Project Title

"Strategies and practices against internal cyber threats in Greek businesses"

TABLE OF CONTENTS

01 Significance

02 Aim / Objectives

03 Key Literature

04 Methodology

05 Limitations / Risks

06 Gantt Chart

01 Significance

Malicious Insider

316 days to identify

4,61 million US $
per incident

20% - 40% of electronic
crime attributed to
internal actors

30% more damage than the
external

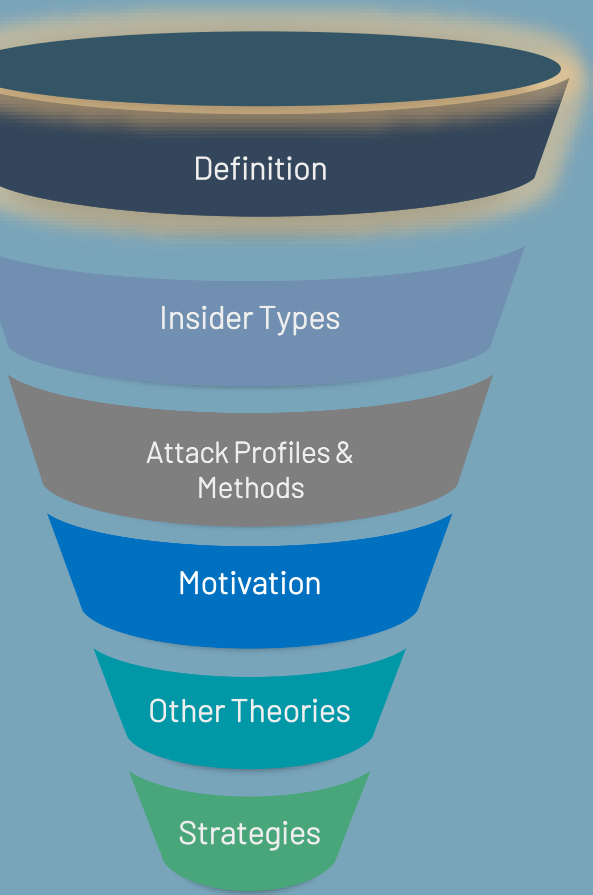
What is the current status of Greek companies regarding cybersecurity controls, and how do they perceive the challenge compared to the literature?

02
Aim / Objectives

Gather data from the industry / recognise similarities and differences / find common ground & compare with literature / enhance the Greek businesses awareness

- Extended literature research
- Get the most from the experts' standpoint
- Examine both technical and non-technical approaches
- Invite more views for debate
- Compare with the literature & conclude
- Maintain the timeline as scheduled

03
Key Literature

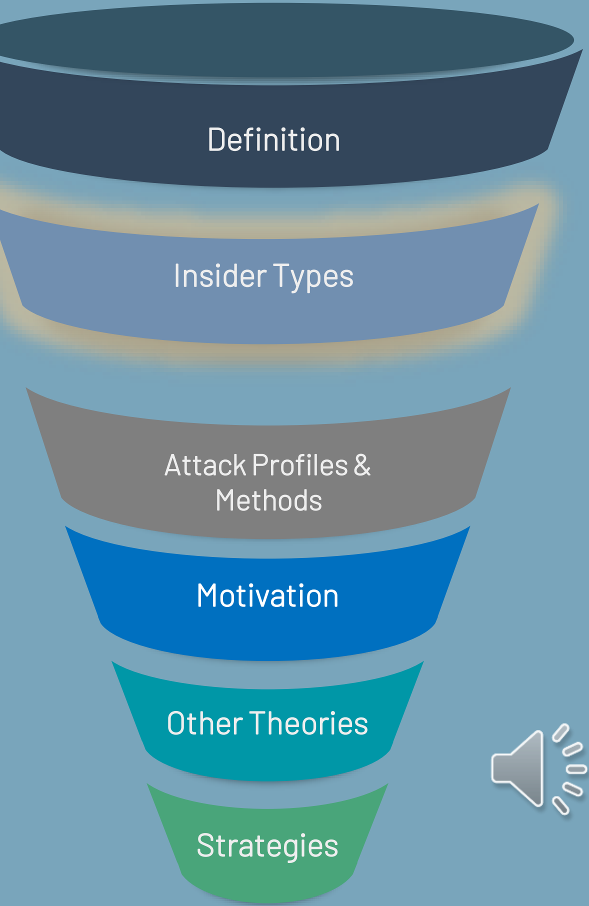


An insider is a person who has or used to have authorised access to one or more assets of an organisation and uses that access purposefully or unintentionally to harm the organisation.

(CERT, 2018)

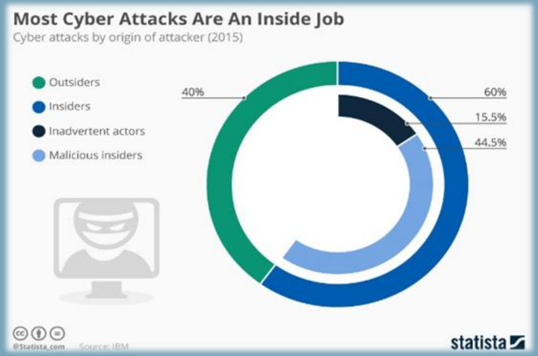
- An ex-employee
- A third party vendor
- Company’s janitor
- A disgruntled employee
- An unaware use

03
Key Literature



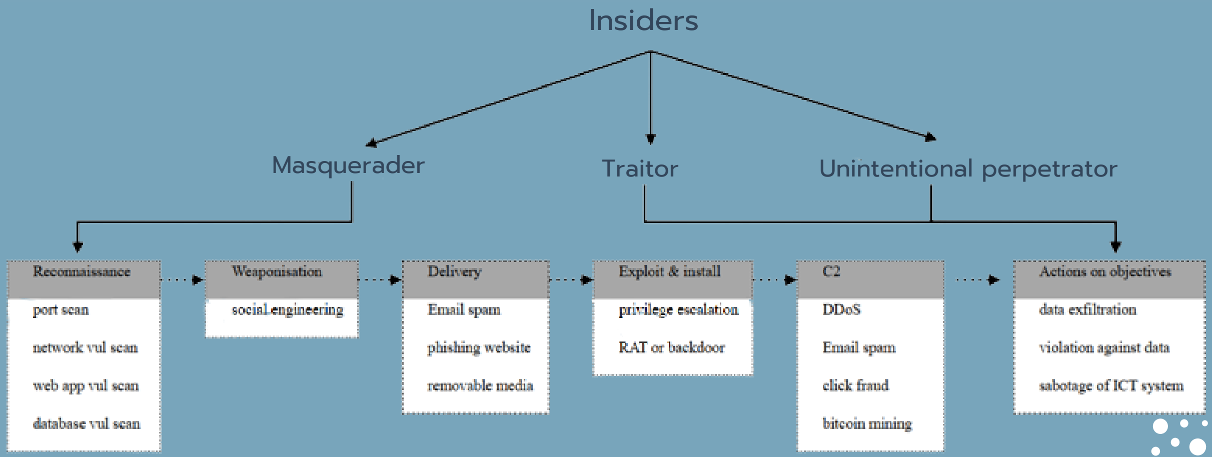
Intentional or Malicious type

Unintentional type


Most Cyber Attacks Are An Inside Job

Cyber attacks by origin of attacker (2015)

@Statista.com Source: IBM


Insiders

Masquerader

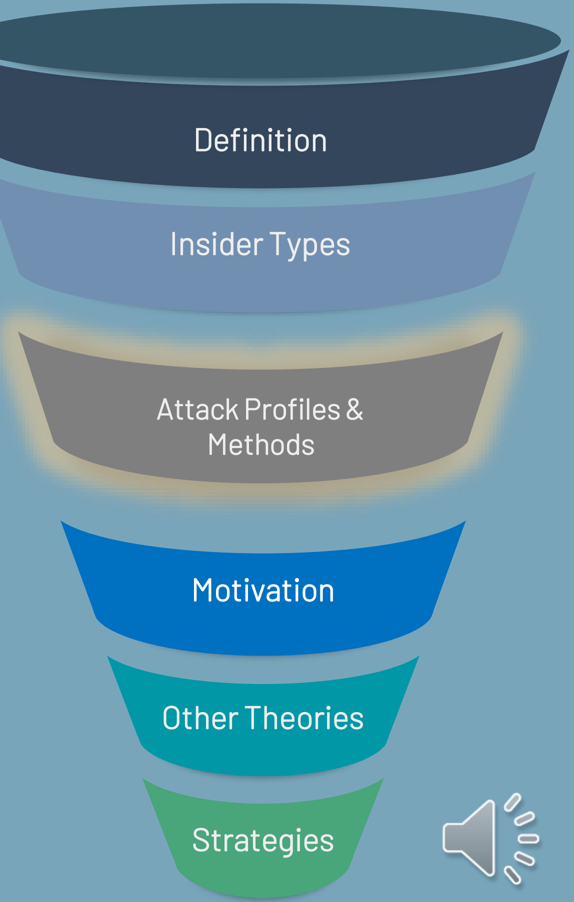
Traitor

Unintentional perpetrator

Reconnaissance	Weaponisation	Delivery	Exploit & install	C2	Actions on objectives
port scan	social engineering	Email spam	privilege escalation	DDoS	data exfiltration
network vul scan		phishing website	RAT or backdoor	Email spam	violation against data
web app vul scan		removable media		click fraud	sabotage of ICT system
database vul scan				bitcoin mining	

(Liu et al., 2018)

03
Key Literature



Definition

Insider Types

Attack Profiles & Methods

Motivation

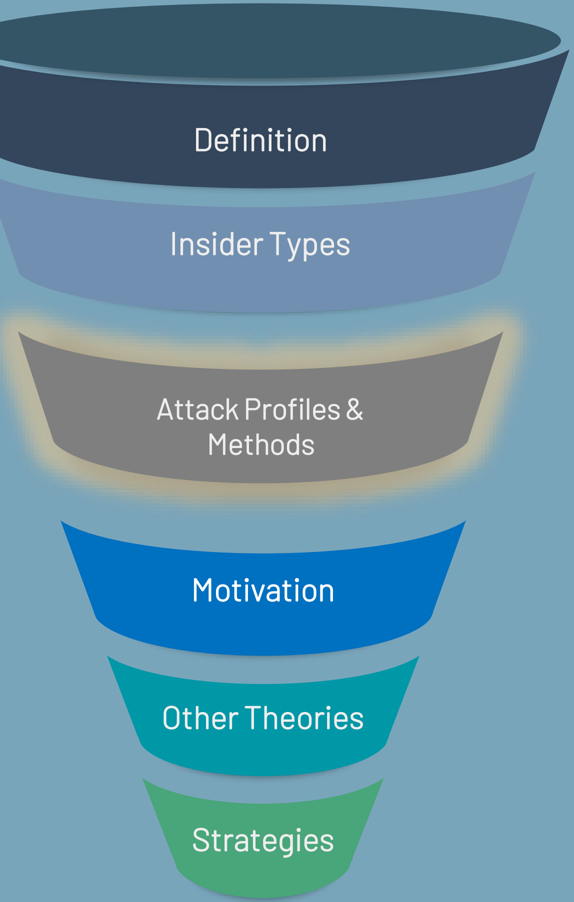
Other Theories

Strategies

- Low-intensity & slow-moving attack succeeded to avoid detection and do more damage.
- In most cases, a lack of technical expertise was not an issue
- The financial impact of managerial roles was shown to be greater than that of lower-level positions.
- Most events discovered during an audit, clients' complaints or coworkers' suspicions
- Due of its perceived safety, scammers frequently sought for information that may be used to identify individuals.

Cummings et al. (2012)

03
Key Literature



Definition

Insider Types

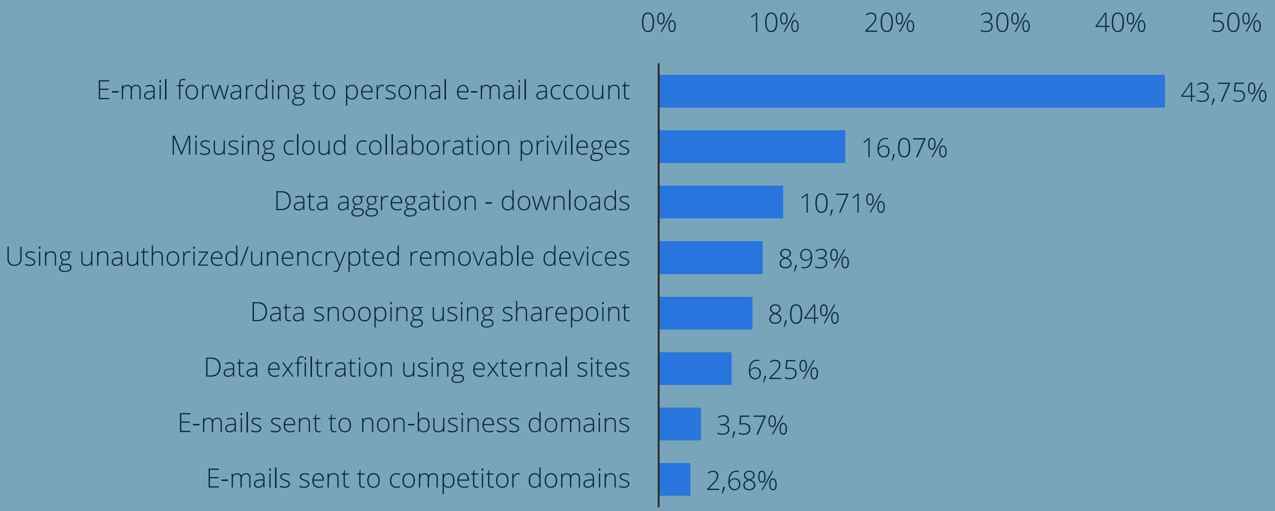
Attack Profiles & Methods

Motivation

Other Theories

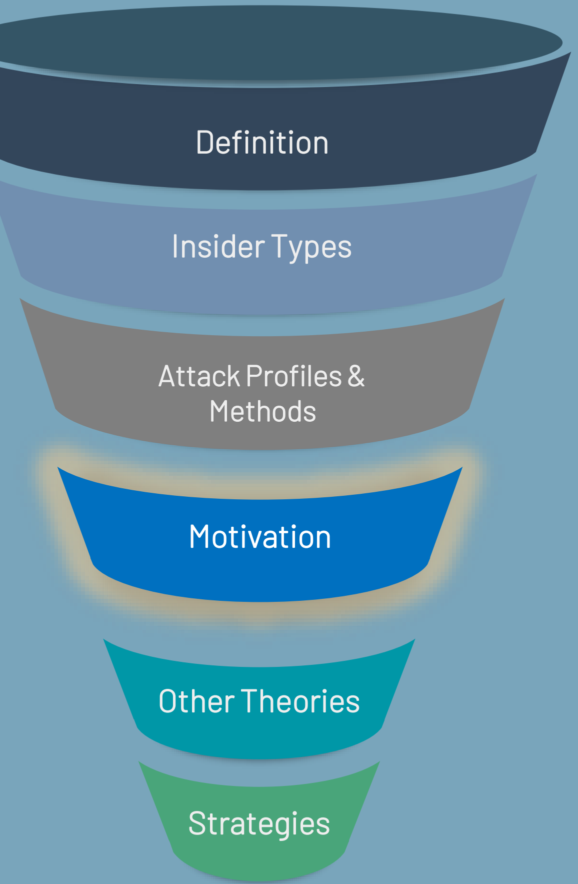
Strategies

Most common data exfiltration behaviors during insider threats in the United States in 2020



Note(s): United States; 2020; 300 incidents; across 8 different industry verticals
Further information regarding this statistic can be found on page 8.
Source(s): Securonix; ID 1155846

03
Key Literature



- Financial
- Political beliefs
- Personal

(Cole & Ring, 2006)

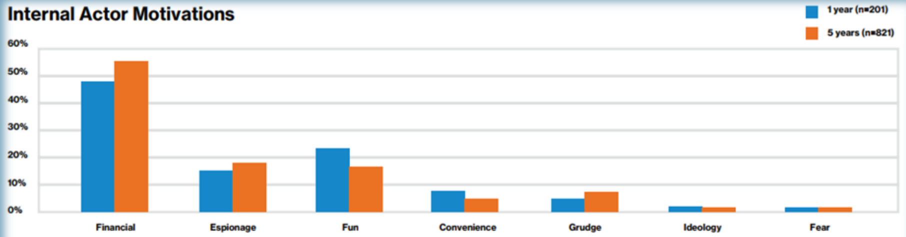
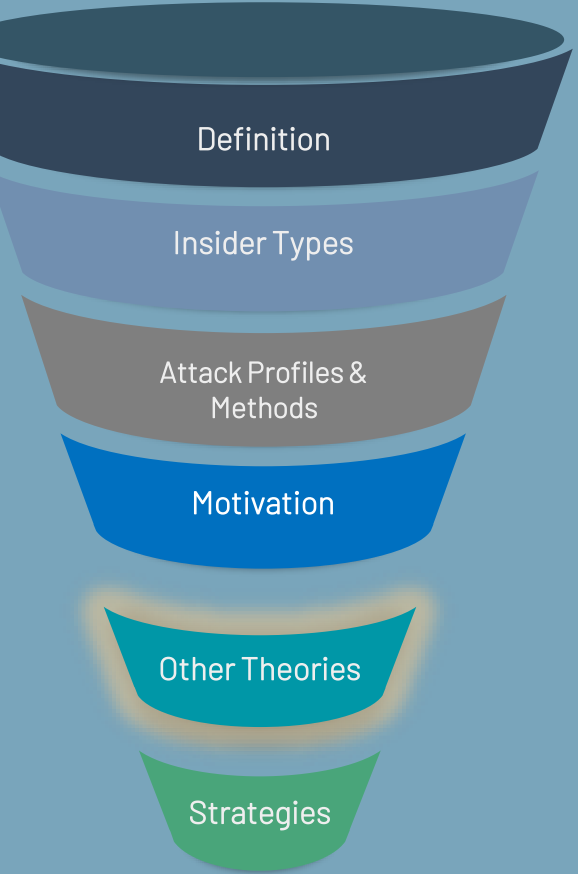


Figure 7.
Internal Actor Motivations within Insider Privilege and Misuse Breaches

(Verizon, 2021)

03
Key Literature



- Deliberate markers
- Meaningful errors
- Preparatory behaviour
- Correlated usage patterns
- Verbal behaviour
- Personality traits

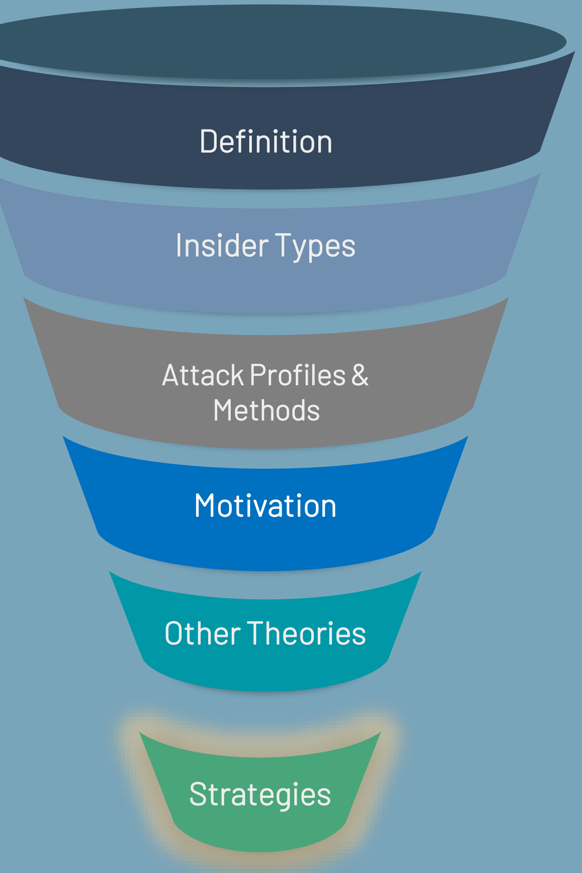
→ (Schultz, 2002)

Dark Triad Personality theory

MOC theory (motivation, opportunity, capability)

Theory of Planned Behaviour (TPB)

03
Key Literature



Definition

Insider Types

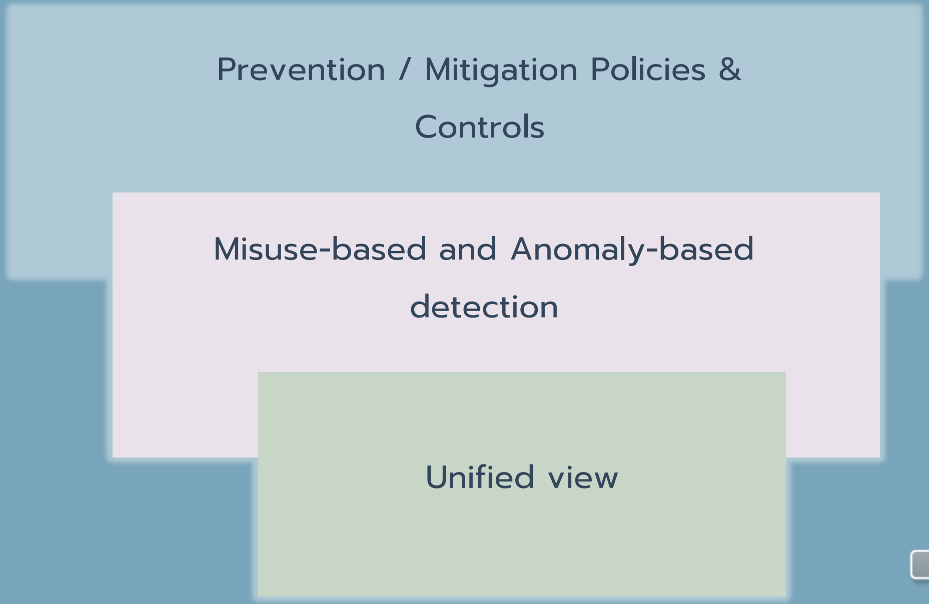
Attack Profiles & Methods

Motivation

Other Theories

Strategies

Access Control, Anti-Virus, Firewalls, IDS, IPS, SIEM Honeypots etc.



Prevention / Mitigation Policies & Controls

Misuse-based and Anomaly-based detection

Unified view

(Homoliak et al., 2019)

04

Methodology

PHASE 1

Form the Meeting Questions /
Candidate recruitment
Online meetings

PHASE 2

1st Phase data evaluation &
questionnaire design

PHASE 3

2nd Phase Questionnaire
responds and analysis

PHASE 4

Conclusion & Report

05

Limitations / Risks

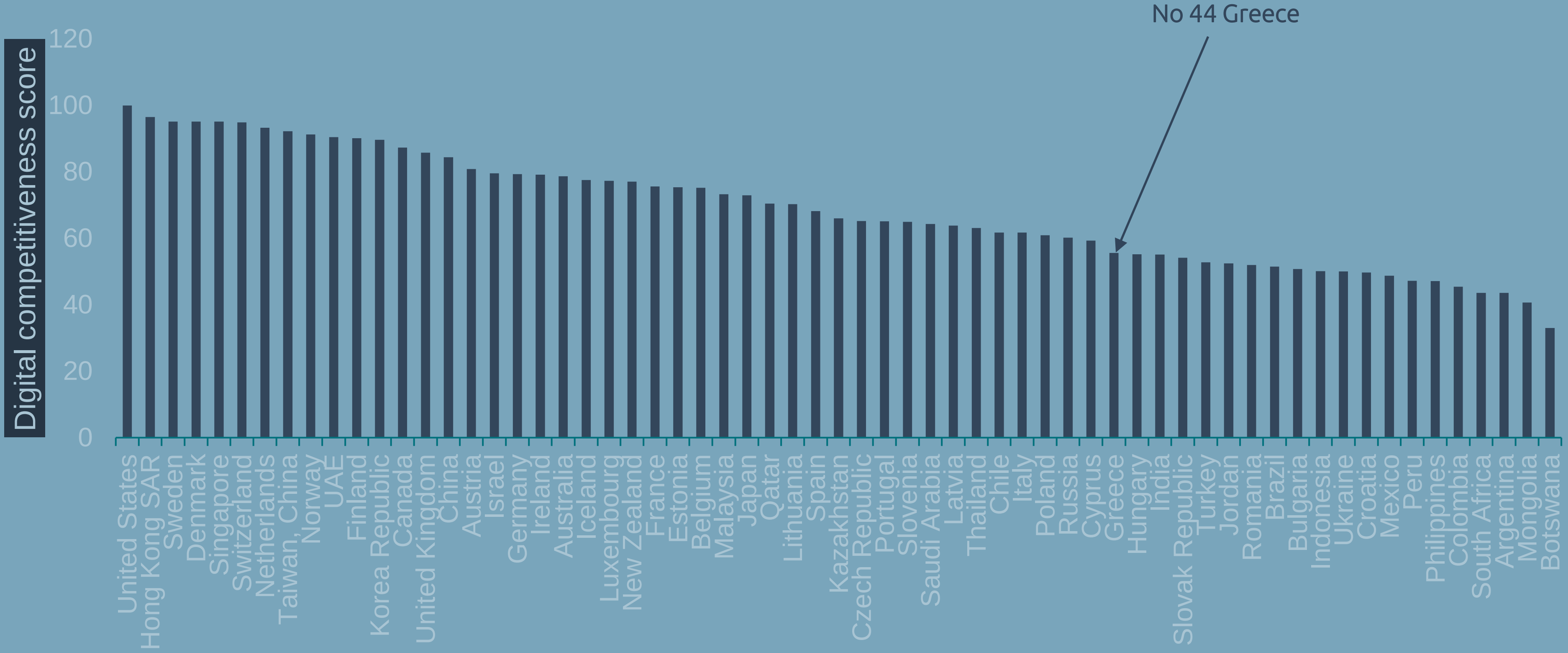
- Small group of experts
- Bias expected from the experts’ industry & experience
- Not all questions are expected to be answered – Additional candidates to minimise the problem
- Greece has low digital transformation index
- Trust issues / non-disclosure issues – Lack of depth

Ethics

- All participants will be adults
- Anonymity for the participants
- Confidentiality of the questions / Consent for Record
- Encrypted data
- Only one expert / company

Country-level digital competitiveness rankings worldwide as of 2021

Digital competitiveness rankings by country worldwide 2021


No 44 Greece

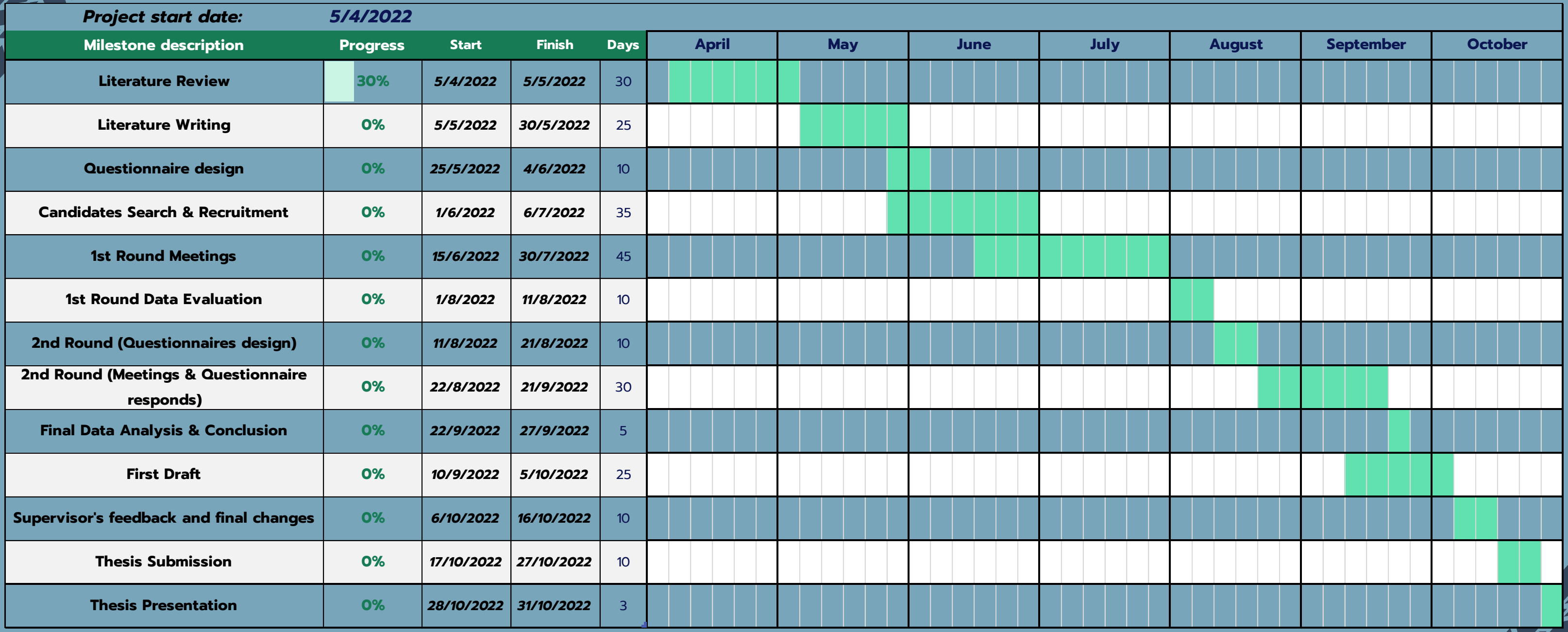
Note(s): Worldwide; 2021

Further information regarding this statistic can be found on page 8.

Source(s): International Institute for Management Development; ID 1042743

06

Gantt Chart



Project start date: ***5/4/2022***

Milestone description	Progress	Start	Finish	Days
Literature Review	30%	*5/4/2022*	*5/5/2022*	30
Literature Writing	0%	*5/5/2022*	*30/5/2022*	25
Questionnaire design	0%	*25/5/2022*	*4/6/2022*	10
Candidates Search & Recruitment	0%	*1/6/2022*	*6/7/2022*	35
1st Round Meetings	0%	*15/6/2022*	*30/7/2022*	45
1st Round Data Evaluation	0%	*1/8/2022*	*11/8/2022*	10
2nd Round (Questionnaires design)	0%	*11/8/2022*	*21/8/2022*	10
2nd Round (Meetings & Questionnaire responds)	0%	*22/8/2022*	*21/9/2022*	30
Final Data Analysis & Conclusion	0%	*22/9/2022*	*27/9/2022*	5
First Draft	0%	*10/9/2022*	*5/10/2022*	25
Supervisor's feedback and final changes	0%	*6/10/2022*	*16/10/2022*	10
Thesis Submission	0%	*17/10/2022*	*27/10/2022*	10
Thesis Presentation	0%	*28/10/2022*	*31/10/2022*	3

“ When there is no enemy within, the enemies outside cannot hurt you.”

Winston S. Churchill

Thank you

CREDITS: This presentation template was created by Slidesgo,
including icons by Flaticon, and infographics & images by Freepik.

REFERENCES

Alotibi, G., Clarke, N., Li, F. and Furnell, S. (2018) The Current Situation of Insider Threats Detection: An Investigative Review. *21st Saudi Computer Society National Computer Conference, NCC 2018*, (2015), pp.1–7. Available from: https://doi.org/10.1109/NCG.2018.8592986.

Azaria, A., Richardson, A., Kraus, S. & Subrahmanian, V.S. (2014) Behavioral analysis of insider threat: A survey and bootstrapped prediction in imbalanced data. *IEEE Transactions on Computational Social Systems*, 1(2), pp.135–155. Available from: https://doi.org/10.1109/TCSS.2014.2377811.

CERT Division (2013) Unintentional Insider Threats: A Foundational Study Available from: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=58744 [Accessed 26 March 2022].

CERT Division (2018) Common Sense Guide to Mitigating Insider Threats Available from: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=540644 [Accessed 1 April 2022].

Cole, E. & Ring, S. (2006) *Insider threat : protecting the enterprise from sabotage, spying, and theft*. Syngress.

Cummings, A., Lewellen, T., Mcintire, D., Moore, A.P. & Trzeciak, R., (2012) Insider threat study: Illicit cyber activity involving fraud in the u.s. financial services sector. *Special Report: CERT Program*, (July).

ENISA (2021) ENISA Threat Landscape 2021. Available from: https://doi.org/10.2824/324797 [Accessed 28 March 2022].

Greitzer F., Kangas L., Noonan C., Brown, C. & Ferryman, T. (2013) Psychosocial Modeling of Insider Threat Risk Based on Behavioral and Word Use Analysis. *e-Service Journal*, 9(1), p.106. Available from: https://doi.org/10.2979/eservicej.9.1.106.

Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y. & Ochoa, M. (2019) Insight into insiders and IT: A survey of insider threat taxonomies, analysis, modeling, and countermeasures. *ACM Computing Surveys*, 52(2). Available from: https://doi.org/10.1145/3303771.

Hunker, J. & Probst, C.W. (2011) Insiders and insider threats an overview of definitions and mitigation techniques. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 2(1), pp.4–27.

REFERENCES

IBM (2021) Cost of a Data Breach Report 2021. Available from: https://www.ibm.com/security/data-breach [Accessed 25 March 2022].

Liu, L., De Vel, O., Han, Q.L., Zhang, J. & Xiang, Y. (2018) Detecting and Preventing Cyber Insider Threats: A Survey. *IEEE Communications Surveys and Tutorials*, 20(2), pp.1397–1418. Available from: https://doi.org/10.1109/COMST.2018.2800740.

Maasberg, M., Warren, J. & Beebe, N.L. (2015) The dark side of the insider: Detecting the insider threat through examination of dark triad personality traits. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2015-March, pp.3518–3526. Available from: https://doi.org/10.1109/HICSS.2015.423.

Magklaras, G.B. and Furnell, S.M. (2002) Insider threat prediction tool: Evaluating the probability of IT misuse. *Computers and Security*, 21(1), pp.62–73. Available from: https://doi.org/10.1016/S0167-4048(02)00109-8.

Mhiqani, M.N. Al, Ahmad, R., Abidin, Z.Z., Yassin, W.M., Hassan, A., Mohammad, A.N. & Clarke, N.L. (2018) A new taxonomy of insider threats: an initial step in understanding authorised attack. *International Journal of Information Systems and Management*, 1(4), p.343. Available from: https://doi.org/10.1504/IJISAM.2018.094777.

Nurse, J.R.C., Buckley, O., Legg, P.A., Goldsmith, M., Creese, S., Wright, G.R.T. & Whitty, M. (2014) Understanding insider threat: A framework for characterising attacks. *Proceedings - IEEE Symposium on Security and Privacy*, 2014-January, pp.214–228. Available from: https://doi.org/10.1109/SPW.2014.38.

Salem, M.B., Hershkop, S. & Stolfo, S. (2008) A Survey of Insider Attack Detection Research. Available from: https://doi.org/10.1007/978-0-387-77322-3_5.

Schultz, E.E. (2002) Predicting insider attacks. *Computers & security*, 21(6), pp.526–531.

Verizon, (2021) Data Breach Investigation Report 2021. *Verizon DBIR*, pp.1–119. Available from: https://www.verizon.com/business/resources/reports/2021-data-breach-investigations-report.pdfx. [Accessed 26 March 2022].