Best Practices Used by Businesses to Maintain Good Cyber Hygiene During Covid19 Pandemic

Tabisa Ncubukezi, Laban Mwansa
Cape Peninsula Universty of Technology
South Africa

Abstract

Businesses using cyberspace are expanding every day, with Internet users performing different activities affecting cyber hygiene. The user's actions may be good or bad – ultimately determining the state of cyber hygiene. Good cybersecurity hygiene requires a thorough implementation of the best practices to improve safety and protect information or resources, while bad practices lead to data corruption, loss and breaches. Compromised cyber hygiene is the result of exposure to various cyber-attacks. Our paper reports the best practices used by different business sectors to maintain cyber hygiene. The study used a qualitative survey mounted on google with 20 business owners and Information Technology managers. We explored the use of best practices to understand business experiences in reducing and avoiding cyber-attacks and improve cyber health. We analyzed the collected data and presented the findings. Cyber essentials have been recommended as the guideline to mitigate cyber risks.

1. Introduction

Covid19 global pandemic caused individuals and businesses to depend on information and communication technology (ICT) for their production. The rate of ICT and Internet use exposed businesses to numerous cyberattacks, which are working full force in finding loopholes that will dent the overall cyber hygiene [15], and [20].

Reference [30] compares the cyber hygiene to personal hygiene. For the personal hygiene, individuals follow a specific guide to improve their health. In contrast, the businesses implement the best cyber hygiene practices to secure and protect their information and other resources against old and emerging cyberattacks. Consequently the best practices are essential in businesses to protect business devices from any software or hardware damage as well as the data loss [30], and [32]. Good cybersecurity hygiene is a major asset and security measure that provides cyber defense. As stated by references [15], and [24] the healthy cyber hygiene requires cyber users to apply proper safety measures to all aspects of cyberspace.

Our work aims to examine best practices used by different businesses to maintain cyber hygiene.

- The study determines the best practices used to maintain the end devices, network, and information.

The rest of the paper presents the background study and the related work on section 2, inquiry method on section 3, results on section 4, discussion and recommendations on section 5, and the conclusion on section 6.

2. Cyber hygiene

In academia, there are many attempts used to describe the term 'cyber hygiene'. As a results, reference [31] describes it as collecting cybersecurity steps to safeguard computer users and other technological devices. While reference [25] describe cyber hygiene as the recommended mitigations plan for the small number of root causes responsible for many cybersecurity incidents. According to [6], the term is also described as the general practice and continuous routine to improve the online platform's safety and security. At the same time, cyber hygiene is a broad term that illustrates components to promote good cyber hygiene at all levels [9], and [8]. Other also use the term in the training context, to train the workforce to guard against common errors and attacks leading to cyber intrusion [4], and [10].

The above descriptions all have something in common which is the safety and security of the information and devices against cyberattacks. For instance, reference [23] explains the importance of cybersecurity at the user, technical, organizational, and economic levels.

The involvement of all sections of the business promotes acceptable cyber hygiene. Cybersecurity's best practices should be prioritized at all levels, including getting personnel to bring their own devices to work (BYOD), all applications and information, the facilities, and encouraging people to maintain good cyber hygiene [13]. Cybersecurity which presents the mitigation strategies against various root causes and cyber incidents should be the major concern when using cyberspace. [25].

 | DOI: 10.20533/jitst.2046.3723.2021.0086

Modern businesses use essential technology as a driving factor while it poses security challenges leading to poor cyber hygiene. Companies must apply best practices to protect the business applications and technology used for both hardware and software [15]. As technology has gained popularity and benefits to industry, the technology requires continuous hardware and software updates, using the latest patches to improve its security [2]. Also, constant investment in up-to-date security measures for both the hardware and software can prevent information and financial losses [12].

Another asset to a business is what facilities are ultimately used to meet the competitive environment for producing the desired outcomes. The facilities which require best practices presents the environment that keeps and protects the hardware infrastructure, requiring thorough safety and security measures to be maintained. As used in this paper, information technology and networking infrastructure facilitate the transmission of data in cyberspace.

The infrastructure comprises networking devices such as routers, switches, hubs, cables, and other additional devices [32]. This networking infrastructure helps with the transmission of data from one point to the other. In businesses, processed data (information) represents a valuable asset of the company because enterprises vary based on their information and how it is handled.

Employees in businesses represent an asset to the company. They have to be involved in the planning and processing of events. Employees of enterprises include management, end-users, and technical people. Business growth depends on the involvement of people and the recognition of the critical role that people play. Employees should participate in the planning, designing, implementing, and testing of cybersecurity technologies to promote good cyber hygiene [6]. There cyber security policy should cover the best practices that can be used for business users and their activities on the cyberspace.

A good cyber hygiene is an integral part of every business. All businesses should prioritize cyber hygiene in all aspects of the cyberspace including the user level, network level, end device level, application and information levels. Proper cyber hygiene requires best practices which are regularly applied. The following section presents the reasons why cyber best practices are essential for both cyber users and the businesses.

2.1. Why best practices to maintain cyber hygiene?

Covid19 pandemic increased cyberspace usage and connection to the world through a simple click. Likewise, the cyberspace has become the way of working which makes people and business vulnerable to cyber risks [24]. The high usage of cyberspace makes peoples' lives easy and exposes their information to cyber threats. There is no doubt that cyber users are vulnerable to various cyber risks [15].

The best way to safe and secure surfing requires proper use of the cyber hygiene best practices. Acceptable practices are necessary to improve, proactively protect, secure, monitor, and maintain everyone's information on the Internet [3], and [7]. The continuous application of the best practices should be a routine that ensures user identity, safety, and information. The best ways help reduce the chances of resource damage, corruption of information, loss of information, and data breach to improve cyber hygiene [17]. The regular use of the best practices to maintain cyber hygiene brings peace of mind with the potential of reaching an excellent business outcome.

2.2. Causes of poor cyber hygiene

Reference [8] discovered that numerous cyber factors had resulted in Africa becoming particularly susceptible to cybercrimes. Their analysis identifies a lack of or minimal cybersecurity awareness, useless legislation policies, and the absence of technical cybersecurity measures. Reference [27] indicated that the lack of a firewall, access control, malware protection, and patch management results in poor cyber hygiene. Bad cyber hygiene becomes extremely dangerous to businesses at large [11]. The same applies to the absence of best practices, which help maintain good cyber health [29]. The recommended best practices to protect against sorts of cyber hygiene is presented below.

2.3. Recommended baseline best practices

The baseline cyber hygiene presents the basic steps required for cyber defense. The baseline is mostly rooted in the frameworks such as the NIST cybersecurity framework. It helps businesses to have a clear, detailed set of best practices to guide how cybersecurity is carried out and measured regularly [3]. Even though there may be no standard best practices for businesses, the baseline set of methods to promote good cyber hygiene has been illustrated [28], and [29].

All Internet users and businesses need to take ownership of their surfing, whether at home or the office. Cyber users must always take cyber hygiene seriously by consistently applying the best practices guarding against all sorts of cyberattacks [24]. These practices include:

- Protecting all the cyberattacks and risks associated with internal and external suppliers;
- Addressing and preventing threats;
- Classifying business assets and services;

 | DOI: 10.20533/jitst.2046.3723.2021.0086

- Responding to business risks by establishing the proper response plan;
- Providing training and education about cybersecurity;
- Establishing constant monitoring of the network and accessing control that accommodates all user privileges;
- Having standardized configurations that will help to protect and recover data; and
- Monitoring the cyber threats.

Among other best practices, the lack of the above essential techniques can lead to poor business cyber hygiene. In addition, references [2], and [3] recommended the basic practices for small businesses against all cyber risks. Also, *Figure 1* suggested other guidelines that individuals can use to maintain good cyber hygiene.

Figure 1. User best practices for cyber hygiene [26]

These practices should continuously be implemented to prevent unauthorized access, loss of information, and data breach. The results of using best practices ultimately improves cyber health and provide safe cyber surfing. The following section explains the baseline practice which complies with the National Institute of Standards and Technology's (NIST) cybersecurity framework (CSF).

2.4. Best practices mapped with NIST CSF

References [28], and [29], explains the need for businesses to comply and align with the NIST cybersecurity framework in order to maintain cyber hygiene. The NIST Framework's primary aim is to provide a detailed structure for organizations to improve ways to prevent, detect, and respond to various cyber incidents [17]. The NIST framework has five core functions and categories: to identify, detect, protect, respond to, and recover from cyber threats [13].

Every core function plays its role in promoting good practice in maintaining balanced cyber hygiene at all business levels. To comply with the *"identify"* core function, they need to understand every asset's leading role and responsibility and their vulnerability and risk to cyber-attacks. With this core function, it would be easy for the business to establish the policies and rules that will protect itself against cyber threats to improve good cyber hygiene [28], and 29].

The second core function is to *"protect"* the businesses by applying appropriate measures to guard against potential cybersecurity incidents. In this stage, organizations should provide necessary training and education about security measures at all levels. The third stage involves steps to *"detect"* cyber incidents and to monitor cyber threats consciously. The fourth core function consists of developing the *"response"* plan, which will clarify the communication channels, clearly taking down the cyber incidents. The last stage is to "*recover*" the impaired services caused by cyber incidents and to prioritize the activities [11], [28], and [29].

When businesses do not comply with the five core functions of the NIST CSF, it becomes challenging to handle cyber incidents properly. Additionally, businesses become vulnerable to cyber incidents that could continuously derail business continuity. Reference [29] suggests that all companies must have a clear, detailed plan that addresses cyber incidents, which will promote good cyber hygiene. There are other studies which were conducted on the cyber hygiene. Their work is presented on the section below.

2.5. Related work

Cyber hygiene is the research field that gained more interest during the Covid19 pandemic, where Internet has become the backbone and the new way of working. Internet dependency helped every family and business to connect, especially during the challenging global lockdown times. With the rise on the Internet use, the cyber hygiene for both users and businesses remains a major concern. We have selected three studies which were also concerned with the safety and security of the cyberspace.

A study by [15] reviewed the current cyber hygiene in businesses. The study reported the cyber threats experienced by SMBs, examining the use of security measures in place and the extent of implementing the current mitigation strategies. A sample of 30 SMB was selected in the Western Cape Province.

Another study conducted by [16] examined individual differences associated with developing cyber hygiene-related knowledge, attitudes, and behaviors. Their results from participants demonstrated information handling, incident reporting, and password management as the essential mechanisms to better cyber hygiene. Results also discussed the importance of understanding human factors' role and the practical implications of computer and information sciences curricula.

 | DOI: 10.20533/jitst.2046.3723.2021.0086

Reference [24] also conducted a study exploring aspects of the Internet, related issues, and protection measures against cyber-attacks to improve cyber-hygiene for both individuals and the group. In their study, they found out that cyber hygiene provides better protection and also in monitoring and maintenance of the networks.

Our paper forms part of the ongoing Ph.D. research focusing on developing and evaluating a cybersecurity framework for small and medium-sized businesses in South Africa. It reports different business sector experiences on the use of best practices to maintain good cyber hygiene.

Our paper's contribution is to compare the perceptions and the use of the best practices used by different sectors to improve cyber health. The study further brings awareness to the cybersecurity field to strengthen and develop defensive mechanisms for both the old and the emerging cyber-attacks. The work will also alert the cyberspace users, business owners, and everyone's impact of not having a proper guideline to improve cyberspace, including device, network, and information hygiene.

3. Method

The paper reports four business sector best practices used as cyber defense to improve cyber hygiene. The participants of this study are the business owners and I.T. managers of small businesses. Our work selected participants from the ICT, events, real estate, and construction sectors. A total of 20 research participants (12 males and 8 females) were selected using purposive sampling to analyze the use of cyber hygiene best practices to improve safety and security. The purposive sampling method helped to obtain different insights about cyber hygiene best practices used by various business sectors.

Data collection. All the participants received emails inviting them to participate in the study. The study used an open-ended qualitative questionnaire due to the lockdown restrictions caused by the Covid19 pandemic. The survey was mounted on google forms received a 100% response rate.

Data analysis. We used narrative analysis to analyze the various meanings and experiences of using cyber best practices for different cyber events. Each sector shared its best ways to improve cyber health.

Ethical clearance. The authors received the university's research ethical clearance certificate, which describes the proper anonymity and confidentiality requirements. The following section presents the study results, followed by the discussions, recommendations, and conclusion.

4. Results

In this section, we report about business experiences on applying best practices to maintain good cyber hygiene. The paper reviews best practices used on end-devices, networks, and information. The data was collected from four different sectors. Out of the selected sample, 30% represented ICT, 20% in media, 25% in real estate, and 25% in the construction sector. The results are presented according to the following subsections: device hygiene, network hygiene, and information.

4.1. Device hygiene

Hundred percent of the ICT sector reported that they protect against malware, 80% continuously update the hardware and software updates, and 100% safeguard access to the devices by using the username and password. On the contrary, the events sector reported that 45% protect against malware attacks, 15% consider software and hardware updates, and 50% use passwords. On the other hand, in real estate sector, 65% safeguard against malware attacks, 70% update their software and hardware updates, and 82% use passwords. Regarding the construction sector, 30% protect against malware attacks, 30% focuses on patch management, and 70% use password protection.

For all malware incidents, 93% of the respondents had antivirus and antispyware software installed on their end-devices, even though they were not sure whether they were always updated. For device protection and network access, all the participants relied on the use of passwords. Fifty-eight percent used the accepted password criteria, a combination of numbers, and a combination of the lower- and upper-case letters of the alphabets and symbols, with a minimum length of eight. In contrast, 41.4% only use either five digits or five letters of the alphabet. Fifty percent of them only changed their passwords every three months, 30% changed their passwords after a year, and 20% had never changed their passwords.

4.2. Network hygiene

Findings revealed that 100% of the ICT sector runs proper configurations with 80% of the firewall use and 65% of the gateway use. Regarding the events sector, 55% run the network configurations while only 15% use the firewall and 40% use the default gateway. Real estate participants revealed that 65% use the network configurations, 55% use the firewall to filter the traffic, and 69% use the gateway. On the contrary, the construction sector has 44% with proper configurations, while 31% use the firewall and 25% that use the gateway.

 | DOI: 10.20533/jitst.2046.3723.2021.0086

4.3. Backing up of the information

The respondents believed that the best practice for maintaining good cyber hygiene was to use the password and sometimes backup the individual work, even though some of their passwords were not strong. Three percent believed in the patch updates, 7% believed in protecting both the end-devices and the networking devices, but only 14% believed in backing up their information. None of the respondents mentioned the availability of a detailed document guiding them on handling cyber incidents properly, which ultimately improves cyber hygiene.

The following section presents the discussion of the findings.

5. Discussion

This paper discusses the best practices used by various business sectors to maintain good cyber hygiene. Carrying out the aim, the paper looked at:

- What basic practices do businesses use to maintain end devices, network hygiene, and the information?

This report is based on four business sectors that participated in this study and presented in the figure below. The participants present 30% from the ICT sector, 20% for events, and 25% for real estate and construction.

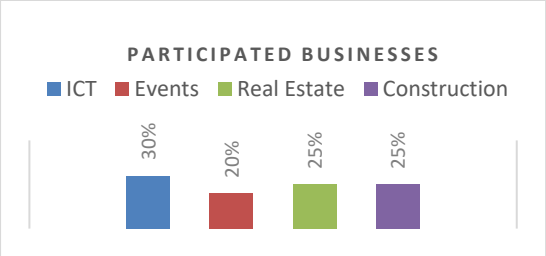

Figure 2. Business sectors

5.1. Basic practices to promote good cyber hygiene

The section reports the best practices used in different sectors to maintain good cyber hygiene. The report is categorized according to the basic practices used for end devices, networks, and information.

5.1.1. Device hygiene. The end devices present any receiving or sending devices which businesses use. Findings revealed that the four various sectors that participated in the study understood end device hygiene and applied the best practices in their way. In this study, we looked at the best practices used for malware attacks, patch management (software and hardware), and access to the device as presented in Figure 3.

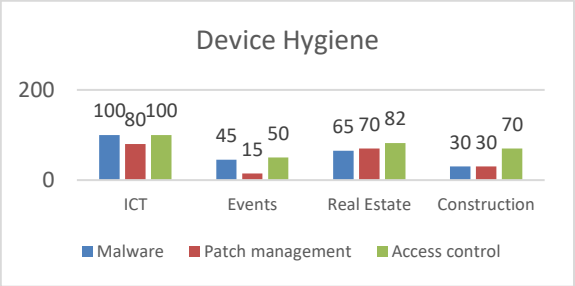

Figure 3. Device hygiene

Regarding device hygiene, the paper looked at the best practices used to protect against unauthorized access, malware attacks, and regular updates for both the hardware and software. The results revealed that users only rely on the use of passwords. A majority do not use the accepted strong combination of the alphabets, numbers, and symbols. References [14], and [22] suggest that all users should always change their passwords every three months. Users must also combine the letters of the alphabet, numbers, and special characters on their passwords.

Reference [27] explains that end devices should be protected against unauthorized access, continuously updating the device software for any available updates [2], [3]. This practice is recommended as the best practice for end devices [27], [19]. Failure to comply with the recommended best practices opens doors to a diverse range of cyber attackers. With the various sectors' experiences on the use of basic practices, it can be concluded that the lack of proper malware protection, patch management, and access control results in poor cyber hygiene.

Bad cyber hygiene becomes extremely dangerous to businesses at large [27] and [11]. The increased usage of technology and users' major role in applying the best practices to maintain cyber hygiene remains different in various sectors [18]. We explore how business sectors use basic practices to promote network hygiene.

5.1.2. Network hygiene. As used in the study, the network hygiene presents the device configurations, the firewall, and the default gateway to filter the incoming and outgoing traffic.

Figure 4 presents various business sectors' responses about their use of the best practices on the network. According to the cyber essentials, a firewall and the gateway are very important to implement on the network to prevent unauthorized access to and from other networks [2], and [24]. Likewise, the configurations protect systems and networks to

 | DOI: 10.20533/jitst.2046.3723.2021.0086

satisfy business needs. The configurations secure information, applications, and network devices.

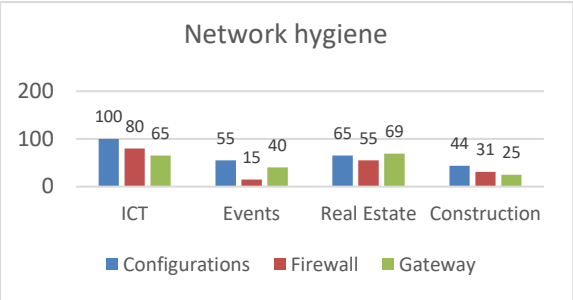

Figure 4. Network hygiene

5.1.3 Backing up of the information. Information is the major asset of the business. Figure 5 presents the findings for information management to maintain cyber health. The ICT sector findings showed that 100% of the participants have a dedicated backup, while 50% only do their backup, and no information is not backed up. The events sector indicated no dedicated person for backing up the business information, 60% at least perform their backup, and 40% do not backup at all.

Regarding the real estate, 70% indicated that they have a dedicated person to back up the information, while 70% perform their backups and 30% do not even back up their information. The construction sector indicated that 43% had dedicated personnel to back up the information, while 58% perform their regular backups, and 57% do not have any information backed up. Backing up of the information is the last safeguard against information loss, misfortune, or information burglary [24].

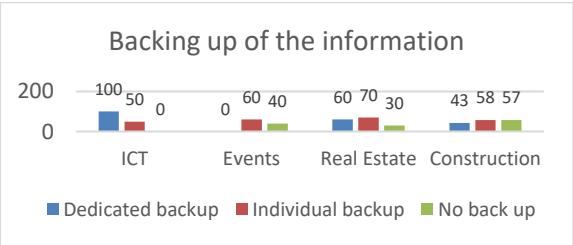

Figure 5. Information hygiene

The use of cyberspace exposes everyone to cyber-attacks and requires basic guidelines to provide a cyber-defense. Undoubtedly, the lack of general cybersecurity in any sector leads to poor cyber hygiene and costs businesses [27]. Reference [1] States that the thorough implementation of the basic practices for cyber hygiene can defeat at least 90 percent of the cyber-attacks.

5.2. Recommendations

Reference [30] suggests that cyber users should always follow the best practices like personal hygiene. He further explains that following the recommended best practice guidelines causes no harm at all. Based on the results of this study, the research recommends the following:

- Internet users should develop an interest in the best practice guidelines to improve the safety of their information. They should read blogs, articles with the latest safety measures, attend webinars, and listen to media. Also, a regular change of the password with appropriate combinations is recommended.
- Businesses should join platforms where recommended, and the latest safety precautions are discussed and made available for everyone. Cyber hygiene should be one of their keys concepts to protect business information and limit data breaches. Further, businesses should invest in maintaining cyber hygiene to promote business continuity. Each business sector should also invest in organizing the cyber compliance office to improve cyber hygiene.
- The government should provide an opportunity for training and awareness sessions for everyone, including businesses, to promote good cyber hygiene.

6. Conclusion

In conclusion, the paper described cyber hygiene, reasons to maintain good cyber hygiene, and best practices to promote cyber hygiene. The article explored how business sectors apply the best ways to promote healthy surfing.

Our work reported the perceptions and best practices used to improve the device, network, and information hygiene. Regarding device hygiene, the paper looked at the best practices used to protect against unauthorized access, malware attacks, and regular updates for both the hardware and software. Findings revealed that the sectors have different understanding and implementation of the best practices to maintain device hygiene.

The paper also reviewed the best practices used to maintain the network. For network hygiene, the study looked at the configurations, the firewall, and the gateway. Findings showed that various sectors are aware of the importance of configuration management, the firewall, and the default gateway even though business sectors sometimes use the firewall and the gateway.

Furthermore, the study looked at the best practices to protect and secure information and data. Results revealed that most business sectors use cyberspace even though they are not protected

 | DOI: 10.20533/jitst.2046.3723.2021.0086

against the single point of failure, data breach, or loss of information. It is evident that some industries do not run any types of backup. In contrast, others perform their backups, and some have their dedicated person to regularly back up the information. A majority of the sectors do not use configuration management to its full potential to improve cyber defense.

Covid19 pandemic has increased the dependency on cyberspace, which quantified the cyber attackers. To protect against different cyber-attacks, every institution should follow the available and recommended guidelines to improve their cyber hygiene. The appropriate best practices suggested by European and cyber essentials assess threats and risks associated with information, hardware, software, transmission media, configurations, email, malware, end-users, email, and other aspects should be used.

7. References

[1] Barnett, J. (2020) 'DOD still needs to work on its cyber hygiene, watchdog finds, Fedscoop'; ttps://www.fedscoop.com/dod-cyber-hygiene-gao-report/ (Access Date: 1 Jan 2020)

[2] Cyber Essentials. 'Cyber essentials scheme - an overview,' https://www.gov.uk/government/Publications/cyber-essentials-scheme-overview, (Access Date: 19 June 2020)

[3] 'European Union Agency for Network and Information Security (ENISA)'. Review of Cyber Hygiene Practices, 2016.

[4] Farwell, J.P., and Rohozinski, R., 2012. The new reality of cyberwar. Survival, 54(4), pp.107-120.

[5] Furnell, S., and Clarke, N. (2012) 'Power to the people? The evolving recognition of human aspects of Security'. Computers and Security, 31(8), pp.983-988.

[6] Hadjizennonos, D. (Online) 'How to have strong cyber hygiene', https://www.bizcommunity.com/article/196/661/204326.html, (Access Date: 12 May 2020).

[7] Henshel, D., Cains, M.G., Hoffman, B., Kelley, T., (2015)' Trust as a human factor in holistic cybersecurity risk assessment', Procedia Manufact, 3, 1117–1124. DOI: 10. 1016/j.promfg.2015.07.186 .

[8] Jansson, K., and von Solms, R., (2013) 'Phishing for phishing awareness'. Behavior and information technology, 32(6), pp.584-593.

[9] Lemieux, F. (2011), 'Investigating cybersecurity threats: Exploring national security and law enforcement perspectives'. 2011 Developing Cyber Security Synergy, p.63.

[10] Maennel, K., Mäses, S. and Maennel, O., (2018), 'Cyber Hygiene: The Big Picture'. In Nordic Conference on Secure IT Systems (pp. 291-305). Springer, Cham.

[11] Martin, R.A., (2014), 'Non-Malicious Taint: Bad Hygiene Is as Dangerous to the Mission as Malicious Intent'. Mitre Corp Bedford Ma Bedford United States.

[12] Mbelli, T.M. and Dwolatzky, B., 2016, June. 'Cyber security, a threat to cyber banking in South Africa: An approach to network and application security'. In 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud) (pp. 1-6). IEEE.

[13] Mehravari, N., (2013), 'Resilience management through the use of CERT-RMM and associated success stories'. IEEE, 'International Conference on Technologies for Homeland Security (HST)', (pp. 119-125). IEEE.

[14] Miedema, T.E., (2018), 'Engaging consumers in cybersecurity'. Journal of Internet Law, 21(8), pp.3-15.

[15] Ncubukezi, T., Mwansa, L., Rocaries, F. (2020), 'A review of the current cyber hygiene in small and medium-sized businesses,' ICITST, 15, pp. 283–288.

[16] Neigel, A.R., Claypoole, V.L., Waldfogle, G.E., Acharya, S., and Hancock, G.M., (2020), 'Holistic cyber hygiene education: Accounting for human factors.' Computers and Security, 92, p.101731.

[17] NIST Special Publication 800-181, "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework." National Institute of Standards and Technology (NIST), (2017, https://doi.org/10.6028/NIST.SP.800-181.

[18] Panda, S., Panaousis, E., Loukas, G. and Laoudias, C., (2020), 'Optimizing Investments in Cyber Hygiene for Protecting Healthcare Users.' In From Lambda Calculus to Cybersecurity Through Program Analysis (pp. 268-291). Springer, Cham.

[19] Parkin, S., Fielder, A., and Ashby, A. (2016), 'Pragmatic Security: Modelling I.T. Security Management Responsibilities for SME Archetypes'. Proceedings of the ACM International Workshop on Managing Insider Security Threats, 2016.

[20] Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., and Zwaans, T., (2017), 'The human aspects of information security questionnaire (HAIS-Q): two further validation studies.' Computers and Security, 66, pp.40-51.

[21] Ponsard, C., Grandclaudon, J. and Dallons, G., (2018), 'Towards a Cyber Security Label for SMEs: A European Perspective.' In ICISSP (pp. 426-431).

[22] Seol, M.W., (2020). 'Managing Information as Records Asset: Public Records Policies in the Digital Transformation Era'. The Korean Journal of Archival Studies, (63), pp.5-36.

[23] Shackelford, S.J., (2016), 'Business and cyber peace: We need you!' Business Horizons, 59(5), pp.539-548.

 | DOI: 10.20533/jitst.2046.3723.2021.0086

[24] Singh, D., Mohanty, N.P., Swagatika, S., and Kumar, S., (2020), 'Cyber-hygiene: The key Concept for Cyber Security in Cyberspace.' Test Engineering and Management, pp. 8145 – 8152.

[25] Souppaya, M., Stine, K., Simos, M., Sweeney, S., and Scarfone, K., (2018), 'Critical cybersecurity hygiene: patching the enterprise.' National Institute of Standards and Technology.

[26] Still, J. (2019) 'Clean up your act- cyber hygiene best practices'. https://www.odu.edu/content/dam/odu/offices/mun/docs/ff-jeremiah-still-cyber-hygiene-2019.pdf?fbclid=IwAR0T0mH895hK_UofY2uk7Re4KNdCqvqSkQbhcUuRvtjDjen0YvVGvn8bbVo, (Access Date: 3 January 2021).

[27] Such, J.M., Ciholas, P., Rashid, A., Vidler, J. and Seabrook, T., 2019. Basic Cyber Hygiene: Does It Work? Computer, 52(4), pp.21-31.

[28] Trevors, M. (Online). 'Mapping Cyber Hygiene to the NIST Cybersecurity Framework, 2019', https://insights.sei.cmu.edu/insider-threat/2019/10/mapping-cyber-hygiene-to-the-nist-cybersecurity-framework.html, [Access date: 25 May 2020].

[29] Trevors, M. and Wallen, C.M., (2017), 'Cyber hygiene: A baseline set of practices. Carnegie-Mellon University', Software Engineering Institute Pittsburgh United States.

[30] Vishwanath, A., (2019), 'Stop saying "Cyber Hygiene is like personal hygiene,' White Paper, December 2019.

[31] Vishwanath, A., Neo, L.S., Goh, P., Lee, S., Khader, M., Ong, G., and Chin, J., (2020), 'Cyber hygiene: The concept, its measure, and its initial tests'. Decision Support Systems, 128, p.113160.

[32] Vishwanath, A., Neo, L.S., P. Goh, (2019), 'Cyber hygiene: The concept, its measure, and its initial tests, Decision Support Systems' (2019), https://doi.org/10.1016/j.dss.2019.113160.

8. Acknowledgements

We would like to thank (NRF) for their financial support on this work and the reviewers for their feedback.

 | DOI: 10.20533/jitst.2046.3723.2021.0086