Baltic J. Modern Computing, Vol. 11 (2023), No. 3, 450-474
https://doi.org/10.22364/bjmc.2023.11.3.07

Information Security Awareness of Librarians in the Baltic countries: A Comparative Analysis

Kate-Riin KONT

Estonian Academy of Security Sciences, Institute of Internal Affairs

kate-riin.kont@sisekaitse.ee

ORCID 0000-0002-9184-2363

Abstract. The aim of this study was to analyse the information security awareness of librarians in the three Baltic countries – Estonia, Latvia and Lithuania – in seven focus areas, which were password management, use of email, use of the Internet, use of social media, use of devices, handling of information and incident prevention and handling. The study was conducted among librarians in Estonia, Latvia and Lithuania. A total of 1,217 librarians from the public, special, school and research libraries of the three Baltic countries responded to the survey. Pearson correlation, average scores and descriptive statistics were used to achieve the research objective. The results revealed that Estonian librarians are more cyber-aware than their Latvian and Lithuanian colleagues, but everyone has their weaknesses. The chosen methodology is well suited for assessing the cyber awareness of not only library employees but also employees of all memory institutions (archives, museums) and identifying training needs.

Keywords: libraries, informal education, cybersecurity, cyber skills, cyber literacy, cyber hygiene, information awareness, human factor, KAB-model, HAIS-Q questionnaire

1. Introduction

Cybersecurity has become one of the highest priorities for businesses and governments. Enhancing and strengthening strategic leadership is key to ensuring that the cybersecurity vision is achieved. There are several different definitions for “information security” and “cyber security” and the terms are often used as synonyms, even though they are not, according to von von Solms and van Niekerk (2013). Let's start with “security”. Its definition gives good guidelines for the examination of cyber security and its definition of professional competence. Security can be divided into four areas. Security is a feeling of safety, knowledge that the chances of possible threats and risks being affected are small. Security is also about recognizing the facts and understanding the situation. Security also includes tolerance of uncertainty and harmful events, resilience. As the last area, security includes the models that make safety concrete and the values on which to rely security is being built. Based on these areas, it is easier to start defining information and cybersecurity (Hakkala et al., 2018, 175). According to

Paulsen and Byers (2019), authors of NIST Glossary, "information security"[1] is defined as

- *The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability*,

while "cybersecurity"[2] has defined by the aforementioned institute with numerous of definitions as

- *Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation*;
- *The process of protecting information by preventing, detecting, and responding to attacks*;
- *The prevention of damage to, unauthorized use of, exploitation of, and—if needed—the restoration of electronic information and communications systems, and the information they contain, in order to strengthen the confidentiality, integrity and availability of these systems* and
- *Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.*

There is also term "cyber security"[3]

- "The ability to protect or defend the use of cyberspace from cyber attacks".

"Computer security" is replaced by the term "cybersecurity"

- *Measures and controls that ensure confidentiality, integrity, and availability of the information processed and stored by a computer. Rationale: Term has been replaced by the term "cybersecurity.*

We can only think abstractly about securing information regardless of its form, technical protection of devices that store or transfer information, planning the company's business processes, mathematical encryption, or everything in between. Cybersecurity can be defined to cover all these areas from protecting the abstract representation of information to the company's business processes, and to protect tangible and intangible resources and interests from risks caused by threats using information and communication technology (Hakkala et al., 2018, 175).

Strategic management of cybersecurity requires identifying and setting goals based on the protection of the digital operating environment. In addition, it requires the coordination of activities and preparedness and the management of large-scale disruptions. To ensure cybersecurity, society must be able to involve various parties and coordinate resources and activities as efficiently as possible. Cyber capability must be developed throughout society, which requires strategic coordination, leadership and executive capability (Lehto and Limnéll, 2020, 139). Recently, more attention has been paid to the role of individual behaviour in mitigating cyber threats. Understanding of how individuals differ in their awareness, knowledge, and cybersecurity behaviours

[1] Glossary: information security, https://csrc.nist.gov/glossary/term/information_security
[2] Glossary: Cybersecurity, https://csrc.nist.gov/glossary/term/cybersecurity
[3] Glossary: Cyber security https://csrc.nist.gov/glossary/term/cyber_security

when exposed to multiple cyber threats is still quite limited (Zwilling et al., 2020). Although they do not want to admit it, the biggest threat to an organisation's privacy and security is its own employees. Employee security awareness is a key link in an organisation's security chain because even the best-protected company is vulnerable without a security culture. The term "safety culture" has been given various definitions. The most common OECD definition is that it "exists when each participant in the information society is aware of relevant security risks and preventive measures based on their role, takes responsibility and takes steps to improve the security of their information systems and networks."[4].

Cooperation between the Baltic states is active in many areas. In terms of cybersecurity, the Baltic states have done a successful job in combating cyber-attacks. According to the 2020 Global Cyber Security Index of the International Telecommunication Union, out of 194 countries, Estonia ranks third after the USA and the UK, Lithuania is the sixth country in terms of cyber protection, and Latvia is fifteenth at the end of the best list[5]. This ranking is based on five pillars: legal, technical, organisational, capacity building and cooperation in cybersecurity measures. Although the majority of cyber threats can be eliminated through the implementation of technical solutions, recently the abuse of technical loopholes has been replaced by the abuse of private data of individuals. Cybersecurity has the biggest mismatch between the level of threat and the level of preparation (Horchakova, 2022). Social engineering, one of the most common cyber threats, has targeted individuals who are the weakest link in security. Ensuring information security is very difficult, and its weakest link is people with little digital literacy, who are exposed to direct or indirect threats, who have a lack of awareness or certain psychological weaknesses that cybercriminals rely on. Security is not a product, but a process. Also, security is not a technological problem, but a human and management problem (ISE, 2019).

This article is structured as follows: the theoretical part provides an overview of the strategic documents and activities of Estonia, Latvia and Lithuania, which should contribute to the achievement of more effective digital and cyber literacy in society, as well as the efforts and important role of libraries as strategic cooperation partners of the state in the development of cyber education and digital literacy of the population. The following is an overview of the methodology used in the study. The Pearson correlation, mean of each focus area and descriptive statistics approach were used to present the research results.

2. Activities and strategies of the Baltic states in enhancing the cyber protection of the state and the population

Each Baltic country deals with its own field. For example, for Latvia it is strategic communication, for Estonia it is cyber defence and for Lithuania it is energy security. The NATO Cooperative Cyber Defence Centre of Excellence[6] in Tallinn is an international centre, think tank and training institution accredited by NATO. Established in 2008, the centre has grown into an important source of knowledge in the field of cyber defence for both NATO and its member states. The security and defence sector of the

[4] https://iccwbo.org/news-publications/news/securing-your-business-made-easier-with-new-icc-guide/
[5] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
[6] https://ccdcoe.org/

Baltic States has established partnerships with the private and academic sectors, all of which must cooperate with each other to maintain situational and technological awareness.

The Information System Authority (ISA)[7], operating in Estonia, in addition to registering and handling cyber incidents on Estonian computer networks, also supervises information systems used to provide vital services, as well as ensuring security through awareness raising, i.e. organising training for information security managers and regular users of institutions.

The work of the Latvian Safer Internet Centre (SIC)[8] established in Latvia is coordinated by the Latvian Internet Association together with the State Inspectorate for the Protection of Children's Rights and the Latvian Municipal Training Centre. The Latvian SIC promotes safer and better use of Internet and mobile technology among children and young people. It develops informative and educational activities, organises awareness-raising activities and ensures the operation of the information and hotline. Every year, the Latvian SIC organises a campaign promoting Safer Internet Day (SID). As part of the campaign, schools, youth centres and libraries are invited to organise various events on this day and throughout the month of February. The Latvian Awareness Centre informs and educates children, teenagers, teachers and parents about the safety of Internet content and possible dangers on the Internet (hate speech, racism, child pornography and paedophilia, emotional harassment on the Internet, identity theft and data abuse, etc.). The main activities implemented and coordinated by the centre are the celebration of the SID in Latvia, the development of educational materials on Internet security for all target groups – children, adolescents, parents, teachers and social workers, the organisation of various seminars, trainings and other activities, the organisation of social campaigns on current topics, the training of teachers, librarians, involvement of kindergartens and universities in Internet security activities, development of closer cooperation with mobile operators and Internet service providers.

All three countries have also developed their own cybersecurity strategy, which is linked to the strategies of other fields. In particular, the digital strategies of the three Baltic countries should be highlighted, which aim to create a basis for lifelong learning of digital and cyber literacy. In addition, the need to increase the awareness of both residents and organisations about the dangers of cybercrime and the ways to avoid them is emphasised, while the State Digitisation Development Programme 2021–2030 of Lithuania also emphasises the development of digital literacy of people with disabilities (SDDP, 2021). In this way, the priority activities established in the cybersecurity strategy are amplified in the development plans of various fields and the safety of cyber space is increased.

Estonia's new eternal society development plan Estonian Digital Agenda until 2030 highlights the set goals and planned directions of action in three areas: 1) developing a digital state, i.e. the use of digital solutions, 2) developing electronic communication, i.e. connectivity, and 3) developing national cybersecurity. The sub-goal of cybersecurity contributes directly to the realisation of the vision of the digital society in 2030 because the goal is to ensure the protection of the digital country, economy and, more broadly, the digital way of life in the public sector. The development plan states that the need to deal with broader digital literacy of the population will continue. There is less and less need to "bring" people to the Internet. Instead, it must be ensured that they have up-to-

[7] https://www.ria.ee/en
[8] https://www.betterinternetforkids.eu/sic/latvia

date skills to deal with digital solutions usefully and safely. By 2030, all Estonian adults should be regular Internet users. This gives an opportunity to ensure their sufficient capacity, including the corresponding basic level of awareness, so that they can use the services of the digital state better and better (EDA, 2021).

Latvia's Digital Transformation Guidelines for 2021–2027 represents a comprehensive strategy for Latvia's digital transformation and includes, among others, ICT education and digital skills, Internet access, modern and efficient public administration, e-services and digital content for society. The Latvian Cabinet of Ministers adopted the policy document in July 2021. The main objectives of the digital skills pillar are 1) basic digital skills for all citizens, 2) digital skills of citizens, and public administration employees to use the latest technologies and digital services, 3) digital skills to create and offer innovative digital services and products, 4) digital skills in the education system, and 5) digital skills in the healthcare system. The goal is that 70% of citizens have at least basic digital knowledge, 45% of citizens' digital skills exceed the level of basic knowledge, and at least 3% of employment is made up of ICT specialists (LDTG, 2021).

The purpose of the Lithuanian State Digitisation Development Programme 2021–2030 is to promote national digitisation in order to increase the opportunities of the public sector, companies and academia for the efficient and safe development and use of innovative products and services. Another aim is to strengthen the digital competence of the population by creating an understanding of the development and importance of emerging technologies. The main goal of developing digital skills is to provide support to vulnerable groups: 1) to enable disabled people to live independently and participate fully in all areas of life, 2) to create an efficient and functioning lifelong learning system for adults to match skills to the needs of the labour market. The goal of the programme is to increase the level of citizens who regularly use the Internet to 90%, and to 60% for citizens with disabilities who use public services and are satisfied with them. One of the goals of the changes is to create an effective lifelong learning system that adapts new technologies and ensures the acquisition and development of knowledge and skills necessary for an active society (SDDP, 2021).

The National Cyber Security Centre under the Ministry of National Defence (NCSC)[9] is the main cybersecurity agency in Lithuania, which is responsible for the unified management of cyber incidents, monitoring and control of compliance with cybersecurity requirements. NCSC's mission is to be a centre of expertise in cybersecurity and a strong cybersecurity incident prevention system in the country. According to the regulations approved by the NCSC, the main operational goals of the institution are to implement the national cybersecurity policy, to perform the tasks of the cybersecurity service, to perform the tasks of the national communications protection service, to carry out information dissemination, research and analysis in the field of cybersecurity. Since 2018, NCSC provides assistance to the state, companies and residents, and makes decisions within its competence together with state institutions and organisations and other economic entities.

The cybersecurity strategies of all three Baltic states emphasise that it is impossible to avoid cyber incidents, even if all available cybersecurity measures are implemented. For this reason, representatives of the public and private sectors must improve the cybersecurity culture of their employees. According to an IBM report published in 2017, the number of cyber incidents caused by employee negligence has increased (in 2017, it

[9] https://www.nksc.lt/en/

was more than 20%, up from 15% in 2016). More than 30% of these cyber incidents happened because employees opened malicious links or documents emailed to them. Routine and regularly updated training for private and public sector employees would increase both employee due diligence and the general cybersecurity culture.

3. Libraries as cooperation partners of the state in raising cyber awareness

Online security has always been one of the key topics in library user training, and it became especially relevant due to the Covid pandemic. Denisenko (2020) emphasises in the publication *Lithuania in the Global Context: National Security and Defence Policy Dilemmas* that "In terms of important subspecies of information security, cybersecurity is understood in terms of the technological, state critical information infrastructure and its protection. Psychological security is understood as the need to protect one's information space (public sphere) from harmful effects, i.e. the flow of propaganda narratives and fake news", while also recognising that when dealing with "information wars", one must talk about cyber war as much as psychological war. It is assumed that different countries prefer different types of "information warfare" – so the US focuses more on the cyber dimension of information warfare, while Russia focuses on psychological warfare. However, it seems that nowadays these differences are gradually disappearing, and in reality, different types of information wars can complement each other (Denisenko, 2020, 235). For libraries, user education has now become as much a part of daily work as lending books. Technologies evolve and risks change. Internet users need to learn every day. The rapid development of digital technologies requires new approaches to education. Formal education systems are not ready to provide citizens with the necessary digital skills to cope with these changes. Informal, non-formal and lifelong education are becoming a more important source of knowledge in this field, and libraries and librarians are expected to play an important role in promoting digital and cyber literacy (Spurava et al., 2021). Libraries thus play an important role in an aspect that has not been discussed in the scientific literature so far – namely, in promoting national security and preventing cybercrime. Above all, these activities must ensure that all citizens have access to information and effective participation in democratic processes. For this, however, the librarians themselves must be ready to acquire new cybersecurity knowledge and continue to raise their cyber awareness. Technological protection can be maximally strong, but information security is only as strong as its weakest link. Therefore, managing the human side of information security is as important as the technical side, it is equally important to continuously strengthen the security awareness culture of organisations and transform this culture into actual security-aware behaviour (Abawajy, 2014). The main reason for increasing security awareness is the need to manage the change in employees' behaviour and attitude towards information security. Information security awareness programmes are designed to create security-oriented cultures throughout the organisation so that people work more securely and protect their organisation's assets. Information security awareness is the establishment, promotion and maintenance of good security habits. The main goal of information security awareness is to change attitudes to bring about a general change in organisational culture. The culture change is the realisation that information security is critical because a security breach can have negative consequences for anyone.

Information security awareness also aims to increase users' understanding of how to follow responsible computer usage practices and why this is necessary. Increased employee awareness should reduce the likelihood of accidental violations and increase the likelihood that suspicious activity will be recognised and reported.

The libraries of Estonia, Latvia and Lithuania are important cooperation partners for their countries in bringing cyber awareness closer to the population. Promoting digital literacy, including the basics of online safety and privacy, has long been an important part of many library services.

For example, in Latvia, every year in February, libraries celebrate SID and organise events dedicated to this day for a large number of stakeholders – from parents and teachers to media professionals and policy makers – who come together to support awareness raising and skills development to ensure the safety and well-being of young people online. Individual consultations and training, and group training are organised, visitors are given various media literacy and Internet safety-related tasks, games and competitions, quizzes, drawing competitions for the youngest, knowledge tests, lectures, seminars, information leaflets, posters are distributed, young people are taught to develop and implement various projects, as well as how to do awareness campaigns, live broadcasts, library classes and shared film viewings, in addition to organising creative workshops and storytelling events. The target group is wide – children, young people, adults and seniors. By working with their users on a daily basis, librarians know the target audience and know how to approach which audience to achieve the best possible result. An adult learner finds motivation and interest in learning useful and feels happy about newly acquired skills or knowledge that they can immediately apply in everyday life. Children and young people are motivated by the opportunity to compete with each other and maybe get a prize, something tangible or tasty. Campaigns that involve a larger number of people simplify the daily work of library staff because less time has to be spent on daily digital skills support and training for users. Information about exciting activities spreads by word of mouth and is therefore the best marketing for library services (Niedra, 2021).

The Lithuanian Librarians' Association monitors and coordinates the initiatives, creativity and ideas of libraries on how to make the use of the Internet safer, how to spread this knowledge to communities and how to involve groups experiencing cultural, informational or social exclusion in these activities. Safer Internet Day has been celebrated in Lithuania since 2006. The celebration of the day has become a week-long event that aims to highlight current digital issues and promote safer use of the Internet and digital technology, especially for children and young people. There are some great examples of unique library activities for Safer Internet Week. One of them is at Kaunas County Library, where attention has been paid to hearing-impaired people and 12 video lectures with sign language interpretation have been prepared for them, the purpose of which is to help critically evaluate and analyse information shared through traditional and modern media, be safer on the Internet, and develop their own skills to create new information and media content. The videos with sign language translations deal with topical topics for everyone: "Modern Internet and its dark side", "Consumer rights and their protection in electronic commerce. What is useful to know?", "Safe e-banking", "Fake news and its distribution", "Report hate speech" and many others (Steponaitiene, 2021).

The Estonian Librarians Association does not coordinate or celebrate Safe Internet Day on the same scale as its southern neighbours, but individual libraries organise various events within the framework of this day. According to the Information System

Authority (RIA), "Since 2007, Estonia has been actively engaged in ensuring cybersecurity at the national level in order to ensure the safety and availability of state institutions and vital services in all situations" (Vaks, 2013). RIA's Cyber Security Service monitors and handles incidents, analyses trends in cyberspace, and writes summaries and threat assessments; cybersecurity prevention activities are carried out, the population is informed about the risks lurking in cyberspace, etc. Prevention activities are carried out systematically, monthly, quarterly and annual summaries are issued, and trainings are organised both one-on-one and through a cyber hygiene test where anyone can check their knowledge. People's cyber hygiene improves year by year, but the application of good practices starts to decrease from the age of 45. There are several campaigns for companies, e-voting (vote safely!), seniors and non-Estonians. The Estonian Librarians Association is a cooperation partner in cybersecurity campaigns organised by the Information System Authority. In the autumn and winter of 2019, RIA organised the awareness campaign "Be IT vigilant!", which continued in 2020. Cooperation with Tallinn Central Library has been very successful in order to bring good practices in cybersecurity to people. In 2020, three online training sessions were held for 44 library employees, the topics of which were good practices, secure passwords, changing settings in different browsers, and examples of the most common frauds. In addition, an information line was opened, where employees of the foreign language department of the Tallinn Central Library gave advice. RIA will continue to see libraries as an irreplaceable partner and their invaluable role in reaching the target audience.

4. Methodology and sample characteristics

The complexity of human nature in relation to information security has long been the subject of research in various branches of science. Their goal has been to understand and analyse how the employee's feelings, beliefs, behaviour, attitude and actions can directly or indirectly, intentionally or unintentionally affect and possibly threaten the organisation's information security. Understanding the root of the problem helps to develop effective security policies and rules and training programmes that could contribute to the development of a security culture (Georgiadou et al., 2022). The knowledge-attitude-behaviour (KAB) model was first proposed by Kruger and Kearney (2006) to measure information security awareness. It is based on the three interrelated components of the social psychological model, namely affect, behaviour and cognition (MacKinnon and Hoey, 2021), which correspond to attitude, behaviour and knowledge. The KAB model has been widely used to explain cybersecurity awareness and behaviour (Parsons et al., 2014; Zwilling et al., 2020). As previous research showed that knowledge alone is not sufficient to produce behavioural change, attitude was added to the KAB model as a necessary mediator to alleviate cognitive dissonance between knowledge and action. Evidence that individuals who possess the necessary information security knowledge and skills may not effectively apply them in their daily work routines has led researchers to focus on bridging the gap between awareness and actual behaviour (Siponen et al., 2007; Workman et al., 2008). The main claim of the KAB model is that knowledge can change behaviour, attitude is often a necessary mediator between knowledge and behaviour. Increased knowledge improves attitudes, resulting in better information security behaviours (Parsons et al., 2014). Thus, knowledge is what (declarative), how (procedural), when and why (conditional) (Schrader and Lawless, 2004).

Parsons et al. (2014) claim that an important foundation for the KAB model to be used correctly is that the variables involved must be clearly specified and that they must be connected to the other variables associated with behavior change. Within research concerning information security awareness, the KAB model is said to constitute a stable theoretical foundation with high validity as a high correlation between knowledge, attitude and behaviour have been proven (Parsons et al., 2014; Parsons et al., 2017). In order for the KAB model to be evaluated correctly, it is required that the variables knowledge, attitude and behaviour are defined with the greatest possible clarity, while these variables are related to each other (Parsons et al., 2014; Parsons et al., 2017). To measure the relationship between the three variables, Parsons et al. conceptualised (2014) the Human Aspects of Information Security Questionnaire (HAIS-Q) based on the KAB model (Table 1). A recurring problem in research using the KAB model has been that the knowledge variable has not been sufficiently specified (Baranowski et al., 2003). Within HAIS-Q, knowledge is defined as knowledge of information security behaviour with reference to "best practice", which is often found in information security standards (Parsons et al., 2017). Parsons et al. (2014) defines knowledge as "knowledge of policy and procedures". The HAIS-Q is based on the two dependent variables attitude and behaviour, and the independent variable knowledge. Prior to the HAIS-Q, survey questionnaires focused narrowly on Information Security Awareness (ISA), such as the use of passwords and smartphone applications.

All seven focus areas used during the current study are derived from Parsons et al. (2017) validation study of the HAIS-Q. In that study, 63 statements linked to seven different focus areas were used, divided into three sub-areas with three statements per sub-area where each statement was linked to either knowledge, attitude or behaviour. That way the HAIS-Q is more comprehensive in capturing the most typical Internet behaviours. The statements are relatively neutral in that they do not highlight intentional positive behaviour or intentional risk behaviour (Parsons et al., 2014). As this study examines librarians, a revision of the questionnaire statements was necessary considering that librarians in general have no specific information security policy to relate to. In order not to completely depart from the previous studies carried out by Parsons et al. (2014) and Parsons et al. (2017), it was considered relevant to choose the statements from Parsons' studies that were considered most appropriate as well as statements based on existing literature, and IT-expert opinions of Tallinn Central Library. This resulted in the selection of statements shown in Table 1.

Table 1. HAIS-Q focus areas and subareas with statements for librarians (table adapted from Ranas et al. 2020, 4)

Focus area	**Subareas**		
Password management	**Knowing**	**Attitude**	**Behaviour**
Using the same password	I use the same passwords on my work devices that I use on my personal devices.	It is safe to use the same passwords for private and work accounts.	I use a different password for my private and work accounts.

Sharing passwords	I leave passwords where I can see them because it is convenient to work and it is impossible to remember everything.	I am aware that leaking passwords can lead to great losses for both the organisation and myself.	I remember passwords or use a password manager whenever possible. If I discover that passwords have been leaked, I will immediately notify the IT department and change the passwords.
Using a strong password	A strong password consists of a combination of letters, numbers and symbols.	It is safe to have a work password with just letters if it contains at least 10 characters.	I use at least 10 characters in my passwords, which are a combination of letters, numbers and symbols.
E-mail use	**Knowing**	**Attitude**	**Behaviour**
Clicking on links in emails sent from known senders	It is perfectly safe to open a link inside an email received from a colleague or a person I know.	I do not believe that emails sent by my colleagues or people I know could contain harmful links.	I open files attached to emails from colleagues or people I know without hesitation.
Clicking on links in emails from unknown senders	I know what harm the malware can do, and I try to prevent it from getting into the work device (clicking on links, etc.).	I find it unlikely that an email sent to my work device has malware attached to it.	If an email from an unknown sender looks interesting, I click on the link it contains without hesitation.
Handling emails from unknown senders	I use a specially secured environment to send problematic incoming emails to the IT department for analysis, if possible without opening the suspicious email received.	It is not necessary to inform the IT department about the received suspicious email.	I forward the received suspicious email to the email address of the IT department for their analysis, without opening the received suspicious email if possible.
Internet use	**Knowledge**	**Attitude**	**Behaviour**
Software use	Using pirated software on work equipment or for personal use is illegal.	It is legal to use pirated software on my work device if my company is not willing to pay for the software.	On my work devices I use software from unofficial sources.
Accessing dubious websites	Internet access on my work device is a state or local government resource and should only be used for business purposes.	There are certain websites I should not visit from my work device.	I have the right to visit any website from my work computer.
Activities on the Internet	An employee cannot be punished for visiting web pages that are not related to work from his/her work device and during working hours.	My employer has the right to restrict the use of social networking sites during working hours.	I spend part of my working time on social networks (doing activities not related to work).
Social media use	**Knowing**	**Attitude**	**Behaviour**
Social media privacy settings	People who post more on social media are more vulnerable to privacy attacks.	It is a good idea to review the privacy settings of your personal accounts from time to time.	I do not manage my social media privacy settings.

Considering consequences	Social networks can be used for malicious purposes.	I believe that social networking sites can be open and share everything that is happening in my life.	I click on links on social networks even if I am not sure they are safe enough to open.
Posting about work	The employer may terminate the contract if the employee has posted an inappropriate work-related message (e.g. shared offensive or confidential content) on a social networking website.	I have the right to share information related to my work on personal social networks (e.g. post information about newsletters or events).	I post on social media only when I have considered that there will be no negative consequences (for the employer or myself).
Use of devices	**Knowing**	**Attitude**	**Behaviour**
Physically securing devices	I log off the device, turn it off, put it into sleep mode, or lock the screen when I am done using the device.	Logging out of the work device or locking it to get away for a moment is not necessary, because I trust my colleagues and I am convinced that my work environment is sufficiently secure.	I always lock the screen when I step away from my work device for a moment.
Using a public Wi-Fi network for sending sensitive information	Using the Internet to work outside the office poses an additional security risk.	I find that security can be a valid reason for limiting telecommuting options.	When working remotely, I use a VPN to connect to my work environment instead of Wi-Fi.
Shoulder surfing	When working on sensitive documents or reading work-related emails, I have to make sure that my computer screen is not visible.	I think it is safe to handle work-related emails or sensitive documents on a public Wi-Fi network.	I send sensitive work files and read work-related emails using a public Wi-Fi network.
Information handling	**Knowing**	**Attitude**	**Behaviour**
Disposing of sensitive printouts	When destroying paper documents with sensitive content, special procedures should be used.	It does not really matter if there are special procedures (at my workplace) for destroying sensitive paper documents or not.	If paper documents containing sensitive information need to be disposed of, I will ensure that they are shredded or destroyed.
Inserting removable media	It is safe to insert a USB stick of unknown origin into a computer as long as the files on it are not opened (for example, simply viewing the list of files on the device).	I think it is safe to insert a USB stick into any computer.	I use USB devices without first checking if they are infected with malware or not.

Handling sensitive materials	I can safely leave paper documents containing sensitive information on my desk overnight.	Paper documents containing sensitive information should not be left on your desk overnight.	I leave paper documents containing sensitive information on my desk, even when I am not there.
Incident prevention and reporting	**Knowing**	**Attitude**	**Behaviour**
Awareness of the need for training	I consider it necessary to regularly (at least once a year) educate myself in the field of cyber hygiene so that I can recognise the most common social manipulation attacks.	I do not think it is necessary to refresh my cyber security knowledge, but the IT department takes care of the cyber security of work equipment.	In order to be able to recognise the most common social manipulation attacks, I regularly participate in cyber security training organised by my employer.
Reporting suspicious behaviour	It is none of my business if I witness my colleague or a library user flouting cybersecurity rules (e.g. downloading illegal software, or playing games on a computer during work hours).	Nothing bad can happen if I ignore the unethical activities of colleagues or library users on institutional devices.	I will immediately notify the IT department of any unethical behaviour by colleagues and/or library visitors that could lead to serious security incidents.
Reporting cyberincidents	Since my institution does not have a unified incident notification system, I report the security incidents that have occurred on my work device to the IT department.	I do not think I should report security incidents to IT because it is not my responsibility or concern.	I always inform the IT department about security incidents on my work device through the institution's incident notification system.
User education	I feel that the cybersecurity knowledge of library users could be better.	To educate users on cybersecurity topics is not the task of the library employees, there is specific training for that.	I consider it necessary to educate library users on cybersecurity topics.

The current survey took place in Estonia from 14.06.2022 to 10.09.2022, in Latvia from 07.10.2022 to 01.12.2022 and in Lithuania from 29.12.2022 to 06.02.2023. The survey questionnaire was distributed by the Estonian Librarians Association, National Library of Latvia, Lithuanian Librarians' Association and Lithuanian Research Library Consortium member lists. The questionnnaire was in the respondent's native language so those librarians whose work does not require intermediate or advanced English language skills could also answer. For this purpose, the Estonian questionnaire was translated into Latvian and Lithuanian and the representatives of the professional organisations of the respective countries were asked to test them. There were 388 respondents from Estonia, 352 from Latvia and 477 from Lithuania. One of the most reliable methods of measuring attitudes is a scale developed by Likert in 1932, which consists of statements, each of which is accompanied by a multi-point scale. When answering, the interviewees were

asked to express their opinion on a 4-point scale: “I completely agree”, “I agree”, “disagree”, “not at all” in the questions of knowledge and attitude, and “always”, “often”, “sometimes” or “never” in the questions of behaviour.” The answers obtained by this method are easy to quantify and analyse. Some researchers argue that it would be more efficient to number such scales so that the respondent can better understand the negative and positive response options. However, Adams et al. (2013) find that most questionnaires ask questions about which the respondent is rather neutral. The same authors recommend using odd-numbered answer options. This makes the analysis process more convenient. On the other hand, there are also opinions (e.g. Brown, 2006; Nunes, 2021) that recommend using an even-numbered scale. It is also called a forced scale because the exclusion of the neutral answer option forces the respondent to take a certain position, and so-called convenience answers are avoided, where one does not bother to delve into the question, but automatically chooses the neutral “don’t know” or “can’t answer”.

Estonians and Latvians have been slightly more diligent daily Internet users than Lithuanians: the average number of users in Estonia only exceeded the 70% limit in 2014, while this limit was exceeded in Latvia in 2017 as well. It can be assumed that due to the pandemic, the number of daily Internet users increased even more, and those people who had managed to avoid it until March 2020 were also forced to go online.

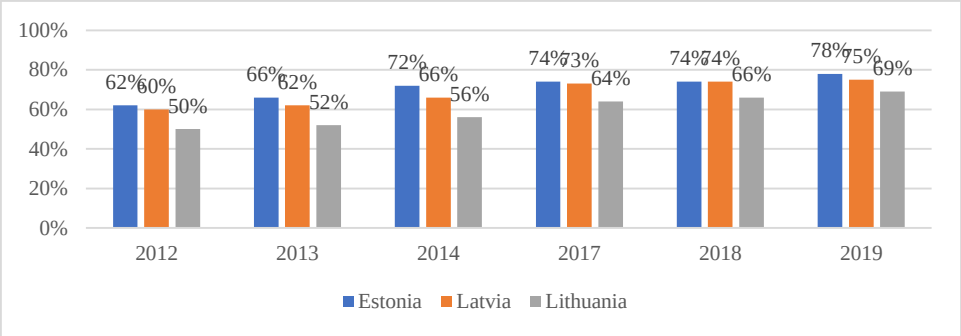

Figure 1. The overview of Estonian, Latvian and Lithuanian everyday Internet users according to the Eurobarometer statistics

The majority of respondents were women (Table 2), which perfectly characterises the gender inequality of library workers to the strong disadvantage of male workers.

Table 2. Demographic distribution of respondents by sex

	Estonia	Latvia	Lithuania
Male	5%	3%	7%
Female	95%	97%	93%

Most respondents from Estonia, Latvia and Lithuania were in the age group 51–60 (32 per cent, 33 per cent and 38 per cent respectively). We can see that more librarians answered in the age groups 21–30, 31–40 in Lithuania, and there were significantly more respondents from Lithuania in the age group 51–60. There seems to be an interesting tendency that in the age groups 41–50 and 61–70 there are significantly fewer library workers from Estonia, Latvia and Lithuania among the respondents, and there are no respondents from Lithuania in the age group 70+. We can probably draw conclusions here about the demographic situation of library workers in general, but it raises questions as to where 51–60-year-old workers suddenly come to libraries, when there are so many fewer of them in the previous and subsequent age groups.

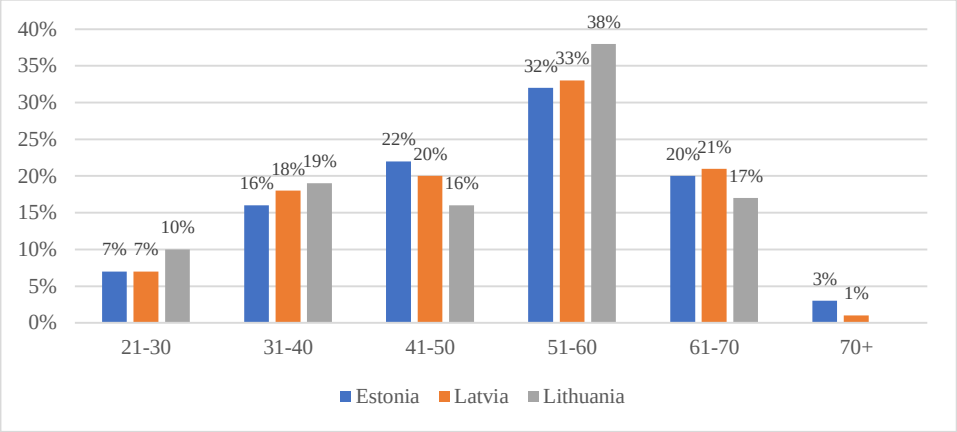

Figure 2. Demographic distribution of respondents by age

Most respondents were among those library employees with less than 5 years of experience in the library (26 per cent in Estonia, 22 per cent in Latvia and 28 per cent in Lithuania). Most of the respondents with 40+ working years work in Latvian libraries, as much as 9 per cent.

From Figure 4, we can see that 62 per cent of Estonian library employees have participated in cybersecurity trainings, Latvia and Lithuania still have room for improvement here. At the same time, the desire to participate in the training is very different – only 21% of Estonian library employees definitely want to participate in the training if possible, increasing to 27% in Latvia and as many as 29% in Lithuania. Certainly, such a percentage of responses shows that on the one hand, a large part of those who wish to do so have already been able to complete cyber training in Estonia, but on the other hand, library associations and employers in all Baltic countries should invest much more strongly in the training of their employees than before. Firstly, so that the staff can protect the library's resources and also the privacy of the users, secondly, in order to be a community centre, where the residents can come for cybersecurity training.

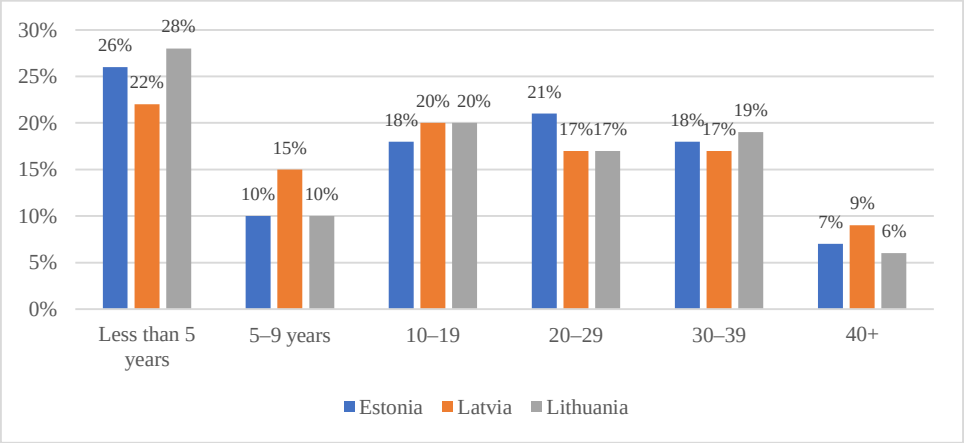

Figure 3. Distribution of respondents by years worked in the library

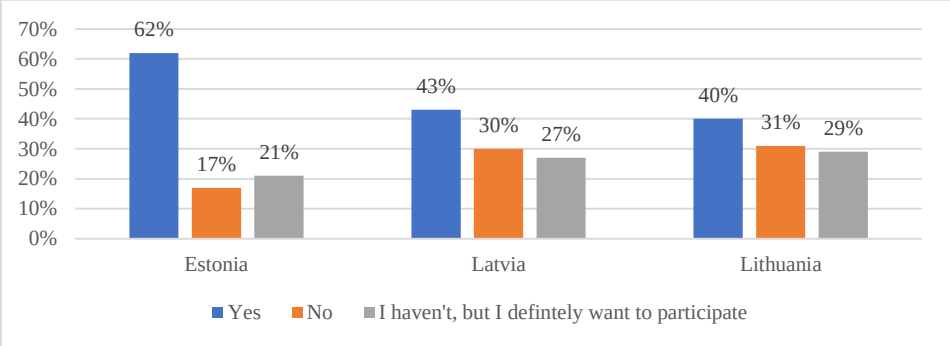

Figure 4. Distribution of library staff responses to the question:
"Have you completed cybersecurity training?"

The characterisation of the sample shows a cross-section of library workers in Estonia, Latvia and Lithuania. We can conclude that the average Baltic librarian is aged 51–60 and has less than 5 years of experience. According to an Oxford University Press study, 83% of librarians working in the US today are women. The only point at which male librarians were the majority was in the 1880s, when men just tipped the scales at 52% of the librarian workforce (Nuttall, 2021). Our survey shows an even greater preponderance – in the Baltic countries, more than 90 per cent of librarians are women.

5. Results

5.1. Correlation analysis of knowledge-attitude-behaviour components

We can confirm that there was a positive relationship between all variables in the knowledge-attitude-behaviour components in all Baltic countries, with correlations ranging from 0.382 to 0.683, indicating a strong relationship but not indicating multicollinearity (Table 3). For example in Magdalinou et al (20123) study Pearson correlations supported that practices of the staff were strongly and positively correlated with knowledge on the organization's policies (0.659) as well as with the attitude of staff towards the organization's policies (0.740). The attitude of staff towards the organization's policies is strongly and positively correlated with the knowledge on the organization's policies (0.692) (Magdalinou et al., 2023, 50). Table 3 shows that Pearson correlations of Estonian librarians are positively correlated with knowledge on the information security (0.498, p=0000<0,05), and the behaviour is positively scorrelated with attitude on the information security (0.491, p=0000<0,05). The behaviour of the employees is strongly and positively correlated with information security knowledge (0.654, p=0000<0,05). Latvian librarians' behavior has a stronger positive correlation with information security knowledge than Estonian and Lithuanian colleagues (0.505, p=0000<0,05), the correlation of the behavior with the attitude towards information security is also positive (0.484, p=0000<0.05) and the employees' attitude towards information security is once again more strongly positively correlated with knowledge than Estonian and Lithuanian colleagues (0.683, p=0000<0,05). The behavior (0.382, p=0000<0.05) and attitude (0.534, p=0000<0.05) of Lithuanian librarians have a weaker positive correlation with information security knowledge compared to Estonian and Latvian colleagues, and the staff's attitude towards information security is also more weakly positively correlated with knowledge (0.461 , p=0000<0.05) compared to counterparts in neighboring countries.

Although comparing with Magdalinou et al (2023) study the correlations were weaker, this provides additional reliability support for the HAIS-Q questionnaire.

Table 3. Pearson Correlation for Knowledge, Attitude and Behaviour

	ESTONIA			LATVIA			LITHUANIA		
	Knowledge	*Attitude*	*Behaviour*	*Knowledge*	*Attitude*	*Behaviour*	*Knowledge*	*Attitude*	*Behaviour*
Knowledge	1			1			1		
Attitude	0.654	1		0.683	1		0.534	1	
Behaviour	0.498	0.491	1	0.505	0,484	1	0,382	0,461	1

5.2. The average scores of the results

The average results in focus areas are shown in Figure 5 and Figure 6 where Figure 5 shows respectively results for knowledge, attitude and behaviour and Figure 6 shows results of the focus areas.

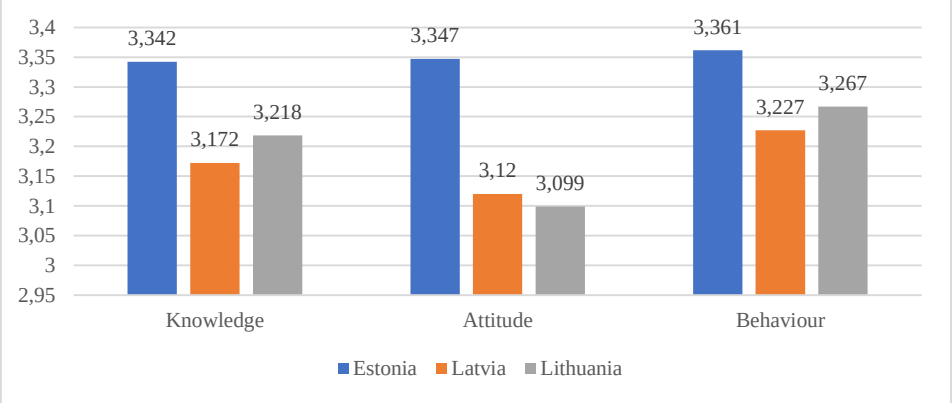

Figure 5. Average scores for knowledge-attitude-behaviour constructs

Figure 5 clearly shows that Estonian librarians' knowledge, attitude and behaviour is stronger than their Latvian and Lithuanian counterparts. In the case of Latvian and Lithuanian librarians, attitude is the weakest area. However, for example, the library staff's overall behaviour is stronger than knowledge and attitude.

For all librarians in Baltic countries, information handling and password management are the strongest focus areas. The weakest areas are use of devices and for Lithuanian librarians, Internet use, and in use of devices and incident prevention and reporting.

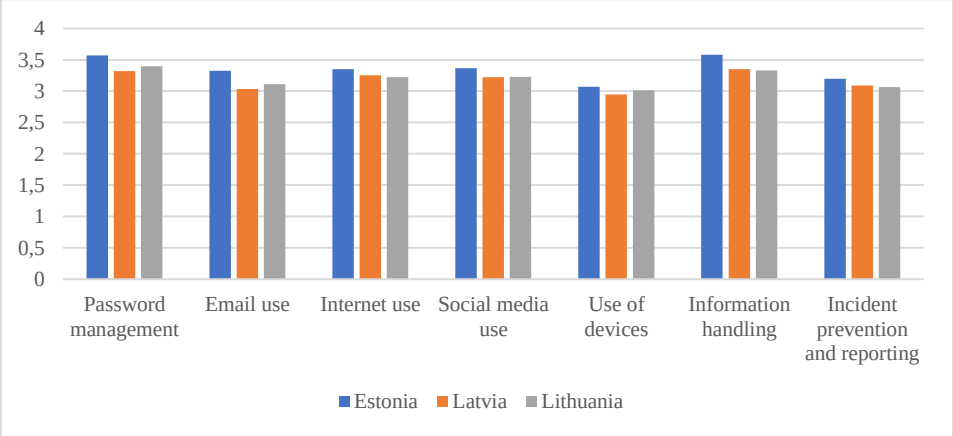

Figure 6. Average scores for focus areas

Incident prevention and handling, which received the second-lowest average score, is probably not a significant problem in small libraries either. However, employees should still be aware of possible dangerous situations and also know how to behave in such situation.

Employees feel that there is little knowledge in the cyber field, both for themselves and for teaching and guiding users. There are complaints about the absence of an IT department or, if there is one, about the lack of cooperation. At the same time, the responsibility for the cyber behaviour of the readers using the computers located in the library and the lack of tools and sufficient rights to control the activities of the users on the Internet are recognised:

We lack not only the knowledge, but also the tools to ensure cybersecurity.

We don't have an IT department for cybersecurity training, but we would attend if we could.

I would like more active cooperation and training from the IT service.

I don't think I know enough about cybersecurity. I've only recently started working at the library, so I'm hoping to learn the basics – something like how to check USB devices for malware before inserting them into the computer; how the password manager works, etc.

I believe the librarian is responsible for what users view and has the right to both reprimand and expel someone from the library.

It is necessary to continue training the library staff. This questionnaire is very necessary to draw conclusions about their knowledge and conduct training.

Library staff do not have tools to help control which websites library patrons visit. Anyone can come to the library and browse all kinds of propaganda portals of the enemy state, comment, and incite riots online.

5.3. Descriptive statistics of the results

Responses were arranged in columns in order of the main three constructs and focus areas. Each line with the respondents' answers was summarised. Based on these summed responses, descriptive statistics were calculated using the Microsoft Excel data analysis tool function. The results are presented in tables 4 and 5. Kurtosis, skewness and the mean have been examined in more detail.

Skewness is a measure of symmetry, or more precisely, the lack of symmetry. In a symmetric distribution, the median and mode coincide. If the mode is to the right of the axis of symmetry (median), it is negative asymmetry. If the maximum is to the left of the axis of symmetry, it is a positive or asymmetry. For a very high positive or negative skewness, the coefficient is below -1 or greater than 1 (Yeng et al., 2021, 474–475).

Table 4 identifies among Estonian, Latvian and Lithuanian librarians knowledge risk (-0.806, 0.036 and -0,902 accordingly) with a moderate skewness (between -1, -0.5 and 0.5, 1), attitude (-0.374, 0.382 and -0.101 accordingly) and behaviour (-0.424, -0.074 and -0.338 accordingly) had a fairly symmetrical skewness coefficient (between -0.5 and between 0.5). Table 5 reveales a moderate coefficient of skewness in password management among Estonian, Latvian and Lithuanian librarians (-0.700, -0.247 and 0.141 accordingly), Internet use (-0.722, -0.157 and -0.845 accordingly) and information handling (-0.755, -0.123 and -0.501 accordingly).

Table 4. Descriptive statistics of knowledge-attitude-behaviour components

	Knowledge Estonia	*Knowledge* Latvia	*Knowledge* Lithuania	*Attitude* Estonia	*Attitude* Latvia	*Attitude* Lithuania	*Behaviour* Estonia	*Behaviour* Latvia	*Behaviour* Lithuania
Mean	70.285	66.619	67,522	70.289	65.520	65.075	70.590	67.770	68.610
Median	71	66	68	71	64	65	71	68	69
Mode	75	62	72	74	62	61	68	68	65
Standard deviation	5.932	5.698	6,267	6,355	6.667	7.248	7.004	7.616	7.3427
Kurtosis	1.126	0.134	2,265	-0.796	-0.352	0.506	0.322	-0.720	-0.035
Skewness	-0.806	0.036	-0,902	-0.374	0.382	-0.101	-0.424	-0.074	-0.338
Range	39	36	45	29	35	51	39	36	41
Minimum	42	44	36	54	49	39	45	48	43
Maximum	81	80	81	83	84	90	84	84	84
Sum	27232	23450	32208	27272	23063	31041	27389	23855	32727
Count	388	352	477	388	352	477	388	352	477

From the point of view of compliance with the normal distribution, in addition to the skewness, the kurtosis or steepness coefficient is an important indicator. In statistics, kurtosis is used to describe the shape of a probability distribution. The kurtosis can be negative, equal to zero, or positive. If the kurtosis is 0, then it is equal to the normal distribution. If the kurtosis is positive, it simply means that fewer data values lie near the mean, and if the kurtosis is negative, it means that more data values lie near the mean. Table 3 shows that the kurtosis of knowledge among Estonian, Latvian and Lithuanian librarians (1.126, 0.134 and 2,265), attitude in the case of Estonia and Latvia is negative (-0.796 and -0.352) and in the case of Lithuania is positive (0.506). Behaviour among Estonian librarians is positive (0.322), and the kurtosis of behaviour of Latvian and Lithuanian librarians is negative (-0.720 and -0.035).

Table 5 revealed positive kurtosis for Internet use (0.459) and information handling (0.034) in Estonia, email use (0.097) and Internet use (0.041) in Latvia, and password management (2.727), Internet use (2.486), social media use (1.614), use of devices (0.191), information handling (0.789) and incident preventing and handling (2.537) in Lithuania.

Table 5. Descriptive statistics of components of focus areas

ESTONIA	*Password management*	*Email use*	*Internet use*	*Social media use*	*Use of devices*	*Information handling*	*Incidents preventing and handling*
Mean	**32.140**	**29.905**	**30.152**	**30.299**	**27.601**	**32.219**	**38.157**
Median	**33**	**30**	**30**	**30**	**28**	**33**	**38**

Mode	34	29	33	30	25	35	38
Standard Deviation	2.940	3.126	2.888	2.746	3.732	3.229	4.962
Kurtosis	-0.306	-0.546	0.459	-0.106	-0.485	0.034	-0.359
Skewness	-0.700	-0.068	-0.722	-0.433	-0.191	-0.755	-0.287
Range	12	14	16	14	19	16	26
Minimum	24	22	20	22	17	20	22
Maximum	36	36	36	36	36	36	48
Sum	12470	11603	11699	11756	10709	12501	14805
Count	388	388	388	388	388	388	388

LATVIA	*Password management*	*Email use*	*Internet use*	*Social media use*	*Use of devices*	*Information handling*	*Incidents preventing and handling*
Mean	29.889	27.275	29.278	29.017	26.497	30.142	27.810
Median	30	27	29	29	26	30	28
Mode	29	27	29	29	27	29	27
Kurtosis	-0.278	0.097	0.041	-0.055	-0.254	-0.463	-0.455
Skewness	-0.247	0.179	-0.157	-0.107	0.187	-0.123	0.062
Range	18	19	13	16	19	15	18
Minimum	18	17	22	20	17	21	18
Maximum	36	36	35	36	36	36	36
Sum	10521	9601	10306	10214	9327	10610	9789
Count	352	352	352	352	352	352	352

LITHUANIA	*Password management*	*Email use*	*Internet use*	*Social media use*	*Use of devices*	*Information handling*	*Incidents preventing and handling*
Mean	30.566	27.979	28.987	29.042	27.103	29.939	27.591
Median	31	28	29	29	27	30	28
Mode	34	27	29	29	26	28	28
Standard Deviation	3.508	3.606	2.483	2.893	3.426	3.510	4.277
Kurtosis	2.727	-0.375	2.486	1.614	0.191	0.789	2.537
Skewness	0.141	-0.094	-0.845	-0.410	-0.080	-0.501	0.368
Range	33	18	21	23	22	21	39
Minimum	20	18	15	13	14	15	15
Maximum	53	36	36	36	36	36	54
Sum	14580	13346	13827	13853	12928	14281	13161
Count	477	477	477	477	477	477	477

The mean scores of Estonian librarians' in knowledge, attitude and behaviour is higher than Latvian and Lithuanian librarians', followed by Lithuania in knowledge and behaviour and by Latvia in attitude. Behaviour seems to be a strongest area of all Baltic librarians' (see table 4). Answers by focus areas show the highest awareness in information handling (32.22), password management (32.14), social media use (30.3) and Internet use (30.3), while the awareness in the other focus areas is below 30. This shows that the average Estonian librarian's cyber awareness is quite good, but there are also areas that need improvement, especially the use of devices (27.6). The mean scores of Latvian librarians' answers by focus areas show the highest awareness also in information handling (30.14), password management (29.88), Internet use (29.27) and social media use (29.0). Use of devices (26.4) show quite low awareness. The mean scores of Lithuanian librarians' answers by focus areas show the highest awareness in password management (30.56) and the lowest awareness in use of devices (27.10). Some comments from respondents:

It's not my job to complain about others, the IT department has anyway made multiple downloads and program installs impossible.

If the link sent is familiar to me, my colleague and I have talked about forwarding it in advance, etc., it is safe to open it. But about the strange link that comes from familiar sender with no comment, I've asked a few times using other communication channels, so far they've been safe too.

I have not received separate cybersecurity training from my employer every year. I got some instructions only when I came to work and the rest is what I learned/previous experience.

There is no IT department, we buy a service and the company can only be contacted in case of a very extraordinary problem (the excuse to the employee: we save money).

There is no such thing as an IT department in the school library, where you can turn to in case of a problem, doubt or some other gut feeling. You have to be competent enough for that.

6. Conclusions

The cybersecurity cooperation of the Baltic states is close, and libraries have an important role to play as cooperation partners of the state in bringing cybersecurity knowledge to the population, raising their awareness and protecting the population from cyber threats.

The role of the library as a public service institution in ensuring cybersecurity could be to create opportunities and conditions for users to get the necessary materials safely while maintaining their privacy and confidentiality. The role of a librarian in ensuring information security and cyber protection is to be aware, to act responsibly, to be helpful when library users need help, and to use the equipment and equipment entrusted to them for the intended purpose. Self-improvement is extremely necessary. It is important to realise that if librarians see a place of risk, they inform the relevant people in the institution, and do not look away. They can raise their awareness through training, and reading relevant literature. Since complete privacy and user security cannot be guaranteed in an online information environment, one of the most important tasks of librarians is to ensure that users are provided with adequate information and understanding of threats to their privacy and security online and how to protect themselves from that. These types of knowledge and skills are important components of

digital literacy, which is reflected in the ability to use information and communication technologies to find, evaluate, create and communicate information. It requires both cognitive and technical skills.

The survey conducted among librarians in the Baltic countries was based on a methodology that has gained wide recognition in the world, where an information security questionnaire based on the KAB model (Human Aspects of Information Security Questionnaire – HAIS-Q) was conceptualised to measure the relationship between three variables (knowledge, attitudes and behaviour). The questionnaire consisted of 63 questions and was adapted perfectly for libraries.

One of the great positive aspects of the HAIS-Q survey is that if a person has not previously paid much attention to cybersecurity threats in the context of libraries, the questions force the respondent to think about these important and topical issues. Thus, answering the questionnaire alone can increase the cyber awareness of library staff. Increasing knowledge, however, is known to improve attitudes, which results in better information security behaviour.

The respondents in all three Baltic countries are characterised by the fact that the majority of employees are aged 51–60. This indicator would need further investigation because there are significantly fewer workers in the previous and subsequent age groups. It is also common that there were most respondents with less than five years of work experience. The results of the survey revealed that the information security awareness of Estonian library staff is better than their Latvian and Lithuanian colleagues. This may be due to the fact that 62 per cent of Estonian library employees have participated in cybersecurity training, while in Latvia and Lithuania, the percentage of those who have participated in the training is only 43% and 40%, respectively. The desire to participate in the training is highest in Lithuania, followed by Latvia and Estonia. Probably, a large part of the applicants in Estonia have already been able to complete cyber training.

Both the average scores and the mean of the scores showed that Estonian librarians' knowledge, attitudes and behaviour in the field of information security are stronger than those of their Latvian and Lithuanian colleagues. At the same time, in all three Baltic countries, librarians' strongest point is their behaviour. This shows that although there may have been little training and the attitude may be repulsive, instinctively one still behaves correctly. This does not support Siponen et al. (2007) and Workman et al. (2008) evidence that individuals who have the necessary information security knowledge and skills may not be able to effectively apply them in their daily work routine. On the other hand, if there were more cybersecurity training, knowledge would increase, attitudes would also improve, and thus their information security behaviour would improve even more. It would be especially necessary to raise awareness in the use of devices. Currently, this focus area shows the lowest awareness among the library staff of all three Baltic countries. The focus area of email use also needs raising of awareness, and in the case of Latvia and Lithuania, prevention and handling of cases is also necessary.

Further recommendations for policy makers, local governments and library management would be to realise that the cyber awareness of library staff is a key issue for the country. All libraries, but especially public libraries, stand on the front line of the information war. Every ordinary citizen who wants it or who, in the opinion of a library employee, needs it, must receive cyber defence training from libraries. Libraries play an important and active role in disseminating information about specific threats to the country's citizens (for example, cyber awareness campaigns, but also crisis management campaigns, etc.). The ever-widening gap between those who have digital literacy and

those who do not, and are therefore unable to protect themselves online, further emphasises the role of libraries in closing this gap. Libraries are not only cultural centres but also regional community centres where residents can receive free digital and cyber literacy training. The library is the heart of the community, and people come there willingly. A librarian should be an educator and a leader in the basics of cyber awareness.

References

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, 33(3), 237-248. https://doi.org/10.1080/0144929X.2012.708787

Allen, I. E., Seaman, C. H. (2007). *Likert Scales and Data Analyses. Quality Progress.* https://www.bayviewanalytics.com/reports/asq/likert-scales-and-data-analyses.pdf

Baranowski, T., Cullen, K.W., Nicklas, T., Thompson, D., Baranowski, J. (2003). Are Current Health Behavioral Change Models Helpful in Guiding Prevention of Weight Gain Efforts? *Obesity Research*, 11, 23S-43S. https://doi.org/10.1038/oby.2003.222

Brown, J. D. (2011). Likert items and scales of measurement? *Shiken Research Bulletin: JALT Testing & Evaluation SIG Newsletter*, 15(1), 10 – 14. https://hosted.jalt.org/test/PDF/Brown34.pdf

Denisenko, V. (2020). Threats of propaganda and the information war on Lithuanian security, *in* Matonytė, I., Česnakas, G., Statkus, N. (eds.), *Lithuania in the Global context: national security and defence policy dilemmas* (pp. 235-248). https://etalpykla.lituanistikadb.lt/object/LT-LDB-0001:J.04~2020~1612288415250/J.04~2020~1612288415250.pdf

EDA (2021). *Estonian Digital Agenda 2030* (2021). Ministry of Economic Affairs and Communications of Estonia. https://mkm.ee/media/6970/download

Georgiadou, A., Mouzakitis, S., Bounas, K., Askounis, D. (2022). A Cyber-Security Culture Framework for Assessing Organization Readiness. *Journal of Computer Information Systems*, 62(3), 452-462. https://doi.org/10.1080/08874417.2020.1845583

ISE (2019). *International Security and Estonia.* (2019). Estonian Foreign Intelligence Service. https://www.valisluureamet.ee/doc/raport/2019-en.pdf

Hakkala, A., Isoaho, J., Virtanen, S. (2018). Cyber security competence in working life, *in* P. Naumanen, J. Liesivuori (eds), *Ready for working life! Visions and perspectives on well-being at work and readiness for working life, as well as methods for their development* (pp. 174-181). https://valte.fi/

Horchakova. A. (2022). Strengthrning the Transatantic Partnership: Challenges and Opportunities for the Baltic States, *in* E. Bilevičiūtė, G. Petkutė, K. Kenstavičienė, (eds.), *Teisinės minties šventė, Studentų mokslinių straipsnių rinkinys*. (pp. 96-106). https://repository.mruni.eu/handle/007/18311

Kruger, H. A., Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security*, 25(4), 289-296. https://doi.org/10.1016/j.cose.2006.02.008

LDTG (2021). *Latvia's Digital Transformation Guidelines for 2021-2027* (In Latvian). Riga. https://likumi.lv/ta/id/324715-par-digitalas-transformacijas-pamatnostadnem-20212027-gadam

Lehto, M., Limnéll, J. (2021). Department o Strategic leadership in cyber security, case Finland. *Information Security Journal: A Global Perspective*, 30(3), 139-148. https://doi.org/10.1080/19393555.2020.1813851

MacKinnon, N. J., Hoey, J. (2021). Operationalizing the Relation Between Affect and Cognition With the Somatic Transform. *Emotion Review*, 13(3), 245–256. https://doi.org/10.1177/17540739211014946

Magdalinou, A., Kalokairinou, A., Malamateniou, F., Mantas J. (2023). InfoSec Practices - a Survey Conducted in Greek Hospitals. *Acta Informatica Medica*, 31(1), 48-52. https://doi.org./10.5455/aim.2023.31

Niedra, I. (2021). *Safer Internet Day: Experiences in Latvian Libraries.* https://www.ifla.org/news/safer-internet-day-experiences-in-latvian-libraries/

Nunes, P., Antunes, M., Silva, C. (2021). Evaluating cybersecurity attitudes and behaviors in Portuguese healthcare institutions. *Procedia Computer Science*, 181, 173-181. https://doi.org/10.1016/j.procs.2021.01.118

Nutall, A. (2021). *Women's work, women's words: feminist library history.* https://bookriot.com/feminist-library-history/

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, 42(May), 165-176. https://doi.org/10.1016/j.cose.2013.12.003

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., Zwaans. T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers & Security*, 66, 40-51. http://dx.doi.org/10.1016/j.cose.2017.01.004

Paulsen, C., Byers, R. (2019). *NISTIR 7298 Rev. 3, Glossary of Key Information Security Terms* (2019). https://doi.org/10.6028/NIST.IR.7298r3

Ranas, T., Fariz, A., Dirgantara, B., Muhamad, A., Ruldeviyan, Y. (2020). Measuring information security awareness of client's information security: case study at PT XYZ. *International Journal of Advances in Electronics and Computer Science*, 7(7), 2394-2835. https://www.iraj.in/journal/journal_file/journal_pdf/12-669-15992140201-6.pdf

SDDP (2021). *State Digitisation Development Programme 2021-2030* (2021). The Ministry of Economy and Innovation of the Republic of Lithuania, Vilnius. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/fff902e44e8c11ec86bdcb0a6d573b32?jfwid=rivwzvpvg

Shrader, P. G., Lawless, K. A. (2004). The knowledge, attitudes, & behaviors approach how to evaluate performance and learning in complex environments. *Performance & Improvement*, 43(9), 8-15. https://doi.org/10.1002/pfi.4140430905

Siponen, M., Pahnila, S., Mahmood, A. (2007). Employees' adherence to information security policies: an empirical study. *Privacy Trust Complex Environonment*, 232, 133–144. https://opendl.ifip-tc6.org/db/conf/sec/sec2007/SiponenPM07.pdf

von Solms, R., van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

Spurava, G., Kotilainen, S., Holma, B. (2021. The Role and Readiness of Librarians in Promoting Digital Literacy: A Case Study From Latvia. *Culture Crossroads*, 20, 71-87. http://www.culturecrossroads.lv/

Steponaitiene, J. (2021). *Safer Internet Day in Lithuanian Libraries.* https://www.ifla.org/news/safer-internet-day-in-lithuanian-libraries/

Vaks, T. (2013). *Summary of the State Information Authority (ISA) on ensuring cybersecurity in 2012*.

Workman, M., Bommer, W.H., Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers & Human Behaviour*, 24(6), 2799–816. https://doi.org/10.1016/j.chb.2008.04.005.

Yeng, P. K., Fauzi, M. A., Yang, B. (2021). Assessing the effect of human factors in healthcare cyber security practice: An empirical study, *in* M. G. Vassilakopoulos, N. N. Karanikolas, G. Stamoulis, V. S. Verykios, C. Sgouropoulou (eds.), *PCI 2021: 25th Pan-Hellenic Conference on Informatics*, Volos, Greece, November 26 - 28, 2021 (pp. 109-114). https://doi.org/10.1145/3503823.3503909

Zwilling, M., Klien, G., Dušan, L., Wiechetek, L., Cetin, F., Basim, H. N. (2020). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, 62(1), 82-97. https://doi.org/10.1080/08874417.2020.1712269

Authors' information

Kate-Riin Kont graduated from the Department of Librarianship and Information Science, Tallinn University in 1995; she earned a MA from the same department in 2004. Since 2009, she has been involved in doctoral studies at Tallinn University, Department of Digital Technologies. Since 2008 she has been working as Head of the Acquisition Division of the Tallinn University of Technology Library and in 2018 she started work in Tallinn Health Care College as a Senior Lecturer in Lifelong Learning Centre. She is a member of the Terminology Working Group of the Estonian Librarians' Association. Since 2014 she leads Collection Development Committee of the Estonian Librarians' Association and acts as a member of EBSCO Information Services Academic Advisory Board. After graduating from Tallinn University School of Digital technologies as PhD in March 2022, she has been working as a cyber security researcher in Estonian Academy of Security Sciences, Institute of Internal affairs.

Received May 22, 2023, revised August 9, 2023, accepted September 1, 2023