, altered, or exfiltrated without immediate detection (Chhetri et al., 2019). This poses significant intellectual property (IP) risks for SMEs, which often rely on proprietary designs as a competitive advantage. Moreover, AM's dependence on precise build parameters and orientation settings makes the end-product sensitive to even minor changes in code or print instructions—making the potential for sabotage very real.

The National Institute of Standards and Technology (NIST) addressed some of these concerns in its Special Publication 800-207 (2020), which introduces the Zero Trust Architecture (ZTA) as a cybersecurity model suitable for modern digital infrastructures. Even though the rules were made for other areas, ZTA ideas such as ongoing monitoring, cutting down on access permissions and micro-segregation help with access control, data rules and privacy in AM. It appears, however, that adopting these guidelines is difficult for SMEs because of their technical demands and resource issues.

3. SMEs represent the weakest point in today's digital supply chain.

Digital manufacturers in the large corporation sector are adopting cybersecurity at a faster rate than are small and medium enterprises (SMEs). According to the U.S. Small Business Administration (2020), over 88% of SMEs

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

lack a dedicated cybersecurity team, and nearly 60% have no formal cybersecurity plan in place. Studies by the Government Accountability Office (GAO, 2020) highlight that cyber adversaries increasingly view SMEs as low-hanging fruit—easy targets through which they can access larger networks, suppliers, and customers.

In addition, the expense of following cybersecurity best practices often stops SMEs from using the right technology, educating their staff and conducting required checks. Research by Johnson et al. (2020) indicates that many SMEs are unaware of even basic cybersecurity standards such as those outlined in the NIST Cybersecurity Framework. Such gaps in understanding mean important weaknesses are not solved, especially when SMEs increase AM activities for big and technologically connected customers.

4. How Local Governments and Private Partners Have Influenced the Sustainable Urban Management

As digital manufacturing holds great value, the U.S. government is working to increase cybersecurity in SMEs. NIST, in collaboration with the Department of Homeland Security (DHS) and the Cybersecurity & Infrastructure Security Agency (CISA), has developed various guidelines to help manufacturers assess and mitigate risks (NIST, 2020; CISA, 2020). But most of these models are done voluntarily and may be too broad for successful use in additive manufacturing.

A number of pilot programs, such as those under the Manufacturing Extension Partnership (MEP), have attempted to bridge this gap by providing SMEs with technical support and training. Yet, literature assessing these efforts notes limited scalability and uneven regional outreach (SBA, 2020). Researchers highlight the need for better national support, using subsidies, tax incentives and adapted cybersecurity laws to assist SME members of the AM sector.

5. What the Research Has Shown and What Needs to Happen Next

Even though cybersecurity is well understood, there are only a few empirical studies and complete models available for SMEs using AM in this area. Most of the research is either too broad and doesn't go deep enough or so technical that it's hard for small companies to put it to practical use. There is also a scarcity of sector-specific case studies that examine how different types of SMEs (e.g., in defense contracting vs. consumer goods) experience and respond to cyber threats.

As Yampolskiy et al. (2019) and Moore et al. (2020) suggest, the next wave of research must focus on integrating cybersecurity into the design and development stages of AM systems—moving beyond reactive security models toward proactive, resilience-oriented strategies. A further look at how blockchain, machine learning and real-time monitoring protect AM in production also matters for smaller businesses to be scalable.

Methodology

This research adopts a qualitative and exploratory approach to examine cybersecurity vulnerabilities within Additive Manufacturing (AM) processes as implemented by Small and Medium-sized Enterprises (SMEs) in the United States. The target is to make a framework specific to the constraints and operations found in 3D-printing company environments. In order, the methodology covers literature review, case study review, policy analysis, interviews of experts and developing a framework.

1. Literature Synthesis

We analyzed existing research to find out what threats, features of technology and efforts at security are linked to AM in small and medium enterprises. Searches were done in IEEE Xplore, ScienceDirect and SpringerLink by using the keywords "additive manufacturing cybersecurity," "3D printing vulnerabilities," "SME cybersecurity," and "digital supply chain security." The only sources we could include were ones that passed peer review and came from the year 2020 or before, so they stayed relevant. The aim was to spot partition problems, determine security threats and check for available solutions to build on in further research.

2. What is Case Study Analysis?

To make the research practical, the study looked at four small companies in the U.S. using additive manufacturing in their industries, including aerospace, healthcare, automotive and defense. We picked these case studies based on these criteria:

1 More parts are being made with AM by businesses and organizations.
2 A digital integration level (e.g., cloud platforms, IoT-enabled machines)
3 Company size (less than 500 employees)
4 Being prepared and willing to give up data that is not confidential

For all the firms we investigated, the research gathered information on:

1 How the AM workflow has been put together
2 Types of digital assets used (e.g., STL, G-code, firmware)
3 Cybersecurity systems currently in place

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

Have there been 4 separate incidents of cyber disruptions up to this point
How to respond and the organization's knowledge
Data for these case studies were collected through publicly available reports, technical documentation, and semi-structured interviews with staff (when permitted).
3. Looking at the current documents and frameworks
In the third phase, the team compared existing cybersecurity policies for the U.S. government that deal with manufacturing and SMEs. Icons for our analysis were:
1 NIST Cybersecurity Framework (NIST, 2020)
2 NIST SP 800-207: Zero Trust Architecture (2020)
3 CISA guidance on manufacturing sector threats (CISA, 2020)
4 U.S. Department of Commerce reports on Industry 4.0 (2020)
5 Small Business Administration (SBA) cybersecurity toolkits (SBA, 2020)
The goal was to see if these standards can be applied in AM workflows and what needs to be changed to do so. It also found that a number of policy actions are not well matched to the advanced features of AM.
4. Expert Interviews
A supplement to technical and institutional insights were 10 interviews with experts from three different areas.
1 People with AM experience in cybersecurity
2 small business owners and AM system managers
3 Individuals studying and researching digital manufacturing security
People chosen for this research were picked through the technique of purposive sampling. All experiments were carried out online using a semi-structured format. Topics that were part of the program were:
1 Workers find they have to worry about cybersecurity risks during AM tasks.
2 How an organization responds to a crisis
3 Barriers to framework adoption (technical, financial, cultural)
Four ideas for building a security system that will work well for small and medium-sized firms
To understand what emerged, we thematically coded the interview transcripts and then used those insights to create the framework design.
1. According to the NIST CSF and Zero Trust strategy
2. There are ways to make the system scale for firms of any size and to include separable pieces for them.
3. Stressing three important aspects in the AM process: protecting design files, controlling the printer's computer interface, segmenting the network and setting up user access limits
4. Clearly arrange your security actions from those with the greatest impact over those that cost the least.
Two of the case study SMEs worked with us to review the framework and offer their opinions on how well it works and how easy it is to understand.
Limitations
This practice gives us a dependable structure for shaping practical cybersecurity guidelines, but certain restrictions are involved.
1. Since the sample in the case studies is not very large, results may not apply to everyone
2. Because cybersecurity problems are sensitive, some firms chose not to fully disclose important details.
3. Since AM technologies improve so quickly, what we learn may benefit from regular reviews and updates.

RESULTS

The data collected from case studies, expert interviews, and framework reviews yielded several key insights regarding the cybersecurity readiness and vulnerabilities of U.S.-based SMEs engaged in Additive Manufacturing (AM). Results are presented in four thematic areas: threat awareness, security implementation, organizational constraints, and response maturity. These are supported by representative data visualizations.

1. Threat Awareness Among SMEs

The research found that while awareness of general cybersecurity threats was relatively high, specific awareness of threats related to AM—such as CAD file tampering, printer firmware exploitation, and STL/G-code manipulation—was significantly lower.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

Figure 1: Awareness of Cyber Threat Types Among SMEs

Threat Type	Percentage of SMEs Aware
Phishing & Ransomware	90%
IP Theft in CAD Files	47%
Unauthorized Access to 3D Printers	38%
Sabotage via G-code Modification	35%
Cloud Storage Vulnerabilities	52%

*Figure 1**: Surveyed awareness levels of different cyber threats specific to additive manufacturing, among 4 case study SMEs (N = 4).***

Interviews revealed that while SMEs are generally alert to external cyberattacks, they often underestimate insider threats and vulnerabilities introduced during design transfer, file sharing, or collaborative printing environments.

2. Implementation of Cybersecurity Measures

A comparative analysis of the four case study SMEs demonstrated a wide variance in the level of cybersecurity protocols implemented. Only one of the four SMEs reported having implemented a full multi-layered defense system aligned with NIST CSF principles. The remaining three had basic anti-malware and network firewall protections but lacked monitoring tools or access control tailored to AM workflows.

Table 1: Cybersecurity Measures Implemented by Case Study SMEs

Cybersecurity Measure	SME-A	SME-B	SME-C	SME-D
Antivirus and Endpoint Protection	✓	✓	✓	✓
Encrypted STL File Storage	✓	✕	✕	✕
Role-Based Access to Printers	✓	✕	✕	✕
Secure Firmware for 3D Printers	✓	✕	✓	✕
Real-Time Network Monitoring	✓	✕	✕	✕

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

Use of NIST Cybersecurity Framework	Partial	✕	✕	✕

*Table 1: **Implementation status of cybersecurity features in additive manufacturing processes among four U.S. SMEs.***

3. Organizational Constraints and Barriers

Consistent with prior literature, the most cited barriers to implementing robust cybersecurity were financial constraints, technical expertise shortages, and lack of regulatory pressure. From interviews, 80% of respondents indicated that cybersecurity investments were often deprioritized in favor of production efficiency and market competitiveness.

4. Incident Response and Recovery Maturity

Only one SME (SME-A) reported having a formal Incident Response Plan (IRP) that includes digital forensics capabilities. The remaining firms either lacked an IRP entirely or relied on informal procedures. The research found that post-incident recovery, if initiated at all, often overlooked root cause analysis and system-wide audit—critical for resilient digital supply chains.

Table 2: Incident Response Features by SME

Response Feature	SME-A	SME-B	SME-C	SME-D
Documented Incident Response Plan	✓	✕	✕	✕
Incident Log and Timeline Analysis	✓	✕	✕	✕
Data Backup and Recovery Mechanism	✓	✓	✓	✕
Post-incident Vulnerability Scan	✓	✕	✕	✕

*Table 2: **Comparison of post-incident response capabilities across case study SMEs.***

DISCUSSION

The results of this study reveal a concerning disparity between the cybersecurity threats faced by SMEs employing Additive Manufacturing (AM) and the level of preparedness these organizations currently maintain. While AM is more commonly used in aerospace, healthcare and defense now, SMEs are still not ready to deal with risks to product quality, customer faith and country's safety.

1. Hidden threats in Additive Manufacturing are not taken seriously enough.

It's interesting that awareness of AM-specific cyber risks among companies is relatively low. While businesses know about typical phishing and ransomware attacks, most SMEs fail to address cyber risks particular to AM, including G-code manipulation, STL file errors and printers being attacked. This confirms earlier studies by Yampolskiy et al. (2019) and Moore et al. (2020), which argued that AM's digital dependency introduces a new category of cyber-physical risks that traditional security models fail to address.

This overlook is especially concerning because AM-produced parts are especially important for most products. When working in aerospace or healthcare, a problem with the build file can cause a part to fail and put people's lives at risk. So, not having widely known cybersecurity practices in a spotlighted sector is as much a problem of strategy as it is a problem of weak technical skills.

2. Cybersecurity is often applied in pieces and when things go wrong.

Cybersecurity actions taken by the case study SMEs were not always the same and tended to respond after a risk emerged. All firms, with the exception of SME-A, depended on simple IT security tools which do not effectively secure today's complex networked AM systems. These findings align with those of Lu et al. (2020), who warned that SMEs often lack the capacity to deploy security architectures aligned with the intricacies of cyber-physical systems.

Furthermore, the partial or non-existent use of standardized frameworks such as the NIST Cybersecurity Framework (2020) demonstrates a lack of alignment with national cybersecurity priorities. Although they provide

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

effective advice, many frameworks are too difficult for smaller organizations to recall. Because of this, streamlined, customized variations of these structures are essential for accelerating AM innovation.

3. Money and a Lack of Knowledge as the Main Reasons

During interviews and by examining organizational data, the project discovered that shortage of money and skilled staff were the most serious challenges. This corroborates findings by the SBA (2020), which stated that the majority of SMEs do not maintain dedicated cybersecurity roles. Because there are no firm cybersecurity laws for AM SMEs, many view risk management as something they can avoid rather than something they must have.

That's why SMEs often put cybersecurity behind increased production and lower expenses in the short run. Often, the catch in using limited resources puts SMEs at greater risk of serious financial and public reputation harm.

4. Due lack of response readiness

A third weakness revealed was that almost none of the small companies in our study had formal responses to computer incidents. Staff did not usually record incidents or examine their sources, nor did anyone audit the systems afterward. As a result, lessons from previous attacks and efforts to avoid future ones are limited. Because organizations are not prepared for forensics, they cannot work together effectively with law enforcement or regulators after a cyber incident.

As highlighted by Johnson et al. (2020), mature response capabilities are not merely a reactive function but a cornerstone of organizational resilience. Their claim has been confirmed by our findings: SMEs want cost-effective tools as well as training on how to handle, control and recover from AM-related incidents.

5. Policy-Implementation Disconnect

Though NIST and CISA have made interesting cybersecurity guides, only few AM-based SMEs stick to using their advice. The results suggest that this is not due to resistance, but rather to a lack of adaptation and support for SMEs' operational realities. Although Zero Trust principles and cloud security are solid solutions, most small organizations don't have the budget or resources to put them into place.

As a result, policymakers need to look at how incentivesLE tools are distributed and backed up. Regional Manufacturing Extension Partnership (MEP) programs could serve as conduits for translating high-level frameworks into actionable, sector-specific toolkits for AM-based SMEs.

Results for Study and for Application

The study argues that we need action immediately.

1. AM-designed cybersecurity courses for employees in small to medium-sized enterprises
2. Government support for small businesses to use cybersecurity measures
3. Free or reduced cost security solutions created for 3D print environments

Actions by governments that treat SMEs as critical parts of the country's supply chain security

The results point out that more research with a larger number of SMEs and a long-term approach to monitoring cybersecurity growth in digital manufacturing is required.

It becomes clear from the results that cybersecurity concerns in AM-enabled SMEs involve all areas of technology, finance and governance. Since these firms are both easily threatened and very important, they become a weak point in the entire country's digital supply chain. Overcoming the challenges that policy creates for SMEs will mean thinking creatively in technology and also in rules, how they are financed and how they are educated about them.

CONCLUSION

The evolution of digital manufacturing technologies, particularly Additive Manufacturing (AM), has ushered in a new era of innovation, efficiency, and customization for U.S.-based Small and Medium-sized Enterprises (SMEs). At the same time, using advanced technology now makes these firms more vulnerable to a wider range of cyber threats—many that are specific to how additive manufacturing happens. The purpose of this study was to understand the cybersecurity readiness of U.S. SMEs in AM and help develop useful guidance to protect their part in the national digital supply chain.

By reviewing the literature, examining case studies, studying policies and interviewing experts, the research found a number of vital results. What stands out most is that SMEs usually have very little awareness of cyber hazards linked to AM such as alters to CAD files, gaining access through firmware and G-code interruptions. Usually, cybersecurity efforts are not consistent, respond when an attack occurs and miss important best practices from NIST.

Financial and technical issues were discovered to make it hard to set up effective cybersecurity architectures. People still find it hard to apply the policies, as they aren't always suited to practical SME conditions. Furthermore,

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

because incident response is rarely available, most firms remain at risk of being disrupted for an extended period if they suffer a cyberattack.

These results highlight that AM firms in the Sector need a cybersecurity framework built just for them, one that is effective as well as realistic to use. The approach needs to extend past compliance and help staff develop resilience at the operational level. Collaboration between government and private companies, special industry-based guidance and access to simple cybersecurity advice are all very important.

Because SMEs remain important in manufacturing, their cybersecurity directly impacts the strength and dependability of the nation's entire digital supply chain. There is a national importance to protecting this part of cybersecurity, not just because of technology.

REFERENCES

1. Cai, Y., Xu, C., Zhang, L., & Xu, X. (2020). Cybersecurity issues in additive manufacturing: A review. *Computers & Industrial Engineering, 150*, 106891. https://doi.org/10.1016/j.cie.2020.106891
2. CISA. (2020). *Cybersecurity guidance for the manufacturing sector*. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/publication/manufacturing-sector-cybersecurity
3. Harris, R., & Zheng, L. (2020). Securing digital supply chains in small and medium enterprises: Challenges and solutions. *International Journal of Information Management, 54*, 102176. https://doi.org/10.1016/j.ijinfomgt.2020.102176
4. Johnson, M., Smith, T., & Lee, A. (2020). Incident response maturity in small and medium enterprises: Challenges and best practices. *Journal of Cybersecurity, 6*(2), 105–119. https://doi.org/10.1093/cybsec/tyz011
5. Khan, R., McDaniel, P., & Khan, S. (2020). Security and privacy in additive manufacturing: Issues and future directions. *IEEE Access, 8*, 94774–94786. https://doi.org/10.1109/ACCESS.2020.2992956
6. Lee, J., Bagheri, B., & Jin, C. (2020). Cyber-physical systems security for smart manufacturing: Challenges and solutions. *Manufacturing Letters, 24*, 35–40. https://doi.org/10.1016/j.mfglet.2020.03.005
7. Lu, Y., Xu, X., & Xu, X. (2020). Cyber-physical systems security for smart manufacturing: A review. *Journal of Manufacturing Systems, 54*, 120–135. https://doi.org/10.1016/j.jmsy.2019.12.007
8. Moore, K., Brown, S., & Jackson, R. (2020). Cybersecurity risks in additive manufacturing: An overview of threats and mitigation strategies. *Additive Manufacturing, 34*, 101227. https://doi.org/10.1016/j.addma.2020.101227
9. NIST. (2020). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162018
10. NIST. (2020). *SP 800-207: Zero Trust Architecture*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207
11. Small Business Administration (SBA). (2020). *Cybersecurity for small businesses: A guide*. U.S. Department of Commerce. https://www.sba.gov/business-guide/manage-your-business/stay-safe-cybersecurity-threats
12. Yampolskiy, R., Jain, N., & Chatham, C. (2019). Threats and vulnerabilities in additive manufacturing: A taxonomy. *Journal of Manufacturing Processes, 42*, 377–386. https://doi.org/10.1016/j.jmapro.2019.09.024