

# Cybersecurity Assessment of the Public Sector in Greece

George Drivas<sup>1, 2</sup>, Leandros Maglaras<sup>1, 3</sup>, Helge Janicke<sup>3</sup> and Sotiris Ioannidis<sup>4</sup>

<sup>1</sup>National Cyber Security Authority of Greece, General Secretariat for Digital Policy, Ministry of Digital Policy, Telecommunications and Media, Kallithea, Greece

<sup>2</sup>University of Piraeus, Department of Digital Systems, Piraeus, Greece

<sup>3</sup>De Montfort University, School of Computer Science and Informatics, Leicester, UK

<sup>4</sup>Foundation for Research and Technology, Greece

[g.drivas@gsdp.gr](mailto:g.drivas@gsdp.gr)

[leandros.maglaras@dmu.ac.uk](mailto:leandros.maglaras@dmu.ac.uk)

[heljanic@dmu.ac.uk](mailto:heljanic@dmu.ac.uk)

[sotiris@ics.forth.gr](mailto:sotiris@ics.forth.gr)

**Abstract:** Organizations have to manage new risks, sometimes proactively, sometimes by being constrained by regulations such as GDPR or the NIS directive. To cope with new threats, it is essential to develop or reinforce a real culture of cybersecurity at the organizational level. Before putting anything in place, we must start by assessing the new risks to which we are exposed. The new regulations that the EU is issuing, invite organizations and member states to follow these approaches. National Cyber Security Authority of Greece (NCSA) is responsible for coordinating the public sector and the National Critical Infrastructures (NCIs) of Greece, in order to take all necessary steps towards a secure Greek Cyberspace. Its main objective is to shield the Nation from external threats and to provide a secure digital environment for all citizens of Greece. One important action is the enhancement of digital skills and the development of a strong public and private security culture, exploiting the potential of the academic community and public and private sector actors. NCSA is following a PDCA-cycle approach with strong cooperation of all relevant stakeholders for securing NCIs. NCSA is planning a series of audits for the entire public sector and for NCIs. The assessment of the central governmental ICT structures was selected as an initial phase. For this purpose, NCSA sent structured questionnaires aiming in capturing the general picture of the security situation of central ICT infrastructures. Data collected during this phase are processed and will be used to design the next steps of deepening and expanding of such assessments but also to institute regular and / or emergency control procedures on a permanent basis. The information that has been gathered is analyzed in order to reveal major threats, capacity building priorities, current situation in terms of procedures, security measures and policies and established incident response plans.

**Keywords:** cyber security, public sector, national critical infrastructures

---

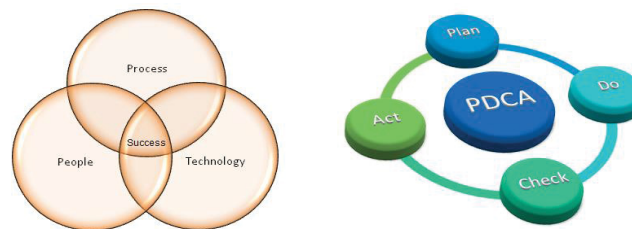
## 1. Introduction

Recently several critical incidents that targeted National Critical Infrastructures (NCIs) have taken place (Maglaras et al, 2019). In September 2018, shortly after Cyber Europe Exercise tested European reaction and cooperation following a cyber attack targeting the aviation sector (Seker and Ozbenli, 2018), information screens in University of Bristol were taken offline to contain an attack similar to so-called "ransomware". Some years ago, in 2015, Ukraine was hit by a massive blackout due to an attack to their SCADA systems, leaving 230K citizens of Ukraine without electricity for several hours. Another attack that took place in 2013, although reported in 2016, targeted a small dam in Rye Brook in New York (Bianco, 2016). The real target of this attack, based on a report of FBI and Homeland security, was Wolf Creek Nuclear Operating Corporation, the impact of which, if successful, would go beyond a single nation. Recently, UK's National Cyber Security Centers (NCSC) is concerned about suspicious attacks that are taking place on UK energy sectors (Kovanen, Nuojua and Lehto, 2018). All of the above are only some of the attacks that are happening every day around the globe and are targeting NCIs, such as oil and gas industry, traffic signal, water sewage building, transportation, and digital infrastructure. It has been shown that a cyberterrorist attack that directly targets a population can have the same effects to those that directly target NCIs (Ayres and Maglaras, 2016).

Following the publication of high-profile security breaches and security incidents, organizations and nations around the globe are increasing their focus and are looking on ways to improve their cyber security assurance (Andreasson, 2011). This will help them protect both their brand and reputation along with the prevention and reduction of financial impacts. Except from technology-related breaches which are due to malicious actors that exploit existing vulnerabilities in technology and that will continue to take place in a regular basis, a big percentage of data breaches or security incidents that are reported are caused by inadvertent human error. Despite the huge surge in interest and acceptance of information security management, incorporating cybersecurity, there still appears to be gaps and weaknesses within organizations. As Critical National

Infrastructures are becoming more vulnerable to cyber attacks, their protection becomes a significant issue for Member States as well. The synergy between the ICS and the IoT has emerged bringing new security challenges. Modern smart societies face new challenges in the area of cyber security, and EU is trying to strengthen Critical Infrastructures by publishing new directives and regulations.

Along with the obligations that directly arise out of the European directives and regulations, Greece and all other member states must take further actions for enhancing cyber security. National Cyber Security Authority of Greece (NCSA) is responsible for coordinating the public sector and the operators of essential services of Greece, in order to take all necessary steps towards a secure Greek Cyberspace. Its main objective is to shield the Nation from external threats and to provide a secure digital environment for all citizens of Greece. One important action is the enhancement of digital skills and the development of a strong public and private security culture, exploiting the potential of the academic community and public and private sector actors. Continuous adaptation of the national institutional framework to the new technological requirements, always in line with the European regulations on data protection and security will help Greece fight cyber-crime. NCSA has issued in 2018 both the National Cyber Security Strategy and the National Law on security of network and information systems (Maglaras et al, 2018). NCSA is planning to follow a PDCA-cycle approach with strong cooperation of all relevant stakeholders for securing NCIs (See Figure 1). A blend of processes, technologies and people is needed to achieve this goal and NCSA must have a general overview of the current situation in terms of hardware, software and security procedures that public sector and NCIs are using. In order to achieve this, a creation of an IT inventory along with a security inventory of all NCIs that reside inside Greece, along with all critical operational centers of the public sector and governmental clouds (Cook et al, 2018) is an essential first step. For that reason a questionnaire was sent to relevant stakeholders aiming in capturing the general picture of the level of security of central ICT infrastructures.



**Figure 1:** Cyber security framework: Success ingredients (left figure) and lifecycle (right figure)

According to the NIS national law, operators of essential services (OES) as well as for the digital service providers (DSP) must introduce appropriate security measures in an effort to achieve a baseline, common level of information security primarily within Greece and in alignment with the European Union (EU) network and information systems. Audits are major enablers to achieve this objective. A security audit is an independent review and examination of system records, activities and related documents using structural procedures and is based on risk exposures (Wood et al, 2017), critical components and business operations of the organization (Tipton and Nozaki, 2007). Having this in mind, along with the necessity to capture the current situation in terms of security as described earlier, NCSA has issued this questionnaire as a pre-audit mechanism.

## 2. Methodology

The questionnaire that was sent to relevant stakeholders was constituted of four main parts of 22 questions in total. Using the initial assessment questionnaire NCSA tried to assess the organizations queried regarding their current level of security, the existence or not of policies, procedures and technical measures, user awareness techniques that they are using and what incident response plans or procedures they have in place. That way we tried to cover all the different aspects that help an organization succeed in the fight against cyber-attacks, procedures, policies, technology and people. The four categories were:

- 1. Current level of security
- 2. Security policies, procedures and technical measures
- 3. User Awareness
- 4. Incident response

The first part consists of six questions regarding the current level of security of the organization. Participants were asked to grade the overall level of security of their organization and answer questions regarding the most

significant threat that according to their opinion exists for their systems. Following questions primarily looked at capacity building needs, cyber attack consequences and cons and pros of enhanced security measures. The second part of the questionnaire included specific questions that tried to capture the current situation of the organization in terms of security policies, procedures and technical measures. In that sense questions about data encryption methods, security mechanisms and self auditing procedures in place were issued to the questioners. A good security awareness program should educate employees about corporate policies and procedures for working with information technology. Employees should receive information about who to contact if they discover a security threat and be taught that data as a valuable corporate asset. For that sense the third part of the questionnaire was focused on the awareness and training of the employees about security and privacy. The fourth part of the questionnaire covered intrusion detection and incident response and handling procedures that the organizations are following. The aim of this project was to assess the security level of central governmental ICS infrastructures of Greece. To meet this aim, the questionnaire was designed to meet six objectives, as follows:

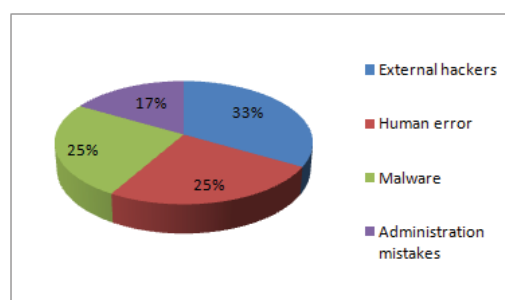
- Build a network of security officers
- To determine major threats to central infrastructures
- To analyze capacity building priorities
- To capture current situation in terms of procedures, security measures and policies
- To determine if there is an incident response plan in place
- To capture training and education policies and mechanisms

### 3. Analysis of results

The data collected from the questionnaires were recorded and interpreted in accordance with the identified objectives of this research. The analysis of the data was designed to explore any similarities, differences or patterns among the responses and any underlying relationships. *More than 30 questioners filled the answers, in some occasions having the same person to fill the whole questionnaire for an organization while in other occasions two or three persons were needed to cover all the activities of the company being assessed. Most of the responders were Directors or Heads of the IT divisions which are in charge for the security management of their organizations. Although public organizations that were assessed covered a big range of different activities, including also critical infrastructures, the exact identity of each organization cannot be revealed since this information is sensitive in terms of national security.*

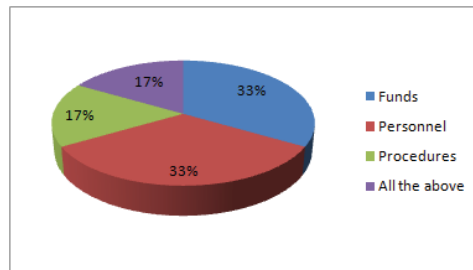
#### 3.1 Current level of security

The first part of the questionnaire primary looked at what is the overall level of security of the organization according to the participants' opinion. The results revealed that 45% of the experts assess their systems as being relatively safe while 55% think that the level of safety of their systems is satisfactory. Participants were asked about their opinion regarding the most significant threat that their systems face. According to a recent research by Evans et al (2019), the majority of incidents within the public sector relate to human error. The research findings has identified that the actual proportion of reported public sector information security incidents that relate to human error is 92.5%. However, as Figure 2 shows, participants feel that external hackers (33%) is the major threat for their systems, followed by human error (25%) and malware infection (25%), while administration/configuration mistakes (17%) is the least significant threat.



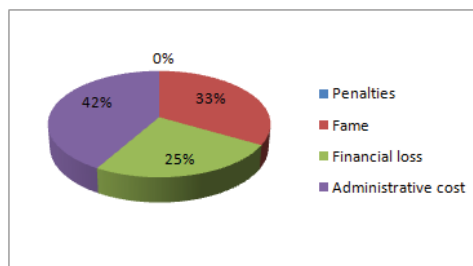
**Figure 2:** Major threat

Training of key stakeholders and key personnel and providing them with the capacities they need to uphold cybersecurity is important for a stable cyber capacity. In that sense we tried to identify the major need that public sector in Greece have in terms of capacity building. Figure 3 shows that organizations identify enhancement of personnel capabilities through training and education along with the increase in numbers of employees that work in specific information security departments as their primary concern with 33%. Increase in funds that are spent for hardware and software security solutions is also a major concern gathering the same number of answers, 33%.



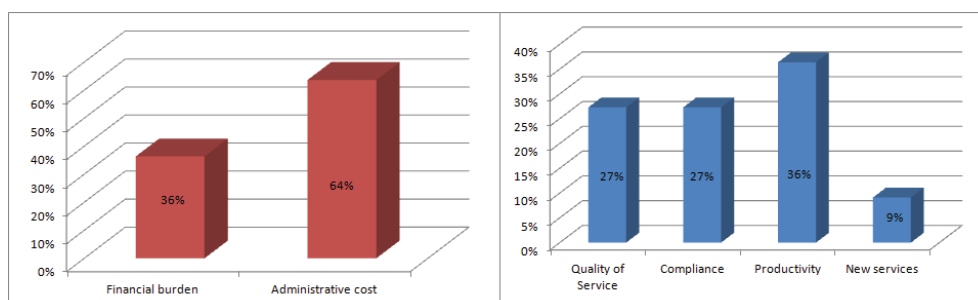
**Figure 3:** Capacity building

Another aspect that the questionnaire looked at was about major concerns of public organizations in Greece, following a data breach or a cyber attack in general. As shown in Figure 4, administrative cost due to following a disaster recovery plan or a mitigation plan for recovering the organization's normal operation is the number one concern with 42%, followed by financial loss and fame with 33% and 25% accordingly. Penalties do not appear to be an important concern for public sector organizations since GDPR and NIS weren't active yet when the questionnaire was issued.



**Figure 4:** Data breach/cyber attack consequences

Pros and cons of a tentative upgrade of the organization's security level were also questioned. As shown in Figure 5 financial burden (37%) and administrative costs (63%) are major negative consequences while on the same time participants expect their organization to be better organized and more productive (37%) after imposing security measures or standard procedures as parts of a security enhancement strategy.

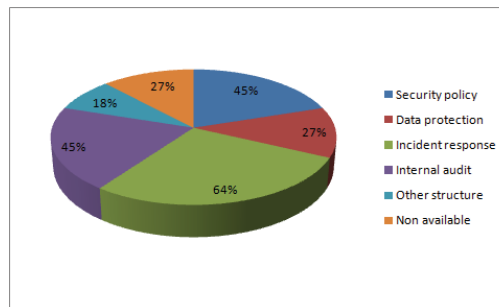


**Figure 5:** Pros and cons of security upgrade

### 3.2 Security policies, procedures and technical measures

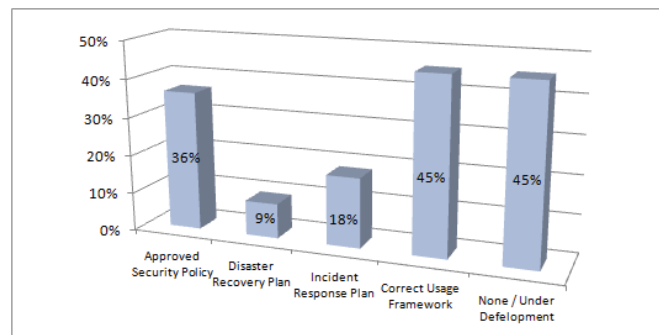
The second part of the questionnaire covered issues regarding any established structures that exist inside the organization, policies that are issued and / or approved, specific security measures that are in place, along with audit plans and procedures that may exist. As shown in Figure 6, 45% of the organizations have a specific department/directorate that is responsible for the implementation and evaluation of the security policy, while on the same time only 28% had a similar structure responsible for protection of personal data. The low

percentage that is observed in regards to data protection is due to the fact that at the time that the questionnaire was issued GDPR was still inactive in Greece.



**Figure 6:** Organizational units

The second part of the questionnaire focused in investigating the existence of security policies, recovery plans, incident handling procedures or a general framework that covers the correct usage of IT equipment and the dissemination of those to all employees. According to the findings, which are presented in Figure 7, almost half of the public organizations (45%) don't have any of the aforementioned documents in place which is an important finding about basic security measures that are missing and should be prioritized in the near future.



**Figure 7:** Security policy / recovery plan

Participants recorder the specific technical measures that the organization is using in order to secure their systems and the data when transmitted or stored in their data centers. Based on the analysis of the data, It was revealed that most of the organizations use a combination of firewalls, anti-spam, antivirus and IDS systems among others. The most common system that almost all participants answered that they are using, was a centrally managed user access control / authentication system while on the other hand a centrally controlled equipment and peripheral device connection control over the internal access network (NAC / Device Control) system was only present at less than 10% of the organizations. With organizations now having to account with an exponential growth of mobile devices accessing their networks and the security risks they bring, it is critical to have tools that provide visibility, access control, and compliance capabilities. A NAC system can deny network access to noncompliant devices, place them in a quarantined area, or give them only restricted access to computing resources, thus keeping insecure nodes from infecting the network (Koh, Oh and Im, 2014).

Responders also answered whether they use commercial or open source solutions for implementing the security measures on their organizations and whether their organization followed an internal audit procedure and how often such audits were conducted. Based on the findings (see Figure 8), most of the organizations follow ad hoc procedures for evaluating the compliance of the organization to the laws and also for assessing the level of security rather than conducting regular internal or external audits.

Finally participants were asked about trainings or certifications in areas related to the security of IT systems, services and infrastructures that employees of the organizations have received recently. Based on the findings, as shown in Figure 9, there was a mix of dedicated trainings, certificates and degrees that employees had. The level of trainings/education was not uniform though. While in several organizations there was a number of trained staff having all of the aforementioned qualifications, in other organizations there was a lack of such trained/expert staff.

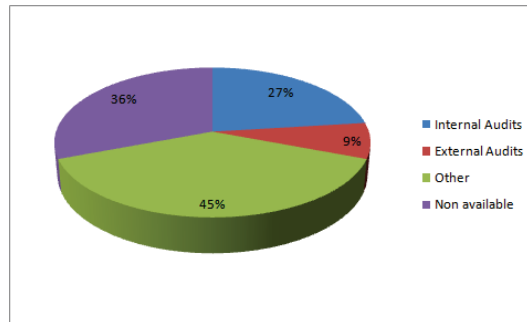


Figure 8: Audits

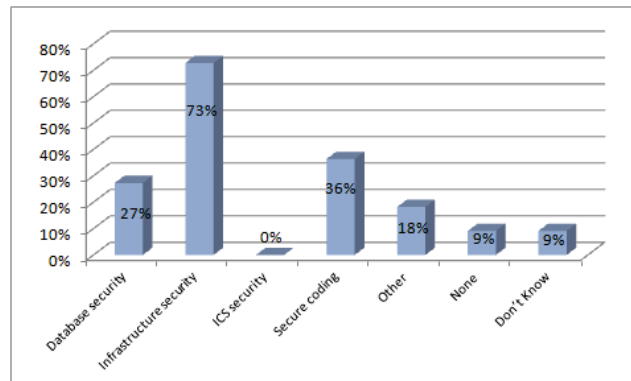


Figure 9: Education

### 3.3 User awareness

User awareness is investigated through the third part of the questionnaire, in terms of relevant policies and mechanisms in place, along with targeted trainings on new legislative requirements (e.g. NIS Directive, GDPR Regulation).

Organizations were questioned about the established mechanisms that they use to educate their users on security and privacy aspects covering areas like new threats, prevention and reaction practices, legislative requirements and more. Figure 10 shows that the majority of organizations (55%) use Informal ways of achieving such awareness, through online sources in an ad-hoc base (e.g. blogs, mailing lists, social media) and only 27% use Formal and established mechanisms, like specialized conferences and trainings. Meanwhile, 45% reported that there is no structured mechanism for user awareness at all.

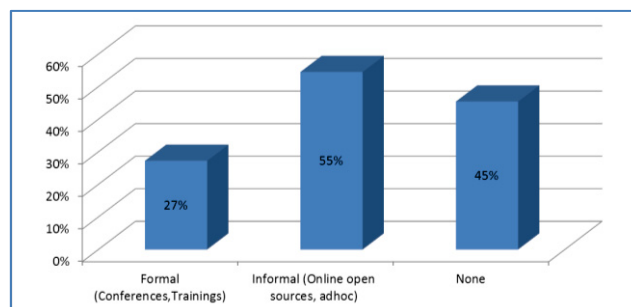
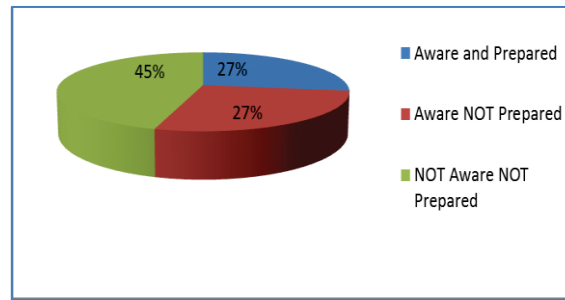


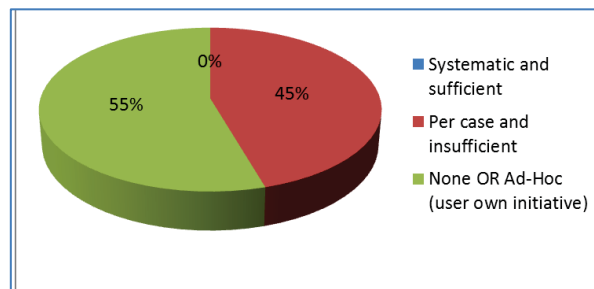
Figure 10: User awareness mechanisms

On Figure 11 the overall satisfaction in terms of awareness and preparedness on new legislative requirements (NIS, GDPR) is presented. It was revealed that 45% of the organizations were neither aware nor prepared. This is evaluated as an expected outcome since both legislations were not into force when the questionnaire was first issued.



**Figure 11:** Legislation awareness (NIS, GDPR)

Overall, responders evaluated the current state on user awareness/training policy on their organizations (see Figure 12). Among them, the majority (55%) reported that there was no policy and that this was only viable by own initiative, or, when such policy existed 45% answered that this was insufficient.

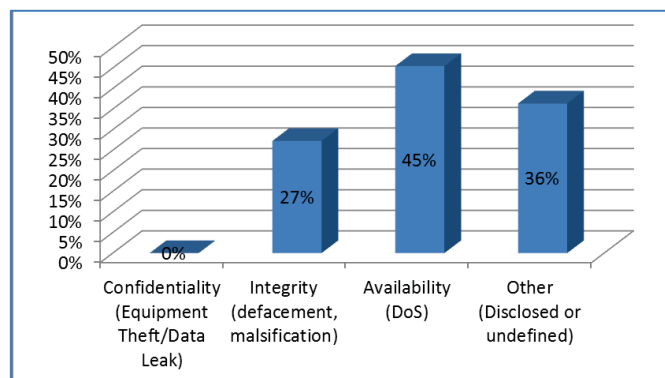


**Figure 12:** User awareness/training policy

### 3.4 Incident response

The final part of the questionnaire was focused on Incident response in terms of timely detection, impact evaluation and reaction procedures.

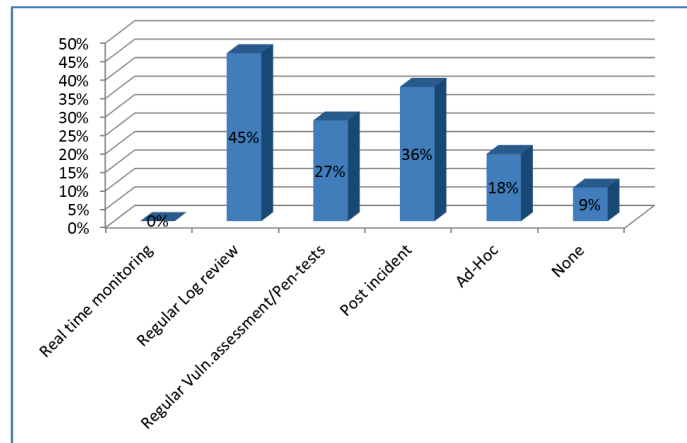
All organizations responded that they have been affected by at least one security incident during the past 12 months and 45% of them had at least one incident relevant to availability disruption, with common type of attack the “Denial of Service” (see Figure 13)



**Figure 13:** Key security principles affected by incidents (past 12 months)

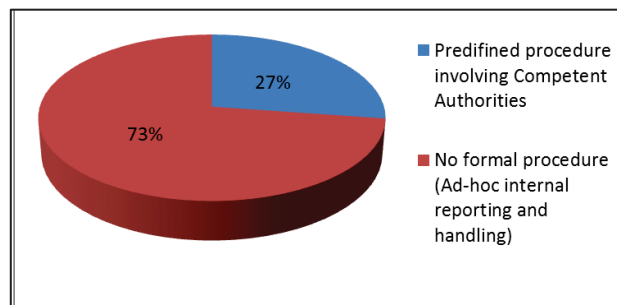
Concerning threat detection, Figure 14 shows that 45% regularly reviewed their log files and 27% tested their systems through vulnerabilities assessment and/or penetration tests regularly (i.e. yearly or sooner). However, it was revealed that none of the responders used a real time monitoring mechanism or a similar procedure. A significant proportion of responders (36%) reported that threats are detected only after a disruptive effect has already occurred and impacted the ICT environment.





**Figure 14:** Threat detection

In light of an incident occurrence, organizations reported that only 27% are following a predefined procedure for filing and handling a security incident with predetermined escalation procedures to Competent Authorities while the rest are handling the incident with an ad-hoc approach led by the IT Department (Figure 15).



**Figure 15:** Incident reporting and handling

#### 4. Discussion

The analysis of the results helped us identify what are the major threats that organizations are facing today, create a picture of the current posture in terms of cyber security and define the priorities for strengthening their security. *One interesting result of the study is that 92,5% of security incidents reported have origin in human errors. Although the second part of the questionnaire was mainly focused on technology such as firewalls, anti-spam, antivirus and IDS, it also covered both organizational and certification issues while on the same time the third part was devoted to human factor in terms of awareness and trainings. Based on this, the study revealed that 45% of the questionnaires responded that there is no structured mechanism for user awareness at all.* One of the main concerns that participants had was about education programs, awareness campaigns and exercises that need to be conducted in a regular basis. Dedicated education programs and awareness campaigns can help strengthen the organization and the nation against cyber-attacks (de Bruijn and Janssen, 2017). The majority of educational programs within the cyber security domain are awareness campaigns (Coventry et al, 2014). These campaigns typically use lectures or presentations to articulate the issues surrounding advanced actors to a wide audience, with little tailoring to specific audiences. Experiential learning on the other hand (Kolb, 2014), is an educational technique based on the assumed importance of experimenting and involvement, proposing that active engagement in a scenario develops personal experiences that form the basis of understanding.

As stated in the National Cyber Security Strategy that NCSA has issued in 2018, National Preparedness Exercises are an important tool for evaluating participating stakeholders' preparedness and for detecting weaknesses and vulnerabilities. The simulation of security incidents offers the opportunity for handling these under conditions similar to actual incidents, through implementation of the relevant security measures taken, and of drafted pertinent contingency plans, so that the stakeholders may proceed with relevant improvements and updates (Cook et al, 2017). For these reasons NCSA has decided that a blend of awareness campaigns, dedicated educational programs and exercises must be conducted in a regular basis along with the competent CSIRT, the National CERT and other major stakeholders. NCSA is conducting, hosting or co-organizing a series of awareness



events with OWASP, OSCE and other organizations that are related to cyber security and continue to organize a series for such events for the upcoming months. NCSA is also participating in PANOPTIS that is organized by the directorate of cyber defense of Ministry of Defense. PANOPTIS exercise is organized since 2010 and involves more than 200 people from Armed Forces and Security Bodies, Academic Sector and Research Centers, Public and Private Sector and in 2019 is dedicated to test NIS procedures and mechanisms.

Cooperation both internally inside the Greek Nation and externally with other member states of the EU and beyond, is critical aspect for succeeding in the battle against cyber-attacks against NCIs, reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs (Boeke, Heintl and Veenendaal, 2015) or even restore peace in the aftermath of a cyber-warfare (Robinson et al, 2018). NCSA has used this questionnaire as a means of initiating a cooperation with relevant stakeholders, create a list of experts that can work together in order to solve problems and increase the overall level of cyber security. In order to strengthen cooperation in European level, NCSA is representing Greece in the NIS cooperation group, in the Horizontal Working Party on cyber issues of the EU, in the informal working group that is set up by OSCE for addressing security of and in the use of information and communication technologies (ICTs), among others. To that sense NCSA is also participating in H2020 and National projects related to cyber security, e.g. CONCORDIA. CONCORDIA, a new H2020 project that started on the 1st of January and lasts for four years, builds a Cybersecurity Competence Network with leading research, technology, industrial and public competences to build the European Secure, Resilient and Trusted Ecosystem.

## **5. Conclusions**

Organizations have to manage new risks, sometimes proactively, sometimes by being constrained by regulations such as GDPR or the NIS directive. To cope with new threats, it is essential to develop or reinforce a real culture of cybersecurity at the organizational level. Before putting anything in place, we must start by assessing the new risks to which we are exposed. The new regulations that the EU is issuing, invite organizations and member states to follow these approaches. However, it is not enough to get in compliance to be well protected. Regulations, which lay down very general principles, must be understood in the light of the organization context, its developments and the risks involved. For that purpose NCSA has created a questionnaire as a pre-audit mechanism that was sent to governmental stakeholders of Greece. Using the information that was collected from the answers of the participants, NCSA managed to create a list of experts, identify major threats that their systems face and capture their current level of cyber security.

## **Acknowledgements**

The authors wish to acknowledge the financial support of the project CONCORDIA, funded under European H2020 Programme (contract No. 830927)

## **References**

- Andreasson, K. J. (Ed.). (2011). *Cybersecurity: public sector threats and responses*. CRC Press.
- Ayres, N. and Maglaras, L. (2016). Cyberterrorism targeting general public through social media. *Security and Communication Networks (WILEY)*, 9(15)
- Bianco, L. J. (2016). *The inherent weaknesses in industrial control systems devices; hacking and defending SCADA systems* (Doctoral dissertation, Utica College).
- Boeke, S., Heintl, C. H. and Veenendaal, M. A. (2015, May). Civil-military relations and international military cooperation in cyber security: Common challenges & state practices across Asia and Europe. In *Cyber Conflict: Architectures in Cyberspace (CyCon)*, 2015 7th International Conference on (pp. 69-80). IEEE.
- Cook, A., Smith, R. G., Maglaras, L. and Janicke, H. (2017). SCIPS: using experiential learning to raise cyber situational awareness in industrial control system. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, 7(2), 1-15.
- Cook, A., Robinson, M., Ferrag, M. A., Maglaras, L. A., He, Y., Jones, K., & Janicke, H. (2018). Internet of cloud: Security and privacy issues. In *Cloud Computing for Optimization: Foundations, Applications, and Challenges* (pp. 271-301). Springer, Cham.
- Coventry, L., Briggs, P., Blythe, J., and Tran, M. (2014). *Using behavioural insights to improve the public's use of cyber security best practices*. Gov. UK report.
- de Bruijn, H., and Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, 34(1), 1-7.
- Evans, M., He, Y., Maglaras, L. and Yevseyeva, I. and Janicke, J. (2019), *Evaluating Information Security Core Human Error Causes (IS-CHEC) Technique in Public Sector and Comparison with the Private Sector*, Elsevier *International Journal of Medical Informatics*

- Kovanen, T., Nuojua, V., and Lehto, M. (2018, March). Cyber Threat Landscape in Energy Sector. In ICCWS 2018 13th International Conference on Cyber Warfare and Security (p. 353). Academic Conferences and publishing limited.
- Koh, E. B., Oh, J., and Im, C. (2014). A study on security threats and dynamic access control technology for BYOD, smart-work environment. In Proceedings of the International MultiConference of Engineers and Computer Scientists (Vol. 2014, pp. 12-14).
- Kolb, D. A. (2014). *Experiential learning: Experience as the source of learning and development*. FT press.
- Maglaras, L., Drivas, G., Noou, K., and Rallis, S. (2018). Nis directive: The case of Greece. *EAI Endorsed Transactions on Security and Safety*, 18, 5.
- Maglaras, L., Ferrag, M. A., Derhab, A., Mukherjee, M., Janicke, H., and Rallis, S. (2019). Threats, Protection and Attribution of Cyber Attacks on Critical Infrastructures. *arXiv preprint arXiv:1901.03899*.
- Robinson, M., Jones, K., Janicke, H., and Maglaras, L. (2018). An introduction to cyber peacekeeping. *Journal of Network and Computer Applications*, 114, 70-87.
- Seker, E., and Ozbenli, H. H. (2018, June). The Concept of Cyber Defence Exercises (CDX): Planning, Execution, Evaluation. In 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security) (pp. 1-9). IEEE.
- Tipton, H. F., and Nozaki, M. K. (2007). *Information security management handbook*. CRC press.
- Wood, A., He, Y., Maglaras, L., and Janicke, H. (2017). A security architectural pattern for risk management of industry control systems within critical national infrastructure.



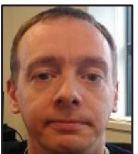
**Filipe Caldeira** is an Adjunct Professor at the Polytechnic Institute of Viseu, Portugal. He is a researcher at the CI&DETS research centre of the Polytechnic Institute of Viseu and at the Centre for Informatics and Systems of the University of Coimbra. His main research interests include ICT security, namely, trust and reputation systems, Smart Cities and Critical Infrastructure Protection. His research papers were published in various international conferences, journals and book chapters. He has been recently involved in some international and national research projects.



**Prof. Walter Dorn** is Professor of Defence Studies at the Royal Military College of Canada (RMC) and the Canadian Forces College (CFC). He teaches officers of rank major to brigadier-general from Canada and about 20 other countries.



**Prof. Helge Janicke** is the Technical Director of De Montfort University's Cyber Technology Institute. He is a general chair of the International Symposium on SCADA and Industrial Control Systems Cyber Security Research (ICS-CSR). He serves on the editorial board and as reviewer for a number of international journals.



**Dr. Michael Robinson** is a cyber security research engineer at Airbus. As part of the architecture, innovation and scouting team he provides cyber expertise to the business and supports state of the art research into new and novel cyber security solutions.



**Dr. Char Sample** is a researcher focused on Threat Intelligence at MITRE and a visiting fellow at the University of Warwick. Dr. Sample has most recently focused her studies on the role of culture in cyber-attack and defence behaviours. Additionally, she has interest in metrics, traffic analysis, risk management and measurement, and predictive models. Dr. Sample's background encompasses commercial, government and most recently academic environments. She continues to try to merge the best features of all three environments.

## Biographies of Contributing Authors

**Ramona Susanty Ab Hamid** has been with CyberSecurity Malaysia for the past 17 years, an agency under the Ministry of Communications and Multimedia, Malaysia. Ramona holds a Degree in Applied Statistics and Operational Research from the University of Science Malaysia (USM) and holds a Postgraduate Diploma in Protective Security Management from International Islamic University Malaysia. She has contributed various publications and presentations related to cyber security and cyber safety besides managing content for CyberSAFETM Program since 2010

**Sokri Abderrahmane** has a Ph.D. in administration from HEC-Montreal. He serves as a Data Scientist for the Canadian Department of National Defence. He taught economics and statistics at different universities. He has published in high-level international journals. His current research interest includes game theory applied to military operations.

**Susana Aldeia** is a full-time Assistant Professor at the Portucalense University. She holds a Phd with mention in Tax Law. She is a researcher at REMIT and IJP. She develops research activities on taxation and accounting. She has been a chartered accountant since 2003 in exercise.

**Vijay Bhuse** is an Assistant Professor of Computer Science at the Grand Valley State University. He received his Ph.D. from Western Michigan University in 2007 and completed his postdoctoral fellowship from the Dartmouth College. He worked in industry before returning to academia. His research interests are Network Security, Wireless Sensor Networks and Secure Coding.

Reproduced with permission of copyright owner. Further reproduction  
prohibited without permission.