Project Title

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

Introduction

This qualitative study aims to dive into the experience of cybersecurity professionals in Greece to identify the best practices and security measures for detecting and mitigating malicious or unintentional insider threat attacks. The following presentation serves as a visual aid for the Research module assignment and is divided into six sections according to the dissertation proposal paradigm:

1	Significance / Contribution to the discipline
2	Research Question / Aim / Objectives
3	Key literature
4	Methodology
5	Limitations / Risks
6	Timeline of proposed activities

1. Significance/Contribution to the discipline

Cybercrime has evolved into one of the most severe challenges modern businesses confront globally. Even though the threat landscape differs by region and industry, the frequency of breaches and the related costs continue to rise significantly, jeopardising organisations' profitability and viability. In most incidents, the human factor is instrumental in this worrying phenomenon and has been targeted as the initial attack vector.

Under IBM's data breach report for 2021, the average cost of a malicious insider breach was $4.61 million, making it the third most prevalent factor, with an average identification timeframe of 316 days.

In a similar vein, Enisa's Threat Landscape study (2021) outlines a concerning trend that exacerbates the situation by addressing collaboration or, even worse, recruitment of corporate staff by external actors, most notably in ransomware cases.

As stated in the CERT Insider Threat Center report (2018), 20% of electronic crime occurrences were thought or proven to be the result of internal actors. The same report found that 30% of respondents believed that insider attacks caused more damage than external ones and targeted primarily customer and employee sensitive data.

Notwithstanding, other sources indicate that the percentage of internal threats incidents is substantially higher, at 40%. (Azaria et al., 2014).

Considering these points and the incredible financial gain that cyber-attacks continue to generate, business leaders and information security professionals worldwide struggle to overcome the insider threat's conundrum through the use of technical and non-technical solutions.

2. Research Question

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

Aim

The project's primary purpose is to collect an efficient number of answers to identify similarities and discrepancies so as to come to a consensus on the best solutions against the internal threat, ultimately providing value and enhancing the cybersecurity posture of Greek businesses.

Objectives

- Conduct literature research for both technological and theoretical approaches to the insider threat.
- Explore the subject from the experts' perspective
- Find the most effective technical and non-technical means (i.e. security awareness training) from the industry experts' perspective
- Invite different opinions and set them for further debate
- Compare the results to those found in the literature
- Conclude and create a blend of commonly recognised security controls
- Compose the final report

3. Key literature related to the project

Definition

According to the CERT National Insider Threat Center (2018), 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.

Hunker and Probst (2011) attribute the difficulty to a commonly accepted internal threat definition in two factors. The extensive networking environment of modern organisations and the dynamic employment factors such as outsourcing contractors or external partners make it difficult to draw a boundary between internal and external threats in most cases. Therefore, an insider could be, for example, an ex-employee with credentials that are still valid, a third-party administrator or a janitor with physical access.

Insider types

The two main categories found in the literature regarding the insider threat rely on the perpetrator's intention. The unintentional insider is the one whose harmful behaviour is ascribed to a lack of security awareness or negligence, contrary to the malicious insider, whose incentives are financial or related to personal psychological traits. (Nurse et al., 2014)

For the unintentional insider, CERT (2013) has identified four types connected to the nature of the threat inducted into the organisation. Accidental data disclosure of sensitive information, malicious code installation as a consequence of social engineering, inappropriate document disposal or loss and portable device loss or theft complete the disparate unintentional types.

Identifying the difference between the intentional and inadvertent insider is a challenging task, and the literature, in many cases, concentrates on alternative characteristics and aspects to classify the insider. For instance, Magklaras and Furnell (2002) distinguish the two main types considering the reason behind Information Technology misuse, whereas Liu et al. (2018) correlate Salem et al. (2008) traitor and masquerader classes, as well as the unintentional type with the APT Kill Chain and its associated threats.

Homoliak et al. (2019) demonstrate a variety of insider classifications collected from previous studies and surveys in their report before systematically mapping the literature taxonomies based on the 5W1H questions (Why, What, When, Where, Who & How).

Attack Profiles and Methods

Insider attacks like those carried out by external actors can include a variety of methods and techniques. The insider's approach includes exploiting technological and physical vulnerabilities and/or abusing/evading regulations and procedures. Malware installation, information exchange, identity spoofing and every other method observed in external actors are also included in the arsenal of the insider (Mhiqani et al., 2018).

Cummings et al. (2012) highlight several noteworthy profile aspects of the insider methodology in their financial sector report:

- Criminals who used low intense and slow-strategy attacks caused more damage and evaded discovery for a more extended period.
- The majority of attacks did not demand technical skills (71% of the incidents had used non-technical means to circumvent the authorisation access)
- Managerial positions were found to have a higher financial impact than the lower-level positions
- The vast majority of instances did not involve collaboration (only 16% of the incidents were found to be cooperative)
- Most events were discovered during an audit or because of consumer complaints and coworker suspicions.
- Individually identifiable information was a frequent target of fraudsters, given that it constitutes a safer choice than other tangible benefits.

Insider Motivation

According to Cole and Ring (2006), there are plenty of factors that may contribute to the motivation of an insider to engage in criminal activity; however, there are three primary motivations that prevail.

Financial: When organisations recruit people to carry out inside assaults, they may deliberately target those who are experiencing financial difficulties or want higher income, which might also be considered a self-contained motivation.

Political beliefs: People are also driven by their political convictions. When these opinions conflict with their employer's, they may provide a compelling reason to undermine the organisation or join with hostile outsiders to the same end.

Personal: This is a two facet factor and entails some form of blackmail. Either the outsider looks into the victim's background in search of essential secrets to use against him, or she tries to set a trapping scenario that will create a new secret to take the employee under her control.

Verizon's Insider threat report (2021) also presents financial incentives as the primary drive for the insider, followed by espionage, fun, convenience, grudge, ideology and fear.

Behavioural – Psychological – Sociological Theories

Numerous research has been conducted to detect and prevent insider threats using behavioural, sociological, and psychological theories.

Schultz (2002) recommends six behavioural indicators that, when quantified using his developed equation, can provide considerable evidence of insider involvement.

Deliberate markers: Occasionally, attackers leave markings on purpose to make a statement. Identifying minor, less evident indicators before the attack occurs could be a pivotal factor in the investigation process for insider attacks.

Meaningful errors: Given that attackers frequently make errors when planning and conducting attacks, investigators can infer the offender's intent and identity by studying the log files and command history.

Preparatory behaviour: elements a person may utilise like system-level commands to probe a device or network before performing the attack.

Correlated usage patterns: similar to the previous category but examined more collectively as a pattern

Verbal behaviour: Verbal indicators that express contempt towards a supervisor or business.

Personality traits such as introversion are believed to be associated with an individual's chance of presenting an insider threat.

Personality characteristics have also been the main focus of another psychosocial study. Greitzer et al. (2013) used indicators as variables in their Bayesian network study, including disgruntlement, disregard for authority, stress, performance and anger management issues, among others, to conclude that system monitoring combined with psychosocial/behavioural indicators could be a helpful solution against the internal perpetrators.

In the same fashion, Maasberg et al.(2015) highlighted ten propositions against the insider threat based on the Dark Triad Personality theory and other precedent behavioural theories like the MOC (motivation, opportunity, capability) and the Theory of Planned Behaviour (TPB).

Prevention and Detection Strategies

Access Control, Anti-Virus, Firewalls, Intrusion Prevention Systems, Security Information and Event Management (SIEM) and Honeypots are just a few of the security solutions available to assist businesses in controlling and mitigating data abuse and system risks. Despite their importance, internal attacks require a more diverse response. The enemy is assumed to be an external variable in the castle-and-moat model, which does not apply to internal actors.

According to Homoliak et al. (2019), a well-designed and robust insider threat protection program should leverage a variety of independent solutions. Mitigation and preventive policies and practices should be the first line of defence, followed by misuse-based and anomaly-based detection. Finally, a dedicated and unified view is required to maximise the integrated implementation's effectiveness.

Alotibi et al.'s (2018) research bolsters the previous point of view by emphasising the heavy IP reliance on most security systems for monitoring and detecting threats as well as the high resource consumption. Additionally, encryption usage may serve as an additional detection constraint, allowing for detection evasion. Hence, the authors argue that a user-behavioural profile method based on user engagement with various applications combined with the network analysis tools may be a more efficient strategy.

4. Methodology/Development strategy/Research Design

The research will be conducted using interviews (mainly conducted online) and questionnaires sent by mail. It will be divided into two rounds, with each round having a distinct objective. The first round of interviews will focus on respondents' perceptions of the most effective security controls and their shortcomings. Similarly, inadequate controls should be questioned, while some open questions in the concluding section of the first round will invite additional subjects or problems for debate.

The initial interview material collection and analysis step will involve technologies such as Otter.ai or another relevant speech-to-text software to generate texts suitable for the NVivo application. NVivo is a popular qualitative data analysis tool that will be used to organise the interviews' material. Before moving on to the second round, the most significant points and themes should have been identified and organised.

The second round of research will use the previous round's data and critical security controls to conduct a poll via questionnaires to examine convergence and divergence factors, aiming to achieve the broadest possible consensus on the most critical controls for insider threat prevention and detection.

In the final part of the research, the rated list of technical and non-technical controls will be compared with those found in the literature.

Experts recruitment / Requirements

Linkedin will be the initial site used to search for Information Security subject matter experts. Candidates should have at least five years of industry experience and have dealt with insider threats, or their roles should involve this responsibility. "Cybersecurity consultant," "Information security analyst," and "Information security manager/director/architect" are all possible search phrases. This study will allow only one participant per company to avoid conflicts of interest.

If the appropriate expert's number has not been reached, additional resources may be used until the appropriate sample has been collected. Professional chambers, human resource companies and peer recommendations will also be included.

A brief email will be sent to the selected individuals outlining the objective of the survey and the process that will follow if they accept to participate. The final number of participants should be thirty and preferably represent a cross-section of business industries.

5. Limitations / Risks expected:

- As with most qualitative research, the results will be affected by the views of a small group of experts derived from Greek businesses.
- Insider threat is a relatively debatable topic and has diverse implications in different businesses. Therefore, the experts' responses should not be perceived as exhausting, even if they will be studied collectively.
- Bias is expected to be established from the cybersecurity managers' expertise and relevant experience. In order to decrease this risk, the survey's interviewees will be chosen from different industries in Greece to form a more diverse sample.
- Not all potential participants will be willing to take place or answer all the questions. Additional participants could mitigate the risk.
- Greece has a lower digital transformation index, and the experts' pool is anticipated to be confined compared to other more tech-savvy countries (source).
- Some participants may hesitate to disclose confidential information about their organisations. As a result, some components may be lacking in depth.

Ethical considerations

The project will ensure confidentiality and anonymity given the survey's inherent sensitivity and the critical nature of the data.

- Given the study's criteria, all volunteers are assumed to be adults; hence, no additional measures will be taken.
- Anonymity: Each respondent will be assigned a unique numerical identification, and his/her identity will be concealed throughout the study.
- Confidentiality should be assured throughout interviews, and an additional agreement will be provided for the recorded sessions.
- Encryption will be used to protect all documents. No data will be stored in plain text at any stage of the procedure.

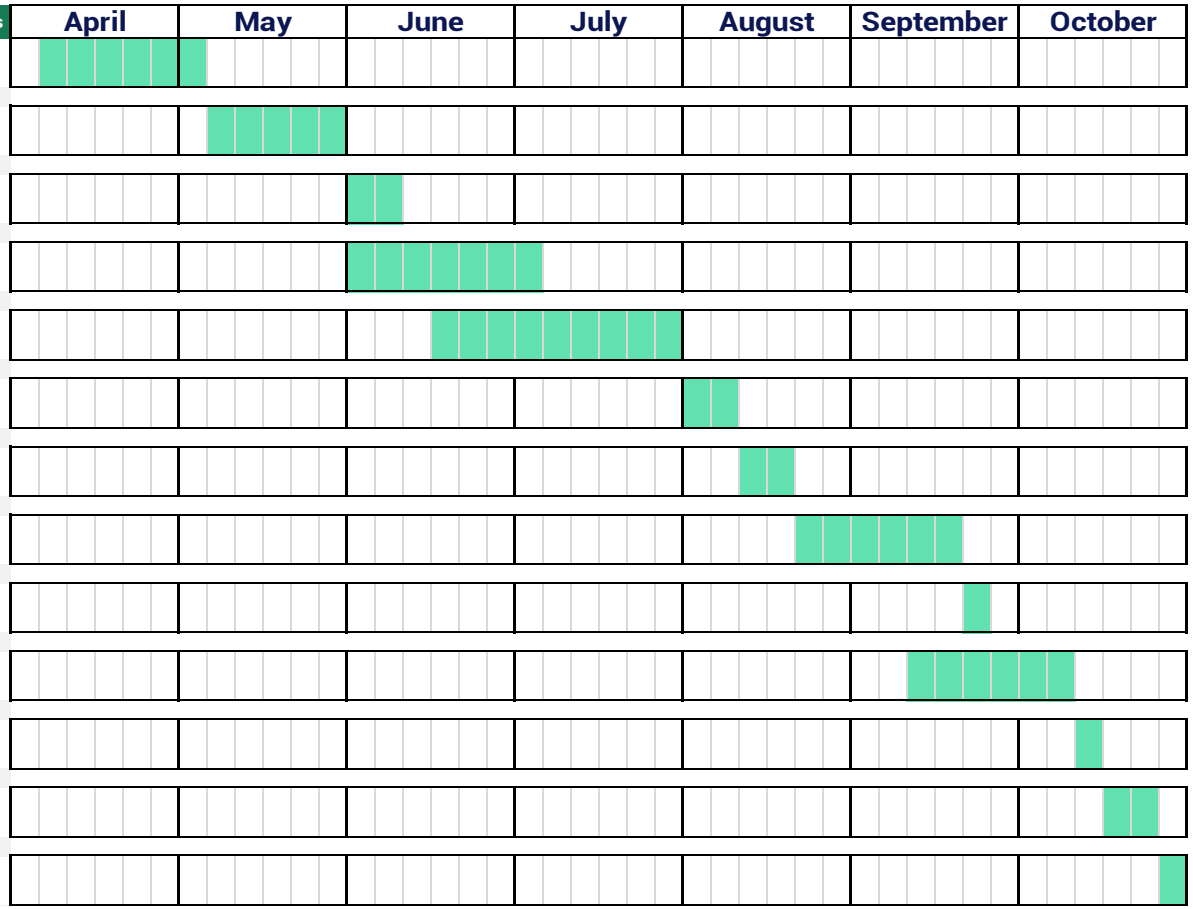
6. Timeline of proposed activities

Essex University stipulates a seven-month dissertation period, which is also considered in this project. Hence, the research will begin in early April and conclude by the end of October.

Spiros Anagnostopoulos

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	20/5/2022	15
Questionnaire design	0%	1/6/2022	11/6/2022	10
Candidates Search & Solicitation	0%	1/6/2022	6/7/2022	35
1st Round Meetings & Questionnaire sending	0%	15/6/2022	30/7/2022	45
1st Round Data Evaluation	0%	1/8/2022	11/8/2022	10
Questionnaire 2nd Round design	0%	11/8/2022	21/8/2022	10
2nd Round Meetings & Questionnaire sending	0%	22/8/2022	21/9/2022	30
Final Data Analysis & Conclusion	0%	22/9/2022	27/9/2022	5
First Draft	0%	2/10/2022	1/11/2022	30
Supervisor's feedback and final changes	0%	12/10/2022	17/10/2022	5
Thesis Submission		17/10/2022	24/10/2022	7
Thesis Presentation		25/10/2022	31/10/2022	6



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.

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].