The role of artificial intelligence (AI) in improving technical and managerial cybersecurity tasks' efficiency

Ruti Gafni
Department of Information Systems, Academic College of Tel Aviv-Yaffo, Tel-Aviv, Israel, and

Yair Levy
College of Computing and Engineering, Nova Southeastern University – Fort Lauderdale/Davie Campus, Fort Lauderdale, Florida, USA

Received 29 April 2024
Revised 15 May 2024
Accepted 17 May 2024

Abstract

Purpose – Artificial intelligence (AI) can assist in the worldwide shortage of cybersecurity workers in technical and managerial roles. Thus, the purpose of this study was to investigate the role of AI in automating many of the routine tasks associated with cybersecurity. As such, AI enables cybersecurity personnel to reduce their workloads and focus on more strategic aspects of their work.

Design/methodology/approach – This study is an exploratory field study. The authors started by conducting a literature review to assess the possibility that AI tools can provide and how they can improve cybersecurity efficacy. Following this, the authors identified the specific core tasks for two cybersecurity work roles (technical and managerial) and searched for specific commercial tools that can perform each of the tasks. Then, the authors used the free ChatGPT 3.5 to list the current cybersecurity systems that use AI for the associated tasks, which the authors then reviewed with the tools' documentation and websites to confirm these tasks were conducted or assisted by AI.

Findings – Results indicated that all 14 cybersecurity tasks of the technical work role are currently noted to be performed by commercial cybersecurity systems with AI-integrated capabilities, while only 11 of the 17 managerial work role tasks currently appear to be performed by AI.

Practical implications – The rapid integration of AI capabilities into commercial cybersecurity systems may suggest that the cybersecurity workforce must be currently trained on how to use AI tools in their daily operations, especially as it pertains to technical cybersecurity work roles.

Social implications – The cybersecurity workforce shortage is reported to exceed four million cybersecurity workers worldwide in 2023. Thus, further understanding of the role of AI in improving the efficiency of technical and managerial cybersecurity tasks is significant.

Originality/value – The value of this research lies in the initial assessment of the current AI capabilities of commercial cybersecurity systems, which will ultimately provide the "super-human" performances resulting from human-AI teaming.

Keywords Cybersecurity tasks efficiency, Artificial Intelligence (AI) for cybersecurity, Cybersecurity workforce productivity, Cybersecurity management

Paper type Research paper

1. Introduction

There is an estimated 625,000 cybersecurity employee shortage in the United States (U.S.) (Cyberseek.org, 2023). Moreover, it is estimated that around 200,000 to 250,000 additional

Information & Computer Security
Vol. 32 No. 5, 2024
pp. 711-728

2056-4961
DOI 10.1108/ICS-04-2024-0102

cybersecurity vacancies are also available at the U.S. Department of Defense (DoD) (DCWF, 2023). Furthermore, according to the Cybersecurity Workforce study of the International Systems Security Certification Consortium, in 2023, there is a shortage of about four million cybersecurity workers worldwide, which increased by 12.6% from the previous year (ISC2, 2023). The recent Whitehouse (2023) National Cyber Workforce and Education Strategy called for significant investments in national programs to increase the production of qualified cybersecurity employees to fill these vacancies. However, such an approach appears to be based on current technologies rather than focusing efforts on research and development to automate many of the current cybersecurity tasks using advanced technologies such as artificial intelligence (AI). In a keynote provided at the Knowledge Management Conference in Geneva, Switzerland, Dr Brian Buckles (2023) stated, "When it comes to cybersecurity workforce shortage, instead of asking for more horses and faster horses, we should ask for a John Deere."

History has provided us with an interesting perspective on how technological advances can greatly enhance productivity. Such technological development takes time and effort. Over the past two centuries, we experienced shorter and shorter times between manual, time-consuming tasks to technologies automating these tasks while doing them faster, cheaper and more effective. This concept can be demonstrated, for example, by agricultural innovations developed by John Deere, such as introducing their tractors to replace manual and horse-powered agricultural processes in cotton picking. Till the mid-19th century, about two-thirds of all worldwide cotton production was produced in the U.S. totally manually. From the early 1920s, John Deere, the U.S. agriculture technology company, has been working on a design of a multirow cotton-picking combine that can collect cotton 525 times faster (or 52,500% more effectively) than handpicking (Bennett *et al.*, 2015; Deere.com, 2023). It took John Deere about 25 years to enhance their combine, whereas in the 1960s, an estimated 96% of all cotton picking in the U.S. was done by machine (Businessmodulehub.com, 2020). According to Bennett *et al.* (2015), "the time required to pick a bale of cotton . . . has decreased from approximately 50 to 70 man-hours [hand-picking] down to eight minutes [machine-based picking]" (p. 226). This type of increased efficiency and time savings is needed in the cybersecurity arena to offset labor shortages.

In 2008, The National Initiative of Cybersecurity Education (NICE) Framework, also known as the Workforce Framework for Cybersecurity, was originally created to help both industry and government to synchronize their cybersecurity workforce by providing a common list of cybersecurity knowledge, skills and abilities that are needed to perform a specific list of cybersecurity tasks associated with the defined work roles. In early 2023, the DoD published the DoD Cyber Workforce Framework (DCWF, 2023), including the 52 NICE Framework work roles and 23 additional work roles in cybersecurity and other cyber-related domains such as software engineering, data analytics and AI. Additionally, the U.S. National Security Agency (NSA) has recognized that the field of cybersecurity can be categorized by both technical and managerial work roles (NSA, 2022). Moreover, according to CyberSeek.org (2023), as of October 2023, there were over 88,000 job openings for the Information Systems Security Manager (OPM ID: 722; NICE ID: OV-MGT-001) and Cyber Defense Analyst (OPM ID: 511; NICE ID: PR-CDA-001), representing about 13.3% of all cybersecurity job openings in the U.S. combined. With the rise and wide use of generative AI, along with technological innovation in the integration of AI into the workforce, especially commercial cybersecurity tools, our initial assumption was that most, if not all, of the core cybersecurity tasks for the two aforementioned work roles, could be automated by AI. Our initial assumption was based on the significant technological innovation that Generative AI such as Chat Generative Pretrained Transformer (ChatGPT) by OpenAI™

and Google Bard™ have demonstrated in recent months, along with the indications provided by many commercial cybersecurity tools that started advertising the integration of Generative AI into their software to aid cybersecurity professionals improved security outcomes, enhanced work role task efficiency and ultimately provide organizational cost-effectiveness. Thus, in this research study, we have started by reviewing prior scientific literature about AI in the context of these two cybersecurity work roles, followed by using the free version of ChatGPT (Ver. 3.5) to assist us with the initial identification of as many commercially available cybersecurity tools as possible that claim to use AI to automate each of the cybersecurity tasks associated with the two work roles. We aimed to provide a current assessment of the role of AI in improving cybersecurity tasks efficiency and to help close the cybersecurity workforce gap. Specifically, this research addressed the following research questions:

RQ1. What key technical and managerial cybersecurity core work role tasks can be automated by AI?

RQ2. What commercial AI vendors, platforms or tools are currently available to automate key technical and managerial cybersecurity core work role tasks?

2. Background

2.1 Cybersecurity and artificial intelligence

Cybersecurity is defined as a "computing-based discipline involving technology, people, information, and processes to enable assured operations. It involves the creation, operation, analysis, and testing of secure computer systems" (CSEC, 2017, p. 16). Cybersecurity also aims to reduce the risks of cyber threats, including malware, phishing, carrier denial attacks, social engineering attacks and man-in-the-middle attacks (Funk, 2022). Cybersecurity and AI must work together to increase cybersecurity awareness within organizations. While cybersecurity threats faced by global businesses are rising in number and sophistication, integrating AI into cybersecurity systems can help reduce such challenges and the burden on cybersecurity personnel (Funk, 2022; Kadel *et al.*, 2022). AI-based approaches for cybersecurity applications appear to be already applied to various tasks, such as access control or user authentication, flexible and continuous network situation awareness, dangerous behavior monitoring, detection of misleading information, data loss prevention, fraud detection, abnormal traffic identification, risk and compliance management, to name a few (Kadel *et al.*, 2022; Krishnappa, 2023; Zhang *et al.*, 2022). According to Kadel *et al.* (2022), businesses use AI to automate cyber protections against different kinds of threats, such as spam and phishing, and to identify malware, fraudulent payments and compromised computers, as well as in forensics investigations. AI's strength is its capability to process and analyze huge quantities of data efficiently, automatically classify it, recognize meaningful patterns and eliminate irrelevant noise (Krishnappa, 2023; Kshetri, 2021; Zeadally *et al.*, 2020; Zhang *et al.*, 2022). By implementing AI, cybersecurity specialists are enabled to respond quickly and mitigate potential threats (Funk, 2022). AI approaches can enhance the performance of conventional slow or insufficient cybersecurity systems to protect efficiently against an increasing range of intricate cyber threats (Kadel *et al.*, 2022). One of the major benefits of AI is that it can learn from experiences and recognize malware even if it was never seen before, enabling proactive protection against potential breaches, even before vulnerabilities are disclosed and rectified to the public, thus stopping them before causing damage. As a result, AI can help address and reduce serious threats such as zero-day vulnerabilities (Kshetri, 2021; Kumar *et al.*, 2023; Tojiboyev and Safoev, 2023).

Furthermore, according to Krishnappa (2023), by examining network traffic and evaluating the oddity of accessed data packets, AI can help identify patterns not easily discovered by humans, such as a potential cyber-attack. AI systems ascertain rules through their training or operation rather than leaning on subject matter experts to devise them, thereby necessitating engineers and programmers to encode the rules into the system (Kroll *et al.*, 2021). Various AI tools can be used to identify and mitigate cyber threats, such as artificial neural networks, expert systems, intelligent agents, machine learning (ML), bio-inspired computing, deep learning and more (Kadel *et al.*, 2022; Krishnappa, 2023). These tools use different types of algorithms or statistical methods to perform their mission, such as decision trees, k-nearest-neighbor algorithms, support vector machines; self-organizing maps and naïve Bayes algorithms (Zeadally *et al.*, 2020). ChatGPT is an advanced AI language model that interacts and communicates with users and generates human-like responses. According to Jeyaraman *et al.* (2023), ChatGPT can be used as a security assistant to investigate and develop security solutions, penetration testing, identify vulnerabilities and correct bugs. Moreover, Al-Hawawreh *et al.* (2023) claim that ChatGPT could be used as a brainstorming tool to generate new ideas related to cybersecurity policy reports, and Ayinde *et al.* (2023) include ChatGPT's capabilities to summarize text, answer questions and to create unbiased automated decision-making systems.

2.2 Artificial intelligence-enabled cybersecurity efficiency

Applying AI can help organizations' management to make better decisions about their business. By automating processes using AI technologies, organizations may save time and substantially boost efficiency while discovering more faults than they could manually, defending against attacks, remediating vulnerabilities that are not even identified or fixed (Krishnappa, 2023; Kumar *et al.*, 2023), assessing customer threats and deciding on customers' ongoing control (Funk, 2022). AI is better and faster than humans to perform repetitive and routine cybersecurity procedures that might fatigue the cybersecurity team (Funk, 2022; Kshetri, 2021) or those requiring collecting and processing large amounts of information, resulting in superior outcomes (Funk, 2022; Kadel *et al.*, 2022; Krishnappa, 2023; Kshetri, 2021; Kumar *et al.*, 2023). The key determinants of AI's efficiency are the quality and quantity of the data the system was trained on (Kshetri, 2021). AI diminishes the cost of breach detection and response, saving between 1% and 15%, with an average of 12% (Kadel *et al.*, 2022). AI thoroughly examines the organization's network to look for any cybersecurity breaches with greater speed and accuracy than human beings, halting cyber-attacks faster (Kshetri, 2021). Signature codes must be compared immediately to identify the cyberattack. Using an AI system, these are done faster, avoiding significant failures and losses (Tojiboyev and Safoev, 2023). ML analyzes existing data and improves over time. Its ability to recognize and detect very small changes from that pattern and to apply them immediately improves its methods and practices continuously (Kadel *et al.*, 2022; Zeadally *et al.*, 2020). Real-time traffic monitoring enables AI technology to immediately detect and act on any unauthorized activity (Tojiboyev and Safoev, 2023). ChatGPT processes natural language prompts and generates responses customized according to the user's requirements and circumstances (Sharma and Dash, 2023). It can be used for searching for diverse, complex and flexible solutions more efficiently and effectively, automatically creating procedures and documents based on common knowledge (Korzynski *et al.*, 2023). AI's efficacy, speed and accuracy allow cybersecurity teams to do their work faster and more effectively instead of spending significant time on manual detection, examining alerts and determining if they are benign or malicious to define their reaction (Kadel *et al.*, 2022). AI optimizes cybersecurity tasks and frees up valuable resources for the organization (Kadel

et al., 2022; Krishnappa, 2023; Kumar *et al.*, 2023). By reducing the time and effort dedicated to policy creation and topography understanding, AI enables cybersecurity teams to focus more on strategic aspects of cybersecurity. This leads to a more robust cybersecurity posture, better threat identification and enhanced protection against cyber threats (Kumar *et al.*, 2023). AI has the potential to support cybersecurity professionals by identifying high-priority areas that need more attention and automating certain tasks that are currently carried out manually, thus reducing their workload and allowing them to focus on more complex and critical tasks. This is especially important when considering the current shortage of cybersecurity professionals worldwide (ISC2, 2023).

2.3 The artificial intelligence cybersecurity workforce revolution

According to the workforce study (ISC2, 2023), while the demand for AI skills is steadily increasing, it is not yet considered as one of the most important requirements for hiring. Skills related to AI are now considered one of the top five categories in terms of in-demand skills. This marks a significant change from the previous year when they were not as highly sought after. As AI technology continues to evolve and impact various areas of cybersecurity threats and defense, the demand for these skills is likely to rise even further in the coming years (ISC2, 2023). AI integration in cybersecurity has displaced workers, as computers' increased efficiency makes them preferable to human experts. Organizations adopting AI in their infrastructures experience increased efficiency and enhanced data security as the technology continuously learns (Tojiboyev and Safoev, 2023). Novel tools and analytical methods simplify the process of distinguishing unusual activities from the typical background. Automated tools can sift through system alerts, forwarding the most critical or actionable items to human operators. These tools realign human tasks, eliminating monotonous incident management and system-state tracking tasks and allowing more time for tool development and other responsibilities (Kroll *et al.*, 2021). AI implementations should be regarded as complex sociotechnical systems rather than simple technical tools. When evaluating their actions, it is essential to consider the human factors, policies and interactions that constitute a larger framework and position specific tools within that environment. Automated systems can exhibit high autonomy or work closely with humans. Certain automated systems are designed to assist human decision-making, like systems prioritizing detected alerts for a Security Operations Center. In contrast, some function independently and make decisions without human intervention, such as firewalls or spam filters (Kroll *et al.*, 2021). According to recent research, generative pretrained transformers (GPT) models are likely to have an impact on the work tasks of around 80% of workers (Ritala *et al.*, 2023). As automation takes over various tasks, there is a possibility that the operators may lose their familiarity with the intricate details of the process. They may become less aware of the specifics of their actions and less competent in understanding or supervising the internal functioning of the automation. This situation can lead to concerns related to the dependability and trustworthiness of the automated process (Kroll *et al.*, 2021). AI exhibits rapid data processing capabilities and excels in recognizing specific scenarios. However, it can be susceptible to disturbances and might not always provide accurate or ethical assessments of novel situations. In contrast, humans are more adaptable and can make swift judgments when confronted with new developments in a network, although they also benefit from machine support to play an auxiliary role (Kroll *et al.*, 2021; Zhang *et al.*, 2022). AI aims to support cybersecurity experts in this domain rather than replacing them entirely. Consequently, it remains essential for experts in the field to step in and apply their network expertise to make informed assessments of the existing network state. AI technology is becoming more significant in promoting automation in the field of

cybersecurity. By automating many of the routine tasks associated with cybersecurity, AI enables cybersecurity personnel to focus on more strategic aspects of their work.

3. Methodology

This study is categorized as a design science, also known as Design and Development research. According to Hevner *et al.* (2004), "Design science … creates and evaluates [Information Technology] IT artifacts intended to solve identified organizational problems" (p. 77). Ellis and Levy (2010) indicated that design and development research is focused on developing an artifact "that can serve to strengthen the interaction in the conceptualization and evaluation cycle" (p. 108). They further indicated that developing "new methods and processes for implementing existing models or using existing tools" (p. 108) constitutes a viable design science artifact. The artifact proposed in this study is the categorization of commercial AI vendors, platforms or tools (*RQ2*) that are currently available to automate cybersecurity core work role tasks (*RQ1*).

To answer the research questions proposed, there is a need to understand the various tasks the cybersecurity workforce copes with. There are two main types of roles in the cybersecurity workforce, technical and managerial roles, which differ in the tasks they perform (NSA, 2022). Therefore, to address *RQ1*, the first step for this study was to identify the roles and specific core tasks for each work role category. Given the magnitude of over 1,000 cybersecurity tasks identified across the 52 work roles in the NICE Framework (NICE Framework Reference Spreadsheet, 2017) and 75 work roles in the DCWF (2023) compounded by the significant cybersecurity workforce shortage (ISC2, 2023), our focus in this study was on the core tasks that are specifically related to two main work roles within the cybersecurity domain. The first is from the managerial cybersecurity aspect, and the second is from the technical cybersecurity aspect. These two work roles are Information Systems Security Manager (OPM ID: 722; NICE ID: OV-MGT-001) and Cyber Defense Analyst (OPM ID: 511; NICE ID: PR-CDA-001), which are critical for any organization. We have identified and used these two work roles as examples to conduct the investigation. The associated core cybersecurity tasks were extracted from the NICE Framework (2017) and the DCWF (2023) to serve as the foundation for addressing *RQ1*. We have assumed at this point that all core cybersecurity tasks for both the technical and managerial work roles can be automated by AI.

The next step in the study addressed *RQ2*, which focused on uncovering the existing commercial AI vendors, platforms or tools that can assist in each technical and managerial cybersecurity work role task. Uncovering such existing commercial AI resources and assessing their ability to use AI to either fully perform, if properly configured, or assist in performing the tasks found in the first step can significantly contribute to the current cybersecurity workforce shortage (ISC2, 2023). To do that, we have unleashed the use of the free ChatGPT version 3.5 to help us generate the data for two tables that will summarize the results of our investigation. We have prompted ChatGPT to provide responses to the specific commercial vendors, platforms or tools that use AI to conduct each core task within the work role. Each of the tasks had its own prompt, following the prompt format: "Which commercial tools use AI to '[tasks]'?" Because of ChatGPT's limitations (Jeyaraman *et al.*, 2023), each commercial tool proposed by ChatGPT was further verified through the commercial company website to confirm its authenticity. The findings of the second step will be analyzed to answer *RQ2* and define what part of the cybersecurity workforce can be empowered by AI tools. Therefore, the significant shortage of human workers in cybersecurity may be reduced, as each worker may empower herself/himself with AI to

form human-AI teams that will ultimately be able to perform the work of a multitude of current cybersecurity workers.

4. Results

The results of the first step, identifying the specific core tasks for both work role categories, are listed in Table 1 for the technical category and Table 2 for the managerial category. Table 1 provides a list of the 14 core cybersecurity tasks from the 2017 NICE Framework in alignment with the 2023 DCWF for the technical work role of Cyber Defense Analyst (OPM ID: 511; NICE ID: PR-CDA-001). Table 2 lists the 17 core cybersecurity tasks from the 2017 NICE Framework in alignment with the 2023 DCWF for the managerial work role. The specific commercial vendors, platforms or tools that use AI to conduct each core task within the identified work role were prompted using the free version of ChatGPT 3.5, which is based on the body of knowledge update as of January 2022.

No.	Task ID NICE	Task ID DCWF	Task description
1	T0023	433	Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources.
2	T0043	472	Coordinate with enterprise-wide cyber defense staff to validate network alerts.
3	T0155	723	Document and escalate incidents (including the event's history, status and potential impact for further action) that may cause ongoing and immediate impact to the environment.
4	T0164	745	Perform cyber defense trend analysis and reporting.
5	T0166	750	Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack.
6	T0178	767	Perform security reviews and identify security gaps in security architecture, resulting in recommendations for inclusion in the risk mitigation strategy.
7	T0198	800	Provide daily summary reports of network events and activity relevant to cyber defense practices.
8	T0214	823	Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts.
9	T0258	956	Provide timely detection, identification and alerting of possible attacks/intrusions, anomalous activities and misuse activities and distinguish these incidents and events from benign activities.
10	T0259	958	Use cyber defense tools for continual monitoring and analysis of system activity to identify malicious activity.
11	T0260	959	Analyze identified malicious activity to determine weaknesses exploited, exploitation methods, effects on system and information.
12	T0293	1,107	Identify and analyze anomalies in network traffic using metadata (e.g. CENTAUR).
13	T0294	1,108	Conduct research, analysis and correlation across a wide variety of all-source data sets (indications and warnings).
14	T0297	1,111	Identify applications and operating systems of a network device based on network traffic.

Source: Created by authors

Table 1. Cybersecurity tasks of the cyber defense analyst (OPM ID: 511; NICE ID: PR-CDA-001)

No.	Task ID NICE	Task ID DCWF	Task description
1	T0147	705	Manage the monitoring of information security data sources to maintain organizational situational awareness.
2	T0157	730	Oversee the information security training and awareness program.
3	T0158	731A*	Participate in an information security risk assessment during the security assessment and authorization process.
4	T0159	733	Participate in the development or modification of the computer environment cybersecurity program plans and requirements.
5	T0192	790	Prepare, distribute and maintain plans, instructions, guidance and standard operating procedures concerning the security of network system(s) operations.
6	T0211	816	Provide system-related input on cybersecurity requirements to be included in statements of work and other appropriate procurement documents.
7	T0215	824	Recognize a possible security violation and take appropriate action to report the incident, as required.
8	T0219	828	Recommend resource allocations required to securely operate and maintain an organization's cybersecurity requirements.
9	T0229	852	Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered.
10	T0234	862	Track audit findings and recommendations to ensure that appropriate mitigation actions are taken.
11	T0248	919	Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals.
12	T0254	947	Oversee policy standards and implementation strategies to ensure procedures and guidelines comply with cybersecurity policies.
13	T0263	962	Identify security requirements specific to an information technology (IT) system in all phases of the system life cycle.
14	T0264	963	Ensure that plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc.
15	T0265	964	Assure successful implementation and functionality of security requirements and appropriate information technology (IT) policies and procedures that are consistent with the organization's mission and goals.
16	T0275	1,016	Support necessary compliance activities (e.g. ensure that system security configuration guidelines are followed, compliance monitoring occurs).
17	T0280	1,032	Continuously validate the organization against policies/guidelines/ procedures/regulations/laws to ensure compliance.

Table 2.
Core cybersecurity tasks of the information systems security manager (OPM ID: 722; NICE ID: OV-MGT-001)

Notes: *Task classified as Core Tasks per NICE Framework (2017), but additional per DCWF (2023)
Source: Created by authors

The core tasks from Tables 1 and 2 were prompted to derive the two sets of results, one for each work role. The results for the second step in the study, which addressed *RQ2*, were provided in Table 3 for Cyber Defense Analyst, a technical role, and Table 4 for Information Systems Security Manager, a managerial role, with the names of the relevant platforms/tools that were identified to perform these indicated tasks, given the table size with the details of each platform/tool. All the tools provided by the different vendors were annotated for each task (the columns of the table). For each vendor, the percent of tasks that have AI tools to assist was calculated (last column). For each task, the number of AI tools that are currently provided was summarized (in the last row of the table).

Cyber Defense Analyst (OPM ID: 511; NICE ID: PR-CDA-001)															
Vendor	Core Tasks and Commercial Tools That Claim To Use AI To Do The Tasks														AI % of total Core Tasks
No. Name	T0023	T0043	T0155	T0164	T0166	T0178	T0198	T0214	T0258	T0259	T0260	T0293	T0294	T0297	
1 Darktrace	Darktrace			Darktrace	Darktrace	Darktrace Cyber AI Platform	Darktrace	Darktrace	Darktrace		Darktrace Cyber AI Platform	Darktrace Enterprise Immune System		Darktrace Enterprise Immune System	71.4%
2 McAfee				McAfee Enterprise Security Manage	McAfee Enterprise Security Manager	McAfee Vulnerability Manage	McAfee Enterprise Security Manage	McAfee Enterprise Security Manager	McAfee Network Security Platform	McAfee MVISION EDR	McAfee Threat Intelligence Exchange		McAfee Enterprise Security Manager (ESM)		64.3%
3 Symantec (now NortonLifeLock)	Symantec (now NortonLifeLock) Network Security			Symantec (now NortonLifeLock) Security Analytics		Symantec (now NortonLifeLock) Security Services	Symantec (now NortonLifeLock) Security Services		Symantec (now NortonLifeLock) Security Services	Symantec (now NortonLifeLock) Endpoint Security	Symantec (now NortonLifeLock) Security Services		Symantec (now NortonLifeLock) Security Services	Symantec (now NortonLifeLock) Network Security	64.3%
4 FireEye	FireEye Network Security	FireEye Helix	FireEye Helix			FireEye Helix			FireEye Network Security	FireEye Endpoint Security	FireEye Threat Intelligence + Mandiant Threat Intelligence (formerly FireEye)			FireEye Network Security	57.1%
5 Fortinet		Fortinet FortiSOAR	Fortinet FortiSOAR	Fortinet FortiSIEM	Fortinet FortiSIEM	Fortinet FortiAI	Fortinet FortiSIEM	Fortinet FortiSIEM	Fortinet FortiGate						57.1%
6 Cisco	Cisco Stealthwatch			Cisco SecureX				Cisco SecureX	Cisco SecureX	Cisco SecureX Endpoint		Cisco Stealthwatch + Cisco Umbrella Investigate		Cisco Stealthwatch	50.0%
7 Splunk		Splunk Phantom	Splunk Phantom	Splunk Enterprise Security	Splunk Enterprise Security		Splunk Enterprise Security	Splunk Enterprise Security					Splunk Enterprise Security		50.0%
8 IBM		IBM Resilient	IBM Resilient	IBM Qradar	IBM Qradar		IBM Qradar	IBM Qradar					IBM Qradar		50.0%
9 Palo Alto Networks	Palo Alto Networks Cortex XDR	Palo Alto Networks Cortex XSOAR+ Demisto (acquired by Palo Alto Networks)	Demisto (acquired by Palo Alto Networks)						Palo Alto Networks Cortex XDR	Palo Alto Networks Cortex XDR				Palo Alto Networks Cortex XDR	42.9%
10 Vectra	Vectra Networks							Vectra Cognito	Vectra Cognito			Vectra Cognito + Vectra Cognito Detect for AWS		Vectra Cognito	35.7%
11 Trend Micro				Trend Micro Deep Security	Trend Micro TippingPoint				Trend Micro Deep Discovery	Trend Micro Apex One					28.6%

Table 3.
Commercial tools that use AI for the 14 core tasks associated with cyber defense analyst (OPM ID: 511; NICE ID: PR-CDA-001)

(*continued*)

Table 3.

12	Fidelis	Fidelis Cybersecurity							Fidelis Elevate			Fidelis Elevate		Fidelis Elevate		28.6%
13	Sumo Logic					Sumo Logic Cloud SIEM		Sumo Logic Cloud SIEM						Sumo Logic Cloud SIEM		21.4%
14	ExtraHop	ExtraHop Reveal(x)											ExtraHop Reveal(x)		ExtraHop Reveal(x)	21.4%
15	Forescout				Forescout Platform		Forescout Platform								Forescout CounterACT	21.4%
16	LogRhythm					LogRhythm Security Information and Event Management (SIEM)		LogRhythm Security Information and Event Management (SIEM)								14.3%
17	SolarWinds				SolarWinds Security Event Manager			SolarWinds Security Event Manager								14.3%
18	AT&T					AlienVault USM (now AT&T AlienVault USM Anywhere)		AlienVault USM (now AT&T AlienVault USM Anywhere)								14.3%
19	Netskope	Netskope Security Cloud				Netskope Security Cloud										14.3%
20	Siemplify (Now Google)		Siemplify	Siemplify												14.3%
21	Cybereason		Cybereason Defense Platform	Cybereason Defense Platform												14.3%
22	D3 Security		D3 Security	D3 Security												14.3%
23	CrowdStrike										CrowdStrike Falcon	CrowdStrike Falcon				14.3%
24	Recorded Future											Recorded Future		Recorded Future		14.3%

(*continued*)

25	Anomali											Anomali		Anomali			14.3%
26	Qualys					Qualys VMDR (Vulnerability Management, Detection, and Response)									7.1%		
27	Tenable					Tenable Nessus Professional									7.1%		
28	Rapid7					Rapid7 InsightVM									7.1%		
29	Microsoft					Microsoft Defender for Endpoint									7.1%		
30	Carbon Black (now VMware):									Carbon Black (now VMware Carbon Black)					7.1%		
31	SentinelOne									SentinelOne					7.1%		
32	Bitdefender									Bitdefender GravityZone Ultra					7.1%		
33	Flowmon												Flowmon		7.1%		
34	Awake Security												Awake Security Platform		7.1%		
35	Gigamon												Gigamon Insight		7.1%		
	Current available	9	8	8	10	10	10	8	9	10	8	7	8	8			

Source: Created by authors

Table 3.

Table 4.
Commercial tools that use AI for the 17 core tasks associated with information systems security manager (OPM ID: 722; NICE ID: OV-MGT-001)

Information Systems Security Manager (OPM ID: 722; NICE ID: OV-MGT-001)																			
Vendor		Core Tasks and Commercial Tools That Claim To Use AI To Do The Tasks																	AI % of total Core Tasks
No.	Name	T0147	T0157	T0158	T0159	T0192	T0211	T0215	T0219	T0229	T0234	T0248	T0254	T0263	T0264	T0265	T0275	T0280	
1	IBM	IBM Qradar		IBM Qradar	IBM Security Guardium			IBM Qradar		IBM Resilient (formerly IBM					IBM Qradar		IBM OpenPages	IBM OpenPages	47.1%
2	Symantec	Symantec (now NortonLifeLock) Security Services		Symantec (now NortonLifeLock) Security Services	Symantec (now NortonLifeLock) Security Services			Symantec Endpoint Detection and Response (EDR)		Symantec (now NortonLifeLock) Security Services					Symantec Security Services	Symantec Control Compliance Suite			41.2%
3	McAfee	McAfee Enterprise Security Manager (ESM)		McAfee MVISION Cloud	McAfee Enterprise Security Manager (ESM)			McAfee MVISION EDR		McAfee MVISION EDR					McAfee MVISION EDR				35.3%
4	FireEye	FireEye Helix		FireEye Helix				FireEye Helix		FireEye Helix					FireEye Helix	FireEye Helix			35.3%
5	ServiceNow										ServiceNow GRC		ServiceNow GRC		ServiceNow GRC	ServiceNow GRC	ServiceNow GRC	ServiceNow GRC	35.3%
6	RSA										RSA Archer		RSA Archer		RSA Archer	RSA Archer	RSA Archer	RSA Archer	35.3%
7	Trend Micro	Trend Micro Deep Security		Trend Micro Cloud One	Trend Micro Deep Security					Trend Micro Deep Security					Trend Micro Deep Security				29.4%
8	LogRhythm	LogRhythm Security Information and Event Management (SIEM)		LogRhythm Security Information and Event Management (SIEM)						LogRhythm NextGen SIEM					LogRhythm NextGen SIEM	LogRhythm NextGen SIEM			29.4%
9	MetricStream										MetricStream GRC Platform		MetricStream GRC Platform			MetricStream	MetricStream + MetricStream Compliance Management	MetricStream	29.4%
10	Fortinet	Fortinet FortiSIEM			Fortinet Security Fabric			Fortinet FortiSIEM		Fortinet FortiSOAR									23.5%
11	Splunk	Splunk Enterprise Security + Splunk Phantom			Splunk Enterprise Security			Splunk Enterprise Security								Splunk Enterprise Security			23.5%
12	Palo Alto Networks							Palo Alto Networks Cortex XSOAR		Palo Alto Networks Cortex XSOAR					Palo Alto Networks Cortex XSOAR	Palo Alto Networks Cortex XSOAR			23.5%
13	Lockpath										Lockpath Keylight GRC Platform		Lockpath Keylight GRC Platform				Lockpath Keylight GRC	Lockpath Keylight GRC	23.5%
14	Forescout			Forescout Platform						Forescout CounterACT					Forescout CounterACT				17.6%
15	SolarWinds	SolarWinds Security Event Manager		SolarWinds Security Event Manager												SolarWinds Security Event Manager (formerly Log & Event Manager)			17.6%
16	CrowdStrike							CrowdStrike Falcon							CrowdStrike Falcon Remediation	CrowdStrike Falcon			17.6%
17	LogicGate												LogicGate GRC				LogicGate GRC	LogicGate GRC	17.6%
18	ZenGRC												ZenGRC				ZenGRC	ZenGRC	17.6%
19	Resolver												Resolver Core				Resolver Core	Resolver Core	17.6%
20	Darktrace	Darktrace Enterprise Immune System						Darktrace Enterprise Immune System											11.8%

(*continued*)

21	Cisco	Cisco SecureX		Cisco SecureX																			11.8%
22	Vectra	Vectra Cognito					Vectra Cognito																11.8%
23	AT&T	AlienVault USM (now AT&T AlienVault USM Anywhere)	AlienVault USM (now AT&T AlienVault USM Anywhere)																				11.8%
24	Cybereason	Cybereason Endpoint Detection and Response							Cybereason Endpoint Detection and Response														11.8%
25	Anomali						Anomali ThreatStream		Anomali ThreatStream														11.8%
26	Qualys		Qualys Vulnerability Management														Qualys Vulnerability Management						11.8%
27	Tenable		Tenable														Tenable.io+ Nessus						11.8%
28	Exabeam		Exabeam Security Management Platform						Exabeam Security Management Platform														11.8%
29	Micro Focus Fortify		Micro Focus Fortify														Micro Focus Security ArcSight						11.8%
30	NopSec Unified VRM		NopSec Unified VRM															NopSec Unified VRM					11.8%
31	Securonix						Securonix Security		Securonix Security														11.8%
32	Nintex								Nintex Promapp		Nintex Promapp												11.8%
33	VComply										VComply								VComply				11.8%
34	AltoCloud										AltoCloud Policy Management								AltoCloud Compliance Management				11.8%
35	Kenna Security																Kenna Security	Kenna Security					11.8%
36	CyberGRX																	CyberGRX	CyberGRX				11.8%
37	BWise																		BWise	BWise			11.8%
38	SAP																		SAP GRC	SAP GRC			11.8%
39	Wolters Kluwer																		Enablon by Wolters Kluwer	Enablon by Wolters Kluwer			11.8%
40	Navex Global																		NAVEX Global + NAVEX One	NAVEX One			11.8%

(*continued*)

Table 4.

Table 4.

41	ProcessUnity																			ProcessUnity	ProcessUnity	11.8%
42	Netwrix Auditor																			Netwrix Auditor	Netwrix Auditor	11.8%
43	Sumo Logic	Sumo Logic Cloud SIEM																				5.9%
44	Netskope	Netskope Security Cloud																				5.9%
45	Rapid7			Rapid7 InsightVM																		5.9%
46	Carbon Black									Carbon Black (VMware Carbon Black) EDR												5.9%
47	Bitdefender	Bitdefender GravityZone Ultra																				5.9%
48	LogPoint	LogPoint SIEM																				5.9%
49	Elastic Security	Elastic Security																				5.9%
50	Check Point	Check Point CloudGuard																				5.9%
51	Tufin			Tufin Orchestration Suite																		5.9%
52	RiskSense			RiskSense																		5.9%
53	Trustwave			Trustwave Security Testing Services + Trustwave SpiderLabs																		5.9%
54	Imperva			Imperva Incapsula																		5.9%
55	Cynet					Cynet 360																5.9%
56	ACL										ACL GRC											5.9%
57	Galvanize										Galvanize HighBond											5.9%
58	Comply Advantage													Comply Advantage								5.9%
59	Ncontracts													Ncontracts								5.9%
60	Nlyte													Nlyte Asset Explorer								5.9%
61	Ansible																		Ansible			5.9%
62	Open Policy Agent (OPA)																		Open Policy Agent (OPA)			5.9%
63	ArcherDX																		ArcherDX			5.9%
64	Compliance.ai																			Compliance.ai	Compliance.ai	5.9%
65	LogicManager																			LogicManager	LogicManager	5.9%
66	Quantivate GRC																			Quantivate GRC	Quantivate GRC	5.9%
	Current available	20	0	19	7	0	0	13	0	14	7	0	13	0	15	16	17	17				

Source: Created by authors

Our results indicated that all 14 core cybersecurity tasks of the technical work role are currently indicated to be performed by at least 7 tools, while 6 of the 17 total core cybersecurity tasks of the managerial work role have no evidence of current AI tools that can perform these tasks. Specifically, for the 11 managerial tasks which are AI-assisted, 7 to 20 tools are provided. However, six tasks do not have even a single AI tool that can assist in performing these tasks. IBM is the vendor with the larger number of tasks covered (47.1%), and Symantec is the second with 41.2%. Nevertheless, most vendors cover less than 18% of the tasks. For all the 14 technical tasks, at least seven different AI tools currently exist. Darkface is the vendor with the largest number of tasks covered (71.4%), and 8 of the 35 vendors cover more than 50% of the tasks. It appears that commercial tools to perform highly managerial and organizational cybersecurity strategies are less common as these are typically the tasks that, until January 2022 (ChatGPT 3.5), appear to fall under the purview of cybersecurity professionals.

5. Conclusions

Automation has the potential to free up humans from monotonous, repetitive or high-attention-demanding tasks, thus providing them with more opportunities for strategic thinking, expediting decision-making, plan implementation and cybersecurity management. As a result, professionals can enhance their efficiency, completing existing tasks with greater precision while gaining the capacity to undertake new responsibilities. The potential implications of AI technologies for cybersecurity are immense. Using various AI tools based on different techniques, technologies and algorithms can assist with many of the different tasks of technical and managerial cybersecurity roles. Nonetheless, these are the first steps of evolution, while commercial companies are developing more and more specific tools, which appear to focus first on the technical cybersecurity tasks. Thus, it reduces overall organizational costs as it can take over repetitive tasks, resulting in using fewer cybersecurity professionals and enabling them to focus on other more strategic and managerial tasks that AI tools currently appear to shy away from. Combining human expertise and machine intelligence is important to leverage the synergies of both humans and machines. Cybersecurity professionals can be more effective in their work with AI-enabled cybersecurity platforms as it helps minimize the time and effort necessary to perform those tasks. We predict that the evolution of AI tools, especially those based on GPT, will simplify the tasks of managerial roles too. However, these platforms may introduce risks, such as biases, privacy breaches and more, that organizations using them must be aware of.

6. Future research

While our work here is preliminary, our study brings several interesting points that should be addressed in future research. Specifically, given the existing use of AI within the technical work role, future research should further assess how much efficiency is occurring. It is important to know that, as of the current state of AI integration, it is unclear to what extent AI and GPT are actually helping professionals become more efficient in what they do or if they cause individuals to actually spend more time trying to figure out how to seek the help of AI to do the tasks they wish it to do. Academic institutions must look closer at the current state of AI usage in cybersecurity and develop opportunities for students during their academic degrees to build their human-AI teaming skills, especially for those seeking to engage in future cybersecurity work

roles. One initial national effort in that direction is led by the NSA in collaboration with the National Science Foundation in establishing the criteria for what students should be required to learn and what competencies are expected from them when graduating from an NSA-designated CyberAI program (https://www.towson.edu/cyberai). The second interesting point where future research may help is to seek empirical results on how much of the labor deficiency is being offset by existing AI tools. Such results can provide predictions and trends in closing the gap for the cybersecurity work shortage. The third point for future research is to help assess the future labor demands, especially in the technical aspect of cybersecurity, given the evolution and trends in using AI tools, as found in our studies, primarily for technical tasks. In summary, future research should help us address the anticipated level of efficiency gained by the use of AI, what is the number of cybersecurity vacant jobs that will be reduced by AI and what will be the future workforce requirements.

References

Al-Hawawreh, M., Aljuhani, A. and Jararweh, Y. (2023), "Chatgpt for cybersecurity: practical applications, challenges, and future directions", *Cluster Computing*, Vol. 26 No. 6, pp. 3421-3436, doi: 10.1007/s10586-023-04124-5.

Ayinde, L., Wibowo, M.P., Ravuri, B. and Emdad, F.B. (2023), "ChatGPT as an important tool in organizational management: a review of the literature", *Business Information Review*, Vol. 40 No. 3, pp. 137-149., doi: 10.1177/02663821231187991.

Bennett, J.M., Woodhouse, N.P., Keller, T., Jensen, T.A. and Antille, D.L. (2015), "Advances in cotton harvesting technology: a review and implications for the John Deere round baler cotton picker", *The Journal of Cotton Science*, Vol. 19, pp. 225-249. https://www.cotton.org/journal/2015-19/2/upload/JCS19-225-CORRECTED.pdf

Buckles, B. (2023), "Rethinking innovation: creative destruction in the information age", *Proceedings of the 2023 Knowledge Management Conference (KM2023),* p. 11. www.iiakm.org/conference/proceedings/KM2023_RefereedProceedingsAbstracts.pdf

Businessmodulehub.com (2020), "History of John Deere cotton pickers", available at: https://www.businessmodulehub.com/blog/history-of-john-deere-cotton-pickers/

CSEC (2017), "Cybersecurity curricular guideline", Joint Task Force on Cybersecurity Education (JTF), available at: https://cybered.acm.org/

Cyberseek.org (2023), "Cybersecurity supply/demand heat map", available at: https://www.cyberseek.org/heatmap.html

DCWF (2023), "DoD cyber workforce framework (DCWF)", available at: https://dodcio.defense.gov/Cyber-Workforce/DCWF/

Deere.com (2023), "Cotton harvesters", available at: https://www.deere.com/en/harvesting/cotton/

Ellis, T.J. and Levy, Y. (2010), "A guide for novice researchers: design and development research methods", *Proceedings of the InSITE 2010: Informing Science+ IT Education Conference, Cassino*, Vol. 10, pp. 107-118, doi: 10.28945/1237.

Funk, P. (2022), "Artificial intelligence and cybersecurity implications for business management", *Journal of International Scientific Publications, Economy and Business*, Vol. 16, pp. 252-261, doi: 10.6084/m9.figshare.21550926.v1.

Hevner, A.R., March, S.T., Park, J. and Ram, S. (2004), "Design science research in information systems", *Management Information Systems Quarterly*, Vol. 28 No. 1, pp. 75-105.

ISC2 (2023), "Cybersecurity workforce study 2023", International Systems Security Certification Consortium (ISC2), available at: https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf

Jeyaraman, M., Ramasubramanian, S., Balaji, S., Jeyaraman, N., Nallakumarasamy, A. and Sharma, S. (2023), "ChatGPT in action: harnessing artificial intelligence potential and addressing ethical challenges in medicine, education, and scientific research", *World Journal of Methodology*, Vol. 13 No. 4, p. 170, doi: 10.5662/wjm.v13.i4.170.

Kadel, R., Shrestha, H., Shrestha, A., Sharma, P., Shrestha, N., Bashyal, J. and Shrestha, S. (2022), "Emergence of AI in cyber security", *International Research Journal of Modernization in Engineering Technology and Science (IRJMETS)*, Vol. 4 No. 12, pp. 1820-1834, doi: 10.56726/IRJMETS32643.

Krishnappa, T. (2023), "A review on artificial intelligence techniques in preventing cyber threats", *International Journal of Engineering Applied Sciences and Technology*, Vol. 8 No. 1, pp. 185-189.

Korzynski, P., Mazurek, G., Altmann, A., Ejdys, J., Kazlauskaite, R., Paliszkiewicz, J., ... Ziemba, E. (2023), "Generative artificial intelligence as a new context for management theories: analysis of ChatGPT", *Central European Management Journal*, Vol. 31 No. 1, pp. 3-13, doi: 10.1108/CEMJ-02-2023-0091.

Kroll, J.A., Michael, J.B. and Thaw, D.B. (2021), "Enhancing cybersecurity via artificial intelligence: risks, rewards, and frameworks", *Computer*, Vol. 54 No. 6, pp. 64-71.

Kshetri, N. (2021), "Economics of artificial intelligence in cybersecurity", *IT Professional*, Vol. 23 No. 5, pp. 73-77, doi: 10.1109/MITP.2021.3100177.

Kumar, S., Gupta, U., Singh, A.K. and Singh, A.K. (2023), "Artificial intelligence: revolutionizing cyber security in the digital era", *Journal of Computers, Mechanical and Management*, Vol. 2 No. 3, pp. 31-42, doi: 10.57159/gadl.jcmm.2.3.23064.

NSA (2022), "National security agency", National Centers of Academic Excellence in Cybersecurity - Cyber Defense (CAE-CD), available at: https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/

NICE Framework (2017), "Workforce framework for cybersecurity (NICE framework)", NIST SP 800-181 Rev. 1, available at: https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/workforce-framework-cybersecurity-nice

NICE Framework Reference Spreadsheet (2017), available at: https://www.nist.gov/document/supplementnicespecialtyareasandworkroleksasandtasksxlsx

Ritala, P., Ruokonen, M. and Ramaul, L. (2023), "Transforming boundaries: how does ChatGPT change knowledge work?", *Journal of Business Strategy*, Vol. 45 No. 3.

Sharma, P. and Dash, B. (2023), "Impact of big data analytics and ChatGPT on cybersecurity", Proceedings of the 4th International Conference on Computing and Communication Systems (I3CS) (pp. 1-6). *IEEE*. 10.1109/I3CS58314.2023.10127411

Tojiboyev, I. and Safoev, N. (2023), "The influence and limitations of AI in cybersecurity domain", *Texas Journal of Engineering and Technology*, Vol. 18, pp. 53-59.

Whitehouse (2023), "National cyber workforce and education strategy", available at: www.whitehouse.gov/wp-content/uploads/2023/07/NCWES-2023.07.31.pdf

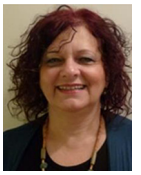
Zeadally, S., Adi, E., Baig, Z. and Khan, I.A. (2020), "Harnessing artificial intelligence capabilities to improve cybersecurity", *IEEE Access*, Vol. 8, pp. 23817-23837, doi: 10.1109/ACCESS.2020.2968045.

Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., ... Choo, K.K.R. (2022), "Artificial intelligence in cyber security: research advances, challenges, and opportunities", *Artificial Intelligence Review*, Vol. 55 No. 2, pp. 1-25, doi: 10.1007/s10462-021-09976-0.

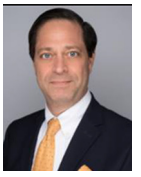
Further reading

DCWF Tool, available at: https://public.cyber.mil/wid/dcwf/

About the authors



Ruti Gafni, PhD, is an Associate Professor, Dean and establisher of the School of Information Systems at The Academic College of Tel Aviv Yaffo, with BSc studies including specialties in Cybersecurity, Digital Innovation and Gamification, and MSc studies including specialties in Data Science and Digital Transformation. She holds a PhD from Bar-Ilan University, Israel (in the Business Administration School), focusing on Information Systems, an MSc from Tel Aviv University, in Information Systems Management, and a BA (Cum Laude) in Economics and Computer Science from Bar-Ilan University. She has more than 40 years of practical experience as a Software Project Manager and Analyst of information systems. Her research interests include cybersecurity and new technology adoption.



Yair Levy, PhD, is a Professor of Information Systems and Cybersecurity at the College of Computing and Engineering at Nova Southeastern University, the Director of the Center for Information Protection, Education and Research (CIPhER) (http://infosec.nova.edu/) and chair of the Cybersecurity Curriculum Committee at the college, along with serving as the Director of the MS and PhD programs in Cybersecurity. He conducts innovative research on the "human factor" in cybersecurity, including social engineering and supply chain cybersecurity. Levy authored numerous peer-reviewed journal articles, conference proceedings, book chapters and other publications. His scholarly research has been cited over 8,000 times. Dr Levy was trained in 2015 by the Federal Bureau of Investigation (FBI) on various topics and actively serves as a Board Member of the FBI-affiliated InfraGard South Florida chapter and serves as the Education Sector Chief. Additionally, he has been serving as the National Colead for the National Security Agency (NSA)'s Community of Practice in Cyber Defense (CoP-CD) (https://www.caecommunity.org/community-of-practice/cyber-defense). He is an active member of the Florida Department of Law Enforcement South Florida Cybercrime Working Group (SFCWG) as part of the Florida Fusion Centers. He consults local, state and federal government agencies on cybersecurity topics. He is also a frequently invited keynote speaker at national and international meetings, as well as regular media interviews as a subject matter expert (SME) on cybersecurity topics. Read more about Dr Levy at: https://sites.nova.edu/levyy/. Yair Levy is the corresponding author and can be contacted at: levyy@nova.edu