CUREX

SECURE AND PRIVATE HEALTH DATA EXCHANGE

Human-centric Cyber Hygiene

Elina Argyridou, Research Associate

Christos Laoudias, Research Lecturer

KIOS Center of Excellence, University of Cyprus

KIOS Research and Innovation Center of Excellence

University of Cyprus

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826404.

Acknowledgements

- CUREX team members contributing to the Cyber Hygiene project deliverable
  - Manos Panaousis (UoG)
  - Caxton Okoh (UoG)
  - Antonio Jesus Diaz Honrubia (UPM)
  - Juan Mora Zamorano (SERMAS)
  - Marc Jofre Cruanyes (FPHAG)
  - Ramon Romeu (FPHAG)
  - Jordi Puig (FPHAG)
  - Diana Navarro (FPHAG)
  - Panos Papachristou (KI)
  - Sokratis Nifakos (KI)
  - Sabine Koch (KI)
  - Stefano Bonacina (KI)
  - Marina Taloyan (KI)

UoG: University of Greenwich; UPM: Universidad Politecnica De Madrid; SERMAS: Servicio Madrileno De Salud; FPHAG: Fundació Privada Hospital Asil de Granollers; KI: Karolinska Institutet

Outline

- Introduction
  - Cyber threats in healthcare
  - Definitions of Cyber Hygiene
  - State-of-the-art on Cyber Hygiene
  - Commercial solutions for cybersecurity training and awareness
  - Recommendations by cybersecurity organisations
- Human-centric Cyber Hygiene
  - Survey-based risk assessment methodology
    - ✓ Survey structure
    - ✓ Risk strategies
    - ✓ Risk categories
    - ✓ Risk procedures
  - Recommended human-centric controls
  - Mapping of controls to risk strategies
- Results and findings

Cybersecurity Facts in Healthcare

- Healthcare has been one of the main targets for adversaries and always among the top-3 most affected domains [Verizon DBIR 2020][1]
- Healthcare has the highest data breach cost of any industry, at an average of $408 per record and $2.2 million per organisation [U.S. HHS][2]
- In 2020, the average worldwide data breach cost for all domains was $3.86 million, while for the healthcare domain was $7.13 million [IBM][3]
- According to the Infosecurity Magazine[4]
  - **38%** of healthcare organisations have experienced personal information (medical) theft cases
  - **59%** of healthcare organisations would need sufficient security budget

[1]2020 Verizon Data Breach Investigations Report [link]
[2]Public Health Emergency, Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients [link]
[3]IBM, How much does a data breach cost? [link]
[4]Tara Seals (Infosecurity magazine), Healthcare Data Breaches Cost $6.2 Billion Per Year, 2016 [link]

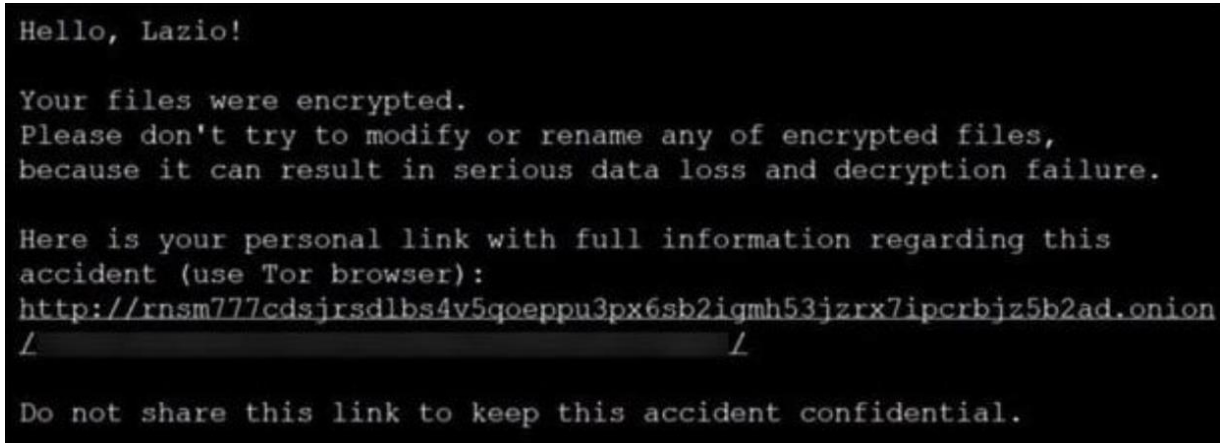
Top-5 Cyber Threats in Healthcare

- U.S Department of Health and Human Services (HHS)[1,2]
  - Email phishing
  - Ransomware
  - Loss of theft of hardware
  - Insider, accidental, or intentional data loss
  - Attacks against smart medical devices
- Centre for Internet Security (CIS)[3]
  - Ransomware
  - Data Breaches
  - DDoS Attacks
  - Insider Threat
  - Business Email Compromise and Fraud Scams

[1]M. Peters, Are You Protected Against the 5 Top Healthcare Cyber Threats?, January 18, 2019 [link]
[2]Public Health Emergency, Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients [link]
[3]Centre for Internet Security, Cyber Attacks: In the Healthcare Sector [link]

Healthcare Cyber Threats in the COVID-19 Era

- COVID-19 is used as a bait to impersonate different medical brands and launch phishing attacks, malspams and ransomware attacks[1]
- Cyber criminals exploit vulnerabilities in Healthcare Information Systems that were deployed in a hurry to fight the pandemic
  - Ransomware attack at Health Service Executive (HSE) of Ireland [May 2021][2]
  - Attack at the Covid-19 vaccination booking system of Regione Lazio in Italy [Aug. 2021][3]



[1]Cedric Nabe (Deloitte), Impact of COVID-19 on Cybersecurity [link]
[2]Independent, Cost of HSE cyber attack 'could rise to half a billion euro' [link]
[3]Franco Tommasi, A note about the ransomware attack against the Covid-19 vaccination booking system of Regione Lazio

What is Cyber Hygiene?

"It is my judgment that the Internet itself is for the most part secure, though there are steps we know can be taken to improve security and resilience. Most of the vulnerabilities arise from those who use the Internet--companies, governments, academic institutions, and individuals alike - ***but who do not practice what I refer to as good cyber hygiene.*** *They are not sufficiently sensitive to the need to protect the security of the Internet community of which they are a part. The openness of the Internet is both its blessing and its curse when it comes to security."*

Vinton Cerf

Statement of Dr. Vinton G. Cerf, Senior Vice President of Internet Architecture & Technology, MCI WorldCom, For the Joint Economic Committee, February 23, 2000 [link].

What is Cyber Hygiene?

- Cyber Hygiene refers to activities that computer system administrators and users can undertake to improve their cybersecurity while online[1]
- Cyber Hygiene is a reference to the practices and steps that users of computers and other devices take to maintain system health and improve online security[2]
  - Like physical hygiene, cyber hygiene is regularly conducted to ward off natural deterioration and common threats
- Cyber Hygiene is a fundamental principle relating to information security[3]
  - It is the equivalent of establishing simple routine measures to minimise the risks from cyber threats

[1]Cybersecurity Forum - What is Cyber Hygiene? [link]
[2]C. Brook, What is Cyber Hygiene? A Definition of Cyber Hygiene, Benefits, Best Practices, and More, December 5, 2018 [link]
[3]ENISA, Review of Cyber Hygiene practices, December 2016. [link]

CUREX “definition” of Cyber Hygiene

*A set of **strategies** and associated **measures** in the form of **human-centric controls** for raising **cybersecurity** and **data privacy** awareness of different **employee** groups in **healthcare** organisations.*

State-of-the-art on Cyber Hygiene

- Motivation for promoting cyber hygiene habits in any environment[1]
  - at least, 20% of end users do not even use an antivirus software
  - older users tend to have more secure habits
- Social marketing in the information security behaviours[2]
  - training programs raise awareness, but do not change the overall behavior
- Understand employees' behaviour through social psychology[3]
  - Re-design additional tasks for cybersecurity to fit into the primary work tasks
- Employees as a "human firewall"[4]

[1]A. A. Cain, et al., "An exploratory study of cyber hygiene behaviors and knowledge", Journal of Information Security and Applications, vol. 42, pp. 36-45, 2018.
[2]D. Ashenden and D. Lawrence, "Can we sell security like soap?: a new approach to behavior change," in NSPW, 2013.
[3]S. L. Pfleeger, et al., "From weakest link to security hero: Transforming staff security behavior," Journal of Homeland Sec. and Emerg. Management, vol. 11, no. 4, pp. 489-510, 2014.
[4]L. Coventry, D. Branley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward", Maturitas, vol. 113, pp. 48-52, 2018.

State-of-the-art on Cyber Hygiene

- "Shadow behaviours" in the healthcare sector[1]
  - Workarounds made by employees to cheat cybersecurity systems and make their daily tasks faster/easier
- Most of the employees show a demotivation when they must follow a specific policy for data protection[2]
  - Recognition and reward, improve the communication, observe real end-user behaviour
- Only basic recommendations are incorporated in the healthcare sector[3]
- Conceptual and operational definitions for Cyber Hygiene[4]
  - Sub-dimensions of Cyber Hygiene: **S**torage and Device, **A**uthentication and Credential, **F**acebook and Social Media, **E**mail and messaging, **T**ransmission and Browsing, **Y**our (S.A.F.E.T.Y.)

[1]Koppel, S. Smith, et al., "Workarounds to Computer Access in Healthcare Organizations: You Want My Password or a Dead Patient?", Studies in Health Technology and Informatics, vol. 208, pp. 215-220, 2015.
[2]K. Renaud and W. Goucher, "Health service employees and information security policies: an uneasy partnership?," Information Management & Computer Security, vol. 20, no. 4, pp. 296-311, 2012.
[3]L. Kim, "Cybersecurity awareness: Protecting data and patients", Nursing Management, vol. 48, no. 4, pp. 65-67, 2017.
[4]A. Vishwanath, et al., Cyber hygiene: The concept, its measure, and its initial tests, Decision Support Systems, Volume 128, 2020.

Commercial Solutions for Training and Awareness

- **80%** of the breaches where due to improper implementation of the protection mechanisms[1]
- A key prerequisite in increasing awareness at all hierarchical levels is through training, especially computer-based trainings
- Key functionalities of a security training programme include:
  - Awareness of threat and mitigating actions
  - Security communication
- Training and education can fulfil multiple objectives including[2]:
  - Complying with regulations that mandate security training
  - Establishing behavioural guidelines supporting disciplinary processes
  - Improving employee knowledge of security and risk topics
  - Motivating required and desired security behaviours

[1]R. Koppel, et al., "Workarounds to Computer Access in Healthcare Organizations: You Want My Password or a Dead Patient?", *Studies in Health Technology and Informatics*, vol. 208, pp. 215-220, 2015

[2]Open Access Government, Cybersecurity in hospitals and care centres, July 2019 [link]

Commercial Solutions for Training and Awareness

- Vendors of security training products differentiate their products through:
  - Varying content formats, lengths, and styles, including mobile capabilities
  - Focusing on gamification
  - Offering multi-language support, some including cultural variants/dialects
  - Offering large libraries of pre-designed contents
  - Adjusting their prices to seek a large share of small and midsize market
  - Exploring possibilities of partnering with core security technology vendors
    - ✓ employee-monitoring vendors
    - ✓ endpoint detection and response vendors
    - ✓ endpoint protection platform vendors
    - ✓ secure email gateway vendors
    - ✓ data security vendors

Commercial Solutions for Training and Awareness

- Gartner's magic quadrant categorises existing vendors in the market for security awareness computer-based training[1]
- Different criteria
  - services and customer satisfaction/experience
  - overall viability of the product or service and ability to meet client requirements
- The quadrant is further divided as:
  - vendors providing security education matching specific use cases (Niche players)
  - vendors providing services that are good functional matches to general security education market requirement (Visionaries)
  - vendors having sustainable customer base and revenue, and products that meet most market requirements (Challengers)
  - vendors providing products/services matching customer requirements (Leaders)

[1]Joanna Huisman (Gartner), Magic Quadrant for Security Awareness Computer-Based Training, July 2019 [link]

Cybersecurity for Healthcare Ecosystem

- Healthcare Ecosystem
  - more than 10 million healthcare professionals
  - more than 15.000 hospitals
  - 28 National Healthcare Systems or Social Security Systems
  - more than 25 cybersecurity agencies and institutions.
- Relevant Cybersecurity Agencies/Organisations
  - European Union Agency for Cybersecurity (ENISA)
  - European Cyber Security Organisation (ECSO)
  - Center for Internet Security (CIS)
    - ✓CIS Critical Security Controls® v8[1]
    - ✓Control 14: Security Awareness and Skills Training

[1]CIS Critical Security Controls® [link]

Recommendations by Cybersecurity Organisations

- Raise cybersecurity awareness
- Secure medical and portable devices
- Protect the network and install a firewall
- Keep computers and credentials healthy
- Conduct risk and vulnerability assessment and perform intrusion testing and auditing
- Secure physical access and health information
- Phishing attacks

Human-centric Cyber Hygiene Solution

- Challenges
  - The cost of cybersecurity and data privacy incidents is rising globally
  - Technical IT-based measures are not sufficient to counter the attacks
  - The role of personnel in the chain of cyber defence is often neglected
- Solution
  - Survey-based risk assessment methodology for Cyber Hygiene
  - Focus on the gaps and needs of individual employee groups
  - Identify the most effective strategy to manage risks
  - Recommend targeted human-centric controls to implement the strategy
- Impact
  - Increase employee confidence in identifying and handling incidents
  - Support the management team by recommending targeted controls that are tailored to the organisation-specific needs

Outline of the Cyber Hygiene Methodology

1. Extract knowledge and assess the needs and gaps of different employee groups at healthcare organisations through a **survey** questionnaire
2. Process and analyse the participants' **responses**
3. Identify the most effective **strategy** to manage each cybersecurity and data privacy risk
4. Recommend targeted human-centric **controls** to implement the strategy
5. The management team can apply the controls to the **workforce** to improve the situation

Survey Structure

- In each healthcare institution, we identified four main employee groups:
  - Administrative
  - Medical/Clinical
  - IT/Technical
  - Executive/Security
- Survey parts
  - First part contains general questions for all employee groups
  - Second part contains additional group-specific questions for IT/Technical staff
  - Third part contains additional group-specific questions for Executive/Security staff
- Survey questions (single or multiple answer)
  - Awareness: YES/NO/I don't know
  - Agreement: 1 = I strongly disagree | 5 = I strongly agree
  - Frequency: 1 = Never | 5 = In every daily activity
  - Knowledge: 1 = I have no knowledge | 5 = I am an expert
  - Satisfaction: 1 = Very disappointing | 5 = Very Satisfying

Survey Methodology – Risk Strategies

Impact – Probability Risk Matrix

Risk Probability		Risk Impact				
		Negligible	Minor	Moderate	Significant	Severe
		1	2	3	4	5
Very Likely	5	Low Med	Medium	Med Hi	High	High
Likely	4	Low	Low Med	Medium	Med Hi	High
Possible	3	Low	Low Med	Low Med	Medium	Med Hi
Unlikely	2	Low	Low	Low Med	Low Med	Medium
Very Unlikely	1	Low	Low	Low	Low	Low Med

Risk Marking = Risk Impact x Risk Probability

Risk Evaluation Matrix

Risk Marking	Risk Evaluation	Risk Strategy	High-Level Action Plan
[20 - 25]	High	Mitigation	**Mitigate** the risk: Improve Skills / Raise Awareness / **Monthly or Weekly** actions for **Beginners** level
[15 - 19]	Medium-High	Reduction	**Reduce** the risk: Improve Skills / Raise Awareness / **Quarterly or Monthly** actions for **Intermediate** level
[10 - 14]	Medium	Monitoring	**Monitor** the risk: Increase Awareness / **Semi-Annually or Quarterly** actions for **Intermediate or Advanced** level
[5 - 9]	Low-Medium	Checking	**Check** the risk: Retain Awareness / **Annually** or **Semi-Annually** interventions for **Advanced** level
[1 - 4]	Low	Acceptance	**Accept** the risk: Acknowledgment / Rewards

Survey Methodology – Risk Categories

- Survey questions are grouped in risk categories based on their topic
  - ➢ Facilitates risk analysis and estimation of the risk profile of each employee group
- Seven risk categories for all employee groups
  - ➢ Separate risk categories specialized to IT/Technical and Executive/Security staff

Risk Category (All employees)	Survey Questions	Risk description
Cyber Hygiene	2, 3, 4	Not aware of what Cyber Hygiene is
Cybersecurity Awareness	8, 11, 13	Not aware of cybersecurity threats in healthcare and related incidents
Data Privacy/Protection Awareness	5, 6, 8, 12, 14	Not aware of what GDPR is, data privacy/protection threats in healthcare and related incidents
Cybersecurity Training	9, 15, 17, 20	Not attending existing training, not considering cybersecurity during daily work, not knowing about internal procedures for cybersecurity threats, limited knowledge about cybersecurity (self-assessed)
Data Privacy/Protection Training	7, 10, 16, 18, 19, 21	Not attending existing training, not considering data privacy during daily work, not knowing about internal procedures for data privacy threats and who is responsible for data protection, managing personal data frequently, limited knowledge about data privacy (self-assessed)
Communication Channels	22, 23, 24	Limited number of communication channels that are available in the organization or preferred by employees, and limited communication with IT personnel
Secure connection and use of devices	25, 26, 27, 28	Not aware of or not following policies, guidelines, or best practices about remote connection, using public access networks, using personal devices (BYOD), and using personal USB sticks

Survey Methodology – Risk Procedures

Risk Impact		Frequency	Agreement	Knowledge	YES/NO/ I don't know	Multiple Answers
1	Low	Daily	Strongly agree	In-depth	YES	All selected
2	Low Medium	Weekly	Agree	Very well		Many selections
3	Medium	Monthly	Can't say	Well	I don't know	Enough selections
4	Medium High	Rarely	Disagree	Heard of it		Few selections
5	High	Never	Strongly disagree	Never heard	NO	One or nothing

Risk Probability		Responses in total (Re)	e.g. Re = 100
1	Very Unlikely	[0 - Re* (1/5))	[0-20)
2	Unlikely	[Re* (1/5) - Re*(2/5))	[20-40)
3	Possible	[Re*(2/5) - Re* (3/5))	[40-60)
4	Likely	[Re* (3/5) - Re*(4/5))	[60-80)
5	Very Likely	[Re*(4/5) - Re]	[80-100]

- Risk Marking (RM) = $\sum_{i=1}^{n}$ (risk(s) impact x risk(s) probability)x RF, Risk Factor (RF)

Recommended Human-centric Controls

- 19 controls related to Training, Awareness, Motivation and Rewarding
- Developed in CUREX and inspired by CIS Control 17* and PANACEA project

No	Control Title	Control Description	Related Resource
C1	Perform a Skills Gap Analysis	Perform a skills gap analysis to understand the skills and behaviors employees are not adhering to, using this information to build a baseline education roadmap.	CIS Sub-control 17.1
C2	Deliver Training to Fill the Skills Gap	Deliver training to address the skills gap identified to positively impact employees' security behavior.	CIS Sub-control 17.2
C3	Implement a Cybersecurity Awareness Program	Create a cybersecurity awareness program for employees to ensure they understand and exhibit the necessary behaviors and skills to help ensure the security of the organization.	CIS Sub-control 17.3
C4	Implement a Data Privacy Awareness Program	Create a data privacy awareness program for employees to ensure they understand and exhibit the necessary behaviors and skills to help ensure the security of the organization.	CIS Sub-control 17.3
C5	Update Awareness Content Frequently	Ensure that the organization's security awareness program is updated frequently to address new technologies, threats, standards, and business requirements.	CIS Sub-control 17.4
C6	Train Workforce on Secure Authentication	Train employees on the importance of enabling and utilizing secure authentication.	CIS Sub-control 17.5
C7	Train Workforce on Identifying Social Engineering Attacks	Train employees on how to identify different forms of social engineering attacks, such as phishing, phone scams, and impersonation calls.	CIS Sub-control 17.6
C8	Conduct Mock Social Engineering Exercises	Conduct mock social engineering attacks (phishing, phone scams, and impersonation calls) to assess the readiness and response level of the employees	CIS Sub-control 17.6
C9	Train Workforce on Sensitive Data Handling	Train employees on how to identify and properly store, transfer, archive, and destroy sensitive information.	CIS Sub-control 17.7
C10	Train Workforce on Causes of Unintentional Data Exposure	Train employees to be aware of causes for unintentional data exposures, such as losing their mobile devices or a USB stick with sensitive data, emailing the wrong person, etc.	CIS Sub-control 17.8

*CIS Control 17: Implement a Security Awareness and Training Program (CIS Controls V7.1)

Recommended Human-centric Controls (cont.)

No	Control Title	Control Description	Related Resource
C11	Train Workforce Members on Identifying and Reporting Incidents	Train employees to be able to identify the most common indicators of an incident and be able to report such an incident.	CIS Sub-control 17.9
C12	Include Cybersecurity in the meetings' agenda	Set Cybersecurity as a standing agenda item at meetings	CUREX project
C13	Include Data Privacy in the meetings' agenda	Set Data Privacy as a standing agenda item at meetings	CUREX project
C14	Introduce nudges to motivate cybersecurity behaviors	Introduce nudges as behavioral interventions to motivate and encourage employees to adopt desirable cybersecurity behaviours that they are already aware of	PANACEA project
C15	Introduce nudges to motivate data privacy behaviors	Introduce nudges as behavioral interventions to motivate and encourage employees to adopt desirable data privacy behaviours that they are already aware of	PANACEA project
C16	Acknowledge employees that behave in a cybersecurity and data privacy responsible way	Acknowledge employees that demonstrate cybersecurity and data privacy behaviors (e.g., report to the IT scam emails, suspicious incidents, etc.) and reward them (e.g., introduce awards like 'Cybersecurity Employee of the Year')	CUREX project
C17	Introduce a cybersecurity and data privacy champion role	Nominate an employee within each department/team in the organization who, given some specific skills and knowledge, will be responsible to promote cybersecurity and data privacy best practices in daily work.	CUREX project
C18	Celebrate Cybersecurity awareness on specific occasions	Introduce a specific day/week/month during the year for celebrating cybersecurity, e.g., the National Cyber Security Awareness Month (NCSAM) observed every October in the USA.	CUREX project
C19	Celebrate Data Privacy/Protection awareness on specific occasions	Introduce a specific day/week/month during the year for celebrating data privacy and protection, e.g., the Data Privacy Day in the USA and the European Data Protection Day both observed every January 28th.	CUREX project

Mapping of Controls to Risk Strategies

- Main idea: As a risk is increasing
  - Strategy changes from "Acceptance" to "Mitigation" → Move from "Rewarding" to "Awareness"/"Training" controls
- A control may have different **implementation levels** depending on the strategy
  - Frequency: Weekly, Monthly, Quarterly, Semi-annually, Annually
  - Content: Beginners, Intermediate, Advanced
  - Target audience: Administrative, Medical/Clinical, IT/Technical, Executive/Security

Risk Category (All employees)	Risk Strategy				
	Mitigation	Reduction	Monitoring	Checking	Acceptance
Cyber Hygiene	C3, C4, C5, C12, C13	C3, C4, C12, C13, C17	C12, C13, C17	C16, C17, C18, C19	C16, C18, C19
Cybersecurity Awareness	C3, C5, C11, C12	C3, C5, C11, C12, C17	C11, C12, C17	C16, C17, C18	C16, C18
Data Privacy/Protection Awareness	C4, C5, C11, C13	C4, C5, C11, C13, C17	C11, C13, C17	C16, C17, C19	C16, C19
Cybersecurity Training	C1, C2, C7, C8, C11	C7, C8, C11, C12, C17	C11, C12, C14, C17	C14, C16, C17, C18	C16, C18
Data Privacy/Protection Training	C1, C2, C9, C10	C9, C10, C11, C13, C17	C11, C13, C15, C17	C15, C16, C17, C19	C16, C19
Communication Channels	C3, C4, C5	C3, C4, C5, C17	C14, C15, C17	C14, C15, C17	-
Secure connection and use of devices	C3, C4, C5, C6, C9, C10	C3, C4, C5, C6, C9, C10, C17	C10, C14, C15, C17	C14, C15, C16, C17, C18, C19	C16, C18, C19

Survey Demographics

HO1	Population	Responses	Confidence Interval (95%)
Administrative	278	15	24.66
Medical/Clinical	1437	29	18.02
Executive/Security	88	16	22.29
IT/Technical	12	11	8.91

- Survey was planned to be released in March 2020
- Delayed due to Covid-19 outbreak
- Open from mid-June 2020 to end of September 2020

HO2	Population	Responses	Confidence Interval (95%)
Administrative	24	16	14.45
Medical/Clinical	2730	178	7.1
Executive/Security	12	3	51.18
IT/Technical	5	2	60.01

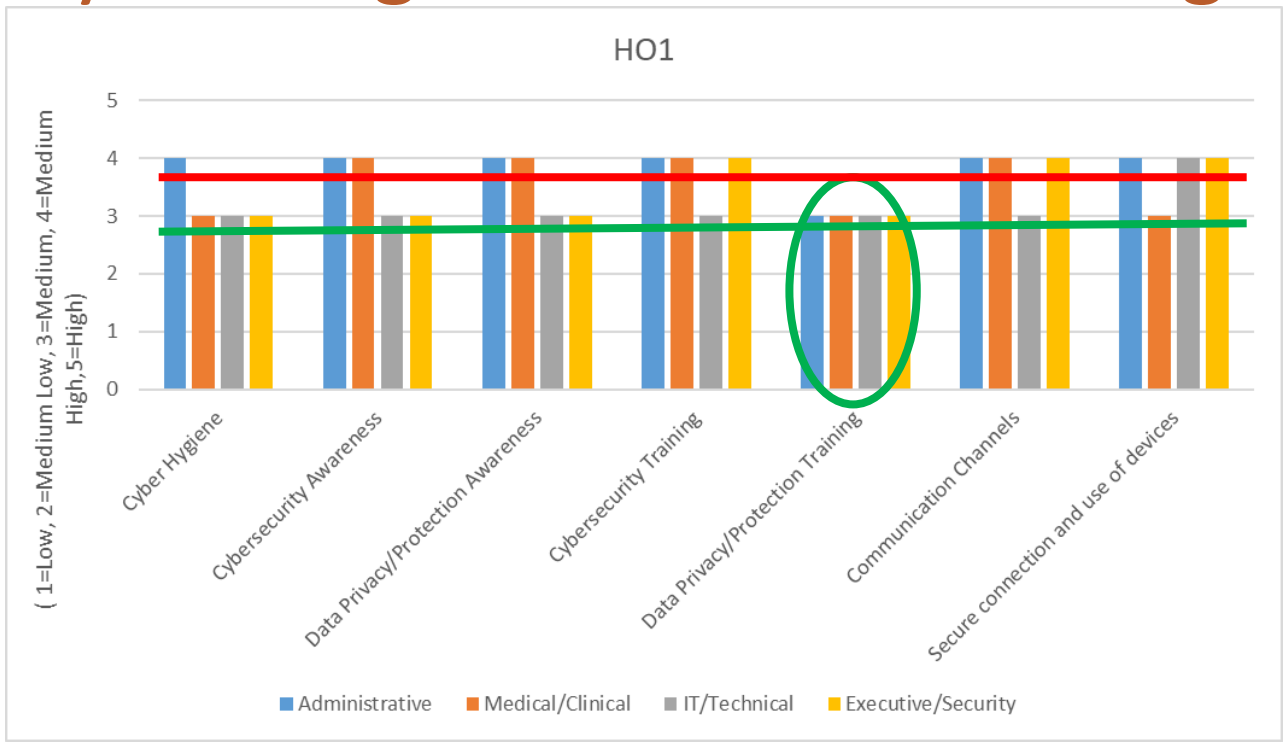
HO3	Population	Responses	Confidence Interval (95%)
Administrative	78	16	21.98
Medical/Clinical	554	70	10.96

HO: Healthcare Organisation
Confidence Interval calculation:
https://www.surveysystem.com/sscalc.htm

Analysis of the Results and Findings

- The analysis of the results is performed with regards to four different Dimensions(D):
  - D1 – Healthcare Organisation
    - ✓ HO1, HO2, HO3
  - D2 – Employee Group
    - ✓ Administrative, Medical/Clinical, IT/Technical, Executive/Security
  - D3 – Specific Risk Category
    - ✓ Cyber Hygiene, Cybersecurity Awareness, Data Privacy/Protection Awareness, Cybersecurity Training, Data Privacy/Protection Training, Communication Channels, Secure connection and use of devices)
  - D4 – Specific Survey Question
    - ✓ Questions 8, 22, 23

Survey Findings: D1-Healthcare Organisation

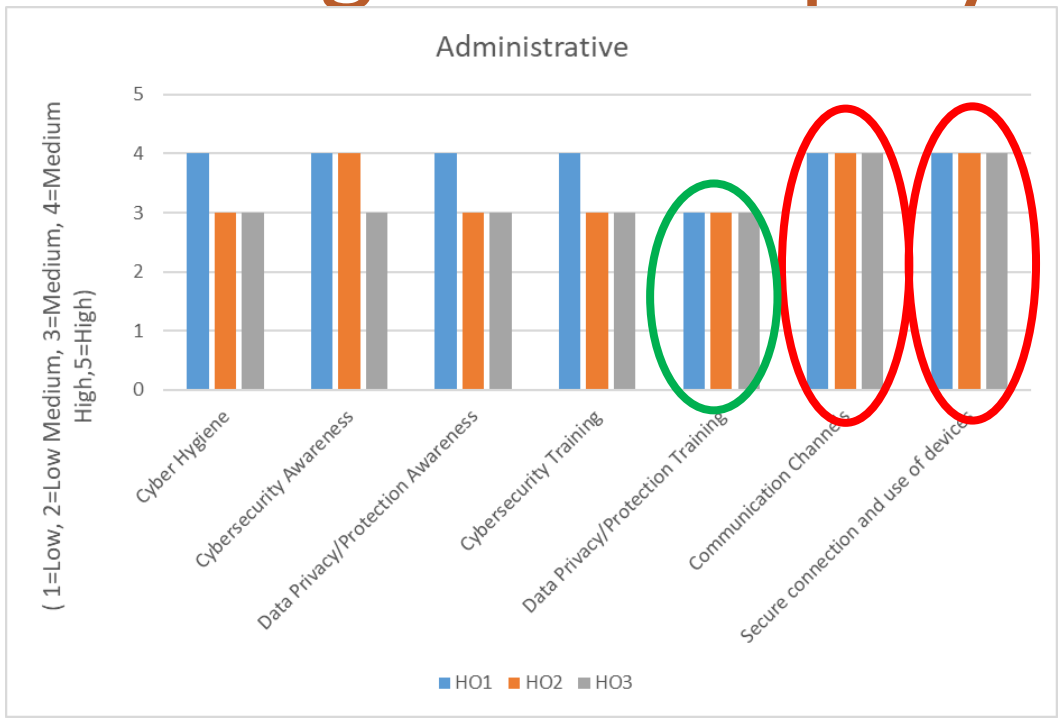


- Risk strategy: “Monitoring” or “Reduction” for all risk categories
- Lowest Risk: “Data Privacy/Protection Training”
  - Risk Strategy: “Monitoring”
  - Recommended controls: Training (C11), Awareness (C13), Motivation (C15, C17)
  - Implementation levels: Semi-annually or Quarterly | Intermediate or advanced

Survey Findings: D1-Healthcare Organisation

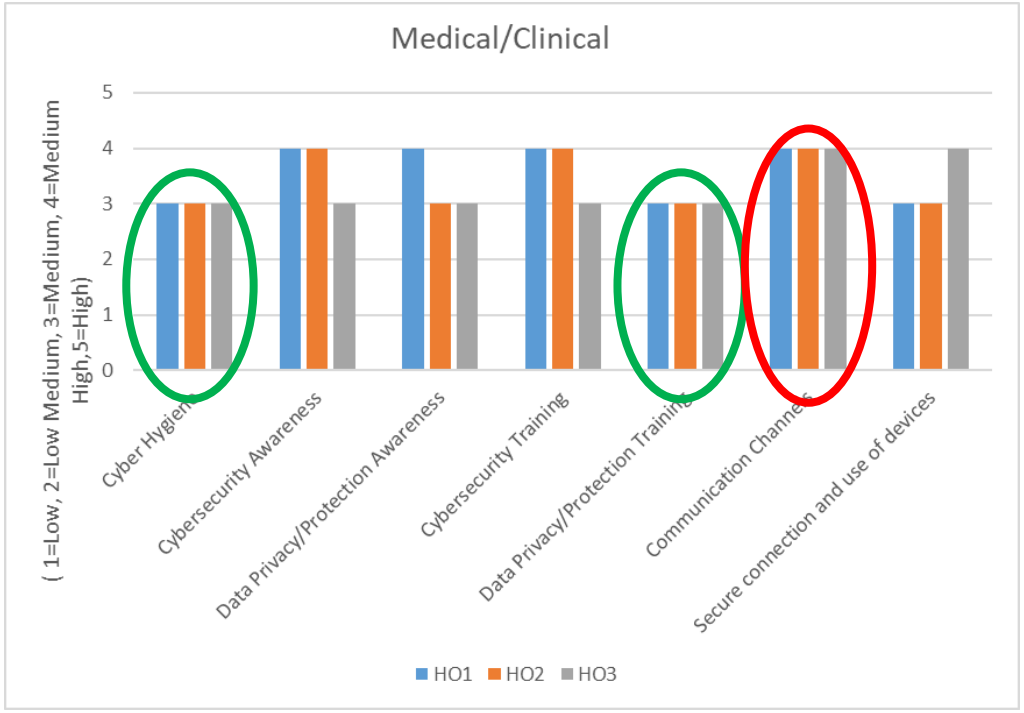
- Risk strategy: “Monitoring” or “Reduction” for most risk categories
- Highest Risk: “Secure connection and use of devices” – IT/Technical group
  - Risk Strategy: “Mitigation”
  - Recommended controls: Training (C6, C9 C10) and Awareness (C3, C4, C5)
  - Implementation levels: Monthly or weekly | Beginners | IT/Technical

Survey Findings: D2-Employee Group



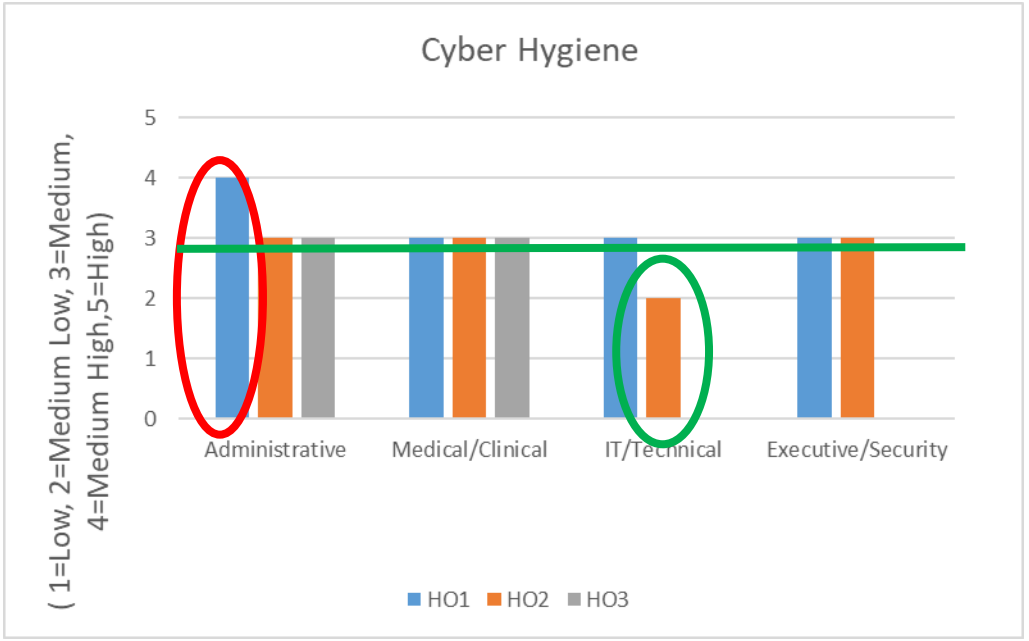
- Lowest Risk: “Data Privacy/Protection Training” with medium level
- Highest Risks: “Communication channels” and “Secure connections and use of devices”
  - Risk Strategy: “Reduction”
  - Recommended controls: Awareness (C3, C4, C5, C6, C9, C10) and Motivation (C17)
  - Implementation levels: Quarterly or monthly | Intermediate | Administrative

Survey Findings: D2 – Employee Group



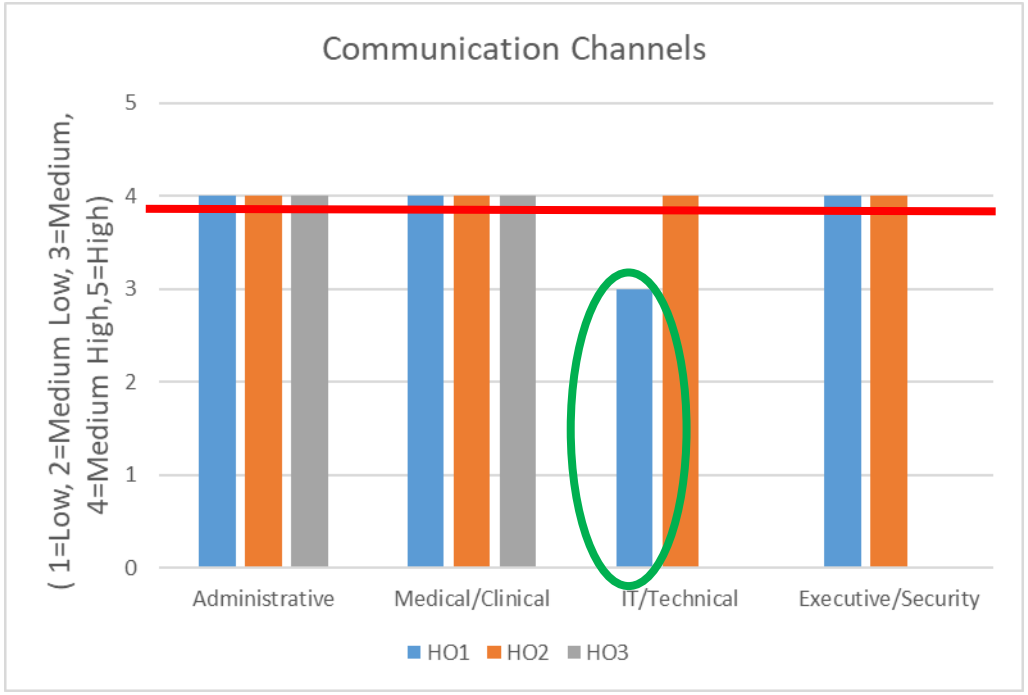
- Lowest Risk: “Cyber Hygiene” and “Data Privacy/Protection Training”
- Highest Risk: “Communication channels”
  - Risk Strategy: “Reduction”
  - Recommended controls: Awareness (C3, C4, C5) and Motivation (C17)
  - Implementation levels: Quarterly or monthly | Intermediate | Medical/Clinical

Survey Findings: D3 – Specific Risk Category



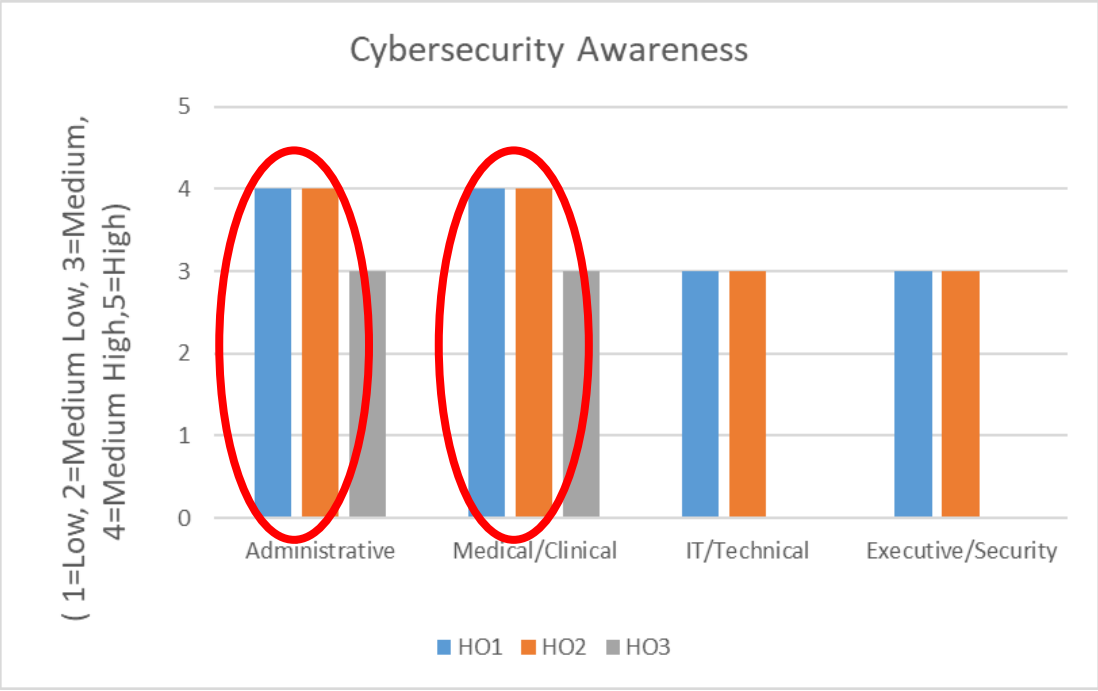
- Lowest Risk: “IT/Technical” employee group at HO2
- Highest Risk: “Administrative” employee group at HO1
  - Risk Strategy: “Reduction”
  - Recommended controls: Awareness (C3, C4,C12, C13) and Motivation (C17)
  - Implementation levels: Quarterly or monthly | Intermediate | Administrative at HO1

Survey Findings: D3 – Specific Risk Category



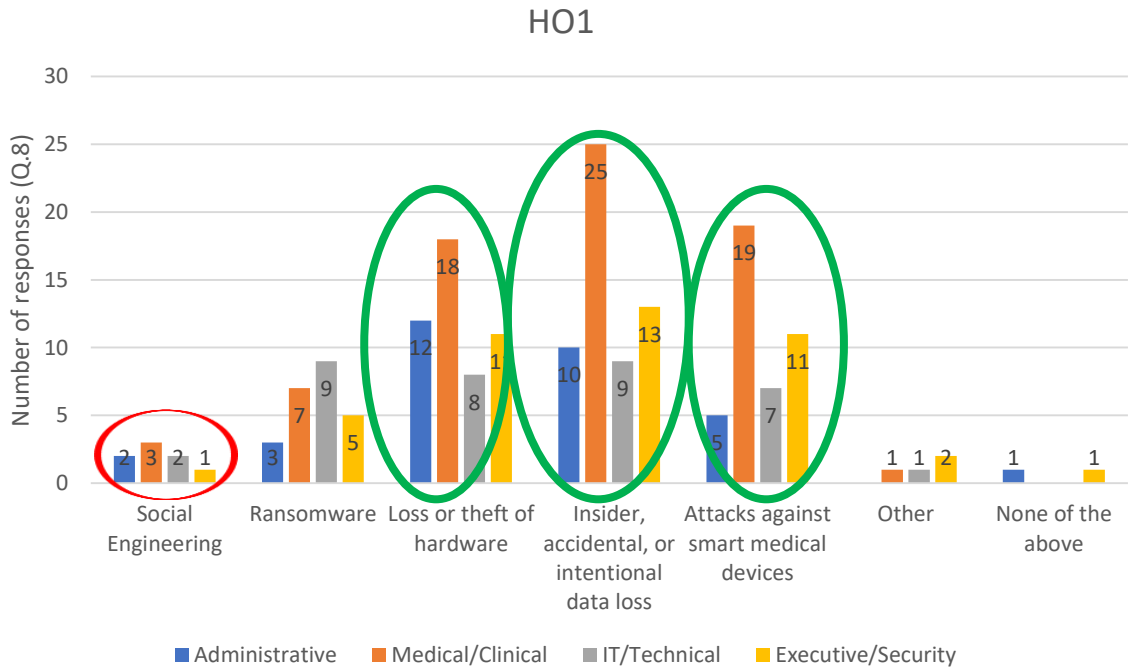
- Lowest Risk: “IT/Technical” employee groups at HO1
- High risks for all employee groups for all HOs
  - Risk Strategy: “Reduction”
  - Recommended controls: Awareness (C3, C4, C5) and Motivation (C17)
  - Implementation levels: Quarterly or monthly | Intermediate

Survey Findings: D3 – Specific Risk Category



- Highest Risk: "Administrative" and "Medical/Clinical" employee groups at HO1 and HO2
  - Risk Strategy: "Reduction"
  - Recommended controls: Training (C11), Awareness (C3, C5, C12) and Motivation (C17)
  - Implementation levels: Quarterly or monthly | Intermediate | Administrative and Medical/Clinical at HO1 and HO2

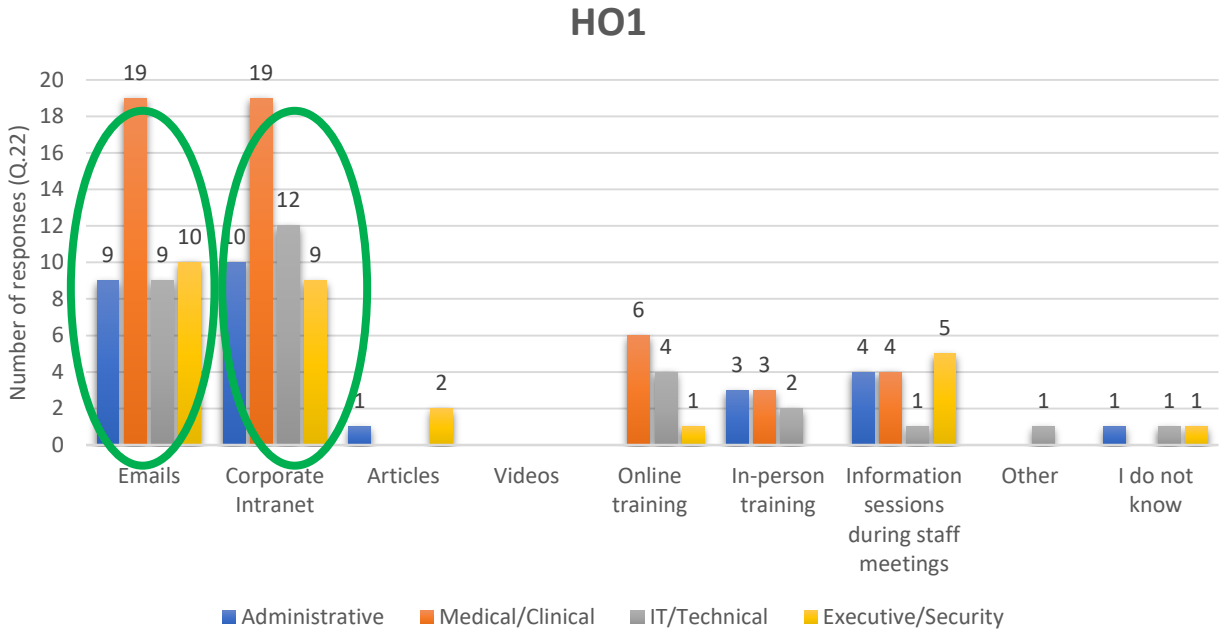
Survey Findings: D4 – Specific Question @ HO1



Q.8: Which of the following cybersecurity and data privacy threats are you aware of?

- Threat category: "Insider, accidental, or intentional data loss" (most popular)
  - Total number of responses: 57/71 (80.3%)
- Threat category: "Loss or theft of hardware"
  - Total number of responses: 49/71 (69%)
- Threat category: "Attacks against smart medical devices"
  - Total number of responses: 42/71 (59.1%)

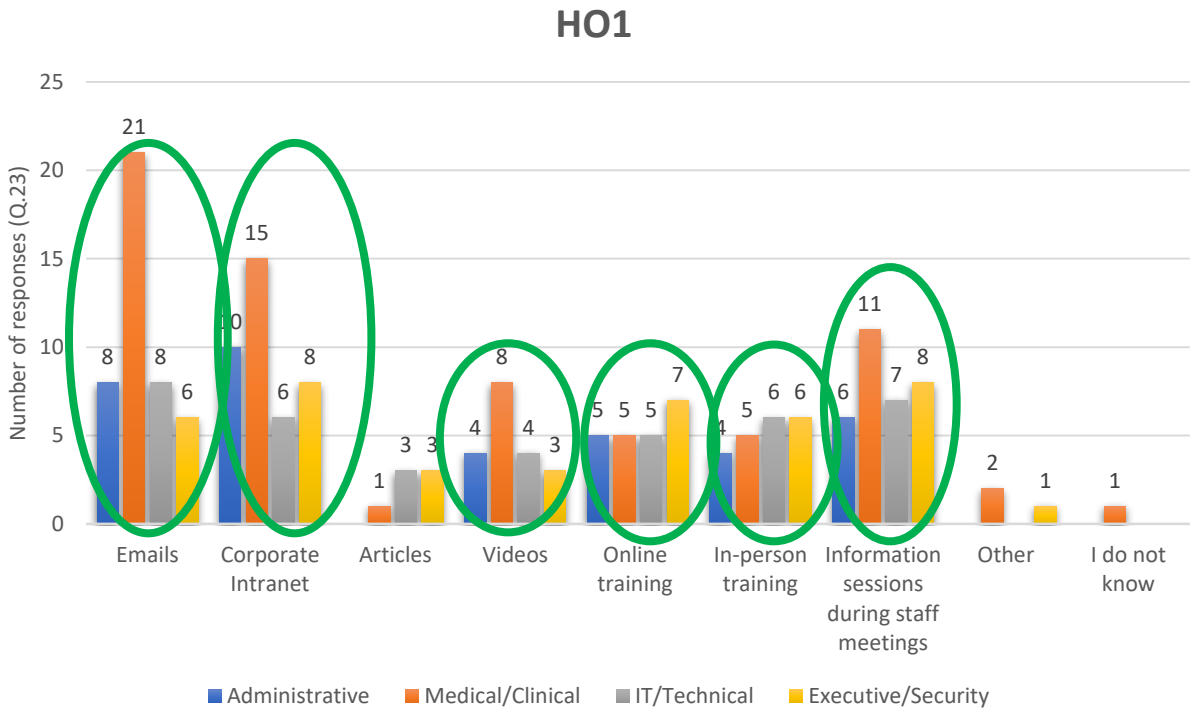
Survey Findings: D4– Specific Question @ HO1



Q.22: Which communication channels are currently used in your organisation to raise awareness on cybersecurity and data privacy?

- Communication channel: “Emails”
  - Total number of responses: 47/71 (66.2%)
- Communication channel: “Corporate Intranet”
  - Total number of responses: 50/71 (70%)

Survey Findings: D4 – Specific Question @HO1



Q.23: Which communication channels would you prefer to learn about cybersecurity and data privacy in your organisation?

- Preferred communication channels:
  - "Emails", "Corporate Intranet", "Information sessions during staff meetings"
- Other preferred communication channels:
  - "Videos", "Online training", "In-person training"

Summary of the Findings

- Administrative and Medical/Clinical employees at HO3 have less high risks compared to HO1 and HO2 → Employees at HO3 seem to have a better understanding of cyber hygiene
- Administrative and Medical/Clinical employees at HO1 and HO2, have medium-high risks in most categories → Need to adopt the recommended controls to raise awareness
- In general, for all employee groups in the three HOs
  - Lowest risk (medium): "Cyber Hygiene", "Data Privacy/ Protection Training" and "Data Privacy/Protection Awareness" Highest risk (medium-high): "Communication channels" and "Secure connection and use of devices"
- Awareness of threats among all employee groups in the three HOs
  - Aware of the threats "Insider, accidental or intentional data loss", "Loss or theft of hardware" and "Attacks against smart medical devices"
  - Not aware of "social engineering attacks", while only employees at HO3 are aware of "ransomware"
- Existing vs Preferred communication channels
  - At HO1 and HO2 "Email" and "Corporate Intranet" are mostly used. At HO3 "Email", "Online Training" and "Information sessions during staff meetings" are mostly used
  - Apart from "Email", all employees prefer to use "Information sessions during staff meetings", "Videos", "Online Training" and "In-person training" → HO1 and HO2 need to introduce or better promote these channels

CUREX
SECURE AND PRIVATE HEALTH DATA EXCHANGE

Thank you!

Elina Argyridou

Research Associate

KIOS Center of Excellence,

University of Cyprus

argyridou.elina@ucy.ac.cy

Christos Laoudias

Research Lecturer

KIOS Center of Excellence,

University of Cyprus

laoudias@ucy.ac.cy

This project has been funded by the European Union's Research and Innovation Program "Horizon 2020" under grant agreement No 826404