Cybersecurity for Small and Medium-Sized Businesses

Oliver A. LUUKKONEN[*], Yeşim ÜLGEN SÖNMEZ[**]

Abstract

Cybersecurity is all the devices and software applications that protect computers, networks, software, critical systems, and data from possible digital threats. The organizations have a responsibility to secure data to maintain customer trust and ensure regulatory compliance. They use cybersecurity measures and tools to protect sensitive data from unauthorized access, as well as prevent disruption to business operations due to unwanted network activity, and implement cybersecurity by streamlining digital defense across employees, processes, and technologies. Small and medium-sized businesses (SMBs) which make up a large portion of organizations, contribute greatly to the economies of many countries. However, SMBs tend to not care enough about cyber security or do not have the resources to implement it. Additionally, cybersecurity research rarely focuses on SMBs. SMBs have extensively switched to remote/hybrid working due to the global pandemic COVID-19 and this transition to remote/hybrid working methods had to adopt new digital strategies and technologies very quickly. This situation has led to the emergence of more cyber risks and cyber-attacks. This study highlights that it is crucial to strengthen SMBs and future preparedness against cybersecurity threats. Specifically, in this study, cyber security problems and deficiencies in SMBs are identified and suggestions are offered to eliminate them. Also, the work has shown the importance of why the countries should give importance to SMB cybersecurity as well as the defense industry and future studies should focus more on SMB cybersecurity applications.

Keywords: *Medium Businesses, Small Businesses, SMBs Cybersecurity, SMB Cyber-attacks, SMB Defense Techniques*

1. Introduction

Daily life that moved to the internet, has introduced many new words into our lives such as *Cybernetics*, *Cyber*, and *Cyberspace* and the transfer of crimes to the internet created the terms *Cyber Crimes* and *Cyber Security*. Cybersecurity is

Original Research Article
Received: 28.07.2023
Accepted: 15.11.2023
[*] MA Student, Department of Computer Science, Sam Houston State University, Huntsville, USA. E-mail: oal006@shsu.edu ORCID https://orcid.org/0009-0009-1384-4118
[**] Dr., Department of Software Engineering, Faculty of Technology, Fırat University, Elazığ, TÜRKİYE. E-mail: phdyus@gmail.com ORCID https://orcid.org/0000-0002-2090-0263

defined as things that are done to protect a person, organization, country and their computer information against crime or attacks carried out using the internet ('Cambridge Dictionary', 2023; Eş & Serdar, 2021).

Cybersecurity is all devices and software applications that protect computers, networks, software, critical systems, and data from possible digital threats. The fact that businesses use technologies such as the internet, intranet, and extranet and that many of their employees carry out internet-connected transactions has made businesses the target of electronic attacks but they have a responsibility to secure data to maintain customer trust and ensure regulatory compliance (Chidukwani, Zander, & Koutsakis, 2022; Eş & Serdar, 2021; Levy & Gafni, 2022).

They use cybersecurity measures and tools to protect sensitive data from unauthorized access, as well as prevent disruption to business operations due to unwanted network activity, and implement cybersecurity by streamlining digital defense across employees, processes, and technologies (Levy & Gafni, 2022).

Small and medium-sized businesses (SMBs) which make up a large portion of organizations, contribute greatly to the economies of many countries. However, SMBs do not care enough about cyber security or do not implement it. Additionally, cybersecurity research also rarely focuses on SMBs. SMBs have switched to remote/hybrid working due to the global pandemic COVID-19 and this transition to remote/hybrid working methods had to adopt new digital strategies and technologies very quickly (İyem & Danyal, 2021; Levy & Gafni, 2022). This situation has led to the emergence of more cyber risks and cyber-attacks.

Small and Medium-Sized Businesses (SMBs) are important for economic development in most countries, especially in the Western world, as they represent the majority of businesses (Levy & Gafni, 2022; Zec, 2015). Gafni and Pavel stated that SMBs, a term generally used in the United States (USA), are known as Small and Medium Enterprises (SMEs) in Europe (Gafni & Pavel, 2019). Sizes vary between countries. Different regions have their definitions of "small or medium" and are usually measured by the number of employees. For example, the European Commission (2022) stated that organizations with less than 250 employees are considered SMEs. While organizations with fewer than 500 employees are considered SMBs in the United States ('U.S. Small Business Administration', 2023), other countries account for SMBs as organizations with fewer than 500 employees.

Throughout the world, SMBs are a huge part of the growing global economy (Paulsen, 2016). It constitutes 90% of the global economy and more than 50% of employment worldwide (Chidukwani et al., 2022). They generate a significant portion of a country's overall national income (GDP) along with creating new jobs that stimulate a country's economic growth ('World Bank SME Finance: Development news, research, data | World Bank', 2023). According to estimates, 600 million jobs will be needed by 2030 to accommodate the growing global workforce, making the development of SMBs a high priority for many governments around the world. Most formal jobs in emerging markets are created by SMBs, which create 7 out of 10 jobs ('World Bank SME Finance: Development news, research, data | World Bank', 2023).

Therefore, in terms of both economy and security, SMBs need to have strong cyber security while taking advantage of all the opportunities offered by today's multi-channel digital world. Many SMBs have had to adopt new digital strategies and technologies very quickly to maintain, stabilize, or diversify their business activities and models during the global pandemic and the rise of remote/hybrid working methods. This situation has led to the emergence of additional cyber risks (Eaves, 2023; Levy & Gafni, 2022).

Two main external threat vectors faced by SMBs stand out; Phishing and Social Engineering in the Supply Chain ecosystem ('Ponemon Institute', 2018). When combined with internal threat vectors including lack of risk assessment, poor access control, data, device and password protection, low levels of investment, inadequate training and awareness, and cyber hygiene culture and skills, this creates a potentially very broad attack surface.

Precautions that SMBs should take against cyber-attacks can be listed as follows;

- All data regarding the company's sellers, customers, and sales should be recorded. In short, a list of all information and assets about the company should be created.
- Many security breaches are caused by outdated software, including security software, web browsers, and operating systems. Therefore, it is of great importance to update all technological tools.
- Regardless of the size of the company, it is necessary to have a backup system. It is necessary to back up old information and switch to an automatic backup system. The backup system will make SMBs feel safe against ransomware attacks, which they frequently encounter.

- It is of great importance for SMBs to inform their employees about e-mail fraud incidents. You need to be careful with unusual connections.
- You need to have an action plan ready against hackers. What to do and the methods to be followed in case of any data breach should be determined.
- SMBs need to use complex passwords for the system they use. Additionally, even if a unique password is used, passwords should be updated frequently.
- It is possible to protect against ransomware, albeit partially, thanks to antivirus programs. Therefore, your antivirus program must be running.
- To fully ensure information security, consultancy services on information security should be obtained. There is a need for a security service provider to step in in case of any threat. Here, attention should be paid to the solution tools and service quality of the service provider. In addition, safety standards and compliance with certificates should be checked.

According to research, 80% of SMBs accept IT security as a priority issue, and 50% of them do not have an IT security expert. It was revealed that 30% of them spent less than 1000 USD on IT security in a year.

With the increasing use of e-commerce and evolving technology, one would think it would be almost a given in this day and age that businesses would be making sure they are secure from constant cyber threats. That is not always the case. While large-sized businesses have the luxury of large budgets to dedicate to cybersecurity and manpower, SMBs are not that fortunate because of the inherent challenges that they face, such as limited resources and manning. These challenges can become a hindrance to an SMB's overall cybersecurity. SMBs' limited budget, lack of manpower, and even lack of knowledge of cybersecurity leave them open to attacks (Sill, 2023). Due to these challenges and SMB's high impact on a given economy, they are consistently targeted by cybercriminals and deemed easy targets. With their limitations, SMBs must maximize their limited resources as best they can. Allowing for a large budget dedicated to cybersecurity manpower, the latest cybersecurity technology, and training is just a pipe dream in most SMBs. Even some recommendations for SMBs are not very cost-effective. Fortunately, there are a significant number of resources and recommendations available to SMBs that are perfect for their meager budgets. Utilizing these cost-effective resources and recommendations will allow SMBs to increase their

cybersecurity awareness, training, and security all while spending little to nothing.

This study highlights that it is crucial to strengthen change and future preparedness against the cybersecurity threat. It reveals the cyber threat landscape for SMBs, and why this is so significant challenge faced. In This study, cybersecurity studies in SMBs are examined. Cyber security problems and deficiencies in SMBs are identified and suggestions are offered to eliminate them. The last finding in our study is that the countries should attach importance to SMB cybersecurity as well as the defense industry and future studies should focus more on SMB cybersecurity applications.

2. Literature Study and Background

Nine new-generation technologies that have entered our lives with Industry 4.0. These technologies consist of simulation, autonomous robots, horizontal and vertical system integration, cyber security, Internet of Things (IoT), additive manufacturing, cloud technology, big data analysis, and augmented reality (Demir, Sarıışık, & Öğütlü, 2022). While researching the design principles of Industry 4.0, they tried to determine the usage potential of some of the new generation technologies mentioned above during the implementation of Industry 4.0. Transactions carried out by SMBs have increased digitally over the internet network with the Industry 4.0 process. Invoicing, payment of taxes, etc. carried out by businesses. Along with many different transactions, digital commerce constitutes the most important of these topics. Digital commerce, which constitutes one of the important applications of digitalization, has significantly increased its importance all over the world, especially during the "2020 Global Pandemic" period. In fact, digitalization applications that have been used in the trade of goods and services for many years have been used in the supply chain and marketing stages (Demir et al., 2022).

This research was conducted on what possible threats, issues, recommendations, and even recommended hardware solutions were sought by previous studies to achieve a better overall potential solution for SMBs. Research Reviews were conducted to better understand previous findings on cybersecurity in SMBs (Levy & Gafni, 2022). This study covers a wide spectrum across different industries and cybersecurity threats/vulnerabilities concerning SMBs to complete a better overall picture rather than just focusing on a specific area. This allows for a more complete solution that would cover most aspects.

2.1. General SMB Cybersecurity

In (Paulsen, 2016), Paulsen researched explained how SMBs are targeted by cybercriminals with little repercussions while also potentially using SMBs as a stepping stone to get access to larger businesses and organizations which could cause even more significant damage to economies. Paulsen gives some general ideas on items that SMBs should take into consideration on how to secure their business. The ideas stated are that cybersecurity checklists are geared more towards actual risk profiles rather than the implementation of the security controls in the checklists, SMBs should conduct a business process analysis to determine critical business resources/processes instead of just hiring security professionals to plug the vulnerabilities. The aim is creating a cybersecurity culture within the SMB through proper training, reinforcement of the training, and ensuring that the right people are hired (Paulsen, 2016).

2.2. SMB Cybersecurity Management Policies

To see about a more technical aspect, (Teymourlouei & Harris, 2019) gave recommendations and techniques such as

- Understanding the level of cybersecurity knowledge of the business,
- Properly training employees,
- Using VPN connections,
- Antivirus software,
- Utilizing possible cloud-based security solutions.

The other recommendations are

- Using proper password management (complex passwords, password expiration, etc.),
- Conducting backups,
- Using utilize encryption for data at rest,
- Securing Wi-Fi networks,
- Utilizing firewalls,
- Enforcing least-privilege.

It even specified utilizing specific software for encryption (VeraCrypt) and VPN (Windscribe) along with introducing a business questionnaire (Chidukwani et al., 2022; 'Ponemon Institute', 2018; Teymourlouei & Harris, 2019).

2.3. SMB Cybersecurity Management

Alahmari and Duncan dealt heavily with cybersecurity risk management using a review procedure that identified cybersecurity risk perspectives for SMBs based on keyword searches among academic databases (Alahmari & Duncan, 2020). The findings on the cybersecurity risk perspectives were threats underestimated by not utilizing proper security and created high-value targets due to weak defense (SMB Threats). Training, behaviour, and commitment played significant roles in security and safety (SMB behaviour), lack of SMB security practices and engagement with research community (SMB Practices), lack of cybersecurity attacks and associated consequences (SMB Awareness), and lack of experts and professionals in executive manager decisions (SMB Decision-Making) (Alahmari & Duncan, 2020).

2.4. Manufacturing SMB Cybersecurity

Heikkila et al. presented cybersecurity in more specialized manufacturing SMBs (Heikkila, Rattya, Pieska, & Jamsa, 2016). They researched discussed cybersecurity risks associated with manufacturing SMBs along with possible solutions for those SMBs. The research discussed ideas like Enterprise Resource Planning (ERP) implementation for SMBs. The biggest cyber-defense limits in SMBs are budget and security awareness. It is costly and complex and it is seen as a risk. The proper and constant training is important role in manufacturing SMBs. Intellectual property theft is a big concern, for manufacturing SMBs that causes too much emphasis being placed on information protection rather than manufacturing process and life cycle security. Manufacturing technology complexity equals higher risk, and SMBs should make use of free material to help security management due to lack of resources and budget (Heikkila et al., 2016).

2.5. Current Cyber Hygiene of SMBs

Manufacturing SMBs showed similar risks with general SMBs which led to research into the next area of current cyber hygiene amongst SMBs. Ncubukezi et al. discussed how cybercrimes have affected SMBs current cyber hygiene (Ncubukezi, Mwansa, & Rocaries, 2020). They found that cyber hygiene varied amongst SMBs with a general lack of standards/guidelines causing bad cyber hygiene along with results showing current security practices and recommendations for good cyber hygiene. The results showed that 93% of malware incidents had antivirus/antispyware software installed, but unsure if they were updated, 83% of SMBs did not dedicated personnel to remind or run device updates, 100% of SMBs relied on passwords for protection that did not

meet criteria, and cybersecurity risk assessment/analysis was not prioritized with employees relying on their knowledge. The recommendations for SMBs were to include proper cybersecurity awareness programs, training, adherence to security measures, and implementing proper security measures (Ncubukezi et al., 2020). Understanding the cybersecurity hygiene of SMBs can allow for an increase in providing suitable solutions.

2.6. Evolution of Cybersecurity Issues in SMBs

With the knowledge gained on the current look of cyber hygiene in SMBs, research focused on the evolution of cybersecurity issues in SMBs. Bhattacharya discussed how changes in information technology have led to an evolution of cybersecurity issues in SMBs in which SMBs tend to fail to evolve with the issues which leave them open for increasing attacks (Bhattacharya, 2015). Bhattacharya presented SMBs constantly fail to put in place proper security policies due to a lack of resources (skills, infrastructure, security assessments, etc.) Information technology evolution has caused SMBs to become more dependent on outsourcing (expertise, cloud computing, etc.). In addition, relying on mobile/portable devices that increase cybersecurity risks, and taking a proactive approach in dealing with evolving cybersecurity threats must include cost-effective, practical, and realistic approaches, which work with the limitations of SMBs (Bhattacharya, 2015).

2.7. Future Proof in SMBs

With the evolution of information technology causing issues with SMBs, research was conducted on possible ways to future-proof cybersecurity in SMBs. Elezaj et al. researched which gave insight on one aspect of future-proofing SMBs (Elezaj, Yayılgan, Abomhara, Yeng, & Ahmed, 2019). They covered Intrusion Detection Systems (IDSs) for SMBs as an important tool for network attacks where an IDS framework consisting of signature-based anomaly detection was utilized to improve the efficiency of detecting network anomalies for SMBs. The research found that challenges facing SMBs regarding IDSs were that there were no IDS public datasets, a gap between intrusion detection results and interpretation, and no self-adaptation. The study further found that utilizing a hybrid IDS (signature-based with anomaly-based) achieved an overall accuracy of 99.9872%. This hybrid IDS checked signature matches first, then tested input on a classifier model and balance to training the model that finally is fed back into the signature database for updating (Elezaj, Yayilgan, Abomhara, Yeng & Ahmed, 2019). This would allow for the self-adaptation of IDSs and protection against possible future

network threats. The biggest concern with utilizing self-adapting IDS is the complexity and cost over regular signature-based IDSs.

2.8. Cyber Attack Impacts on SMBs

Saleem et al. (Saleem, Abedisi, Ande, & Hammoudeh, 2017) presented cybersecurity issues, attack trends, and the effects on SMBs with an emphasis on non-technical individuals. They laid out the cost of attacks, trending threats/challenges, mitigation, and penetration testing value. It stated that attacks like ransomware or the evolution in technology such as cloud and IoT have made it increasingly difficult and costly for SMBs to keep up due to a lack of awareness and emerging threats of IoT device attacks like Mirai are generally caused by a lack of security within the IoT devices. It also provided recommendations in which enterprises should adhere to four security standards (update device software/firmware, encrypt communications/data transfer, strong password policy, and incorporate multi-factor authentication) at a minimum, and conduct regular penetration testing into the SMBs security procedures (Elezaj et al., 2019).

3. Proposed Research and Contributions

While ISO/IEC 27001, COBIT, and NIST have well-laid out standards for cybersecurity frameworks, these are all geared to corporate level-large scale entities in which some of the standards do not fit into SMB concept or there are some others that are more valuable to SMB rather than larger businesses. Moreover, some of the specific standards require extensive workload and/or costs that the SMBs cannot cover. That is why here we base our structure on the common cybersecurity elements that are better fit for SMBs. Specifically, this work proposes to utilize an existing training platform for SMB employees and cost-effective solution to test and patch the system for vulnerabilities.

3.1. SMB Cybersecurity Awareness and Training

Based on the research conducted on cybersecurity in SMBs, indicated that cybersecurity training and awareness were big concerns with SMBs and gave recommendations that proper cybersecurity awareness and training needs to be conducted (Paulsen, 2016; Teymourlouei & Harris, 2019; Elezaj et al., 2019). The greatest issue that SMBs have with conducting proper cybersecurity awareness and training is how to go about it with a limited budget and lack of expertise.

The best solution for SMBs would be to utilize the free and openly available resources online. This is the best cost-effective and time-reducing method for

SMBs. There is no reason that they should re-invent the wheel per se. One of those resources to SMBs for cybersecurity awareness and training is the Department of Defense (DoD) ('Cybersecurity', 2023; Levy & Gafni, 2022) Cyber Exchange Public website (Levy & Gafni, 2022; 'Security Technical Implementation Guides – DoD Cyber Exchange', 2023), This website has numerous free cybersecurity training and awareness modules available to the public. All the modules are self-paced and can be completed usually within an hour, depending on the course. One such course is the Cyber Awareness Challenge training module, which is actually an annual requirement for all DoD personnel to take. It can help give a basic understanding of cybersecurity and increase awareness. These courses can be utilized to satisfy the need for cybersecurity training, awareness, and reoccurring training at SMBs without the need to produce a separate cybersecurity training and awareness program, and with the added bonus of being free.

3.2. Cost-Effective SMB Cybersecurity

Another common concern amongst SMBs found in the literature study was the lack of antivirus/antimalware, firewall, application whitelisting, and encryption software to protect the SMB computers or systems (Teymourlouei & Harris, 2019; Heikkila et al., 2016; Ncubukezi et al., 2020; Saleem et al., 2017). This is a very simple cost-effective solution for SMBs to overcome. This gives SMBs security for antivirus/antimalware, firewall for network protection, and encryption for data at rest, application whitelisting, and code integrity all included with the cost of the OS. While IDSs are valuable assets, utilizing something such as a self-adaptive IDS could be too complex and costly for normal SMBs which leads me to recommend not going the route of hybrid IDSs, but instead sticking with standard signature-based IDSs.

3.3. Securing SMB Computers

The SMB computer's OSs would have to be hardened, firewall setup, and BitLocker to be enabled. This can be a very time-consuming effort where most SMBs would have to hire a dedicated cybersecurity expert to ensure their systems are secure. Most SMBs do not have the time or monetary resources dedicated to handling that, however, there is a very easy cost-effective way to handle it. SMBs can make use of two free applications provided by DoD to secure computers and help with a previous concern in (Paulsen, 2016) that cybersecurity checklists do not show how to implement security controls in checklists. The two free publicly available applications by DoD are Security Content Automation Protocol (SCAP)

and SCAP Compliance Checker (SCC). The applications utilize Defense Information Systems Agency (DISA) created Security Technical Implementation Guides (STIGS) to harden and secure systems ('Security Technical Implementation Guides – DoD Cyber Exchange', 2023). he SCC application is a vulnerability/compliance checker with preloaded STIG benchmarks used to conduct a scan on the computer. While the SCAP application is a Java app used to take the results for the SCC scan and conduct manual STIG checks which were missed by the SCC benchmarks. SCAP can also be used to view STIGs and each of their security requirements. Utilizing SCC and SCAP with the DISA produced STIGs, numerous OSs, applications, and various software can be secured all for no cost to the SMBs.

4. Results and Discussion

SCC and SCAP scans were conducted on a Virtual Machine (VM) loaded with just a plain Enterprise version of Windows 10 (LTSC). The results were recorded to demonstrate on all the security vulnerabilities found with a normal Windows 10 load that would be used by SMBs. Fig. 1 shows how a STIG requirement is displayed in SCAP. The STIG requirement not only discusses why it is recommended, but also how to check for the security requirement, fix action if it is not enabled, and technical references. The SCC application was run with the following Windows 10 benchmarks checked, IE 11 STIG, MS Dot Net Framework STIG, Windows 10 STIG, Windows Defender Antivirus STIG, and Windows Firewall STIG. Fig. 2 shows the SCC application upon start up and Fig 3 shows the results of the SCC application scan.

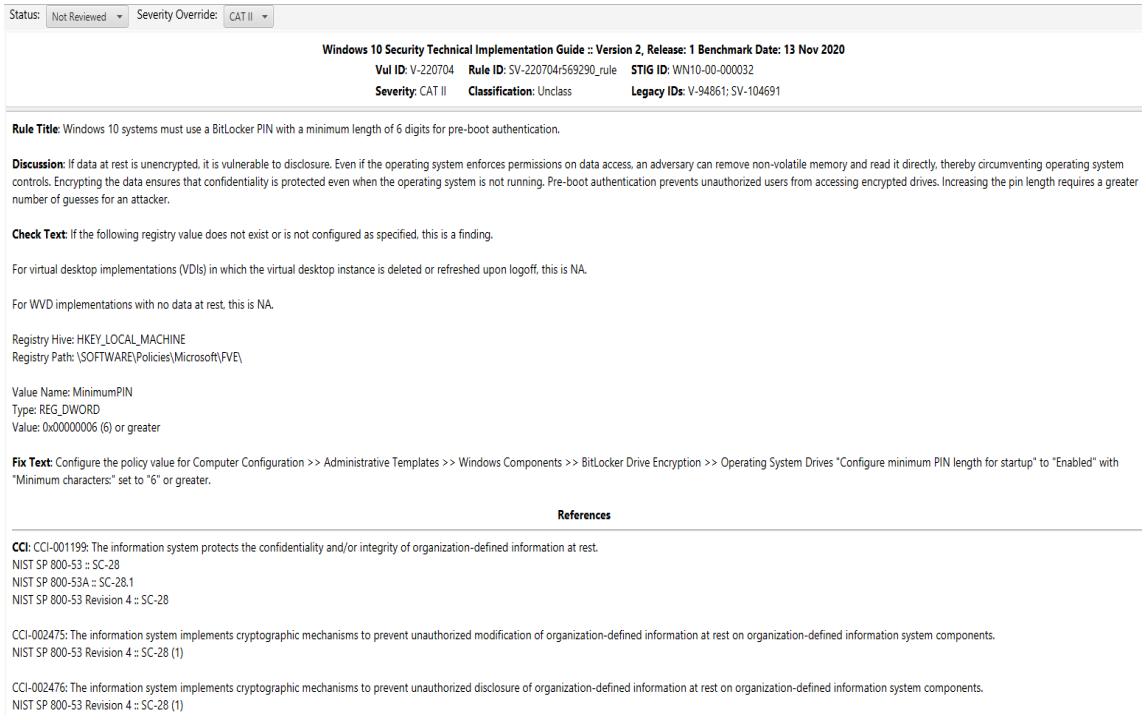


Fig. 1. STIG Security Requirement Displayed in SCAP

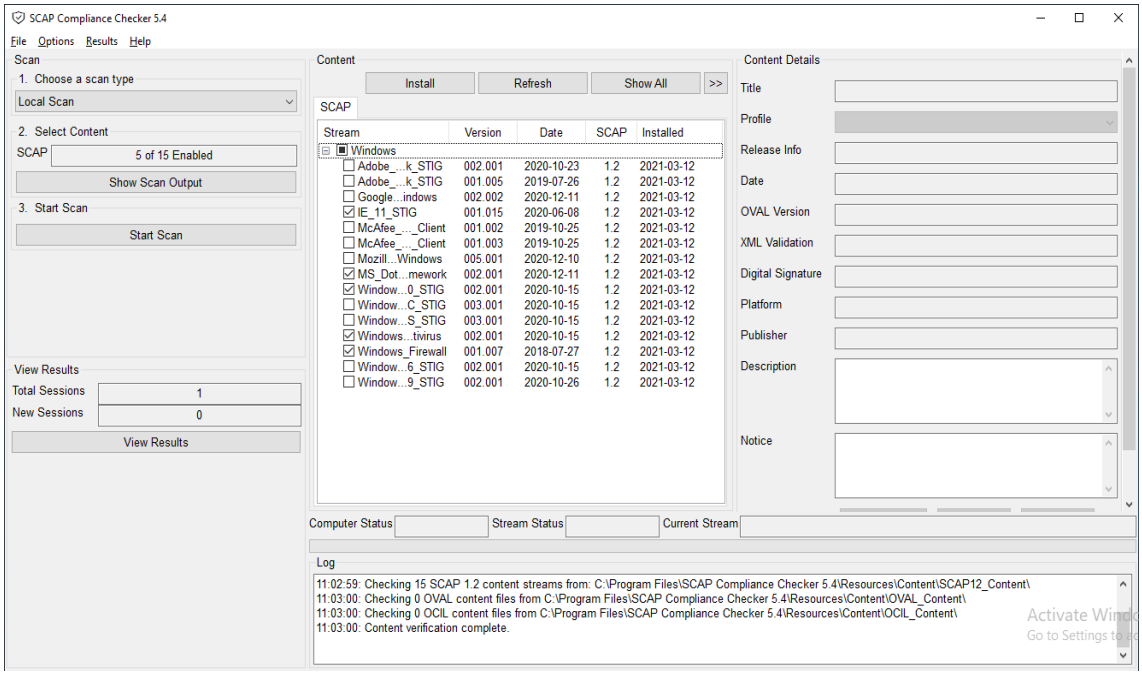
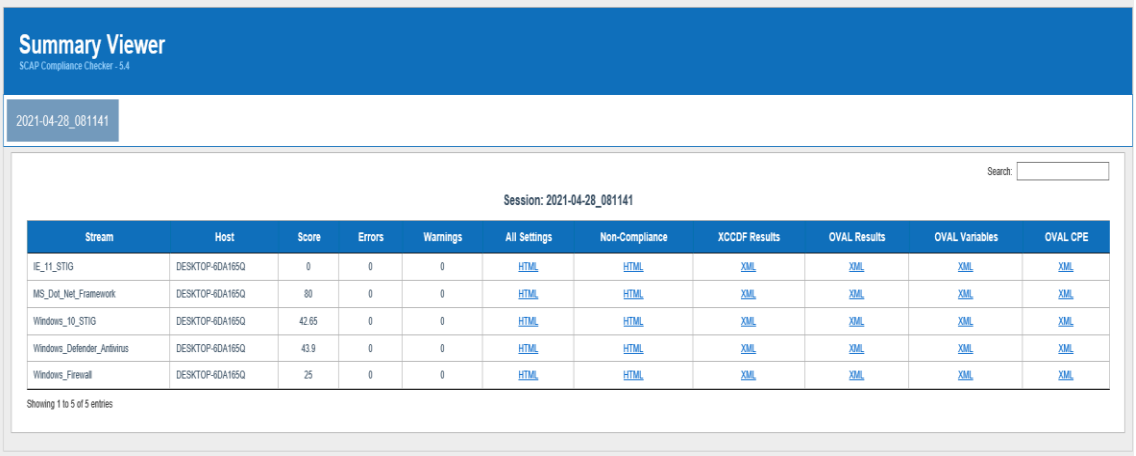


Fig. 2. Starting Stage of SCC Application



Summary Viewer

SCAP Compliance Checker - 5.4

2021-04-28_081141

Search:

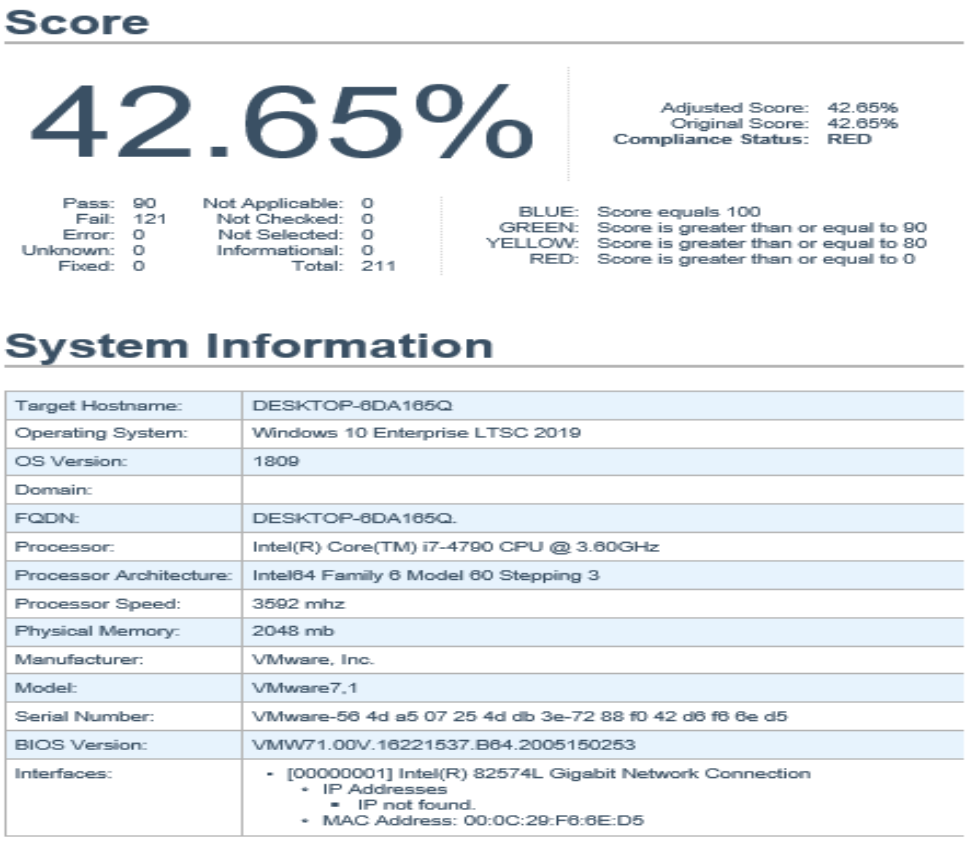
Session: 2021-04-28_081141

Stream	Host	Score	Errors	Warnings	All Settings	Non-Compliance	XCCDF Results	OVAL Results	OVAL Variables	OVAL CPE
IE_11_STIG	DESKTOP-6DA165Q	0	0	0	HTML	HTML	XML	XML	XML	XML
MS_Dot_Net_Framework	DESKTOP-6DA165Q	80	0	0	HTML	HTML	XML	XML	XML	XML
Windows_10_STIG	DESKTOP-6DA165Q	42.65	0	0	HTML	HTML	XML	XML	XML	XML
Windows_Defender_Antivirus	DESKTOP-6DA165Q	43.9	0	0	HTML	HTML	XML	XML	XML	XML
Windows_Firewall	DESKTOP-6DA165Q	25	0	0	HTML	HTML	XML	XML	XML	XML

Showing 1 to 5 of 5 entries

Fig. 3. SCC Scan Results on the SMB Computer

The SCC application scans showed a score of 0% for IE 11, 80% for MS Dot Net Framework, 42.65% for Windows 10, 43.9% for Windows Defender Antivirus, and 25% for Windows Firewall. The higher the score, the more score the area is. As can be seen, a basic Windows 10 system is not very secure. Each individual section can be viewed independently in either HTML or XML. Fig 4 shows a small clip of the breakdown from the Windows 10 section.



Score

42.65%

Adjusted Score: 42.65%
Original Score: 42.65%
Compliance Status: RED

Pass: 90
Fail: 121
Error: 0
Unknown: 0
Fixed: 0

Not Applicable: 0
Not Checked: 0
Not Selected: 0
Informational: 0
Total: 211

BLUE: Score equals 100
GREEN: Score is greater than or equal to 90
YELLOW: Score is greater than or equal to 80
RED: Score is greater than or equal to 0

System Information

Target Hostname:	DESKTOP-6DA165Q
Operating System:	Windows 10 Enterprise LTSC 2019
OS Version:	1809
Domain:	
FQDN:	DESKTOP-6DA165Q.
Processor:	Intel(R) Core(TM) i7-4790 CPU @ 3.60GHz
Processor Architecture:	Intel64 Family 6 Model 60 Stepping 3
Processor Speed:	3592 mhz
Physical Memory:	2048 mb
Manufacturer:	VMware, Inc.
Model:	VMware7,1
Serial Number:	VMware-56 4d a5 07 25 4d db 3e-72 88 f0 42 d6 f6 6e d5
BIOS Version:	VMW71.00V.16221537.B64.2005150253

Interfaces:	- [00000001] Intel(R) 82574L Gigabit Network Connection
	  - IP Addresses
	  - IP not found.
	  - MAC Address: 00:0C:29:F6:6E:D5

Fig.4. SCC Scan Results on Windows 10

The SCC application automatically saves the results in various formats that can be imported into various applications, such as OVAL for OpenSCAP (OSCAP) and XCCDF for SCAP. The results are time-stamped based on the date/time format and saved under the user's profile in Windows. To get the most accurate results for the SCAP application, the following STIGs were downloaded and imported into the SCAP application, MS Dot Net Framework V2R1, MS IE11 V1R19, MS Windows 10 V2R1, MS Windows Defender Antivirus V2R1, and Windows Firewall V1R7. Using the SCC application results, the saved XCCDF XML files can now be imported into the SCAP application for manual STIG checks. The SCAP application is a Java-based application that requires the latest version of JRE to be installed to run the application. Fig 5 shows the SCAP application upon start up and Fig 6 shows the results of the imported SCC application scans.

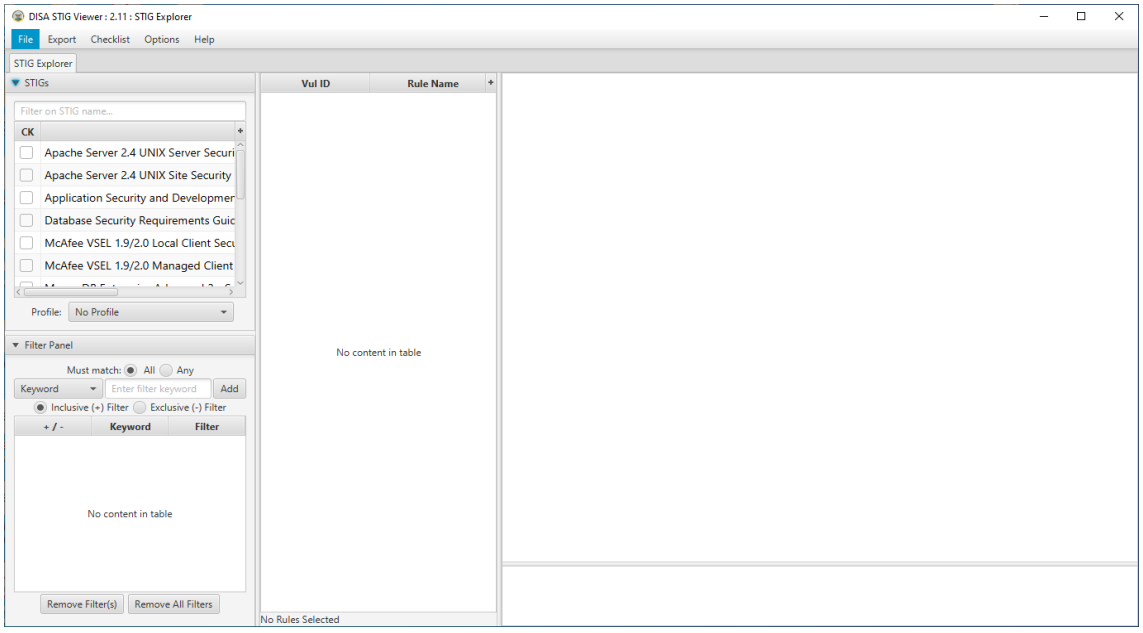


Fig. 5. SCAP Application upon Start-up

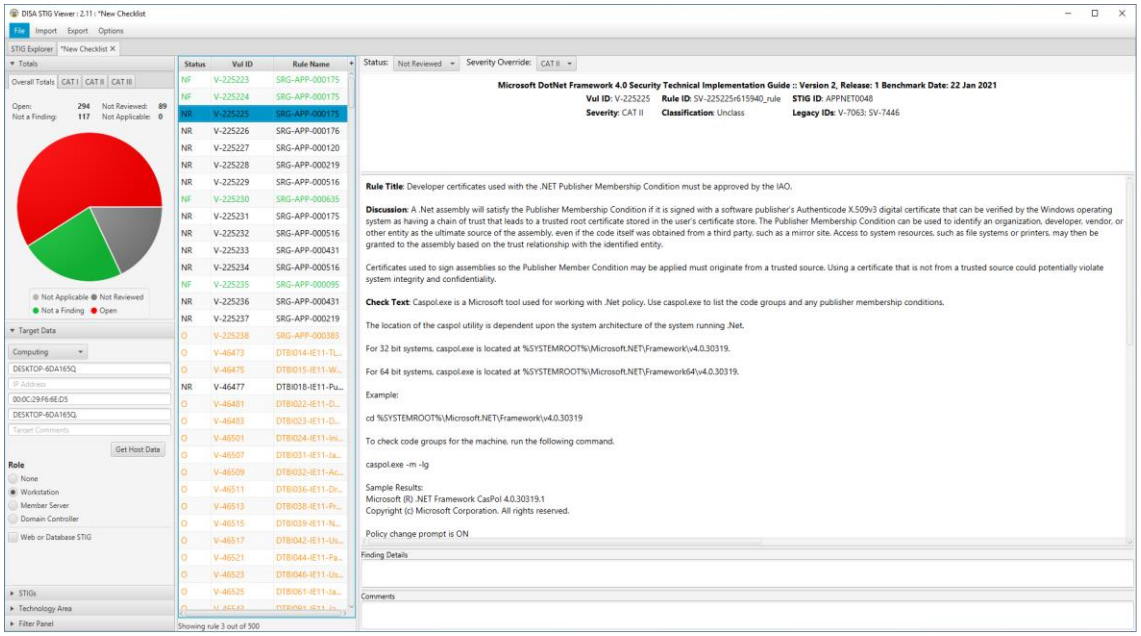


Fig. 6. SCAP Results Obtained from Windows 10 Test Computer

Once the results were loaded and a checklist created, the SCAP application showed a total of 500 findings which 294 were "Open", 117 were "Not a Finding", 89 were "Not Reviewed", and 0 were Not Applicable. Each STIG requirement can be then viewed individually and further assessments can be done to determine fix actions, further guidance, or determination if it is applicable at all.

5. Conclusions and Future Work

SMBs have special requirements that require special considerations to meet their specific needs. Using cost-effective methods that do not hinder their resources (time, manning, and revenue) is the best solution possible instead of relying on the generally accepted cybersecurity standards offered by ISO, NIST, etc. By using free openly available training along with applications designed by the DoD, such as SCC and SCAP, SMBs can ensure that they are as protected as they possibly can be. The items shown are readily available to all and should be utilized as a part of overarching cybersecurity defense.

There will always be a need to find better approaches to securing SMBs. The ones provided offer the bonus of being maintained and updated constantly by the DoD and DISA. This ensures that the latest STIGs and applications are the most up-to-date to better assist SMBs in securing themselves as effectively as possible.

Although the proposed work proved to be effective for a Windows 10 local machine-based SMB, it is also important to note that with sophisticated

Advanced Persistent Threats capabilities and increasing zero-day attacks, the SMB will need to be always on alert for such threats and continue with the regular updates on the systems, training of the employees, and checking other standardizations to enhance the security of such systems. In the near future, we plan to extend this work to other server capabilities and Bring Your Own Device platforms used in SMBs. Also, focusing on a specific SMB type can help the company to create a better-customized security mechanism.

Acknowledgment

The authors of this paper extend their appreciation to Dr. Cihan VAROL for his contribution.

REFERENCES

ALAHMARI, A. & DUNCAN, B. (2020). Cybersecurity risk management in small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence. In *Int. Conf. on Cyber Situational Awareness, Data Analytics and Assessment* (pp. 1–5). Retrieved from https://doi.org/10.1109/CyberSA49311.2020.9139638

BHATTACHARYA, D. (2015). Evolution of cybersecurity issues in small businesses, Technology. In *4th Annual Conference on Research in Information* (p. 11). Chicago, Illinois, USA. Retrieved from https://doi.org/10.1145/2808062.280806

CAMBRIDGE DICTIONARY. (2023). Retrieved 7 October 2023, from https://dictionary.cambridge.org/tr/

CHIDUKWANI, A., ZANDER, S., & KOUTSAKIS, P. (2022). A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations. *IEEE Access*, 10(August), 85701–85719. Retrieved from https://doi.org/10.1109/ACCESS.2022.3197899

CYBERSECURITY. (2023). Retrieved 8 October 2023, from https://business.defense.gov/Work-with-us/Cybersecurity/

DEMİR, S., SARIIŞIK, G., & ÖĞÜTLÜ, A. S. (2022). KOBİ lerin Endüstri 4.0 Farkındalık ve Olgunluk Seviyesinin Belirlenmesi: Şanlıurfa İli Örneği (Determination of Industry 4.0 Awareness and Maturity Level of SMEs: The Example of Şanlıurfa Province). *Journal of Business Research - Turk*, 14(4), 2938–2955. Retrieved from https://doi.org/10.20491/isarder.2022.1543

EAVES, S. (2023). Security for Small and Medium-Sized Businesses | IoT Security Podcast | PSA Certified. Retrieved 7 October 2023, from https://www.psacertified.org/blog/iot-security-for-small-medium-businesses-podcast/

ELEZAJ, O., YAYILGAN, S. Y., ABOMHARA, M., YENG, P., & AHMED, J. (2019). Data-Driven Intrusion Detection System for Small and Medium Enterprises. In *IEEE 24th Int. Workshop on Computer Aided Modeling and Design of Communication Links and Networks* (pp. 1–7). Limassol, Cyprus. Retrieved from https://doi.org/10.1109/CAMAD.2019.8858166.

EŞ, A., & SERDAR, N. (2021). SİBER Saldirilara Karşı Kobilerin Farkındalık Düzeylerini Incelenmesi: Ankara Ili Örneği. *Journal of Duzce University Institute of Social Sciences*, 11(1), 133–151.

GAFNI, R., & PAVEL, T. (2019). The invisible hole of information on SMB's cybersecurity. *Online Journal of Applied Knowledge Management (OJAKM)*, 7(1), 14–26.

HEIKKILA, M., RATTYA, A., PIESKA, A. S., & JANSA, J. (2016). Security Challenges in Small- and Medium-Sized Manufacturing Enterprises. In *Int. Symp. On Small-scale Intelligent Manufacturing Systems* (pp. 25–30). Narvik, Norway. Retrieved from https://doi.org/10.1109/SIMS.2016.7802895

IYEM, C., & DANYAL, Y. (2021). Teknoloji Geliştirme Bölgelerinde COVID-19 Pandemisi Üzerine Nitel Bir Araştırma: KOBİ'lerde Dayanıklılığı Artırmak İçin Acil Durum ve İş Sürekliliği. *Ekonomik ve Sosyal Boyutlarıyla PANDEMİ*, 89–162.

LEVY, Y., & GAFNI, R. (2022). Towards the quantification of cybersecurity footprint for SMBs using the CMMC 2.0. *Online Journal of Applied Knowledge Management*, 10(1), 43–61. Retrieved from https://doi.org/10.36965/ojakm.2022.10(1)43-61

NCUBUKEZI, T., MWANSA, L., & ROCARIES, F. (2020). A Review of the Current Cyber Hygiene in Small and Medium-sized Businesses, In *15th Int. Conf. for Internet Technology and Secured Transactions* (pp. 1–6). London, United Kingdom. Retrieved from doi: 10.23919/ICITST51030.2020.9351339

PAULSEN, C. (2016). Cyber Securing Small Businesses. *Computer*, 49(8), 92–97. Retrieved from https://doi.org/10.1109/MC.2016.223

PONEMON INSTITUTE. (2018). Retrieved from Https://www.keepersecurity.com/assets/pdf/Keeper-2018-Ponemon-Report.pdf

SALEEM, J., ABEDISI, B., ANDE, R., & HAMMOUDEH, M. (2017). A state of the art survey – Impact of cyber-attacks on SME's. In *Int. Conf. on Future Networks and Distributed Systems '17* (pp. 1–7). Cambridge, United Kingdom. Retrieved from https://doi.org/10.1145/3102304.3109812.

SECURITY TECHNICAL IMPLEMENTATION GUIDES – DoD CYBER EXCHANGE. (2023). Retrieved 8 October 2023, from https://public.cyber.mil

TEYMOURLOUEI, H. & HARRIS, V. E. (2019). Effective methods to monitor IT infrastructure security for small business. In *Computational Science and Computational Intelligence* (pp. 7–13). Las Vegas, NV, USA. Retrieved from

https://doi.org/10.1109/CSCI49370.2019.00009

U.S. SMALL BUSINESS ADMINISTRATION (2023). Retrieved 7 October 2023, from https://www.sba.gov/business-guide/manage-your-business/stay-safe-cybersecurity-threatsVerizon

WORLD BANK SME FINANCE: Development news, research, data | World Bank. (2023). Retrieved 6 October 2023, from https://www.worldbank.org/en/topic/smefinance

ZEC, M. (2015). Cyber security Measures in SMEs: a study of IT professionals' organizational cyber security awareness. *Linnaeus University, Kalmar. Zugriff Unter Http://Www …*, 1–99. Retrieved from https://www.diva-portal.org/smash/get/diva2:849211/ATTACHMENT01.pdf