Research Article

Adapting Cybersecurity Maturity Models for Online Startups and Small Businesses

Adhitya Sundar

Flower Mound High School, Flower Mound, Texas, 75028, USA

ABSTRACT

This research examines the understanding and application of cybersecurity practices by internet companies. Due to a lack of understanding and limited resources, online startups and small businesses are more susceptible to cyber threats, including ransomware, malware, phishing, and non-social engineering attacks, such as system vulnerabilities. This study analyzes current models of cybersecurity maturity and modifies them to fit the specific requirements and limitations of online startups and small businesses. As part of the process, a comparison of current models and suggestions for a customized model suitable for new digital enterprises is presented.

Keywords: Cybersecurity; Maturity Models; NIST CSF; Online startups; Small Business

INTRODUCTION

In this modern world, Online startups and small businesses are rapidly establishing themselves, often with limited resources, few employees, and a strong focus on stability, growth, and innovation. While this speed enables them to respond to business needs quickly, it also exposes them to various cybersecurity threats, such as ransomware attacks, phishing, and software vulnerabilities. Since these businesses often operate with a low budget and do not have a dedicated team of IT experts, they are an easy target for both social and non-social cyberattacks. Larger organizations and industries often adopt structured cybersecurity models, such as the NIST cybersecurity Framework (CSF), Capability Maturity Model Integration (CMMI), or ISO/IEC 27001, to manage their cybersecurity practices. However, these models are designed to support larger organizations with extensive resources and technical capabilities, as well as complex infrastructure. For online startups and small businesses, these frameworks are often too complex, with extensive documentation, costly tools, and rigid processes that cannot be easily scaled down. As a result, small businesses struggle to adopt formal cybersecurity policies.

According to a recent study, there is a notable difference in structured security practices between the enterprise and startup sectors, with over 80% of Fortune 500 companies reporting alignment with cybersecurity frameworks like NIST CSF or ISO/IEC 27001, while less than 20% of small businesses report any formal adoption of cybersecurity frameworks (10).

This study examines the challenges associated with existing cybersecurity models and investigates how they can be adapted to meet the specific needs of online startups and small businesses in terms of cost, simplicity, and adaptability. By analyzing the core structure of these models, this research aims to propose a simplified model

Corresponding author: Adhitya Sundar, E-mail: adhityasundar@gmail.com.

Received July 19, 2025**; Accepted** August 4, 2025
https://doi.org/10.70251/HYJR2348.34217224

that addresses the cybersecurity challenges faced by small emerging organizations (9).

LITERATURE REVIEW

Recent studies and industry literature present the current cybersecurity models used by prominent corporations and enterprises. Frameworks such as the Capability Maturity Model Integration (CMMI) and the National Institute of Standards and Technology (NIST) Cybersecurity Framework enable larger established organizations to assess and improve their cybersecurity operations through these structured frameworks and standard operating procedures. Because these models are designed to handle complex systems and extensive infrastructure, they are useful tools for businesses with existing infrastructure (6).

However, it is evident that there aren't many cybersecurity approaches tailored to the requirements of online startups and small businesses. The contexts in which startups and established organizations operate are significantly different. They frequently experience extreme pressure to expand rapidly, which may lead them to take shortcuts in areas such as security. Many of them have little to no dedicated IT staff, small teams, and tight budgets. Additionally, establishing cybersecurity may become even more challenging due to the technical debt that results from moving too quickly without adequate preparation.

While highlighting these difficulties, several recent studies have refrained from providing workable solutions for online startups and small businesses. These organizations often lack the structure, staffing, and long-term stability that most maturity models assume (1). This leaves a significant research gap, emphasizing the need for cybersecurity frameworks that are easy to use, adaptable, and affordable for smaller, online-first companies. This review of the literature lays the foundation for creating a more useful model that better suits the startup environment.

METHODS AND MATERIALS

This research utilizes a qualitative approach, reviewing established cybersecurity maturity models and conducting a theoretical analysis of how each can be applied or modified for startups. Key criteria include model function, approach, and maturity structure to identify their suitability and limitations across industries. Sources include white papers, academic journals, and cybersecurity readiness tools.

The typical cybersecurity maturity levels range from Level 1 to Level 5, as outlined in Table 1. In general, a cybersecurity maturity model helps organizations to assess risk, improve, and measure their cybersecurity capabilities using a structured framework. In other words, it demonstrates how effectively an organization is protected against cyberattacks. Some of the most widely used cybersecurity maturity models across various industries are National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), Cybersecurity Capability Maturity Model (C2M2), Capability Maturity Model Integration (CMMI) – Security Adaptation, Cybersecurity Maturity Model Certification (CMMC), International Organization for Standardization / International Electrotechnical Commission 27001 (ISO/IEC 27001) Maturity Approach and COBIT (Control Objectives for Information and Related Technologies). Table 2 provides a high-level overview of limitations and risks associated with each maturity model of cybersecurity.

Risk Evaluation

The risk evaluation of each security model is depicted in Figure 1, which assumes a risk level ranging from 1 to 3. Low risk is denoted by a 1, medium risk by a 2, and high risk by a 3. These risk level rankings were produced using an author-developed technique that considered factors such as implementation costs, technical knowledge required, audit difficulty, and scalability for small businesses. The scores were impacted by real-world constraints faced by businesses with limited resources as well as trends observed in cybersecurity research, even though they were not produced by a formal

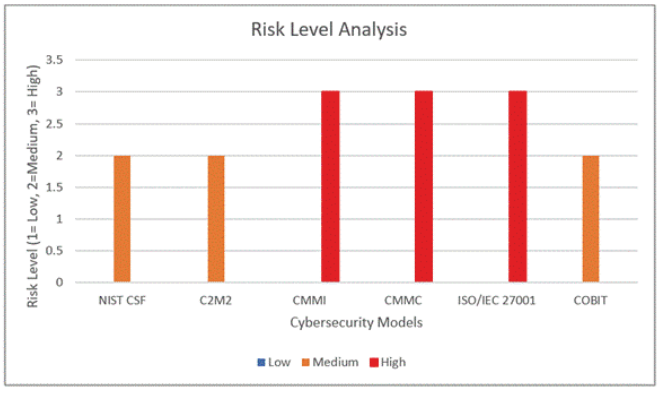

Figure 1. The risk evaluation of each security model.

Table 1. The typical Cybersecurity maturity levels range from Level 1 to Level 5

Level	Name and Description	Why it matters	Graduation criteria from one level to another
0	"Non-existent" where there are no policies or processes in place	It is a high risk as the business is completely vulnerable with no recovery process.	Lack of cybersecurity knowledge; to move to the next level, start understanding basic threats and establishing asset awareness.
1	"Initial Level," where documented policies and actions are inconsistent	In Level 1, there is some awareness, but there is no reliability.	Determine important assets, assign informal responsibilities, and start using basic controls to advance to level 2.
2	"Managed Level" where security control exists but is inconsistent	Even with the implementation of basic controls like firewalls and antivirus software, the risk still exists if protection is inconsistent.	A certain amount of staff awareness training and the uniform implementation of fundamental policies across departments are necessary to reach level 3.
3	"Defined" where security processes are standardized	This approach ensures everyone follows the process through a solid baseline	Role clarity, structured onboarding, and clear documentation are necessary for graduation from this level.
4	"Measured" where security is tracked with metrics and effectiveness is assessed.	This level allows the business to track the progress on what is working and not to make informed decisions.	Implementing a feedback loop (such as logging and reporting) and measurable security KPIs are priorities to move to the next level of graduation.
5	"Optimized" where security is continuously improved	Businesses stay proactive for any cyberthreats	Maintain continuous improvement, constant development via automation, threat intelligence, and frequent updates. maintained by a security culture that is proactive and flexible.

Table 2. Limitations and risks associated with each maturity model of cybersecurity

Model	Implementation approach used	Maturity Structure	Limitation	Risk
NIST CSF	This model is a functional based approach that focuses on (Identify, Protect, Detect, Respond, Recover).	No formal levels	Lacks implementation guidance; Organizations must define their own	Incomplete or inconsistent security coverage
C2M2	This model is a domain-based approach and independently scored	Level 1-3	Qualitative scoring is subjective and broad. Relies on assessor judgement than precise metrics	Critical risks may be under or over estimated
CMMI	This model is a process-based approach and improves process through measurement	Level 1-5	Requires significant resources and formal process discipline	Organizations may skip implementation, leaving gaps in controls
CMMC	This model is a tiered requirement that focuses on meeting the lower-level requirements first	Level 1-5 in CMMC 1.0	Complex compliance requirements and frequent revisions	Organizations may fail audits or face loss due to outdated controls
ISO/IEC 27001	This model is a control-based approach implements a set of security controls	No formal levels	Pass/fail certification hides variations in maturity – does not reflect how mature an organization maturity process	Certified entities may neglect ongoing improvement leading to exposures
COBIT	This model is a Governance focused approach which aligns business goals with security	Level 0 (non-existent) to Level 5	Emphasizes IT governance over operational security controls	Strategic alignment may exist without real-world threat defense

statistical model or expert panel. The models offer clear implementation paths that are generally applicable with a low risk level, suitable for all industrial sizes, according to risk level 1. Models classified as "risk level 1 (low risk)" offer clear implementation pathways, require minimal training, and are readily adaptable to all business sizes with minimal financial or technological strain. Although none of the models examined in this study satisfy this low-risk criterion, for microbusinesses and sole owners, NIST's Small Business Cybersecurity Corner offers clear, practical advice. Although it is not a comprehensive maturity model, its inclusion highlights what low-risk cybersecurity support can look like in practice [9]. However, these materials have not been included in the core model evaluation of this study, as they are not officially structured like full-scale maturity models. Risk category 2 (medium risk) denotes flexible frameworks that are not overly complicated but that need support tools for implementation or modest training for accurate interpretation. If this model is misinterpreted, there is a medium chance that issues could arise. Level of risk 3 High risk denotes that the models are costly, intricate, and need specialized personnel and capital. Serious security flaws could result from the improper implementation of this approach. According to the graph, models such as ISO/IEC 27001, CMMC, and CMMI are considered high-risk since they require formal audits, are expensive, and have complicated structures. However, due to their flexibility and scalability, models like C2M2, COBIT, and NIST CSF are classified as having a medium risk. For any implementation, however, they still require a systematic method.

Analysis

These cybersecurity maturity models were readily utilized by larger organizations, government agencies, and the private sector. Usually, these models are supported by a large team of IT departments, specialized cybersecurity teams, and substantial funding. On the other side, online startups and small businesses face many obstacles. The majority have limited resources; therefore, they are unable to afford full-time cybersecurity employees, expensive consultants, or advanced security solutions. For example, implementing a formal framework like ISO/IEC 27001 can cost anywhere from $20,000 to $50,000 or more, just for certification and auditing. Similarly, depending on the size and complexity of the company, CMMC Level 2 compliance has been projected to cost anywhere from $100,000 to $250,000 (1, 4). In reality, when companies focus on expansion, product development, or client acquisition, cybersecurity is often viewed as a "nice to have" rather than a top priority. Many small organizations struggle to fully apply typical frameworks designed for enterprise-scale operations due to their limited financial flexibility. Online startups and small businesses are defined in this study as companies with fewer than 50 workers. It is assumed that many of these companies lack an IT department and rely on general staff to perform various tasks for their daily operations. Mid-sized businesses can deploy enterprise-level frameworks when they have more than 100 employees and a consistent IT budget (10).

Apart from financial limitations, there is also a knowledge gap. The majority of startup founders and small business owners lack cybersecurity expertise. They may feel overpowered or unsure of where to start when confronted with intricate frameworks that are complex and filled with technical language. These companies risk implementing the framework poorly or abandoning it entirely if they don't have a clear plan tailored to their specific size. Hiring a full-time expert to bridge this knowledge gap, such as a Chief Information Security Officer (CISO), can cost anywhere from $150,000 to over $250,000 annually in the US. Even mid-level security hires, such as security analysts or IT compliance heads, often command yearly salaries of $90,000 to $120,000, which the majority of startups cannot afford (5).

Two other important issues are staffing and time. Employees at many companies work in small teams and often assume multiple responsibilities. A thorough cybersecurity program may simply not have enough time or human resources to be thoroughly researched, planned, and implemented. It can be challenging to prioritize security above regular business operations, even if they understand its importance. These models' intricacy simply exacerbates the issue. Their breadth and structure can be demoralizing for smaller companies, even as they are comprehensive and efficient for larger ones. Consequently, implementation often turns out to be incomplete, inconsistent, or out of sync with the real threats that the company faces.

In the end, challenges including a lack of funds, time, experience, and intricate designs burden online startups and small businesses, making them more vulnerable to cyber threats. They may not have the necessary defenses against ransomware, phishing scams, data breaches, and other emerging online threats if they lack adequate funds and mentorship. These restrictions make it difficult for them to implement even the most fundamental security measures, which leads to uneven protections, haphazard

choices, and an over-reliance on luck rather than planning. Without affordable, user-friendly frameworks that are appropriate for their size, many businesses remain susceptible to ransomware attacks, phishing scams, data breaches, and operational disruptions that could negatively impact their growth or survival.

Framework for Small Organizations

Online startups and small firms face several cybersecurity challenges when attempting to deploy advanced cybersecurity frameworks designed for larger enterprises, due to various factors, including a lack of dedicated and skilled staff, financial constraints, and other obstacles. This section presents an easy-to-use, adaptable NIST Cybersecurity Framework (CSF) tailored to meet the needs of smaller enterprises. This simplified version, in contrast to the full enterprise implementation, concentrates only on critical controls that can be implemented without a dedicated IT staff or enterprise infrastructure, such as multi-factor authentication, robust password enforcement, basic software patching, and explicit incident response procedures. By providing step-by-step instructions utilizing easily accessible tools, the goal is to make cybersecurity more affordable and actionable.

In this simplified framework, the five main security functions that form the foundation of the NIST Cybersecurity Framework are:

- **Identify** (knowing assets and risks),
- **Protect** (protecting systems and data),
- **Detect** (keeping an eye out for cybersecurity events),
- **Respond** (acting when incidents happen), and
- **Recover** (resuming regular operations following a breach).

This version of the framework enables startups to gradually expand their cybersecurity maturity over time, rather than attempting a full-scale deployment all at once, by emphasizing modular processes and low-cost implementation methodologies. Figure 2 presents a sample of a basic high-level process flow for small and internet startups utilizing NIST CSF.

Apart from the above, it is crucial to remember

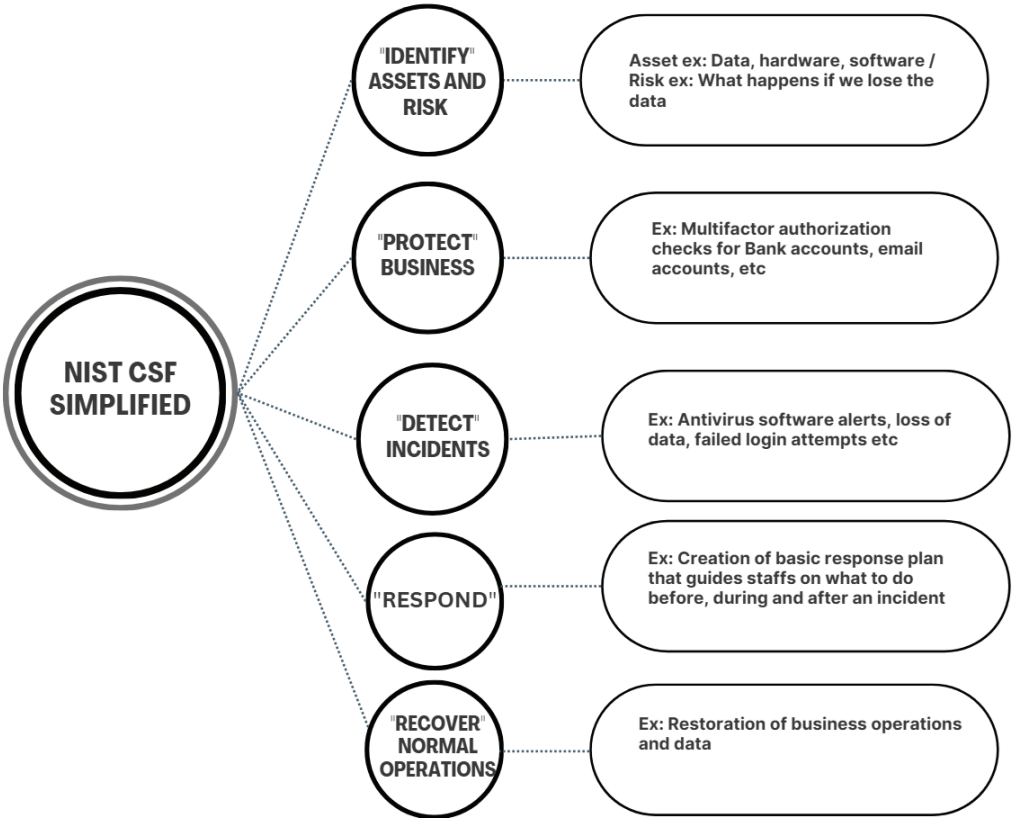

Figure 2. Author created high-level process flow for small and internet startups utilizing NIST CSF.

that the NIST CSF model still has limits, even in this modified version that is suited to the requirements of "online startups and small businesses." Because the NIST CSF lacks simple, user-friendly dashboards, it is more challenging for startups to gauge their degree of maturity or monitor advancements. There are no useful, straightforward templates that small firms can use for their daily operations. Additionally, startups struggle to identify the most recent emerging risks without access to subscriptions. Small entrepreneurs still rely on manual log checks and simple alert systems, as they cannot afford paid security information and event management (SIEM) and security operations center (SOC) tools, such as Splunk, IBM QRadar, Cortex XSOAR, or CrowdStrike. Another drawback is that, regarding these five fundamental functions, many small firms continue to disregard cybersecurity, and many employees operate their companies without receiving the necessary awareness training. Plans may exist on paper, but there are still no practical testing drills in place. Maintaining SMEs and documentation maintenance controls is still a challenge for many entrepreneurs. Many employees of small businesses take cybersecurity for granted and are unaware of its importance. This results from a lack of understanding and instruction to enforce the necessity of protection. As a result, their safeguards and training procedures are not adequately evaluated or maintained in the event of an emergency. Additionally, they are unaware of how to track the most recent program upgrades, password changes, user access levels, or versions. They are unaware of the most recent vulnerabilities and assaults because many good basic security procedures are not followed on a regular basis.

RESULTS

To bridge the gaps of lack of automation infrastructure, limited staff awareness, periodic drills, high cost, etc., Online Startups and Small businesses can "Identify" the function and asset mapping and can utilize free tools like Center for Internet Security (CIS) controls or NIST's cybersecurity starter kit for strengthening their asset mapping capabilities. They can also perform frequent software and patch management updates, and search for inexpensive Google Authenticator apps, BitLocker, or ProtonMail programs to "Protect" their business accounts. Small business owners should think about utilizing lightweight antivirus software with warnings, such as Avast products, to "Detect" occurrences. They can use pre-made, basic templates to conduct basic tabletop exercises with a recurring evaluation process to "Respond" to incident plans. They can create a basic recovery checklist and set up a basic Google Drive or Dropbox account to "Recover" their business. In addition, Online Startups and Small businesses should collaborate with nearby educational institutions or cybersecurity incubators to offer free audits and consulting, as well as utilize community-based resources. They can also take advantage of cloud security defaults, such as those provided by Microsoft Office or Google Workspace, which have built-in safeguards that support NIST's objectives. According to the *NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide*, the Framework "*is not a one-size-fits-all approach to managing cybersecurity risks*," and encourages organizations to adapt it based on their "*own risk tolerances, priorities, threats, vulnerabilities, requirements, etc*." (9). Based on this, Table 3 provides a basic go-to checklist for Online startups and small businesses to use as a quick reference guide.

Small businesses can train their staff using free tools like Google's Phishing Quiz and watch beginner-level short videos on YouTube from CISA and NIST to raise awareness. To monitor key activities, startups can utilize built-in alerts from Google Workspace or Microsoft Defender, which work similarly to many free antivirus programs and provide robust protection for Windows PCs right out of the box. The business owner or representative can check access logs on platforms such as Google Drive or Dropbox and manage user access via tools like Google Admin Console, monitoring the environment practically with low-cost steps. These straightforward best practices can help small organizations become more resilient to cybersecurity threats and serve as a great backup plan for their urgent security requirements.

CONCLUSION

This study highlights the importance of protecting small businesses in the same manner as models safeguard larger corporations and governmental bodies. Online startups and small businesses are essential to the growth of the regional economy and the creation of jobs. Cybersecurity is a significant and complex challenge for online startups and small businesses in the modern world. The protection of online startups and small businesses is a shortcoming of the current cybersecurity approach, which largely concentrates on safeguarding major organizations and government agencies. Implementing cybersecurity policies presents several challenges for small organizations, including a lack of subject matter

Table 3: Go-to Checklist

Simplified NIST CSF Checklist		
Roles and Responsibilities	Yes	No
Employees understand user roles		
Employees understand basic potential risks (phishing emails, unknown links, ransomware, etc)		
Create an inventory list of assets (ex: Laptops, iPads, accounts, and customer data)		
Employee understands the company's cybersecurity goals and risk tolerance		
Appoint someone to oversee cybersecurity responsibilities		
Employees use strong passwords and multi-factor authentication		
All software and applications are up to date and current		
Antivirus software is in place		
Delete the former employee's user access		
Periodic training for current employees about basic cybersecurity threats (		
Monitor and log failed login attempts		
Monitor unusual device slowdown incidents		
Have a response plan in place (Ex: who to notify when incident occurs)		
Ensure data gets backed up regularly		
Review lessons learned after incidents		
Create a business continuity contact list in case of incidents		

experts, budgetary constraints, limited resources, time constraints, and financial limitations. Resolving these challenges and constraints is crucial. In reality, most online startups and small businesses rely on manual procedures with no major automation processes, with less regular review training, inadequate business continuity plans, or disaster recovery procedures. These challenges and difficulties can be resolved by developing flexible cybersecurity models, such as modifying the NIST CSF, and adapting its fundamental features, including "(Identify, Protect, Detect, Respond, Recover)" to small businesses in a simplified manner. This can help meet end users' needs through efficient, scalable solutions, such as using free or inexpensive tools for basic security. Even with their limited resources, small business owners may avoid ransomware attacks, phishing scams, and other data breaches by using this type of customized sequence to create a solid, dependable foundation. In addition, to bridge the gap, it is crucial to teach online startups and small businesses how to collaborate with local community organizations, academic institutions, or work with cybersecurity incubators, utilizing built-in cloud security features and free public frameworks like CIS Controls. The cybersecurity future of online startups and small businesses depends on inexpensive solutions, mentorship, support, and awareness from the local community, in addition to updated maturity models. Even smaller organizations can expand safely in this digital era by adhering to these best practices.

REFERENCES

1. Annamalai D & Satyam A. (2023). *Unaware, unfunded, and uneducated: A systematic review of SME cybersecurity.* arXiv preprint arXiv:2309.17186. Available from: https://doi.org/10.48550/arXiv.2309.17186 (accessed on 2024-03-22)
2. Brezavšček A & Baggia A. *Recent trends in information and cyber security maturity assessment: A systematic literature review.* Systems. 2023; 13 (1): 52. Available from: https://doi.org/10.3390/systems13010052 (accessed on 2024-03-22)
3. CyberSaint. (2023, March 22). *Cybersecurity maturity models you could align with.* CyberSaint. Available from:

https://www.cybersaint.io/blog/cybersecurity-maturity-models-you-could-align-with (accessed on 2024-03-22)
4. Cybersecurity and Infrastructure Security Agency (CISA). (n.d.). *Cybersecurity best practices*. U.S. Department of Homeland Security. Available from: https://www.cisa.gov/topics/cybersecurity-best-practices (accessed on 2024-03-22)
5. Cybersecurity Ventures. (2023). *Cybersecurity jobs report: 2023–2025.* Available from: https://cybersecurityventures.com/jobs/ (accessed on 2024-03-22)
6. National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity, version 1.1.* Available from: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (accessed on 2024-03-22)
7. National Institute of Standards and Technology (NIST). (2022, July 21). *Cybersecurity challenges and opportunities for small businesses: Field hearing testimony.* U.S. Department of Commerce. Available from: https://www.nist.gov/speech-testimony/cybersecurity-challenges-and-opportunities-small-businesses-field-hearing (accessed on 2024-03-22)
8. National Institute of Standards and Technology (NIST). (n.d.). *Small business cybersecurity corner.* U.S. Department of Commerce. Available from: https://www.nist.gov/itl/smallbusinesscyber (accessed on 2024-03-22)
9. National Institute of Standards and Technology. (2024). *NIST Cybersecurity Framework 2.0: Small business quick-start guide (NIST Special Publication 1300).* U.S. Department of Commerce. Available from: https://doi.org/10.6028/NIST.SP.1300 (accessed on 2024-03-22)
10. National Cybersecurity Alliance & CybSafe. (2022). *Oh Behave! The annual cybersecurity attitudes and behaviors report.* Available from: https://www.getcybersafe.gc.ca/en/resources/oh-behave-annual-cybersecurity-attitudes-and-behaviors-report-2022 (accessed on 2024-03-22)
11. Rea-Guamán AM, San Feliu T, Calvo-Manzano JA & Sanchez-Garcia ID. *Comparative study of cybersecurity capability maturity models.* In A. Mas et al. (Eds.), *Communications in Computer and Information Science* (2017; 770: 100–113). Springer. Available from: https://www.researchgate.net/publication/319640924_Comparative_Study_of_Cybersecurity_Capability_Maturity_Models (accessed on 2024-03-22). https://doi.org/10.1007/978-3-319-67383-7_8
12. U.S. Department of Defense. (2021). *Cybersecurity Maturity Model Certification (CMMC) model overview, version 2.0.* Office of the Under Secretary of Defense for Acquisition and Sustainment. Available from: https://dodcio.defense.gov/Portals/0/Documents/CMMC/ModelOverview_V2.0_FINAL2_20211202_508.pdf (accessed on 2024-03-22)