NICHO, M. and MCDERMOTT, C.D. 2019. Dimensions of 'socio' vulnerabilities of advanced persistent threats. In Begušić, D., Rožić, N., Radić, J. and Šarić, M. (eds.) Proceedings of the 27th International software, telecommunications and computer networks conference 2019 (SoftCOM 2019), 19-21 September 2019, Split, Croatia. Piscataway: IEEE [online], article ID 8903788. Available from: https://doi.org/10.23919/SOFTCOM.2019.8903788

Dimensions of 'socio' vulnerabilities of advanced persistent threats.

NICHO, M. and MCDERMOTT, C.D.

2019

Dimensions of 'Socio' Vulnerabilities of Advanced Persistent Threats

Mathew Nicho
College of Technology Innovation
Zayed University
Dubai, United Ara Emirates
mathew.nicho@zu.ac.ae

Christopher D. McDermott
School of Computing and Digital Media
Robert Gordon University
Aberdeen, United Kingdom
c.d.mcdermott@rgu.ac.uk

***Abstract*—Advanced Persistent Threats (APT) are highly targeted and sophisticated multi-stage attacks, utilizing zero day or near zero-day malware. Directed at internetworked computer users in the workplace, their growth and prevalence can be attributed to both socio (human) and technical (system weaknesses and inadequate cyber defenses) vulnerabilities. While many APT attacks incorporate a blend of socio-technical vulnerabilities, academic research and reported incidents largely depict the user as the prominent contributing factor that can weaken the layers of technical security in an organization. In this paper, our objective is to explore multiple dimensions of socio factors (non-technical vulnerabilities) that contribute to the success of APT attacks in organizations. Expert interviews were conducted with senior managers, working in government and private organizations in the United Arab Emirates (UAE) over a period of four years (2014 to 2017). Contrary to common belief that socio factors derive predominately from user behavior, our study revealed two new dimensions of socio vulnerabilities, namely the role of organizational management, and environmental factors which also contribute to the success of APT attacks. We show that the three dimensions postulated in this study can assist Managers and IT personnel in organizations to implement an appropriate mix of socio-technical countermeasures for APT threats.**

***Index Terms*—advanced persistent threats (APT), spear-phishing, user vulnerabilities**

I. Introduction

APT remains a formidable threat due to the integration of 'Socio' (non- technical) and technical threat vectors used for reconnaissance, exploration, access, system exploitation, and data exfiltration from systems. In this respect, APT is characterized through the use of zero-day or near zero-day malware. Multiple threat agents and advanced cyber techniques are deployed to gain entry, escalate privileges, move stealthily, target servers containing sensitive data, and undertake data exfiltration, whilst remaining undetected over long periods of time. APT threats by nature are stealthy, targeted and data focused [1]. Detection is challenging using traditional defense methodologies [2] as they tend to stay inside the network or repeat intrusions multiple times, until they are able to accomplish their goals [3]. As highly complex, sophisticated and well-resourced threats, they are often aimed towards the government sector [4] [5]. The goal of an APT attack is not just to gather a target entitys data, but to accomplish it undetected [6].

APTs often rely on social engineering attack vectors namely spear-phishing and water-holing [7] [8]. In this respect, the human factor is a critical element in an organizational computer system, as it is a vulnerable link; the only factor that exercises initiative, and the factor that transcends all the other elements of the entire system [9]. Consequently, end users in the workplace are said to be the weakest link in information systems security [10] [11]. Motivated by this problem we explore the dimensions of user related vulnerabilities (socio) that largely contribute to APT attacks. In this paper the term 'Socio' is used to refer to non-technical vulnerabilities of APT since the dimensions of 'Socio' are yet to be ascertained from an APT context.

The paper is structured as follows. Section II discusses multiple perspectives of APT threats and attacks, to understand their purpose and propagation. Section III explores existing literature in relation to the 'Socio' aspect. Section IV outlines the methodology used throughout the study. Section V presents findings, with discussion, in the light of innovative facts, presented in Section VI. Finally, conclusions, limitations and areas of further research, are presented in Section VII.

II. APT Perspectives

APT attacks are highly targeted attacks with clearly defined goals, which typically target governments or businesses, due to their substantial intellectual property value [12] [13]. While APT threats have drawn increased attention from the industrial security community, a comprehensive and clear understanding of the APT research problem is lacking [12]. The National Institute of Standards and Technology (NIST) described APTs as "an adversary who possesses sophisticated levels of expertise and significant resources, which allow it to create opportunities to achieve its objectives by using multiple attack vectors" [14]. APTs target large corporations and foreign governments, with the objective of stealing information or compromising information systems. APTs are not usually deployed to bring down a business, but to stay embedded within its systems and extract information at a slow and undetected pace [15]. As highly advanced networked entities, typical of organized groups, they conduct hostile cyber-attacks against connected computers; if on a local network or the internet [13]. Using stealth techniques, they aim to continuously monitor, admin-

istrate, and steal specific target data in the long term, while staying undetected [16]. Thus, advanced persistent threats: (i) pursue their objectives repeatedly over an extended period of time; (ii) adapt to defenders efforts to resist them; and (iii) maintain the level of interaction needed to execute their objectives [12]. In this respect APTs are considered one of the most vicious examples of a cyberthreat that are not easy to detect or prevent. As APTs launch attacks in multiple domains of the target information systems network, and in multiple stages, using packets that may not be malicious, it is extremely challenging for most current intrusion detection systems (IDS) to detect them [17].

A. APT Attack Methodology

APTs use multiple attack techniques and tactics that are executed with stealth and are targeted specifically to achieve a defined goal, most often espionage, remaining inside the network for a long time [8] [18]. Attacks are typically carried out via communication channels such as email or instant messaging by masquerading as legitimate and trustworthy entities [19]. APTs follow a very precise attack type because it employs indirect attacks on the terminals of the employees working for the target, as well as direct attacks. For this reason, it is very difficult to detect and handle an APT [20]. In contrast to typical security incidents, these domestic and overseas hacking attempts have occurred as a result of long-term and persistent attempts, not by individual hackers but by groups, for a special purpose of obtaining important information and data about governments or specific companies [20].

While the APT process goes through six distinct phases (reconnaissance, delivery, exploitation, operation, data collection, and exfiltration) when targeting data [21], they also traverse or target through one or more of the four planes ,namely the physical plane (P), user plane (U), network plane (N), application plane (A), or any other emerging planes [22]. Hence, APT require a holistic perspective.

III. 'Socio' VULNERABILITIES OF APT

Existing research has focused on generic intrusion detection, with little application to APTs [13]. Hence, APT is a serious issue for current detection methods because these methods depend on known signatures of attacks, while APTs make heavy use of unknown security holes for attacks [18]. The defensive tools, procedures and other controls commonly put in place to handle commodity security threats are often ineffective against targeted APT-style attacks [23]. This is due to the major role played by the human factor in the APT propagation chain that paves the way for its initial entry into the network.

Computer users being independent agents who make their own choices, represent one of the most persistent vulnerabilities in many computing systems [24]. Hence, phishers find it easier to exploit humans rather than breaking into a system directly [25]. While news headlines tend to highlight wide-scale attacks against large enterprises that hit millions of customers, it has been shown that most attacks actually target small and medium sized businesses, and often are much more costly to smaller targets [26]. APTs which rely heavily on spear phishing, find an easy path through human weaknesses. Spear phishing (a major threat vector of APT) involves a deceptive approach, whereby hackers acquire sensitive information from targeted victims by appearing to come from a trusted source [27]. In this respect, unintentional mistakes by users, due to poor cybersecurity skills, results in up to 95 per cent of cyber threats to organizations [28] Finally, the prevention and detection of APT continues to be a challenge, due to attackers constantly changing and evolving their advanced techniques and methods to remain undetected [29].

IV. Methodology

Nine respondents directly managing information security and governance in separate organizations, across multiple sectors of industry (financial, media, information technology services, government, aviation, and oil sector), were selected for interview. Respondents were selected using five criteria to ensure appropriate coverage of required topics. Criteria consisted of organizational size (>100 employees); relevant industry experience (ten years); relevant security and/or governance role within their IT department; industry-relevant certifications in the IS security domain (CISM, CISSP, ISO 27001); and experience implementing at least one relevant information security framework (ISO 27K, local ISMS, COBIT DS 5, ITIL).

Interviews were transcribed, validated through subsequent telephonic interviews, and imported to NVIVO 10 (qualitative analysis software). Analysis followed guidelines proposed by Whittaker [30], where (1) data (especially the interview data) was coded, (2) transcribed text was systematically examined to identify key concepts, (3) data was grouped into constructs and (4) searched for relationships between a category/factors and its concepts to view interrelationships.

V. Findings

This section includes the first two steps of Whittaker namely coding and identifying key concepts. In this respect 24 free nodes were identified (see Table 1). Prior to getting answers to the key research question, we elicited responses on the multiple perspectives of APT.

Respondents were unanimous in their assertion that 'zero day' attacks, inherent in APT threats, cannot be completely prevented. Regarding commercial APT detection and prevention solutions, respondents stated that "vendors may have APT solutions for a simple attack vector of an APT. However, they do not have a solution for every possible type of APT attack vector". The conclusion that "APT vectors can only be controlled to some extent, but not 100 percent", points to the role of humans, whose behaviour is unpredictable compared to systems. Word count suggested by Leech and Onwuegbuzie [31] was used as a measure of relative emphasis, to rank vulnerabilities being discussed by the respondents.

TABLE I
NON-TECHNICAL VULNERABILITIES MOSTLY ATTRIBUTED TO USERS

Non-Technical Vulnerabilities	Sources / Frequency	Coverage (words)
Management (9)		***2469***
Lack of knowledge on the relevance to IT security	3/3	640
Lack of knowledge on IT security	3/4	401
Risk management	2/2	333
Lack of resources	1/1	309
Audit focus	1/3	235
Lack of policies	1/3	182
Speed of delivery	1/1	150
Over confidence	1/1	141
Lack of monitoring	1/1	78
Employees (10)		***1402***
Employee mistakes	4/7	380
Lack of awareness of APT	2/5	257
Not reading communications	2/2	214
Unethical behavior	1/1	202
Low awareness of security among non-IT staff	3/3	172
Low motivation	3/4	96
Accessibility vs Security	1/1	30
Issues with training	1/1	21
Not reading security policies	1/1	20
Consumer preference	1/1	10
Environmental (5)		***253321***
Multiple attack vectors	2/2	273
Online profiles	1/1	143
Lack of inter-vendor communications	1/2	98
Low security research in MENA region	1/1	57
Regulatory vulnerabilities	1/1	51

VI. DISCUSSION

This section describes the final two steps outlined by Whittaker, namely grouping of nodes under inductive constructs and observation of relationships between constructs. Inductive coding (constant comparison analysis) was used to identify nineteen vulnerabilities, which were categorized into three inductive themes (factors) namely management, employees and environmental. Figure 1 illustrates the three dimensions based on their relative weights. Contrary to statements and assumptions in academic and practitioner fora regarding the emphasis of the user as a conduit for APT attacks, we find the overarching role of 'management' in APT attacks. In this respect, 'management' refers to the decision-making body in the upper middle and lower layers, with regard to information systems. Secondly, the role of environmental factors is a surprising finding in this study.

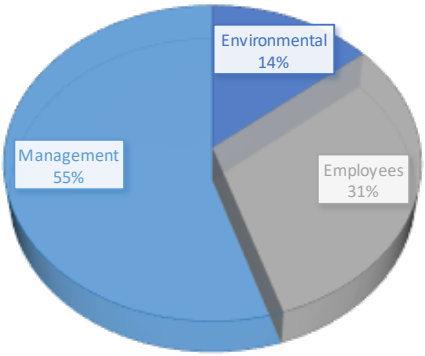

Fig. 1. Socio Vulnerability Dimensions of APT

A. Management

The role of management was discussed extensively by respondents, compared to the remaining two themes, with lack of knowledge particularly highlighted. Here, a lack of knowledge is considered from two perspectives. First, a lack of knowledge regarding the relevance of security by managers which has been termed "revenue centric". It was suggested that priority is given to satisfy the customer in terms of time and performance, resulting in security being compromised. Second, a lack of knowledge on IT security has been termed as "segmented security". Here, security is viewed as an isolated segment rather than a whole. In this respect IT personnel are comfortable and assured of security in their own compartment, but unware from a system perspective. This presents a serious vulnerability when APT traverse through the six phases and four planes (Section II-A).

A security plan starts with risk management and thus a "risk profile with a threat matrix" is relevant. Occasionally, managers cite a lack of resources in terms of money and appropriate IT staff. In this respect "people dont have enough resources to commit to security, because their focus is functionality. . . . So, the weakness I feel is, again, number one first give people resources, number two - find the right people, and number three - retain them." Analysis identified three issues within this factor. The first being to simply pass the audit rather than ensure security. Second, a complacency until the next audit was conducted, and thirdly was the issue of 'patching'. An example is the use of. . .

> *"stand-alone products. If auditors ask to remove this application, we raise it as a ticket to x. X says that it is not a bug and hence we are not going to remove it. We only provide a service like this if there is a bug in it. They deny the request and we cannot touch the product as it is a stand-alone product and hence we only do the patching. This kind of risk is noted as a known risk in the audit report and we do the patching for this. This patch is not going to work for long and is temporary only where the security risk remans as such."*

To ensure robust security, policies should focus proportionally on all three domains namely people, processes and technology. Where managers focus on the functionality of applications, rather than security testing, vulnerability will exist. "Many managers dont think that a cyber security incident will it affects them. They have this attitude that it wont affect them. They somehow feel that for no valid reason, for no justifiable reason that they are immune to all this." Adequate monitoring as part of "PDCA [Plan, Do, Check, Act] need to be implemented" to ensure that security management is a continuous process.

B. Employees

Employee mistakes are a major cause of APT attacks. In this respect the respondents stated "while we have people, processes and technology; people are the weakest link in the information security." Two weaknesses cited were "Naivety that makes them trust people by default" and "attackers exploit the fact that one person trusts the other". Second, another major issue cited by respondents was the lack of awareness (detection) of methods used by APTs, which respondents attributed to a lack of training. Two major issues highlighted by respondents was the neglect of IT security communications, and the lack of knowledge of security policies within the organizations. Regarding the latter, one respondent stated that there was a tendency by employees to sign security policies (which they are required to read and accept) without reading them. Respondents signposted 'unethical behavior' by developers finding and using short cuts, resulting in issues with password management for network administrators. In this aspect two factors may play a role. First is the management factor 'speed of delivery' and second is the employee factor 'accessibility vs security'. Regarding the latter, one respondent attributed blame to both the employees and management in their choice and preference for speed and ease of access to information in computer systems, over IT security. Issues with training is linked to multiple factors across all three dimensions. Respondents cited two major issues in this respect, namely the current unattractive delivery of training currently utilised by organizations (that makes the employees "disinterested") and the "dont care" attitude of employees towards training. Lastly, consumers preference for fanciful gadgets (that can connect to organizational networks) without knowing their inherent security issues, was highlighted as providing an easy conduit for APT vectors.

C. Environmental Factors

Two issues were cited in 'multiple attack vectors' namely competency of the IS security manager and linked and inherited privileges built into online applications. Regarding competency, which respondents termed as 'vertical' and 'horizontal' knowledge, a distinction was made whereby APT attackers are experts in their own vector (vertical), whereas an IS security manager has overall surface knowledge (horizontal) in most of the known vectors. The second highlighted issue was the default permissions built into applications by companies, which generated major concerns within the IT domain of organizations. Respondents highlighted 'online profiles' and the ease with which hackers can gain information regarding a person or organizations or its IT architecture, as another major concern. Competition and rivalry among competing anti malware vendors was highlighted as a major stumbling block, since it restricts the sharing of information regarding 'zero day' and APT threats. The fourth factor was a general lack of research in cyber security in the Middle East and North African (MENA) region, compared to North America, Europe, East Asia and Oceania. Respondents had a final word of caution to regulatory authorities. "IT products and services vendors must comply with certain regulations of a specific country where they are based." However, standardization of regulations may propose changes that may not be applicable to specific products or services.

Analysis and evaluation of the factors highlighted interrelationships and overlap across factors and dimensions, such that we find many cause and effect relationships to be present. This is due to the inherent presence of people, processes and technology to varying degrees in each of these factors, such that it can be viewed from three dimensions. In this respect, the three dimensions can provide managers with information on formulating holistic strategies to combat APT threats without forming a 'weak link' in any of the three dimensions.

VII. Conclusion

APTs penetrate organizational networks using 'socio', and 'technical' methods. Academic and commercial research surrounding APT incidents largely depict the user as the prominent weakness and conduit into a system, along with specific technical vulnerabilities. As a result, there is a lack of research surrounding the dimensions of the 'socio' (non-technical) factors that influence the user, which often result in unintentional mistakes. This paper addresses this literature gap, and in doing so presents two interesting and unique results. First, we present the prominent role management play in IS decisions which greatly contribute to the 'socio' aspect. Secondly, we also present the unique role external factors play in the 'socio' aspect that indirectly promote APTs entry into organizational systems.

Our study is not without its limitations. First, our study focused only on the 'socio' vulnerabilities rather than the countermeasures. Future studies on corresponding vulnerabilities could enrich this domain. Second, we found cause and effect relationships between the factors in the dimensions which we did not explore further. Future research could analyze the intricate relationships found. Third, since only managers were interviewed, not employees or computer users, bias could be present in the responses. This could however form the basis for further research in the area. The research in this paper provides unique insights into the three dimensions namely management, employees and environmental factors that can be considered by organizations when planning, implementing, and controlling APT threats.

REFERENCES

[1] J. V. Chandra, N. Challa, and S. K. Pasupuleti, "Advanced persistent threat defense system using self-destructive mechanism for cloud security," in *2016 IEEE International Conference on Engineering and Technology (ICETECH)*, March 2016, pp. 7–11.

[2] Q. Zhang, H. Li, and J. Hu, "A study on security framework against advanced persistent threat," in *2017 7th IEEE International Conference on Electronics Information and Emergency Communication (ICEIEC)*, July 2017, pp. 128–131.

[3] W. Matsuda, M. Fujimoto, and T. Mitsunaga, "Detecting apt attacks against active directory using machine leaning," in *2018 IEEE Conference on Application, Information and Network Security (AINS)*, Nov 2018, pp. 60–65.

[4] D. Moon, H. Im, J. D. Lee, and J. H. Park, "Mlds: Multi-layer defense system for preventing advanced persistent threats," *Symmetry*, vol. 6, no. 4, pp. 997–1010, 2014. [Online]. Available: https://www.mdpi.com/2073-8994/6/4/997

[5] B. Thakar and C. Parekh, "Advance persistent threat: Botnet," in *Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies*, ser. ICTCS '16. New York, NY, USA: ACM, 2016, pp. 143:1–143:6.

[6] A. Alshamrani, S. Myneni, A. Chowdhary, and D. Huang, "A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities," *IEEE Communications Surveys Tutorials*, vol. 21, no. 2, pp. 1851–1877, Secondquarter 2019.

[7] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, "Advanced social engineering attacks," *Journal of Information Security and Applications*, vol. 22, pp. 113 – 122, 2015, special Issue on Security of Information and Networks.

[8] A. Niakanlahiji, J. Wei, and B. Chu, "A natural language processing based trend analysis of advanced persistent threat techniques," in *2018 IEEE International Conference on Big Data (Big Data)*, Dec 2018, pp. 2995–3000.

[9] M. Adeka, S. Shepherd, and R. Abd-Alhameed, "Resolving the password security purgatory in the contexts of technology, security and human factors," in *2013 International Conference on Computer Applications Technology (ICCAT)*, Jan 2013, pp. 1–7.

[10] K. Guo, Y. Yuan, N. Archer, and C. Connelly, "Understanding non-malicious security violations in the workplace: A composite behavior model," *J. Manage. Inf. Syst.*, vol. 28, no. 2, pp. 203–236, Oct. 2011.

[11] R. Paans and I. Herschberg, "Computer security: The long road ahead," *Computers Security*, vol. 6, no. 5, pp. 403 – 416, 1987.

[12] P. Chen, L. Desmet, and C. Huygens, "A study on advanced persistent threats," in *Communications and Multimedia Security*, B. De Decker and A. Zúquete, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 63–72.

[13] G. Vert, B. Gonen, and J. Brown, "A theoretical model for detection of advanced persistent threat in networks and systems using a finite angular state velocity machine (fast-vm)," *International Journal of Computer Science and Application*, May 2014.

[14] Y. Wang, Y. Wang, J. Liu, and Z. Huang, "A network gene-based framework for detecting advanced persistent threats," in *2014 Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*, Nov 2014, pp. 97–102.

[15] K. Wright. (2014) Uk is the no. 1 target for advanced persistent threat cyber attacks. [Online]. Available: http://www.itgovernance.co.uk/blog/uk-is-the-no-1-target-for-advanced-persistent-threat-cyber-attacks/

[16] K. K.-Y. Chang, "Advanced persistent threat : Malicious code hidden in pdf documents," 2014.

[17] F. J. Aparicio-Navarro, K. G. Kyriakopoulos, I. Ghafir, S. Lambotharan, and J. A. Chambers, "Multi-stage attack detection using contextual information," in *MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM)*, Oct 2018, pp. 1–9.

[18] I. Ghafir and V. Penosil, "Advanced persistent threat attack detection: An overview," *International Journal of Advances in Computer Networks and Its Security (IJCNS)*, vol. Volume 4, 2014.

[19] N. Shashidhar and L. Chen, "A phishing model and its applications to evaluating phishing attacks," 01 2011.

[20] I. Jeun, Y. Lee, and D. Won, "A practical study on advanced persistent threats," in *Computer Applications for Security, Control and System Engineering*, T.-h. Kim, A. Stoica, W.-c. Fang, T. Vasilakos, J. G. Villalba, K. P. Arnett, M. K. Khan, and B.-H. Kang, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 144–152.

[21] P. Giura and W. Wang, "Using large scale distributed computing to unveil advanced persistent threats," 2012.

[22] ——, "A context-based detection framework for advanced persistent threats," *2012 International Conference on Cyber Security*, pp. 69–74, 2012.

[23] (2012) Lifecycle of an advanced persistent threat. [Online]. Available: http://www.redteamusa.com/LifecycleofanAdvancedPersistentThreat.pdf

[24] R. Wash and M. M. Cooper, "Who provides phishing training?: Facts, stories, and people like me," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, ser. CHI '18. New York, NY, USA: ACM, 2018, pp. 492:1–492:12.

[25] B. B. Gupta, N. A. G. Arachchilage, and K. E. Psannis, "Defending against phishing attacks: taxonomy of methods, current issues and future directions," *Telecommunication Systems*, vol. 67, no. 2, pp. 247–267, Feb 2018.

[26] Editor, "Big threats for small businesses," 2013.

[27] T. N. Jagatic, N. A. Johnson, M. Jakobsson, M. Jakobsson, and F. Menczer, "Social phishing," *Commun. ACM*, vol. 50, no. 10, pp. 94–100, Oct. 2007.

[28] M. Carlton, Y. Levy, and M. Ramim, "Mitigating cyber attacks through the measurement of non-it professionals cybersecurity skills," *Information and Computer Security*, vol. 27, 02 2019.

[29] M. Ussath, D. Jaeger, Feng Cheng, and C. Meinel, "Advanced persistent threats: Behind the scenes," in *2016 Annual Conference on Information Science and Systems (CISS)*, March 2016, pp. 181–186.

[30] S. Whittaker, "Qualitative research in transfusion medicine: closing the gap," *ISBT Science Series*, vol. 1, pp. 133 – 139, 08 2006.

[31] N. Leech and A. Onwuegbuzie, "Qualitative data analysis: A compendium of techniques and a framework for selection for school psychology research and beyond," *School Psychology Quarterly*, vol. 23, pp. 587–604, 12 2008.