UNIVERSITY OF TARTU
Institute of Computer Science
Cyber Security Curriculum

Christian Tschida

The Way to the Specialist and Management Level of Cyber Hygiene Initiative

Master's Thesis (30 ECTS)

Supervisor(s): Sten Mäses
Raimundas Matulevičius

Tartu 2017

The Way to the Specialist and Management Level of Cyber Hygiene Initiative

Abstract:

Cybercrime and state sponsored espionage is still growing rapidly. The number of affected organizations increases day by day. Some know that they are effected, some still do not know. The user is a main factor in cyber security incidents. No two humans are the same (e.g. fingerprints, skill, knowledge, attitude). The behaviour of humans is influenced by various factors. The goal of the Cyber Hygiene Initiative is to adopt internal guidelines for comprising the best behavioural principles for cyber hygiene, as well as to create an e-learning platform, where these guidelines get implemented. The prototype, of the Cyber Hygiene e-learning course was implemented and tested in the Estonian Defence Forces in early 2016. This thesis builds up on this. It tries to clarify what data should be available to the specialists and what information should be reported to the management. This shall help to create the specialist and management level of the Initiative. The methodological foundation of the e-learning course was well laid with other theses. This thesis introduces the methodology and shows the results, what kind of data and reporting should be implemented on the specialist- and management-level. Decision makers and managers have now an Executive summary available, to take specialists view into account and to implement proper reporting. Additional to many interviews with specialists and security experts, a questionnaire was created to raise coverage. The testing of the questionnaire was done at an international well known think tank. Results from the interviews and the survey indicated that the methodology proves to be valid for improving reporting and should help with implementation. The developed methodology and questions will be further considered at CybExer Technologies, a joint venture of BHC Lab and bytelife, who contracted with EDA for a period of 3 years at the end of 2016 to further improve the programme and include the specialist- and management-level.

Keywords:

Cyber Hygiene Initiative, e-learning, specialist, expert, management, reporting

CERCS: P170 Computer science, numerical analysis, systems, control

TEE SPETSIALISTI JA JUHTKONNA TASEME SUUNAS KÜBERHÜGIEENI INITSIATIIVI RAAMES

Lühikokkuvõte:

Küberruumi kuritarvitused, s.h küberkuritegevuse arvukus ja riikide huvides ning nende poolt toetatud spionaaž, näitavad jätkuvalt kasvutrendi. Samuti suureneb igapäevaselt küberintsidentidest mõjutatud organisatsioonide ja ettevõtete arv. Paljud neist saavad teada küberründe ohvriks langemisest suhteliselt ruttu, kuid esineb juhtumeid, kus sihtmärgil puudub võimekus oma turvasüsteemi lubamatut tungimist ise avastada. Küberintsidentide ja –rünnete peamiseks võimaldavaks faktoriks on saanud IT infrastruktuuri kasutaja. Kasutajast tuleneva riski maandamist raskendab asjaolu, et ei ole olemas kahte ühesuguse käitumismustriga inimest. Erinevused esinevad mistahes faktorites alates füsioloogilistest (sõrmejäljed) ja lõpetades teadmiste, kogemuse ja iseloomuomadustega.

Küberruumis aktsepteeritavate käitumisjuhiste väljatöötamiseks ja rakendamiseks on ellu kutsutud 'Küberhügieeni initsiatiiv', mille üheks kõrvaleesmärgiks on nimetatud reeglite kasutamist soodustava e-õppe platvormi loomine. Küberhügieeni e-õppe keskkonna testversiooni katsetas Eesti kaitsevägi esmakordselt 2016. aasta lõpus. Sellest katsetusest saadud kogemusest käesolev lõputöö räägibki. E-kursust aluseks võttes, analüüsib uurimus, missugune informatsioon peaks olema tehtud kättesaadavaks IT spetsialistidele ja missugune informatsioon tuleks edastada juhtkonnale. Töö üheks eesmärgiks on aidata kaasa küberhügieeni initsiatiivi sees spetsialistide ja juhtkonna taseme loomisele ja eristamisele.

E-õppe kursuse metoodiline alus sobitus hästi varasemate töödega. Antud töö tutvustab uurimuse tulemusi ja metoodikat, näitamaks missuguseid andmeid ja raporteerimist peaks rakendama nii spetsialistide kui ka juhtkonna tasemel. Juhtkonna ja juhataja jaoks on uueks võimaluseks intsidentide kokkuvõte, mis on võtnud arvesse spetsialistide teadmised, rakendamaks korrektset raporteerimist. Lisaks paljudele intervjuudele spetsialistidega ja turvalisuse ekspertidega, loodi laiema info saamiseks küsimustik. Küsimustiku tõhusust katsetati rahvusvaheliselt tuntud mõttekojas. Küsimustiku ja intervjuude tulemused viitavad sellele, et see metoodika on kehtiv, parandamaks raporteerimist ning vastumeetmete rakendamist. Väljatöötatud metoodikat ja küsimustikku on kavas rakendada küberõppusel, s.t. BHC Laboratory ja ByteLife'i ühisettevõtmisel, millel on 2016.aastal sõlmitud 3-aastane leping EDA'ga õppeprogrammi edasiarendamiseks ning spetsialistide ja juhtkonna taseme õppe lisamiseks.

Võtmesõnad:

küberhügieeni initsiatiiv, e-õpe, spetsialist, ekspert, juhtkond, raporteerimine

CERCS: P170 Arvutiteadus, arvutusmeetodid, süsteemid, juhtimine (automaatjuhtimisteooria)

Table of Contents

List of Abbreviations and Terms

ACO [1]	Allied Command Operations see also SHAPE
ACT [8]	Allied Command Transformation
Bi-SC	Bi-Strategic Command (ACO and ACT)
BSI [22]	Bundesamt für Sicherheit in der Informationstechnik Federal Office for Information Security (Germany)
BYOD	Bring Your Own Device
CCDCOE [29]	NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia
CD	Cyber Defence
CEB	Corporate Executive Board
CERT [31] [30]	Crisis Emergency Response Team
CIRC [2]	Computer Incident Response Capability
CISSP	Certified Information Systems Security Professional
CMM [3]	Capability Maturity Model (Carnegie Mellon university)
COBIT [4]	Control Objectives for Information and related Technology from ISACA
COSO [5]	The Committee of Sponsoring Organizations of the Treadway Commission
CS	Cyber Security
CSO	Chief Security Officer
CyCon [6]	International Conference on Cyber Conflict
DCWF	Development of a Cyber Security Workforce, see NCWF
DRESMARA [7]	Regional Department of Defense Resources Management Studies
EDA [9]	European Defence Agency
e.g.	Example given
ENHIS	Estonian National Health Information System
EU [10]	European Union
E&T	Education and Training
EUROSOX [12] [11]	8th directive of the EU for accounting RICHTLINIE 2008/30/EG

	DES EUROPÄISCHEN PARLAMENTS UND DES RATES
HR	Human Resources
ILIAS [13]	ILIAS (Integriertes Lern-, Informations- und Arbeitskooperations-System [German for "Integrated Learning, Information and Work Cooperation System"]
ISACA [14]	Information Systems Audit and Control Association
(ISC)²	International Information System Security Certification Consortium
ISKE [15]	infosüsteemide kolmeastmeline etalonturbe süsteem an information security standard that is developed for the Estonian public sector. based on a German information security standard – IT Baseline Protection, see BSI
IT	Information Technology
LS [16]	Locked shields
MC [17]	Military Committee the senior military authority in NATO
MNCD [18]	Multinational Cyber Defence Smart Defence Project for Education and Training
MOD	Ministry of Defence
NAC [19]	North Atlantic Council the principal political decision-making body within NATO
NATO [20]	North Atlantic Treaty Organization
NCIA [21]	NATO Communications and Information Agency
NCIS	NATO Communications and Information Systems
NCWF [23]	NICE Cyber Security Workforce Framework
NDPP [24]	NATO Defence Planning Process
NICE [23]	National Initiative for Cyber Security Education (US)
NIST [25]	National Institute of Standards and Technology (US)
RQ	Research Question
SHAPE [26]	NATO Supreme Headquarters Allied Powers Europe
SOX [27]	Sarbanes-Oxley Act of 2002
TNA	Training Needs analysis
TUT [28]	Tallinn University of Technology

US	United States of America
Val	Value management

For my father and my son
My father Josef who fought and won his battle against cancer
and my son Alexander, who had to miss me,
while I was working, studying and living half a world away
Hoping to be an example to never ever give up

List of Figures

List of Tables

1 Introduction

This thesis adds up on theses for improving the general user-level of the Cyber Hygiene Initiative. The three foreseen levels for the training are correlating also with used standards and recommendations [32]. It collects data from Cyber Security experts in form of interviews and a survey to identify what data is important to have for the specialists and what they think would be of value for the management to know. A proposal of information for reporting is given in the condensed form of an Executive summary for the management. It is now on managers to decide, what information of this list they want to get reported in what form and frequency. Especially in governmental organisations it seems to be a problem to implement business best practices. In this thesis, it is emphasized that payment is a factor for specialists to consider to change to better paid positions, so it is of utmost importance to treat their specialists in a proper manner and keep them motivated.

1.1 Problem Statement

Many security standards ask for basic user training. Under others NIST [25], COBIT [4], ISO [33], BSI [34], ISKE [15]. What some managers in European Union still seem to be unaware of, is the applicability of EUROSOX [12], which gives responsibility to: "Assure effective corporate governance, internal controls and risk management.".

The Cyber Hygiene Initiative is a multilateral initiative to change that. The basic user level was tested on a nation-wide scale in the Estonian Defence Forces. The specialist- and management-level is still to be created. In the discussion and interviews with TUT and bytelife a possible way of implementing feedback in that programme was valuable. The following research questions are aiming at the specialists to develop a well-founded proposal from the expert-level. With that proposal, the management can decide, what information, they want to get reported in the form and frequency they need.

1.2 Research Questions

The development of the questions was driven from the need to gain a better understanding of expert knowledge, that should be transferred to the management level. The main source for the development of the questions to answer was the guidelines document (see Appendix 3).

- RQ 1: What statistical data to collect?
- RQ 2: What to report?
- RQ 3: What are the biggest threats?

With the question 53 the respondents shall have the opportunity to give additional input and advice. The availability of open questions and comment fields shall grant the collection of unexpected and innovative answers from the respondents, to catch even information that was not thought of before.

As a warm up, of what to expect, please notify how one the respondents phrased it: "If these above impediments are getting in my way and I cannot change them I will leave. There is not shortage of demand."

The development of the topic follows the chapters:

Introduction, Background Information, Methodology, Implementation and Conclusion.

The starting conditions are rather good, because a test-version of basic user awareness training was already implemented, but the specialist- and management-level is still to be created and this thesis can give valuable input for the further improvement.

1.3 Acknowledgements

I must thank a lot of people who made this thesis possible. Being so proud, that I was allowed to work at the Cooperative Cyber Defence Centre of Excellence (CCDCOE) as first representative of a partner nation, thankful for the acceptance I found at my work, at the university and Estonia itself, I hope I have seen enough examples from people in Estonia high up in the hierarchy, that were always reachable for requests, that I can follow that behaviour, to be reachable and open for needs from other people, the whole rest of my live. I have found a second home and even if my origin or my career might make it necessary to move on, I will stay the rest of my live connected to Estonia. Thank you everybody in Estonia for the warm welcome and the amazing time you made possible for me. I want to thank my supervisors Sten Mäses and Raimundas Matulevičius for countless critical questions to increase the argumentative depth of statements, taking distance from too strong argumentation and having a proper understanding for what it means to work and study at the same time. Estonian governmental representatives for their openness to questions, their reachability and their support. Beginning with Mihkel Tikk, Director of Cyber Policy Department of the Estonian Ministry of Defence, Kusti Salm and Teet Laeks. Lauri Almann and Andrus Kivisaar from BHC Lab, Janek Gridin from bytelife, my workmates from the CCDCOE, especially Kenneth Geers for pointing me to his former research, Lauri Aasmann for translating my abstract to Estonian and Clare Lain for giving me the luxury to have a native English speaker as proof-reader. I want to thank Jimmy Heschl contributing to COBIT and Head of Digital Security at Red Bull, thank you for your refreshing approach to security. All the friends and colleagues I had the pleasure to get to know, and maybe even being sometimes annoying always wanting to speak about how to improve awareness training and all respondents. And thank you to all those who preferred to stay nameless in the fog of anonymity. And to those I counted mistakenly to that group, I apologise. Thank you all!

1.4 The Contribution of the Author

The implementation of Cyber Security, Cyber Defence and Cyber Awareness into the Agenda of states is an ongoing process. Many Nations came up with strategies that foresee the implementation of Cyber Security and give foresights in what they want to achieve. The how is often still a challenge. That is also valid for awareness and implementation of best practices.

The purpose of this thesis is to give answers on a possible way of implementing feedback in the specialist- and management-level in developing a well-founded proposal from the expert-level. With that proposal, the management can decide, what information, they want to get reported in the form and frequency they need.

The specific contribution of the author is:

- Collecting expert and management data on a large scale, from Experts from Asia, America and Europe, on a level that is unusual for a thesis.
- Creation of a re-usable and adaptable questionnaire, that is methodological mature, tested and delivering necessary data.
- The creation of a short Executive summary, taking into account the input from high level individuals, stressing that they are too busy to read long reports and recommendations.

2 Background Information

Many security standards ask for basic user training. Under others NIST [23], COBIT [4], ISO [35], BSI [22], ISKE [36]. What some managers in European Union still seem to be unaware of, is the applicability of EUROSOX, which gives responsibility to: “Assure effective corporate governance, internal controls and risk management.” [12].

It is not as strict as the SOX that is applicable for the US, which states: “SOX auditing requires that internal controls and procedures can be audited using a control framework like COBIT. Log collection and monitoring systems must provide an audit trail of all access and activity to sensitive business information.” [37]

A white-paper which tries to explain that, provided at the law oversight page of the US phrases it: “For the top management of a public company to discharge its obligations to oversee the financial reporting process, it must identify, understand, and assess the factors that may cause the financial statements to be fraudulently misstated.” [38]

References to training: “Principle 3:

Senior management should have responsibility for implementing the operational risk management framework... and all levels of staff should understand their responsibilities with respect to operational risk management. Senior management should also have responsibility for developing policies, processes and procedures for managing operational risk in all... material products, activities, processes and systems.” [38]

And to make the intent clearer SEC Commissioner Cynthia Glassman summarized the intent of these sections in a speech on September 27, 2002 to the American Society of Corporate Secretaries. “Recognizing that awareness must precede action, Sarbanes-Oxley and the Commission’s rules require the CEO and Board to make certain that procedures are in place to ensure that they hear bad news. Under the Commission’s recently adopted rules, these procedures must ensure that all material information - both financial and non-financial – gets to those responsible for reporting it to the investing public.” [38]

But how to do it? What statistical data to collect, and what and how to report to the management?

More and more governments [23] [39] try to take over business best practices [40]. Still it seems that some governments struggle with adapting those practices. If future governments want to retain their employees and avoid a drain to economy, it will be of utmost importance to adapt to business best practices. But in doing so, they should also keep old words of wisdom at the back of their mind: “By attempting to govern an army in the same way as he administers a kingdom, being ignorant of the conditions which obtain in an army. This causes restlessness in the soldier's minds.” [41] Going for a basic user awareness training, is a good way to start, but once employees will be trained and skilled, they should also get paid properly. When payment is not the way the government of a nation can go, it should at least treat their employees well, otherwise there might be no way, to keep their skilled people. The US government has proven it is more than aware of that [39].

Incentives for three levels of experience are explicitly mentioned in their Cyber Security Workforce development kit [39].

Tips to retain entry-level Staff

- Foster an environment where diverse perspectives are welcome
- Encourage two-way dialogue for open communication
- Provide frequent feedback on job performance
- Ensure that cyber professionals have quality supervision and mentorship
- Provide opportunities to acquire new skills through established training, challenging job assignments, and career paths
- Recognize staff for strong work performance

Tips to retain Mid-career:

- Emphasize work-life balance; encourage taking time to pursue activities and interests
- Provide opportunities to obtain advanced training and certifications
- Allow information sharing within the organization and professional forums
- Offer challenging job assignments
- Include employees in decision making and innovation
- Implement reward programs

Tips to retain Executive staff

- Provide advanced training and development opportunities
- Create tailored development plans that identify leadership competencies and areas for development
- Recognize leaders for their successes and accomplishments
- Consider performance and loyalty-based bonuses to retain staff
- Promote cyber executives to develop intellectual capital and create information sharing mechanisms

2.1 Related Work

Boeke is mainly dealing with the binary choice of putting Cyber Defenders into the Intelligence community or not, but he also stresses the importance of training [42].

Fellow colleagues from the Tallinn Technical university were writing about the Cyber Hygiene Initiative, mainly dealing with the basic user training level. Sumin’s thesis [43] is mainly dealing with the development of a scientific framework for improving the basic user training and the content. He agrees with Kevin Mitnick [44] that “People are the key factor to either success or failure of cyber security in organizations”.

Suarez tested people after a cyber hygiene training by sending them phishing e-mails [45]. An interesting aspect he mentions, is the preference for class room learning from students, is surprisingly high. A conclusion, that goes further than his one, is that e-learning should be personally announced, advertised and a mentor programme for employees might be beneficial. A main reason for creating an e-learning course is the big target audience and the cost related to train a big number of people. Nevertheless, it is important, that at each location or office of an organisation, somebody takes care of the employees, especially the new ones. Mentoring programmes are one of the best practices proposed for tackling that issue.

There is some research out there on how to create and validate basic user awareness training like the thesis of Veseli [46] from Norwegian Grovjik university. Her conclusion is, that besides social engineering campaigns, traditional class room lectures get the highest acceptance and improve of behaviour, but finally concludes also, that with big geographical scattering of the training audience, there is no way around web-based training. Gamification also seems to be a hot topic [47].

Fredmund Malik's book [48] is a proposal for a manager who wants to understand why the Germans are able to produce such a good quality of things, and are world market leaders in a lot of fields.

The People Capability Maturity Model

There is lots of literature about management, motivation and best practices. Managers should be aware of that. It is an estimation that most universities give at least an overview of those, but if that is wrong, there is a lot of literature out there for increasing management skills. What shall be pointed to, is the collection of best practices from the Carnegie Mellon university, that was also implemented in the new draft of the NIST standard of creating a capable workforce [23]. "The People Capability Maturity Model (People CMM) can help organizations successfully address their critical human capital issues. The People CMM employs a process maturity framework as a foundation for best practices for managing and developing an organization's workforce. Based on the best current practices in fields such as human resources, knowledge management, and organizational development, the People CMM guides organizations in improving their processes for managing and developing their workforce. The People CMM helps organizations characterize the maturity of their human capital practices, establish a program of continuous workforce development, set priorities for improvement actions, integrate workforce development with process improvement, and establish a culture of excellence." [3] But for some reasons governments sometimes struggle with the implementation. To research why, should be tackled in future work. For companies there are studies, why they are not performing to their best potential and proposals what to change. The following subchapter shows management failures and their solutions.

Five Performance Management Failures and their Solutions

Research from CEB, which unite 80% of the Fortune 1000 companies [49] is claiming, that the average company is harming it's potential with failing performance management strategies. Following you find a shortened overview, taken from their study.

1 You don't know what it is.

> Every organisation or firm has to figure out for themselves, what makes performance and performance management for them.
>
> > First define it.
> >
> > > Key process activities have not only to be reported, but also get used to increase the performance. Employee behaviour must be aligned with organizational objectives.

2 You do not prioritize objectives.

Prioritize ruthlessly.

3 It is too complex and insufficiently connected to your strategy.

Focus on behaviours and milestones, not just high level metrics.

4 It is not human.

An increased contribution should also trigger an increase in reward or benefits. Performance management systems must adapt to reward networked performance, encourage a new set of competencies, and enable collaboration across the enterprise. Only 23% of HR executives believe their performance management processes accurately reflect employee contributions.

Align business performance management to HR performance management.

5 It does not create a climate that allows employees to adapt.

Create an adaptable review system.

Successful firms set escalation and divestment triggers ahead of time; reduce their metrics to the highly relevant; ensure their reviews look at changes to the operating environment before metrics; and regularly report on human capital, market, and operational factors, as well as financial factors [50].

2.2 Necessity of Awareness Training in relevant Security / IT/ Accounting Standards

As stated above in the introduction to the main chapter, many security standards like NIST [20], COBIT [3], ISO [32], BSI [26] and ISKE [33] demand training and all-user training in their applicability and recognition, or certification according to that standard. In the following subchapters, a short overview over the standards will be given. In general business companies are doing feedback in their organisation and try to receive it from their customers. In the analogue world, an eminent method to get more information about the customer and bind him to the enterprise are customer cards, but the future is data itself [51] [52] [53] [54].

ISO

The ISO, the International Organization for Standardization, develop and publish International Standards. For sure to mention here is the ISO-27000 family [55].

ISO/IEC 27000:2016 Information technology, Security techniques, Information security management systems, Overview and vocabulary

The one that your organisation could certify against is the next one:

ISO/IEC 27001 - Information security management

ISO/IEC 27002:2013 - Information technology, Security techniques, Code of practice for information security controls

ISO/IEC 27003:2010 - Information technology, Security techniques, Information security management system implementation guidance

ISO/IEC 27004:2009 - Information technology, Security techniques, Information security management, Measurement

When certifications are a topic, it is always worth mentioning one of the most standards, that companies certify against.

ISO 9001:2015 - Quality management systems, Requirements

interesting might also be:

ISO 31000:2009 Risk management, Principles and guidelines

NIST, NICE and NCWF

The NIST, NICE and NCWF are aiming at increasing the cyber security in the US.

NIST: The National Institute of Standards and Technology is a non-regulatory federal agency within the U.S. Department of Commerce. NIST's mission is to promote innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve the quality of life [56].

NICE: The National Initiative for Cybersecurity Education (NICE), led by the National (US) Institute of Standards and Technology (NIST), is a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development. The mission of NICE is to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development. NICE fulfils this mission by coordinating with government, academic, and industry partners to build on existing successful programs, facilitate change and innovation, and bring leadership and vision to increase the number of skilled cybersecurity professionals helping to keep the US secure [23].

NCWF: The NICE Cybersecurity Workforce Framework (NCWF) is a national resource that categorizes and describes cybersecurity work. It provides employers, employees, educators, students, and training providers with a common language to define cybersecurity work as well as a common set of tasks and skills required to perform cybersecurity work. Through the process of identifying the cybersecurity workforce and using a standard set of terms they work together to educate, recruit, train, develop, and retain a highly-qualified workforce [23].

The Sarbanes-Oxley Act

The Sarbanes-Oxley Act (SOX) is a law in the US and makes the use of frameworks obligatory for public companies: “After consideration of the comments, we have modified the final requirements to specify that management must base its evaluation of the effectiveness of the company's internal control over financial reporting on a suitable, recognized control framework that is established by a body or group that has followed due-process procedures, including the broad distribution of the framework for public comment.” [57] like the following frameworks.

COSO

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a joint initiative of the five private sector organizations for accounting and auditing. It is dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management, internal control and fraud deterrence [5].

SOX states: “The COSO Framework satisfies our criteria and may be used as an evaluation framework for purposes of management's annual internal control evaluation and disclosure requirements." [57] But the COSO frameworks aims more at governance and management for accuracy in accounting and auditing [5].

The elegance in COBIT 5 which will be explained in the next subchapter is that it states:" Connect to, and, where relevant, align with, other major frameworks and standards in the marketplace, such as Information Technology Infrastructure Library (ITIL®), The Open Group Architecture Forum (TOGAF®), Project Management Body of Knowledge (PMBOK®), PRojects IN Controlled Environments 2 (PRINCE2®), Committee of Sponsoring Organizations of the Treadway Commission (COSO) and the International Organization for Standardization (ISO) standards. This will help stakeholders understand how various frameworks, good practices and standards are positioned relative to each other and how they can be used together." [58]

COBIT

COBIT 5: A Business Framework for the Governance and Management of Enterprise IT has clarified management level processes and integrated COBIT 4.1, Val IT [59] and Risk IT [60] content into one process reference model, but there are still some differences, like enablers were not called like that in COBIT 4.1.

COBIT 5 is based on 5 key principles and 7 supporting enablers for governance and management of enterprise IT:

- Principle 1: Meeting Stakeholder Needs

- Principle 2: Covering the Enterprise End-to-end

it integrates governance of enterprise IT into enterprise governance. It covers all functions and processes within the enterprise and considers all IT-related governance and management enablers to be enterprise-wide and end-to-end, e.g. inclusive of everything and everyone, internal and external, that is relevant to governance and management of enterprise information and related IT.

- Principle 3: Applying a Single, Integrated Framework

COBIT 5 aligns with other relevant standards and frameworks at a high level, and thus can serve as the overarching framework for governance and management of enterprise IT.

- Principle 4: Enabling a Holistic Approach

Efficient and effective governance and management of enterprise IT require a holistic approach, taking into account several interacting components. The COBIT 5 framework defines seven categories of enablers:

- Principles, Policies and Frameworks
- Processes
- Organisational Structures
- Culture, Ethics and Behaviour
- Information
- Services, Infrastructure and Applications
- People, Skills and Competencies

- Principle 5: Separating Governance from Management

Governance ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritisation and decision making; and monitoring performance and compliance against agreed-on direction and objectives.

Management plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives [58].

The COBIT framework was created from

ISACA®: With 95,000 constituents in 160 countries, ISACA (www.isaca.org) is a leading global provider of knowledge, certifications, community, advocacy and education on information systems (IS) assurance and security, enterprise governance and management of IT, and IT-related risk and compliance. Founded in 1969, the non-profit, independent ISACA hosts international conferences, publishes the ISACA® Journal, and develops international IS auditing and control standards, which help its constituents ensure trust in, and value from, information systems. It also advances and attests IT skills and knowledge through the globally respected Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in Risk and Information Systems Control TM (CRISCTM) designations. ISACA continually updates COBIT®, which helps IT professionals and enterprise leaders fulfil their IT governance and management responsibilities, particularly in the areas of assurance, security, risk and control, and deliver value to the business [58].

BSI Grundschutz

The German Bundesamt für Sicherheit in der Informationstechnik, or Federal Office for Information Security in English provides with the BSI Grundschutz (base line protection) a framework and guidance that is far more detailed than the rather generous ISO/IEC standards. The aim is to achieve an appropriate security level for all types of information of an organisation. IT-Grundschutz uses a holistic approach to this process. Through proper application of well-proven technical, organisational, personnel, and infrastructural safeguards, a security level is reached that is suitable and adequate to protect business-related information having normal protection requirements. In many areas, IT-Grundschutz even provides advice for IT systems and applications requiring a high level of protection. The nice thing here, is, that it automatically fulfils the requirements for a certification against ISO/ IEC 27001 and due to it's still big size it was also the starting point for the Estonian ISKE, that further compresses this big load of basic protection measures [34].

ISKE

The preparation and development of ISKE is based on a German information security standard – IT Baseline Protection Manual (IT-Grundschutz in German) – which has been adapted to suit the Estonian situation. ISKE is compulsory for state and local government organisations who handle databases/registers [15].

A three-level baseline system means three different sets of security measures for three different security requirements have been developed (different databases and information systems may have different security levels).

But on the example of dealing with health-data, even representatives from the Estonian ministry of social affairs had to admit: "Additionally, from the Ministry's perspective, the training of healthcare professionals and persuading them to use these unified standards, classifications and nomenclatures in making entries to ENHIS takes time and effort.” [61] Even when they were speaking about the standards of putting the data in the Estonian National Health Information System (ENHIS), it shows at least initial training is necessary, with new developments.

3 Methodology

In the following subchapters, the history and methodology of the development of the thesis will be explained. Structured in timeline, which explains the timely sequence of events, from getting aware of the topic, until decision to write the thesis on that topic and relevant events that happened. The next subchapter elaborates on the opportunity, that was used to leverage communication with experts at all. In the process of developing this thesis, several experts were spoken with. Mainly semi-structured interviews and structured interviews were conducted. Coordination meetings were held in ministries of defence, mainly the Estonian and the companies developing the content. A subchapter is explaining the Cyber Hygiene Initiative. The next subchapter sheds some light on getting support, the next one on the Research questions and how the development and testing of the questionnaire was done. Finally the target audience is explained.

3.1 Timeline

In the Figure 1 a timeline is given from the signature of the Pledge to mitigate Human-related Risks in Cyber space by launching the Cyber Hygiene Initiative. Only the main events with direct relation to the thesis are shown. Single opportunities for interviews, like MNCD-workshops, EDA-events, TNA-workshops and single appointments are not included, because there was no direct impact to the development of the Initiative. Locked shields participants made the target audience for the survey and at the CyCon, the Initiative was introduced to a wider audience.

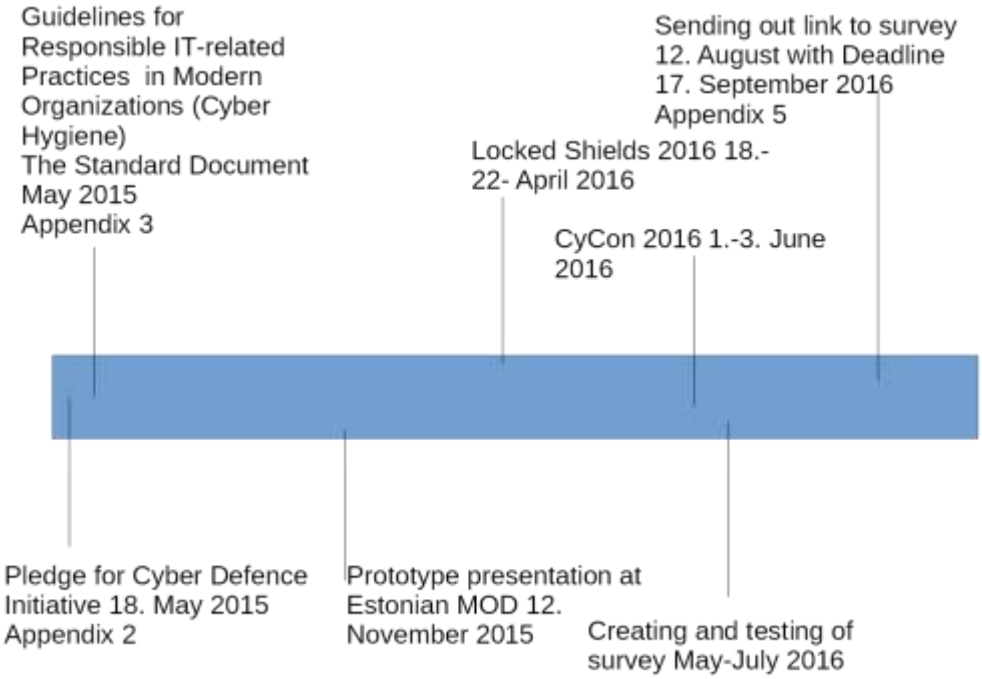

Guidelines for Responsible IT-related Practices in Modern Organizations (Cyber Hygiene)
The Standard Document
May 2015
Appendix 3
Sending out link to survey 12. August with Deadline 17. September 2016
Appendix 5
Locked Shields 2016 18.-22- April 2016
CyCon 2016 1.-3. June 2016
Pledge for Cyber Defence Initiative 18. May 2015
Appendix 2
Prototype presentation at Estonian MOD 12. November 2015
Creating and testing of survey May-July 2016

Figure 1 timeline

3.2 Taking Advantage of the Opportunity

The position as Staff Officer in the Education and Exercise branch at the CCDCOE gave valuable insights in mutual perspectives. Working there in the International project groups, like assistance to a NATO-wide awareness campaign and assistance to ACT in their role as Department Head for Cyber Defence, gave countless opportunities to speak with international experts in various workshops on that topics. So, there was opportunity to speak with representatives of ministries and nations all over the world. Leading 2 projects at my work and including into that projects, representing the CCDCOE to other organisations and events gave plenty of opportunities to speak to experts. There was possibility to observe as a stakeholder in the Multinational Cyber Defence Education and Training project. In the project assistance to Department Head assisting ACT there were structured interview workshops organised. The role as observer for the CCDCOE in the Project Team Cyber Defence at the EDA gave another opportunity to speak to experts. Even 2 authors of the DCWF could be spoken with. Various experts from universities from different nations and representatives of the NCIA were conversation partners. Furthermore, there was opportunity to speak with the chiefs of NATO NCIRC and EU-CERT.

3.3 Cyber Hygiene Initiative

In late 2015 there was a notification to participate in the prototype presentation for the Cyber Defence Initiative as national representative. After attending that meeting, it seemed, that only writing a report, about that one event, would not be sufficient any more. Interest was woken and further involvement seemed to be interesting. This thesis deals with that and more information is to be found in the Appendices. Initially started as bilateral initiative under the Latvian presidency of the European Union between Estonian and Latvia, soon other nations joined the Initiative. Estonia contracted BHC Lab for the content creation in cooperation with TUT.

3.4 Getting Support

In creating the survey and during first feedback conversations the issue of sensitivity came up. To enable a better participation and reduce the uncertainty at the side of the fillers of the questionnaire, several measures were taken. Estonian MOD was contacted to get support for a thesis and a questionnaire granted. See Appendix 4. Further interviews with BHC Lab, bytelife and CybExer Technologies were conducted to get a better understanding, what problems were still unsolved and to tackle. The basic user training was quite sufficient covered already, but support for the experts-level and outlook to the management-level was appreciated.

3.5 Development and Testing of the Questionnaire

In addition to experts-interviews, a questionnaire was created and tested with the personnel of the CCDCOE to collect more expert-input. 3 test-versions were tested and with the feedback given, the final questionnaire developed and the survey conducted. That enabled an even broader perspective, than solely interviews would have allowed.

3.6 Target Audience

Target audience were several well-known experts and the mailing list of the biggest multinational technical cyber defence exercise in the world: Locked Shields. The expected number of experts to reach with the invitation to fill the survey was 200-250 and with a return quote of 28 the expected 10% [8] return was over expectancy. Filtering out the incomplete answers, still 14 were left and out of these 7 technical specialists from various well known organisations were left, and 2 even would have agreed on getting cited with their name. Answers came from NATO, NCIA, Royal Holloway university, US Airforce, Belgian MOD, Romanian Education Centre DRESMARA, civilian company, and of course the CCDCOE. All participants of the survey are well known experts in their field and combined with the conducted interviews it can be stated that the outcome is well based on expert-knowledge, even when the numbers could have been bigger. Experts in that field are scarce, and most of them are overloaded with their duties. There is high confidence to express what the community of International experts would like to tell the management. It is not a claim to speak for all experts, though.

As additional benefit might be considered that the building of the questionnaire was coordinated with a former expert [62] of the CCDCOE who conducted research and questionnaire for a PHD thesis.

Locked Shields

The Locked Shields [16] is a technical life-fire exercise. It is the biggest and most advanced international live-fire cyber defence exercise in the world. In 2016 20 blue teams defending “their” networks as incident responders were involved in Locked Shields 2016. The exercise is organised each year, since 2010 by the Tallinn-based CCDCOE, and focuses on training the of security experts who protect national IT systems on a daily basis. Over 550 people and a total of 26 nations were involved in Locked Shields 2016. 20 Blue Teams representing 19 nations and NATO Computer Incident Response Capability (NCIRC) participated in the exercise. Some teams were joint teams, which means that nations teamed up. While the organizers of the exercise were gathered in Tallinn, Estonia, the participating Blue Teams had online access to the exercise networks and most worked from their home countries [9].

The Blue Teams are tasked to maintain the networks and services of a fictional country, Berylia under intense pressure. This includes handling and reporting incidents, solving forensic challenges as well as responding to legal, media and scenario injects.

Realistic technologies, networks and attack methods were in the focus of Locked Shields 2016 to stay abreast with market developments. More than 1700 possible attacks were carried out against Blue Teams and over 1500 virtualised systems were deployed during Locked Shields 2016. The virtual Blue Team networks are custom-built and include a variety of services and platforms. For example, the Blue Teams had to maintain several servers, online services and an industrial control system.

Locked Shields 2016 was organised in cooperation with the Estonian Defence Forces, the Finnish Defence Forces, the Swedish Defence College, the British Army, the United States European Command, and numerous other partners [16].

Global Programming and Department Head

The Project of assistance to ACT in their role as Department Head for Cyber Defence gave countless opportunities to speak with international experts in various workshops on those topics. It gave opportunity to speak with experts throughout NATO. The global programming is NATO’s approach to and worldwide (including partners) [63] coordination of education and individual training. The main policies [64] and directives [65] [66] [67] are regulating the education, individual training, collective training and exercises for NATO. At the moment there are negotiations ongoing between ACT and the steering committee [68] of the CCDCOE to transfer the role of the Department Head from ACT to CCDCOE to coordinate all education offers for the NATO field of speciality, called the Discipline: Cyber Defence in NATO.

MNCD

The mission of this project is to fulfil Nations' and NATO's CD E&T shortfalls identified in the GAP analysis that will be performed in cooperation with ACT, in order to support Nations and NATO to comply with NDPP Capability Targets. Offers Allies CD E&T Activities (from strategic to technical level) not available through NATO, national, bilateral or commercial arrangements; contributes to NCIS & Cyber School Capability Building links ACT Gap Analysis with NCIS&CS future activities; promotes NATO Certification high quality of courses and interoperability of experts; Multinational Character greater flexibility and benefits with participation of EU, Industry and Partners [69]

EDA

The European Defence Agency [9] supports the Member States of the European Union and the Council in their effort to improve European defence capabilities in the field of crisis management and to sustain the European Security and Defence Policy as it stands now and develops in the future. They have 3 mission statements:

- supporting the development of European defence capabilities and military cooperation;
- stimulating defence **Research and Technology** (R&T) and strengthening the European defence industry;
- acting as a military interface to EU policies.

EDA acts as a catalyst, promotes collaborations, launches new initiatives and introduces solutions to improve defence capabilities. It is the place where Member States willing to develop capabilities in cooperation do so. It is also a key facilitator in developing the capabilities necessary to underpin the Common Security and Defence Policy of the Union [70]. One of their capability programmes deals with Cyber Defence and aims at technology and education [3]. As representative of the CCDCOE as observer to the Project Team Cyber Defence, it was also an opportunity to speak to high level representatives, that are usually hard to reach for interviews.

CyCon

The International Conference on Cyber Conflict is organised by the NATO Cooperative Cyber Defence Centre of Excellence. Every year, over 500 decision-makers and experts from government, military and industry from all over the world approach the conference's key theme from legal, technology and strategy perspectives, often in an interdisciplinary manner. CyCon 2017 will focus on the fundamental aspects of cyber security with a theme of *Defending the Core.* The 9th International Conference on Cyber Conflict will be held in Tallinn May 30 through June 2, 2017 [6].

4 Implementation

With a target audience for the survey spread over the globe, it was an obvious conclusion to use automated tools for collecting the needed data with the survey. There are plenty of tools available, but surveymonkey is mentioned in almost every overview of tools [25] [69]. That was one reason to choose surveymonkey. The most practical reason to use surveymonkey was, that it is already in use at the CCDCOE for collecting all kinds of feedback, especially from the Courses, the CCDCOE offers.

After the test run with the ILIAS-based awareness-training, there will be follow-on activity with a new 3 years EDA contract for further improving the Cyber Hygiene Initiative together with the joint-venture CybExer Technologies.

During the Pilot-iteration of a high-level seminar at the CCDCOE end of November 2016, results were already implemented on a General-rank-level-course, that also was attended from the Ambassadors of Austria and Ireland to the Republic of Estonia. Their Feedback is also implemented in the Executive Summary.

Different approaches to education were also discussed during CyCon, e-learning was part of that discussion [72].

4.1 Development and Testing of Questionnaire

Over the timeframe from march to August 2016 3 versions of a questionnaire were tested, based on interviews, with written and oral feedback the final version was created in August 2016.

Several interviews were conducted with the representative from the Estonian Defence Forces, MSc student in parallel and responsible for the implementation of the Cyber Hygiene Initiative to the Estonian Defence Forces. He gave a lot of valuable feedback for the questionnaire, already reflecting the feedback he was receiving.

Various experts gave valuable input. To just name a view Wolfgang Röhrig Project Officer from the European Defence Agency, Paulo Nunes the Project Lead from the NATO Smart Defence project MNCD Multinational Cyber Defence project for education and training, Stefanie Shively from the US Ministry of Defence, working on the DCWF Development of a capable cyber workforce, the draft for the NIST standard was just released on time in November 2016 [6].

After the development of the test-versions Draft in March 2016, Version 0.5 in April 2016 and Version 0.8 in July 2016 of the questionnaire and testing with the personnel of the CCDCOE, the questionnaire Version 1.0 was separated in the main questionnaire with the relevant questions for the thesis and additional questions in August 2016, that were identified as still interesting for the CCDCOE, but without direct impact for the thesis. All together 55 questions were asked in the final questionnaire.

A grouping of questions to topics seems to be possible and the results will be presented according to that grouping.

Grouping of the questions, as far as applicable, is presented in Table 1.

Table 1 Grouping of survey questions

grouping	Question number
target audience verification	1
comfort creation and personal data	2, 54, 55
Education	3, 43
Experience, ability	7, 8, 11, 12, 13
perceived threats and policies	4, 6
confidence, self-discipline and validation	5, 26, 27, 28, 39, 40, 41,
workload	10
circumstances allowing collaborative behaviour and testing	29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 42, 44, 45, 46, 47, 48
advice and optional proposals to the management	23, 25, 53
“current success” in reporting:	26
motivation, demotivation, danger of losing experts	9, 49, 50, 51, 52
outsiders	20
Initiative specific	21, 22
“What is at stake?”: cooperation success and danger in (critical infrastructure) protection (risk and risk management)	14, 15, 16, 17, 18, 19

4.2 Presentation of Main Results

The main audience was foreseen to be the technical specialist. Still the majority was feeling they belong to the management. It seems to be fair to assume that this is not that kind of management, that is responsible for implementation of basic user training now. But time goes by and if in the future, they will have higher positions, and keep in mind there was this survey once,

one of the objectives of this thesis: to increase awareness, was reached already.

The target audience could be reached, even when management numbers were higher, nevertheless valuable information for what and how to report from the specialist level to the management was collected.

Personal data was given quite often, so it is concluded that comfort creation was well received. The rate of people stopping to fill, during filling the questionnaire was lower as expected, with a questionnaire containing 55 questions [73].

Education was quite high, but that was expected, due to aiming at specialists. The average was far over the average in the population [74].

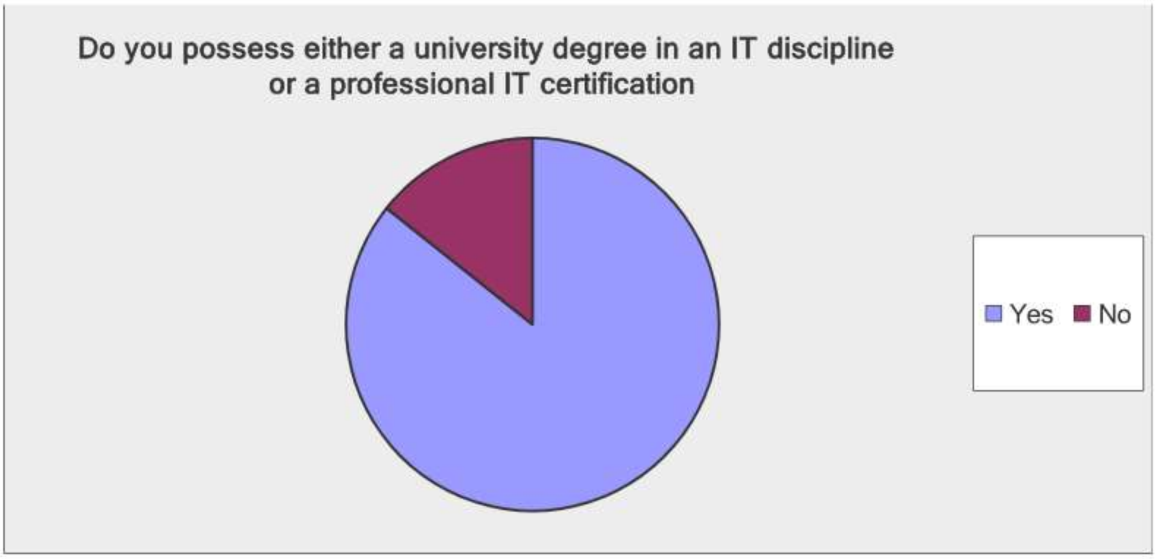


Figure 2 education of the specialists

Even when the education is quite high already, the specialists are willing to continue learning. The way they want to do it, is shown in the following Figure 3.

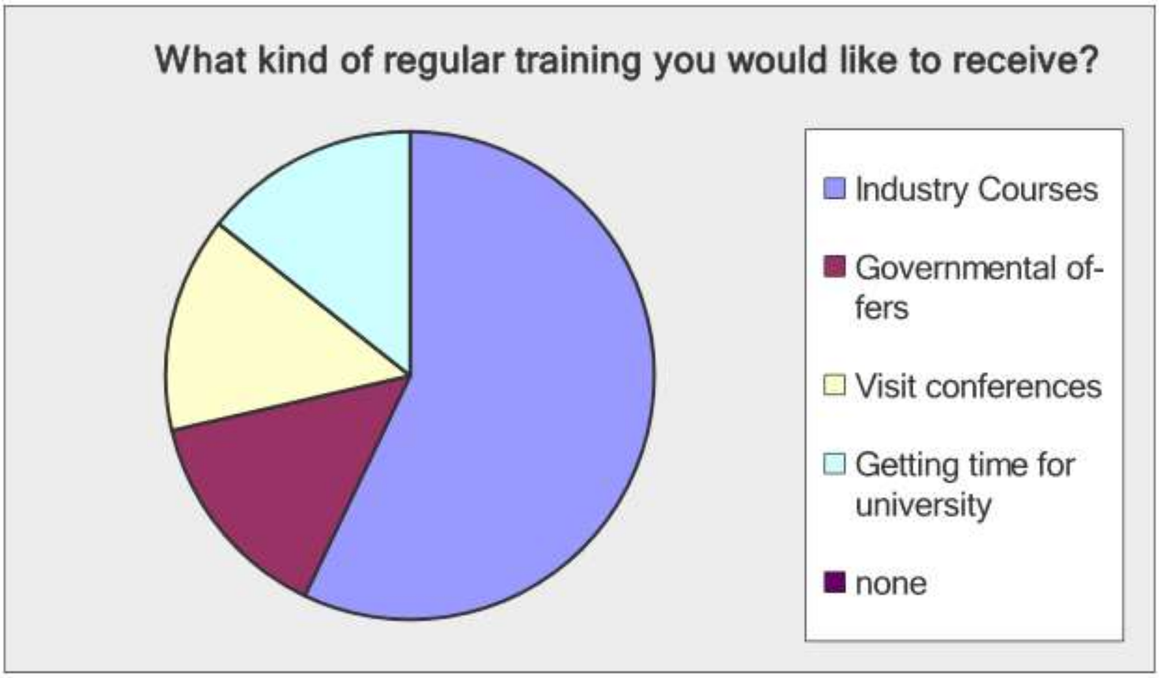


Figure 3 specialists training preferences

The answers about experience and ability show that the respondents were highly experienced, able and honest in their answers.

The perceived threats and policies are mainly congruent with research of Antivirus vendors of what to expect in the future [75].

The respondents showed that they are aware of the importance of self-discipline and mainly show confidence and self-discipline [76].

The respondents mainly stated that the workload does not allow a proper inspection of the traffic in their organisations. That can have devastating consequences [77].

Most of the respondents show that they would value circumstances allowing collaborative behaviour and testing, but also that they are sometimes not even allowed to conduct testing [78] [79]. That will be shown in Figure 4.

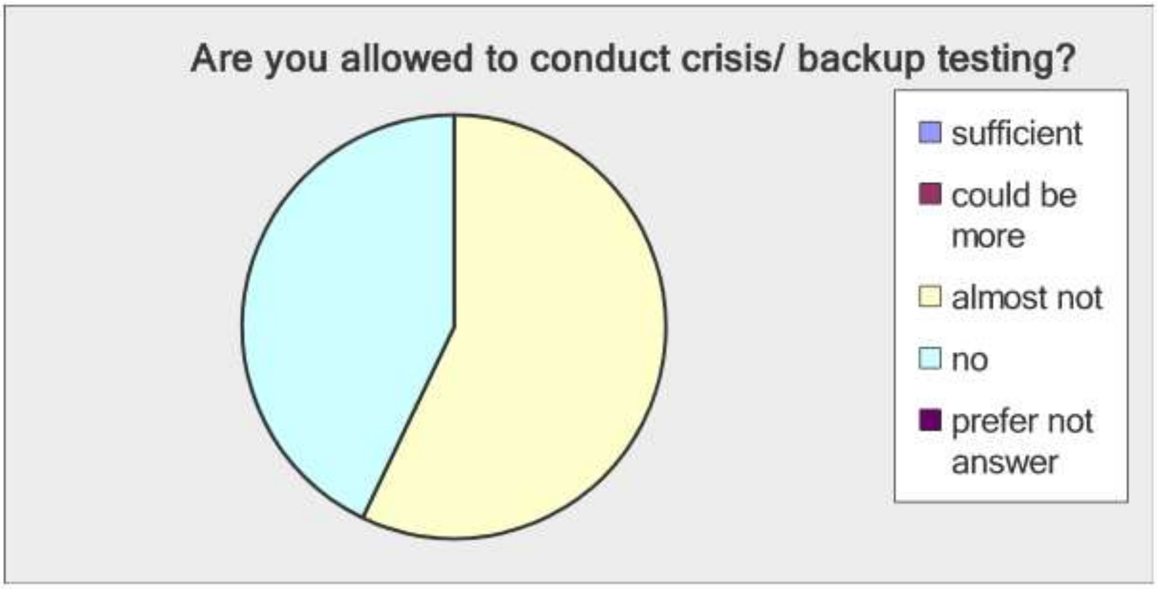


Figure 4 specialists answer if they are allowed to conduct testing

The advice and optional proposals to the management are presented in the Executive summary and all the proposals can be seen in Appendix 5

“Current success” in reporting to the management was surprisingly well perceived. Why there is still struggle to implement all the proposals, has to be content of future work.

The majority of specialists either answered that there is a chance that they might change to a better paid position in the economy, or did not want to answer. That is one of the main indicators, that either salaries for experts should be raised, or at least the treatment should be excellent to avoid the risk of losing them. This will be shown in Figure 5.

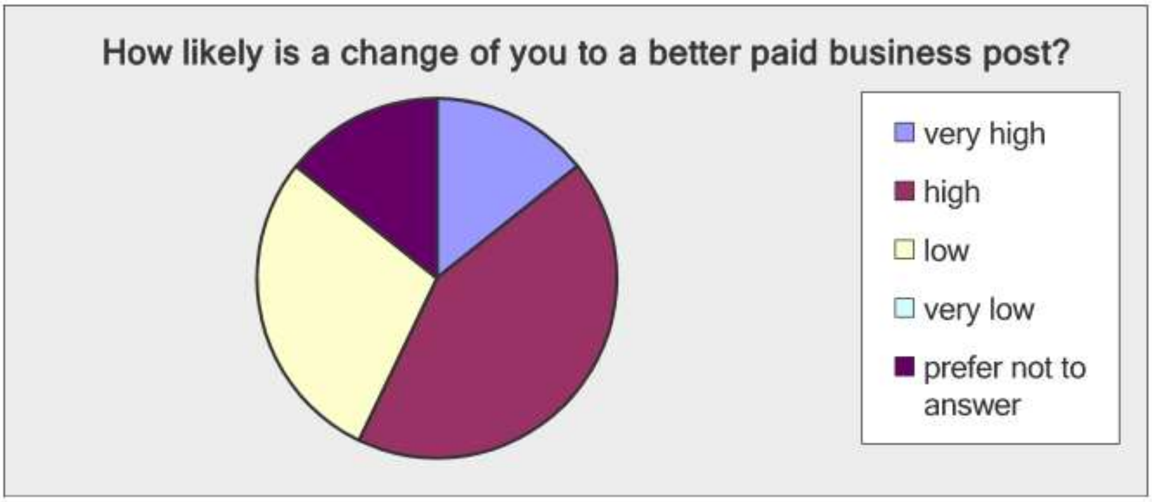


Figure 5 likeliness of specialists changing in a better paid business position

The majority of the respondents think, that outside of the professional environment, only about 25% of the population understand the basics of computers and computer security. That indicates that the education systems are not yet delivering what the people need to survive in a digital society [80].

More than half of the respondents have heard about the Cyber Hygiene Initiative before the survey and the majority welcomes the narration based approach.

There seems to be a good awareness under the respondents about "What is at stake?": co-operation success and dangers in critical infrastructure protection is highly spread. Future work should guarantee, that this risks are mirrored in Cyber security strategies [81].

Figure 6 shows the answers to the question 1: Please rate which group you think you belong to.

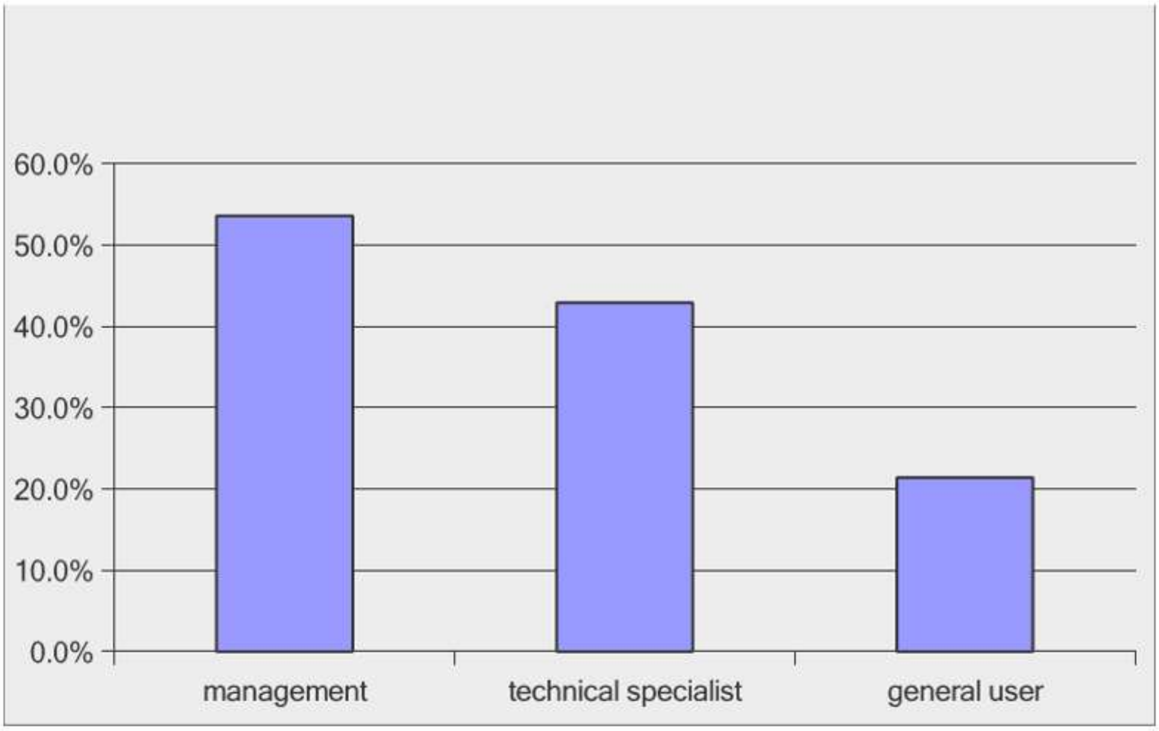


Figure 6 perceived groups of participants

It seems to be obvious from the table, but it shall still be mentioned, that multiple answers were possible to this question. The following figures in this chapter are filtered for complete and specialist results, that means it shows only the data from the respondents, that declared themselves as specialist and the questionnaires were filled completely. When deviating from it, it will be mentioned. In the following figures the filtered results are shown. 3 out of seven 7 specialists are also tasked with management tasks.

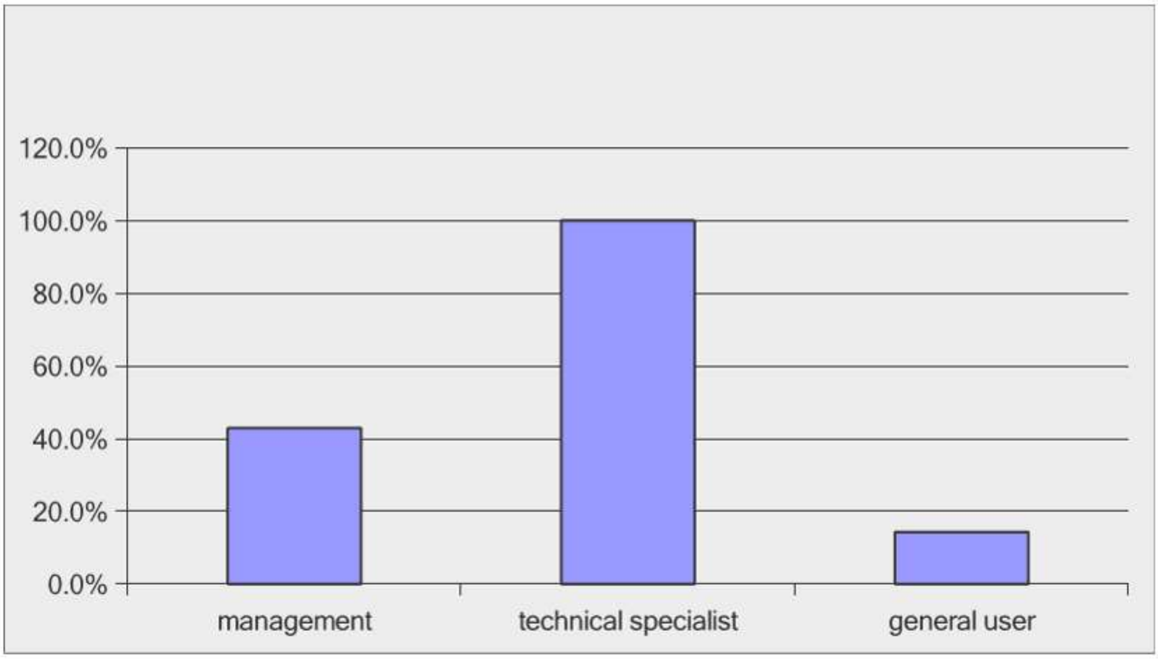


Figure 7 survey data filtered for specialists

All results are available in Appendix 5. The last 2 questions, question 54: Respondent details containing personal data will be removed. Question 55: Do you agree to get cited with your name, was consequently removed also, even when 2 respondents would have agreed to that.

Most the experts hold a university degree or certification. Interestingly, that is not the case with management positions.

Experience and Ability

Interesting is that the specialists rate other specialists and themselves as very good or good. The fact, that they grade the specialists in their organisation even higher as themselves, show some modesty and honesty and let conclude, that the answers were given quite open and frankly. Figure 8 shows the perceived quality of experts. The answers from the filtered for completeness and being specialist to question 7: How would you rate the quality (character, willingness to work and further educate themselves) of the IT security *personnel* that is currently in place? For simplicity reasons, the categorisation of answers, or the categories of agreement, were kept as often as possible, throughout the questionnaire, to avoid confusion at the respondent, and was direct outcome of the feedback from testing. Strongly agree can be understood as rated as very good, following that logic.

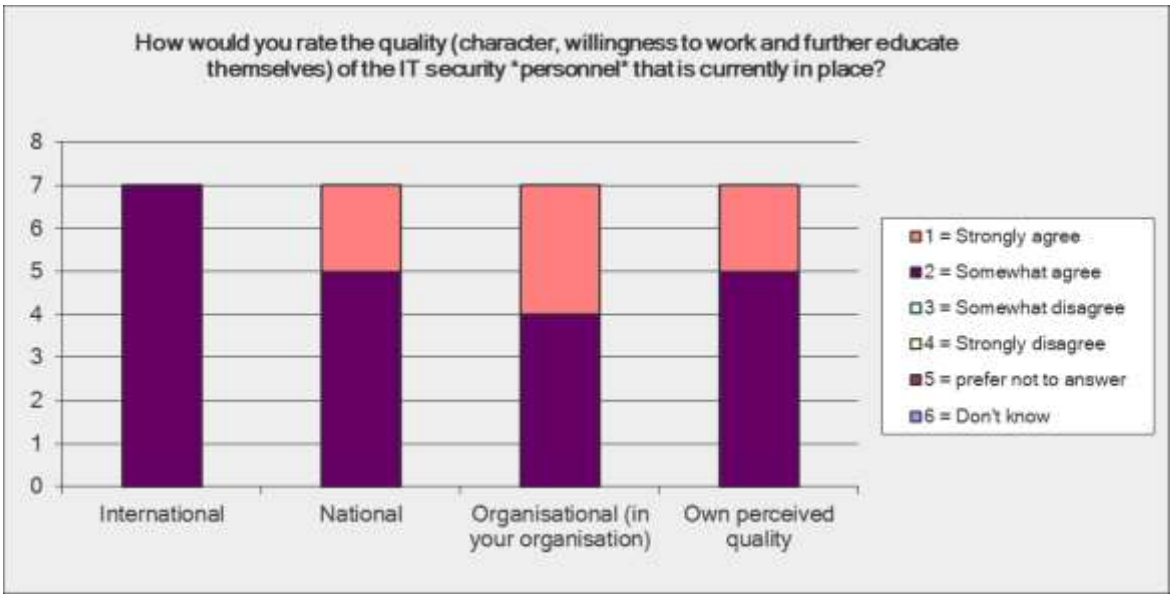


Figure 8 quality of personnel

The impression of honesty in the answers is even deepened in the answers to the perceived own skill-set available. The further questions for experience also shows that experts were reached, 57% were even involved in a cyber intrusion investigation and 2 even in a court case, almost all state they are having contacts to a CERT.

Other relevant Findings

The ranking of threats also shows that these experts mainly come to the same conclusions like vendors for security solutions [23] [65] [83].

The main findings and conclusions are densed in an Executive summary, that you find in the following chapter. Conversations and semi-structured interviews with experts and high-level decision-makers gave the advice to keep it as short as possible. The vice-chancellor of the Republic of Austria gave that advice also, when I had the chance to discuss the idea with him, during a visit of a presidential visit with a delegation to Estonia at a time, where he still was minister.

Executive Overview to the Management

- Define for yourself what makes an expert for you and your organisation. Indicators can be:
    - university degree
    - certificates
    - courses
    - knowledge
    - skills
    - attitude
    - experience
    - testing, yes/ no

    - There is no right or wrong. They have to fulfil their tasks, and you have to be sure they're doing the right things in the right way.

- Once you got experts in your organisation: treat and pay them right, otherwise you might lose them.
- Experts have to learn a lot, that usually means they are highly intrinsically motivated. Keep them motivated.
- Regularly train your employees, and your experts. Experts want to be on the cutting edge, allow them to courses of industry, even when they are expensive. Malfunction could be even more expensive.
- Make sure their work-load is right.
- Ensure they feel their work is meaningful.
- Ask the right things for reporting.
  - in the form and frequency most suitable for you.
  - Explain why the reporting is important
    - No reporting for the sake of doing it, ask your employees, so they feel valued and their participation gives them a feeling of appreciation. According to this survey data that could be asked:
      - Basic training participation (min. annually)
      - number of incidents in comparison with former period
        - choose period wisely and according to your organisation, minimum annually, or quarterly, monthly, weekly, daily
      - shortfalls
      - number of requests for new functionality
- Give clear guidance for situations where workarounds are appropriate and where not. (Enable mission commander to deviate, but in a guided manner. Missions themselves are a high-risk event, risk management has to take the higher level of risk-acceptance into account)
- Policies should include acceptable times for implementing new functionalities
- Have a process for improvement proposals from the employees to be noticed and heard.
  - Consider awards for good proposals. Keep motivation up.
- Give clear guidance for prioritisation
- Balance business needs with security
  - risks can also be accepted, when the potential gain justifies it, but highest level has to decide, or at least give guidance
- Allow, enable and conduct crisis and recovery testing. The outcome might be horrible, but a real crisis might be even worse. Find your right frequency (min. annually).
- Scenarios to train:
  - social engineering like e-mail fishing campaigns

  - security audits
  - power outage
  - server breakdown
  - break-in attempts
  - phone system is not working.
- Create a good culture of communication in your organisation.
- Risk management is a high management/ leadership responsibility.
  - Be sure to give priorities according to the business needs.
- Resources have to be sufficient for the given priorities.
- Further improve reporting
  - Ask your employees what they want to report /what they want you to know
  - automatise reporting
  - continuously improve reporting better metrics for main security areas
  - benchmarking
  - take losses into account, financial and reputational

MOD is the last resort of a state, so there have to be differences to firms. For a state, it is just no option to stand still and let an insurance jump in and pay for the damage, so there must be differences in crisis management and in preparation for it, and how much of the budget can be spent for that. The 2 % of the GDP that NATO asks, is still lower than the proposals from a 2.24% that are proposed for an average family in America for insuring your belongings [84].

5 Conclusions

It seems to be good practice to cite a wise man from the past in the field of Cyber Security. This chance shall be used. The threats, risks and opportunities may seem endless and new, but already over 2500 years ago, the people were confronted with endless numbers: “There are not more than five cardinal tastes (sour, acrid, salt, sweet, bitter), yet combinations of them yield more flavours than can ever be tasted.” [41]

This thesis mainly answered the most important research questions, that were identified in interviews with experts, literature research, the conducted survey and the conclusions drawn from it. For the reporting, it gives proposals, what the specialists see as important, and they think the management should know. It is on the gouvernance and management now, to validate, and give guidance in what form and frequency they want to be informed. Due to their responsibilities for risk management and accounting, they should at least be interested.

5.1 Main Questions

The main questions that should be answered were:

What statistical Data to collect?

Basic training participation (min. annually)

- number of incidents in comparison with former period
  - choose period wisely and according to your organisation, minimum annually, or quarterly, monthly, weekly, daily
- shortfalls
- number of requests for new functionality

What to report?

That has to be determined by the management in cooperation with their specialists and their employees. The more involvement the employees and specialists sense, the higher their motivation will remain. All employees have their role in recognising break-in attempts, social engineering, or recognising, if a system, like the phone system is not working and to know where to report unusual events. A proposal from expert’s perspective is offered.

What are the biggest Threats?

Abuse of vulnerabilities, that comes with the technology. It is a never-ending challenge for security personnel. Security is a process, not a product [85].

In ranking out of this survey, the experts rank following as top 5

Bring your own device BYOD

Spread of malware through removable media

Abuse of authentication mechanisms (e.g. weak passwords)

Abuse of wireless access points

Social engineering

Following the 6 seemingly most urgent quotes are given

As one of the respondents phrased it: “If these above impediments are getting in my way and I cannot change them I will leave. There is not shortage of demand.”

Besides the opportunity to comment on all questions,

Question 53 was dedicated to collect additional input: If you could advise your national leadership, what specific recommendations would you have to help your government or organisation to achieve a higher level of cyber security?

“Educate the management to understand security. See security as part of business/governance process, not as an independent silo that dictates rules without consideration for its impact on business.”

“Start with cyber risk management at the highest level in order to ensure that the critical assets have been properly defined so that policies, controls and priorities can be defined in line with business/operational needs.”

“Everyone should have a basic understanding of cyber security. It is not just a matter for technical people. The government's current initiatives are doing well in this area (education and awareness) and should continue.”

“Be honest about the "inconvenience" of maintaining good cyber security. On the business side the need to improve security systems, and on the general population side, the need to keep more personal information private.”

“National Cyber-Awareness Centre including ALL Stakeholder from the public sector with participation from the private sector (CI).”

The Final Question

But how to do it? What statistical data to collect, and what and how to report to the management?

This was the goal of this thesis and there is hope it provides answers to the problems stated in the Introduction. The further development of the Cyber Hygiene Initiative will show how successful the implementation of a system, that trains all users, gives the specialists the data that are important, and finally find a channel to the management, to tell the bad news, that sometimes it seems nobody wants to bring or receive.

5.2 Call for Action

The specialists view is given. Not really for the 1st time. It is now on decision-makers and management to implement the proposals. The top-level support was given at the Warsaw-summit [86] including the Cyber Defence pledge. The 2nd row has to act now. No further excuses should be found. The political will took too long to build, but now it is articulated and signed.

In case the knowledge how to implement this measures is not there, build it up, or delegate to proper personnel as soon as possible.

5.3 Future Work

Future work and latest developments are presented in this subchapter.

In the last interview in the beginning of November 2016 with BHC Lab [39], bytelife [40] and CybExer Technologies [41] it was told that a three years’ contract with EDA was entered to further develop the programme and a transition away from ILIAS to a new to develop platform is considered. The validation of that new approach is for sure a promising topic for further research.

The results of the questionnaire that was conducted as additional questions should be further researched.

More feedback from the experts' community and research on the management-level how to convince them to implement best practices, benchmarking and implementation of new developments.

"Current success" in reporting to the management was surprisingly well perceived. Why there is still struggle to implement all the proposals has to be content of future work.

What management really wants to know and what happens with reports are for sure an interesting topic for future research.

There seems to be a good awareness under the respondents about "What is at stake?": cooperation success and dangers in critical infrastructure protection is highly spread.

But for some reasons governments sometimes struggle with the implementation. Those reasons should be addressed in future research.

6 References

[1] NATO, “Allied Command Operations (ACO).” [Online]. Available: http://www.nato.int/cps/en/natohq/topics_52091.htm. [Accessed: 26-Nov-2016].

[2] “NCI Agency - Cyber Security.” [Online]. Available: https://www.ncia.nato.int/Our-Work/Pages/Cyber-Security.aspx. [Accessed: 27-Nov-2016].

[3] B. Curtis, B. Hefley, and S. Miller, “People capability maturity model (P-CMM) version 2.0,” 2009.

[4] “Isaca, COBIT: A Business Framework for the Governance and Management of Enterprise IT. 2013.”

[5] “Home.” [Online]. Available: http://www.coso.org/. [Accessed: 29-Nov-2016].

[6] “Cycon | Agenda.” [Online]. Available: https://ccdcoe.org/cycon/agenda.html. [Accessed: 23-Nov-2016].

[7] “DRESMARA.” [Online]. Available: http://www.dresmara.ro/index_en.html. [Accessed: 27-Nov-2016].

[8] “Allied Command Transformation.” [Online]. Available: http://www.act.nato.int/. [Accessed: 26-Nov-2016].

[9] “European Defence Agency.” [Online]. Available: https://www.eda.europa.eu/. [Accessed: 27-Nov-2016].

[10] “EUROPA - European Union website, the official EU website.” [Online]. Available: https://europa.eu/european-union/index_en. [Accessed: 26-Nov-2016].

[11] “LexUriServ.do.” [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:081:0053:0056:DE:PDF. [Accessed: 26-Nov-2016].

[12] “What is EuroSox - WhatisEuroSox.pdf.” [Online]. Available: http://www.copenhagencompliance.com/eurosox/WhatisEuroSox.pdf. [Accessed: 23-Nov-2016].

[13] “ILIAS E-Learning.” [Online]. Available: http://www.ilias.de/docu/goto_docu_root_1.html. [Accessed: 27-Nov-2016].

[14] “Information Technology - Information Security – Information Assurance | ISACA.” [Online]. Available: https://www.isaca.org/Pages/default.aspx?cid=1002083&Appeal=SEM&gclid=CM2N0aWjx9ACFUtkGQodE_wP_Q. [Accessed: 26-Nov-2016].

[15] “IT Baseline Security System ISKE - Estonian Information System Authority.” [Online]. Available: https://www.ria.ee/en/iske-en.html. [Accessed: 26-Nov-2016].

[16] “Locked Shields 2016,” Apr-2016. [Online]. Available: https://www.ccdcoe.org/locked-shields-2016. [Accessed: 26-Nov-2016].

[17] NATO, “Military Committee (MC).” [Online]. Available: http://www.nato.int/cps/en/natohq/topics_49633.htm. [Accessed: 26-Nov-2016].

[18] “MNCDET.” [Online]. Available: http://www.mncdet-pt.net/. [Accessed: 26-Nov-2016].

[19] NATO, “North Atlantic Council (NAC).” [Online]. Available: http://www.nato.int/cps/en/natohq/topics_49763.htm. [Accessed: 26-Nov-2016].

[20] NATO, “NATO - Homepage,” *NATO*, 2015. [Online]. Available: http://www.nato.int/. [Accessed: 26-Nov-2016].

[21] “NCI Agency.” [Online]. Available: https://www.ncia.nato.int/Pages/homepage.aspx. [Accessed: 27-Nov-2016].

[22] “BSI - The BSI.” [Online]. Available: https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html. [Accessed: 26-Nov-2016].

[23] “The National Initiative for Cybersecurity Education (NICE).” [Online]. Available: http://csrc.nist.gov/nice/framework/. [Accessed: 21-Nov-2016].

[24] NATO, “Defence Planning Process.” [Online]. Available: http://www.nato.int/cps/en/natohq/topics_49202.htm. [Accessed: 27-Nov-2016].

[25] “National Institute of Standards and Technology | NIST.” [Online]. Available: https://www.nist.gov/. [Accessed: 26-Nov-2016].

[26] “SHAPE | SHAPE.” [Online]. Available: http://www.shape.nato.int/. [Accessed: 26-Nov-2016].

[27] “Sarbanes-Oxley Act of 2002 - soa2002.pdf.” [Online]. Available: https://www.sec.gov/about/laws/soa2002.pdf. [Accessed: 26-Nov-2016].

[28] “Homepage < Tallinn University of Technology.” [Online]. Available: http://ttu.ee/en/. [Accessed: 26-Nov-2016].

[29] “NATO Cooperative Cyber Defence Centre of Excellence.” [Online]. Available: https://ccdcoe.org/. [Accessed: 26-Nov-2016].

[30] “CERT Estonia.” [Online]. Available: https://www.ria.ee/en/cert-estonia.html. [Accessed: 26-Nov-2016].

[31] “CERT-EU News Monitor.” [Online]. Available: https://cert.europa.eu/cert/plainedition/en/cert_about.html. [Accessed: 26-Nov-2016].

[32] “PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf.” [Online]. Available: https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf. [Accessed: 28-Nov-2016].

[33] “ISO - International Organization for Standardization.” [Online]. Available: http://www.iso.org/iso/home.html. [Accessed: 29-Nov-2016].

[34] “BSI - IT-Grundschutz.” [Online]. Available: https://www.bsi.bund.de/EN/Topics/IT-Grundschutz/itgrundschutz_node.html.

[35] “International Organization for Standardization, Information technology Security techniques Code of practice for information security controls. 2014, p. 11,12.”

[36] RIA, “RIA kyberturbe ylevaade 2012,” 2016. [Online]. Available: https://www.ria.ee/public/publikatsioonid/EISA_on_Cyber_Security_2012.pdf. [Accessed: 23-Nov-2016].

[37] “Sarbanes Oxley 101: SOX Compliance Requirements for 302, 404, 906.” [Online]. Available: http://www.sarbanes-oxley-101.com/. [Accessed: 23-Nov-2016].

[38] “SOX302404Strategies.” [Online]. Available: https://www.sec.gov/rules/proposed/s74002/card941503.pdf. [Accessed: 23-Nov-2016].

[39] “Cybersecurity WORKFORCE DEVELOPMENT TOOLKIT - cybersecurity workforce development toolkit.pdf.” [Online]. Available: https://niccs.us-cert.gov/sites/default/files/documents/pdf/cybersecurity workforce development toolkit.pdf?trackDocs=cybersecurity workforce development toolkit.pdf. [Accessed: 21-Nov-2016].

[40] V. Lipman, “7 Management Practices That Can Improve Employee Productivity.” [Online]. Available: http://www.forbes.com/sites/victorlipman/2013/06/17/7-management-practices-that-can-improve-employee-productivity/. [Accessed: 21-Nov-2016].

[41] S. Tzu, “The art of war,” West view press, 1994.

[42] S. Boeke, “First Responder or Last Resort ? The role of the Ministry of Defence in national cyber crisis management countries,” no. September, 2016.

[43] A. Sumin, “Evaluation Methodology for Cyber Awareness Course,” Tallinn University of Technology, 2016.

[44] “Mitnick, D. K., Simon, L. W. The art of deception. Wiley publishing, Inc., Indiana: 2012.”

[45] D. D. S. Medina, “Information Security Awareness Web-based Courses Assessment,” 2016.

[46] I. Veseli, “Measuring the Effectiveness of Information Security Awareness Program,” Gjøvik University College, 2011.

[47] N. A. G. Arachchilage, “Security Awareness of Computer Users: A Game Based Learning Approach,” School of Information Systems, Computing and Mathematics Brunel University, 2012.

[48] F. Malik, “Managing Performing Living Effective Management for a New World,” Campus, 2015.

[49] geolounge, “Fortune 1000 Companies List for 2015,” Jul-2015. [Online]. Available: https://www.geolounge.com/fortune-1000-companies-list-for-2015/. [Accessed: 04-Dec-2016].

[50] “5 Solutions to Performance Management Challenges | CEB Blogs.” [Online]. Available: https://www.cebglobal.com/blogs/5-reasons-your-performance-management-is-a-failure/. [Accessed: 29-Nov-2016].

[51] C. Poelma, “Analyzing the Science Behind Customer Loyalty,” May-2016. [Online]. Available: https://www.entrepreneur.com/article/272038. [Accessed: 29-Nov-2016].

[52] “10 Studies That Reveal What Customers WANT You To Know About Them.” [Online]. Available: https://blog.kissmetrics.com/what-customers-want/. [Accessed: 29-Nov-2016].

[53] “Corine Noordhoff, Pieter Pauwels, Gaby Odekerken-Schröder, (2004) ‘The effect of customer card programs: A comparative study in Singapore and The Netherlands’, International Journal of Service Industry Management, Vol. 15 Iss: 4, pp.351 - 364.” .

[54] S. Magids, A. Zorfas, and D. Leemon, “The New Science of Customer Emotions,” Nov-2015. [Online]. Available: https://hbr.org/2015/11/the-new-science-of-customer-emotions. [Accessed: 29-Nov-2016].

[55] “ISO 27000 - ISO 27001 and ISO 27002 Standards.” [Online]. Available: http://www.27000.org/. [Accessed: 01-Dec-2016].

[56] P. Corey, “NIST General Information,” Dec-2008. [Online]. Available: https://www.nist.gov/director/pao/nist-general-information. [Accessed: 29-Nov-2016].

[57] “Final Rule: Management’s Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports; Rel. No. 33-8238.” [Online]. Available: https://www.sec.gov/rules/final/33-8238.htm#iib3a. [Accessed: 29-Nov-2016].

[58] “Cobit 5.” [Online]. Available: http://www.isaca.org/cobit/Pages/CobitFramework.aspx. [Accessed: 29-Nov-2016].

[59] “Business Technology Management - IT Governance Framework - Val IT | ISACA.” [Online]. Available: http://www.isaca.org/knowledge-center/val-it-it-value-delivery-/pages/val-it1.aspx. [Accessed: 29-Nov-2016].

[60] “Risk IT Framework for Management of IT Related Business Risks.” [Online]. Available: http://www.isaca.org/knowledge-center/risk-it-it-risk-management/pages/default.aspx. [Accessed: 29-Nov-2016].

[61] “laws_estonia_en.pdf.” [Online]. Available: http://ec.europa.eu/health/ehealth/docs/laws_estonia_en.pdf. [Accessed: 29-Nov-2016].

[62] “Strategic_Cyber_Security_K_Geers.PDF.” [Online]. Available: https://ccdcoe.org/publications/books/Strategic_Cyber_Security_K_Geers.PDF. [Accessed: 27-Nov-2016].

[63] NATO, “Partners.” [Online]. Available: http://www.nato.int/cps/en/natohq/51288.htm. [Accessed: 27-Nov-2016].

[64] “MC 458/3 NATO policy on Education and Training.” .

[65] “Bi-SC 75-2 NATO Education, Training, Exercise and Evaluation Directive.” .

[66] “Bi-SC 75-3 NATO Exercise Directive.” .

[67] “Bi-SC 75-7 NATO Education and Individual Training Directive.” .

[68] “Structure,” May-2014. [Online]. Available: https://www.ccdcoe.org/structure-0. [Accessed: 27-Nov-2016].

[69] “MNCD outline.” [Online]. Available: http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2014_10/20141029_141020-8_Nunes.pdf. [Accessed: 27-Nov-2016].

[70] “Mission.” [Online]. Available: https://www.eda.europa.eu/Aboutus/Missionandfunctions. [Accessed: 27-Nov-2016].

[71] “Survey Research Tools :: Institutional Research :: Swarthmore College.” [Online]. Available: http://www.swarthmore.edu/institutional-research/survey-research-tools. [Accessed: 23-Nov-2016].

[72] “BPG_06_Internet-Based_Research.” [Online]. Available: http://www.admin.ox.ac.uk/media/global/wwwadminoxacuk/localsites/curec/documents/BPG_06_Internet-Based_Research.pdf. [Accessed: 23-Nov-2016].

[73] “How Much Time are Respondents Willing to Spend on Your Survey? | SurveyMonkey Blog,” Feb-2011. [Online]. Available: https://www.surveymonkey.com/blog/2011/02/14/survey_completion_times/. [Accessed: 27-Nov-2016].

[74] “Educational attainment statistics - Statistics Explained.” [Online]. Available: http://ec.europa.eu/eurostat/statistics-explained/index.php/Educational_attainment_statistics. [Accessed: 27-Nov-2016].

[75] “Kaspersky Personal & Family Security Software.” [Online]. Available: http://usa.kaspersky.com/. [Accessed: 23-Nov-2016].

[76] “MAGTOO_FINAL.” [Online]. Available: http://dspace.ut.ee/bitstream/handle/10062/1315/noorveelembi.pdf. [Accessed: 27-Nov-2016].

[77] “Workload and Performance of Employees.” [Online]. Available: http://journal-archieves8.webs.com/256-267.pdf. [Accessed: 27-Nov-2016].

[78] “Employee motivation and organizational performance.” [Online]. Available: ftp://ftp.repec.org/opt/ReDIF/RePEc/rse/wpaper/R5_5_DobreOvidiuIliuta_p53_60.pdf. [Accessed: 27-Nov-2016].

[79] B. et al Mathews P., “European quality management practices: The impact of national cultures.”

[80] E. Dyson, “Release 2.0: A Design for Living in the Digital Age,” Broadway Books, 1997.

[81] “Cyber Security Strategy Documents,” Jun-2014. [Online]. Available: https://www.ccdcoe.org/strategies-policies. [Accessed: 27-Nov-2016].

[82] Cassie, “Top Online Security Threats of 2015,” Jul-2015. [Online]. Available: https://securethoughts.com/top-online-security-threats-of-2015/. [Accessed: 23-Nov-2016].

[83] Cisco, “Midyear Cybersecurity Report,” 2016.

[84] “The Average Budget Percentage for Home Insurance.” [Online]. Available: http://finance.zacks.com/average-budget-percentage-home-insurance-11552.html. [Accessed: 29-Nov-2016].

[85] “Essays: The Process of Security - Schneier on Security.” [Online]. Available: https://www.schneier.com/essays/archives/2000/04/the_process_of_secur.html. [Accessed: 30-Nov-2016].

[86] NATO, “Warsaw Summit Communiqué - Issued by the Heads of State and Gov ernment participating in the meeting of the North Atlantic Council in Warsaw, 8-9 July 2016.” [Online]. Available: http://www.nato.int/cps/en/natohq/official_texts_133169.htm. [Accessed: 27- Nov-2016].

Appendix

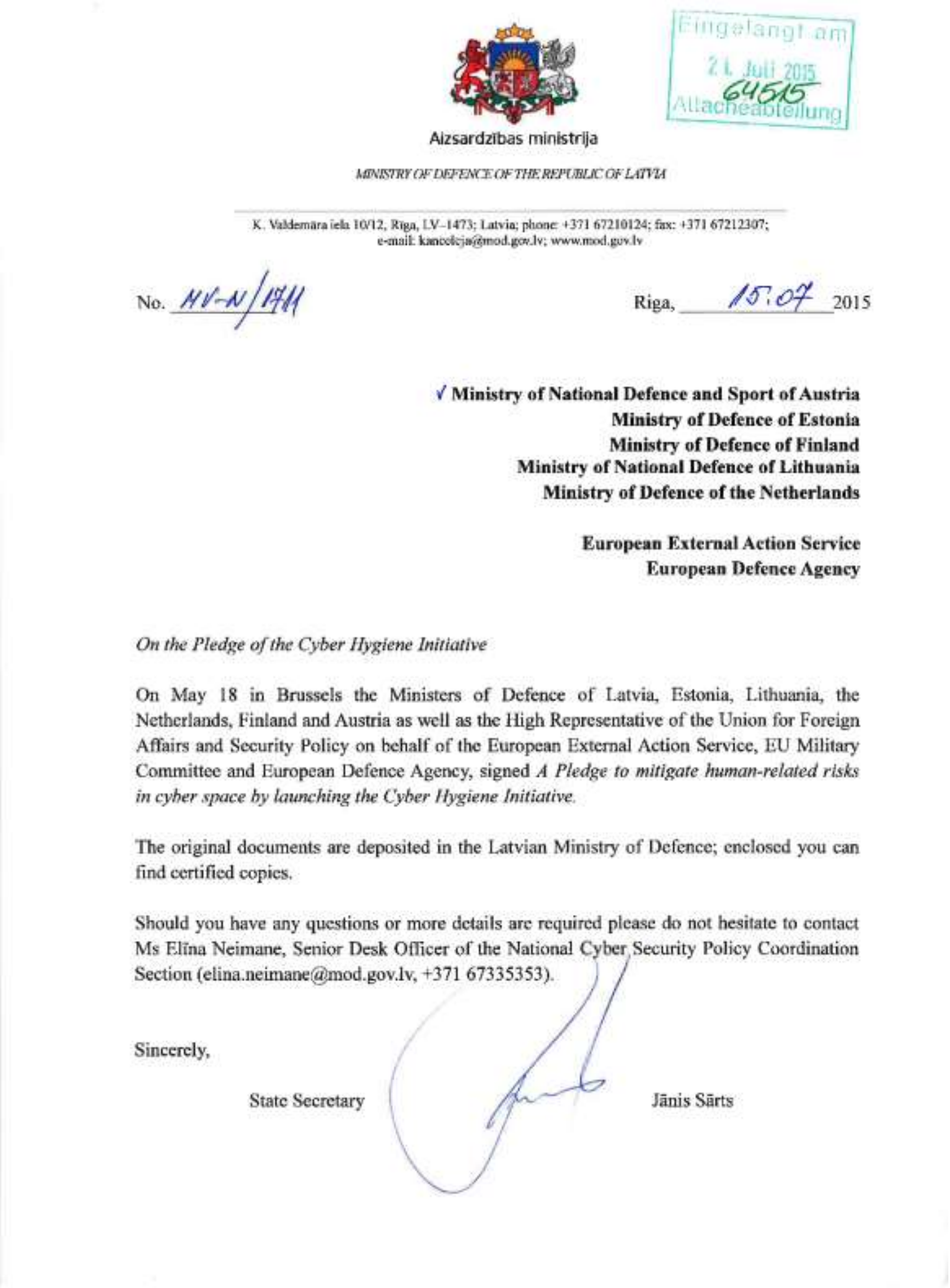
I. Executive Overview to the management

- Define for yourself what makes an expert for you and your organisation. Indicators can be:
    - university degree
    - certificates
    - courses
    - knowledge
    - skills
    - attitude
    - experience
    - testing, yes/ no
        - There is no right or wrong. They have to fulfil their tasks, and you have to be sure they're doing the right things in the right way.
- Once you got experts in your organisation: treat and pay them right, otherwise you might lose them.
- Experts have to learn a lot, that usually means they are highly intrinsically motivated. Keep them motivated.
- Regularly train your employees, and your experts. Experts want to be on the cutting edge, allow them to courses of industry, even when they are expensive. Malfunction could be even more expensive.
- Make sure their work-load is right.
- Ensure they feel their work is meaningful.
- Ask the right things for reporting.
    - in the form and frequency most suitable for you.
    - Explain why the reporting is important
        - No reporting for the sake of doing it, ask your employees, so they feel valued and their participation gives them a feeling of appreciation. According to this survey data that could be asked:
            - Basic training participation (min. annually)
            - number of incidents in comparison with former period
                - choose period wisely and according to your organisation, minimum annually, or quarterly, monthly, weekly, daily
            - shortfalls
            - number of requests for new functionality

- Give clear guidance for situations where workarounds are appropriate and where not. (Enable mission commander to deviate, but in a guided manner. Missions themselves are a high-risk event, risk management must take the higher level of risk-acceptance into account)
- Policies should include acceptable times for implementing new functionalities
- Have a process for improvement proposals from the employees to be noticed and heard.
    - Consider awards for good proposals. Keep motivation up.
- Give clear guidance for prioritisation
- Balance business needs with security
    - risks can also be accepted, when the potential gain justifies it, but highest level must decide, or at least give guidance
- Allow, enable and conduct crisis and recovery testing. The outcome might be horrible, but a real crisis might be even worse. Find your right frequency (min. annually).
- Scenarios to train:
    - social engineering like e-mail fishing campaigns
    - security audits
    - power outage
    - server breakdown
    - break-in attempts
    - phone system is not working.
- Create a good culture of communication in your organisation.
- Risk management is a high management/ leadership responsibility.
    - Be sure to give priorities according to the business needs.
- Resources must be sufficient for the given priorities.
- Further improve reporting
    - Ask your employees what they want to report /what they want you to know
    - automatise reporting
    - continuously improve reporting better metrics for main security areas
    - benchmarking
    - take losses into account, financial and reputational

MOD is the last resort of a state, so there have to be differences to firms. For a state, it is just no option to stand still and let an insurance jump in and pay for the damage, so there must be differences in crisis management and in preparation for it, and how much of the budget can be spent for that. The 2 % of the GDP that NATO asks, is still lower than the proposals from a 2.24% that are proposed for an average family in America [82].

II. The Cyber Hygiene Initiative



Aizsardzības ministrija

MINISTRY OF DEFENCE OF THE REPUBLIC OF LATVIA

K. Valdemāra iela 10/12, Riga, LV–1473; Latvia; phone: +371 67210124; fax: +371 67212307;
e-mail: kanceleja@mod.gov.lv; www.mod.gov.lv

No. MV-N/1711

Riga, 15.07 2015

✓ **Ministry of National Defence and Sport of Austria**
Ministry of Defence of Estonia
Ministry of Defence of Finland
Ministry of National Defence of Lithuania
Ministry of Defence of the Netherlands

European External Action Service
European Defence Agency

On the Pledge of the Cyber Hygiene Initiative

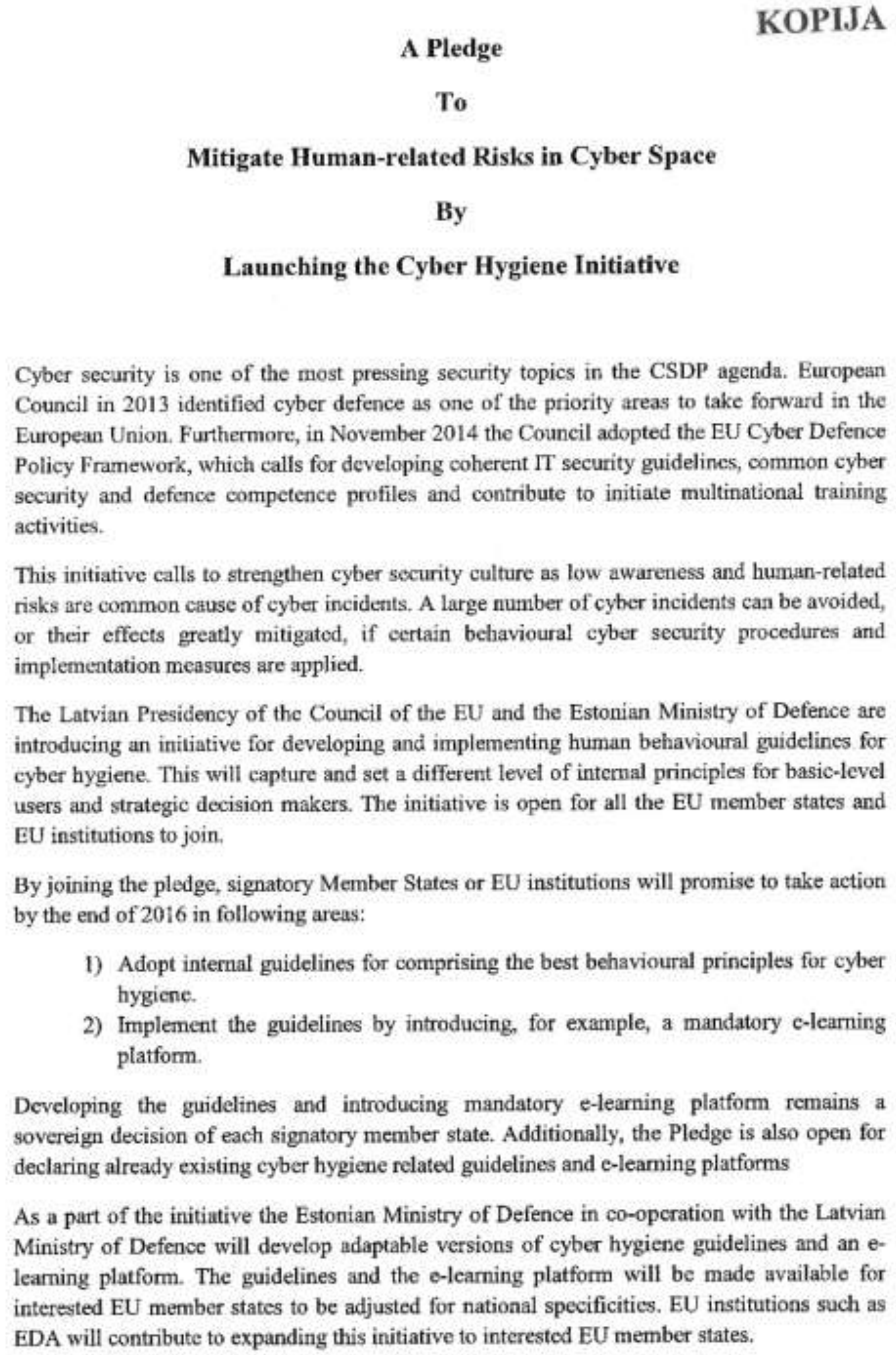
On May 18 in Brussels the Ministers of Defence of Latvia, Estonia, Lithuania, the Netherlands, Finland and Austria as well as the High Representative of the Union for Foreign Affairs and Security Policy on behalf of the European External Action Service, EU Military Committee and European Defence Agency, signed *A Pledge to mitigate human-related risks in cyber space by launching the Cyber Hygiene Initiative.*

The original documents are deposited in the Latvian Ministry of Defence; enclosed you can find certified copies.

Should you have any questions or more details are required please do not hesitate to contact Ms Elīna Neimane, Senior Desk Officer of the National Cyber Security Policy Coordination Section (elina.neimane@mod.gov.lv, +371 67335353).

Sincerely,

State Secretary Jānis Sārts



KOPIJA

A Pledge

To

Mitigate Human-related Risks in Cyber Space

By

Launching the Cyber Hygiene Initiative

Cyber security is one of the most pressing security topics in the CSDP agenda. European Council in 2013 identified cyber defence as one of the priority areas to take forward in the European Union. Furthermore, in November 2014 the Council adopted the EU Cyber Defence Policy Framework, which calls for developing coherent IT security guidelines, common cyber security and defence competence profiles and contribute to initiate multinational training activities.

This initiative calls to strengthen cyber security culture as low awareness and human-related risks are common cause of cyber incidents. A large number of cyber incidents can be avoided, or their effects greatly mitigated, if certain behavioural cyber security procedures and implementation measures are applied.

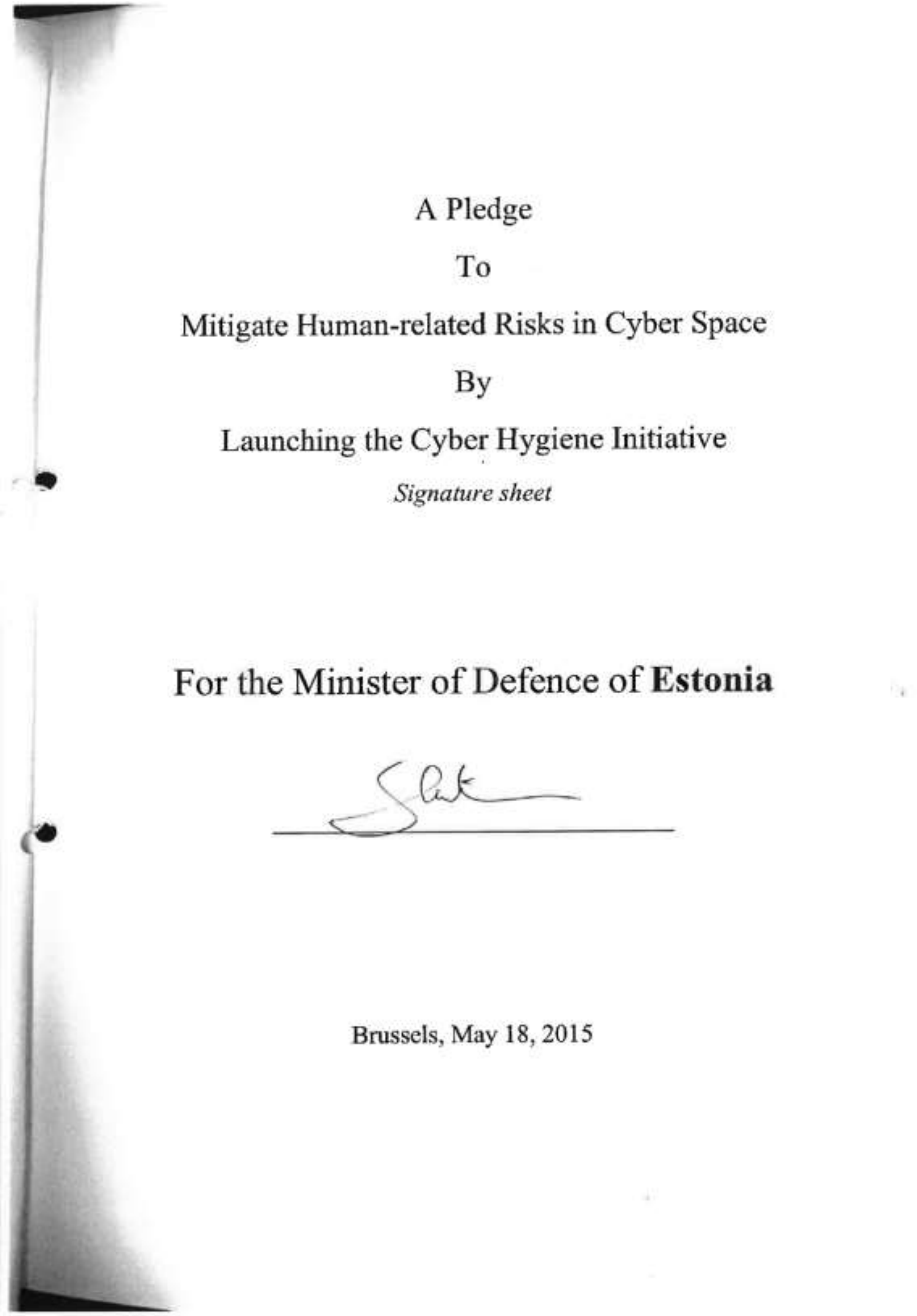
The Latvian Presidency of the Council of the EU and the Estonian Ministry of Defence are introducing an initiative for developing and implementing human behavioural guidelines for cyber hygiene. This will capture and set a different level of internal principles for basic-level users and strategic decision makers. The initiative is open for all the EU member states and EU institutions to join.

By joining the pledge, signatory Member States or EU institutions will promise to take action by the end of 2016 in following areas:

1) Adopt internal guidelines for comprising the best behavioural principles for cyber hygiene.
2) Implement the guidelines by introducing, for example, a mandatory e-learning platform.

Developing the guidelines and introducing mandatory e-learning platform remains a sovereign decision of each signatory member state. Additionally, the Pledge is also open for declaring already existing cyber hygiene related guidelines and e-learning platforms

As a part of the initiative the Estonian Ministry of Defence in co-operation with the Latvian Ministry of Defence will develop adaptable versions of cyber hygiene guidelines and an e-learning platform. The guidelines and the e-learning platform will be made available for interested EU member states to be adjusted for national specificities. EU institutions such as EDA will contribute to expanding this initiative to interested EU member states.



A Pledge

To

Mitigate Human-related Risks in Cyber Space

By

Launching the Cyber Hygiene Initiative

Signature sheet

For the Minister of Defence of **Estonia**

Brussels, May 18, 2015

A Pledge

To

Mitigate Human-related Risks in Cyber Space

By

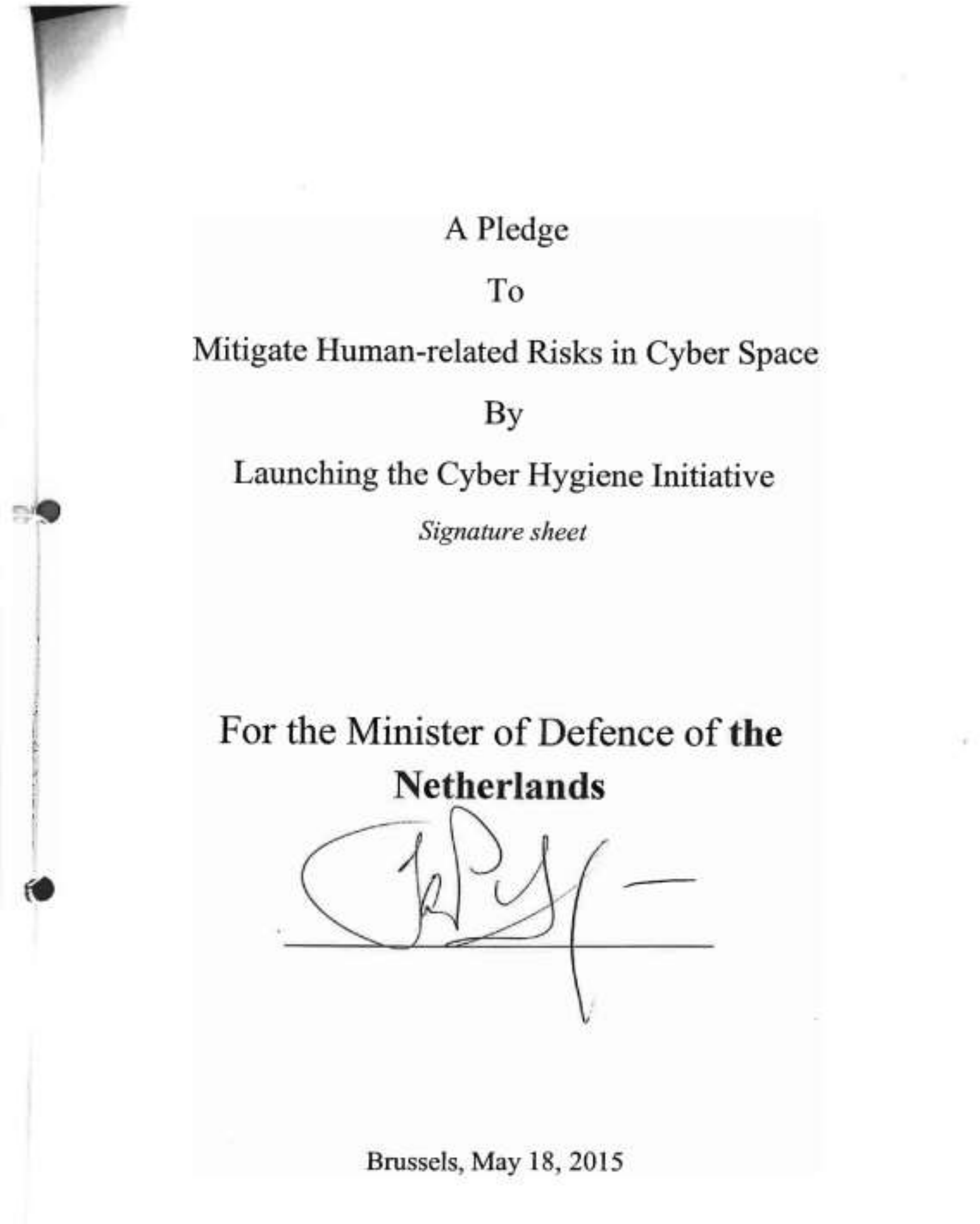
Launching the Cyber Hygiene Initiative

Signature sheet

For the Minister of Defence and Sports of

Austria

Brussels, May 18, 2015



A Pledge

To

Mitigate Human-related Risks in Cyber Space

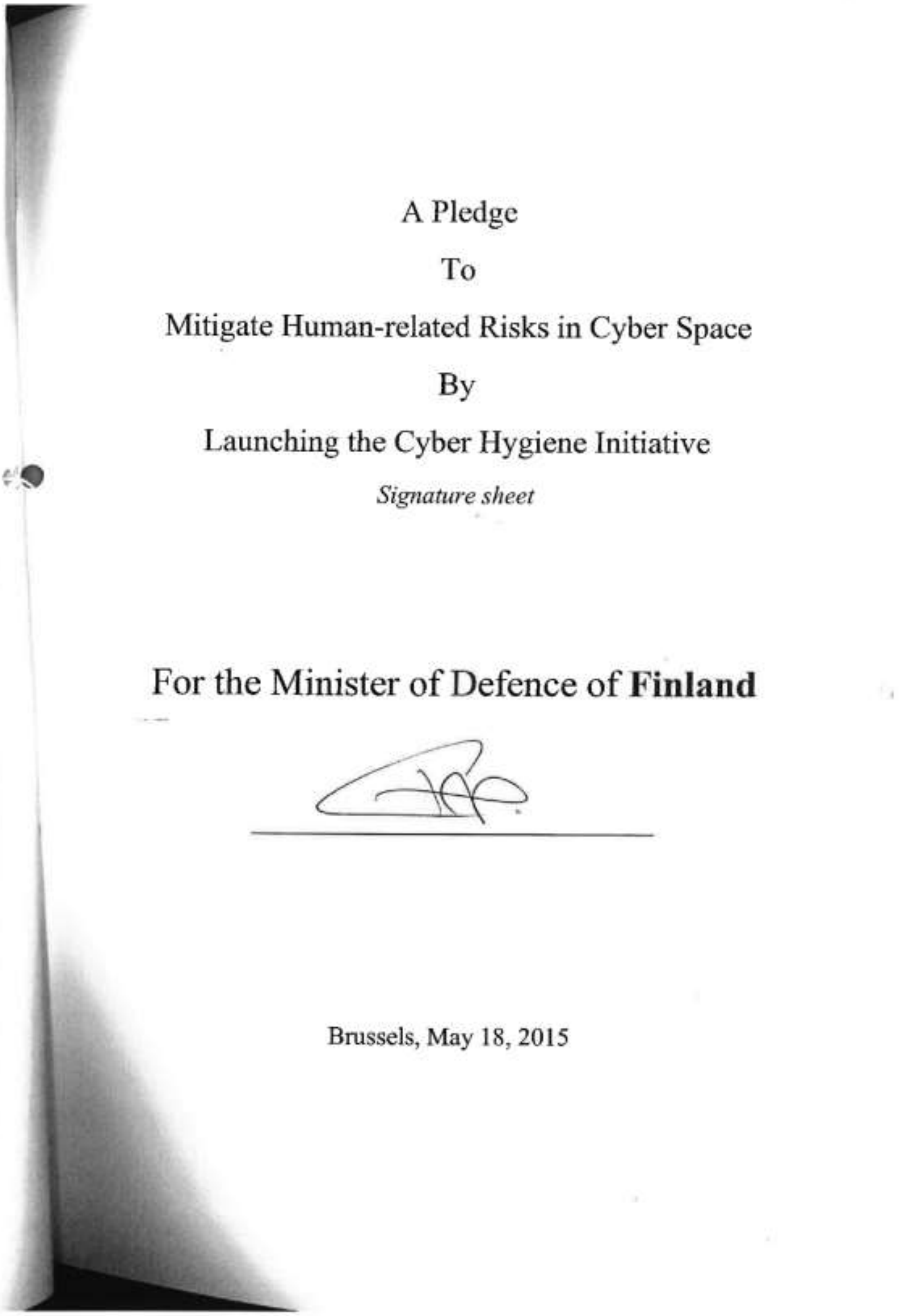
By

Launching the Cyber Hygiene Initiative

Signature sheet

For the Minister of Defence of **the Netherlands**

Brussels, May 18, 2015



A Pledge

To

Mitigate Human-related Risks in Cyber Space

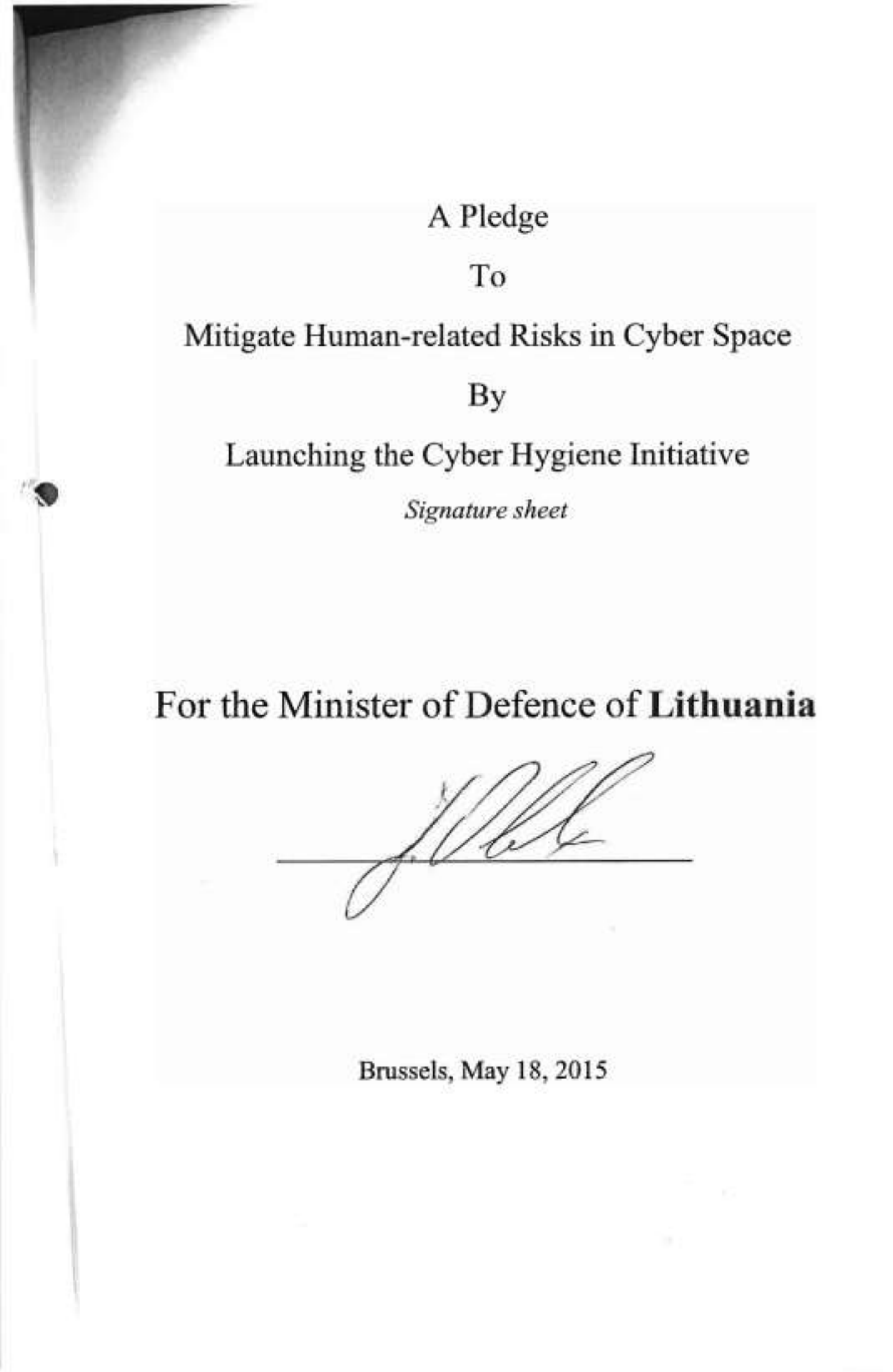
By

Launching the Cyber Hygiene Initiative

Signature sheet

For the Minister of Defence of **Finland**

Brussels, May 18, 2015



A Pledge

To

Mitigate Human-related Risks in Cyber Space

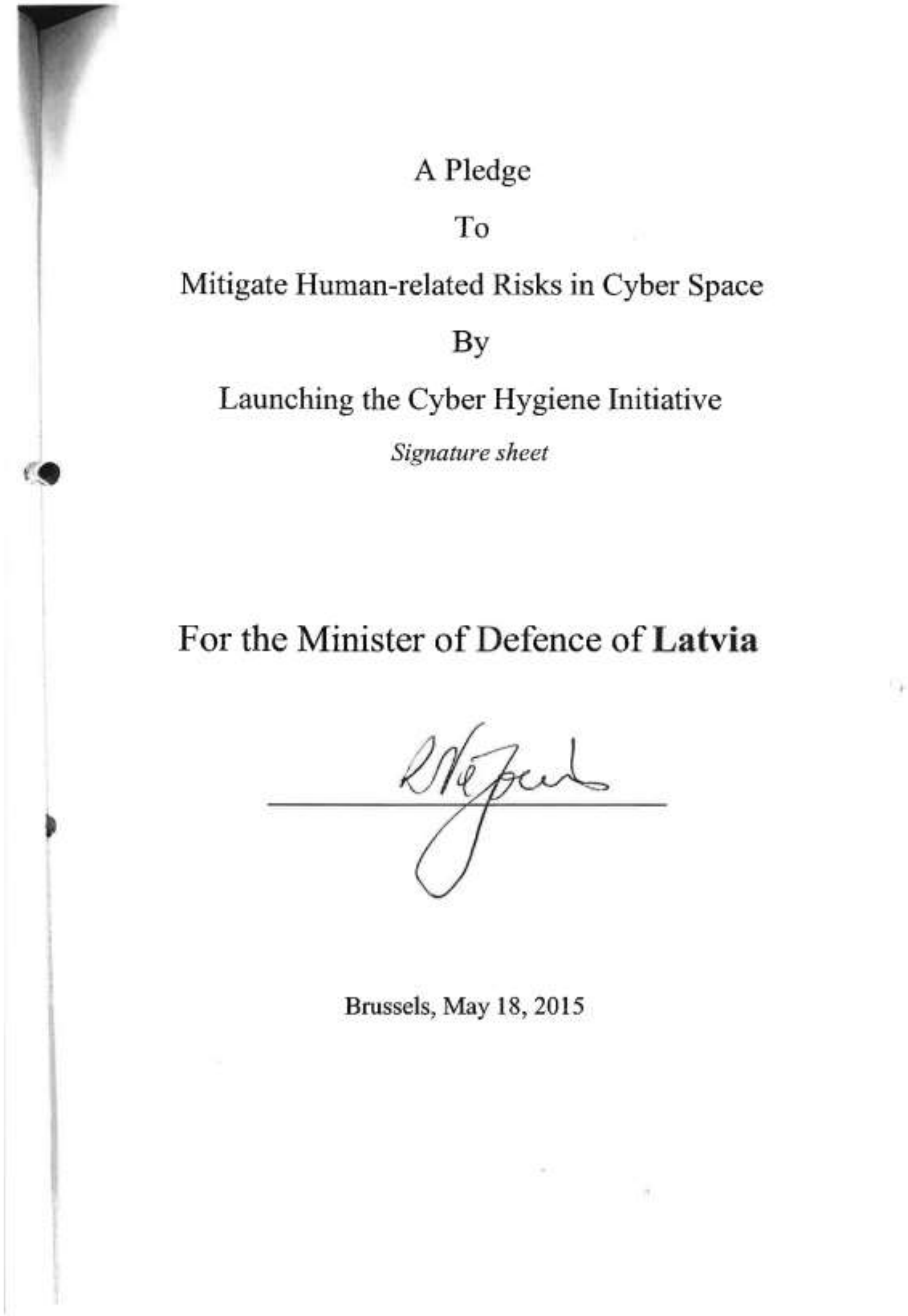
By

Launching the Cyber Hygiene Initiative

Signature sheet

For the Minister of Defence of **Lithuania**

Brussels, May 18, 2015



A Pledge

To

Mitigate Human-related Risks in Cyber Space

By

Launching the Cyber Hygiene Initiative

Signature sheet

For the Minister of Defence of **Latvia**

Brussels, May 18, 2015

A Pledge

To

Mitigate Human-related Risks in Cyber Space

By

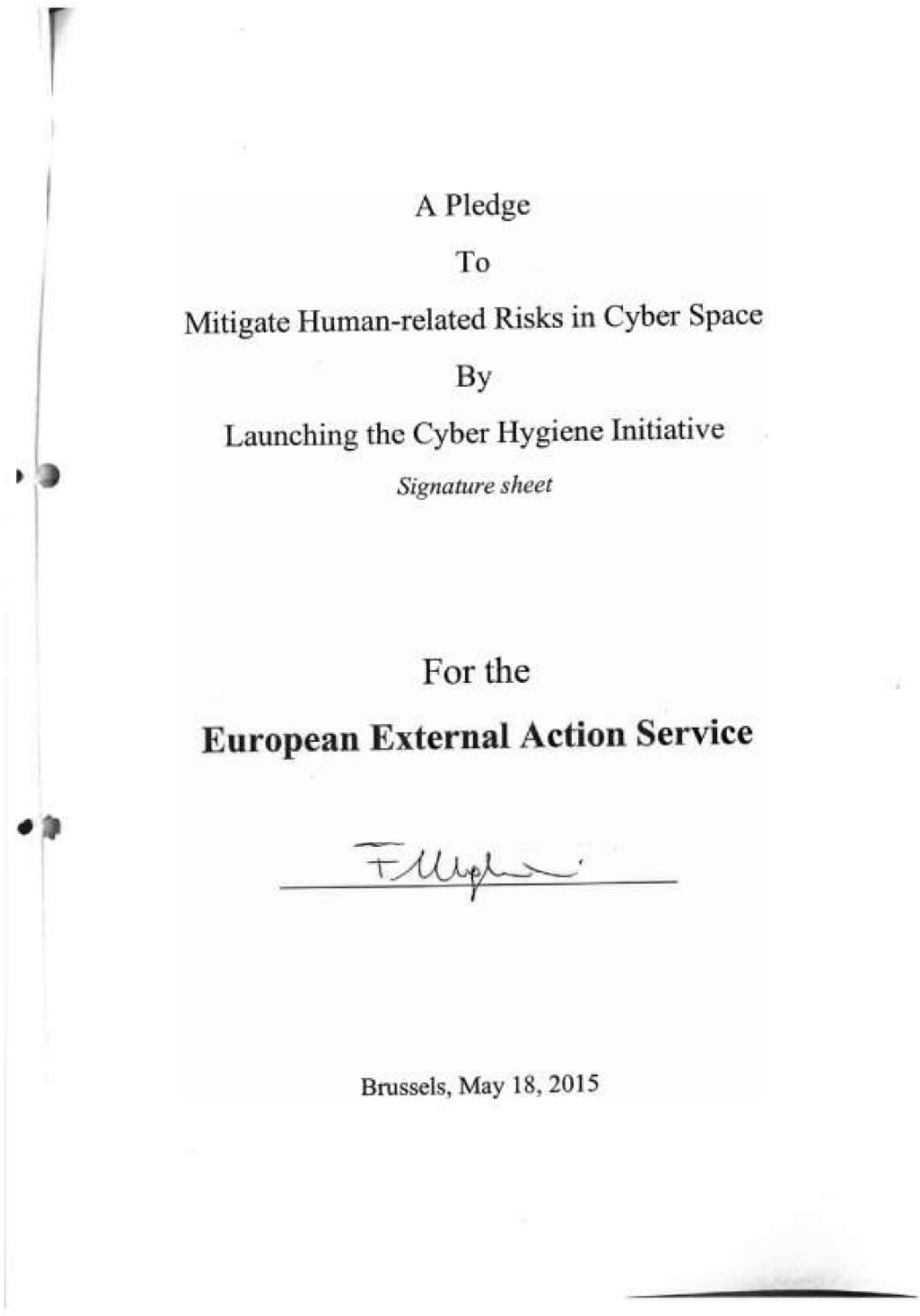
Launching the Cyber Hygiene Initiative

Signature sheet

For the

European Union Military Committee

Brussels, May 18, 2015



A Pledge

To

Mitigate Human-related Risks in Cyber Space

By

Launching the Cyber Hygiene Initiative

Signature sheet

For the

European External Action Service

Brussels, May 18, 2015

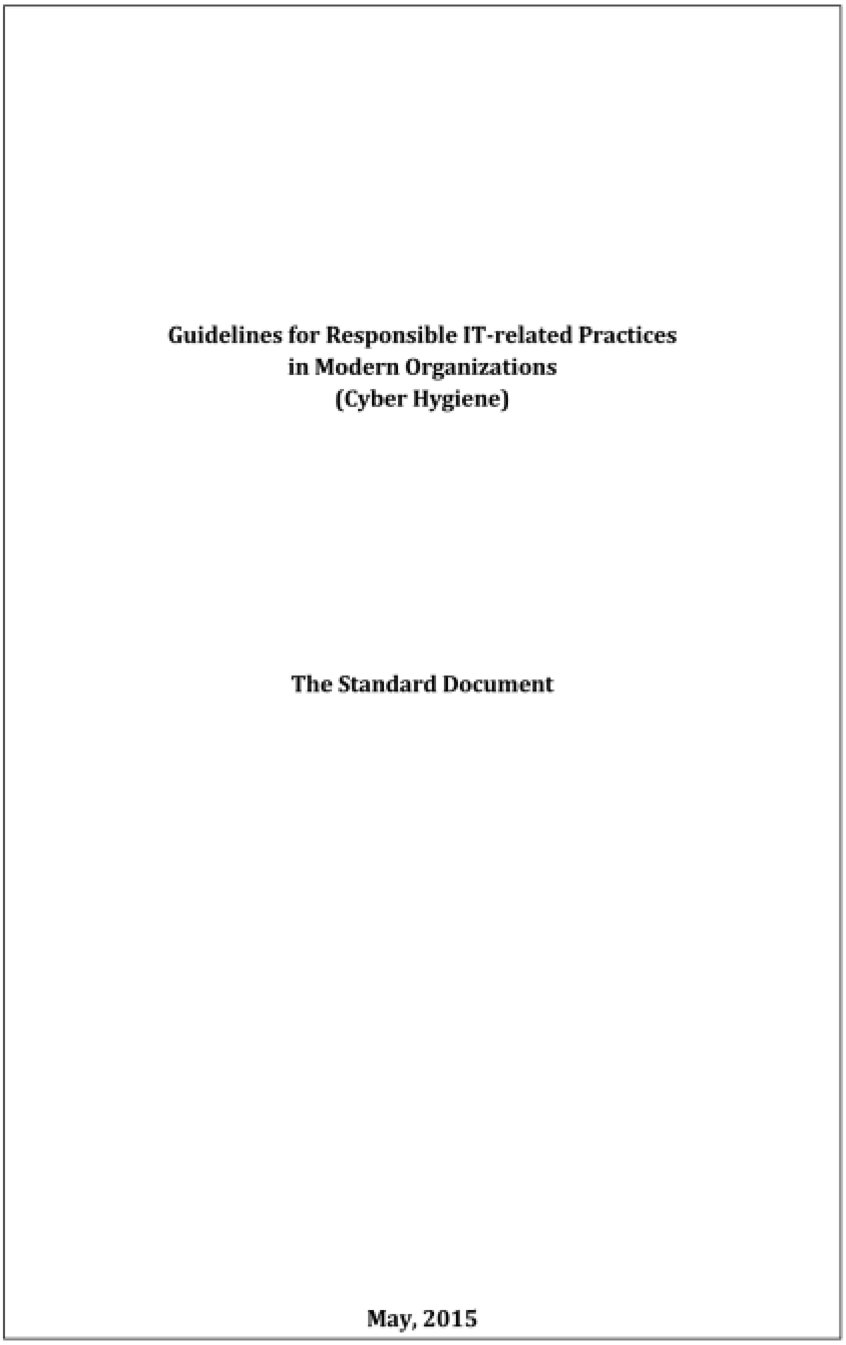
Šeit numurētas, cauršūtas un apzīmogotas 9 ([illegible]) lapas.

LATVIJAS REPUBLIKAS AIZSARDZĪBAS MINISTRIJA
LIETVEDĪBAS NODAĻA

LR Aizsardzības ministrijas
Lietvedības nodaļas vadītāja
E.Kļaviņa Rīgā, 20 15. g. 04. 06

KOPIJA PAREIZA

III. Guidelines Document from BHC Lab



Guidelines for Responsible IT-related Practices
in Modern Organizations
(Cyber Hygiene)

The Standard Document

May, 2015

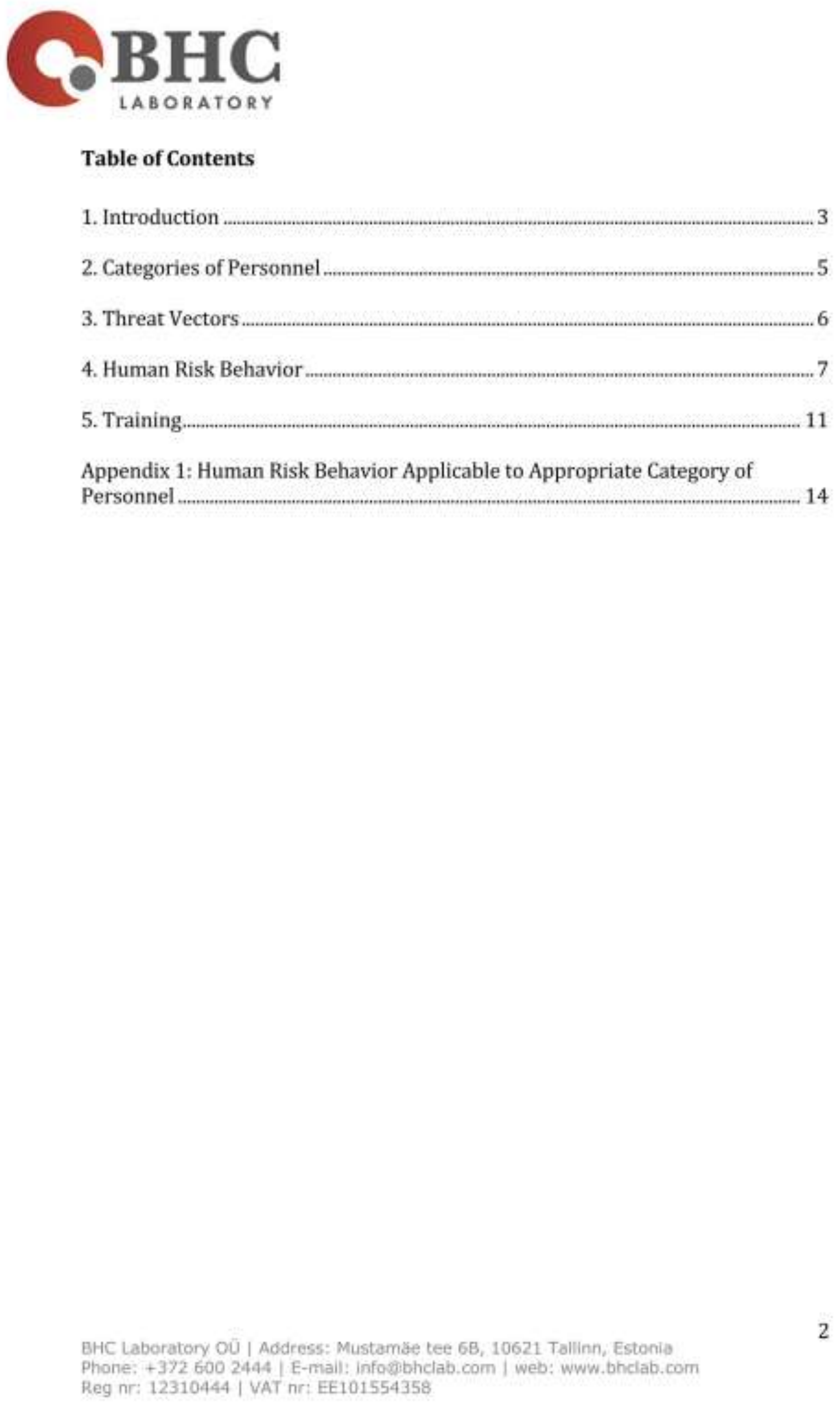
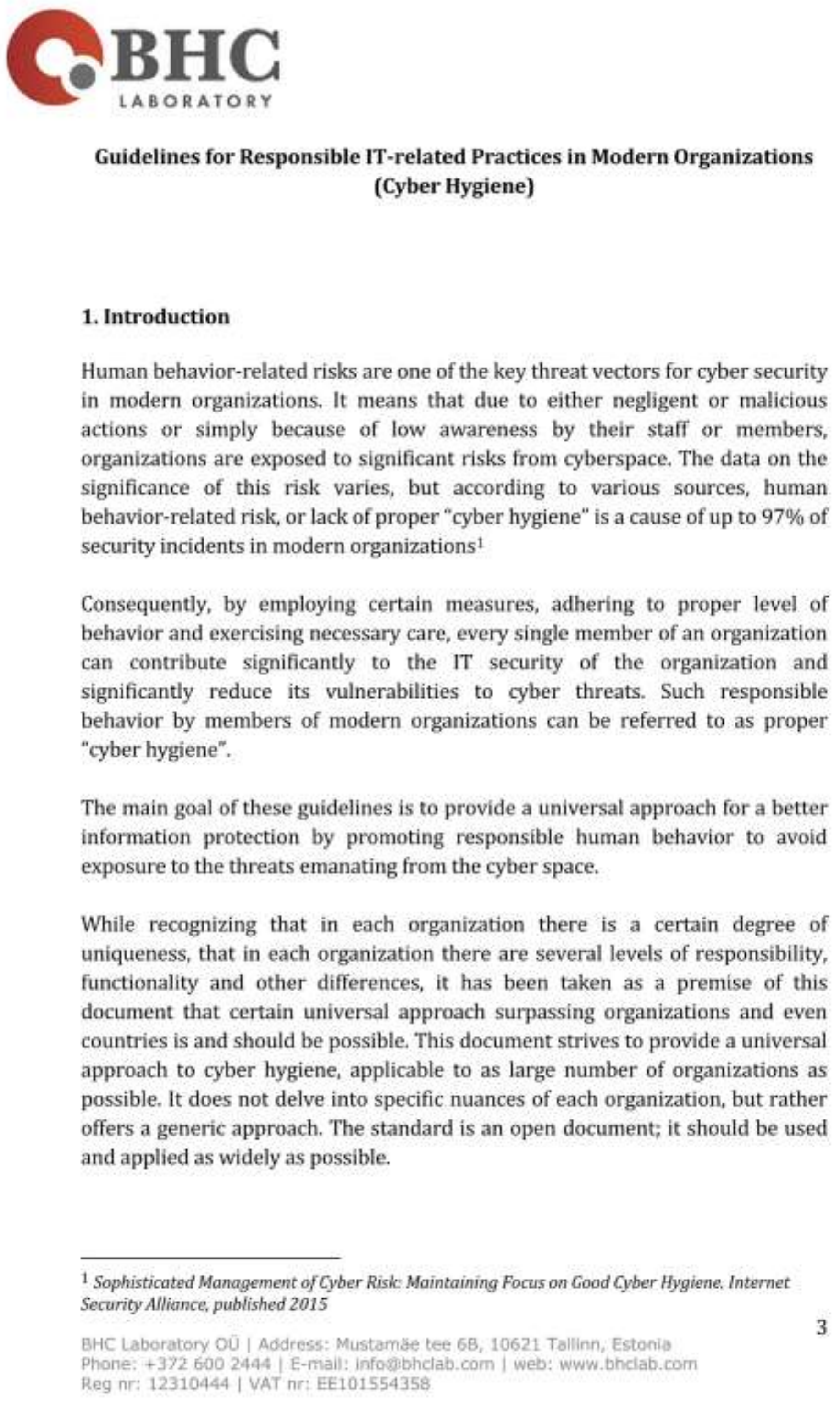


Table of Contents



Guidelines for Responsible IT-related Practices in Modern Organizations (Cyber Hygiene)

1. Introduction

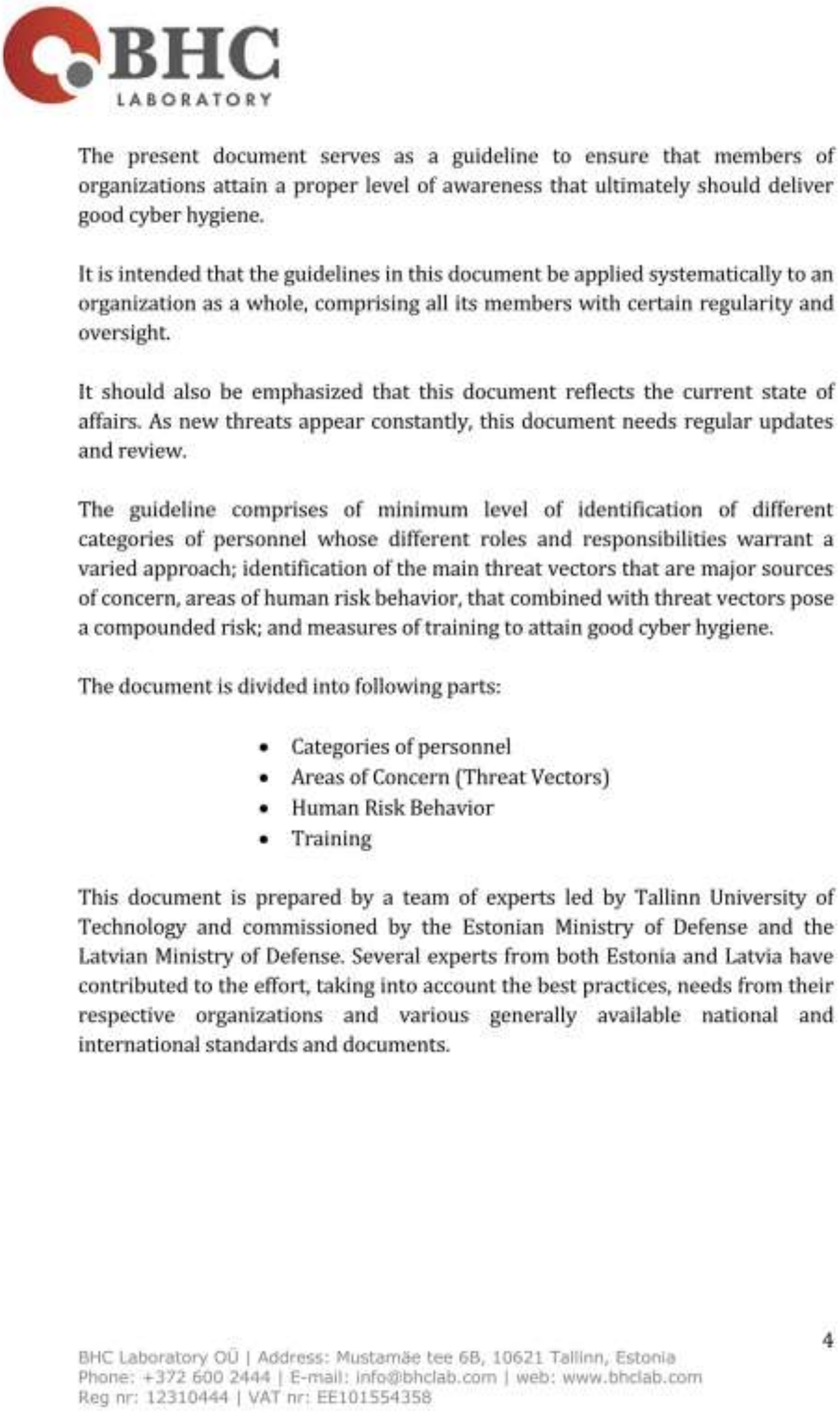
Human behavior-related risks are one of the key threat vectors for cyber security in modern organizations. It means that due to either negligent or malicious actions or simply because of low awareness by their staff or members, organizations are exposed to significant risks from cyberspace. The data on the significance of this risk varies, but according to various sources, human behavior-related risk, or lack of proper "cyber hygiene" is a cause of up to 97% of security incidents in modern organizations[1]

Consequently, by employing certain measures, adhering to proper level of behavior and exercising necessary care, every single member of an organization can contribute significantly to the IT security of the organization and significantly reduce its vulnerabilities to cyber threats. Such responsible behavior by members of modern organizations can be referred to as proper "cyber hygiene".

The main goal of these guidelines is to provide a universal approach for a better information protection by promoting responsible human behavior to avoid exposure to the threats emanating from the cyber space.

While recognizing that in each organization there is a certain degree of uniqueness, that in each organization there are several levels of responsibility, functionality and other differences, it has been taken as a premise of this document that certain universal approach surpassing organizations and even countries is and should be possible. This document strives to provide a universal approach to cyber hygiene, applicable to as large number of organizations as possible. It does not delve into specific nuances of each organization, but rather offers a generic approach. The standard is an open document; it should be used and applied as widely as possible.

[1] *Sophisticated Management of Cyber Risk: Maintaining Focus on Good Cyber Hygiene. Internet Security Alliance, published 2015*



The present document serves as a guideline to ensure that members of organizations attain a proper level of awareness that ultimately should deliver good cyber hygiene.

It is intended that the guidelines in this document be applied systematically to an organization as a whole, comprising all its members with certain regularity and oversight.

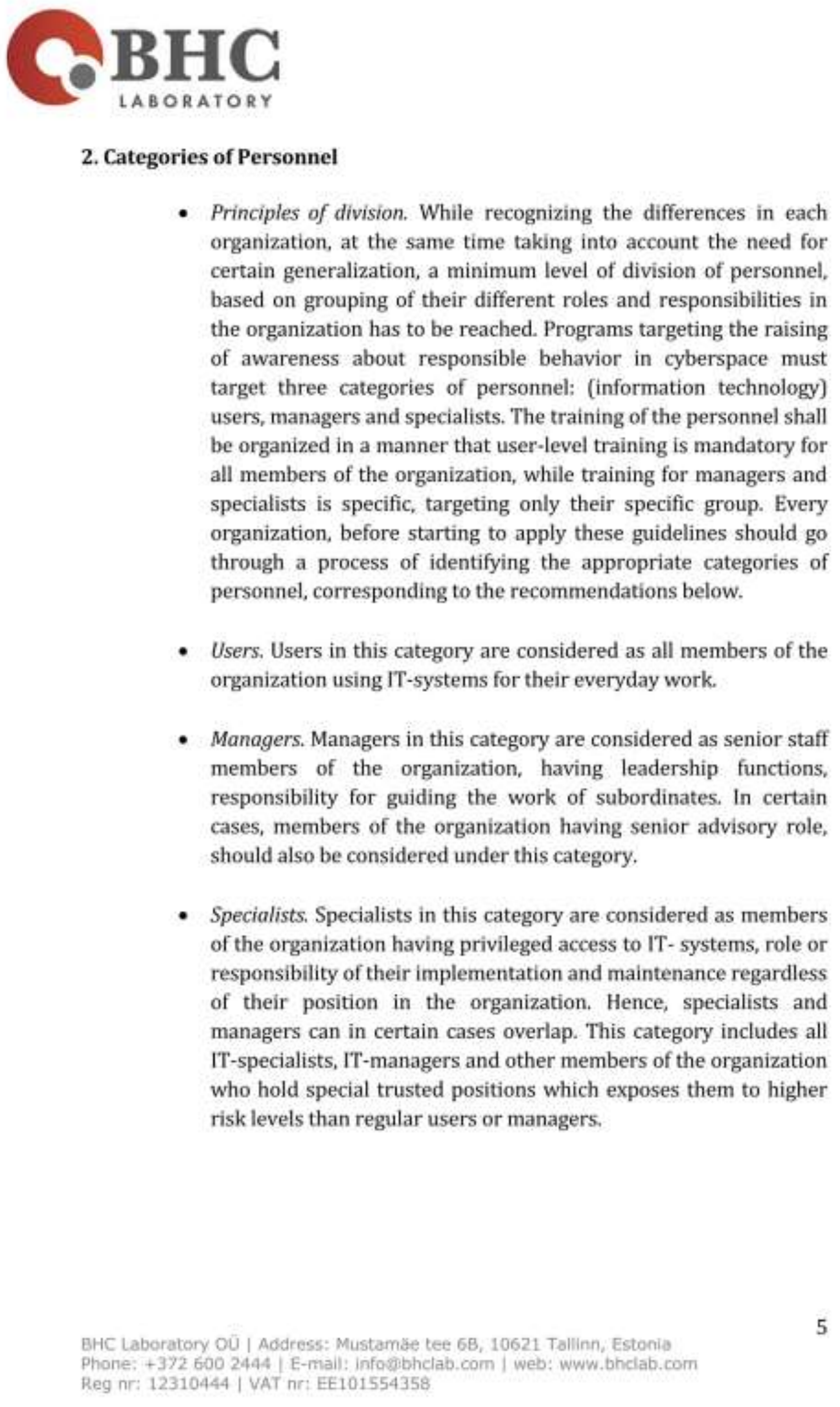
It should also be emphasized that this document reflects the current state of affairs. As new threats appear constantly, this document needs regular updates and review.

The guideline comprises of minimum level of identification of different categories of personnel whose different roles and responsibilities warrant a varied approach; identification of the main threat vectors that are major sources of concern, areas of human risk behavior, that combined with threat vectors pose a compounded risk; and measures of training to attain good cyber hygiene.

The document is divided into following parts:

- Categories of personnel
- Areas of Concern (Threat Vectors)
- Human Risk Behavior
- Training

This document is prepared by a team of experts led by Tallinn University of Technology and commissioned by the Estonian Ministry of Defense and the Latvian Ministry of Defense. Several experts from both Estonia and Latvia have contributed to the effort, taking into account the best practices, needs from their respective organizations and various generally available national and international standards and documents.



2. Categories of Personnel

- *Principles of division.* While recognizing the differences in each organization, at the same time taking into account the need for certain generalization, a minimum level of division of personnel, based on grouping of their different roles and responsibilities in the organization has to be reached. Programs targeting the raising of awareness about responsible behavior in cyberspace must target three categories of personnel: (information technology) users, managers and specialists. The training of the personnel shall be organized in a manner that user-level training is mandatory for all members of the organization, while training for managers and specialists is specific, targeting only their specific group. Every organization, before starting to apply these guidelines should go through a process of identifying the appropriate categories of personnel, corresponding to the recommendations below.

- *Users.* Users in this category are considered as all members of the organization using IT-systems for their everyday work.

- *Managers.* Managers in this category are considered as senior staff members of the organization, having leadership functions, responsibility for guiding the work of subordinates. In certain cases, members of the organization having senior advisory role, should also be considered under this category.

- *Specialists.* Specialists in this category are considered as members of the organization having privileged access to IT- systems, role or responsibility of their implementation and maintenance regardless of their position in the organization. Hence, specialists and managers can in certain cases overlap. This category includes all IT-specialists, IT-managers and other members of the organization who hold special trusted positions which exposes them to higher risk levels than regular users or managers.

3. Threat Vectors

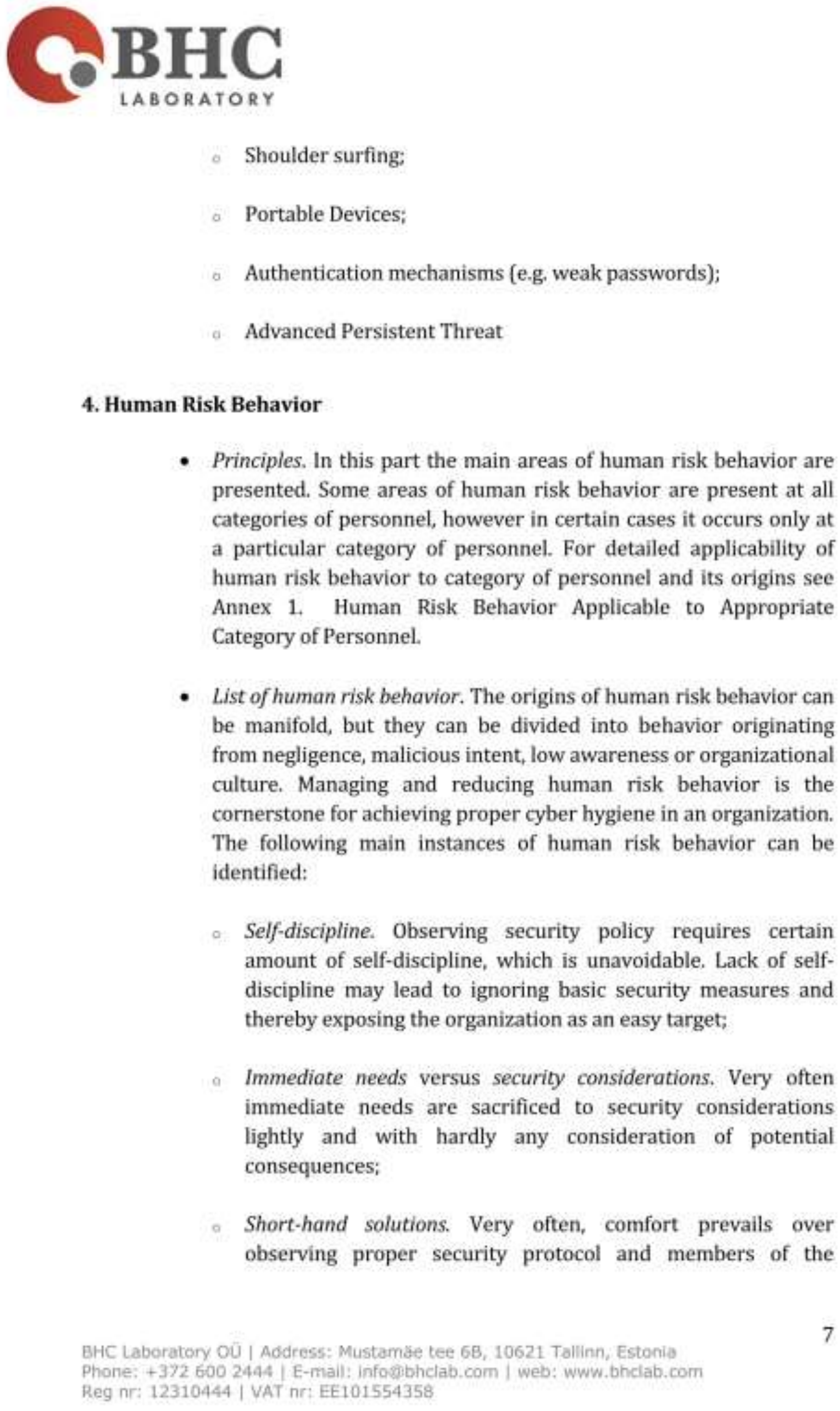
- *Principles.* The threat vectors represent objective, outside risks that are directed against an organization's information assets or infrastructure from the cyberspace, but also from direct access to systems. The risks originating from these threat vectors often materialize through irresponsible, uninformed or malicious activities of the members of the organization.

- *Applicability.* Threat vectors as presented in this document are applicable to all categories of personnel.

- *Exposure.* It should be emphasized that members of the organization are vulnerable to the threat vectors below not only at their work environment but they are exposed to those threats also outside their organization in various social situations and environments (e.g. home, through children, spouse, relatives, friends and using their IT devices in unsecure environments, etc).

- *List of threat vectors.* The following main threat vectors are identified; they represent the current state of affairs. It should be noted that cyber threats are ever-evolving and the list below needs constant updating:

  - Viruses, worms, Trojans and other malicious code (malware);
  - E-mail related risks, such as fake e-mails, unknown e-mail attachments, phishing, e-mail links, double extensions;
  - Websites with malicious content;
  - Wireless access points, unsecured and shared;
  - Social networks, social media, social engineering;
  - Bring Your Own Device (BYOD), work data on private device, private data on work device;
  - Removable media;



- Shoulder surfing;
- Portable Devices;
- Authentication mechanisms (e.g. weak passwords);
- Advanced Persistent Threat

4. Human Risk Behavior

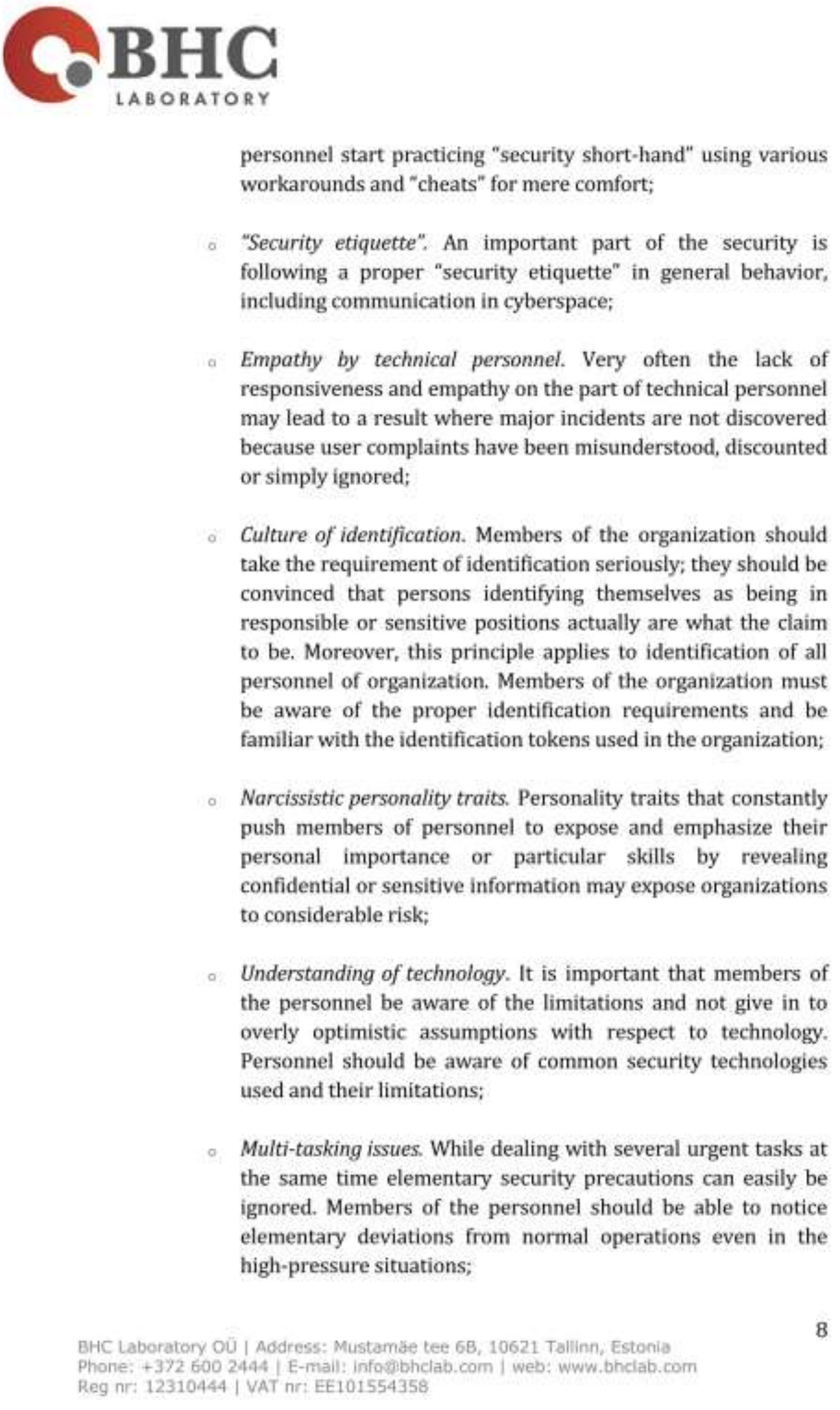
- *Principles.* In this part the main areas of human risk behavior are presented. Some areas of human risk behavior are present at all categories of personnel, however in certain cases it occurs only at a particular category of personnel. For detailed applicability of human risk behavior to category of personnel and its origins see Annex 1. Human Risk Behavior Applicable to Appropriate Category of Personnel.

- *List of human risk behavior*. The origins of human risk behavior can be manifold, but they can be divided into behavior originating from negligence, malicious intent, low awareness or organizational culture. Managing and reducing human risk behavior is the cornerstone for achieving proper cyber hygiene in an organization. The following main instances of human risk behavior can be identified:

    - *Self-discipline*. Observing security policy requires certain amount of self-discipline, which is unavoidable. Lack of self-discipline may lead to ignoring basic security measures and thereby exposing the organization as an easy target;

    - *Immediate needs* versus *security considerations*. Very often immediate needs are sacrificed to security considerations lightly and with hardly any consideration of potential consequences;

    - *Short-hand solutions*. Very often, comfort prevails over observing proper security protocol and members of the



personnel start practicing "security short-hand" using various workarounds and "cheats" for mere comfort;

- *"Security etiquette".* An important part of the security is following a proper "security etiquette" in general behavior, including communication in cyberspace;

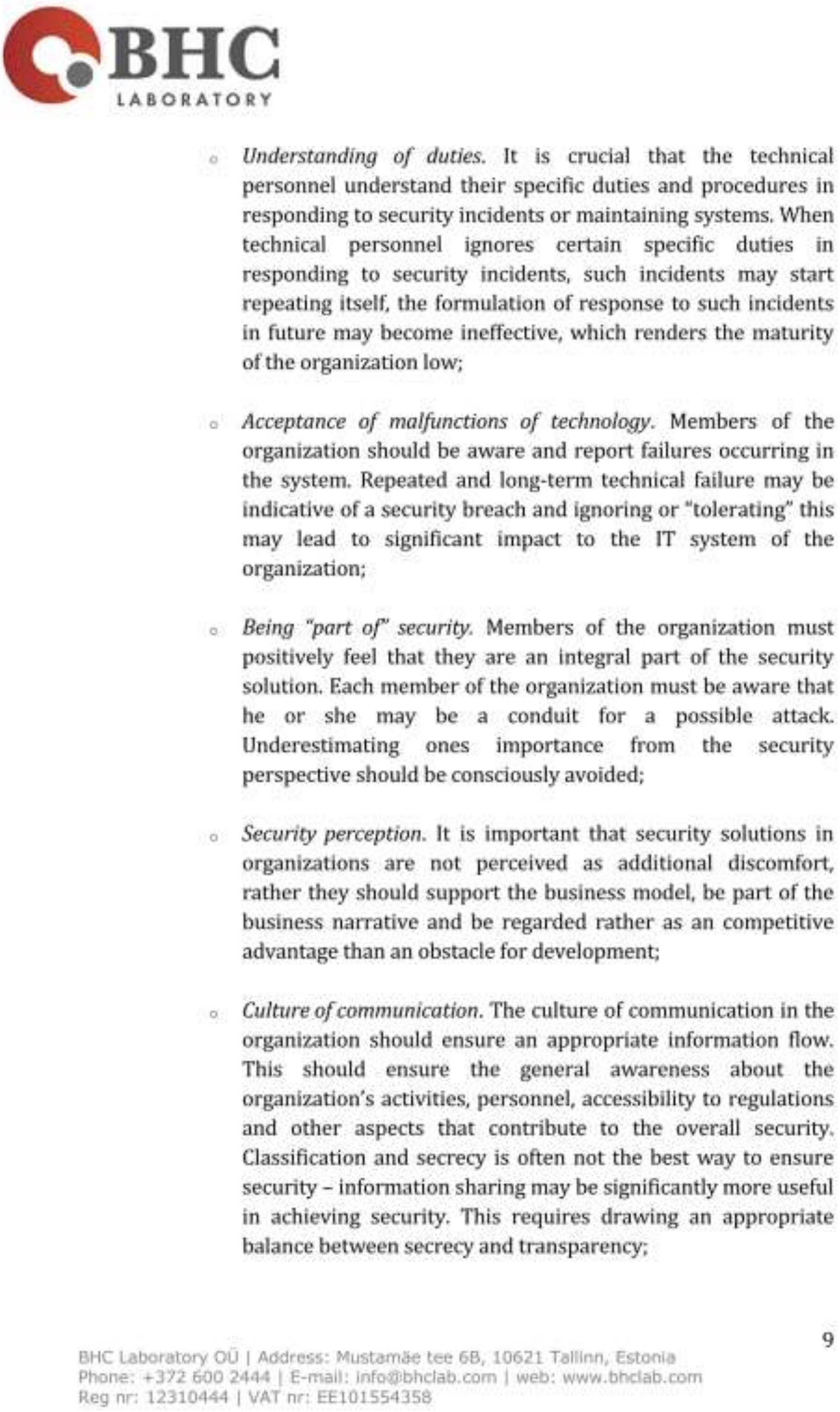
- *Empathy by technical personnel.* Very often the lack of responsiveness and empathy on the part of technical personnel may lead to a result where major incidents are not discovered because user complaints have been misunderstood, discounted or simply ignored;

- *Culture of identification.* Members of the organization should take the requirement of identification seriously; they should be convinced that persons identifying themselves as being in responsible or sensitive positions actually are what the claim to be. Moreover, this principle applies to identification of all personnel of organization. Members of the organization must be aware of the proper identification requirements and be familiar with the identification tokens used in the organization;

- *Narcissistic personality traits.* Personality traits that constantly push members of personnel to expose and emphasize their personal importance or particular skills by revealing confidential or sensitive information may expose organizations to considerable risk;

- *Understanding of technology.* It is important that members of the personnel be aware of the limitations and not give in to overly optimistic assumptions with respect to technology. Personnel should be aware of common security technologies used and their limitations;

- *Multi-tasking issues.* While dealing with several urgent tasks at the same time elementary security precautions can easily be ignored. Members of the personnel should be able to notice elementary deviations from normal operations even in the high-pressure situations;



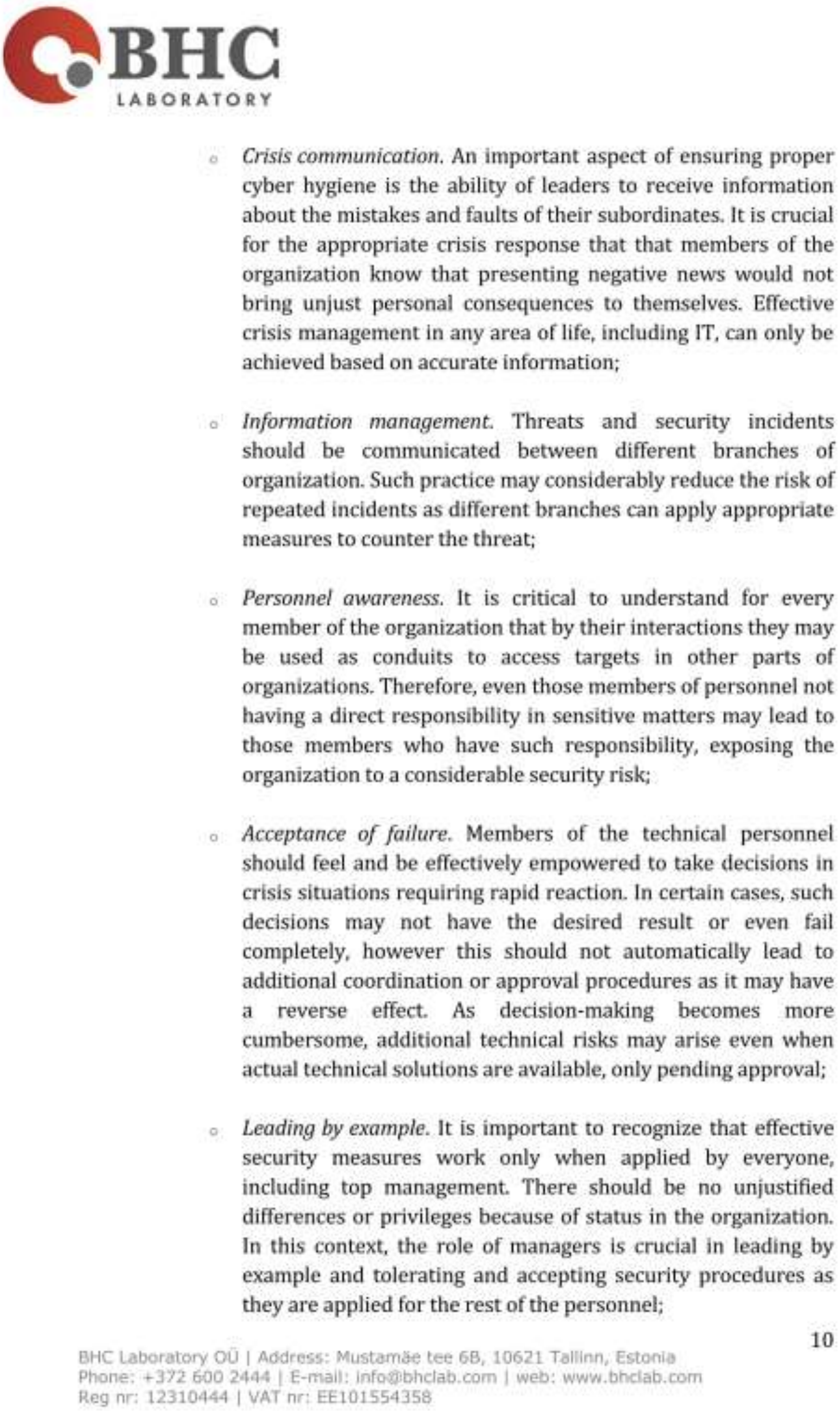
- *Understanding of duties.* It is crucial that the technical personnel understand their specific duties and procedures in responding to security incidents or maintaining systems. When technical personnel ignores certain specific duties in responding to security incidents, such incidents may start repeating itself, the formulation of response to such incidents in future may become ineffective, which renders the maturity of the organization low;

- *Acceptance of malfunctions of technology.* Members of the organization should be aware and report failures occurring in the system. Repeated and long-term technical failure may be indicative of a security breach and ignoring or "tolerating" this may lead to significant impact to the IT system of the organization;

- *Being "part of" security.* Members of the organization must positively feel that they are an integral part of the security solution. Each member of the organization must be aware that he or she may be a conduit for a possible attack. Underestimating ones importance from the security perspective should be consciously avoided;

- *Security perception.* It is important that security solutions in organizations are not perceived as additional discomfort, rather they should support the business model, be part of the business narrative and be regarded rather as an competitive advantage than an obstacle for development;

- *Culture of communication.* The culture of communication in the organization should ensure an appropriate information flow. This should ensure the general awareness about the organization's activities, personnel, accessibility to regulations and other aspects that contribute to the overall security. Classification and secrecy is often not the best way to ensure security – information sharing may be significantly more useful in achieving security. This requires drawing an appropriate balance between secrecy and transparency;



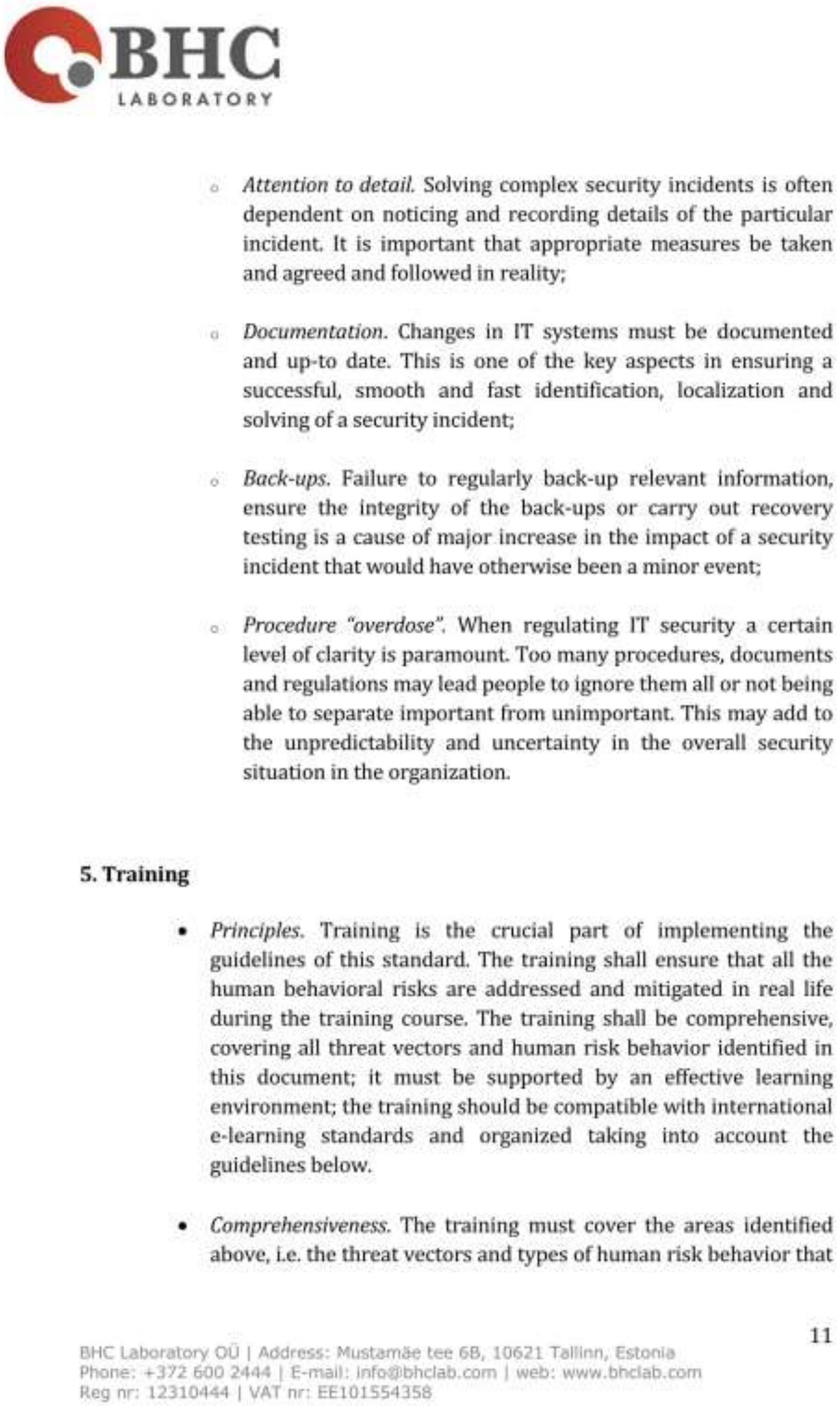
- *Crisis communication.* An important aspect of ensuring proper cyber hygiene is the ability of leaders to receive information about the mistakes and faults of their subordinates. It is crucial for the appropriate crisis response that that members of the organization know that presenting negative news would not bring unjust personal consequences to themselves. Effective crisis management in any area of life, including IT, can only be achieved based on accurate information;

- *Information management.* Threats and security incidents should be communicated between different branches of organization. Such practice may considerably reduce the risk of repeated incidents as different branches can apply appropriate measures to counter the threat;

- *Personnel awareness.* It is critical to understand for every member of the organization that by their interactions they may be used as conduits to access targets in other parts of organizations. Therefore, even those members of personnel not having a direct responsibility in sensitive matters may lead to those members who have such responsibility, exposing the organization to a considerable security risk;

- *Acceptance of failure.* Members of the technical personnel should feel and be effectively empowered to take decisions in crisis situations requiring rapid reaction. In certain cases, such decisions may not have the desired result or even fail completely, however this should not automatically lead to additional coordination or approval procedures as it may have a reverse effect. As decision-making becomes more cumbersome, additional technical risks may arise even when actual technical solutions are available, only pending approval;

- *Leading by example.* It is important to recognize that effective security measures work only when applied by everyone, including top management. There should be no unjustified differences or privileges because of status in the organization. In this context, the role of managers is crucial in leading by example and tolerating and accepting security procedures as they are applied for the rest of the personnel;



- *Attention to detail.* Solving complex security incidents is often dependent on noticing and recording details of the particular incident. It is important that appropriate measures be taken and agreed and followed in reality;

- *Documentation*. Changes in IT systems must be documented and up-to date. This is one of the key aspects in ensuring a successful, smooth and fast identification, localization and solving of a security incident;

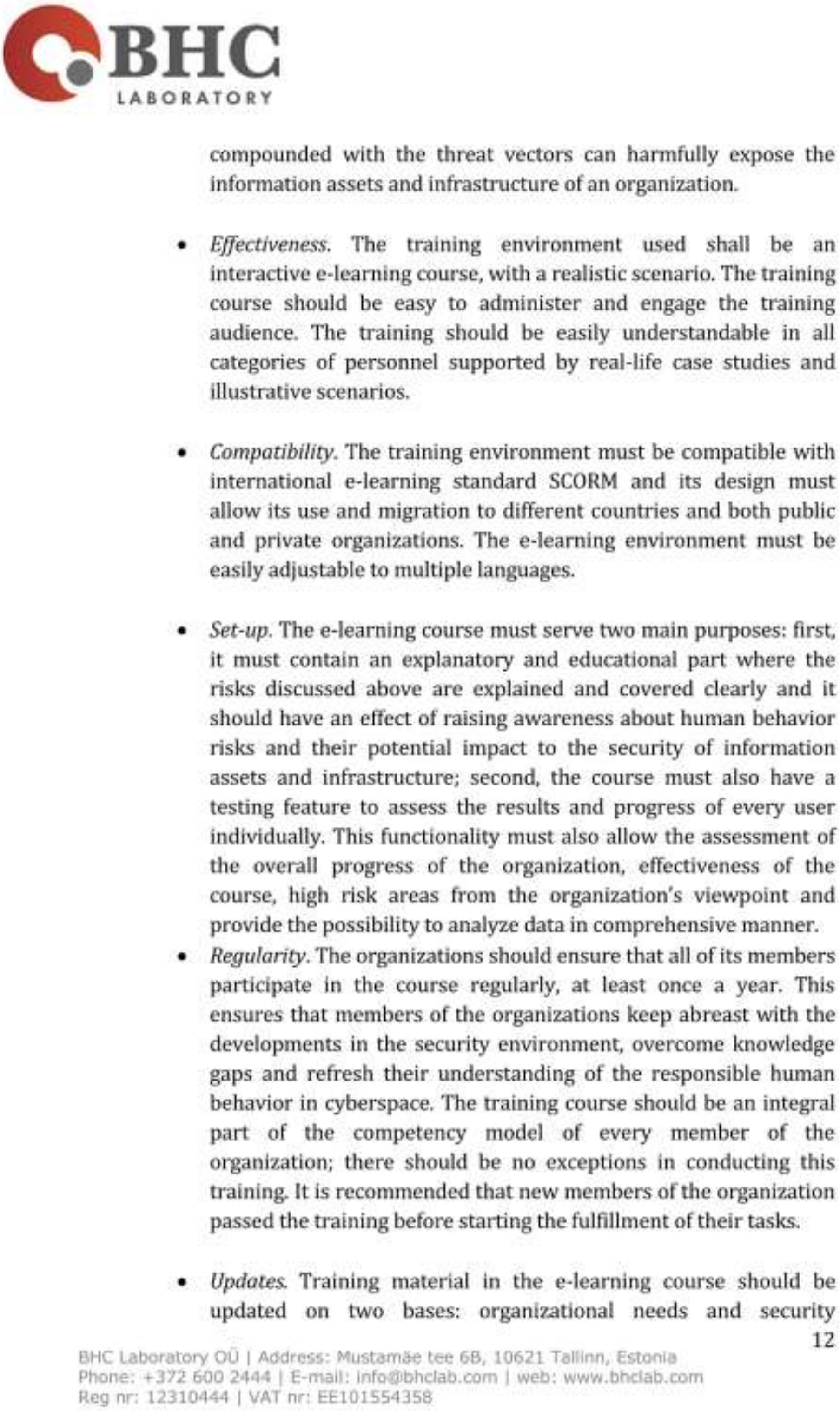
- *Back-ups*. Failure to regularly back-up relevant information, ensure the integrity of the back-ups or carry out recovery testing is a cause of major increase in the impact of a security incident that would have otherwise been a minor event;

- *Procedure "overdose"*. When regulating IT security a certain level of clarity is paramount. Too many procedures, documents and regulations may lead people to ignore them all or not being able to separate important from unimportant. This may add to the unpredictability and uncertainty in the overall security situation in the organization.

5. Training

- *Principles*. Training is the crucial part of implementing the guidelines of this standard. The training shall ensure that all the human behavioral risks are addressed and mitigated in real life during the training course. The training shall be comprehensive, covering all threat vectors and human risk behavior identified in this document; it must be supported by an effective learning environment; the training should be compatible with international e-learning standards and organized taking into account the guidelines below.

- *Comprehensiveness*. The training must cover the areas identified above, i.e. the threat vectors and types of human risk behavior that



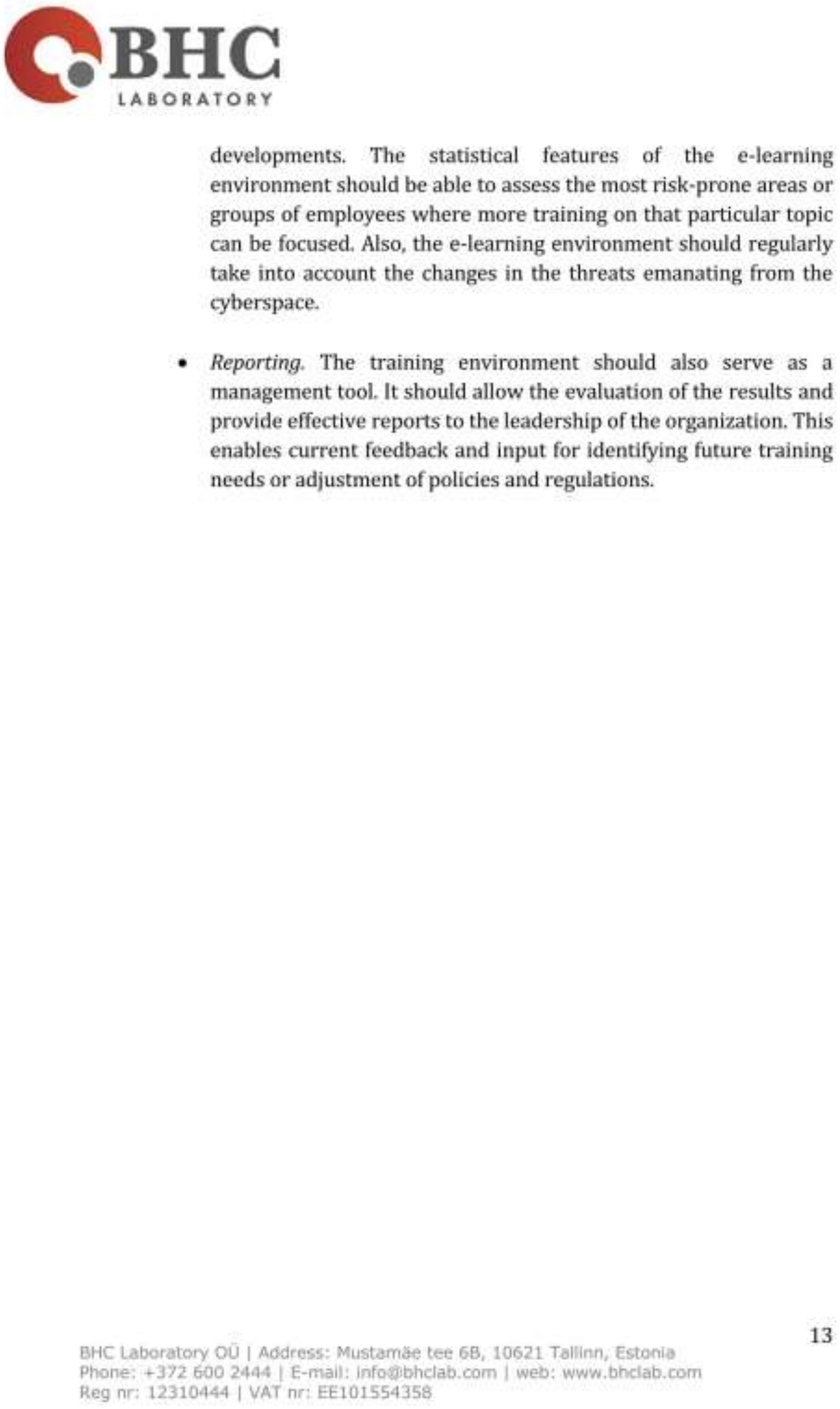
compounded with the threat vectors can harmfully expose the information assets and infrastructure of an organization.

- *Effectiveness.* The training environment used shall be an interactive e-learning course, with a realistic scenario. The training course should be easy to administer and engage the training audience. The training should be easily understandable in all categories of personnel supported by real-life case studies and illustrative scenarios.

- *Compatibility.* The training environment must be compatible with international e-learning standard SCORM and its design must allow its use and migration to different countries and both public and private organizations. The e-learning environment must be easily adjustable to multiple languages.

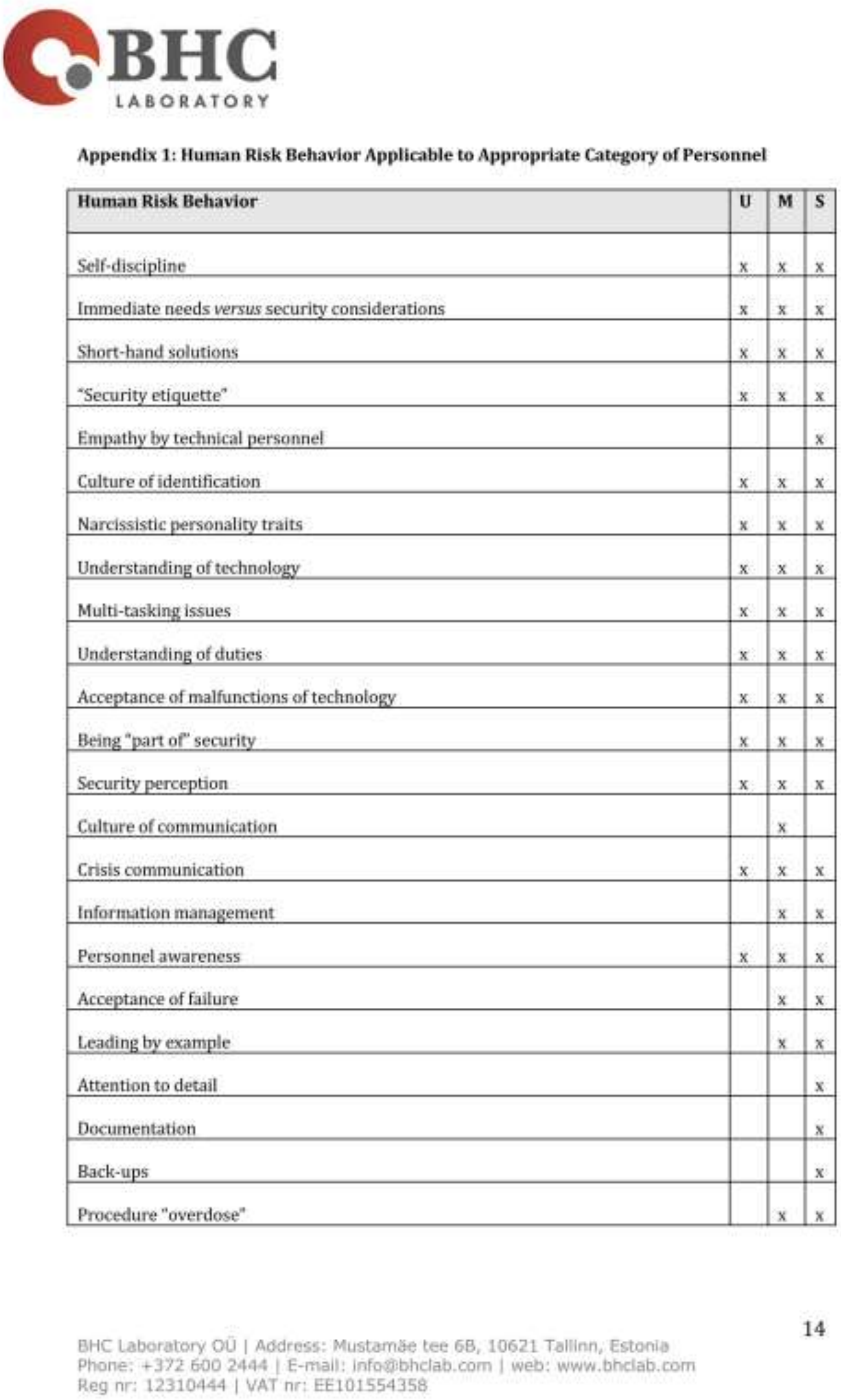
- *Set-up.* The e-learning course must serve two main purposes: first, it must contain an explanatory and educational part where the risks discussed above are explained and covered clearly and it should have an effect of raising awareness about human behavior risks and their potential impact to the security of information assets and infrastructure; second, the course must also have a testing feature to assess the results and progress of every user individually. This functionality must also allow the assessment of the overall progress of the organization, effectiveness of the course, high risk areas from the organization's viewpoint and provide the possibility to analyze data in comprehensive manner.
- *Regularity.* The organizations should ensure that all of its members participate in the course regularly, at least once a year. This ensures that members of the organizations keep abreast with the developments in the security environment, overcome knowledge gaps and refresh their understanding of the responsible human behavior in cyberspace. The training course should be an integral part of the competency model of every member of the organization; there should be no exceptions in conducting this training. It is recommended that new members of the organization passed the training before starting the fulfillment of their tasks.

- *Updates.* Training material in the e-learning course should be updated on two bases: organizational needs and security



developments. The statistical features of the e-learning environment should be able to assess the most risk-prone areas or groups of employees where more training on that particular topic can be focused. Also, the e-learning environment should regularly take into account the changes in the threats emanating from the cyberspace.

- *Reporting.* The training environment should also serve as a management tool. It should allow the evaluation of the results and provide effective reports to the leadership of the organization. This enables current feedback and input for identifying future training needs or adjustment of policies and regulations.



Appendix 1: Human Risk Behavior Applicable to Appropriate Category of Personnel

Human Risk Behavior	U	M	S
Self-discipline	x	x	x
Immediate needs *versus* security considerations	x	x	x
Short-hand solutions	x	x	x
"Security etiquette"	x	x	x
Empathy by technical personnel			x
Culture of identification	x	x	x
Narcissistic personality traits	x	x	x
Understanding of technology	x	x	x
Multi-tasking issues	x	x	x
Understanding of duties	x	x	x
Acceptance of malfunctions of technology	x	x	x
Being "part of" security	x	x	x
Security perception	x	x	x
Culture of communication		x	
Crisis communication	x	x	x
Information management		x	x
Personnel awareness	x	x	x
Acceptance of failure		x	x
Leading by example		x	x
Attention to detail			x
Documentation			x
Back-ups			x
Procedure "overdose"		x	x

14

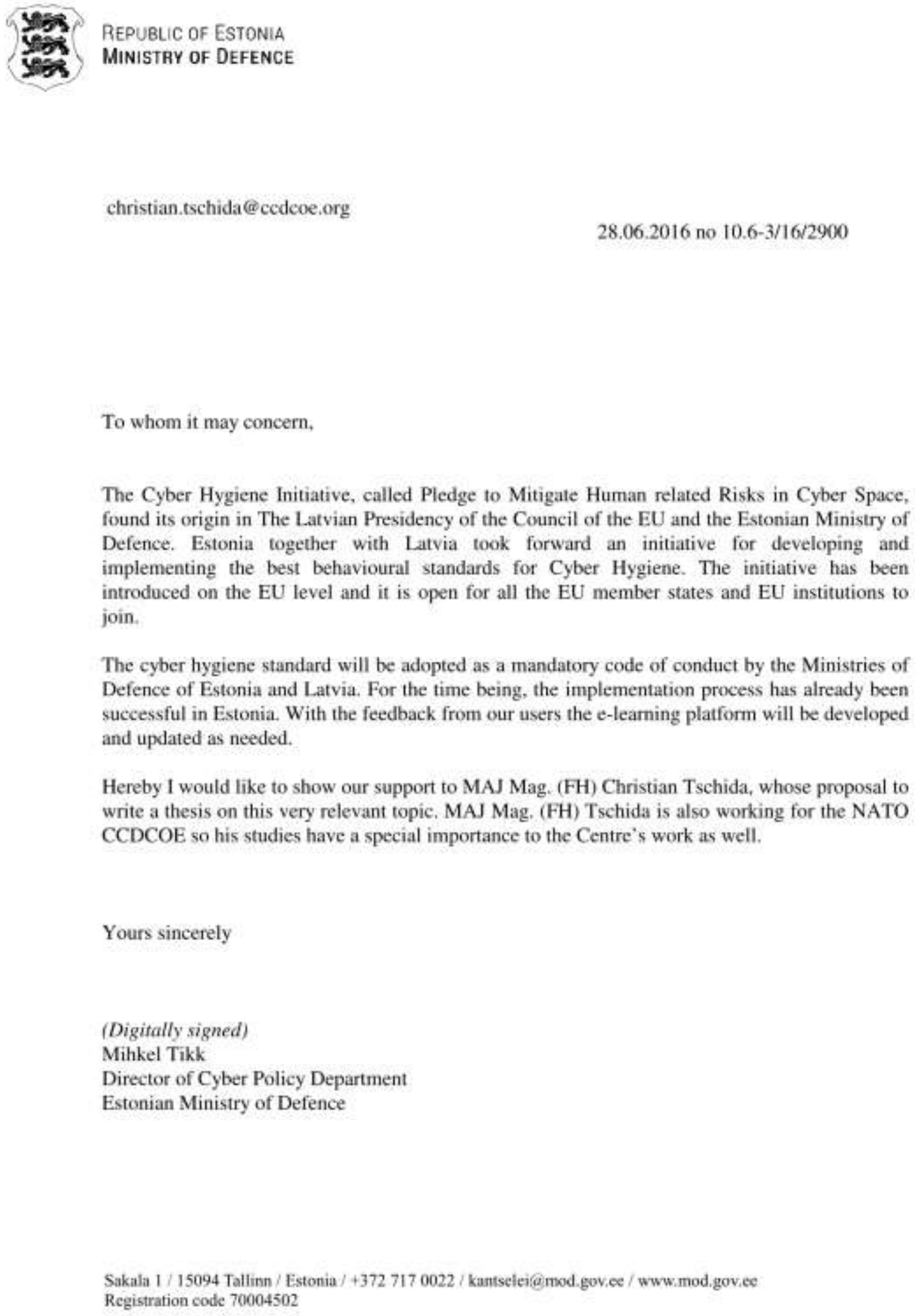
BHC Laboratory OÜ | Address: Mustamäe tee 6B, 10621 Tallinn, Estonia
Phone: +372 600 2444 | E-mail: info@bhclab.com | web: www.bhclab.com
Reg nr: 12310444 | VAT nr: EE101554358

BHC
LABORATORY

15

BHC Laboratory OÜ | Address: Mustamäe tee 6B, 10621 Tallinn, Estonia
Phone: +372 600 2444 | E-mail: info@bhclab.com | web: www.bhclab.com
Reg nr: 12310444 | VAT nr: EE101554358

IV. Letter of Estonian MOD



REPUBLIC OF ESTONIA
MINISTRY OF DEFENCE

christian.tschida@ccdcoe.org

28.06.2016 no 10.6-3/16/2900

To whom it may concern,

The Cyber Hygiene Initiative, called Pledge to Mitigate Human related Risks in Cyber Space, found its origin in The Latvian Presidency of the Council of the EU and the Estonian Ministry of Defence. Estonia together with Latvia took forward an initiative for developing and implementing the best behavioural standards for Cyber Hygiene. The initiative has been introduced on the EU level and it is open for all the EU member states and EU institutions to join.

The cyber hygiene standard will be adopted as a mandatory code of conduct by the Ministries of Defence of Estonia and Latvia. For the time being, the implementation process has already been successful in Estonia. With the feedback from our users the e-learning platform will be developed and updated as needed.

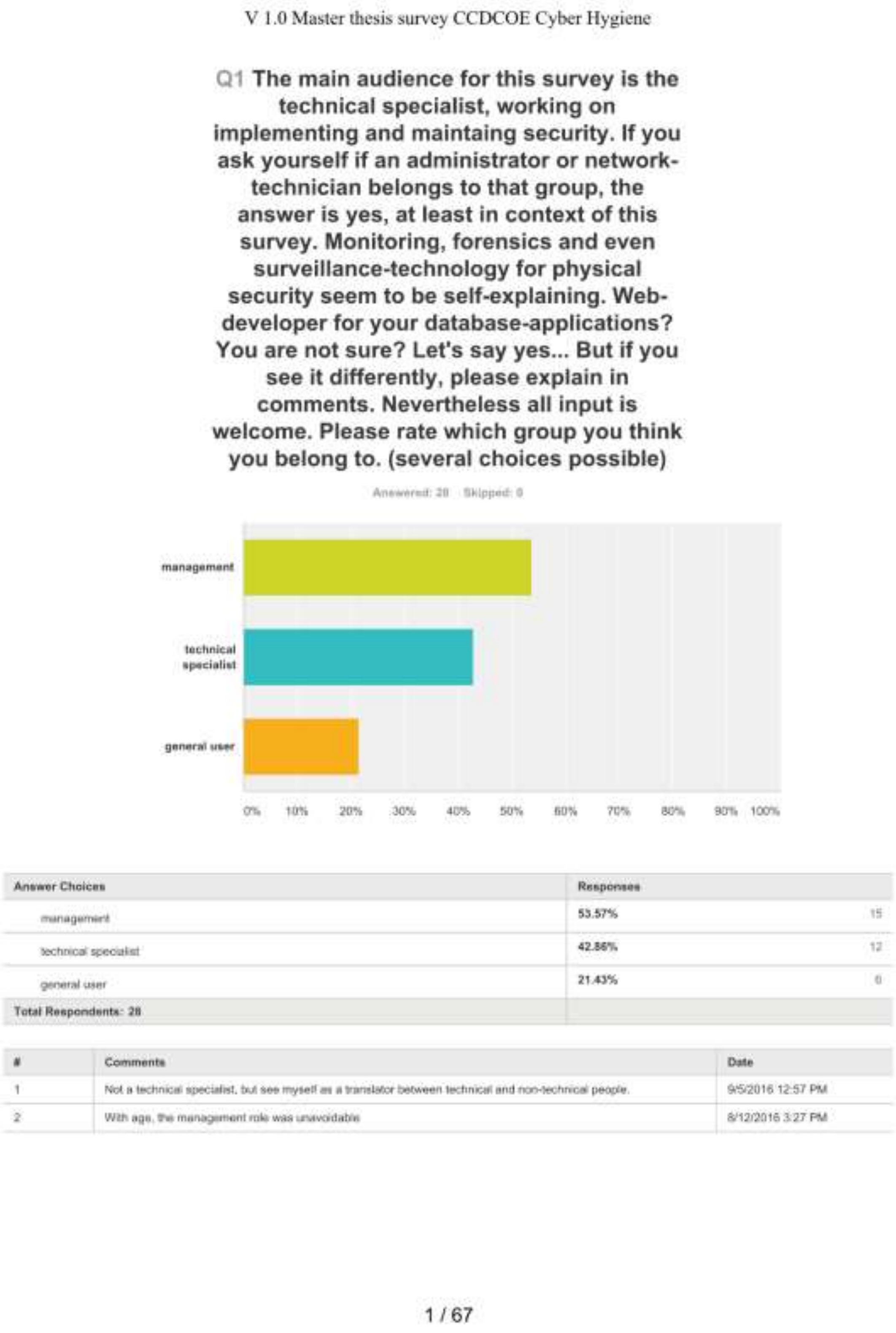
Hereby I would like to show our support to MAJ Mag. (FH) Christian Tschida, whose proposal to write a thesis on this very relevant topic. MAJ Mag. (FH) Tschida is also working for the NATO CCDCOE so his studies have a special importance to the Centre's work as well.

Yours sincerely

(Digitally signed)
Mihkel Tikk
Director of Cyber Policy Department
Estonian Ministry of Defence

Sakala 1 / 15094 Tallinn / Estonia / +372 717 0022 / kantselei@mod.gov.ee / www.mod.gov.ee
Registration code 70004502

V. The Survey Data



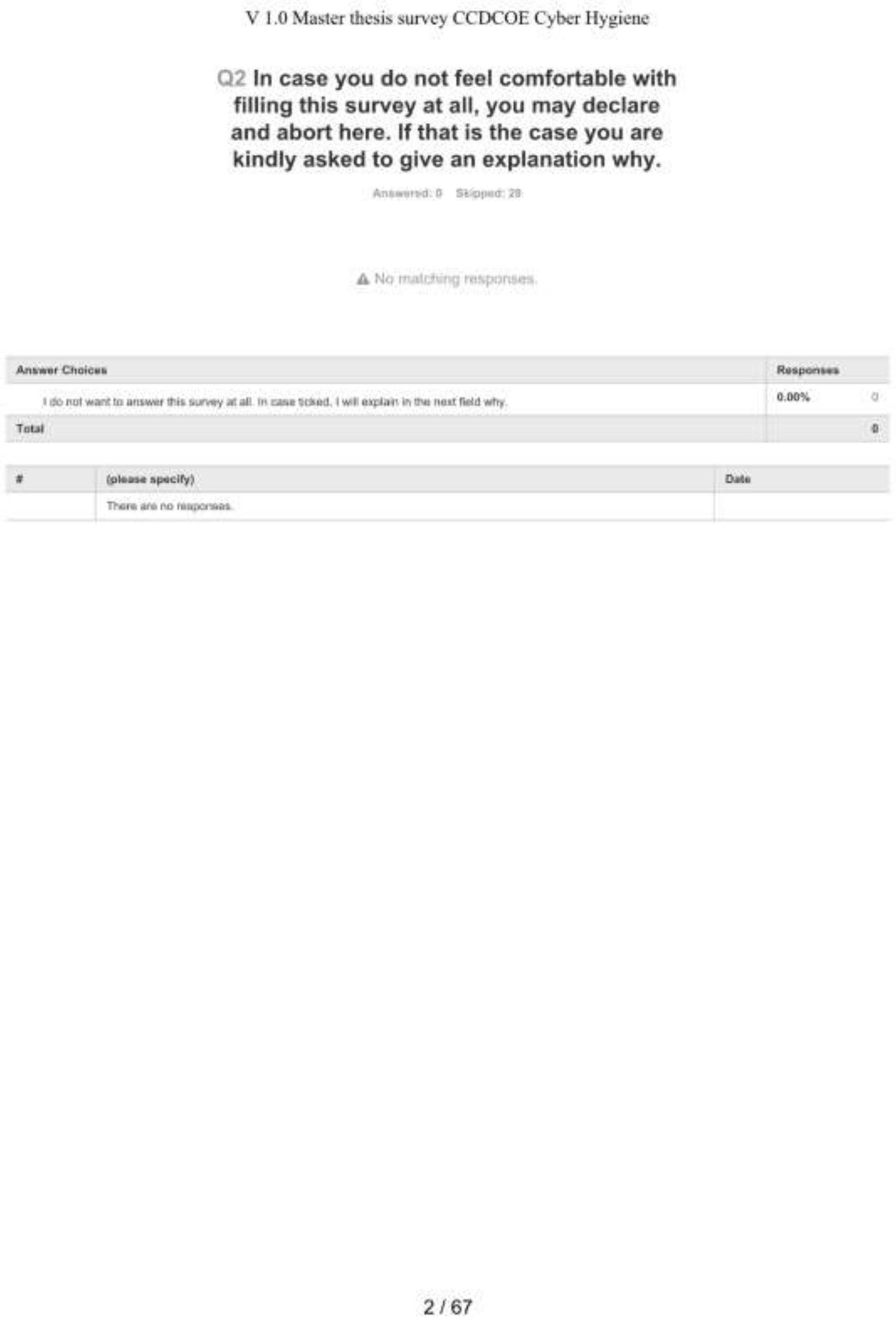
V 1.0 Master thesis survey CCDCOE Cyber Hygiene

Q1 The main audience for this survey is the technical specialist, working on implementing and maintaing security. If you ask yourself if an administrator or network-technician belongs to that group, the answer is yes, at least in context of this survey. Monitoring, forensics and even surveillance-technology for physical security seem to be self-explaining. Web-developer for your database-applications? You are not sure? Let's say yes... But if you see it differently, please explain in comments. Nevertheless all input is welcome. Please rate which group you think you belong to. (several choices possible)

Answered: 28 Skipped: 0

Answer Choices	Responses	
management	53.57%	15
technical specialist	42.86%	12
general user	21.43%	6
Total Respondents: 28		

#	Comments	Date
1	Not a technical specialist, but see myself as a translator between technical and non-technical people.	9/5/2016 12:57 PM
2	With age, the management role was unavoidable	8/12/2016 3:27 PM



V 1.0 Master thesis survey CCDCOE Cyber Hygiene

Q2 In case you do not feel comfortable with filling this survey at all, you may declare and abort here. If that is the case you are kindly asked to give an explanation why.

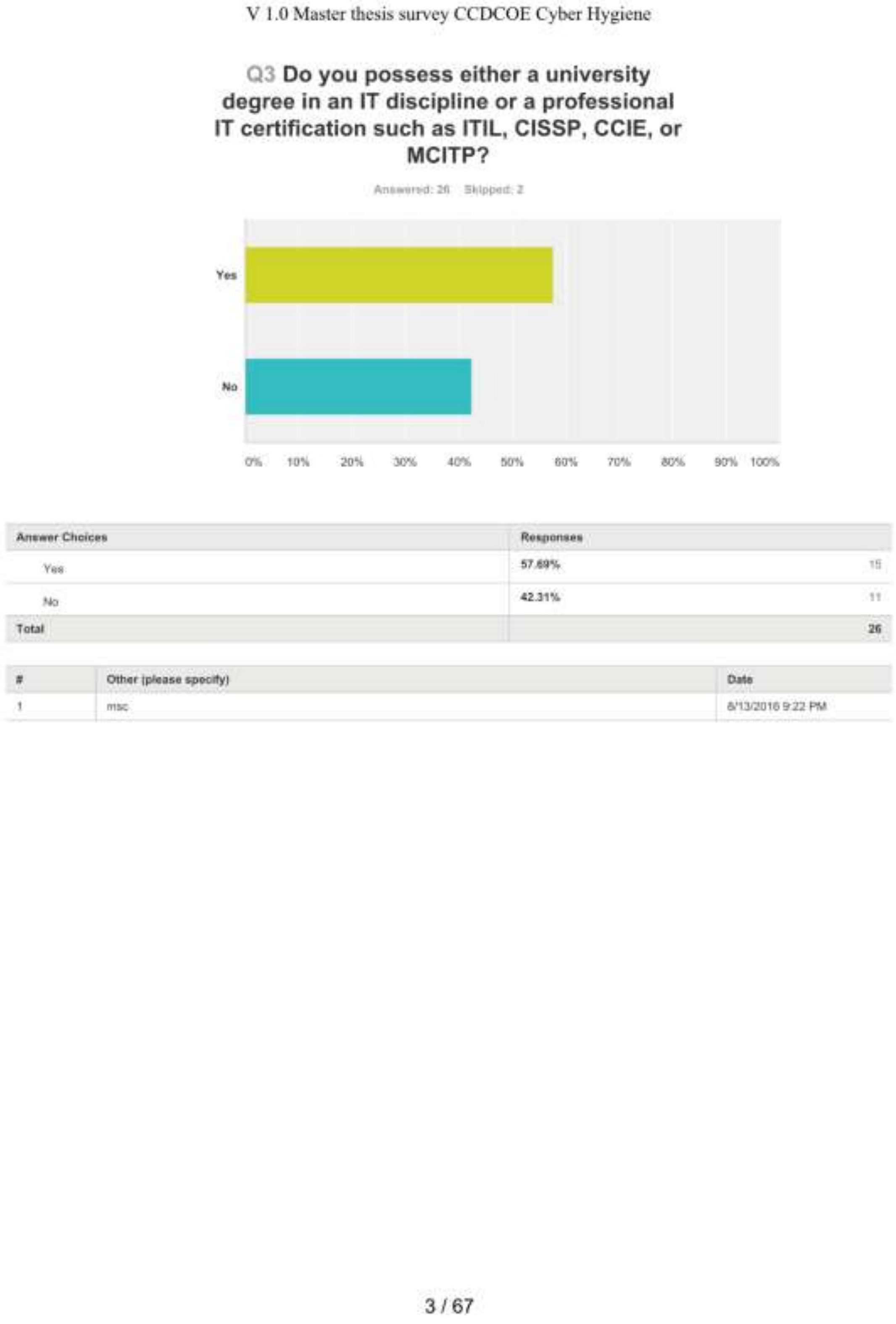
Answered: 0 Skipped: 28

▲ No matching responses.

Answer Choices	Responses	
I do not want to answer this survey at all. In case ticked, I will explain in the next field why.	0.00%	0
Total		0

#	(please specify)	Date
	There are no responses.	

2 / 67



V 1.0 Master thesis survey CCDCOE Cyber Hygiene

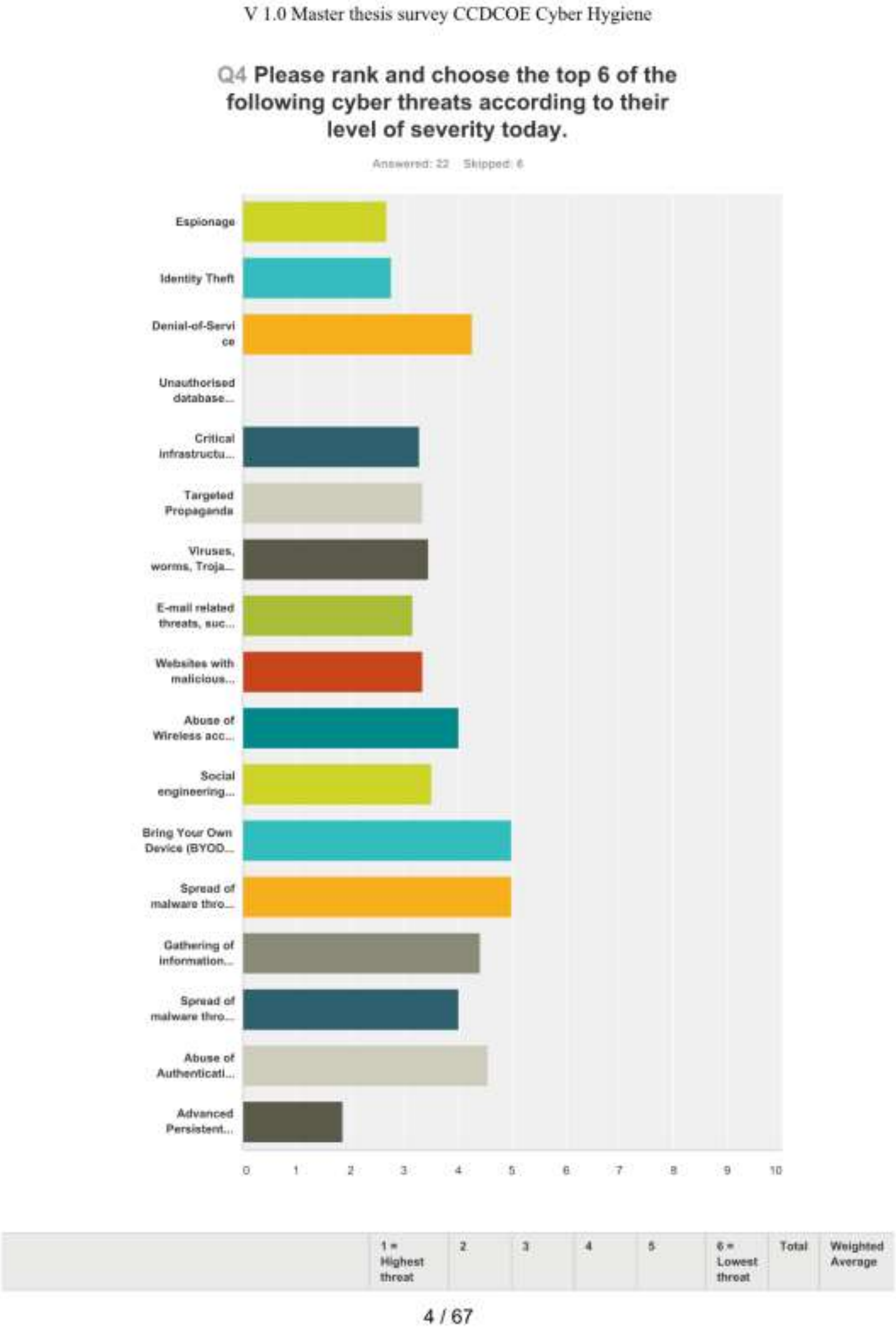
Q3 Do you possess either a university degree in an IT discipline or a professional IT certification such as ITIL, CISSP, CCIE, or MCITP?

Answered: 26 Skipped: 2

Answer Choices	Responses	
Yes	57.69%	15
No	42.31%	11
Total		26

#	Other (please specify)	Date
1	msc	8/13/2016 9:22 PM

3 / 67



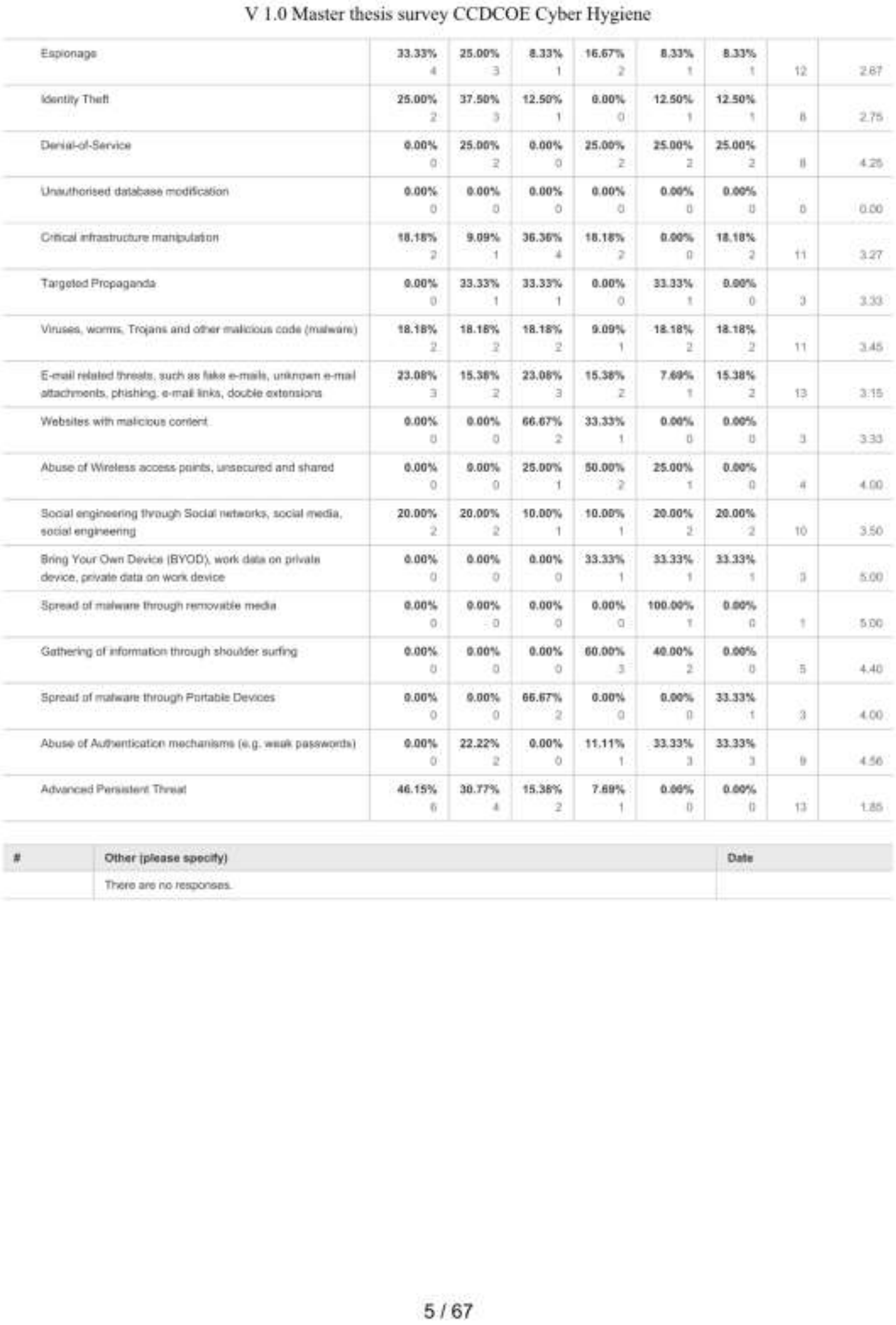
V 1.0 Master thesis survey CCDCOE Cyber Hygiene

Q4 Please rank and choose the top 6 of the following cyber threats according to their level of severity today.

Answered: 22 Skipped: 6

	1 = Highest threat	2	3	4	5	6 = Lowest threat	Total	Weighted Average

4 / 67

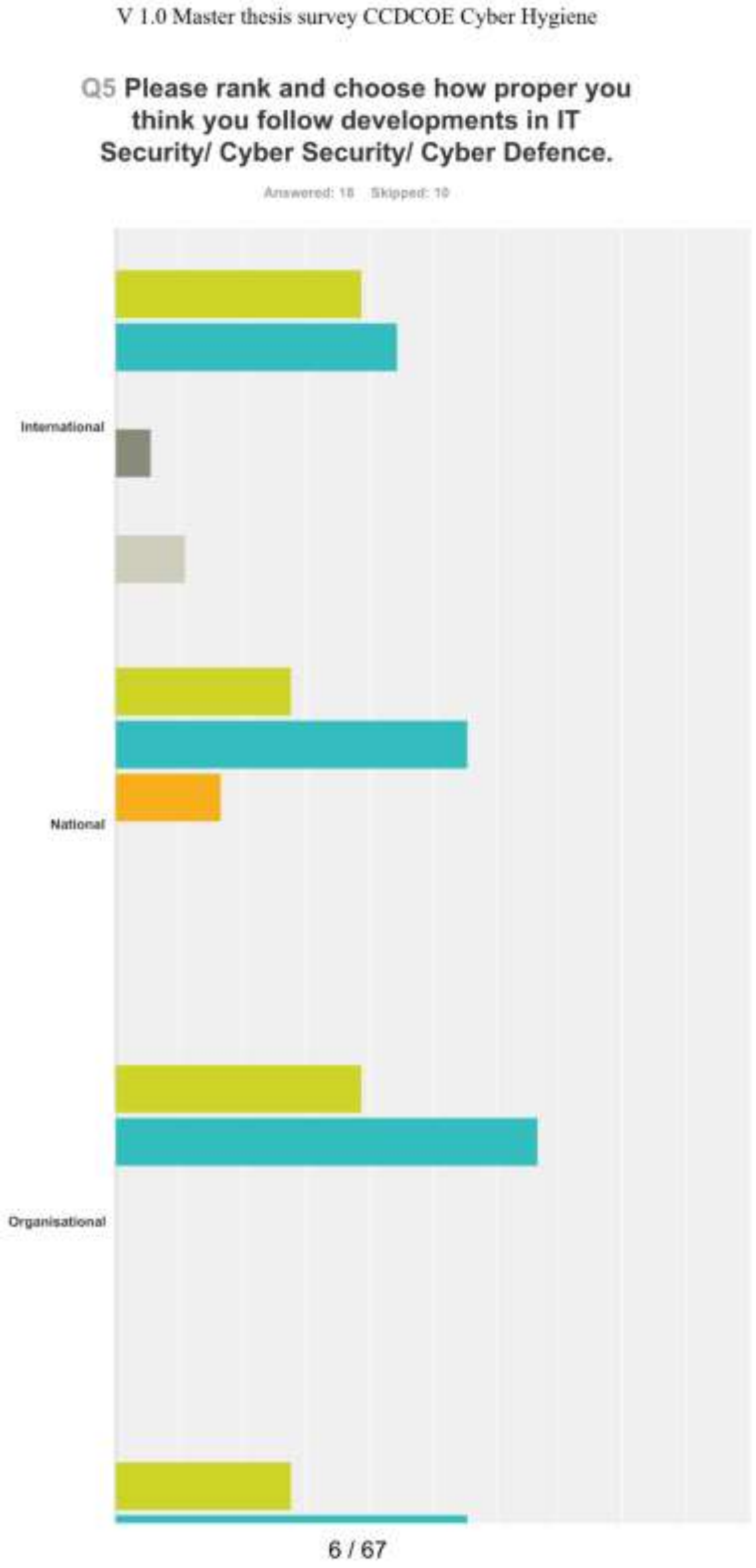


V 1.0 Master thesis survey CCDCOE Cyber Hygiene

Espionage	33.33% 4	25.00% 3	8.33% 1	16.67% 2	8.33% 1	8.33% 1	12	2.67
Identity Theft	25.00% 2	37.50% 3	12.50% 1	0.00% 0	12.50% 1	12.50% 1	8	2.75
Denial-of-Service	0.00% 0	25.00% 2	0.00% 0	25.00% 2	25.00% 2	25.00% 2	8	4.25
Unauthorised database modification	0.00% 0	0.00% 0	0.00% 0	0.00% 0	0.00% 0	0.00% 0	0	0.00
Critical infrastructure manipulation	18.18% 2	9.09% 1	36.36% 4	18.18% 2	0.00% 0	18.18% 2	11	3.27
Targeted Propaganda	0.00% 0	33.33% 1	33.33% 1	0.00% 0	33.33% 1	0.00% 0	3	3.33
Viruses, worms, Trojans and other malicious code (malware)	18.18% 2	18.18% 2	18.18% 2	9.09% 1	18.18% 2	18.18% 2	11	3.45
E-mail related threats, such as fake e-mails, unknown e-mail attachments, phishing, e-mail links, double extensions	23.08% 3	15.38% 2	23.08% 3	15.38% 2	7.69% 1	15.38% 2	13	3.15
Websites with malicious content	0.00% 0	0.00% 0	66.67% 2	33.33% 1	0.00% 0	0.00% 0	3	3.33
Abuse of Wireless access points, unsecured and shared	0.00% 0	0.00% 0	25.00% 1	50.00% 2	25.00% 1	0.00% 0	4	4.00
Social engineering through Social networks, social media, social engineering	20.00% 2	20.00% 2	10.00% 1	10.00% 1	20.00% 2	20.00% 2	10	3.50
Bring Your Own Device (BYOD), work data on private device, private data on work device	0.00% 0	0.00% 0	0.00% 0	33.33% 1	33.33% 1	33.33% 1	3	5.00
Spread of malware through removable media	0.00% 0	0.00% 0	0.00% 0	0.00% 0	100.00% 1	0.00% 0	1	5.00
Gathering of information through shoulder surfing	0.00% 0	0.00% 0	0.00% 0	60.00% 3	40.00% 2	0.00% 0	5	4.40
Spread of malware through Portable Devices	0.00% 0	0.00% 0	66.67% 2	0.00% 0	0.00% 0	33.33% 1	3	4.00
Abuse of Authentication mechanisms (e.g. weak passwords)	0.00% 0	22.22% 2	0.00% 0	11.11% 1	33.33% 3	33.33% 3	9	4.56
Advanced Persistent Threat	46.15% 6	30.77% 4	15.38% 2	7.69% 1	0.00% 0	0.00% 0	13	1.85

#	Other (please specify)	Date
	There are no responses.	

5 / 67

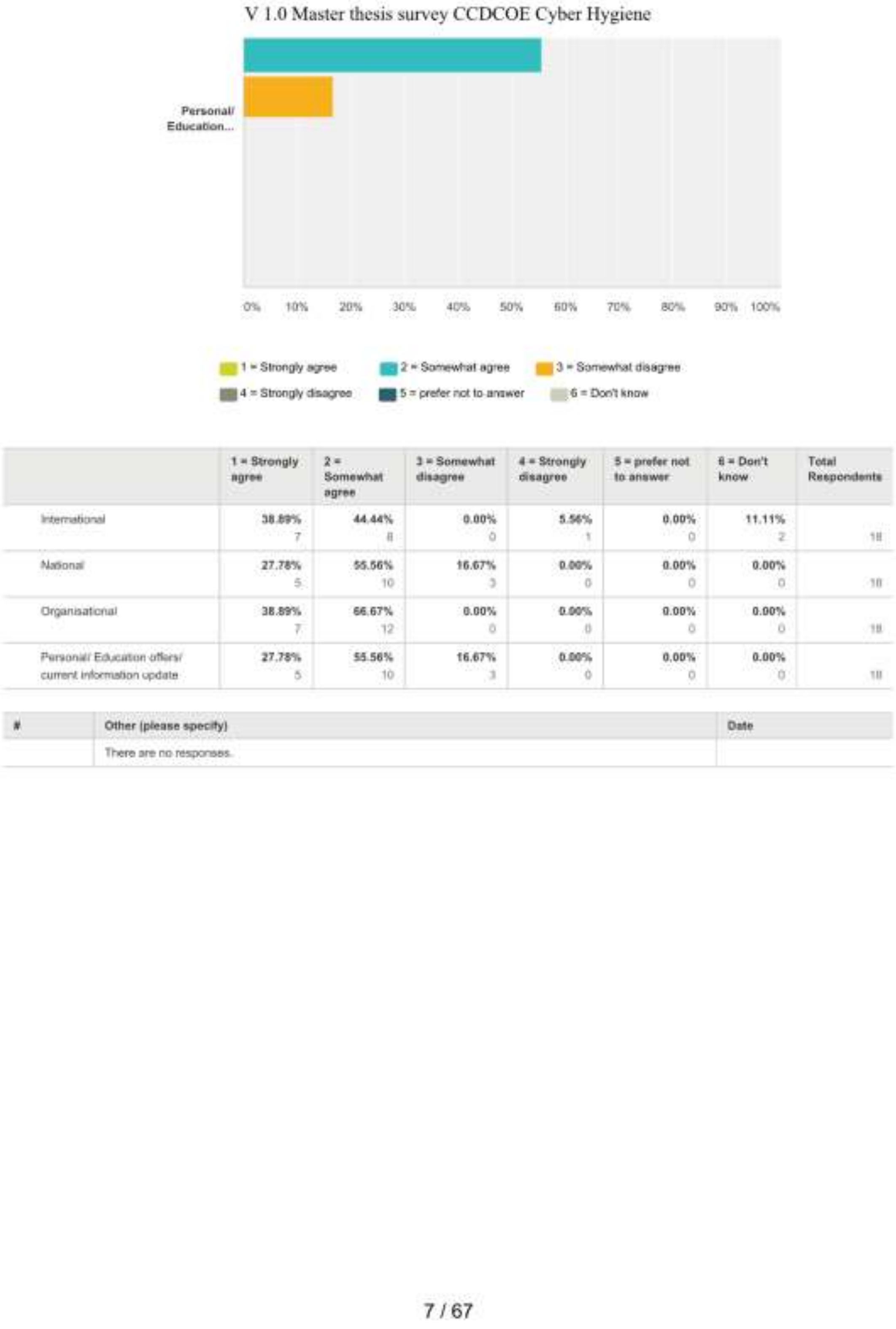


V 1.0 Master thesis survey CCDCOE Cyber Hygiene

Q5 Please rank and choose how proper you think you follow developments in IT Security/ Cyber Security/ Cyber Defence.

Answered: 18 Skipped: 10

6 / 67

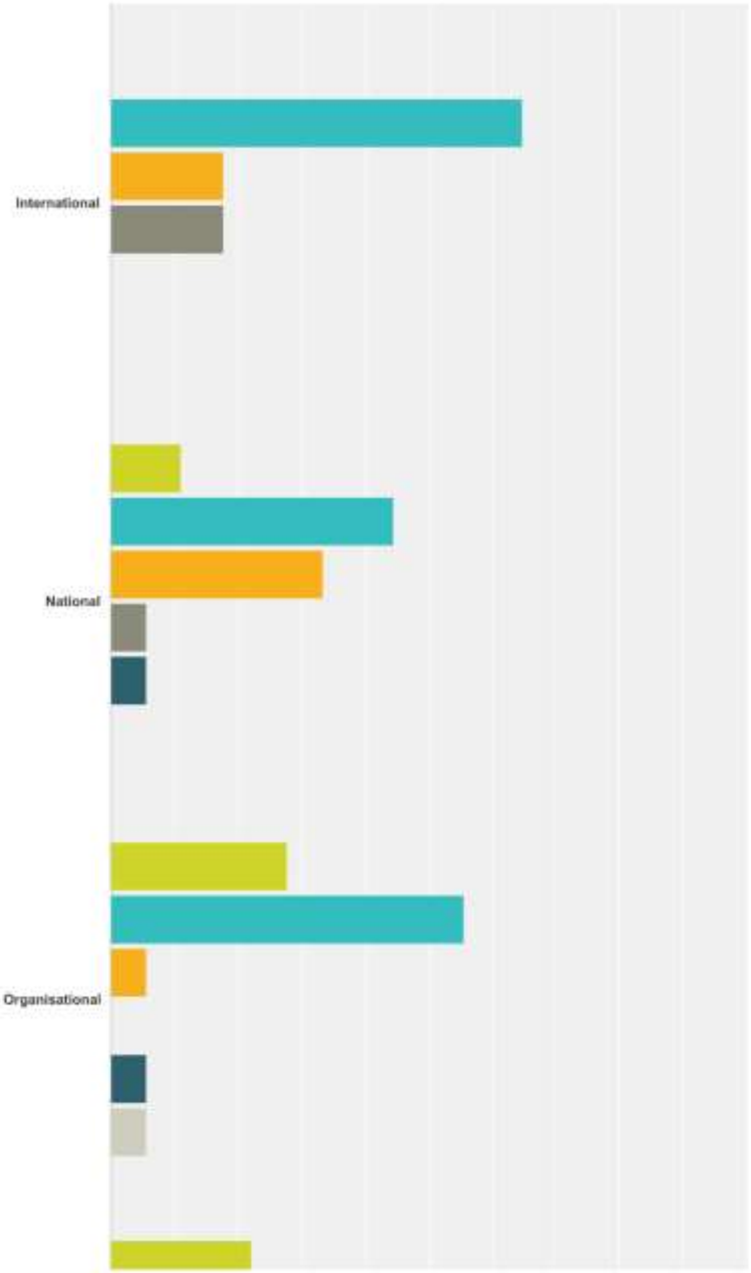


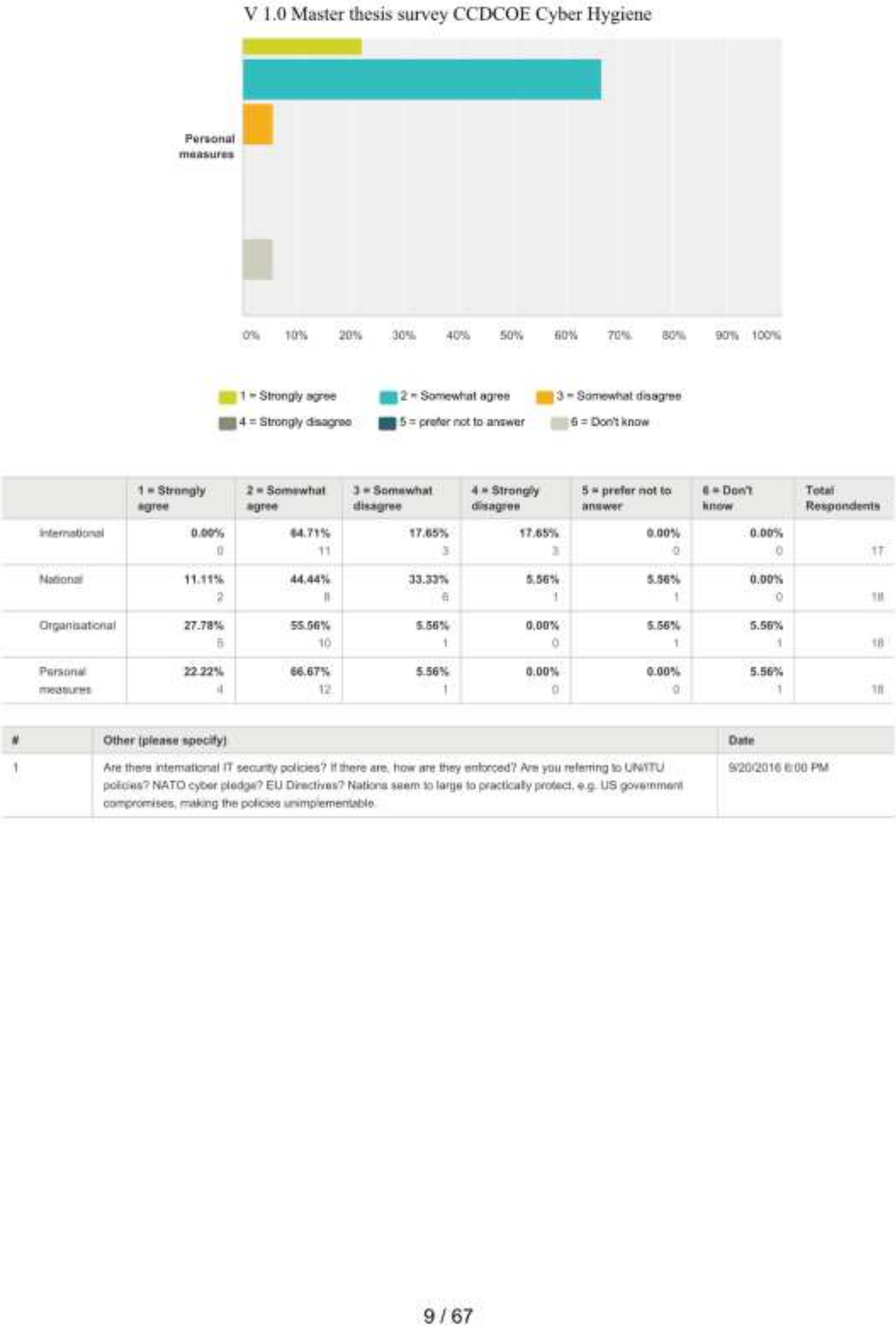
	1 = Strongly agree	2 = Somewhat agree	3 = Somewhat disagree	4 = Strongly disagree	5 = prefer not to answer	6 = Don't know	Total Respondents
International	38.89% 7	44.44% 8	0.00% 0	5.56% 1	0.00% 0	11.11% 2	18
National	27.78% 5	55.56% 10	16.67% 3	0.00% 0	0.00% 0	0.00% 0	18
Organisational	38.89% 7	66.67% 12	0.00% 0	0.00% 0	0.00% 0	0.00% 0	18
Personal/ Education offers/ current information update	27.78% 5	55.56% 10	16.67% 3	0.00% 0	0.00% 0	0.00% 0	18

#	Other (please specify)	Date
	There are no responses.	

Q6 How would you rate your confidence in IT security policies. How good you think they protect security criteria, like confidentiality, integrity and availability?

Answered: 18 Skipped: 10





V 1.0 Master thesis survey CCDCOE Cyber Hygiene

🟨 1 = Strongly agree
🟦 2 = Somewhat agree
🟧 3 = Somewhat disagree
⬛ 4 = Strongly disagree
⬛ 5 = prefer not to answer
⬜ 6 = Don't know

	1 = Strongly agree	2 = Somewhat agree	3 = Somewhat disagree	4 = Strongly disagree	5 = prefer not to answer	6 = Don't know	Total Respondents
International	**0.00%** 0	**64.71%** 11	**17.65%** 3	**17.65%** 3	**0.00%** 0	**0.00%** 0	17
National	**11.11%** 2	**44.44%** 8	**33.33%** 6	**5.56%** 1	**5.56%** 1	**0.00%** 0	18
Organisational	**27.78%** 5	**55.56%** 10	**5.56%** 1	**0.00%** 0	**5.56%** 1	**5.56%** 1	18
Personal measures	**22.22%** 4	**66.67%** 12	**5.56%** 1	**0.00%** 0	**0.00%** 0	**5.56%** 1	18

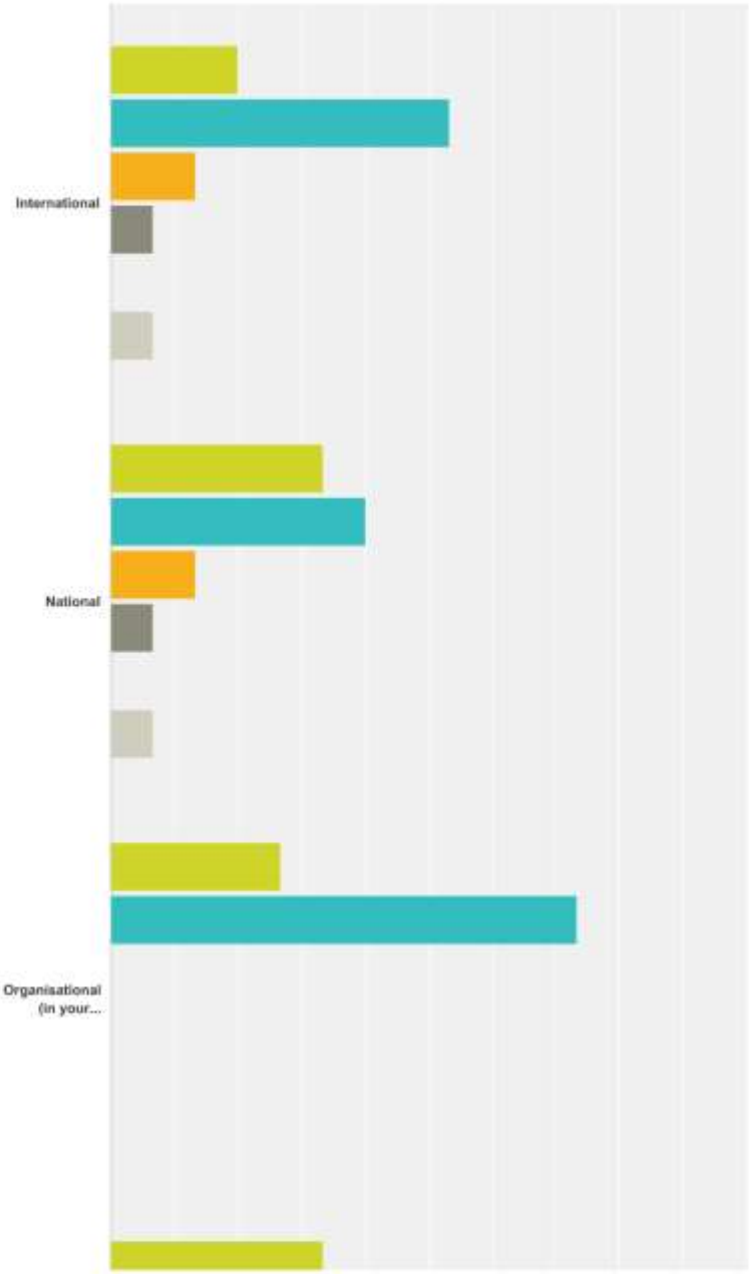
#	Other (please specify)	Date
1	Are there international IT security policies? If there are, how are they enforced? Are you referring to UN/ITU policies? NATO cyber pledge? EU Directives? Nations seem to large to practically protect, e.g. US government compromises, making the policies unimplementable.	9/20/2016 6:00 PM

9 / 67

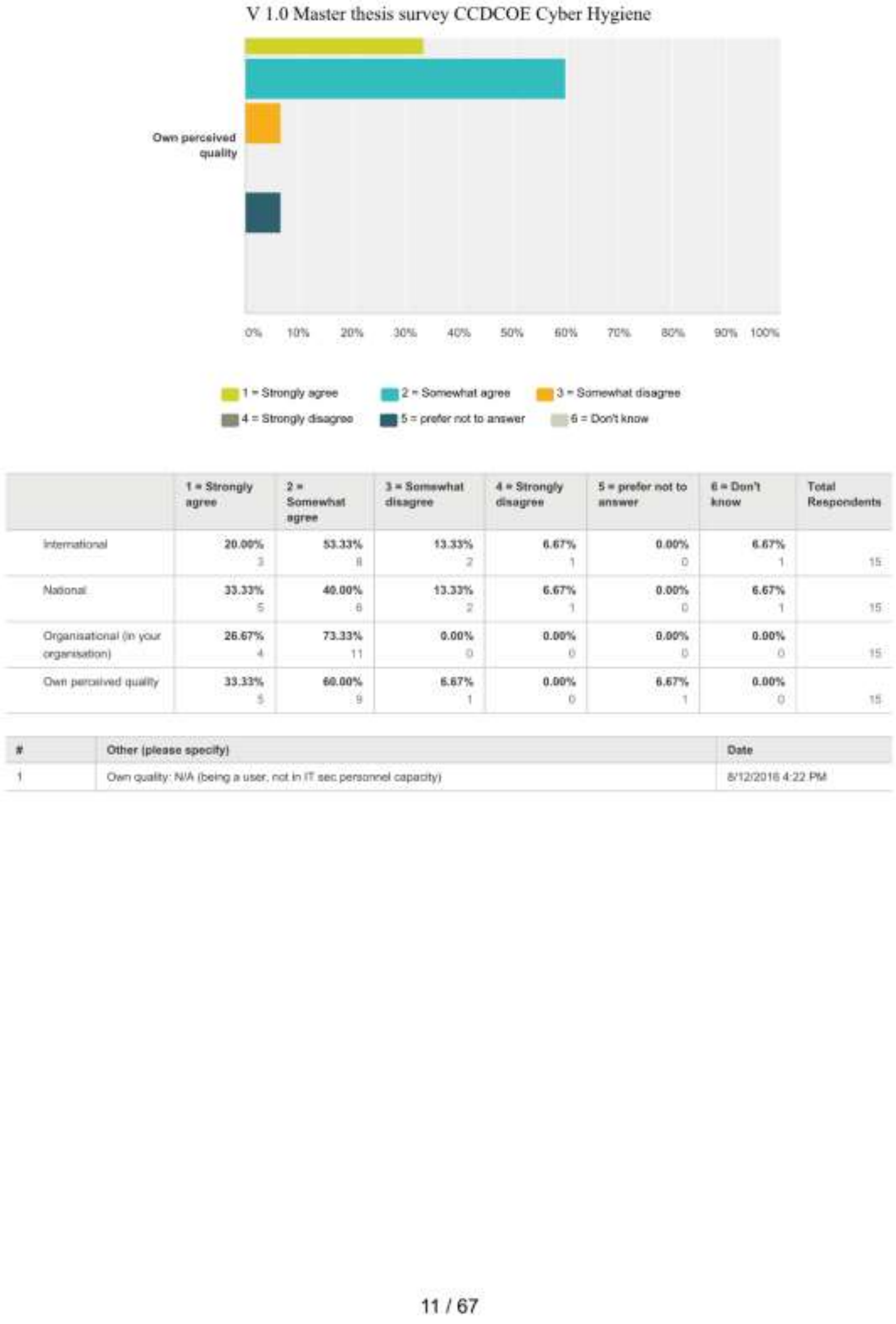
V 1.0 Master thesis survey CCDCOE Cyber Hygiene

Q7 How would you rate the quality (character, willingness to work and further educate themselves) of the IT security *personnel* that is currently in place?

Answered: 15 Skipped: 13



10 / 67



V 1.0 Master thesis survey CCDCOE Cyber Hygiene

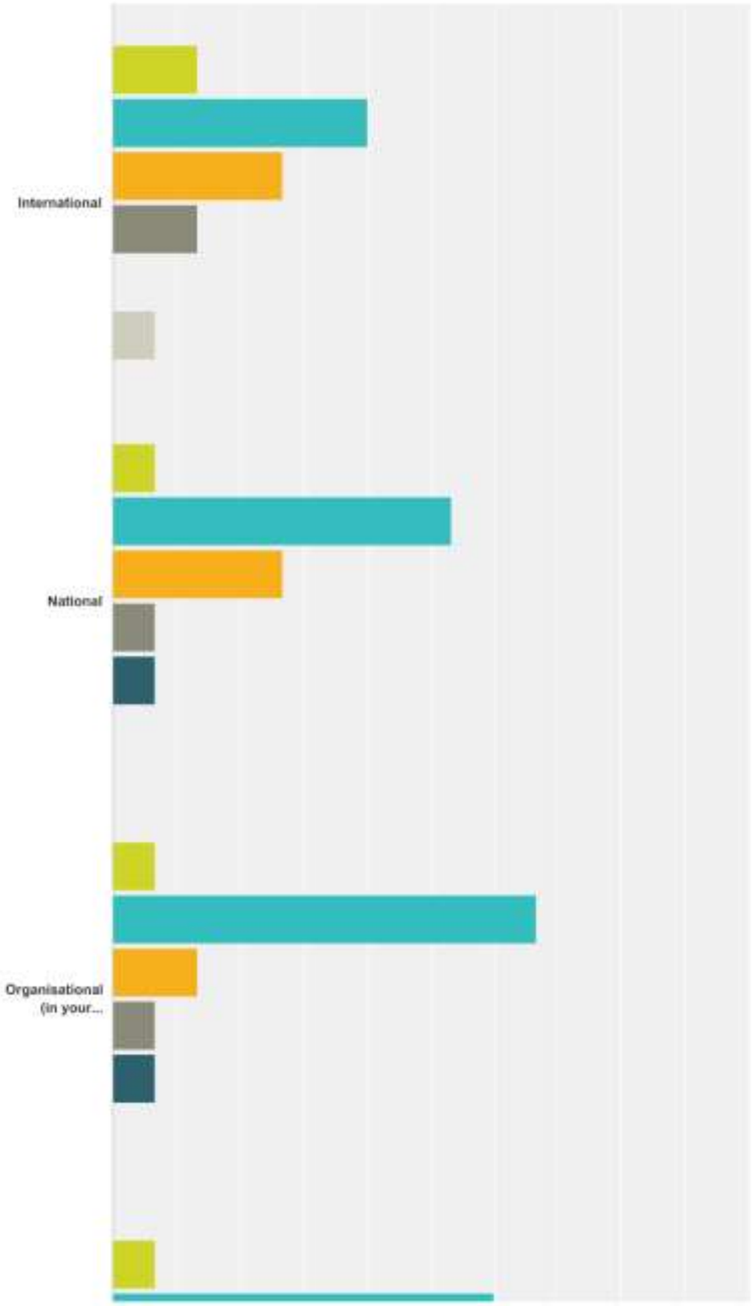
	1 = Strongly agree	2 = Somewhat agree	3 = Somewhat disagree	4 = Strongly disagree	5 = prefer not to answer	6 = Don't know	Total Respondents
International	**20.00%** 3	**53.33%** 8	**13.33%** 2	**6.67%** 1	**0.00%** 0	**6.67%** 1	15
National	**33.33%** 5	**40.00%** 6	**13.33%** 2	**6.67%** 1	**0.00%** 0	**6.67%** 1	15
Organisational (in your organisation)	**26.67%** 4	**73.33%** 11	**0.00%** 0	**0.00%** 0	**0.00%** 0	**0.00%** 0	15
Own perceived quality	**33.33%** 5	**60.00%** 9	**6.67%** 1	**0.00%** 0	**6.67%** 1	**0.00%** 0	15

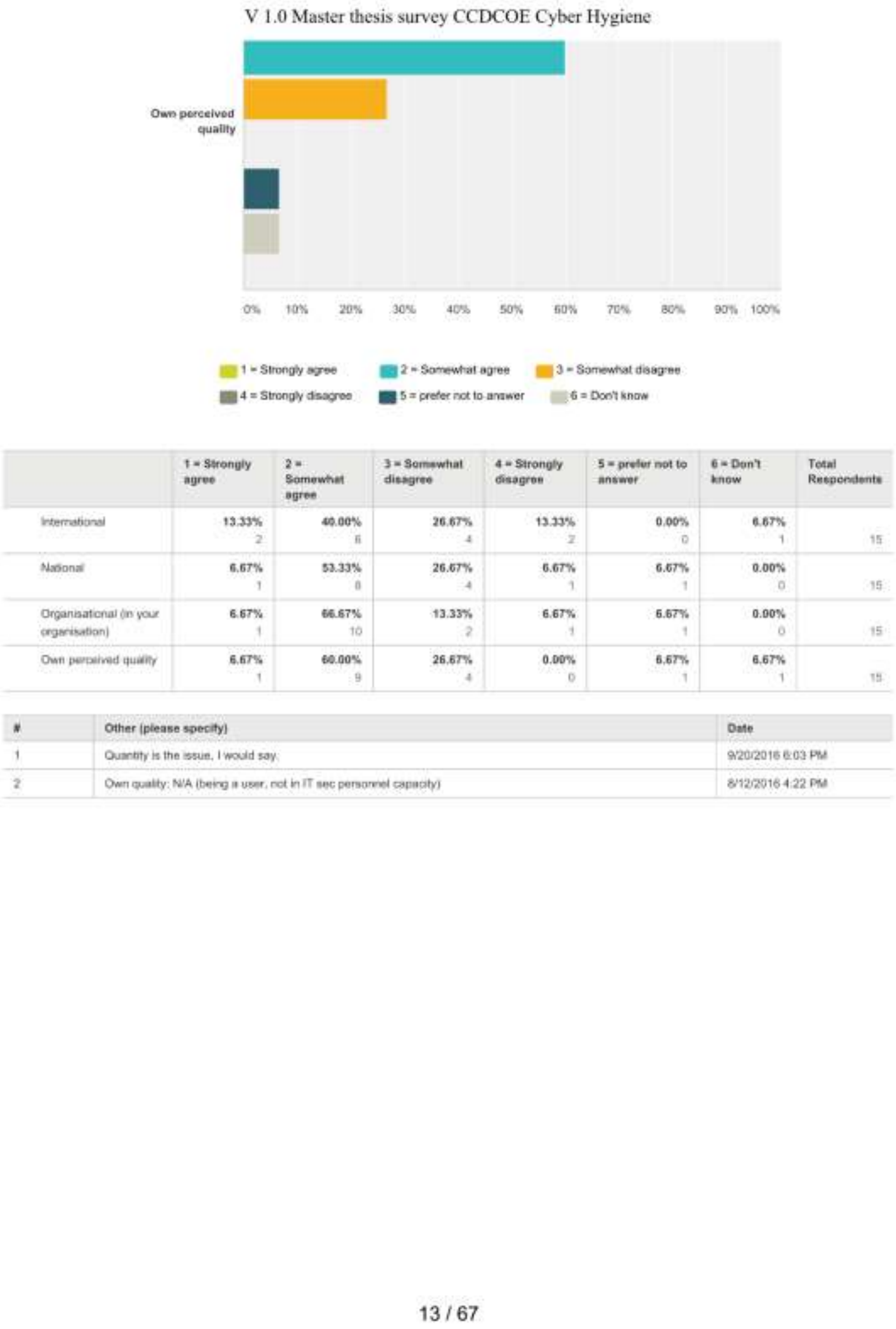
#	Other (please specify)	Date
1	Own quality: N/A (being a user, not in IT sec personnel capacity)	8/12/2016 4:22 PM

11 / 67

Q8 How would you rate the skill-set (skills needed to fulfill the tasks) of the IT security *personnel* that is currently in place?

Answered: 15 Skipped: 13



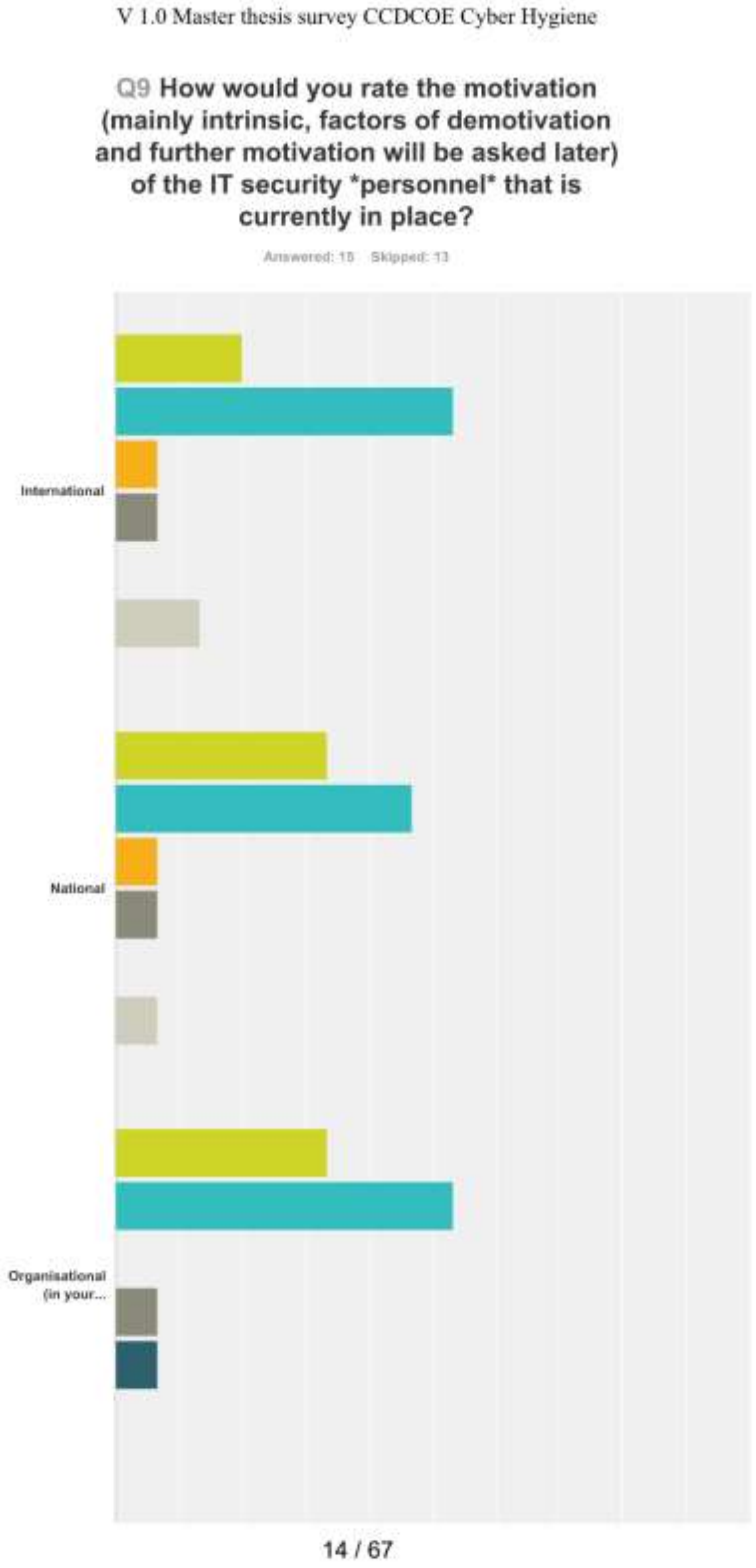


V 1.0 Master thesis survey CCDCOE Cyber Hygiene

	1 = Strongly agree	2 = Somewhat agree	3 = Somewhat disagree	4 = Strongly disagree	5 = prefer not to answer	6 = Don't know	Total Respondents
International	13.33% 2	40.00% 6	26.67% 4	13.33% 2	0.00% 0	6.67% 1	15
National	6.67% 1	53.33% 8	26.67% 4	6.67% 1	6.67% 1	0.00% 0	15
Organisational (in your organisation)	6.67% 1	66.67% 10	13.33% 2	6.67% 1	6.67% 1	0.00% 0	15
Own perceived quality	6.67% 1	60.00% 9	26.67% 4	0.00% 0	6.67% 1	6.67% 1	15

#	Other (please specify)	Date
1	Quantity is the issue, I would say.	9/20/2016 6:03 PM
2	Own quality: N/A (being a user, not in IT sec personnel capacity)	8/12/2016 4:22 PM

13 / 67

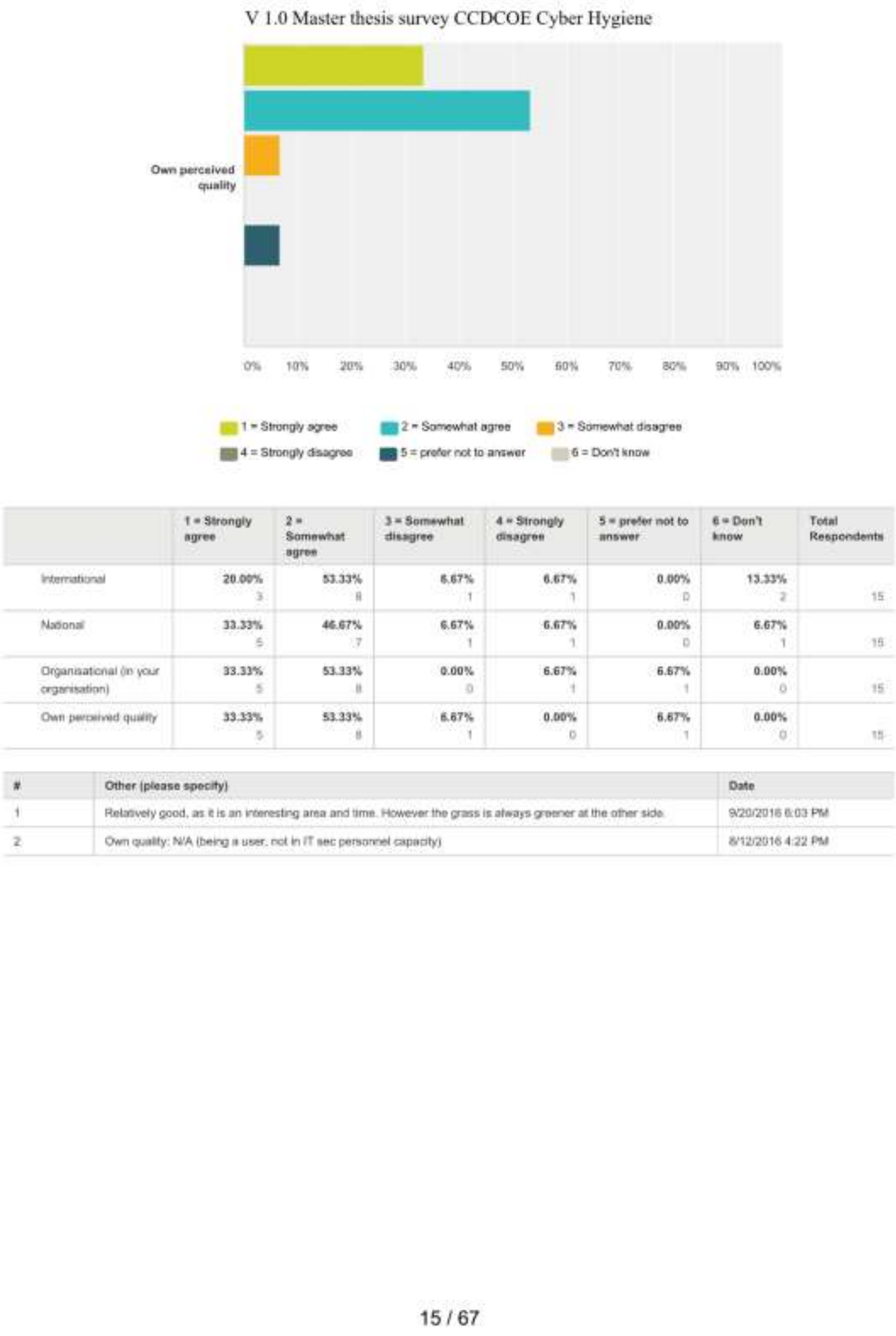


V 1.0 Master thesis survey CCDCOE Cyber Hygiene

Q9 How would you rate the motivation (mainly intrinsic, factors of demotivation and further motivation will be asked later) of the IT security *personnel* that is currently in place?

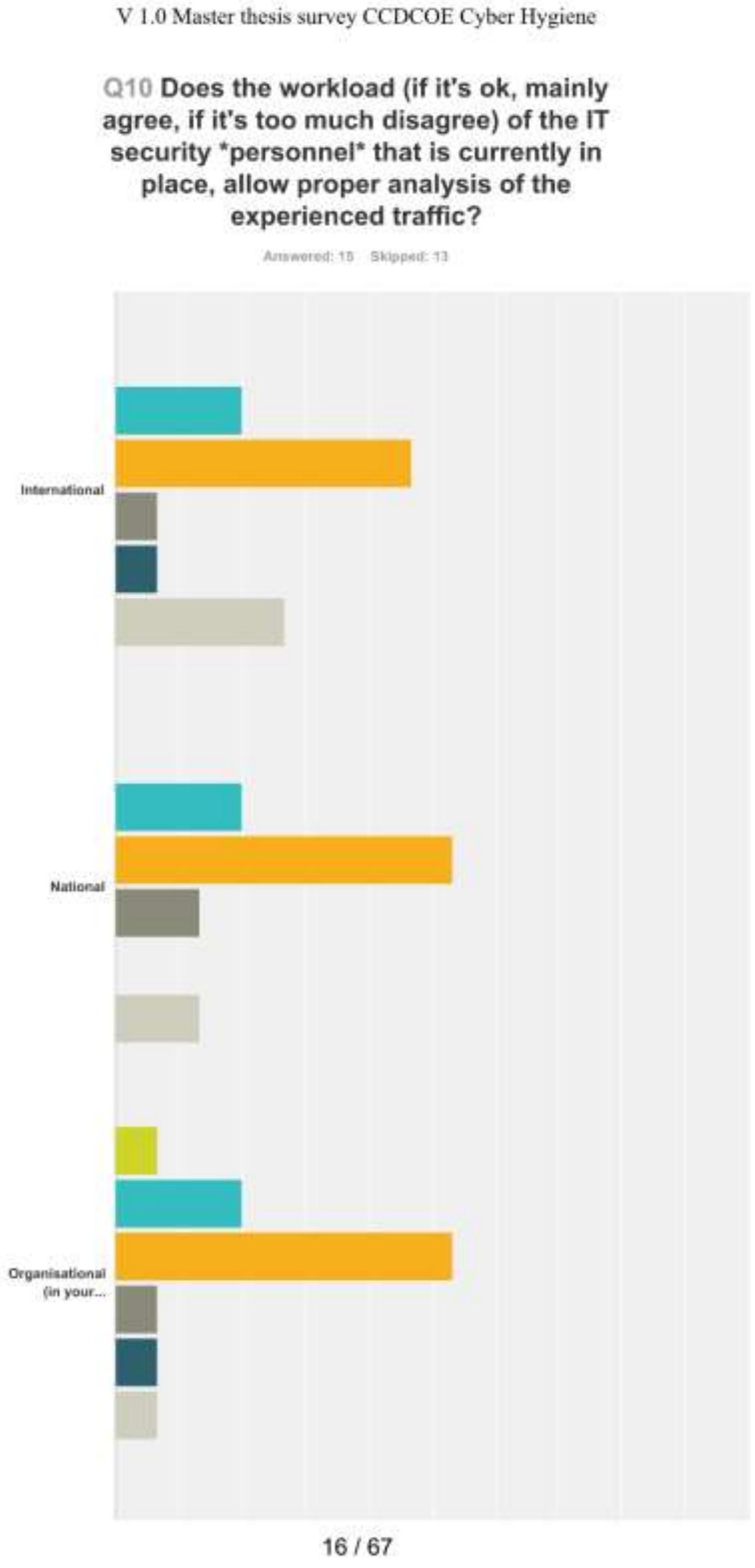
Answered: 15 Skipped: 13

14 / 67



	1 = Strongly agree	2 = Somewhat agree	3 = Somewhat disagree	4 = Strongly disagree	5 = prefer not to answer	6 = Don't know	Total Respondents
International	20.00% 3	53.33% 8	6.67% 1	6.67% 1	0.00% 0	13.33% 2	15
National	33.33% 5	46.67% 7	6.67% 1	6.67% 1	0.00% 0	6.67% 1	15
Organisational (in your organisation)	33.33% 5	53.33% 8	0.00% 0	6.67% 1	6.67% 1	0.00% 0	15
Own perceived quality	33.33% 5	53.33% 8	6.67% 1	0.00% 0	6.67% 1	0.00% 0	15

#	Other (please specify)	Date
1	Relatively good, as it is an interesting area and time. However the grass is always greener at the other side.	9/20/2016 6:03 PM
2	Own quality: N/A (being a user, not in IT sec personnel capacity)	8/12/2016 4:22 PM

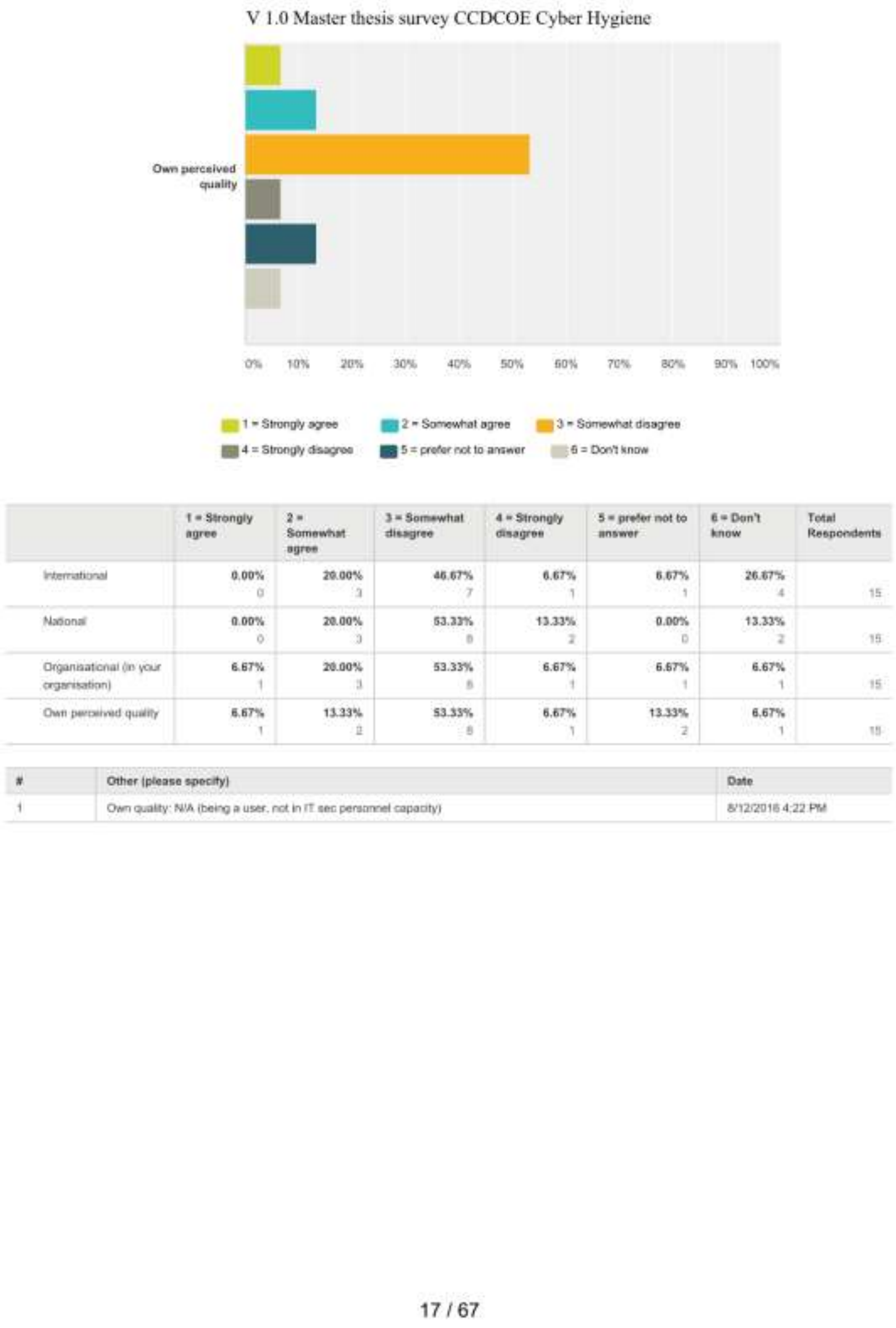


V 1.0 Master thesis survey CCDCOE Cyber Hygiene

Q10 Does the workload (if it's ok, mainly agree, if it's too much disagree) of the IT security *personnel* that is currently in place, allow proper analysis of the experienced traffic?

Answered: 15 Skipped: 13

16 / 67



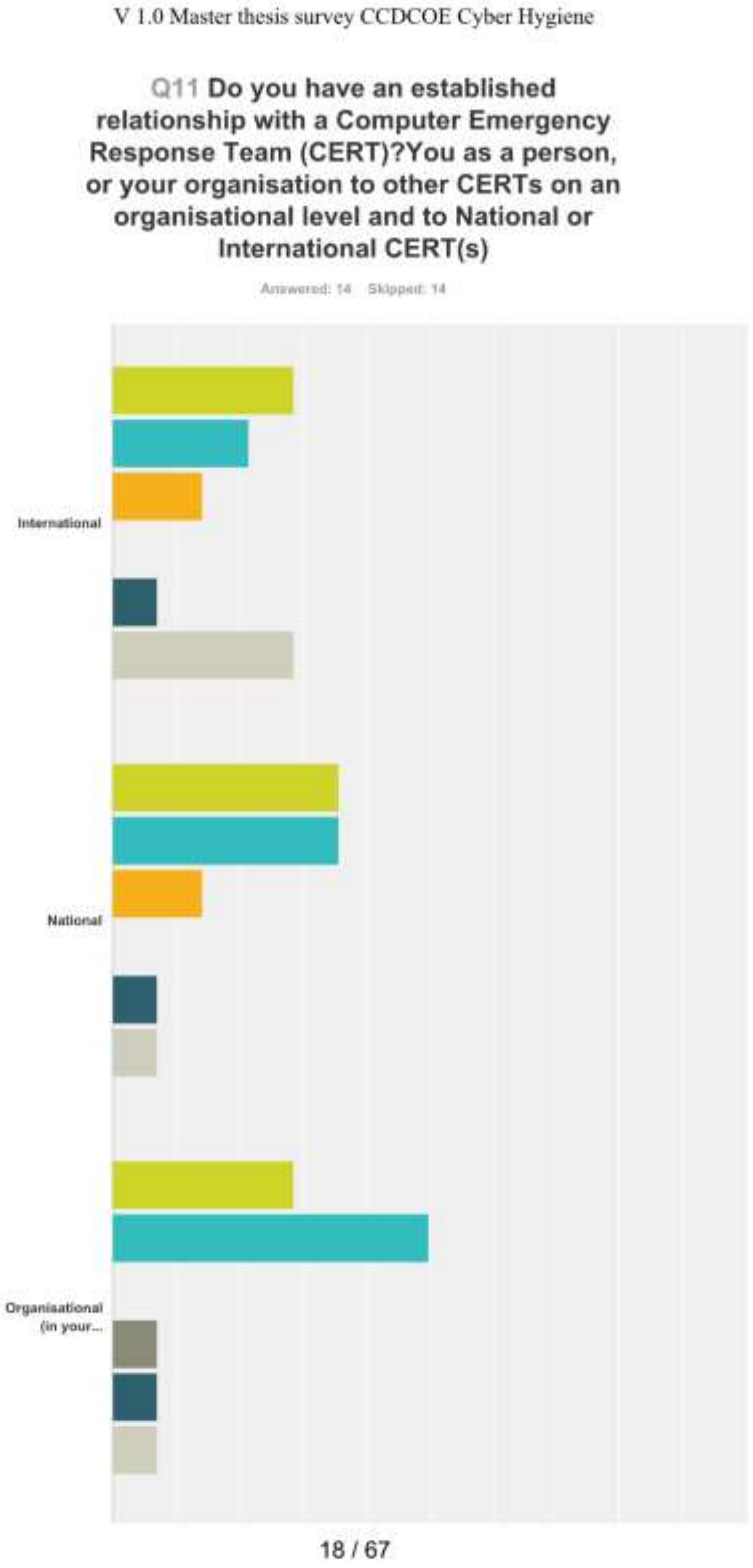
V 1.0 Master thesis survey CCDCOE Cyber Hygiene

- 🟩 1 = Strongly agree
- 🟦 2 = Somewhat agree
- 🟧 3 = Somewhat disagree
- ■ 4 = Strongly disagree
- ■ 5 = prefer not to answer
- □ 6 = Don't know

	1 = Strongly agree	2 = Somewhat agree	3 = Somewhat disagree	4 = Strongly disagree	5 = prefer not to answer	6 = Don't know	Total Respondents
International	0.00% 0	20.00% 3	46.67% 7	6.67% 1	6.67% 1	26.67% 4	15
National	0.00% 0	20.00% 3	53.33% 8	13.33% 2	0.00% 0	13.33% 2	15
Organisational (in your organisation)	6.67% 1	20.00% 3	53.33% 8	6.67% 1	6.67% 1	6.67% 1	15
Own perceived quality	6.67% 1	13.33% 2	53.33% 8	6.67% 1	13.33% 2	6.67% 1	15

#	Other (please specify)	Date
1	Own quality: N/A (being a user, not in IT sec personnel capacity)	8/12/2016 4:22 PM

17 / 67

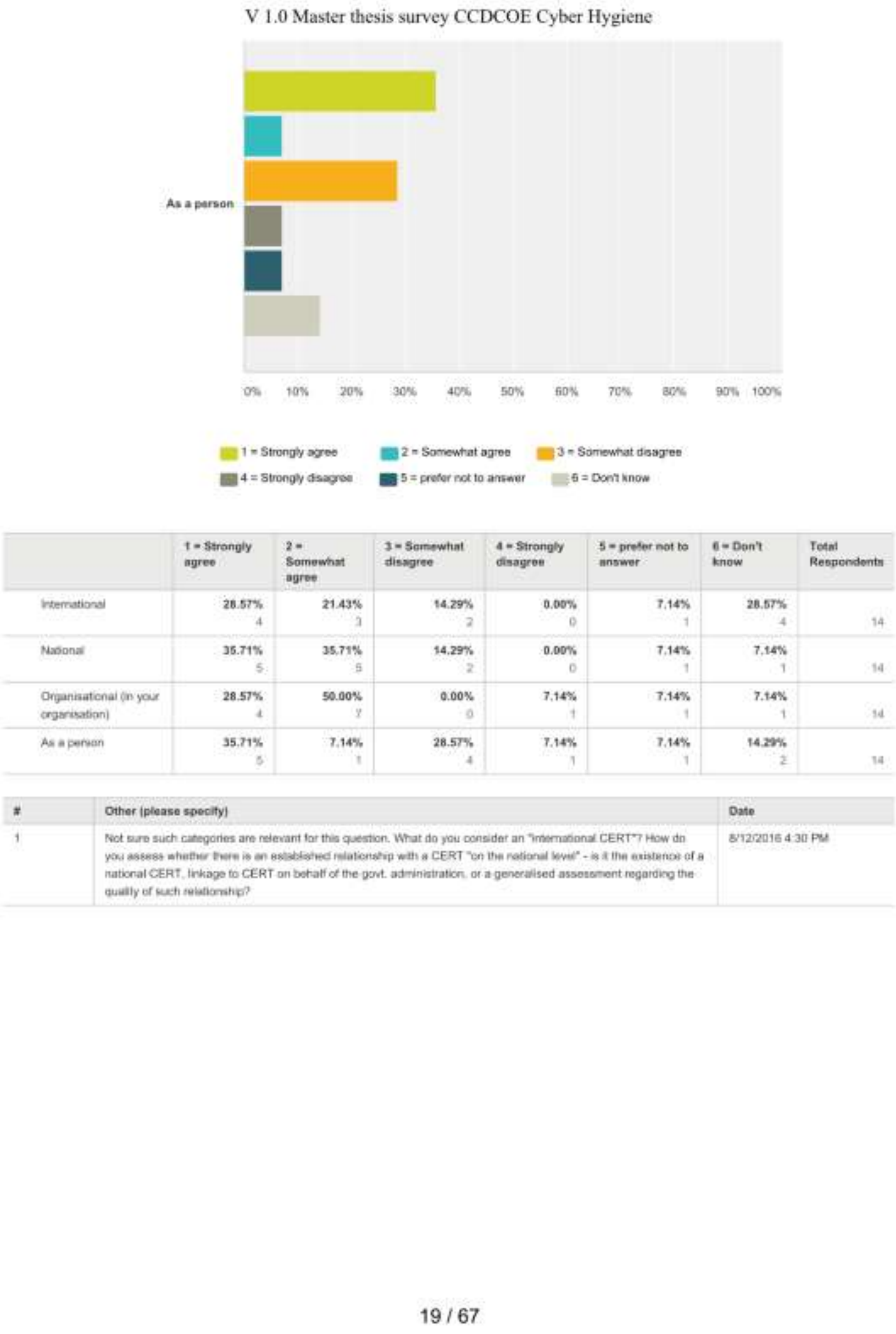


V 1.0 Master thesis survey CCDCOE Cyber Hygiene

Q11 Do you have an established relationship with a Computer Emergency Response Team (CERT)?You as a person, or your organisation to other CERTs on an organisational level and to National or International CERT(s)

Answered: 14 Skipped: 14

18 / 67



V 1.0 Master thesis survey CCDCOE Cyber Hygiene

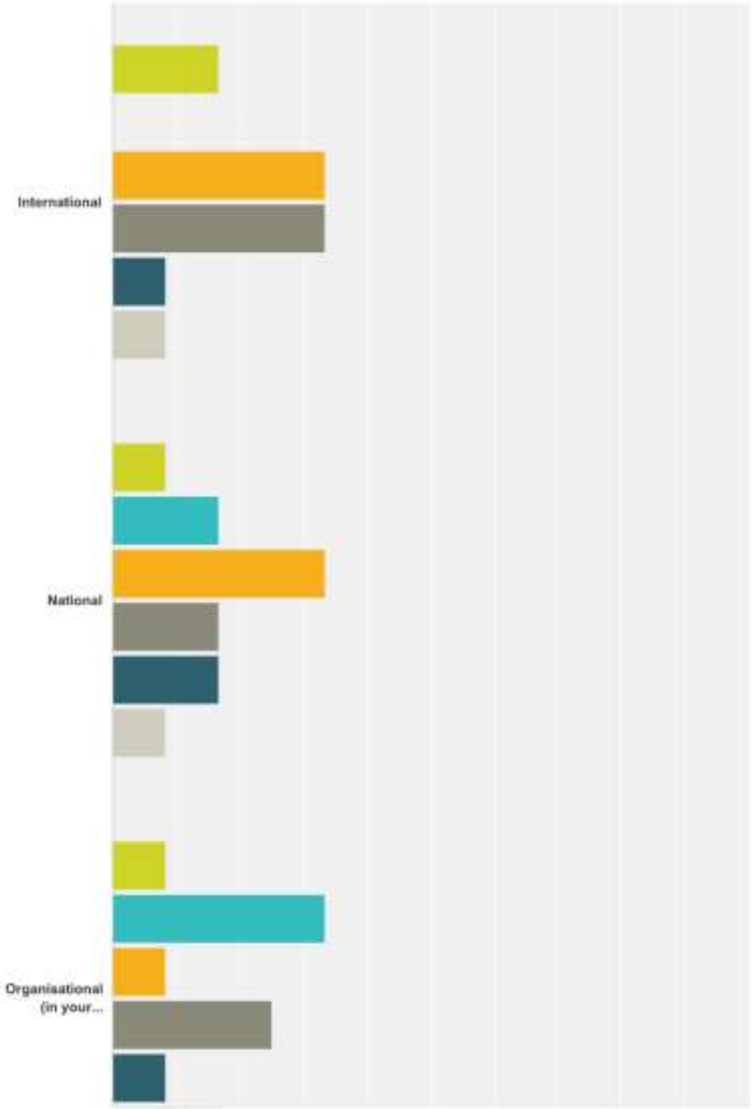
	1 = Strongly agree	2 = Somewhat agree	3 = Somewhat disagree	4 = Strongly disagree	5 = prefer not to answer	6 = Don't know	Total Respondents
International	28.57% 4	21.43% 3	14.29% 2	0.00% 0	7.14% 1	28.57% 4	14
National	35.71% 5	35.71% 5	14.29% 2	0.00% 0	7.14% 1	7.14% 1	14
Organisational (in your organisation)	28.57% 4	50.00% 7	0.00% 0	7.14% 1	7.14% 1	7.14% 1	14
As a person	35.71% 5	7.14% 1	28.57% 4	7.14% 1	7.14% 1	14.29% 2	14

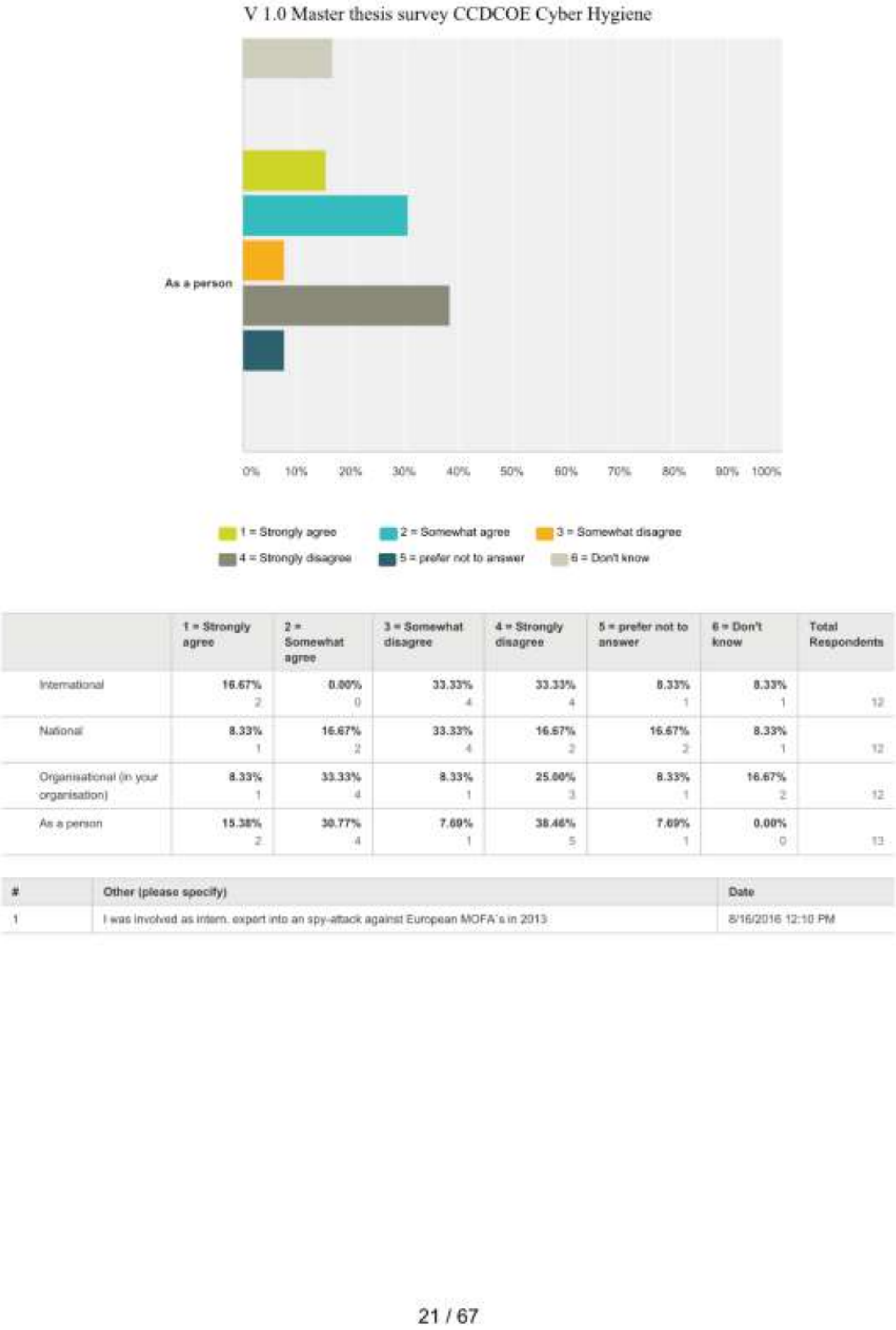
#	Other (please specify)	Date
1	Not sure such categories are relevant for this question. What do you consider an "International CERT"? How do you assess whether there is an established relationship with a CERT "on the national level" - is it the existence of a national CERT, linkage to CERT on behalf of the govt. administration, or a generalised assessment regarding the quality of such relationship?	8/12/2016 4:30 PM

19 / 67

Q12 Have you participated in a cyber intrusion investigation? You as a person (out of interest, if it lead to an "official" dealing (maybe even court-case), please mention that in Organisational agreement and National. If it was an international case... Fell free to comment on more details, if your special case was more complex.

Answered: 13 Skipped: 15



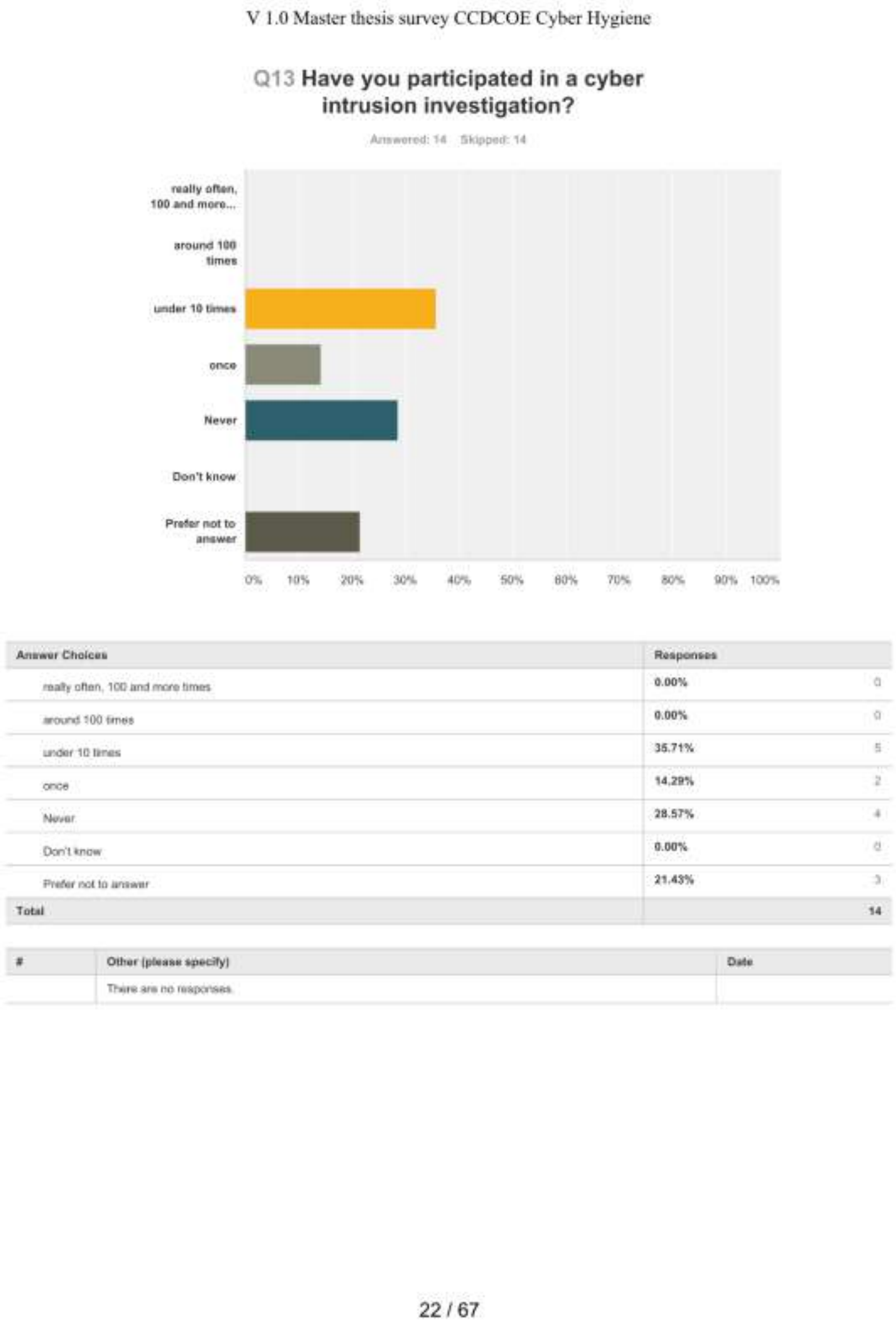


V 1.0 Master thesis survey CCDCOE Cyber Hygiene

	1 = Strongly agree	2 = Somewhat agree	3 = Somewhat disagree	4 = Strongly disagree	5 = prefer not to answer	6 = Don't know	Total Respondents
International	16.67% 2	0.00% 0	33.33% 4	33.33% 4	8.33% 1	8.33% 1	12
National	8.33% 1	16.67% 2	33.33% 4	16.67% 2	16.67% 2	8.33% 1	12
Organisational (in your organisation)	8.33% 1	33.33% 4	8.33% 1	25.00% 3	8.33% 1	16.67% 2	12
As a person	15.38% 2	30.77% 4	7.69% 1	38.46% 5	7.69% 1	0.00% 0	13

#	Other (please specify)	Date
1	I was involved as intern. expert into an spy-attack against European MOFA´s in 2013	8/16/2016 12:10 PM

21 / 67

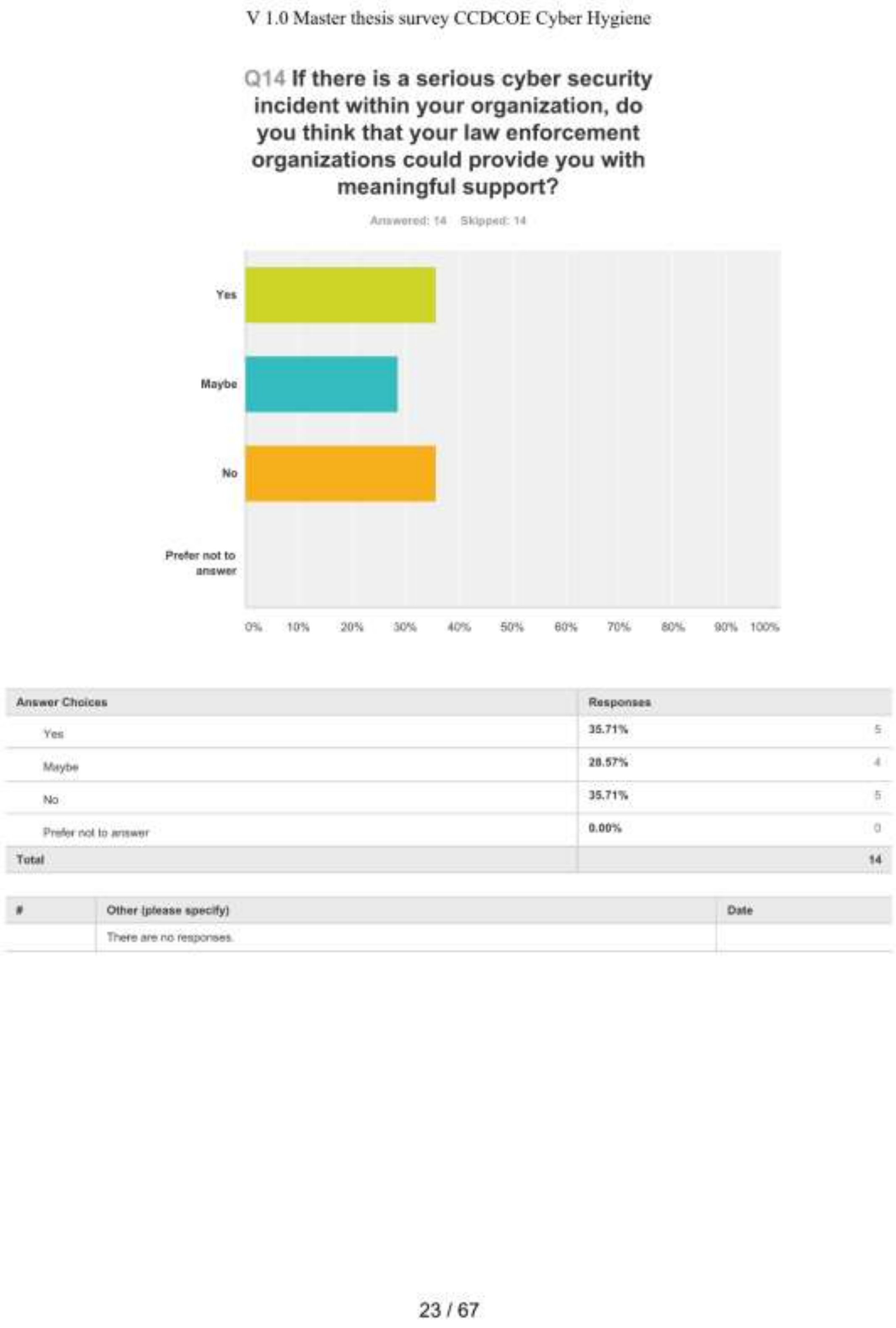


Q13 Have you participated in a cyber intrusion investigation?

Answered: 14 Skipped: 14

Answer Choices	Responses	
really often, 100 and more times	0.00%	0
around 100 times	0.00%	0
under 10 times	35.71%	5
once	14.29%	2
Never	28.57%	4
Don't know	0.00%	0
Prefer not to answer	21.43%	3
Total		14

#	Other (please specify)	Date
	There are no responses.	



V 1.0 Master thesis survey CCDCOE Cyber Hygiene

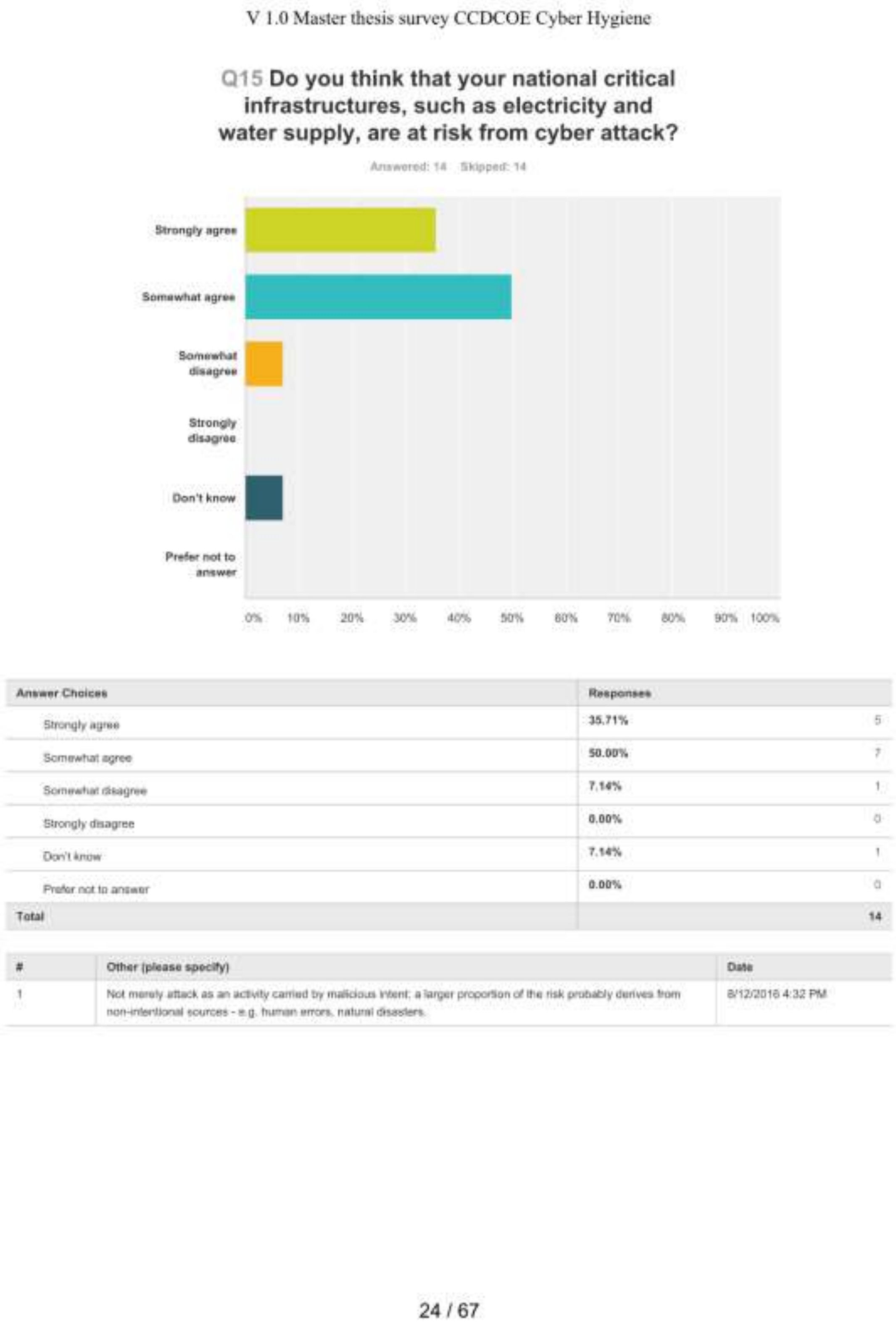
Q14 If there is a serious cyber security incident within your organization, do you think that your law enforcement organizations could provide you with meaningful support?

Answered: 14 Skipped: 14

Answer Choices	Responses	
Yes	35.71%	5
Maybe	28.57%	4
No	35.71%	5
Prefer not to answer	0.00%	0
Total		14

#	Other (please specify)	Date
	There are no responses.	

23 / 67



V 1.0 Master thesis survey CCDCOE Cyber Hygiene

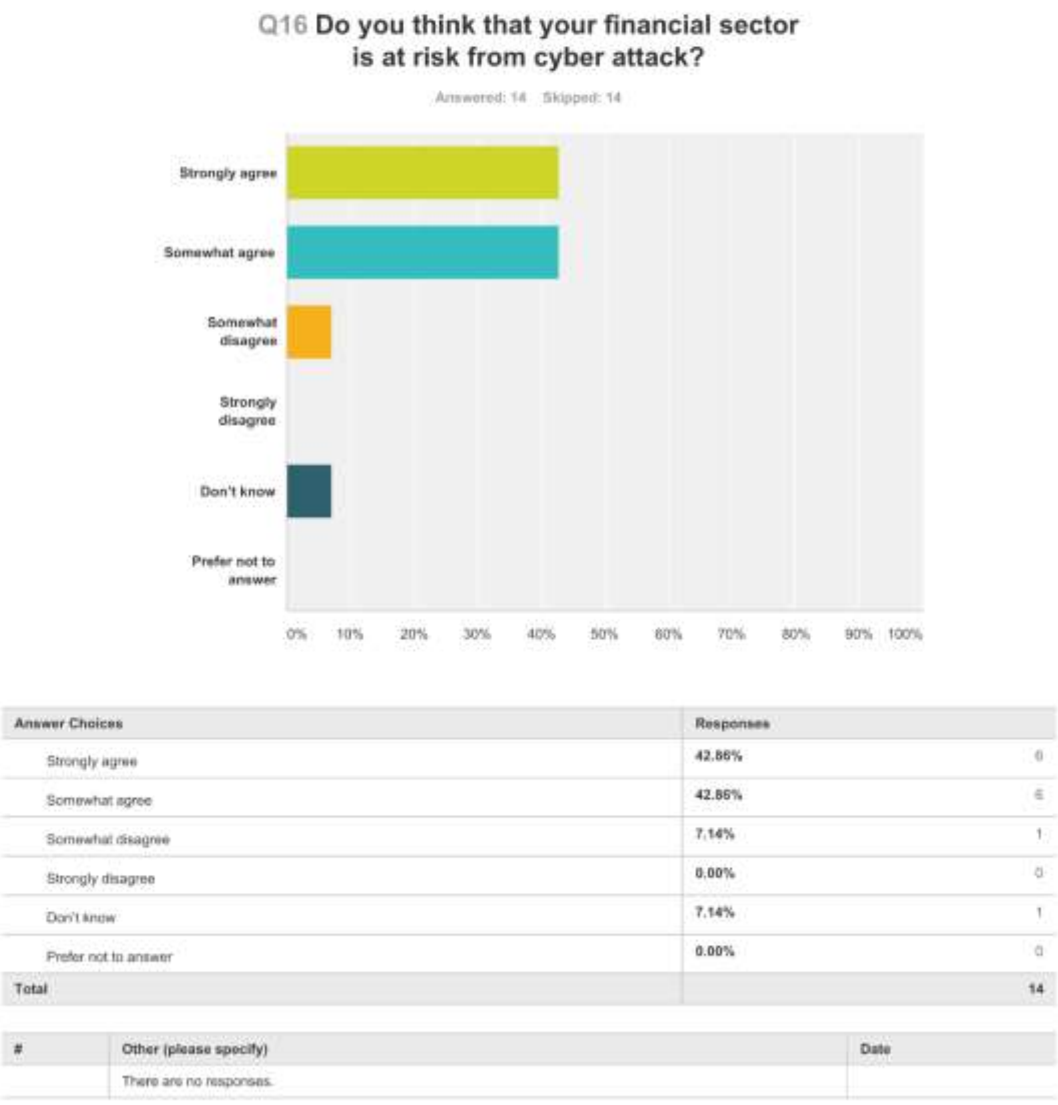
Q15 Do you think that your national critical infrastructures, such as electricity and water supply, are at risk from cyber attack?

Answered: 14 Skipped: 14

Answer Choices	Responses	
Strongly agree	35.71%	5
Somewhat agree	50.00%	7
Somewhat disagree	7.14%	1
Strongly disagree	0.00%	0
Don't know	7.14%	1
Prefer not to answer	0.00%	0
Total		14

#	Other (please specify)	Date
1	Not merely attack as an activity carried by malicious intent; a larger proportion of the risk probably derives from non-intentional sources - e.g. human errors, natural disasters.	8/12/2016 4:32 PM

24 / 67

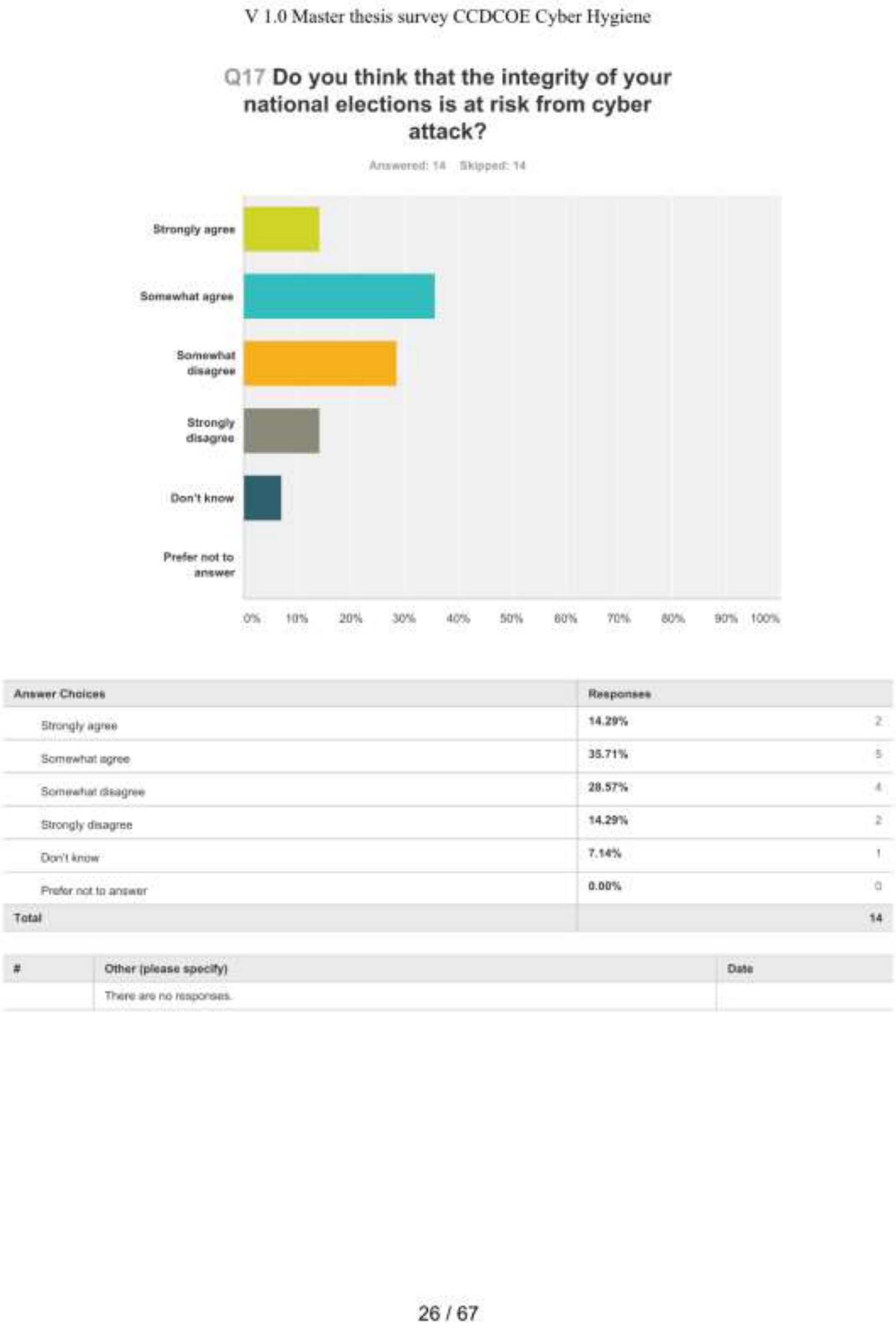


Q16 Do you think that your financial sector is at risk from cyber attack?

Answered: 14 Skipped: 14

Answer Choices	Responses	
Strongly agree	42.86%	6
Somewhat agree	42.86%	6
Somewhat disagree	7.14%	1
Strongly disagree	0.00%	0
Don't know	7.14%	1
Prefer not to answer	0.00%	0
Total		14

#	Other (please specify)	Date
	There are no responses.	



V 1.0 Master thesis survey CCDCOE Cyber Hygiene

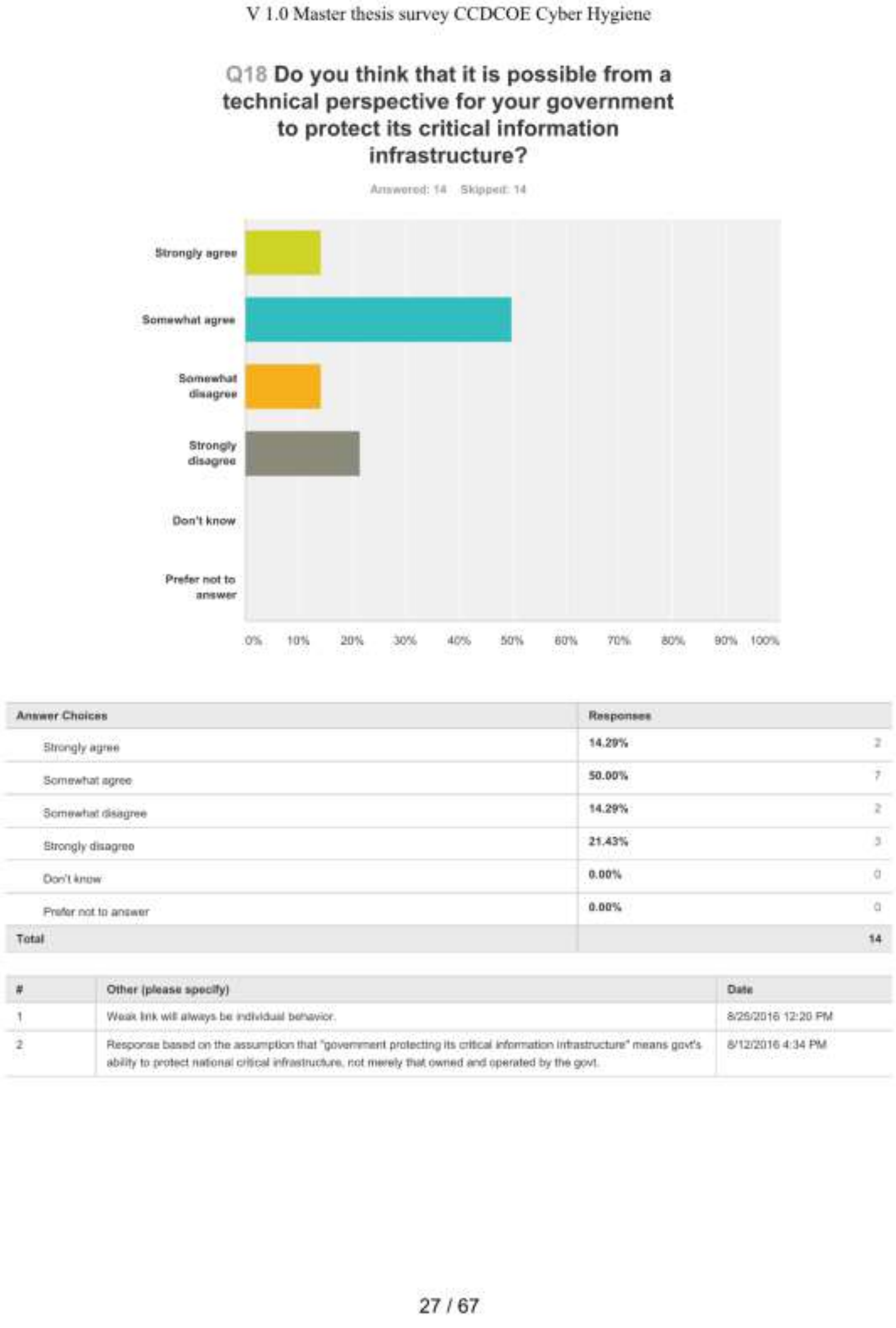
Q17 Do you think that the integrity of your national elections is at risk from cyber attack?

Answered: 14 Skipped: 14

Answer Choices	Responses	
Strongly agree	14.29%	2
Somewhat agree	35.71%	5
Somewhat disagree	28.57%	4
Strongly disagree	14.29%	2
Don't know	7.14%	1
Prefer not to answer	0.00%	0
Total		14

#	Other (please specify)	Date
	There are no responses.	

26 / 67

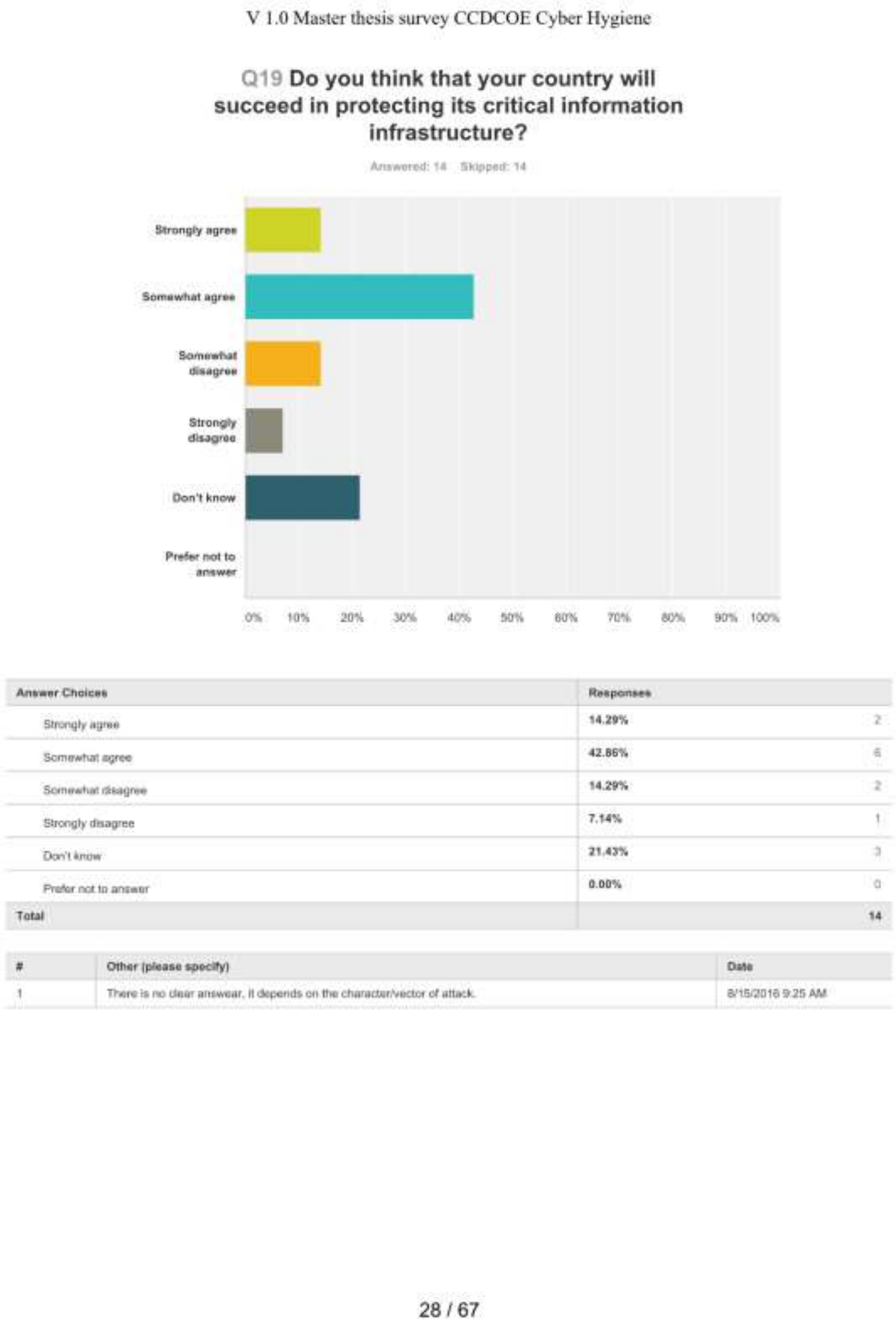


Q18 Do you think that it is possible from a technical perspective for your government to protect its critical information infrastructure?

Answered: 14 Skipped: 14

Answer Choices	Responses	
Strongly agree	14.29%	2
Somewhat agree	50.00%	7
Somewhat disagree	14.29%	2
Strongly disagree	21.43%	3
Don't know	0.00%	0
Prefer not to answer	0.00%	0
Total		14

#	Other (please specify)	Date
1	Weak link will always be individual behavior.	8/26/2016 12:20 PM
2	Response based on the assumption that "government protecting its critical information infrastructure" means govt's ability to protect national critical infrastructure, not merely that owned and operated by the govt.	8/12/2016 4:34 PM



V 1.0 Master thesis survey CCDCOE Cyber Hygiene

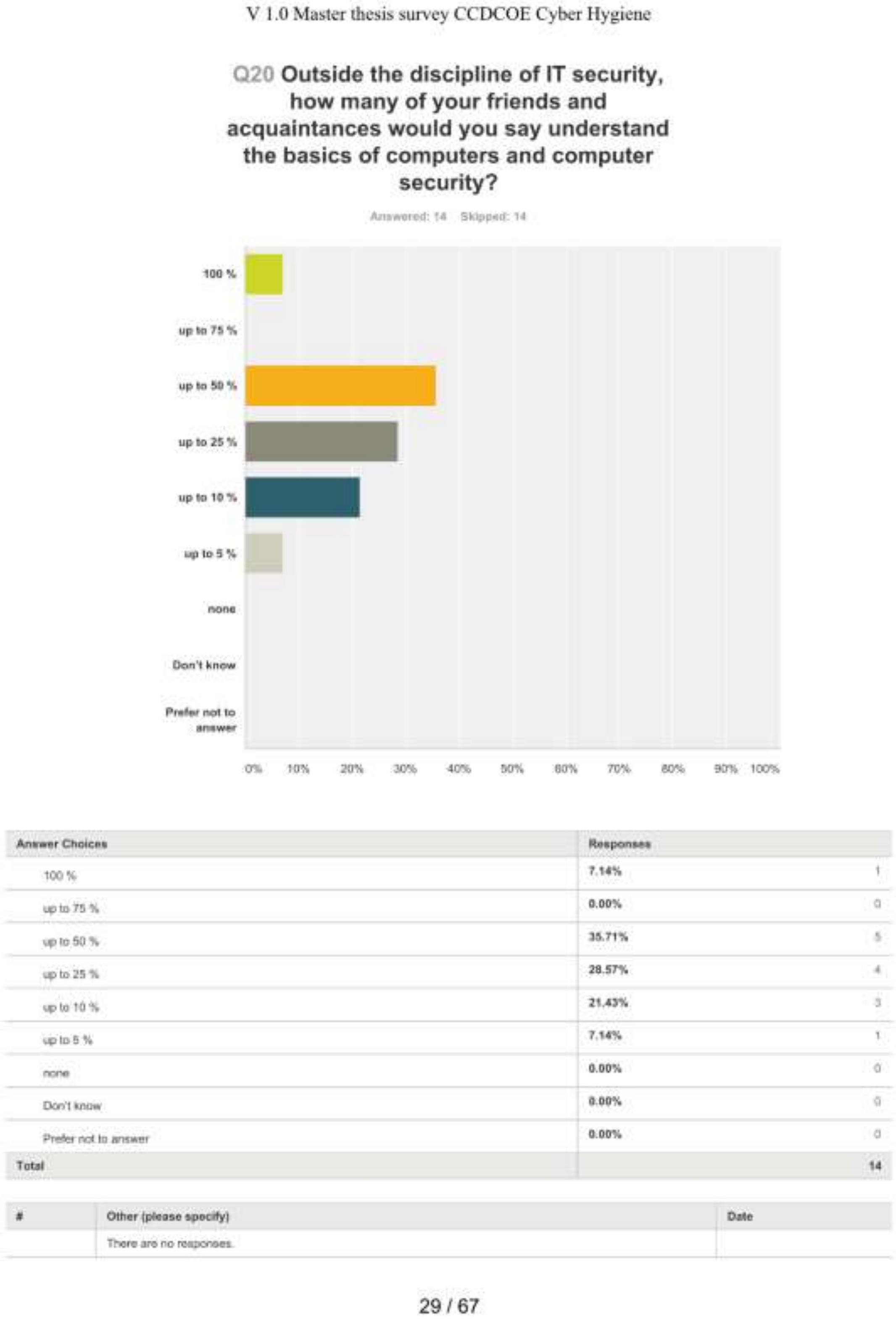
Q19 Do you think that your country will succeed in protecting its critical information infrastructure?

Answered: 14 Skipped: 14

Answer Choices	Responses	
Strongly agree	14.29%	2
Somewhat agree	42.86%	6
Somewhat disagree	14.29%	2
Strongly disagree	7.14%	1
Don't know	21.43%	3
Prefer not to answer	0.00%	0
Total		14

#	Other (please specify)	Date
1	There is no clear answear. It depends on the character/vector of attack.	8/15/2016 9:25 AM

28 / 67



V 1.0 Master thesis survey CCDCOE Cyber Hygiene

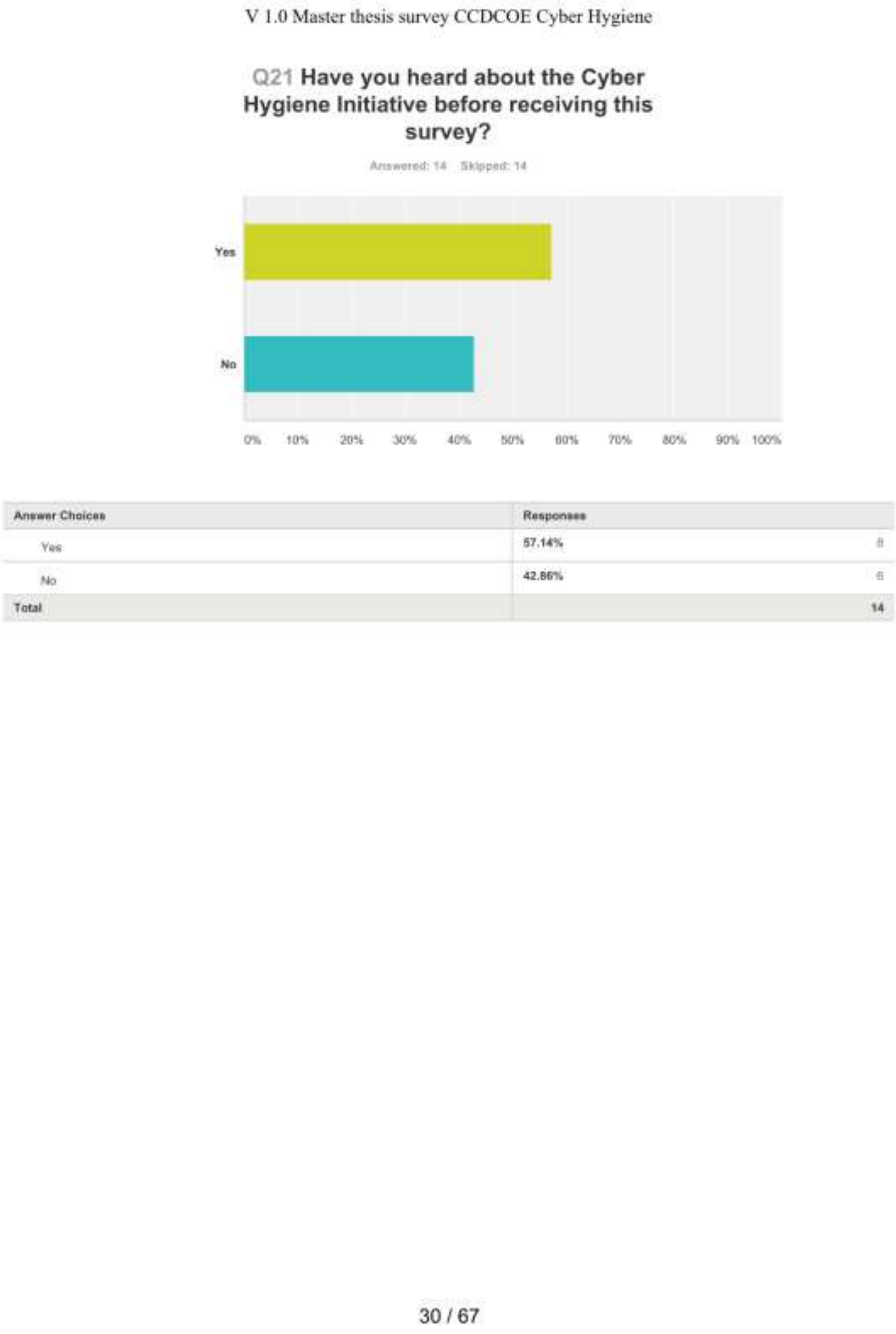
Q20 Outside the discipline of IT security, how many of your friends and acquaintances would you say understand the basics of computers and computer security?

Answered: 14 Skipped: 14

Answer Choices	Responses	
100 %	7.14%	1
up to 75 %	0.00%	0
up to 50 %	35.71%	5
up to 25 %	28.57%	4
up to 10 %	21.43%	3
up to 5 %	7.14%	1
none	0.00%	0
Don't know	0.00%	0
Prefer not to answer	0.00%	0
Total		14

#	Other (please specify)	Date
	There are no responses.	

29 / 67



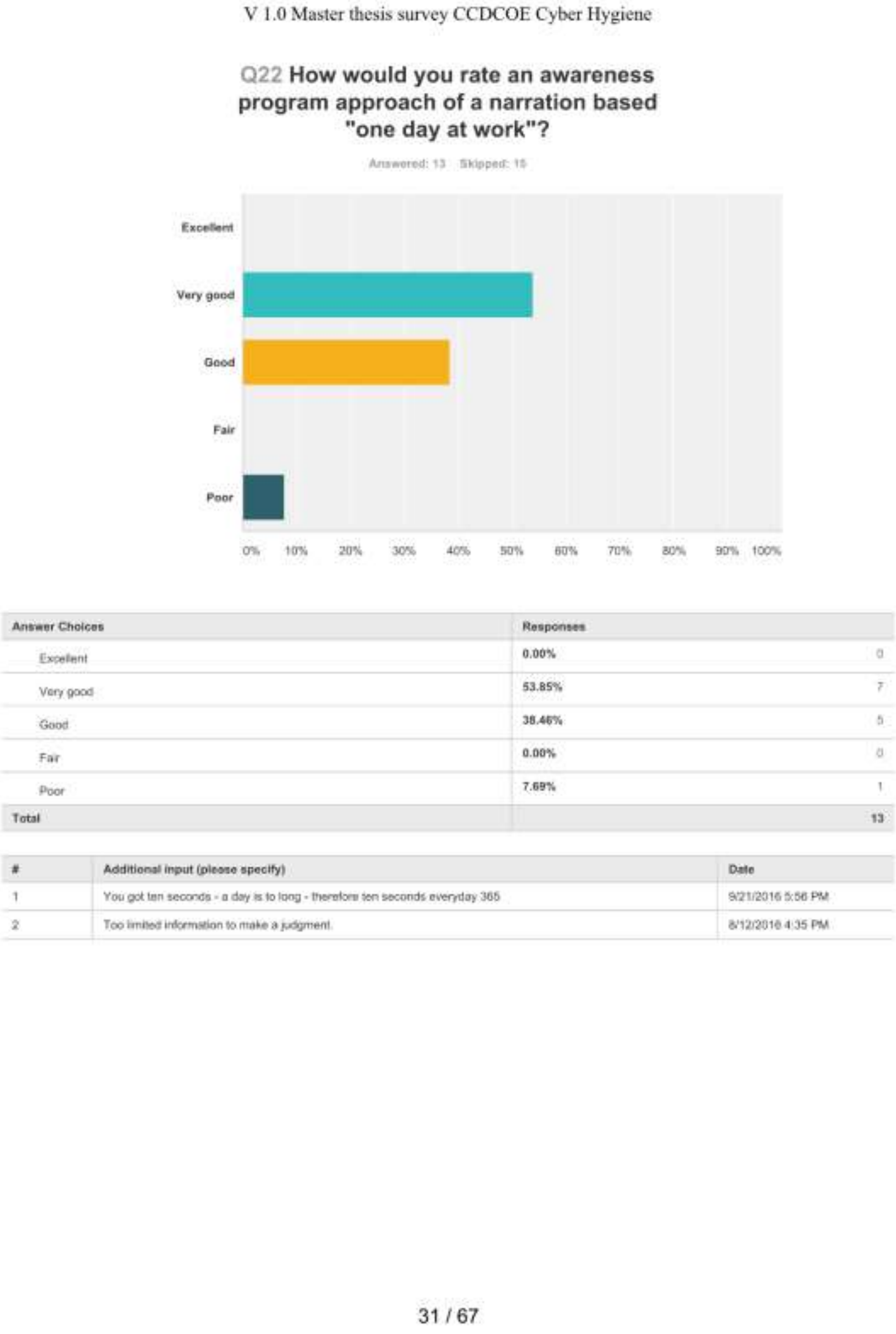
V 1.0 Master thesis survey CCDCOE Cyber Hygiene

Q21 Have you heard about the Cyber Hygiene Initiative before receiving this survey?

Answered: 14 Skipped: 14

Answer Choices	Responses	
Yes	57.14%	8
No	42.86%	6
Total		14

30 / 67



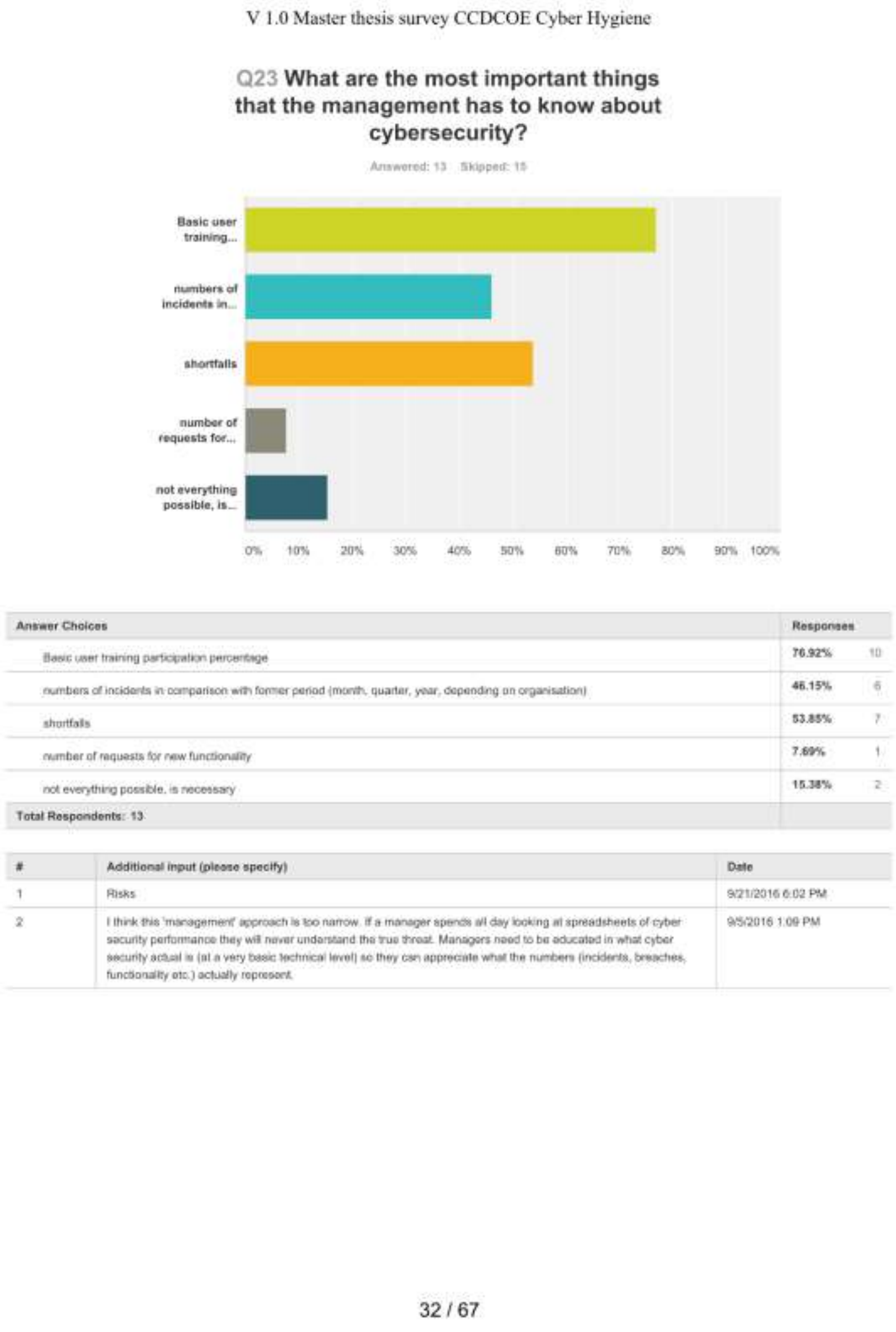
V 1.0 Master thesis survey CCDCOE Cyber Hygiene

Q22 How would you rate an awareness program approach of a narration based "one day at work"?

Answered: 13 Skipped: 15

Answer Choices	Responses	
Excellent	0.00%	0
Very good	53.85%	7
Good	38.46%	5
Fair	0.00%	0
Poor	7.69%	1
Total		13

#	Additional input (please specify)	Date
1	You got ten seconds - a day is to long - therefore ten seconds everyday 365	9/21/2016 5:56 PM
2	Too limited information to make a judgment.	8/12/2016 4:35 PM



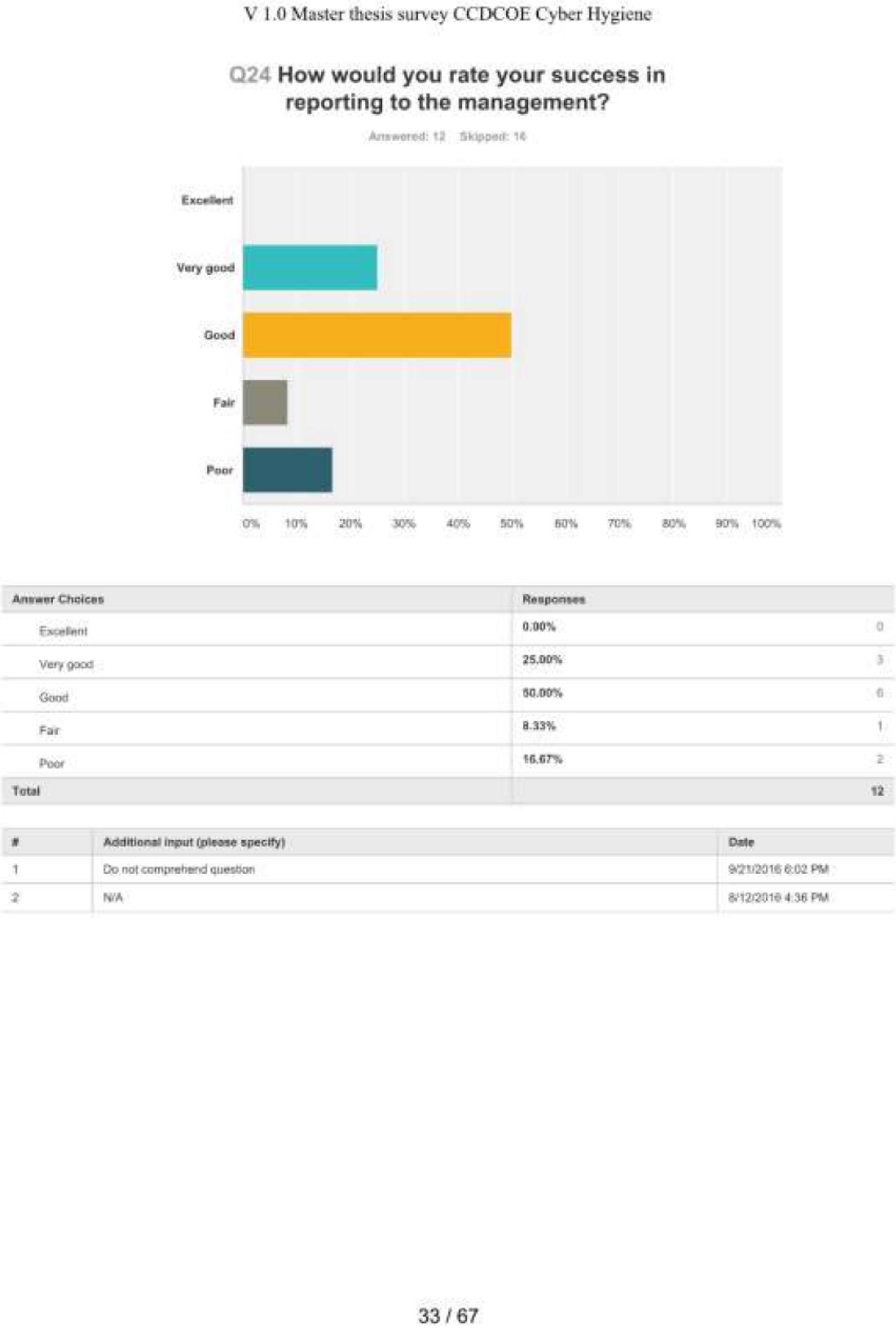
Q23 What are the most important things that the management has to know about cybersecurity?

Answered: 13 Skipped: 15

Basic user training...
numbers of incidents in...
shortfalls
number of requests for...
not everything possible, is...
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%

Answer Choices	Responses	
Basic user training participation percentage	**76.92%**	10
numbers of incidents in comparison with former period (month, quarter, year, depending on organisation)	**46.15%**	6
shortfalls	**53.85%**	7
number of requests for new functionality	**7.69%**	1
not everything possible, is necessary	**15.38%**	2
Total Respondents: 13		

#	Additional input (please specify)	Date
1	Risks	9/21/2016 6:02 PM
2	I think this 'management' approach is too narrow. If a manager spends all day looking at spreadsheets of cyber security performance they will never understand the true threat. Managers need to be educated in what cyber security actual is (at a very basic technical level) so they can appreciate what the numbers (incidents, breaches, functionality etc.) actually represent.	9/5/2016 1:09 PM



V 1.0 Master thesis survey CCDCOE Cyber Hygiene

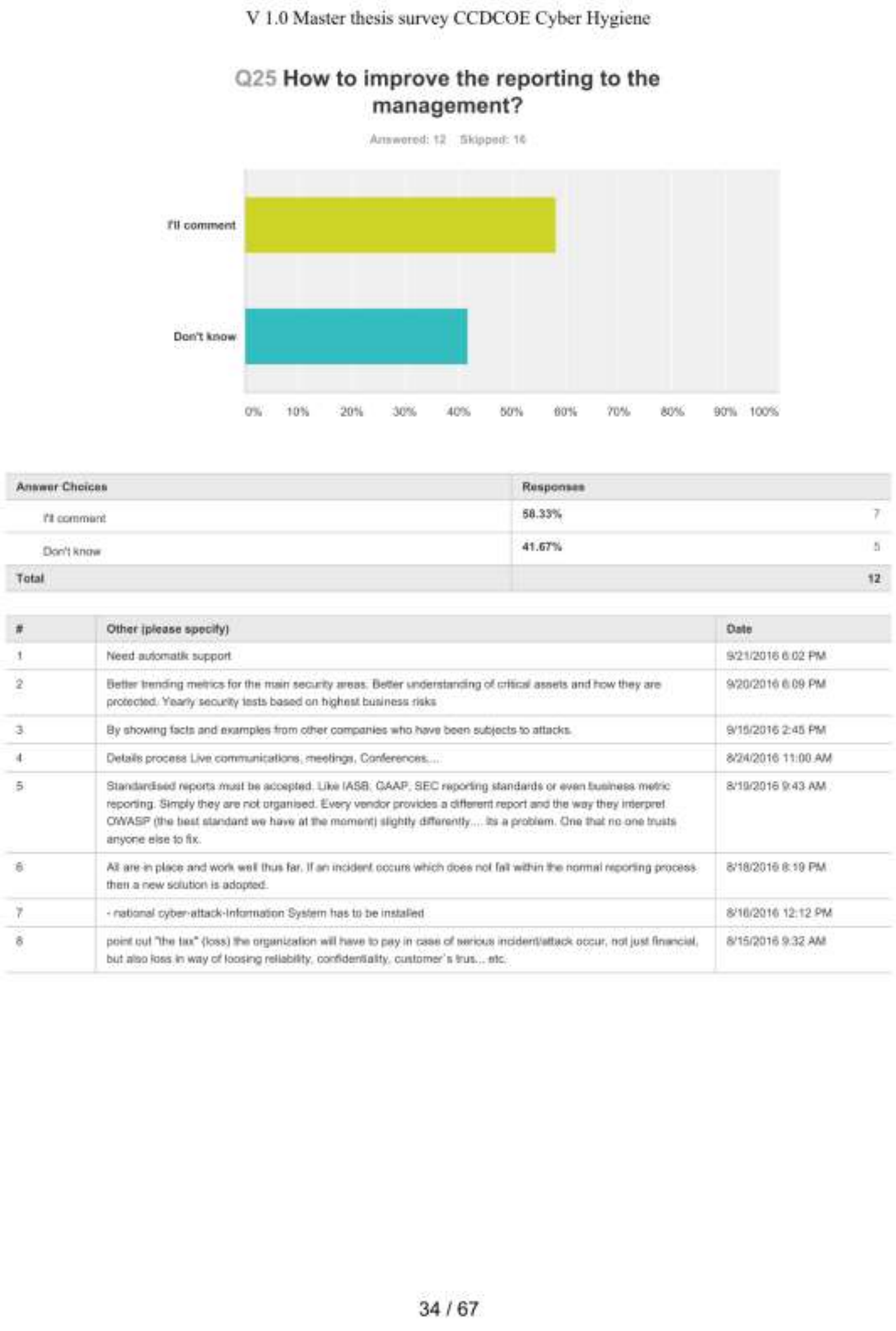
Q24 How would you rate your success in reporting to the management?

Answered: 12 Skipped: 16

Answer Choices	Responses	
Excellent	0.00%	0
Very good	25.00%	3
Good	50.00%	6
Fair	8.33%	1
Poor	16.67%	2
Total		12

#	Additional input (please specify)	Date
1	Do not comprehend question	9/21/2016 6:02 PM
2	N/A	8/12/2016 4:36 PM

33 / 67



V 1.0 Master thesis survey CCDCOE Cyber Hygiene

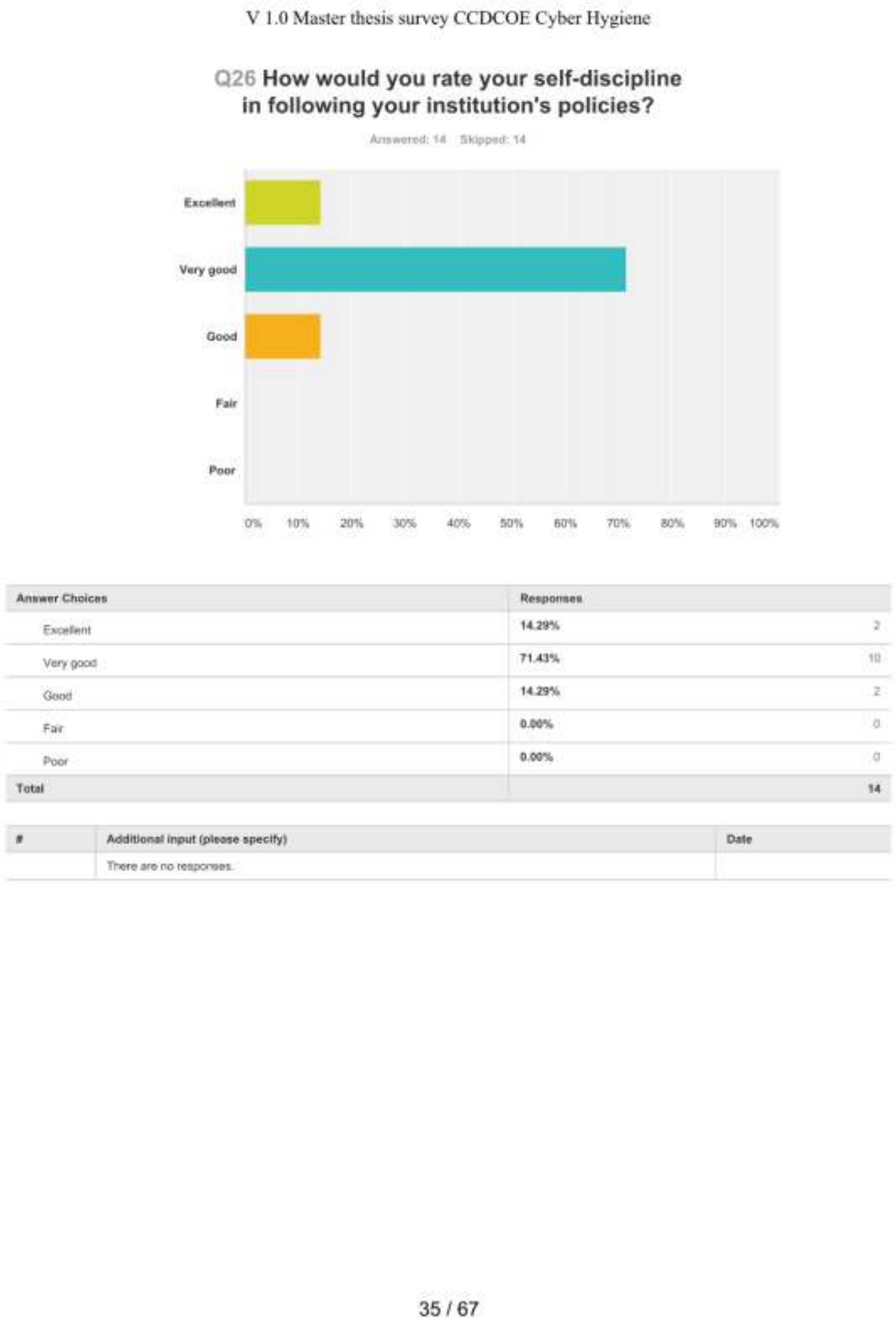
Q25 How to improve the reporting to the management?

Answered: 12 Skipped: 16

Answer Choices	Responses	
I'll comment	58.33%	7
Don't know	41.67%	5
Total		12

#	Other (please specify)	Date
1	Need automatik support	9/21/2016 6:02 PM
2	Better trending metrics for the main security areas. Better understanding of critical assets and how they are protected. Yearly security tests based on highest business risks	9/20/2016 6:09 PM
3	By showing facts and examples from other companies who have been subjects to attacks.	9/15/2016 2:45 PM
4	Details process Live communications, meetings, Conferences....	8/24/2016 11:00 AM
5	Standardised reports must be accepted. Like IASB, GAAP, SEC reporting standards or even business metric reporting. Simply they are not organised. Every vendor provides a different report and the way they interpret OWASP (the best standard we have at the moment) slightly differently.... Its a problem. One that no one trusts anyone else to fix.	8/19/2016 9:43 AM
6	All are in place and work well thus far. If an incident occurs which does not fall within the normal reporting process then a new solution is adopted.	8/18/2016 8:19 PM
7	- national cyber-attack-Information System has to be installed	8/16/2016 12:12 PM
8	point out "the tax" (loss) the organization will have to pay in case of serious incident/attack occur, not just financial, but also loss in way of loosing reliability, confidentiality, customer's trus... etc.	8/15/2016 9:32 AM

34 / 67



V 1.0 Master thesis survey CCDCOE Cyber Hygiene

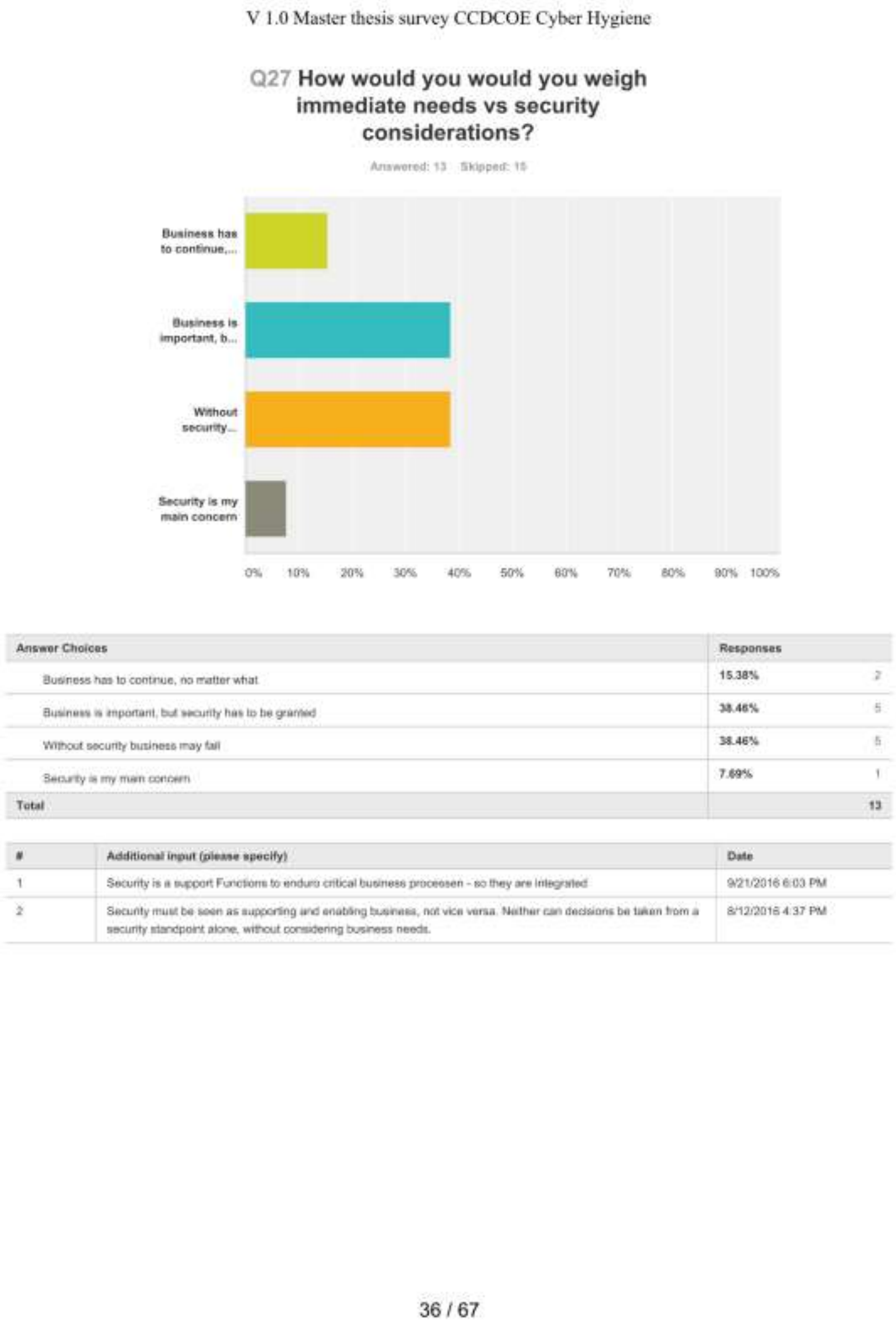
Q26 How would you rate your self-discipline in following your institution's policies?

Answered: 14 Skipped: 14

Answer Choices	Responses	
Excellent	14.29%	2
Very good	71.43%	10
Good	14.29%	2
Fair	0.00%	0
Poor	0.00%	0
Total		14

#	Additional input (please specify)	Date
	There are no responses.	

35 / 67



V 1.0 Master thesis survey CCDCOE Cyber Hygiene

Q27 How would you would you weigh immediate needs vs security considerations?

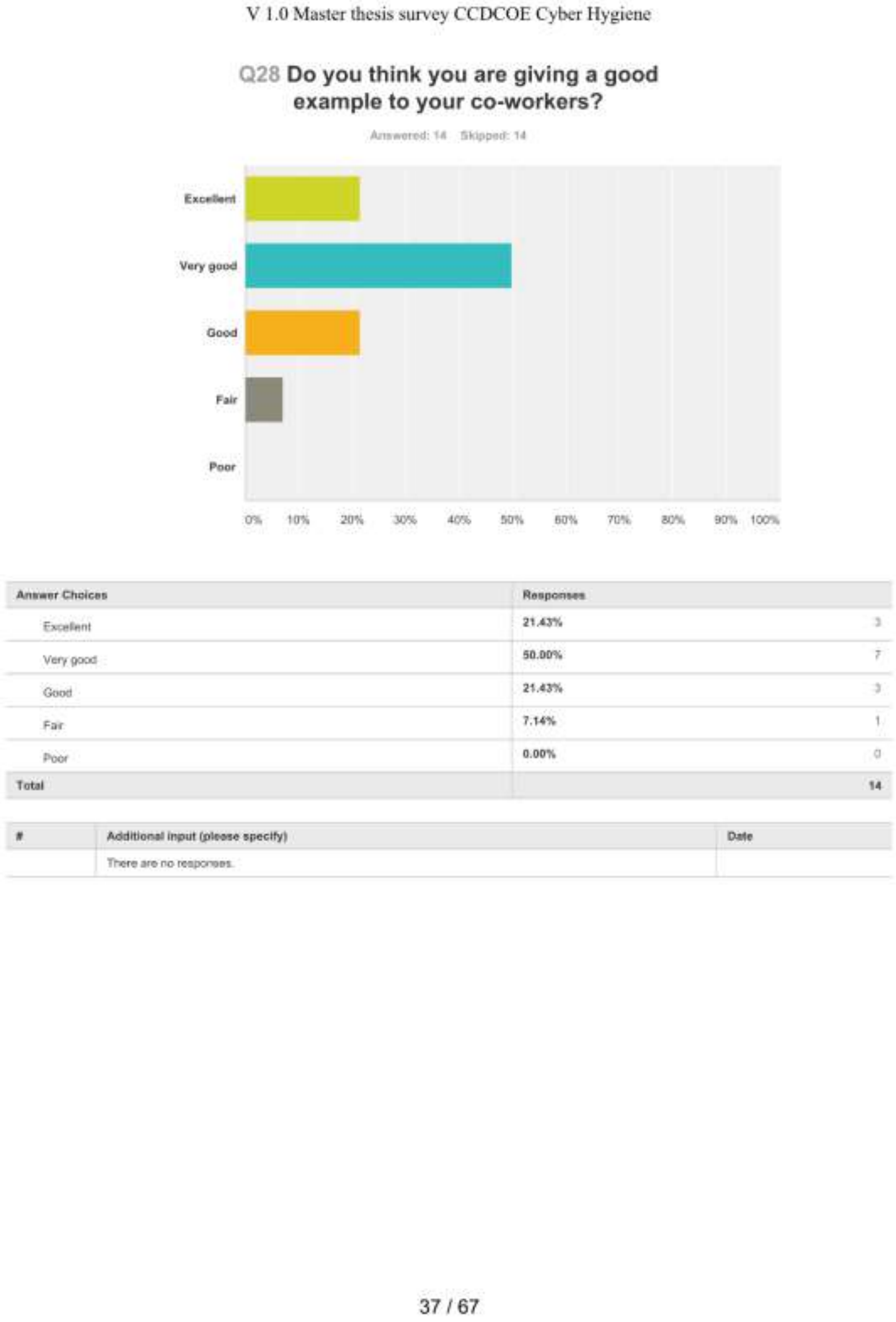
Answered: 13 Skipped: 15

Business has to continue,...
Business is important, b...
Without security...
Security is my main concern
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%

Answer Choices	Responses	
Business has to continue, no matter what	15.38%	2
Business is important, but security has to be granted	38.46%	5
Without security business may fail	38.46%	5
Security is my main concern	7.69%	1
Total		13

#	Additional input (please specify)	Date
1	Security is a support Functions to enduro critical business processen - so they are integrated	9/21/2016 6:03 PM
2	Security must be seen as supporting and enabling business, not vice versa. Neither can decisions be taken from a security standpoint alone, without considering business needs.	8/12/2016 4:37 PM

36 / 67



V 1.0 Master thesis survey CCDCOE Cyber Hygiene

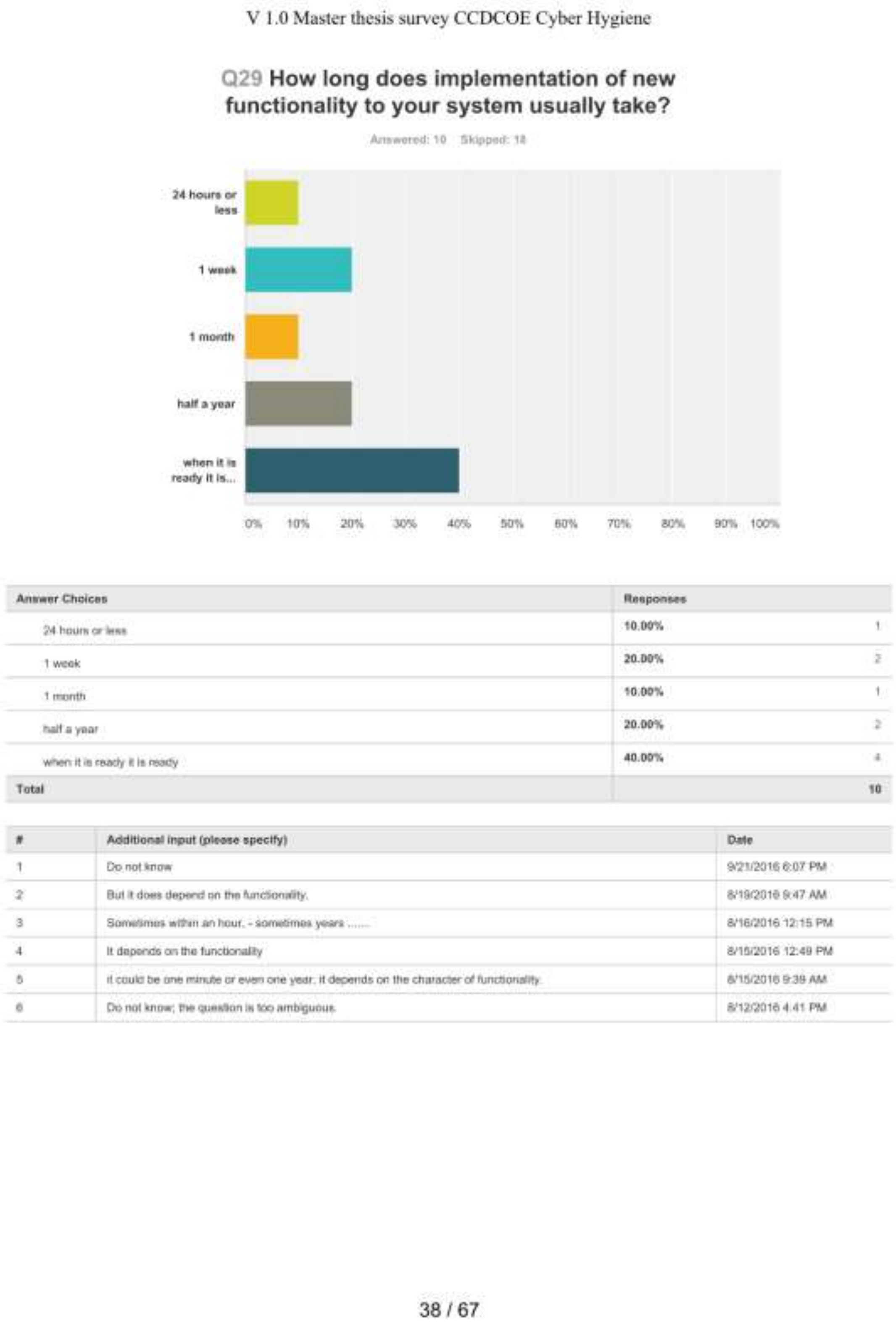
Q28 Do you think you are giving a good example to your co-workers?

Answered: 14 Skipped: 14

Answer Choices	Responses	
Excellent	21.43%	3
Very good	50.00%	7
Good	21.43%	3
Fair	7.14%	1
Poor	0.00%	0
Total		14

#	Additional input (please specify)	Date
	There are no responses.	

37 / 67

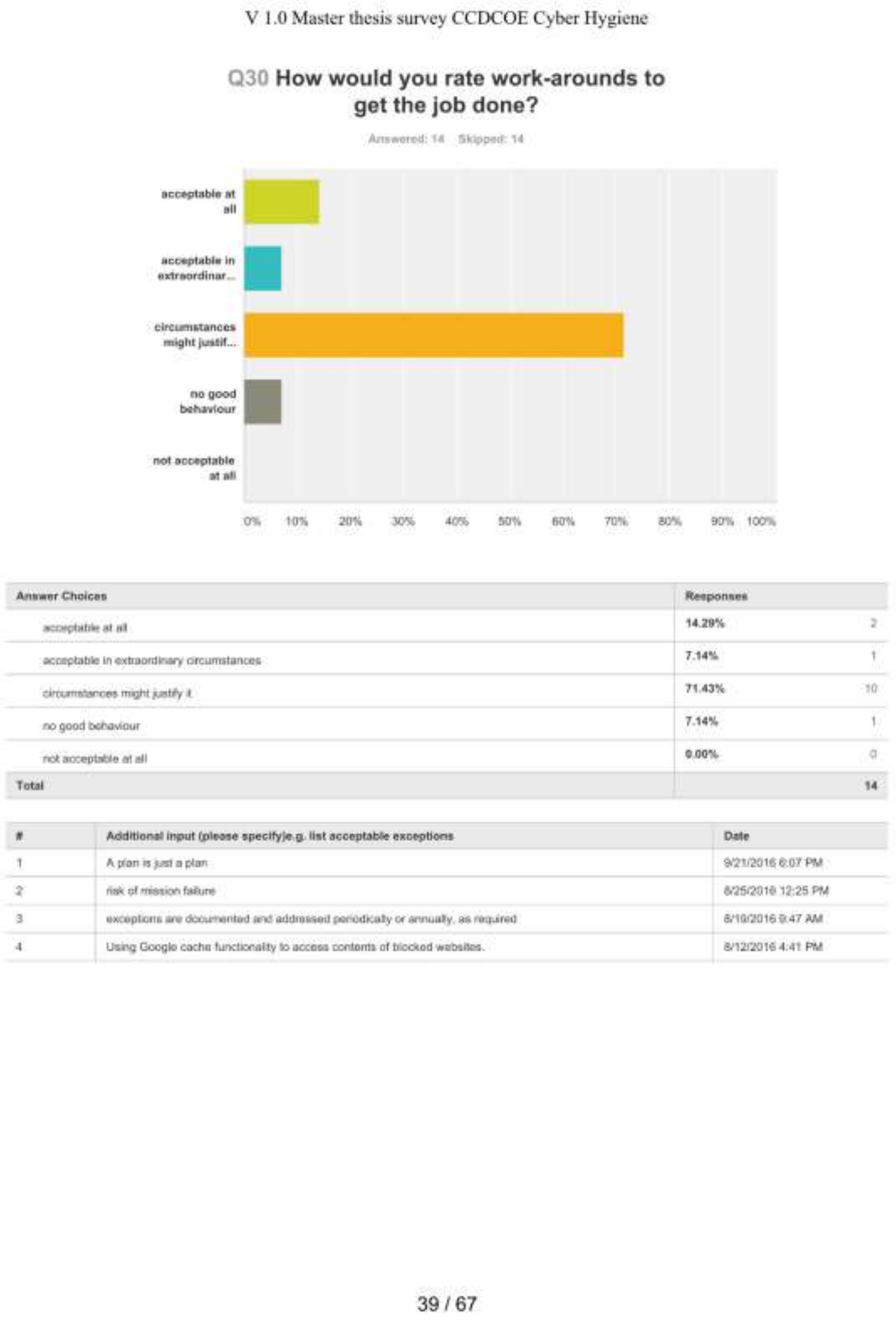


Q29 How long does implementation of new functionality to your system usually take?

Answered: 10 Skipped: 18

Answer Choices	Responses	
24 hours or less	10.00%	1
1 week	20.00%	2
1 month	10.00%	1
half a year	20.00%	2
when it is ready it is ready	40.00%	4
Total		10

#	Additional input (please specify)	Date
1	Do not know	9/21/2016 6:07 PM
2	But it does depend on the functionality.	8/19/2016 9:47 AM
3	Sometimes within an hour, - sometimes years	8/16/2016 12:15 PM
4	It depends on the functionality	8/15/2016 12:49 PM
5	it could be one minute or even one year, it depends on the character of functionality.	8/15/2016 9:39 AM
6	Do not know; the question is too ambiguous.	8/12/2016 4:41 PM



V 1.0 Master thesis survey CCDCOE Cyber Hygiene

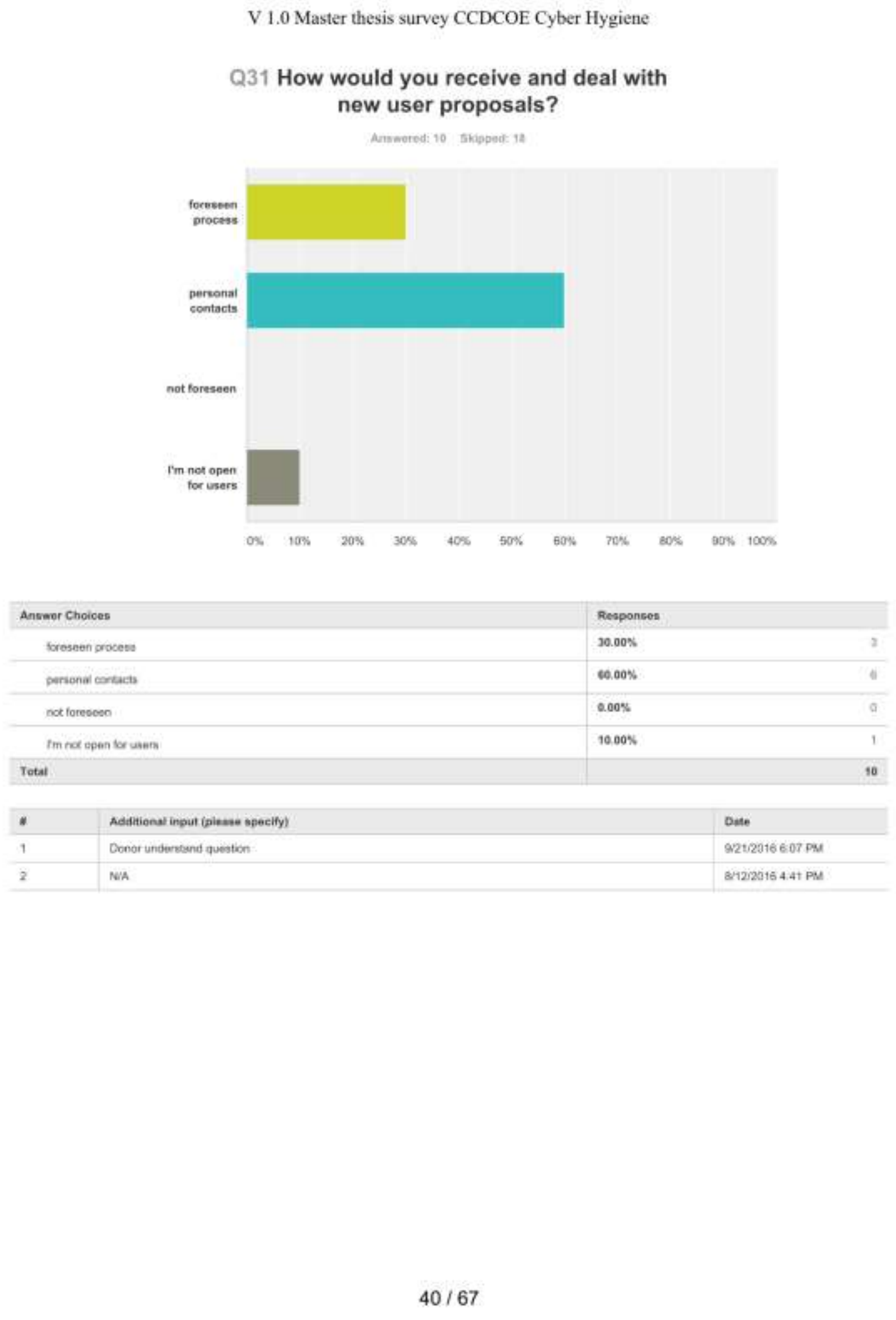
Q30 **How would you rate work-arounds to get the job done?**

Answered: 14 Skipped: 14

Answer Choices	Responses	
acceptable at all	14.29%	2
acceptable in extraordinary circumstances	7.14%	1
circumstances might justify it	71.43%	10
no good behaviour	7.14%	1
not acceptable at all	0.00%	0
Total		**14**

#	Additional input (please specify)e.g. list acceptable exceptions	Date
1	A plan is just a plan	9/21/2016 6:07 PM
2	risk of mission failure	8/25/2016 12:25 PM
3	exceptions are documented and addressed periodically or annually, as required	8/19/2016 9:47 AM
4	Using Google cache functionality to access contents of blocked websites.	8/12/2016 4:41 PM

39 / 67



V 1.0 Master thesis survey CCDCOE Cyber Hygiene

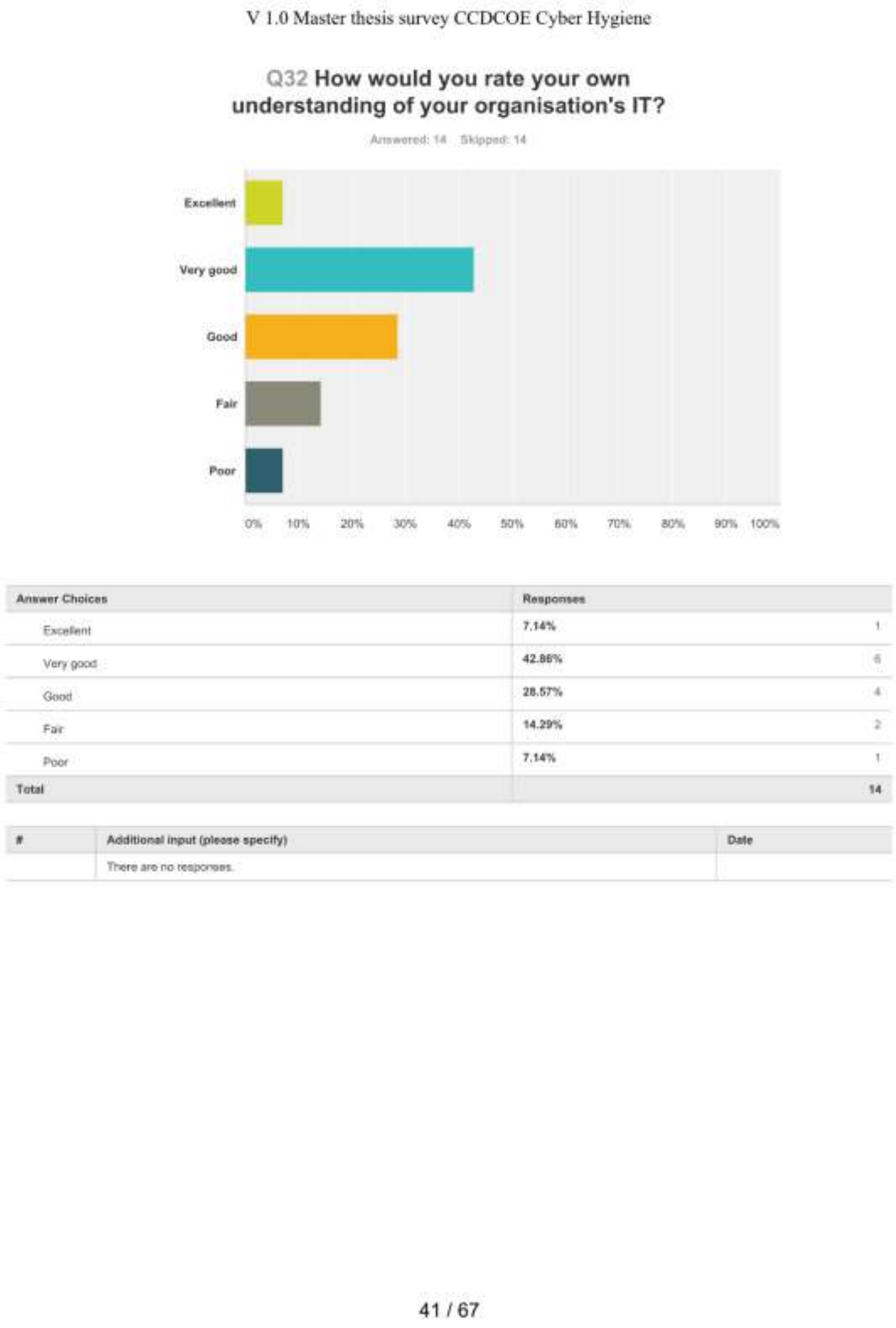
Q31 How would you receive and deal with new user proposals?

Answered: 10 Skipped: 18

Answer Choices	Responses	
foreseen process	30.00%	3
personal contacts	60.00%	6
not foreseen	0.00%	0
I'm not open for users	10.00%	1
Total		10

#	Additional input (please specify)	Date
1	Donor understand question	9/21/2016 6:07 PM
2	N/A	8/12/2016 4:41 PM

40 / 67



V 1.0 Master thesis survey CCDCOE Cyber Hygiene

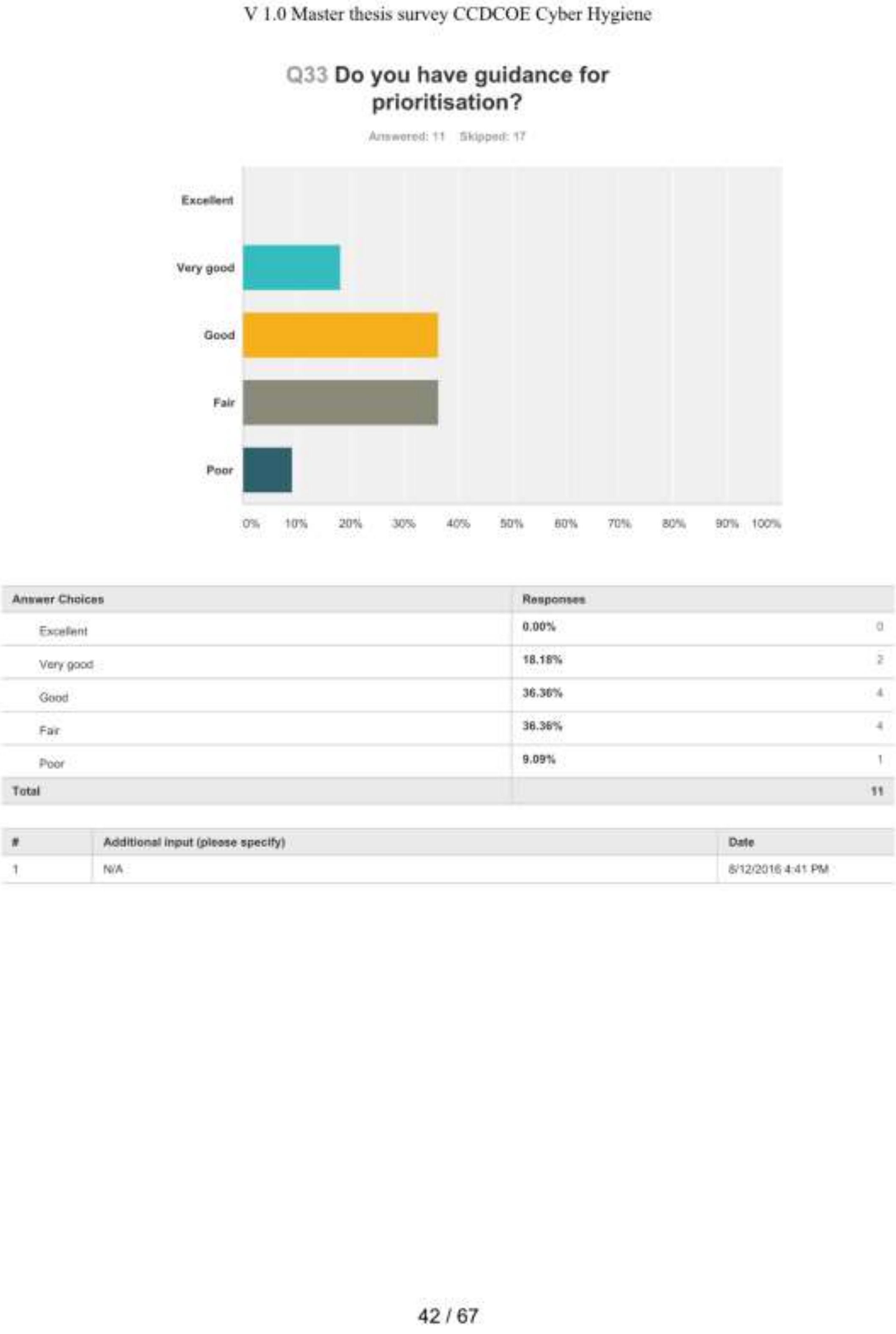
Q32 How would you rate your own understanding of your organisation's IT?

Answered: 14 Skipped: 14

Answer Choices	Responses	
Excellent	7.14%	1
Very good	42.86%	6
Good	28.57%	4
Fair	14.29%	2
Poor	7.14%	1
Total		14

#	Additional input (please specify)	Date
	There are no responses.	

41 / 67



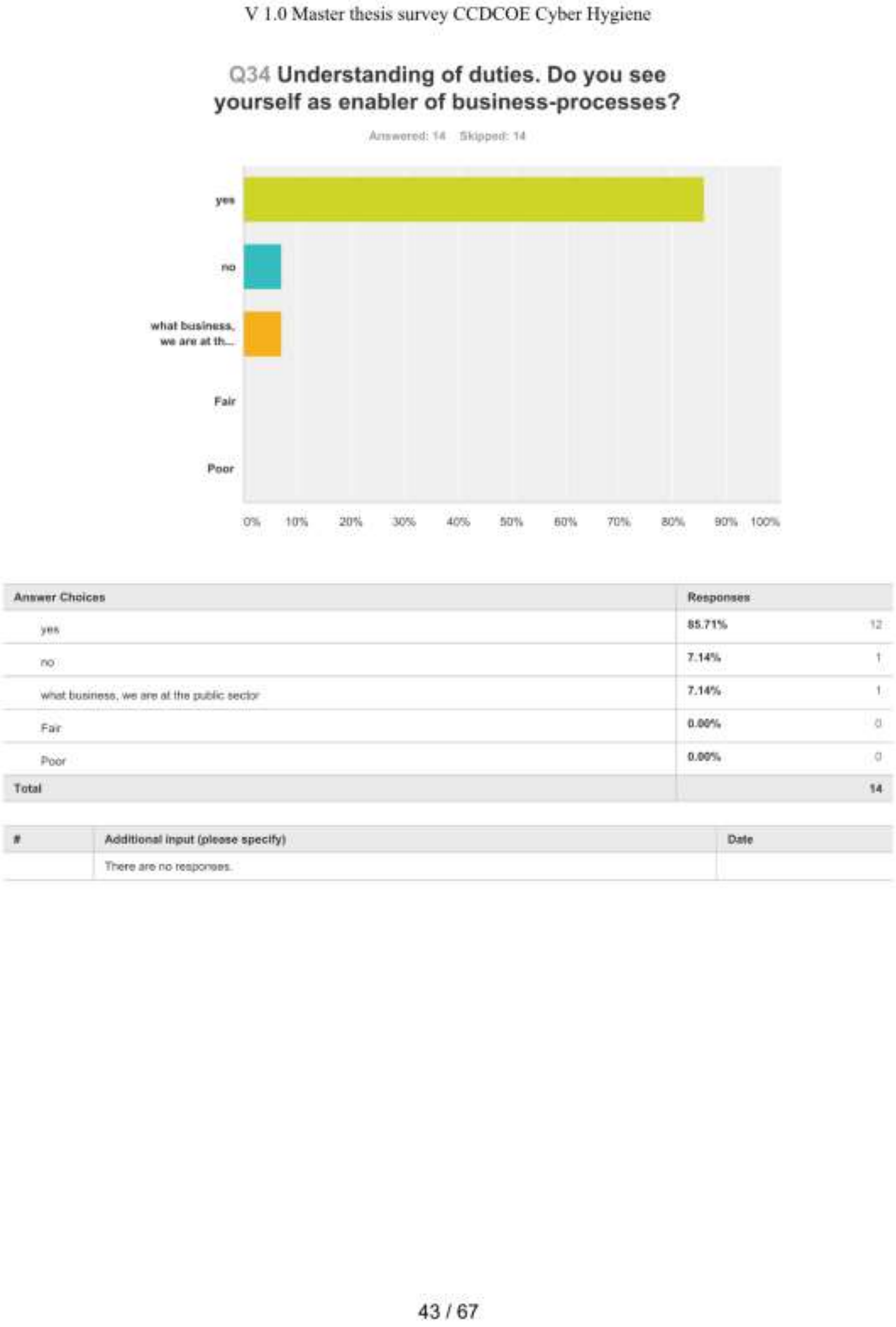
V 1.0 Master thesis survey CCDCOE Cyber Hygiene

Q33 Do you have guidance for prioritisation?

Answered: 11 Skipped: 17

Answer Choices	Responses	
Excellent	0.00%	0
Very good	18.18%	2
Good	36.36%	4
Fair	36.36%	4
Poor	9.09%	1
Total		11

#	Additional input (please specify)	Date
1	N/A	8/12/2016 4:41 PM



V 1.0 Master thesis survey CCDCOE Cyber Hygiene

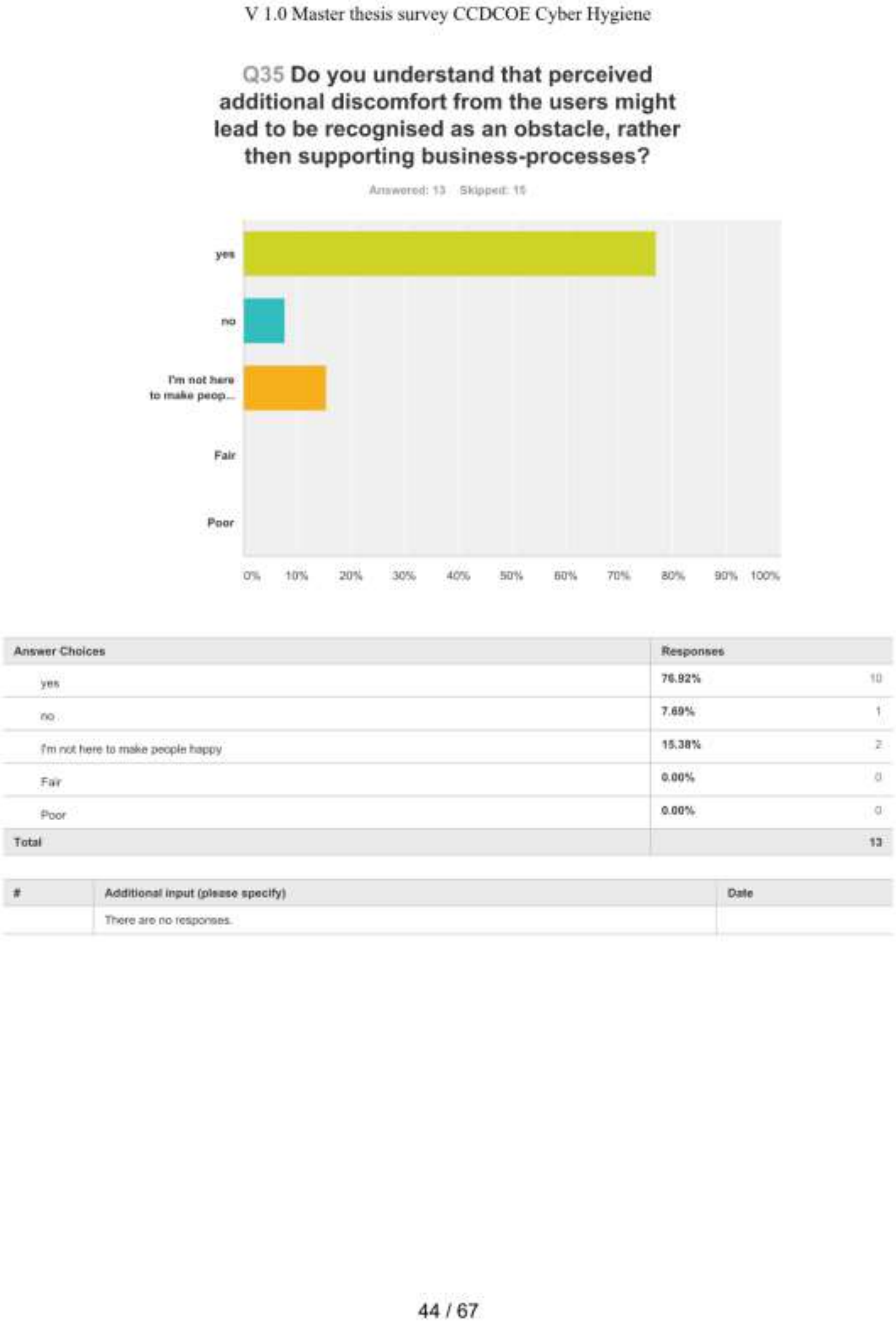
Q34 Understanding of duties. Do you see yourself as enabler of business-processes?

Answered: 14 Skipped: 14

Answer Choices	Responses	
yes	85.71%	12
no	7.14%	1
what business, we are at the public sector	7.14%	1
Fair	0.00%	0
Poor	0.00%	0
Total		14

#	Additional input (please specify)	Date
	There are no responses.	

43 / 67



V 1.0 Master thesis survey CCDCOE Cyber Hygiene

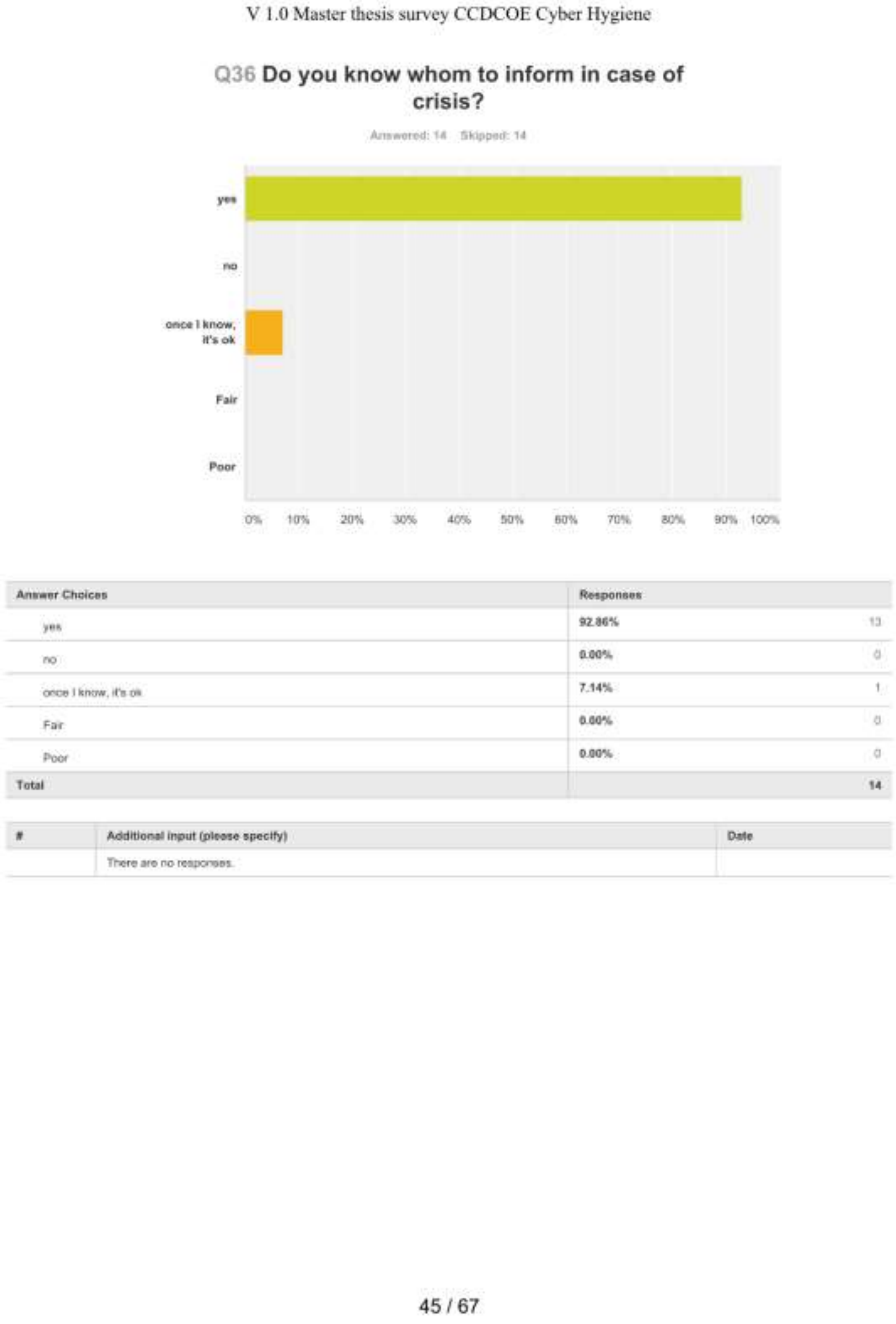
Q35 Do you understand that perceived additional discomfort from the users might lead to be recognised as an obstacle, rather then supporting business-processes?

Answered: 13 Skipped: 15

Answer Choices	Responses	
yes	76.92%	10
no	7.69%	1
I'm not here to make people happy	15.38%	2
Fair	0.00%	0
Poor	0.00%	0
Total		13

#	Additional input (please specify)	Date
	There are no responses.	

44 / 67



V 1.0 Master thesis survey CCDCOE Cyber Hygiene

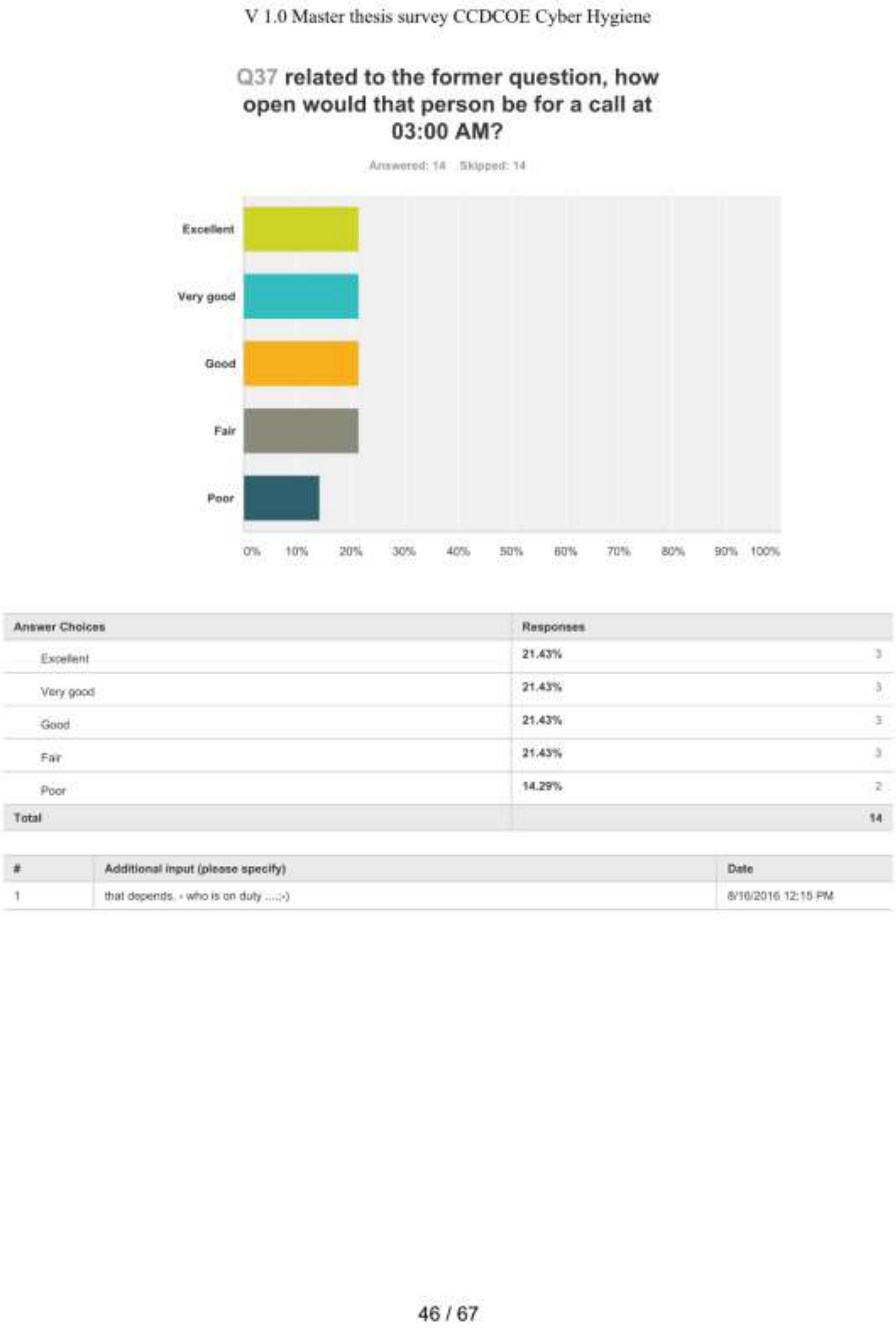
Q36 Do you know whom to inform in case of crisis?

Answered: 14 Skipped: 14

Answer Choices	Responses	
yes	92.86%	13
no	0.00%	0
once I know, it's ok	7.14%	1
Fair	0.00%	0
Poor	0.00%	0
Total		14

#	Additional input (please specify)	Date
	There are no responses.	

45 / 67

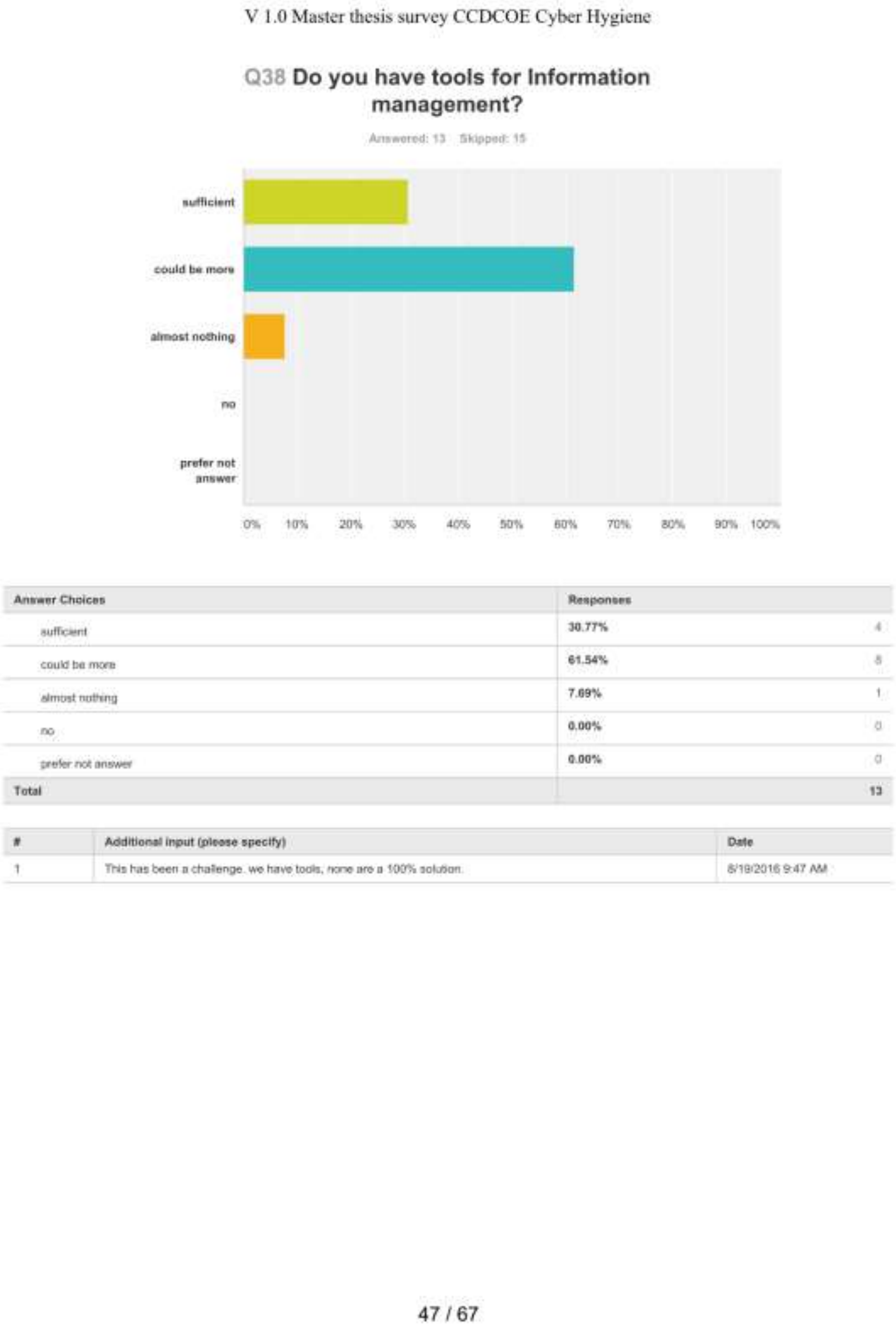


Q37 related to the former question, how open would that person be for a call at 03:00 AM?

Answered: 14 Skipped: 14

Answer Choices	Responses	
Excellent	21.43%	3
Very good	21.43%	3
Good	21.43%	3
Fair	21.43%	3
Poor	14.29%	2
Total		14

#	Additional input (please specify)	Date
1	that depends. - who is on duty ....;-)	8/16/2016 12:15 PM



V 1.0 Master thesis survey CCDCOE Cyber Hygiene

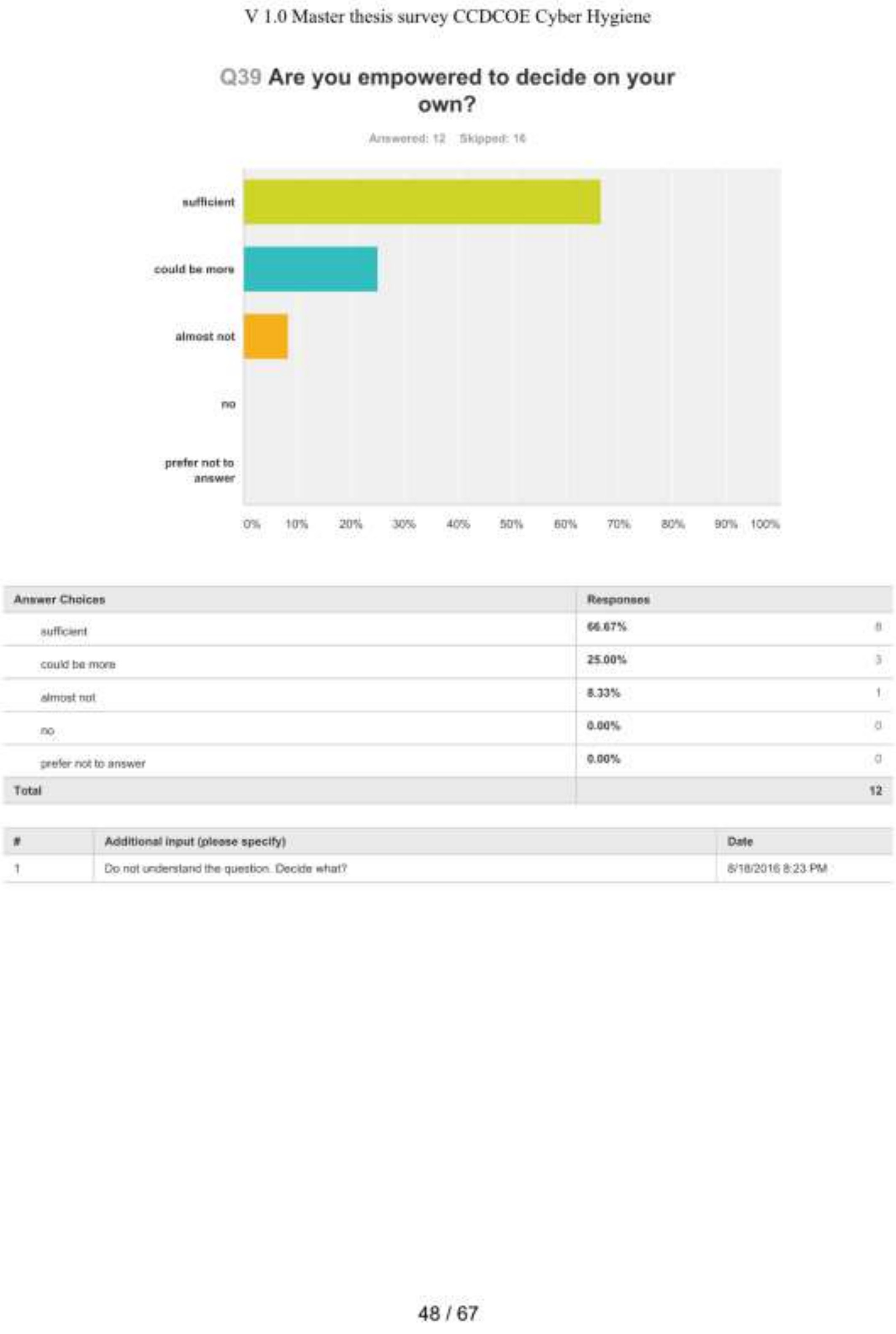
Q38 Do you have tools for Information management?

Answered: 13 Skipped: 15

Answer Choices	Responses	
sufficient	30.77%	4
could be more	61.54%	8
almost nothing	7.69%	1
no	0.00%	0
prefer not answer	0.00%	0
Total		13

#	Additional input (please specify)	Date
1	This has been a challenge. we have tools, none are a 100% solution.	8/19/2016 9:47 AM

47 / 67

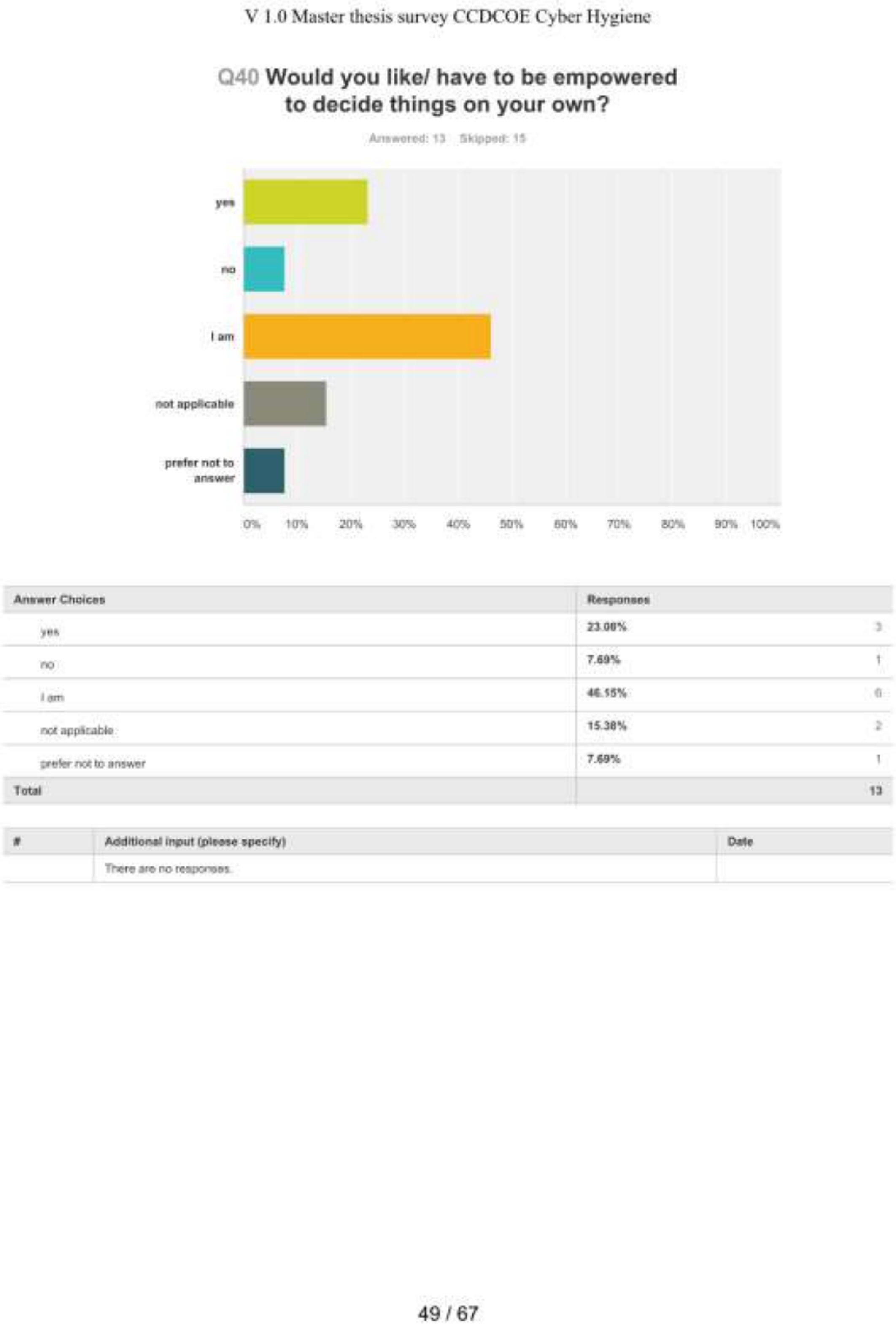


Q39 Are you empowered to decide on your own?

Answered: 12 Skipped: 16

Answer Choices	Responses	
sufficient	66.67%	8
could be more	25.00%	3
almost not	8.33%	1
no	0.00%	0
prefer not to answer	0.00%	0
Total		12

#	Additional input (please specify)	Date
1	Do not understand the question. Decide what?	8/18/2016 8:23 PM

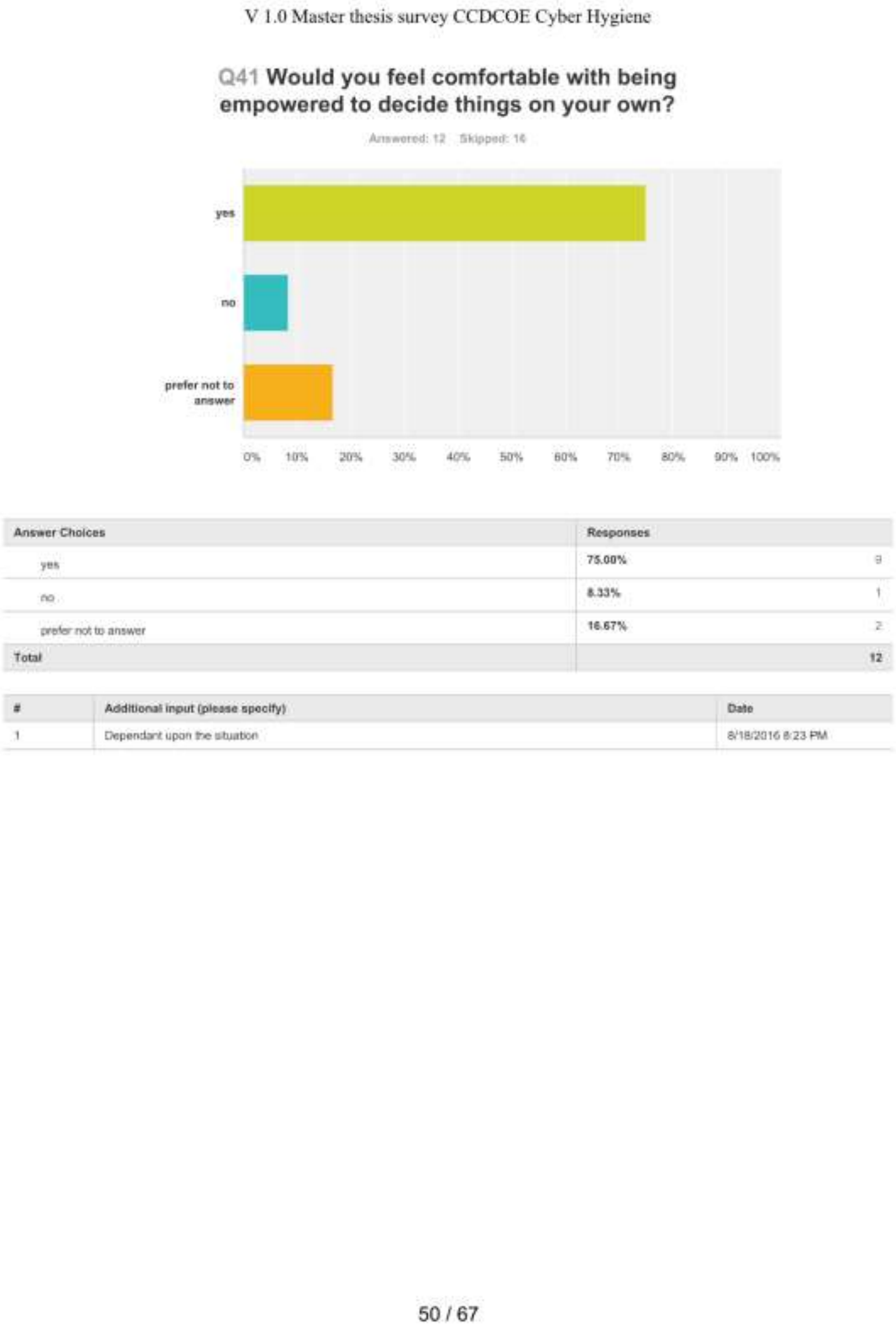


Q40 Would you like/ have to be empowered to decide things on your own?

Answered: 13 Skipped: 15

Answer Choices	Responses	
yes	23.08%	3
no	7.69%	1
I am	46.15%	6
not applicable	15.38%	2
prefer not to answer	7.69%	1
Total		13

#	Additional input (please specify)	Date
	There are no responses.	

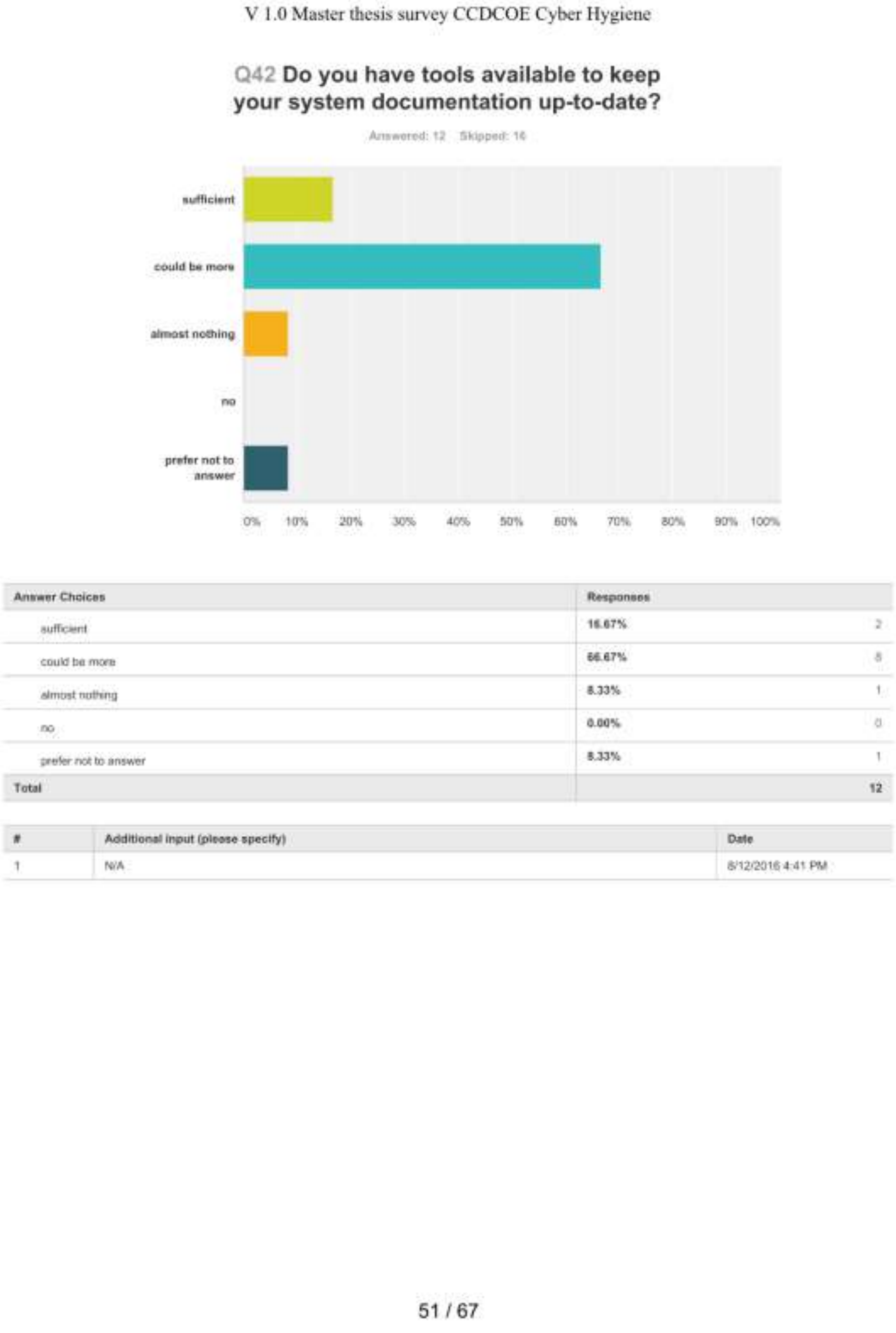


Q41 Would you feel comfortable with being empowered to decide things on your own?

Answered: 12 Skipped: 16

Answer Choices	Responses	
yes	75.00%	9
no	8.33%	1
prefer not to answer	16.67%	2
Total		12

#	Additional input (please specify)	Date
1	Dependant upon the situation	8/18/2016 8:23 PM



V 1.0 Master thesis survey CCDCOE Cyber Hygiene

Q42 Do you have tools available to keep your system documentation up-to-date?

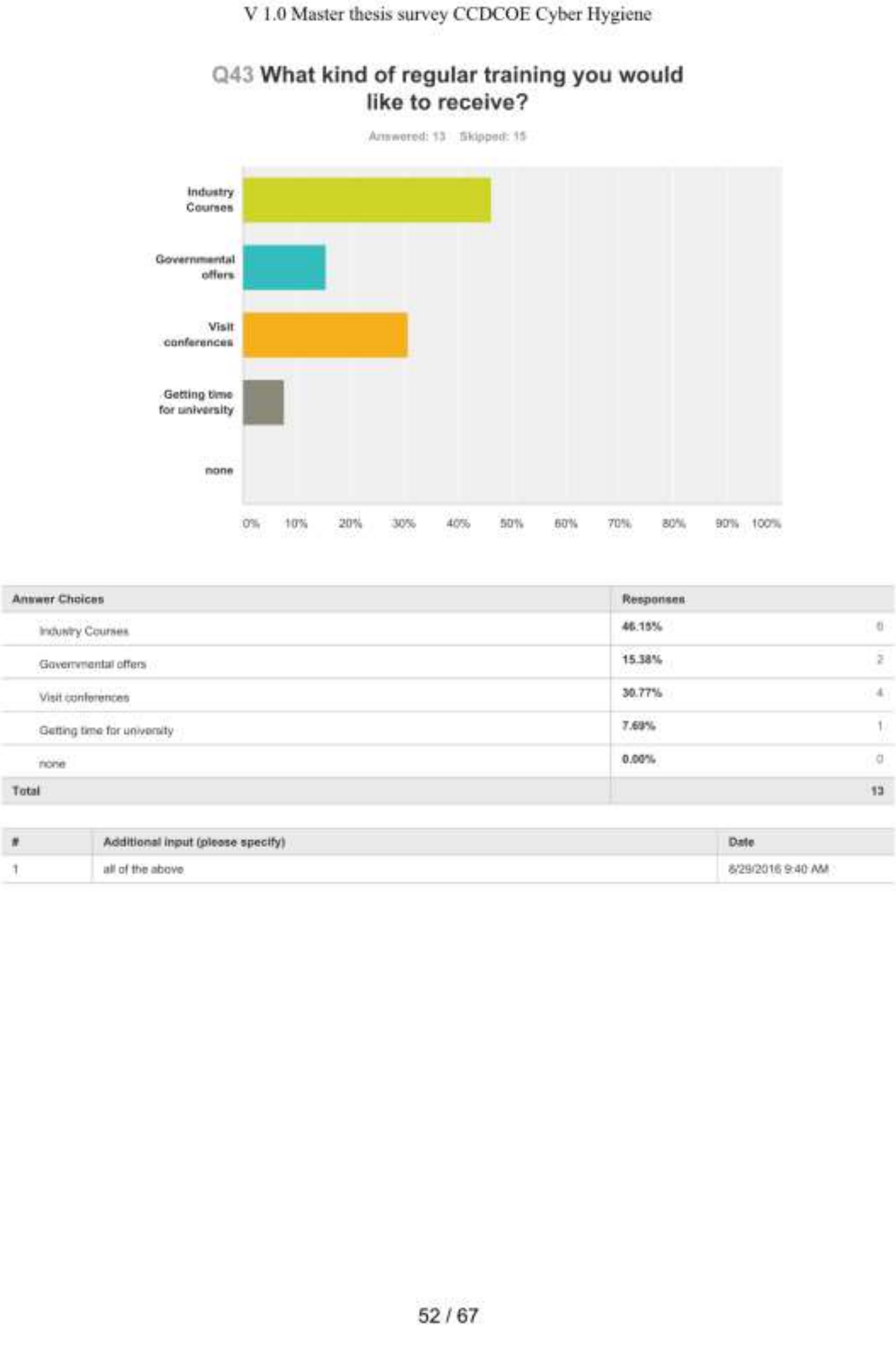
Answered: 12 Skipped: 16

Answer Choices	Responses	
sufficient	16.67%	2
could be more	66.67%	8
almost nothing	8.33%	1
no	0.00%	0
prefer not to answer	8.33%	1
Total		12

#	Additional input (please specify)	Date
1	N/A	8/12/2016 4:41 PM

51 / 67

V 1.0 Master thesis survey CCDCOE Cyber Hygiene



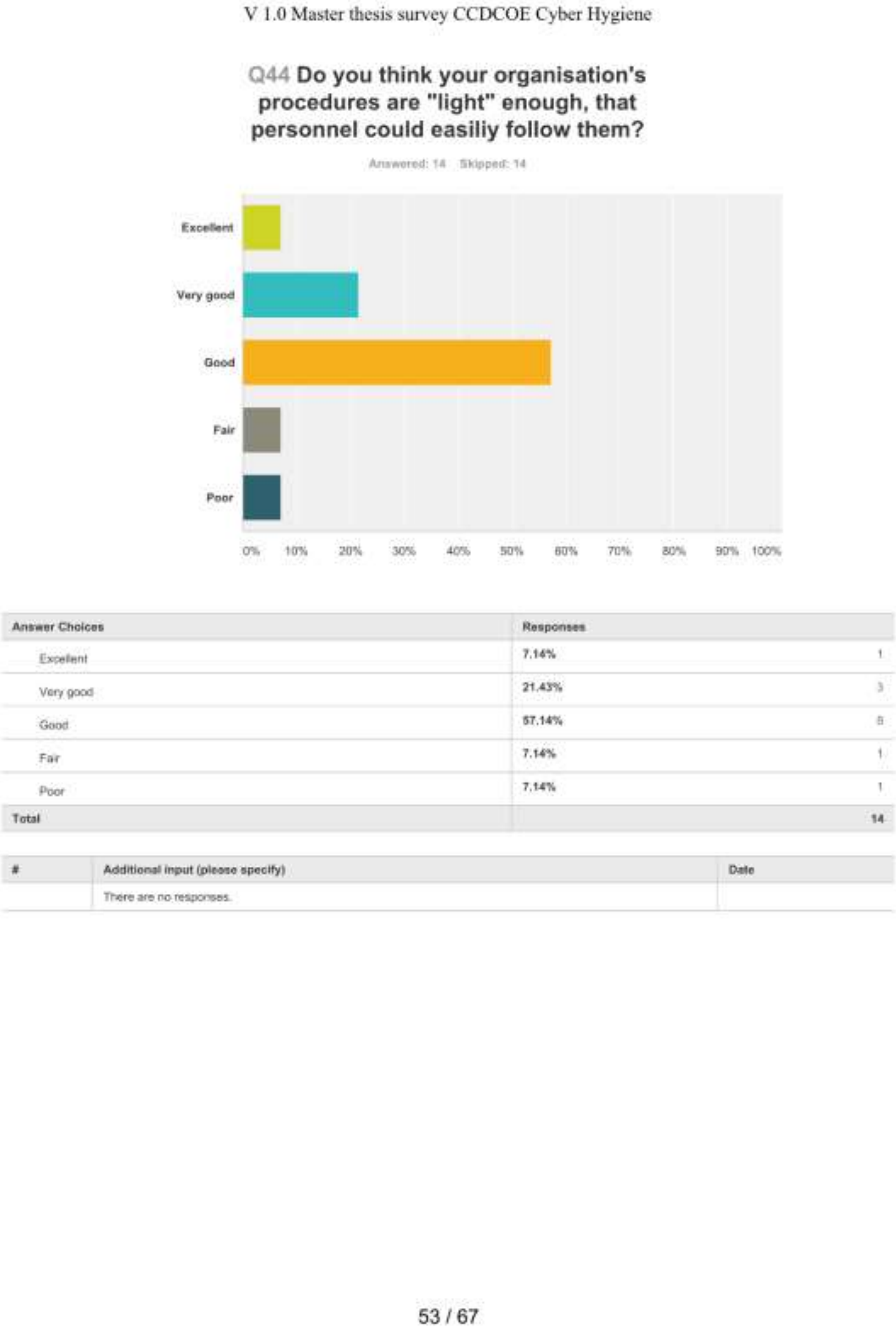
Q43 What kind of regular training you would like to receive?

Answered: 13 Skipped: 15

Answer Choices	Responses	
Industry Courses	46.15%	6
Governmental offers	15.38%	2
Visit conferences	30.77%	4
Getting time for university	7.69%	1
none	0.00%	0
Total		13

#	Additional input (please specify)	Date
1	all of the above	8/29/2016 9:40 AM

52 / 67



V 1.0 Master thesis survey CCDCOE Cyber Hygiene

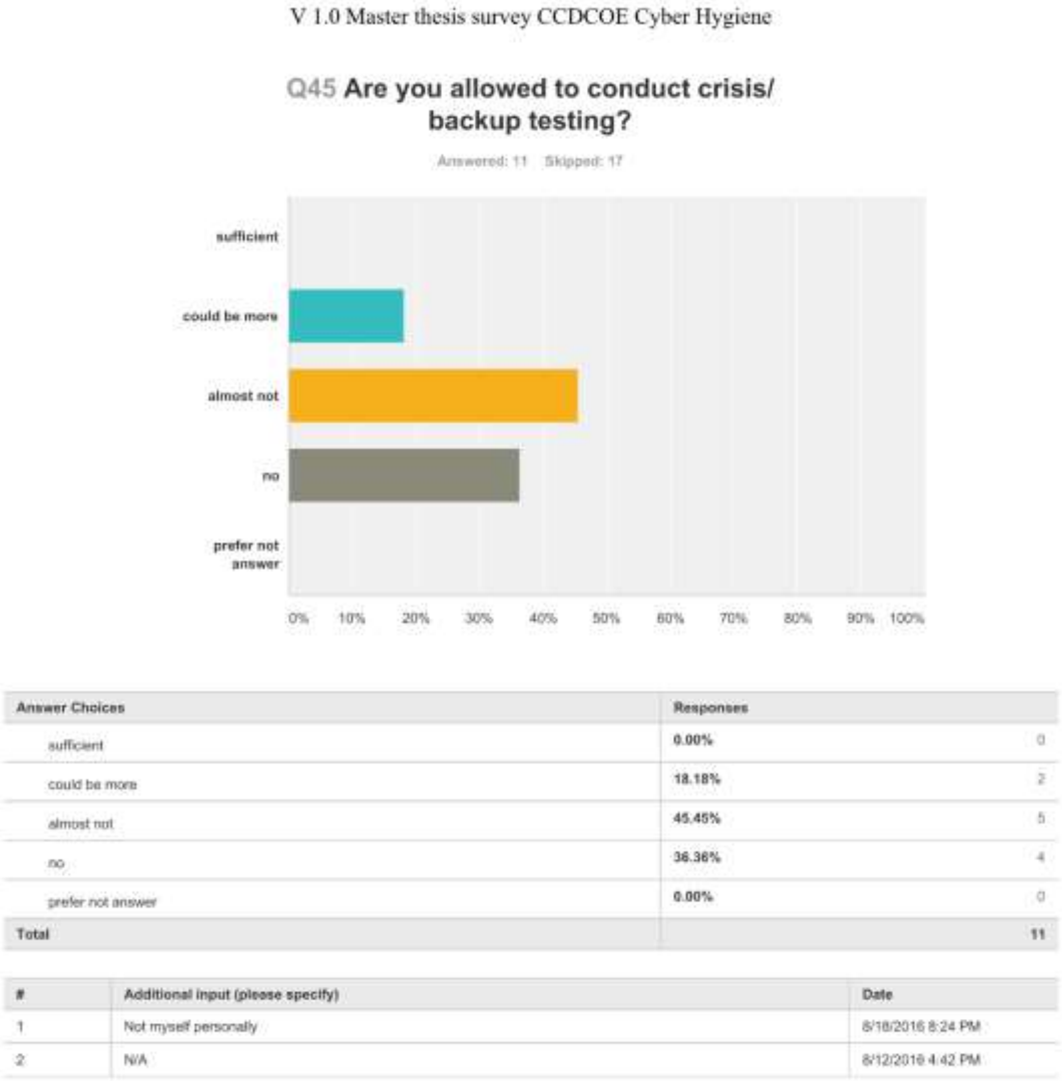
Q44 Do you think your organisation's procedures are "light" enough, that personnel could easiliy follow them?

Answered: 14 Skipped: 14

Answer Choices	Responses	
Excellent	7.14%	1
Very good	21.43%	3
Good	57.14%	8
Fair	7.14%	1
Poor	7.14%	1
Total		14

#	Additional input (please specify)	Date
	There are no responses.	

53 / 67



V 1.0 Master thesis survey CCDCOE Cyber Hygiene

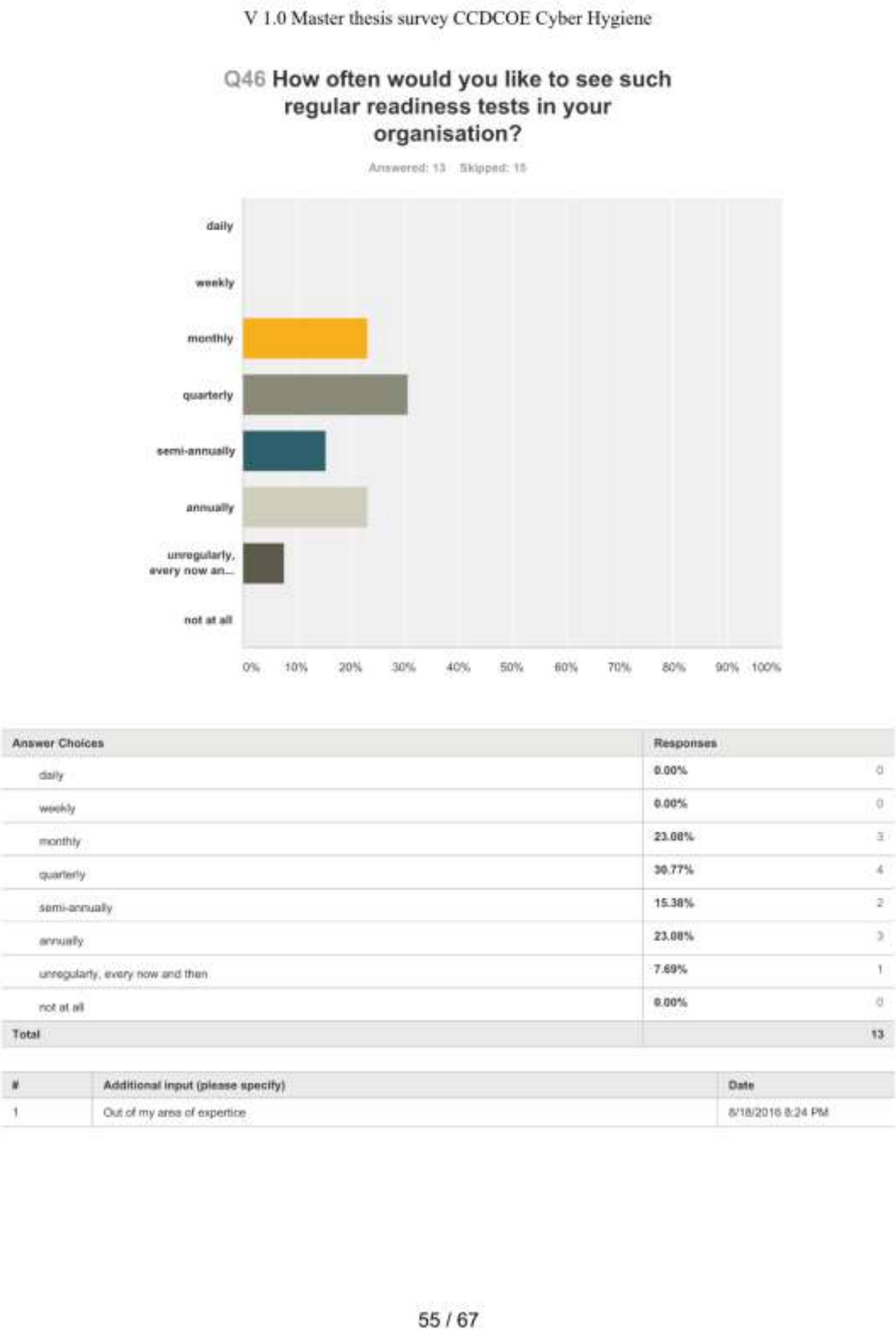
Q45 Are you allowed to conduct crisis/ backup testing?

Answered: 11 Skipped: 17

Answer Choices	Responses	
sufficient	0.00%	0
could be more	18.18%	2
almost not	45.45%	5
no	36.36%	4
prefer not answer	0.00%	0
Total		11

#	Additional input (please specify)	Date
1	Not myself personally	8/18/2016 8:24 PM
2	N/A	8/12/2016 4:42 PM

54 / 67



V 1.0 Master thesis survey CCDCOE Cyber Hygiene

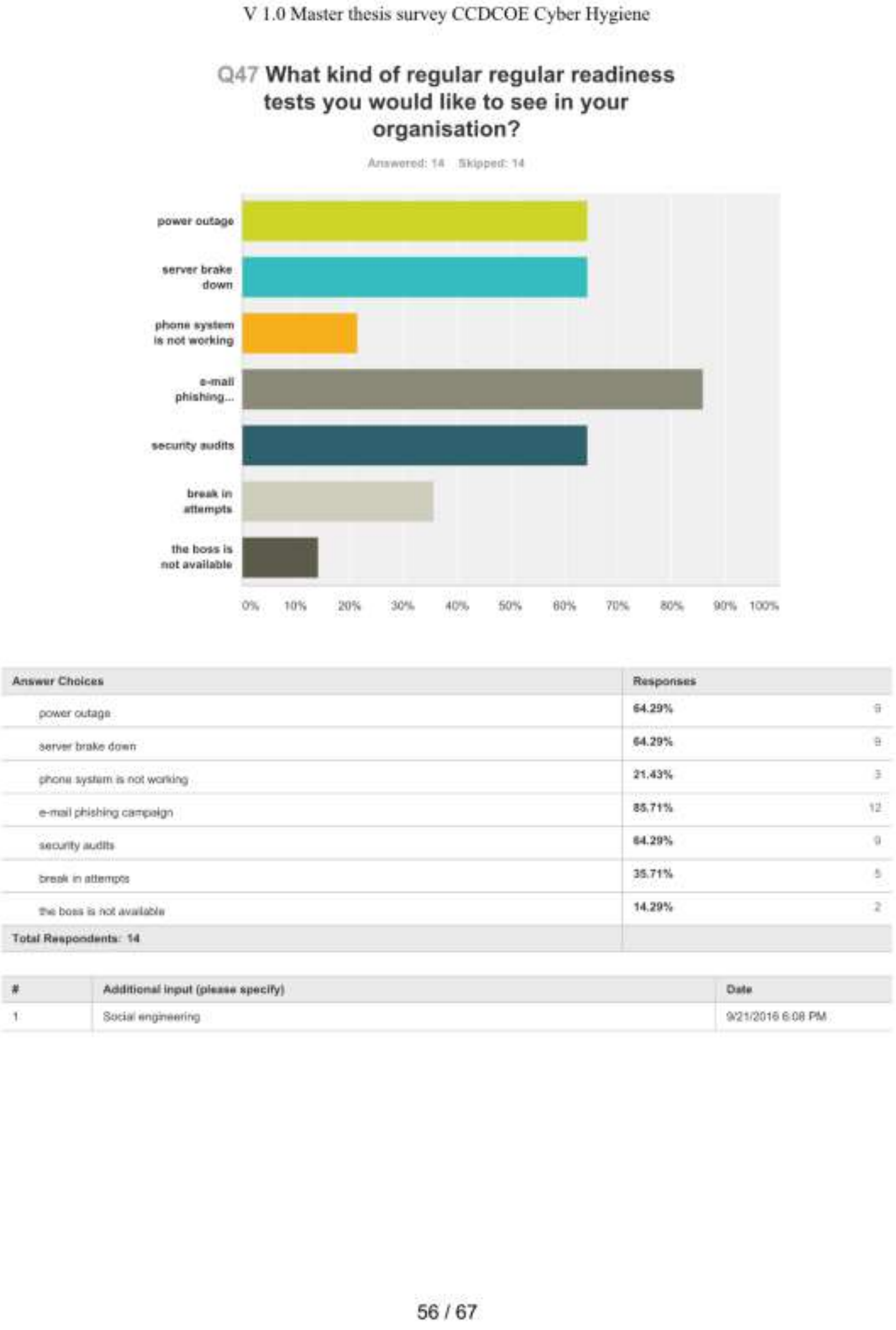
Q46 How often would you like to see such regular readiness tests in your organisation?

Answered: 13 Skipped: 15

Answer Choices	Responses	
daily	0.00%	0
weekly	0.00%	0
monthly	23.08%	3
quarterly	30.77%	4
semi-annually	15.38%	2
annually	23.08%	3
unregularly, every now and then	7.69%	1
not at all	0.00%	0
Total		13

#	Additional input (please specify)	Date
1	Out of my area of expertice	8/18/2016 8:24 PM

55 / 67



V 1.0 Master thesis survey CCDCOE Cyber Hygiene

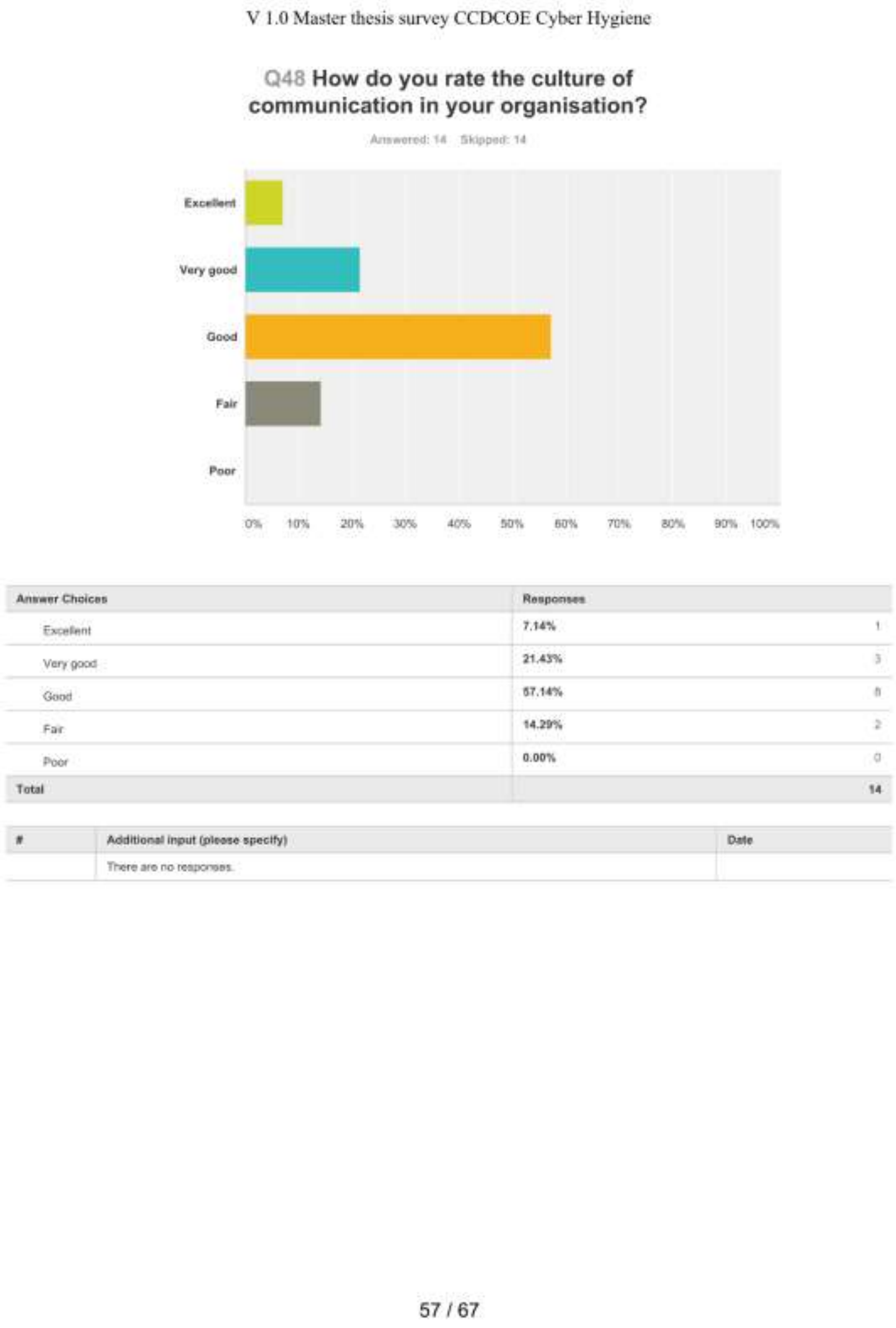
Q47 What kind of regular regular readiness tests you would like to see in your organisation?

Answered: 14 Skipped: 14

Answer Choices	Responses	
power outage	64.29%	9
server brake down	64.29%	9
phone system is not working	21.43%	3
e-mail phishing campaign	85.71%	12
security audits	64.29%	9
break in attempts	35.71%	5
the boss is not available	14.29%	2
Total Respondents: 14		

#	Additional input (please specify)	Date
1	Social engineering	9/21/2016 6:08 PM

56 / 67

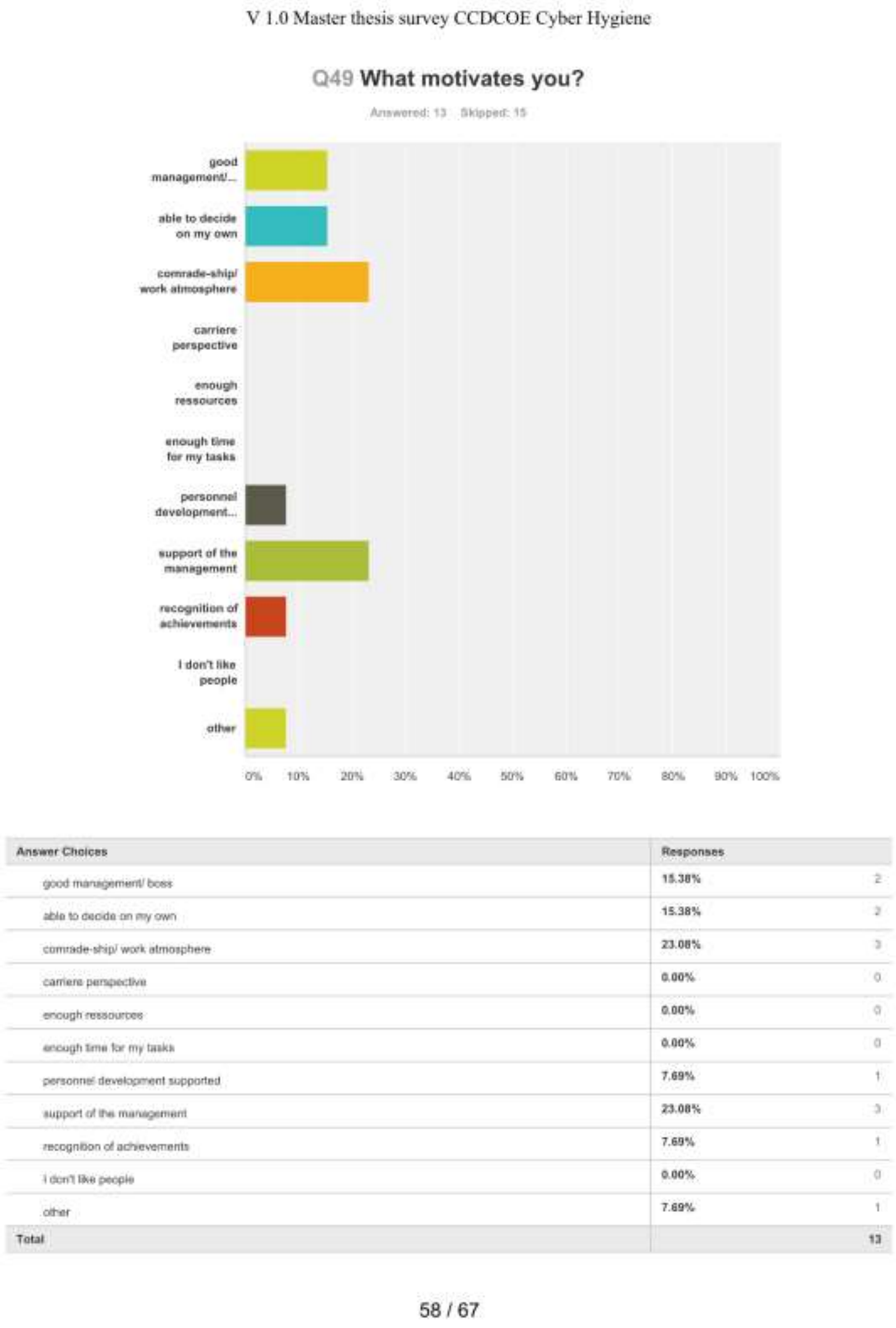


Q48 How do you rate the culture of communication in your organisation?

Answered: 14 Skipped: 14

Answer Choices	Responses	
Excellent	7.14%	1
Very good	21.43%	3
Good	57.14%	8
Fair	14.29%	2
Poor	0.00%	0
Total		14

#	Additional input (please specify)	Date
	There are no responses.	



V 1.0 Master thesis survey CCDCOE Cyber Hygiene

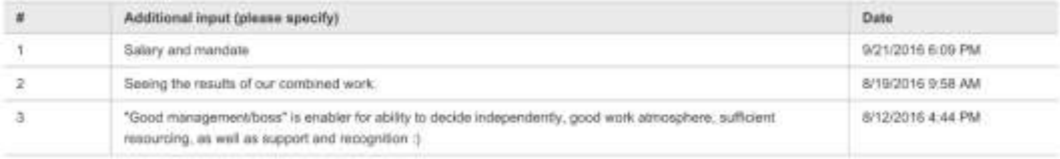
Q49 What motivates you?

Answered: 13 Skipped: 15

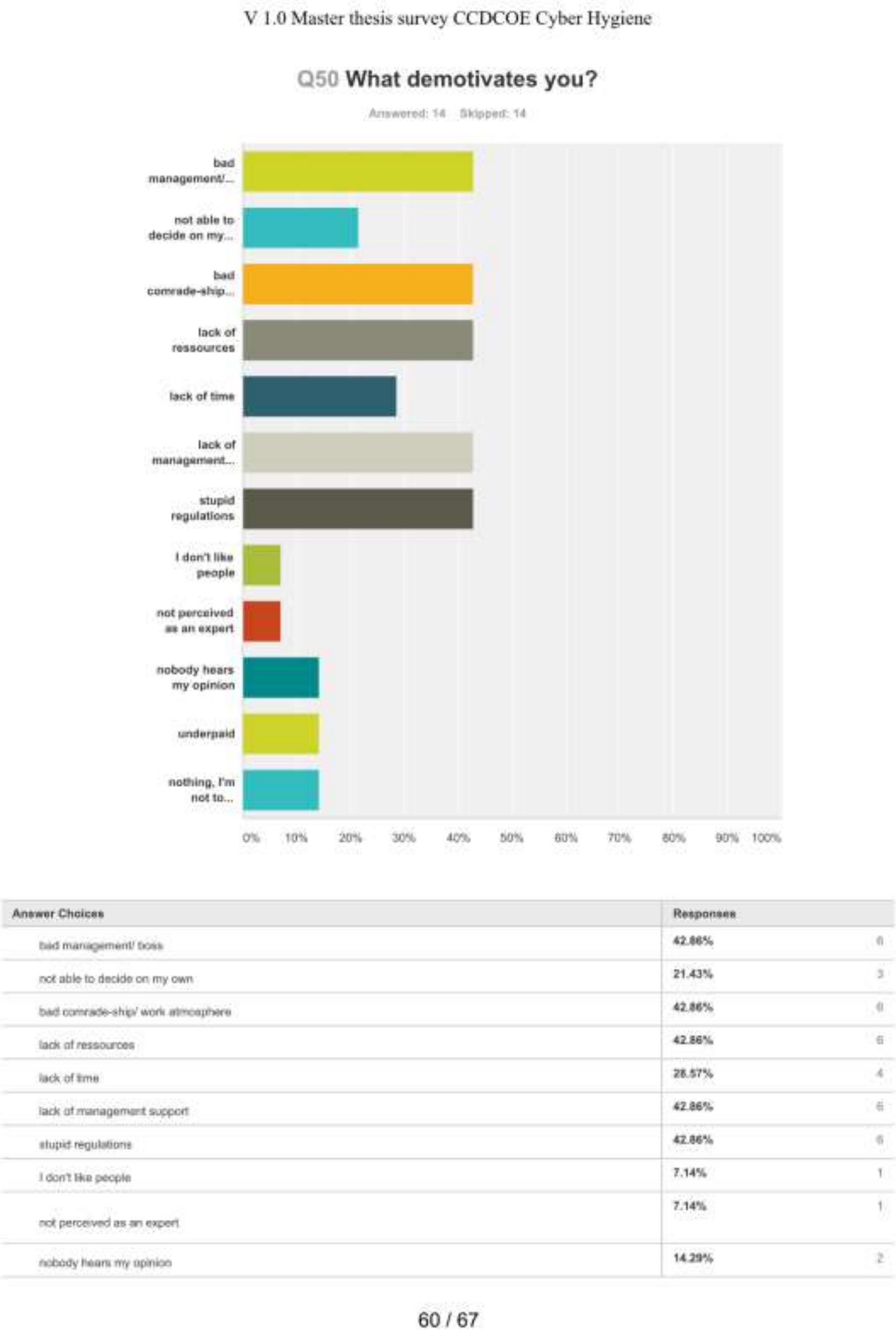
Answer Choices	Responses	
good management/ boss	15.38%	2
able to decide on my own	15.38%	2
comrade-ship/ work atmosphere	23.08%	3
carriere perspective	0.00%	0
enough ressources	0.00%	0
enough time for my tasks	0.00%	0
personnel development supported	7.69%	1
support of the management	23.08%	3
recognition of achievements	7.69%	1
I don't like people	0.00%	0
other	7.69%	1
Total		13

58 / 67

V 1.0 Master thesis survey CCDCOE Cyber Hygiene



#	Additional input (please specify)	Date
1	Salary and mandate	9/21/2016 6:09 PM
2	Seeing the results of our combined work.	8/19/2016 9:58 AM
3	"Good management/boss" is enabler for ability to decide independently, good work atmosphere, sufficient resourcing, as well as support and recognition :)	8/12/2016 4:44 PM



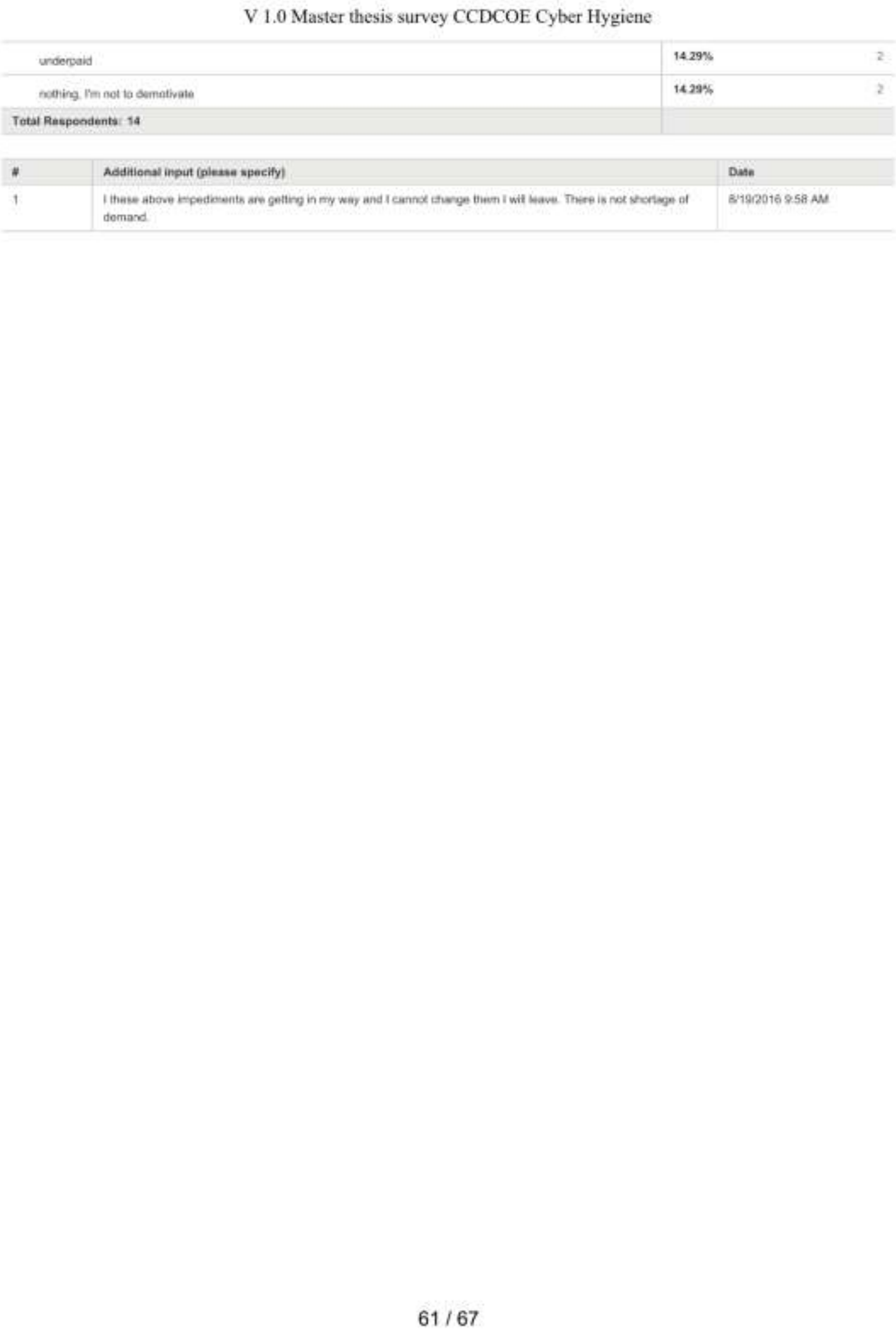
V 1.0 Master thesis survey CCDCOE Cyber Hygiene

Q50 What demotivates you?

Answered: 14 Skipped: 14

Answer Choices	Responses	
bad management/ boss	42.86%	6
not able to decide on my own	21.43%	3
bad comrade-ship/ work atmosphere	42.86%	6
lack of ressources	42.86%	6
lack of time	28.57%	4
lack of management support	42.86%	6
stupid regulations	42.86%	6
I don't like people	7.14%	1
not perceived as an expert	7.14%	1
nobody hears my opinion	14.29%	2

60 / 67

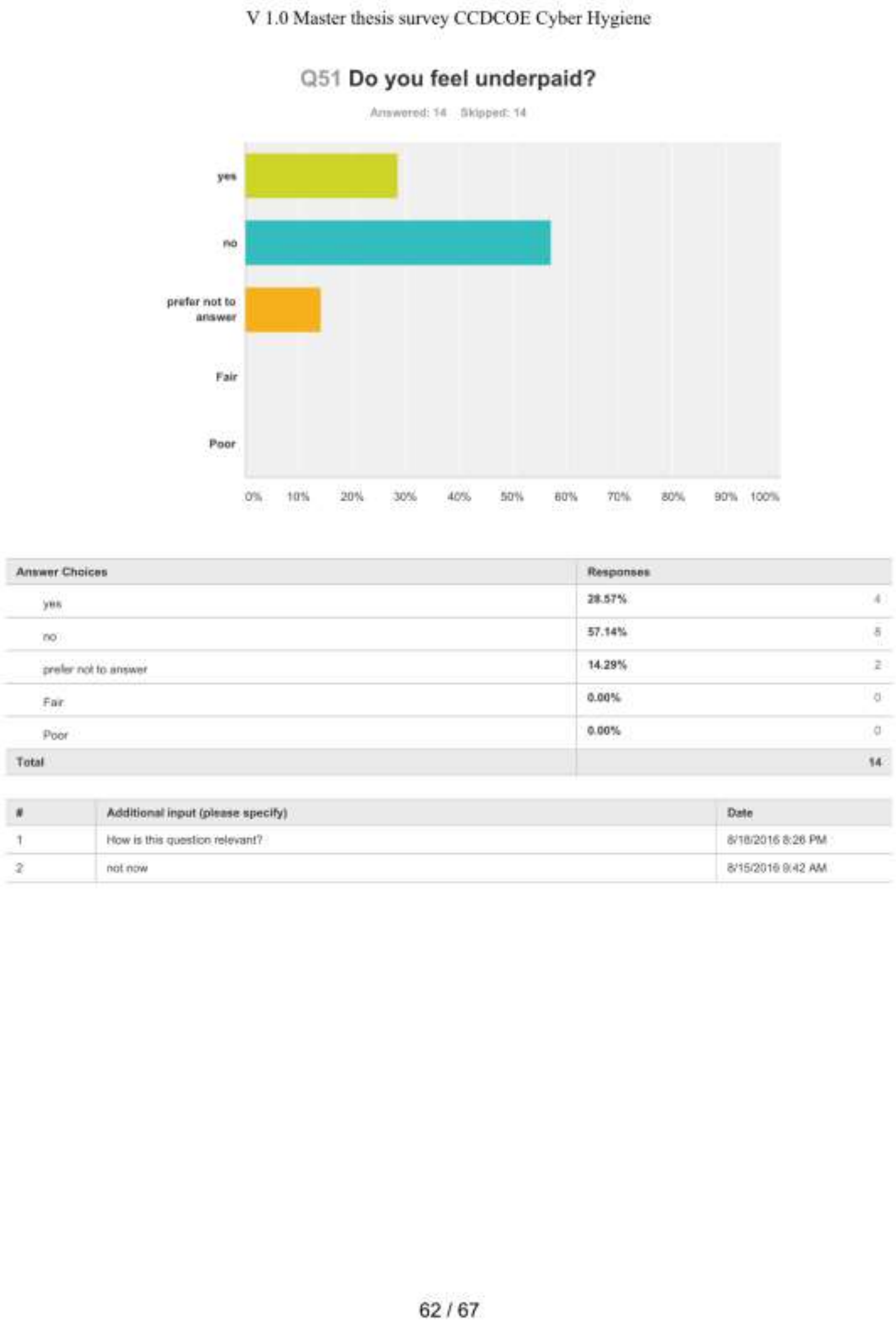


V 1.0 Master thesis survey CCDCOE Cyber Hygiene

underpaid	**14.29%**	2
nothing, I'm not to demotivate	**14.29%**	2
Total Respondents: 14		

#	Additional input (please specify)	Date
1	I these above impediments are getting in my way and I cannot change them I will leave. There is not shortage of demand.	8/19/2016 9:58 AM

61 / 67

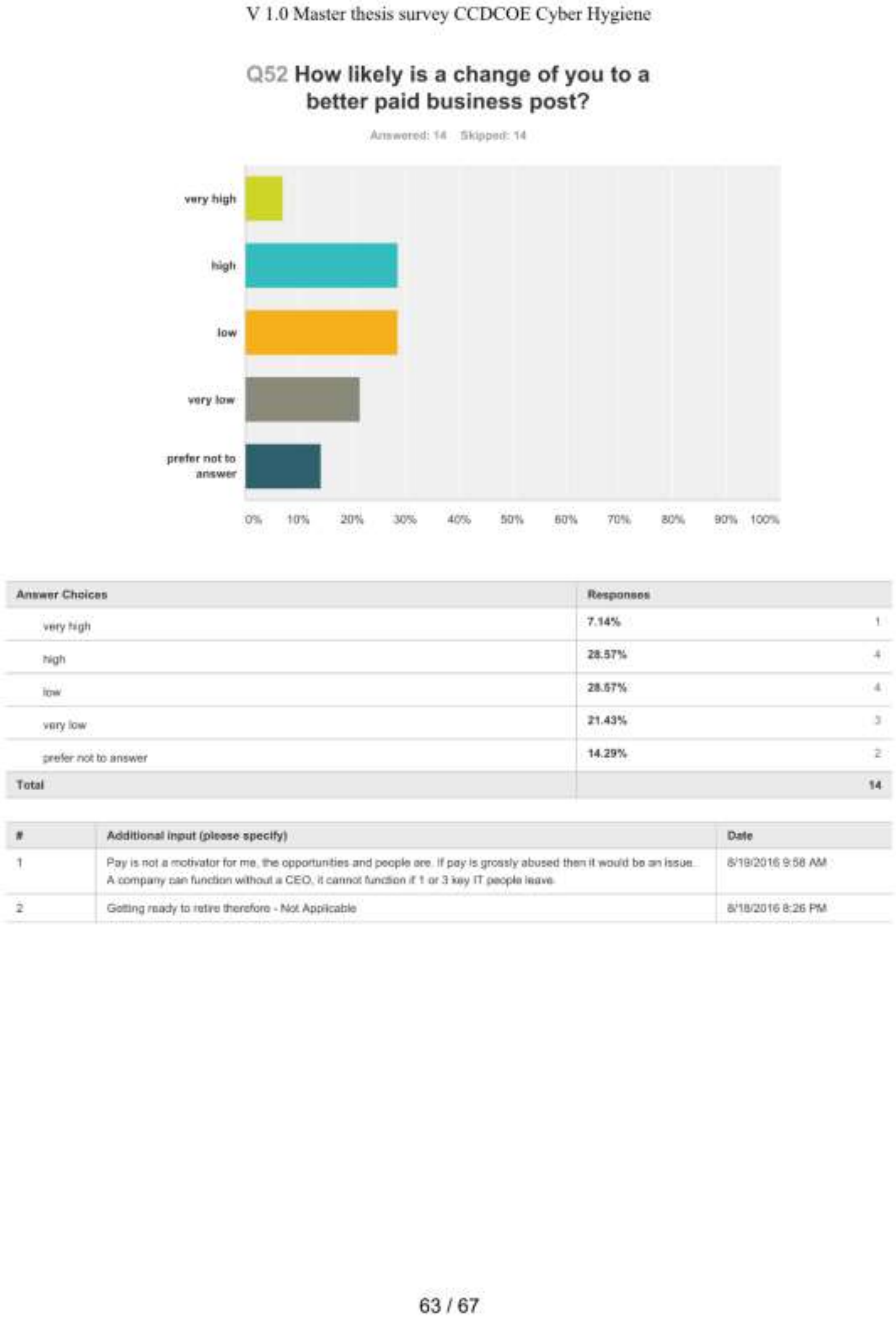


Q51 Do you feel underpaid?

Answered: 14 Skipped: 14

Answer Choices	Responses	
yes	28.57%	4
no	57.14%	8
prefer not to answer	14.29%	2
Fair	0.00%	0
Poor	0.00%	0
Total		14

#	Additional input (please specify)	Date
1	How is this question relevant?	8/18/2016 8:26 PM
2	not now	8/15/2016 9:42 AM



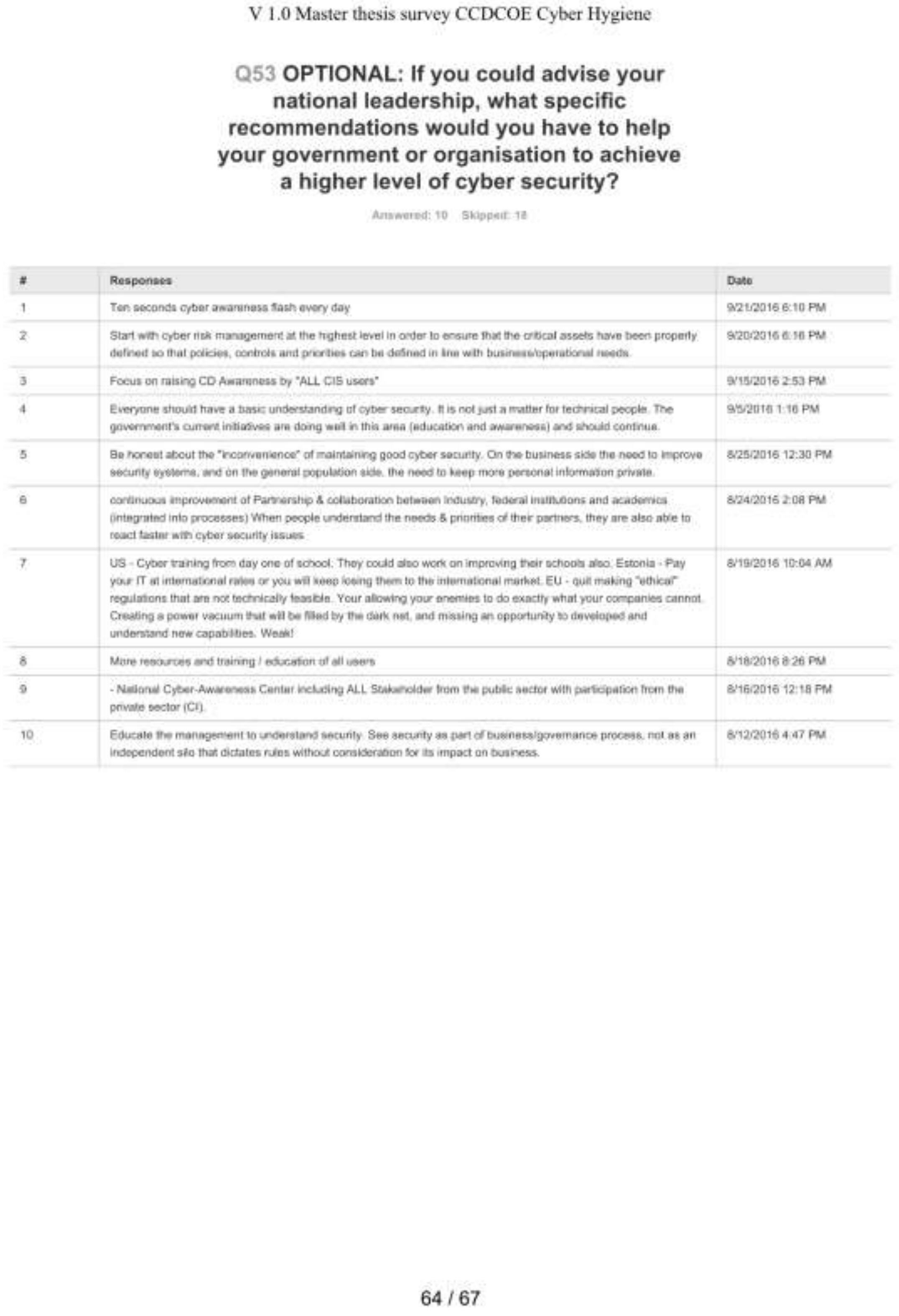
V 1.0 Master thesis survey CCDCOE Cyber Hygiene

Q52 How likely is a change of you to a better paid business post?

Answered: 14 Skipped: 14

Answer Choices	Responses	
very high	7.14%	1
high	28.57%	4
low	28.57%	4
very low	21.43%	3
prefer not to answer	14.29%	2
Total		14

#	Additional input (please specify)	Date
1	Pay is not a motivator for me, the opportunities and people are. If pay is grossly abused then it would be an issue. A company can function without a CEO, it cannot function if 1 or 3 key IT people leave.	8/19/2016 9:58 AM
2	Getting ready to retire therefore - Not Applicable	8/18/2016 8:26 PM



V 1.0 Master thesis survey CCDCOE Cyber Hygiene

Q53 OPTIONAL: If you could advise your national leadership, what specific recommendations would you have to help your government or organisation to achieve a higher level of cyber security?

Answered: 10 Skipped: 18

#	Responses	Date
1	Ten seconds cyber awareness flash every day	9/21/2016 6:10 PM
2	Start with cyber risk management at the highest level in order to ensure that the critical assets have been properly defined so that policies, controls and priorities can be defined in line with business/operational needs.	9/20/2016 6:16 PM
3	Focus on raising CD Awareness by "ALL CIS users"	9/15/2016 2:53 PM
4	Everyone should have a basic understanding of cyber security. It is not just a matter for technical people. The government's current initiatives are doing well in this area (education and awareness) and should continue.	9/5/2016 1:16 PM
5	Be honest about the "inconvenience" of maintaining good cyber security. On the business side the need to improve security systems, and on the general population side, the need to keep more personal information private.	8/25/2016 12:30 PM
6	continuous improvement of Partnership & collaboration between industry, federal institutions and academics (integrated into processes) When people understand the needs & priorities of their partners, they are also able to react faster with cyber security issues	8/24/2016 2:08 PM
7	US - Cyber training from day one of school. They could also work on improving their schools also. Estonia - Pay your IT at international rates or you will keep losing them to the international market. EU - quit making "ethical" regulations that are not technically feasible. Your allowing your enemies to do exactly what your companies cannot. Creating a power vacuum that will be filled by the dark net, and missing an opportunity to developed and understand new capabilities. Weak!	8/19/2016 10:04 AM
8	More resources and training / education of all users	8/18/2016 8:26 PM
9	- National Cyber-Awareness Center including ALL Stakeholder from the public sector with participation from the private sector (CI).	8/16/2016 12:18 PM
10	Educate the management to understand security. See security as part of business/governance process, not as an independent silo that dictates rules without consideration for its impact on business.	8/12/2016 4:47 PM

64 / 67

VI. License

Non-exclusive licence to reproduce thesis and make thesis public

I, **Christian Tschida**,

(*author's name*)

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to:

   1.1. reproduce, for the purpose of preservation and making available to the public, including for addition to the DSpace digital archives until expiry of the term of validity of the copyright, and

   1.2. make available to the public via the web environment of the University of Tartu, including via the DSpace digital archives until expiry of the term of validity of the copyright,

of my thesis

The Way to the Specialist and Management Level of Cyber Hygiene Initiative,

(title of thesis)

supervised by Sten Mäses and Raimundas Matulevičius,

(supervisor's name)

2. I am aware of the fact that the author retains these rights.

3. I certify that granting the non-exclusive licence does not infringe the intellectual property rights or rights arising from the Personal Data Protection Act.

Tartu, **21.12.2016**