Assessing Cyber Security Threats and Risks in the Public Sector of Greece

G Drivas[1], L Maglaras[2], H Janicke[2], S Ioannidis[3]

[1]Department of Digital Systems
University of Piraeus
Piraeus, Greece

E-mail: george.drivas@unipi.gr

[2]Faculty of Computing
Engineering and Media
De Montfort University
Leicester, United Kingdom

Email: leandros.maglaras@dmu.ac.uk; heljanic@dmu.ac.uk

[3]Foundation for Research and Technology
Crete, Greece

Email: sotiris@ics.forth.gr

Abstract: *Organisations having to cope with new threats and risks are increasing their focus and looking at novel ways to improve their cyber security assurance. As critical national infrastructures are becoming more vulnerable to cyberattacks, their protection becomes a significant issue for EU member states. The National Cyber Security Authority of Greece (NCSA) takes all necessary steps towards a secure Greek cyberspace. This article presents the findings from the assessment of the main governmental ICT infrastructures in terms of major threats, capacity-building priorities, as well as the current situation in terms of procedures, security measures and policies, and established incident response plans.*

Keywords: *Cyber Security, Cybersecurity, Cyber Attack, Cyberattack, Public Sector, National Critical Infrastructures*

Introduction

Recently, several critical incidents that targeted National Critical Infrastructures (NCI) have taken place (Maglaras *et al.* 2019). In September 2018, shortly after the "Cyber Europe" exercise tested the European reaction and cooperation following a cyberattack targeting the aviation sector (Seker & Ozbenli 2018), information screens in Bristol airport were taken offline by a real "ransomware" style attack. In 2015, Ukraine was hit by a massive blackout due to an attack on 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 from the FBI and the Department of 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 Center (NCSC) has been concerned about suspicious attacks that are taking place on the UK energy sector (Kovanen, Nuojua & Lehto 2018). All the above are only some of the attacks that are happening every day around the globe and are targeting NCI, such as the oil and gas industry, traffic signals, water sewage buildings, transportation, and digital infrastructure. It has been shown that a cyber-terrorist attack that targets an NCI might have the same impact to a terrorist attack directly targeting a population (Ayres & Maglaras 2016).

Following the publication of high-profile security breaches and security incidents, organisations and nations around the globe are increasing their focus and are looking at ways to improve their cybersecurity 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 on 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 and of incorporating cybersecurity, there still appear to be gaps and weaknesses within organisations Rafferty (2016). As NCI are becoming more vulnerable to cyberattacks, their protection becomes a significant issue for EU member states as well. The synergy between the Information and Communication Systems (ICS) and the Internet of Things (IoT) has emerged, bringing new security challenges. Modern smart societies face new challenges in the area of cyber security, and the EU is trying to protect critical infrastructures through 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. NCSA is responsible for coordinating the public sector and the Operators of Essential Services (OES) 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 in 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, in line with the European regulations on data protection and security, will help Greece fight cybercrime. In 2018, NCSA issued 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 (**Figure 1**, below). A blend of processes, technologies and people are 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, the creation of an IT inventory and a security inventory of all NCIs that reside inside Greece, along with all critical operational centres 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 to assess the level of security posture of the main governmental Information and Communication Technologies (ICT) infrastructures.

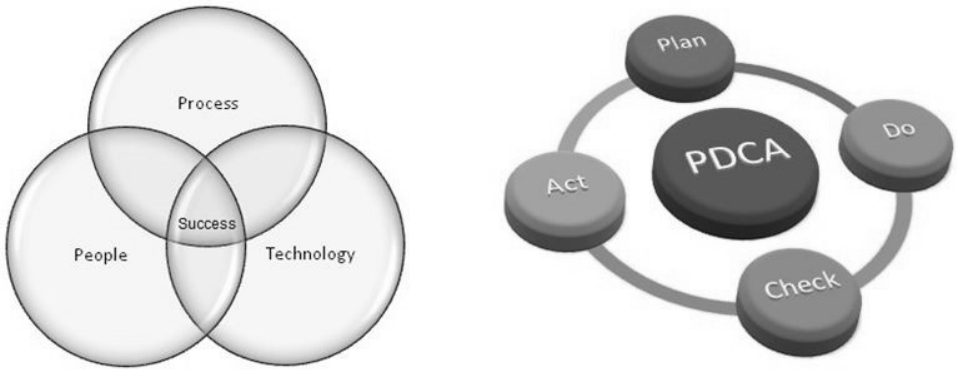


Figure 1: Cybersecurity framework: Success ingredients (left figure) & lifecycle (right figure)

According to the Network and Information Security (NIS) related national law, OES as well as the Digital Service Providers (DSP) must introduce appropriate security measures 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 organisation (Tipton & Nozaki 2007). Having this in mind, along with the necessity of reflecting the current cybersecurity posture of public sector as described earlier, NCSA has issued a questionnaire as a pre-audit mechanism.

Methodology

The aim of this questionnaire was to assess the overall security posture of the main governmental ICS infrastructures of Greece, and it was designed to meet six objectives, as follows:

- To build a network of security officers
- To determine major threats to main ICT infrastructures
- To analyse 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

The questionnaire sent to relevant stakeholders consisted of four main parts and a total of 22 questions. Using the initial assessment questionnaire, NCSA tried to assess the respondents' organisations 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. This approach attempted to cover all the different aspects that help an organisation succeed in the fight against cyberattacks, including procedures, policies, technology, and people. Therefore, the questionnaire was structured in four areas:

- Current level of security
- Security policies, procedures, and technical measures
- User awareness
- Incident response

The first part consisted of six questions regarding the current level of security of the organisation. Participants were asked to grade the overall level of security of their organisation and to answer questions regarding the most significant threat that, in their opinion, exists for their systems. The questions primarily looked at capacity-building needs, cyberattack consequences, and the pros and cons of enhanced security measures. The second part of the questionnaire included specific questions that tried to capture the current posture of the organisation in terms of security policies, procedures, and technical measures. Questions about data encryption methods, security mechanisms, and self-auditing procedures in place, were also included. A good security awareness program should educate employees about corporate policies and procedures for working with information technology. Employees should receive information about whom to contact if they discover a security breach and should be taught that data is a valuable corporate asset. Accordingly, the third part of the questionnaire was focused on employee security and privacy awareness and training. The fourth part of the questionnaire covered intrusion detection and incident response and handling procedures that the organisations are following.

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 respondents provided answers; on some occasions the same person completed the whole questionnaire for an organisation, while on other occasions two or three people were needed to cover all the activities of the company being assessed. Most of the respondents were directors or heads of the IT divisions which are accountable for the security management of their organisations. Although public organisations that were assessed covered a wide range of different activities, including critical infrastructures, the identity of each organisation cannot be revealed as this information is sensitive in terms of national security.

Current level of security

The first part of the questionnaire primarily assessed the overall level of security of the organisation according to the respondent's(s') opinions. The results revealed that 45% of the experts assessed their systems as being relatively safe while 55% thought that the level of safety of their systems was satisfactory. Participants were asked about their opinion regarding the most significant threat that their systems might encounter. According to recent research by Evans *et al*. (2019), most incidents within the public sector relate to human error. The research findings have identified that the actual proportion of reported public-sector information-security incidents that relate to human error is 92.5%. However, as **Figure 2**, below, shows, participants believe external hackers (33%) are the most significant threat to their systems, followed by

human error (25%) and malware infection (25%), while administration/configuration mistakes (17%) is the least significant threat.

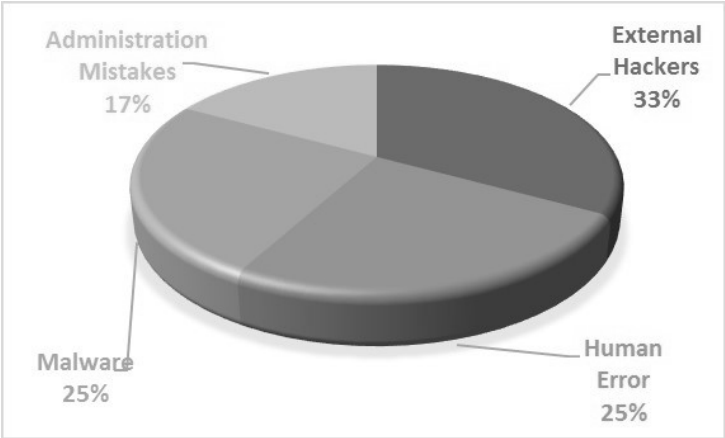


Figure 2: Major threats

Training of key stakeholders and other key personnel and providing them with the capacities they need to maintain cybersecurity are important for a stable cyber capacity. Consequently, the study tried to identify the major needs that the public sector in Greece has in terms of capacity building. **Figure 3**, below, shows that organisations 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 a primary concern reaching to 33%. Increasing funding, for hardware and software security solutions, is also a major concern reaching also to 33%.

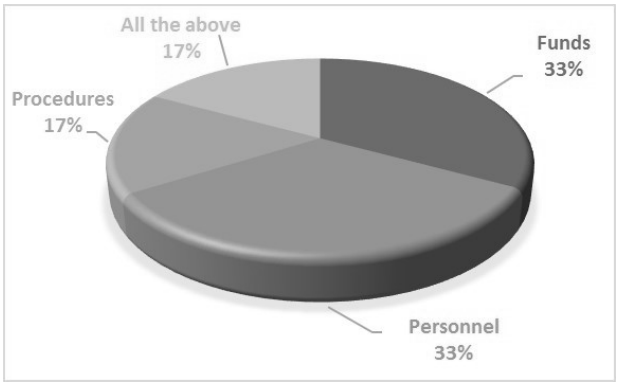


Figure 3: Capacity building

Another aspect that the questionnaire looked at had to do with the major concerns of public organisations in Greece following a data breach or a cyberattack in general. As shown in **Figure 4**, below, administrative costs associated with executing a disaster recovery plan or a mitigation plan for recovering the organisation's normal operation is the number one concern (42%), followed by financial loss and fame (33% and 25%, respectively). Penalties do not appear to be an important concern for public sector organisations since the General Data Protection Regulation (GDPR) and the Network and Information Security (NIS) directive were not yet active when the questionnaire was completed.

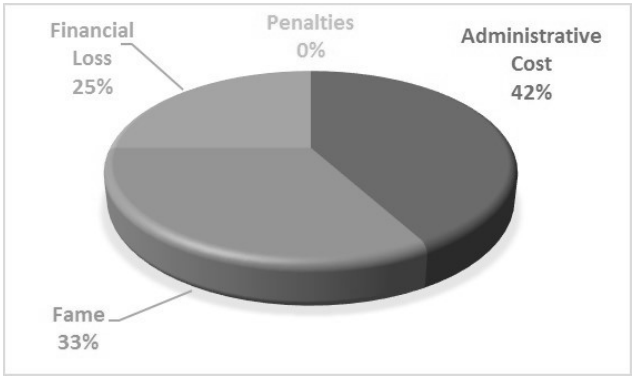


Figure 4: Data breach & cyberattack consequences

The pros and cons of a tentative upgrade of the organisation's security posture were also questioned. As shown in **Figure 5**, below, financial burden (36%) and administrative costs (64%) are major negative consequences, while, at the same time, participants expect their organisation to be better organised and more productive (36%) after imposing security measures or standard procedures as parts of a security enhancement strategy.

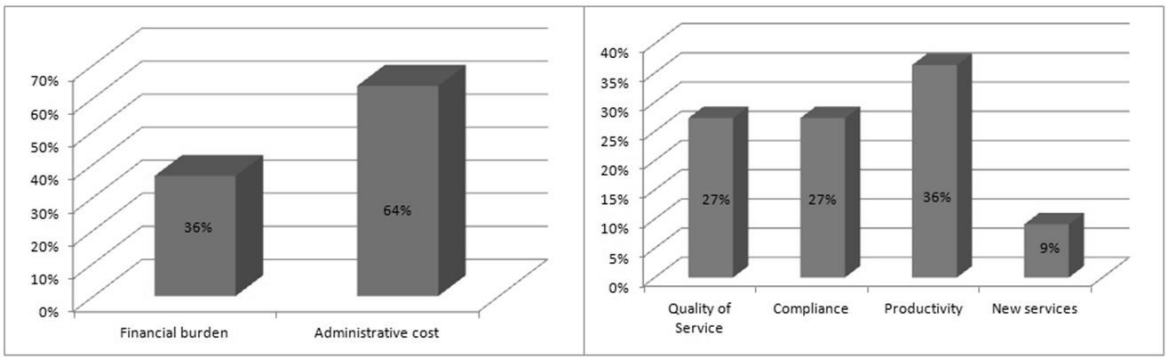


Figure 5: Pros and cons of security upgrades

Security Policies, Procedures, and Technical Measures

The second part of the questionnaire covered issues regarding the established information-security management structures that exist inside the organisation, existing policies, specific security measures in place, along with related audit plans and procedures. As shown in **Figure 6**, below, 45% of the organisations have a specific department/directorate that is responsible for the implementation and evaluation of the security policy, while at the same time only 27% had a similar structure responsible for protection of personal data. The low percentage observed with respect to data protection is because the GDPR was not yet active in Greece at the time that the questionnaire was completed.

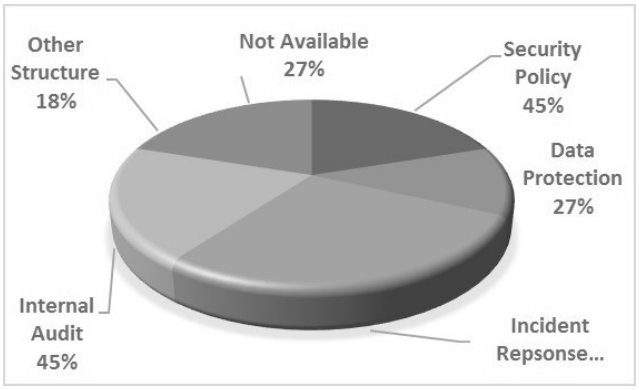


Figure 6: Organisational units

The second part of the questionnaire also focused on investigating the existence of formal security policies, recovery plans, incident handling procedures, or a general framework covering the correct usage of IT equipment, and the dissemination of these to all employees. According to the findings, which are presented in **Figure 7**, below, almost half of the public organisations (45%) do not have any of the aforementioned documents in place, which is an important outcome regarding basic security measures that are missing and should be developed expeditiously.

Respondents recorded the specific technical measures that their organisations are using in order to secure their systems and data, when transmitted or stored in their data centres. Analysis of the data revealed that most of the organisations use a combination of firewalls, anti-spam, anti-virus, and IDS systems, among others. The most common system that almost all participants are using is a firewall; 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 organisations (**Table 1**, p. 103, below). With organisations now having to deal with an exponential growth of mobile devices accessing their networks and the security risks they bring along, it is crucial to have tools that provide visibility, access control, and compliance capabilities. An NAC system can deny network access to non-compliant devices, can place them in a quarantined area, or can give them only restricted access to computing resources, thus keeping insecure nodes from infecting the network (Koh, Oh & Im 2014).

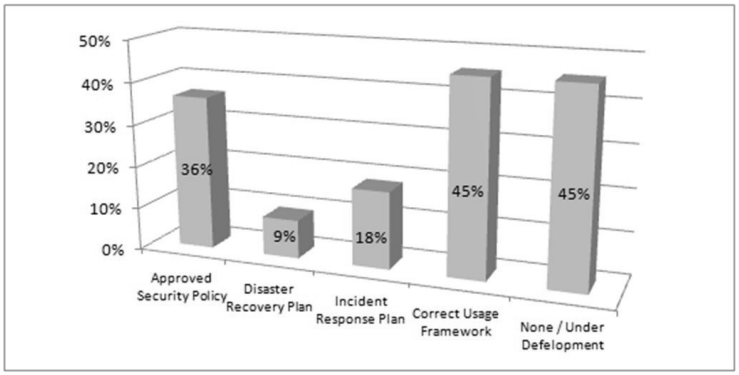


Figure 7: Security policy/recovery plan

Respondents also answered whether they use commercial or open source solutions for implementing the security measures and whether their organisation followed an internal audit procedure and, if so, how often such audits were conducted. Based on the findings (**Figure 8**), most of the organisations follow *ad-hoc* procedures for evaluating legal compliance and for assessing the level of security, as opposed to conducting regular internal or external audits.

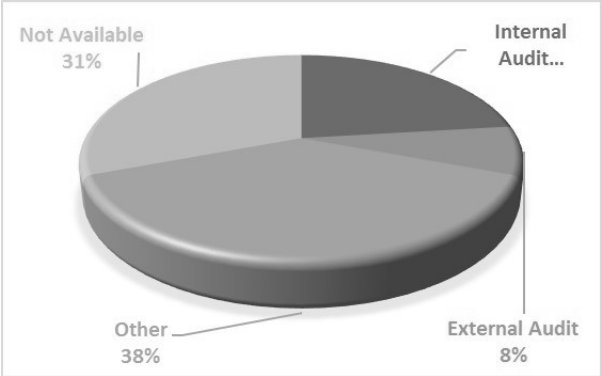


Figure 8: Audits

Encryption is a method for reducing overall risk, although it is not a substitute for other information protection controls, such as physical access, authentication, authorisation, or network controls. The authors, therefore, asked the participants about encryption in their organisations. Important data must be encrypted when transmitted across networks to protect against eavesdropping of network traffic by unauthorised users. Likewise, stored data, especially those that include personal data or passwords, must be encrypted in order to protect them from unauthorised access (Ferrag *et al*. 2018). Based on the findings (**Figure 9**, below) most of the organisations use encryption during transmission (80%) while only 40% use encryption at rest.

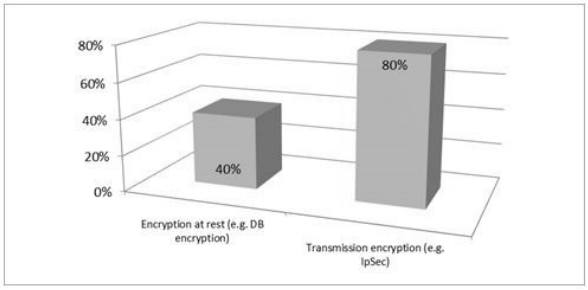


Figure 9: Encryption

Technical Measure	Description	Percentage
Mail protection system	Email Anti-spam / Anti-phishing / Anti mal-ware	82%
Endpoint Anti-virus/ Anti-malware	Active protection against virus and malware infections on computers	82%
Access Control	Centrally managed user access / authentication system	82%
Centrally Managed Backup System	A process that involves automatically replicating data from remote sites and sending it over a network to a main (centralised) location for storage	73%
Software update/patch management	A centrally managed software update management system	45%
NAC/Device Control	A centrally controlled equipment and peripheral device connection system over the internal access network	9%
URL/Content filtering	A centrally managed system to control access to addresses and content types of the Internet	82%
Network Management System (NMS)	The NMS identifies, configures, monitors, up-dates, and troubleshoots network devices in an enterprise network	45%
Event log management	A security information and event management (SIEM) tool for collecting and analysing event data to identify malicious activity	45%
Remote Access Control System	A centralised system for controlling and managing remote connections to the corporate network	55%
Firewall	A network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules	100%
IDS/IPS	A device or software application that monitors a network or systems for malicious activity or policy violations	63%

Table 1: Security measures

Finally, participants were asked about training and certifications that employees of the organisations have received recently in areas related to the security of IT systems, services, and infrastructures. Based on the findings, as shown in **Figure 10**, below, there was a mix of areas where dedicated training, certificates, and degrees were acquired. Infrastructure security related ones reach 73%, and none was reported related to ICS security, which is considered as the most specialised and comprehensive. The level of training/education was not uniform, though. While in several organisations there were several trained staff having most of the aforementioned qualifications, in other organisations this kind of staff was lacking.

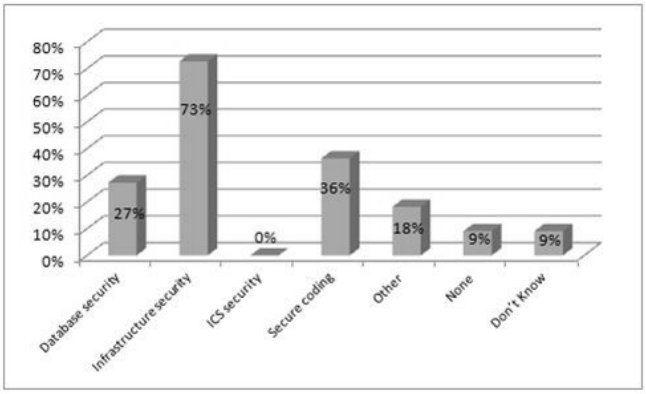


Figure 10: Education

User awareness

User awareness was investigated using the third part of the questionnaire, in terms of relevant policies and mechanisms in place, along with targeted training on new legislative requirements (for example, the NIS directive and GDPR regulation).

Organisations were questioned about the established mechanisms they use to educate their users on security and privacy aspects, covering areas such as new threats, prevention, and reaction practices; legislative requirements; and more. **Figure 11**, below, shows that most organisations (64%) use informal ways of achieving such awareness through online sources in an *ad-hoc* base (such as blogs, mailing lists, or social media) while only 27% use formal and established mechanisms, like specialised conferences and trainings. Meanwhile, 45% reported that there is no structured mechanism for user awareness at all.

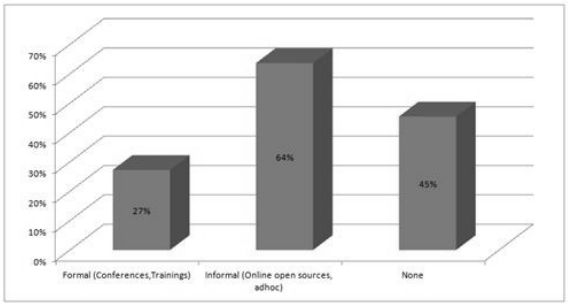


Figure 11: User awareness mechanisms

In **Figure 12**, below, the overall satisfaction in terms of awareness of and preparedness for new legislative requirements (NIS, GDPR) is presented. It was revealed that 45% of the organisations were neither aware nor prepared for them. This is to be expected, since neither was in force when the questionnaire was first issued.

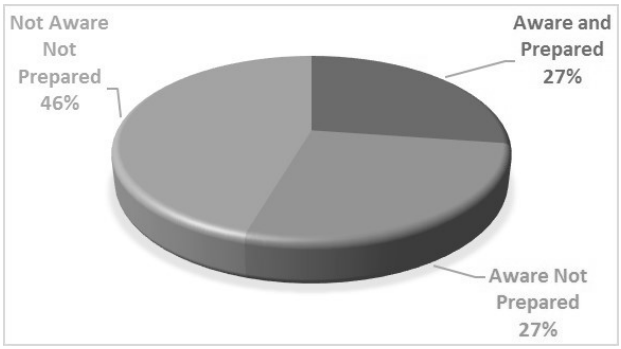


Figure 12: Legislation awareness (NIS, GDPR)

Overall, respondents evaluated the current state of user awareness/training policy in their organisations (**Figure 13**, below). Among them, 55% reported that there was no policy in place and trainings were conducted only by employee's own initiative; and when such a policy existed (remaining 45%) they answered that this was considered inadequate.

Incident response

The final part of the questionnaire was focused on incident response in terms of timely detection, evaluation of impact, and reaction procedures. All organisations 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 that disrupted availability, with 'denial of service' being the most common type of attack (**Figure 14**, below).

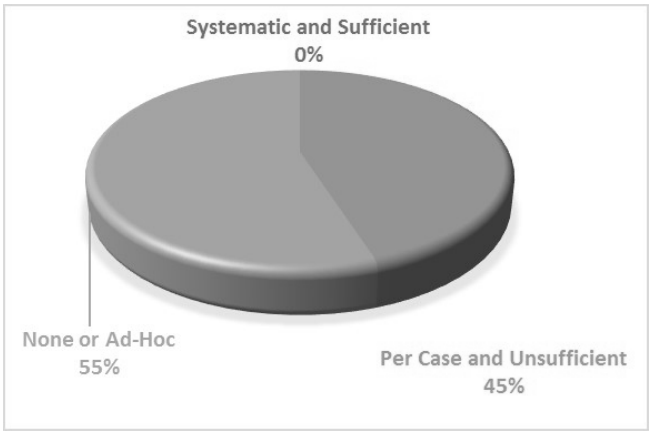


Figure 13: User awareness/training policy

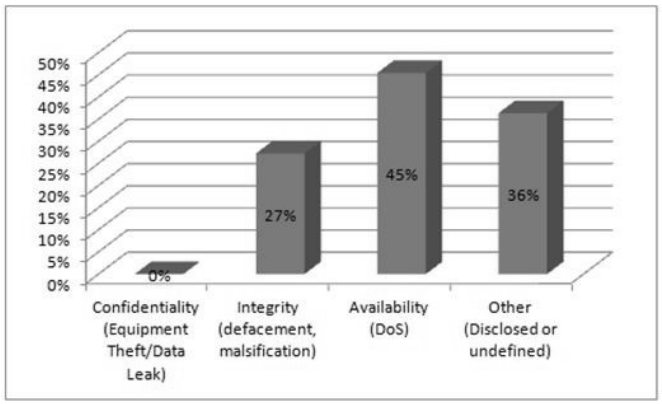


Figure 14: Key security principles affected by incidents (past 12 months)

Concerning threat detection, **Figure 15**, below, shows that 45% regularly reviewed their log files, and 27% tested their systems through vulnerabilities assessments and/or penetration tests regularly (yearly or more frequently). 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 has impacted the ICT environment.

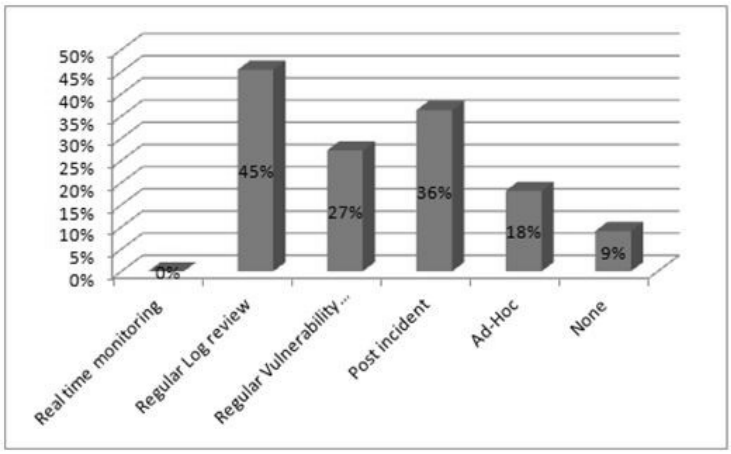


Figure 15: Threat detection

With respect to an incident occurrence, organisations reported that only 27% are following a pre-defined procedure for filing and handling a security incident with predetermined escalation procedures to competent authorities, while the rest are handling the incidents with an *ad-hoc* approach led by the IT department (**Figure 16**, below).

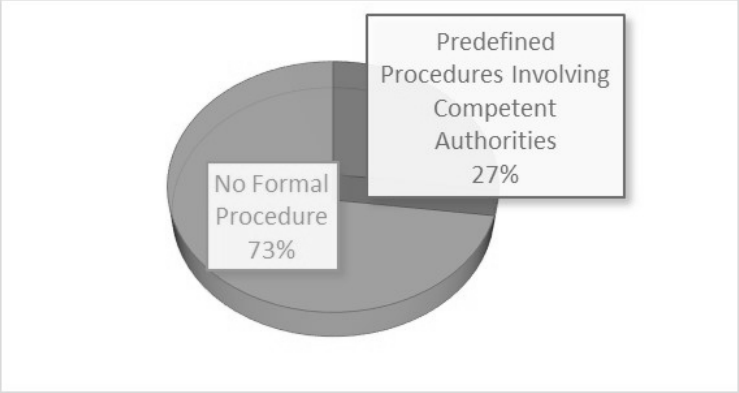


Figure 16: Incident reporting and handling

Further analysis

In order to reveal any dependencies between the different findings of the questionnaire, the authors examined the possibility of using the chi-square test. The value of the chi-square test is that it can reveal whether there is a statistical relationship between the variables in a cross-classification answer table. While the chi-square test is a very useful means of testing for a relationship, it suffers from several weaknesses. One weakness with the test is that it does not indicate the nature of the relationship. Another weakness is the inaccuracy on small sample size. Given that the questionnaire was distributed among a limited number of people (less than 50), the authors decided to use a statistical test called Fisher's exact test (McHugh 2013).

Based on the analysis conducted using Fisher's exact test, it was found that a weak relationship exists between organisations that have all the required software licenses and the relevant maintenance contracts in place for updating them and providing security updates, and those that were affected by a security incident the past 12 months. On the other hand, the data demonstrated a very strong relationship between organisations that carry out information and education activities in order to meet partial needs and those that have a pre-defined recording and response process, which includes (where appropriate) briefing of the relevant authorities (for example, senior management, national CERT, and data protection authorities). These correlations led to two findings. First, education activities, even if they are not carried out in a systematic way, help organisations understand their cyber security needs in terms of establishing necessary incident reporting and incident handling mechanisms. Secondly, organisations that do not yet understand the importance of cyber security do not educate their personnel properly and do not establish procedures that might help them manage and recover after a cyber security incident.

Discussion

Cyberattacks in recent years, especially those targeting systems that keep or process critical information, are becoming more sophisticated. Critical national infrastructures are high value targets of cyberattacks, since essential information or services depend on their systems and their protection becomes a significant issue that is concerning both organisations and nations (Choo 2011). Attacks to such critical systems include penetrating a network and installing malicious tools or programs that can reveal sensitive data or can alter the behaviour of specific physical

equipment (Ten, Manimaran & Liu 2010). To manage this growing trend, academics and industry professionals are joining forces to develop novel systems and mechanisms that can defend their systems.

In December 2018, Greece published national law *L. 4577/2018*. The law incorporated *Directive 2016/1148* of the European Parliament and of the Council into Greek law. Specifically, it incorporated measures for a common, high level of security for network and information systems in Europe. For organisations falling within the scope of the law, Greece's National Cyber Security Authority, in collaboration with the relevant Cyber Security Incident Response Team (CSIRT) and other organisations and entities, perform the following:

- Assess the technical and organisational measures implemented by OES, in order to manage risks related to the security of network and information systems used in their activities, regarding their suitability and their proportionality.
- Assess the suitability of the measures implemented by OES for the avoidance and the minimisation of the impact caused by incidents affecting the security of network and information systems used for the provision of their basic services, aiming to assure their business continuity.

Bearing this in mind, along with the previously mentioned necessity to capture the current security posture, NCSA has issued an initial questionnaire as a pre-audit mechanism (Drivas *et al.* 2019). Analysing the results helped the authors identify the major threats that organisations are facing today, creating a holistic view of the current posture related to cyber security and defining the priorities for strengthening this posture. Although the second part of the questionnaire was mainly focused on technology, such as firewalls, anti-spam, anti-virus, and IDS, it also covered organisational and certification issues. At the same time, the third part was devoted to human factors in terms of awareness and training. Based on this, 45% of the study respondents indicated 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 on a regular basis. Dedicated education programs and awareness campaigns can help strengthen the organisations and the nation against cyberattacks (de Bruijn & Janssen 2017). Most educational programs within the cybersecurity domain are awareness campaigns (Coventry *et al.* 2014). These campaigns typically use lectures or presentations to articulate complex issues to a wide audience, with little tailoring to specific audiences. Experiential learning, on the other hand, 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 comprehending (Kolb 2014).

As stated in the National Cyber Security Strategy, that NCSA 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 an opportunity to handle these like 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 on a regular basis along with the competent CSIRT, the National CERT, and other major stakeholders. NCSA is conducting, hosting, or co-organising

a series of awareness events with the Open Web Application Security Project (OWASP), the Organisation for Security and Cooperation in Europe (OSCE), and other organisations that are related to cyber security; NCSA is also participating in "Panoptis", a cyber security competition organised by the Cyber Defense directorate of the Ministry of Defense. "Panoptis" is an annual exercise begun in 2010; it involves more than 200 people from the armed forces and other security bodies, the academic sector, and public/private research centres. "Panoptis 2019" tested NIS procedures and mechanisms.

Cooperation, both inside Greece and externally with other member states of the EU and beyond, is critical to succeed in the battle against cyberattacks on NCIs to reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs (Boeke, Heinl & Veenendaal 2015) or even to restore peace in the aftermath of cyberwarfare (Robinson *et al*. 2018). NCSA has used this questionnaire as a means of initiating cooperation with relevant stakeholders, creating a list of experts that can work together to solve problems and increase the overall level of cybersecurity. In order to strengthen cooperation in Europe, 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 established by the OSCE for addressing security of and use of Information and Communication Technologies (ICTs); and others. NCSA is also participating in Horizon 2020 (H2020) and national projects related to cyber security such as CONCORDIA (Cyber security cOm-peteNCe fOr Research anD InnovAtion). CONCORDIA is a new, four-year H2020 project begun in January 2019. Its goal is to build a 'cybersecurity competence network' with leading research, technology, industrial, and public competencies, thus creating a secure, resilient, and trusted European computing ecosystem.

Conclusions

Organisations must proactively manage new risks, often while being constrained by regulations such as GDPR and the NIS directive. To cope with new threats, it is essential to develop or reinforce a cybersecurity culture at the organisational level. Before initiating any action, organisations must start by assessing the new risks to which they are exposed. The new EU regulations encourage organisations and member states to comply. However, it is not enough to simply become compliant. Regulations establishing general cybersecurity principles must be applied in the context of each organisation, its mission, and the inherent risks involved. For this reason, NCSA has created a questionnaire as a pre-audit mechanism for government stakeholders in Greece. Using the information collected from the responses, NCSA developed a list of experts, identified the major threats on their systems, and recorded their organisations' current security posture. Consequently, NCSA decided to introduce a common, horizontal security policy along with a set of baseline security requirements for OES and DSP and to implement a model based on Capability Maturity Model Integration (CMMI) that defines different levels of maturity, and against which the security performance of each organisation will be assessed in the near future.

Acknowledgements

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

References

Andreasson, KJ 2011, *Cybersecurity: Public sector threats and responses*, CRC Press.

Ayres, N & Maglaras, L A 2016, 'Cyberterrorism targeting the general public through social media', *Security and Communication Networks*, vol. 9, pp. 2864-75.

Bianco, LJ 2016, *The inherent weaknesses in industrial control systems devices; Hacking and defending SCADA systems*, PhD thesis, Utica College, Utica, NY, US.

Boeke, S, Heinl, CH & Veenendaal, MA 2015, 'Civil-military relations and international military cooperation in cyber security: Common challenges & state practices across Asia and Europe', *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*, IEEE, pp. 69-80.

Choo, K-KR 2011, 'The cyber threat landscape: Challenges and future research directions', *Computers & Security*, vol. 30, pp. 719-31.

Cook, A, Robinson, M, Ferrag, MA, Maglaras, LA, He, Y, Jones, K & Janicke, H 2018, 'Internet of cloud: Security and privacy issues', *Cloud Computing for Optimization: Foundations, Applications, and Challenges*, Springer, pp. 271-301.

Cook, A, Smith, RG, Maglaras, L & Janicke, H 2017, 'Scips: Using experiential learning to raise cyber situational awareness in industrial control system', *International Journal of Cyber Warfare and Terrorism (IJCWT)*, vol. 7, pp. 1-15.

Coventry, L, Briggs, P, Blythe, J & Tran, M 2014, *Using behavioural insights to improve the public's use of cyber security best practices improve the public's use of cyber*, UK Government Office for Science.

de Bruijn, H & Janssen, M 2017, 'Building cybersecurity awareness: The need for evidence-based framing strategies', *Government Information Quarterly*, vol. 34, pp. 1-7.

Drivas, G, Maglaras, L, Janicke, H & Ioannidis, S 2019, 'Cyber security assessment of the public sector in Greece', *18th European Conference on Cyber Warfare and Security (ECCWS 2019)*, Academic Conferences and Publishing International (ACPI).

Evans, M, He, Y, Maglaras, L, Yevseyeva, I & Janicke, H 2019, 'Evaluating information security core human error causes (IS-CHEC) technique in public sector and comparison with the private sector', *International Journal of Medical Informatics*, vol. 127, pp. 109-19.

Ferrag, MA, Maglaras, L, Argyriou, A, Kosmanos, D & Janicke, H 2018, 'Security for 4g and 5g cellular networks: A survey of existing authentication and privacy-preserving schemes', *Journal of Network and Computer Applications*, vol. 101, pp. 55-82.

Koh, EB, Oh, J & Im, C 2014, 'A study on security threats and dynamic access control technology for byod, smart-work environment', *Proceedings of the International MultiConference of Engineers and Computer Scientists*, vol. 2, pp. 1-6.

Kolb, DA 2014, *Experiential learning: Experience as the source of learning and development*, FT Press, Upper Saddle River, NJ, US.

Kovanen, T, Nuojua, V & Lehto, M 2018, 'Cyber threat landscape in the energy sector', *ICCWS 2018 13th International Conference on Cyber Warfare and Security*, Academic Conferences and Publishing International Limited, p. 353.

Maglaras, LA, Drivas, G, Noou, K & Rallis, S 2018, 'NIS directive: The case of Greece.', *ICST: Transportation Security and Safety*, vol. 4, p. e1.

Maglaras, L, Ferrag, MA, Derhab, A, Mukherjee, M, Janicke, H & Rallis, S 2019, 'Threats, protection and attribution of cyber attacks on critical infrastructures', arXiv:1901.03899, Cornell University, Ithaca, NY, US.

McHugh, ML 2013, 'The chi-square test of independence', *Biochemia Medica*, vol. 23, no. 2, pp. 143-9.

Rafferty, B 2016, 'Dangerous skills gap leaves organisations vulnerable', *Network Security*, vol. 2016, pp. 11-13.

Robinson, M, Jones, K, Janicke, H & Maglaras, L 2018, 'An introduction to cyber peacekeeping', *Journal of Network and Computer Applications*, vol. 114, pp. 70-87.

Seker, E & Ozbenli, HH 2018, 'The concept of cyber defence exercises (cdx): Planning, execution, evaluation', *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, IEEE, pp. 1-9.

Ten, C-W, Manimaran, G & Liu, C-C 2010, 'Cybersecurity for critical infrastructures: Attack and defense modeling', *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, vol. 40, pp. 853-65.

Tipton, HF & Nozaki, MK 2007, *Information security management handbook*, CRC Press.

Wood, A, He, Y, Maglaras, L & Janicke, H 2017, 'A security architectural pattern for risk management of industry control systems within critical national infrastructure', *International Journal of Critical Infrastructures*, vol. 13, nos. 2-3.

Authors

B David is a PhD student at ENSAM for (C + V)^o Laboratory. His research is mainly focused on malware analysis, security under Windows operating system, networks, kernel development, and vulnerabilities. He also works in data analysis and design of automatic tools to collect and manage big data. He likes to teach and share knowledge with anyone who asks. He has already participated in several conferences including iAWACS, C0c0n, Ground Zero Summit, EICAR, ECCWS, Defcon, ZeroNight.

M Delong is a PhD student at ENSAM for (C + V)^o Laboratory. His researches are mainly focused on distributed networks, anonymous communications, and blockchain technology. He also works in Open Source INTelligence, design tools for automatic, large-scale data gathering and data analysis. He has already made conferences including ICCWS, ECCWS, FORSE, and C0c0n XII.

G Drivas is the Head of the Network & Information Security Department of the Greek National Cyber Security Authority. He received a B.Sc. in Computer Engineering from the University of West Attica in 2006 and an M.Sc. in Information Security from the University of Piraeus in 2012, where he currently is conducting PhD research in the area of Cybersecurity Governance. He is experienced in the field of ICT and especially in the field of Digital Systems and Information Security, both in the private and the public sector. He has worked in the Banking, Telecommunications, Research & Development, Healthcare and Central Public Administration sectors, with active involvement in issues related to security management, ICT security auditing as well as managing large ICT projects. He has served as national representative to European and international committees (for example, EUNIS Cooperation Group, CEF Taskforce, OSCE, OECD) and has participated to national and European projects on Cybersecurity issues.

Dr. PC Duvenage is an intelligence officer with extensive experience in various aspects of this profession. In the course of his career, he served as an officer in the South African armed forces and in the intelligence services. He holds, in his personal capacity, a Senior Research Fellowship at the Academy for Computer Science and Software Engineering, University of Johannesburg. He has a PhD from the University of Pretoria and a PhD from the University of Johannesburg.

E Filiol is an Associate Professor at ENSIBS, Vannes, an Associate Professor at CNAM, Paris, an associate professor at Moscow's HSE University in the field of information and systems security and a senior consultant in cybersecurity and intelligence. He directed the research of the ESIEA group and its cybersecurity laboratory for 12 years. He spent 22 years in the French Army (Infantry/Marine Groups). He holds an engineering degree in cryptology, a doctorate in applied mathematics and computer science from the École Polytechnique and an authorisation to conduct research (HDR) in information from the University of Rennes. He holds several NATO intelligence certifications. He is the editor-in-chief of the *Journal in Computer Virology and Hacking Techniques* published by Springer. He regularly presents at international conferences in the field of security (Black Hat, CCC, CanSecWest, PacSec, Hack.lu, Brucon, H2HC...). He enjoys walking and hiking and playing the bass guitar (jazz).

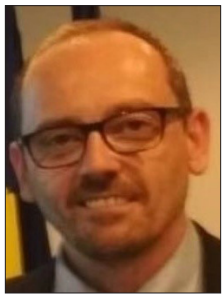
IA Iftimie is the former Information Operations Deputy Chief at the United States Cyber Command, where he was awarded the Defense Meritorious Service Medal for creating "an intelligence community publicly available information strategy for analysts to predict and attribute network exploitations against the Department of Defense Information Networks". He is currently a Doctoral Candidate (ABD) in Vienna, Austria, and holds a Bachelor of Business Administration in International Business from the George Washington University in Washington, D.C.; a Master of Arts (M.A.) in Strategic Security from the National Defense University in Washington, D.C.; and an M.A. in International Security from Bundeswehr University in Munich. He is also a recent graduate of the Harvard Kennedy School Executive Program in Cybersecurity Policies and of the Swedish Defense University. Most recently, he served as a Visiting Research Fellow at a NATO Center of Excellence and has taught numerous courses in the field of critical energy infrastructure security at various universities and defense colleges around the world.

Dr. S Ioannidis received a B.Sc. degree in Mathematics and an M.Sc. degree in Computer Science from the University of Crete in 1994 and 1996, respectively. In 1998, he received an M.Sc. degree in Computer Science from the University of Rochester; in 2005, he received his Ph.D. from the University of Pennsylvania. Ioannidis held a Research Scholar position at the Stevens Institute of Technology until 2007 and since then he is a Principal Researcher at the Institute of Computer Science of the Foundation for Research and Technology - Hellas. His research interests are in the areas of systems and network security, security policy, privacy, and high-speed networks. Ioannidis has authored more than 100 publications in international conferences and journals, as well as book chapters, and has both chaired and served on numerous program committees in prestigious conferences, such as ACM CCS, IEEE S&P, etc. Ioannidis is a Marie Curie Fellow and has participated in numerous international and European projects. He has coordinated several European and National projects (for example, PASS, EUINCOOP, GANDALF, etc.), and currently is the project coordinator of the IB-DAAS and THREAT-ARREST, C4IIOT H2020, and CERTCOOP INEA/CEF European projects.

Prof. H Janicke is the Technical Director of De Montfort University's Cyber Technology Institute. He is the Head of School of Computer Science and Informatics. His interests are covering formal verification techniques and their application to CyberSecurity, SCADA, and Industrial Control System Security as well as aspects of Cyber Warfare. He established DMU's Airbus Group Centre of Excellence in SCADA Cyber Security and Forensics Research in 2013. 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.

VJ Jaquire has been within the field of cyber and information security for over 20 years within government and the private sector focusing on strategy, performance management and operations. He holds an Honours Degree in Management from Henley University and a master's and PhD in Informatics from the University of Johannesburg - specialising in strategies for cyber counterintelligence maturity and the security of cyberspace. He has published various academic papers on cyber strategies and cyber counterintelligence maturity. His professional certifications include CISSP, CISM and CCISO.

L Leenen is an Associate Professor in Computer Science at the University of the Western Cape in South Africa. She worked as a Principal Researcher focusing on defence related research at the Council for Scientific and Industrial Research in South Africa until the end of 2018. Her areas of specialisation are Artificial Intelligence applications in Cyber Defence and mathematical modeling. She is the Chair of the International Federation for Information Processing's Working Group 9.10 on ICT Uses in Peace and War.



Dr. L Maglaras is a Senior Lecturer in the School of Computer Science and Informatics of De Montfort University conducting research in the Cyber Security Centre. He obtained the B.Sc. (M.Sc. equivalent) in Electrical and Computer Engineering from Aristotle University of Thessaloniki, Greece in 1998; M.Sc. in Industrial Production and Management from the University of Thessaly in 2004; and M.Sc. and PhD degrees in Electrical & Computer Engineering from the University of Thessaly in 2008 and 2014, respectively. In 2018, he was awarded a second PhD in Intrusion Detection in SCADA systems from the University of Huddersfield. He served on the Editorial Board of several International peer-reviewed journals such as *IEEE Access, Elsevier ICT Express, and Wiley Journal on Security & Communication Networks*. He is a Senior Member of the Institute of Electrical & Electronic Engineers (IEEE).

J Rajamäki is Principal Lecturer in Information Technology at Laurea University of Applied Sciences and Adjunct Professor of Critical Infrastructure Protection and Cyber Security at the University of Jyväskylä, Finland. He holds a D.Sc. degree in electrical and communications engineering from Helsinki University of Technology, and a PhD in mathematical information technology from University of Jyväskylä.

Dr. T Ramluckan is an academic and researcher in the Information Technology and Governance field and has worked in the Higher Education sector for the past 12 years. In 2017 she graduated with a Doctor of Administration degree in Information Systems & Technology and Public Administration, School of Management, IST and Governance from the University of KwaZulu-Natal. She is currently a post-doctoral researcher in international cyber law at the University of KwaZulu-Natal's School of Law. In addition, she serves on the International Federation for Information Processing (IFIP) working group 9.10 on ICT Uses in Peace and War and the Global Commission on the Stability of Cyberspace (GCSC) Research Advisory Group (RAG). She has contributed to the SABS working group for ISO/IEC standards for information security and is an ISACA South Africa Chapter Academic Advocate at UKZN. She is a reviewer for the *International Journal of Cyber Warfare and Terrorism*, the *Journal of Contemporary Management,* the Annual International Conference on Cyber Warfare and Security and the Annual European Conference on Cyber Warfare and Security.

J van den Berg started studying mathematics and physics at Delft University of Technology in 1970. In 1977, he received the diploma of Mathematical Engineer. From 1977-89, he lectured courses in mathematics, physics, and computer science in institutes of higher education in The Netherlands, and mathematics and physics at the secondary school of Nampula (Mozambique). From 1989-2006, he worked at the Econometric Institute of Erasmus University Rotterdam, lecturing courses in computer science and economics, and did research in computational intelligence, with applications in combinatorial optimisation, finance, agriculture, philosophy, bibliometrics, among others. He finalised his PhD-thesis entitled 'Neural Relaxation Dynamics' in 1996. From 2006 up till now, he works at Delft University of