National Cybersecurity Strategies in the Healthcare Industry of Israel and the Netherlands: A Comparative Overview

Stefan Weenk

The rapid pace of society's technological innovations has created a set of transformative opportunities in the healthcare industry, notably elevating the quality of life while subsequently serving as a permeable arena for cybercriminals. The core function of healthcare is maintaining people's well-being and, in some cases, it constitutes a meaningful portion of national economic output. Growing cybersecurity risks to the critical infrastructure sector pose a threat to national security, prompting government response. This study compares the current national cybersecurity strategies and regulations used by Israel and the Netherlands to protect the healthcare sector against cyber threats and presents recommendations for future strategies and regulations.

Keywords: Healthcare industry, technology, national cybersecurity strategies and regulations, Internet of Medical Things (IoMT), critical infrastructure sector

Introduction

The healthcare sector has been one of the beneficiaries of the mounting technological advancements;[1] its purpose and operations are central to people's

Stefan Weenk earned a BA degree in Security Management Studies from Saxion University of Applied Sciences, Netherlands. He is a former research intern in the Cyber Security program at the INSS.

[1] Sanjay Poonen, "Health Care Innovation Harnessing New Technology to Benefit Patients," *Forbes*, April 2, 2018, https://www.forbes.com/sites/forbestechcouncil/2018/04/02/health-care-innovation-harnessing-new-technologies-to-benefit-patients/#4d7afdf45a88.

wellness and, in some instances, representative of a significant portion of national economic output.[2] Emerging technologies and digitization play an instrumental role in the development of related products, services, and research, benefiting patients and providers. The integration of genetics and biology with big data and Artificial Intelligence—referred to as the "medical automation and information revolution"—has had an enhancing effect in research, revolutionizing drug production, personalized medicine, and clinical workspaces, and has altered the practical delivery of diagnosis and care.[3] Digitized health increases efficiency and effectiveness of medical systems, improving prescription management, remote healthcare, monitoring, and clinical operations.[4] Added value is further achieved by geographic scope, demonstrative of the Da Vinci Surgical Systems, or the use of robotic systems aiding surgeons to perform delicate operations from different locations.[5] The convergence of emerging technologies, information systems, and interconnected medical devices and networks, referred as the Internet of Medical Things (IoMT), is developed in disruptive and critical ways across healthcare systems.[6]

Cybersecurity Risks in the Healthcare Industry

A byproduct of the progress in digital health is the coinciding risk of IoMT and medical devices, as well as digital medical applications, software, information

[2] "Health Care and Cyber Security: Increasing Threats Require Increased Capabilities," *KPMG* (September 2015), 1–6; "Critical Infrastructure Sectors," *US Department of Homeland Security (CISA)*, February 2, 2019, https://www.dhs.gov/cisa/critical-infrastructure-sectors; "Critical Infrastructure Sectors," *European Cooperation Network on Critical Infrastructure Protection (euconcip)*, March 15 2019, https://www.euconcip.org/; Lior Tabansky, "Critical Infrastructure Protection against Cyber Threats," *Military and Strategic Affairs* 3, no. 2 (2011): 61–78.

[3] "2018–2019 Innovation in Israel Overview," *Israel Innovation Authority* (January 14, 2019): 60–62; Poonen, "Health Care Innovation Harnessing New Technology To Benefit Patients."

[4] Deloitte Center for Health Solutions, *Connected Health How Digital Technology Is Transforming Health and Social Care* (London: Deloitte Center of Health Solutions, 2015), 1–40; "2018–2019 Innovation in Israel Overview."

[5] Interview with Eliav N., November 25, 2018.

[6] Safi Oranski, "Obstacles on the Path to Comprehensive IoMT Security," *Cyber MDX*, November 26, 2018, https://www.cybermdx.com/blog/obstacles-on-the-path-to-comprehensive-iomt-security.

systems, and security devices (firewalls and anti-virus).[7] Subsequently, these can jeopardize data, including organizational intellectual property, such as medical research, experiments, and findings; financial and billing information associated with electronic funds transfer (EFT); and patient information and medical history associated with electronic health records (her) or electronic medical records (EMR).[8] Ultimately, this will compromise the stability of healthcare operations and service delivery and will cause substantial cost in damages and settlements, harming the welfare of the people.[9]

To demonstrate the reality of the security weakness in medical infrastructure, researchers at Ben-Gurion University Cyber Security Research Center in Israel developed a malware that exploits vulnerabilities of medical imaging devices, such as CT and MRI machines, as well as the networks that process the scans. In the blind study, the altered CT scans—depicting cancerous nodes—deceived accomplished radiologists in misdiagnosing the conditions.[10] To the extent of public knowledge, this scenario has yet to transpire to the effect of directly causing injury or death. Most cyberattacks affecting the healthcare sector involve data breaches of electronic health records (EHR), caused by network vulnerabilities of hospitals, healthcare service providers such as insurance companies, and related supply-chain actors.[11]

[7] Aurore Le Bris and Walid El-Asri "State of Cybersecurity & Cyber Threats in Healthcare Organizations Applied Cybersecurity Strategy for Managers," ESSEC Business School posted by Jean-Loup Richet on *Journal of Strategic Threat Intelligence*, January 10, 2017, https://blogs.harvard.edu/cybersecurity/2017/01/10/cybersecurity-cyber-threats-in-healthcare-organizations/; Barbara Filkins, *Health Care Cyberthreat Report* (SANS Institute and Norse, February 2014), 1–42; "Health Care and Cyber Security: Increasing Threats Require Increased Capabilities."

[8] Le Bris and El-Asri "State of Cybersecurity & Cyber Threats in Healthcare Organizations Applied Cybersecurity Strategy for Managers"; Filkins, *Health Care Cyberthreat Report*; "Health Care and Cyber Security: Increasing Threats Require Increased Capabilities."

[9] Le Bris and El-Asri "State of Cybersecurity & Cyber Threats in Healthcare Organizations Applied Cybersecurity Strategy for Managers"; Filkins, Health Care Cyberthreat Report; "Health Care and Cyber Security: Increasing Threats Require Increased Capabilities."

[10] Kim Zetter, "Hospital Viruses: Fake Cancerous Nodes in CT Scans, Created by Malware, Trick Radiologists," *Washington Post*, April 3, 2019, https://www.washingtonpost.com/technology/2019/04/03/hospital-viruses-fake-cancerous-nodes-ct-scans-created-by-malware-trick-radiologists/.

[11] Le Bris and El-Asri, "State of Cybersecurity and Cyber Threats in Healthcare Organizations Applied Cybersecurity Strategy for Managers"; Filkins, *Health Care Cyberthreat Report*.

An estimated quarter of all data breaches in the United States occur in the healthcare industry.[12] A notable case was illustrated by a new group of hackers discovered by Symantec in early 2015, referred to as Orangeworm. They deployed Kwampirs, a tailored malware targeting systems affecting computers of healthcare providers and third-party vendors across several sectors that provide services to the health industry, gaining unauthorized access to EHR and medical imaging devices, such as MRI and X-ray equipment.[13] In 2018, a phishing attack against staff email accounts at the Wisconsin-based UnityPoint Health resulted in the data breach of 16,000 patients, followed by a second attack on its business systems, resulting in the data breach of 1.4 million patients.[14] From 2015 to 2018, hackers targeted the Singapore state-health database, exploiting the records of 1.5 million patients including those of Prime Minister Lee Hsien Loong.[15] In 2018, the computer of an employee at the New York-based Med Associates, a healthcare billing claims vendor, was comprised, and more than 270,000 patients' records were exposed.[16] During the same year, the Missouri-based Cass Regional Medical Center, Blue Springs Family Care, and LabCorp were hit with ransomware attacks, preventing the use of their communication systems and EHR systems.[17] In June 2017, the computer networks of two to three hospitals were reportedly

[12] Poonen, "Health Care Innovation Harnessing New Technology to Benefit Patients."

[13] Jessica Davis, "New Hacking Group Targeting Healthcare Infects Mri, X-Ray Machine," *Healthcare IT News,* April 24, 2018, https://www.healthcareitnews.com/news/new-hacking-group-targeting-healthcare-infects-mri-x-ray-machine; Security Response Attack Investigation Team, "New Orangeworm Attack Group Targets the Healthcare Sector in the U.S., Europe, and Asia," *Symantec*, April 23, 2018, https://www.symantec.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia.

[14] Jessica Davis, "1.4 Million Patient Records Breached in Unitypoint Health Phishing Attack," *Healthcare IT News*, July 13, 2018, https://www.healthcareitnews.com/news/14-million-patient-records-breached-unitypoint-health-phishing-attack.

[15] Jessica Davis, "Hackers Breach 1.5 Million Singapore Patient Records, Including the Prime Minister's," *Healthcare IT News*, July 20, 2018, https://www.healthcareitnews.com/news/hackers-breach-15-million-singapore-patient-records-including-prime-ministers.

[16] Jessica Davis, "270,000 Patient Records Breached in Med Associates Hack," *Healthcare IT News*, June 20, 2018, https://www.healthcareitnews.com/news/270000-patient-records-breached-med-associates-hack.

[17] Jessica Davis, "Update: Ransomware Attack on Cass Regional Shuts down HER," *Healthcare IT News*, July 11, 2018, https://www.healthcareitnews.com/news/update-ransomware-attack-cass-regional-shuts-down-ehr; Jessica Davis, "Ransomware, Malware Attack Breaches 45,000 Patient Records," *Healthcare IT News*, July 26, 2018, https://www.healthcareitnews.com/news/ransomware-malware-attack-breaches-45000-patient-records.

breached in Israel, although Israel's National Cyber Directorate confirmed only two, in fact, were attacked, resulting in the removal of fifty outdated and exposed computers.[18]

Regulation in the Healthcare Sector in Israel and the Netherlands

During the CyberMed seminar held at the Cybertech Tel Aviv conference in January 2019, the cybersecurity of the Israeli healthcare systems was deemed below par and unprepared for the pervasive threat to health communication networks, devices, and to the organizations as a whole. According to the director of Hadassah University Hospital, essential critical infrastructure is in compliance; yet for other elements, such as remote devices, the cybersecurity level is less resilient. The shift toward digital health propelled by emerging technologies and connectivity creates new challenges with a wider scope, threating the reputation of healthcare organizations.[19]

In comparison, in 2015, only 56 percent of the Dutch hospitals met the standards for information security in the healthcare industry (NEN-7510120).[20] Since May 2017, the measures have been binding and compliance has been a prerequisite across the healthcare industry in order to gain access to citizen service numbers.

The rising number of cyberattacks targeting networks and devices throughout the critical infrastructure sector endangers the utility and trust of healthcare providers and services. These attacks have led to initiatives to enhance the organizational resilience and robustness across the healthcare arena, including in organizations servicing the industry, and to amending a national cyber security strategy.

National Cybersecurity Strategies

Cybersecurity has materialized as an integral domain of organizational security, defined by the technology corporation CISCO as "the practice of

[18] Globes Correspondent, "Cyber Attack Hits Israeli Hospitals," *Globes*, June 29, 2017, https://en.globes.co.il/en/article-cyber-attack-hits-israeli-hospitals-1001194803; Judy Siegel-Itzkovich and Sharon Udasin,"Cyber Attacks Hit Israeli Hospitals as Globe Battles New Computer Virus," *Jerusalem Post*, June 29, 2017, https://www.jpost.com/Israel-News/Israel-thwarts-hackers-from-cyber-attack-on-hospitals-498256.

[19] Ami Rojkes Dombe, "CyberMed: Cyber Threats and Challenges in Healthcare," *Israel Defense*, January 28, 2019, https://www.israeldefense.co.il/en/node/37255.

[20] CPB Netherlands Bureau for Economic Policy Analysis, *Cyber Security Assessment (CSRA) for the Economy* (The Hague: CPB Netherlands Bureau for Economic Policy Analysis, 2017), 1–41.

protecting systems, networks, and programs from digital attacks."[21] In 2011, "Ten National Cyber Security Strategies: A Comparison" was presented at the International Conference on Critical Information Infrastructure Security (CRITIS), wherein it described that "[at both the European level and] international level a harmonized definition of Cyber Security is clearly lacking."[22]

The formulation of national security strategies within the European Union is relatively recent and can be traced to the early 2000s. Establishing these strategies encourages policymakers to identify strategic objectives and provide a guide on how to reach those strategic objectives. A well-known statement in the security sector is that "cybersecurity is only as strong as the weakest link."[23] An organization can have the best cybersecurity structure, which can be, nonetheless, counter-productive without a comprehensive cybersecurity risk management system.[24] The cybersecurity evolution—the trail of events that catalyzed Dutch and Israeli cyber resolutions—requires clarification in order to understand the essence of both nations' current cybersecurity strategies. The strategy comparison will focus on how the Netherlands and Israel confront cybersecurity challenges and how both nations distinguish properties linked to cybersecurity policies.

The following criteria are based on the fundamental topics in the "NCSS Good Practice Guide"[25] and the research conducted by Luiijf and others[26] and will be used to compare the national cybersecurity strategies of Israel and the Netherlands. The first key issue is **risk governance at a strategic and national level**. One strategy of an organization is creating a wide-ranging master plan, which explains how the mission and objectives will be

[21] "What is Cybersecurity," *CISCO*, December 2, 2018, https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html.

[22] H.A.M. Luiijf, Kim Besseling, Maartje Spoelstra, and Patrick de Graaf, "Ten National Cyber Security Strategies: A Comparison," in *Critical Information Infrastructure Security*, ed. Sandro Bologna, Bernhard Hämmerli, Dimitris Gritzalis, and Stephen Wolthusen (Berlin: Springer, 2013), 1–17.

[23] Niels Nagelhus Schia, "'Teach a Person How To Surf': Cyber Security as Development Assistance," *Norwegian Institute of International Affairs*, no. 4 (2016): 1–36.

[24] Gabi Siboni and Hadas Klein, "Guidelines for the Management of Cyber Risks," *Cyber, Intelligence, and Security* 2, no. 2 (2018): 23–38.

[25] European Union Agency for Network and Information Security (ENISA), *NCSS Good Practice Guide, Designing and Implementing National Cyber Security Strategies* (Heraklion: ENISA, 2016), 1–59.

[26] Luiijf, Besseling, Spoelstra, and de Graaf, "Ten National Cyber Security Strategies: A Comparison."

achieved. The second key issue is the **national regulatory environment**, which is part of the overall national strategy of governments. The third key issue is major **stakeholders of the national cybersecurity strategies**. Moreover, this includes information about the landscape of the stakeholders, representative of multiple disciplines, who are involved in the process of developing the national cybersecurity strategy. The fourth key issue is the **definition of critical infrastructures and critical objects**. The final key issue **is cyber intelligence and cybersecurity awareness**. This section will expand on activities of cyber intelligence agencies and government bodies as they relate to resources availed to healthcare institutions and increasing cybersecurity awareness on a national level.

Risk Governance at a Strategic and National Level

The first key issue applied in analyzing a national cybersecurity strategy is risk governance. Risk governance offers organizations and states potential benefits and opportunities. Development of risk governance enables organizations and their environment to change while minimizing the negative consequences of the associated risks.

Risk Governance in Israel

Over the past decade, Israel's risk governance has shifted from its initial focus on the protection of computerized information infrastructures and databases prescribed by regulations to a more direct approach of protecting cyberspace with civil-military strategic interactions and public-private cooperation.[27] Although organizations face many challenges in cyber systems, academic and government programs are actively developing new operation and technical solutions that will improve the countermeasures and response to attacks.[28] In 2016, the National Cyber Directorate and the Ministry of Health implemented MedSOC, a security operations center for the medical industry. MedSOC probes attacks in the healthcare sector and publishes relevant information on its network; moreover, the portal is supported by

[27] Michael Raska, *Confronting Cybersecurity Challenges: Israel's Evolving Cyber Defense Strategy* (Singapore: S. Rajaratnam School of International Studies, January 2015), https://www.rsis.edu.sg/wpcontent/uploads/2015/01/PR150108_-Israel_Evolving_Cyber_Strategy_WEB.pdf.

[28] "Cyber Security Risk Governance," *International Risk Governance Council* (October 2015), 1–33.

the Computer Emergency Response Team (CERT-IL) under the National Cyber Directorate.[29]

Domestic regulation in Israel references international standards, in accordance to Government Resolution 2443 "Advancing National Regulation and Governmental Leadership in Cyber Security." Generally, all organizations are recommended or required to meet ISO/IEC 27001 and ISO 15408, the applicable standards for "organizational information security management systems" and evaluation measures for information technology security, respectively.[30] Designated organizations are required to meet additional measures based on national critical infrastructure criteria and the regulatory body. In 2012, the Ministry of Health issued Government Circular 18/2012, subjecting all healthcare organizations and associated service providers to comply with ISO 27799. It provided parameters in respect to the entity's "information security risk environment in selection, implementation, and management of controls," regarding "organizational information security standards and information security management practices."[31] The Ministry of Health has developed advanced healthcare certification together with the Standards Institution of Israel by adopting common criteria of other ISO standards.[32]

Medical equipment is manufactured with locked systems, hindering access to operating systems. Leading the National Cyber Directorate's medical research lab together with the Ichilov Hospital in quality regulations (government provided) testing of medical devices, the National Cyber Directorate provides knowledge and equipment, while Ichilov provides the

[29] Interview with Eliav N., November 25, 2018.

[30] Eli Greenbaum, "Israel Chapter on Cybersecurity – Getting the Deal Through," *Yigal Arnon & Co. Law Firm*, February 1, 2018, https://www.arnon.co.il/member/4358/articles; ISO/IEC 27001: 2013 Information technology- Security techniques- Information security management systems- Requirements," ISO, October 2013, https://www.iso.org/standard/54534.html; "ISO/IEC 15408–1:2009 Information technology-Security techniques-Evaluation criteria for IT security-Part 1: Introduction and general model," ISO, January 2014, https://www.iso.org/standard/50341.html.

[31] Greenbaum, "Israel Chapter on Cybersecurity-Getting the Deal through," "ISO 27799:2008 Health informatics- information security management in health using ISO/IEC 27002," ISO, July 2008, https://www.iso.org/standard/41298.html; "ISO 27799:2016 Health informatics- Information security management in health using ISO/IEC 27002," ISO, July 2016, https://www.iso.org/standard/62777.html.

[32] Interview with Yaniv P., January 6, 2019.

testing space. The assessments include a penetration test, network connectivity, and a vulnerability test.[33]

Risk Governance in the Netherlands

In 2018, in response to the opportunities and risks as a result of the digitization of the healthcare industry in the Netherlands, in addition to other challenges of data privacy and the Internet of Things (IoT),[34] Z-CERT was founded. The establishment was part of an initiative of the Dutch Association of Hospitals (Nederlandse Vereniging van Ziekenhuizen), the Dutch Federation of University Medical Centers (Nederlandse Federatie van Universitair Medische Centra), the Common Health Service Netherlands, and the Dutch National Cyber Security Center (NCSC). Z-CERT offers specialized services to healthcare institutions by providing in-depth knowledge of medical networks, applications, and devices.[35]

Medical devices must be assessed before admitted to the market, in order to determine whether the devices have been produced in accordance with the requirements of Directive 93/42/EEC and Directive 2007/47/EC regarding medical devices. Most of the development of medical devices is designed according to privacy and security principles, which means that the company that develops the medical devices has to pay attention to privacy-enhancing measures, also known as privacy-enhancing technologies (PET), as does the supply-chain vendors.[36]

Information security is the responsibility of the individual healthcare institution. The standards NEN 7510 and NEN 7512, which hospitals have to meet, ensure how information security and privacy can be achieved. Every hospital has to decide which standard best suits the risk environment of the hospital, with the exception of the statutory standards.[37]

The National Regulatory Environment

In order to regulate and reinforce cybersecurity measures in the healthcare industry, governments create regulations, requiring the healthcare industry to implement proper cybersecurity measures. Implementing regulations in

[33] Interview with Eliav N., November 25, 2018.
[34] Interview with Hessel B., December 17, 2018.
[35] Interview with Hessel B., December 17, 2018.
[36] Interview with Hessel B., December 17, 2018.
[37] Interview with Hessel B., December 17, 2018.

the healthcare industry by placing the liability upon the organizations—as a result of rising lawsuits and fines for non-compliance by governmental agencies—creates greater cooperation.

Regulations in Israel

To ensure that public and private organizations can act upon cybersecurity threats, it is necessary to establish an (inter)national regulatory environment and/or an appropriate policy framework to frequently evaluate the strategies and objectives for cybersecurity and adjust them accordingly. Israel has implemented several privacy and cybersecurity protection laws since 1981 to deal with general privacy protection. Key regulations are the Privacy Protection Act of 1981;[38] the amended Privacy Protection Act of 2001;[39] Resolution 3611 of Advancing National Cyberspace Capabilities in 2011;[40] and Resolution 2444 of Advancing the National Preparedness for Cyber Security in 2015.[41] In 2018, the Israeli government published a draft in Hebrew of its cybersecurity law and issued a call for public comment. It represents years of consultation and debate concerning Israel's approach to cybersecurity and will combine cybersecurity legislation and policy with several new innovations.[42]

The Privacy Protection Act (PPA) constitutes the main regulation of Israeli data protection law. The law has two elements: The first is the general privacy protection and the second deals specifically with databases and is much closer to "informational" data protection law.[43] The PPA developed over time and has been amended nine times since it was first adopted in 1981. In 2001, the PPA introduced additional regulations, replicating European data protection terms and creating greater harmony with European standards.

The Israeli Law, Information and Technology Authority (ILITA) was created by government decision no. 4660 and established within the Ministry of Justice in September 2006. The mission of ILITA is to reinforce personal data protection, regulate the use of electronic signatures, and increase the

[38] Ian Bourne, *A Guide to Data Protection in Israel* (Israeli Law, Information and Technology Authority [ILITA], January 2010).

[39] Bourne, *A Guide to Data Protection in Israel.*

[40] "Resolution 3611—Advancing National Cyberspace Capabilities," *Israel's Prime Minister's Office* (August 7, 2011), 1–6.

[41] Deborah Housen-Couriel, *National Cyber Security Organisation: Israel* (Tallinin: Cyber Defense Center of Excellence NATO, 2017).

[42] Bourne*, A Guide to Data Protection in Israel.*

[43] Greenbaum, "Israel Chapter on Cybersecurity—Getting the Deal Through."

enforcement of privacy and IT-related offenses. ILITA also acts as a central knowledge base within the government for technology-related legislation and governmental IT large projects, such as eGov.[44] In 2011, resolution 3611 created the National Cyber Bureau (NCB), which was established to strengthen protection of critical national infrastructure, and regulate powers and responsibilities in the cyber realm.[45]

In 2012, the Ministry of Health published Circular 18/2012, which requires all healthcare institutions to obtain certification under ISO 2779. It also requires all service providers that hold either medical information or information regarding the infrastructure of the institution to comply with the standards of ISO 27799. [46]

Regulations in the Netherlands

To understand the Dutch national cybercrime and information security laws, it is useful to map the history of legislation leading up to the current (inter) national regulatory environment and/or an appropriate policy framework. With respect to cybercrime legislation in the Netherlands, the key regulations are the Computer Crime Act (Wet computercriminaliteit) of 1993[47] and the Computer Crime II Act (Wet computercriminaliteit II) of 2006; and the recent amendment resulting in the Computer Crime III Act.[48]

Informational privacy or data protection violations could be prosecuted on the basis of data interference (Article 350a of the Dutch Criminal Code[49]), but the Netherlands has no specification in its criminal law that specifically addresses data protection violations. The Data Protection Act (Wet bescherming

[44] “Resolution 3611—Advancing National Cyberspace Capabilities.”

[45] Interview with Eliav N., November 25, 2018; Greenbaum, “Israel Chapter on Cybersecurity—Getting the Deal Through.”

[46] Deborah Housen-Couriel, “A Look at Israel’s New Draft Cybersecurity Law,” The Federmann Cyber Security Center Cyber Law Program The Hebrew University of Jerusalem (first appeared on Net Politics, published by the Council on Foreign Relations), August 5, 2018,https://csrcl.huji.ac.il/people/look-israels-new-draft-cybersecurity-law-new-draft-cybersecurity-law.

[47] Government of the Netherlands: Ministry of Justice and Security, “Computer Crime Act” (October 28, 1993), 1–33 [Dutch].

[48] The Government of the Netherlands: Ministry of Justice, “Computer Crime Act II,” (July 4, 2006), 1–2 [Dutch]; The Government of the Netherlands: Ministry of Justice and Security “Computer Crime Act;” (October 8, 2018), 1–33 [Dutch].

[49] “Dutch Criminal Code,” *Official Publication of the Kingdom of the Netherlands* (April 22, 2015): 165 [Dutch].

persoonsgegevens) of 2000[50] is mainly enforced by administrative measures given by the government and was updated in 2015 to ensure that data leaks are reported by organizations and to extend the administrative power of the Dutch Data Protection Board (College bescherming persoonsgegevens).[51]

At the international level, the Netherlands, a member of the European Union, implemented the "Council Framework Decision 2005/222/JHA . . . on attacks against information systems" of February 2005. As a result of attacks against information systems and increased threats from organized crime, the European Union replaced the Framework Decision with "Directive 2013/40/EU . . . on attacks against information systems" in August 2013.[52]

The first EU-wide legislation specifically focusing on cybersecurity is called the Directive on Security of Network and Information Systems (NIS Directive). It provides legal measures to boost the overall level of cybersecurity and synchronizes cybersecurity policies between nations, ultimately to support the society and economy by enhancing digital readiness and minimizing cyber incidents. The preparation of the General Data Protection Regulation (GDPR) took four years before it was finally approved by the EU Parliament on April 14, 2016. The aim of the GDPR is to protect all EU citizens from privacy and data breaches. The main differences with the new GDPR and the previous directive are its extended EU-wide jurisdiction and fines for organizations that breach the GDPR regulations.[53] Designating a data protection officer (DPO) in the Netherlands is only mandatory if the organization meets the requirements of the GDPR. Each controller or processor is required to appoint a DPO if the organization is a government body or another public organization and in cases where processing includes (a) large-scale regular

[50] "The Data Protection Act," *Official Publication of the Kingdom of the Netherlands* (July 6, 2000): 1–25 [Dutch].

[51] "Amendment of the Data Protection Act," *Official Publication of the Kingdom of the Netherlands* (June 4, 2015): 1–8 [Dutch].

[52] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems," *Official Journal of the European Union* (March 16, 2005): 67–71; "Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA," *Official Journal of the European Union* (August 14, 2013): 8–14.

[53] "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)," *Official Journal of the European Union* (May 4, 2016): 1–88.

and systematic monitoring of individuals, or (b) large-scale processing of sensitive personal data.[54]

Key Stakeholders of the National Cybersecurity Strategy

It is important to recognize the relevant stakeholders within the healthcare industry, as those who are involved in primary processes in the healthcare institutions. The all-inclusive national cybersecurity strategies of relevant stakeholders aid in achieving an optimized level of situational awareness, and in turn increase the yields of all strategy factors.[55]

Stakeholders in Israel

Israel is one of the pioneers of stakeholder cybersecurity cooperation among government institutions, academia, and private-sector organizations. Cybersecurity cooperation is a natural extension of the already-existing pattern of national cooperation in other areas,[56] and is reflected in one of Israel's flagship initiatives, the CyberSpark Innovation Initiative project in Be'er Sheva.

A multi-stakeholder process enables bringing together the appropriate and relevant actors. The context and scope of the strategy process, in particular the stage, helps significantly to determine the stakeholder profile. The organization responsible in this development of the national cybersecurity strategies in Israel is the National Cyber Directorate, involving stakeholders from three categories—the national sphere, civilian sphere, and national-international organizations—all relevant to the strategy's aim. The national sphere comprises government ministries and agencies that have knowledge and are associated with the healthcare industry, legislation, and cybersecurity. Stakeholders from the civilian sphere include the Israeli police and its national cyber unit, as well as academic entities. The national-international sphere includes the healthcare institutions, health maintenance organizations (HMOs), and international standardization organizations, among others.

Internal stakeholders include the chief information security officers (CISO), representatives from the IT divisions, and management in the

[54] Global Legal Group, *The International Comparative Legal Guide to Data Protection 2018* (n.p.: Global Legal Group, 2018).

[55] Alexander Klimburg, ed. *National Cyber Security Framework Manual* (Tallinin: NATO CCD COE 2012).

[56] "A Look at Israel's New Draft Cybersecurity Law."

healthcare institutions. The Israeli healthcare industry is confronted with several international standards related to cyber information security; hence, it is beneficial to involve actors spanning branches of responsibility and knowledge within the framework of preparing a national cybersecurity strategy for the healthcare industry.

Stakeholders in the Netherlands

The Dutch cabinet created the National Cyber Security Strategy 2 (NCSS2) together with a wide range of public and private organizations, knowledge institutions, and civil society organizations. With the creation of the NCSS2, the government is shaping an integrated approach to cyber crime, which it announced in the coalition agreement.

On January 1, 2012, the Cyber Security Council (CSR) was formed in the Netherlands. The CSR is an independent advisory body composed of the Dutch cabinet and high-ranking representatives from public and private-sector organizations.[57] The Dutch government can depend on a wide range of public-private partnerships for the creation of a comprehensive and sound healthcare-related national cybersecurity strategy in the future. Two cooperatives, the Dutch healthcare-Information Sharing and Analysis Center (ISAC), and Z-CERT ensure that the healthcare industry is better protected by sharing information, ranging from cyberattacks across sectors and capability trends, among others.

Cyber diplomacy is another objective in the Netherlands' National Cybersecurity Strategy and aims to develop a hub for expertise on international law and cybersecurity. The hub will promote peaceful use of the digital domain and will bring together international experts and policymakers, diplomats, military personnel, and NGOs to share knowledge with existing institutes. International experts include those from the European Cybercrime Center 3 (EC3 – Europol) and Interpol Global Complex for Innovation (IGCI), which is a research development facility.[58]

[57] Government of the Netherlands, "The National Cyber Security Center (NCSC) bundles knowledge and expertise," January 12, 2012, https://www.government.nl/latest/news/2012/01/12/the-national-cyber-security-center-ncsc-bundles-knowledge-and-expertise.

[58] Annegret Bendiek, "The European Union's Foreign Policy Toolbox in International Cyber Diplomacy," *Cyber, Intelligence, and Security* 2, no. 3 (2018): 57–71.

Critical Infrastructures and Critical Objects

Understanding an organization's assets is not only necessary from a strategic business perspective but also from a (cyber) security perspective. Assets can be defined as tangible and intangible resources and capabilities that enable an organization to achieve its strategic objectives.[59]

Critical Infrastructure in Israel

The National Cyber Security Authority (NCSA) within the Prime Minister's Office, created the "cyber defense methodology for an organization" in June 2017. Protecting organizations within Israel is a component of its national defense concept, focused on protecting the Israeli economy and its vital components against any disruption. The NCSA's document supports organizations to define and map their assets, create risk assessment, and inspect their current cybersecurity systems. Israel's national cybersecurity strategy clearly focuses on mapping the critical and secondary assets of an organization and its links to suppliers. The supply chain is one of the greatest risks for an organization. As dependence on third-parties becomes increasingly critical in the healthcare industry, organizations are compelled to enhance and adapt their risk management processes.

A risk assessment of healthcare institutions conducted by the Ministry of Health revealed that some institutions depend on multiple systems supported by one external provider (third-party or supplier). The ministry also discovered that most of the Israeli hospitals are using the same system of this provider.[60] "The National Cyber Directorate is creating a healthcare-specific cyber strategy with a number of stakeholders to address the rising threat against cyberattacks in the healthcare sector," according to a representative from the agency.[61]

Critical Infrastructure in the Netherlands

The Dutch national cybersecurity strategy is developed to create a well-defined governance model with a dynamic balance between security, freedom, and social-economic benefits. At the same time, the Dutch government has tried to adapt the responsibilities that apply in physical security to cybersecurity

[59] Mark Frigo and James Hurley, "Understanding Your Organization's Genuine Assets," *Strategic Finance,* February 2014.

[60] Interview with Yaniv P., January 6, 2019.

[61] Interview with Eliav N., November 25, 2018.

and intends to do that by creating a dialogue with organizations that deal with cyber threats. The Dutch government is currently not active in creating conditions and measures for the cybersecurity of supply chain of businesses or the healthcare industry, but a proposal for European legislation creates conditions and measures for ICT products and services.[62] Moreover, there is currently no healthcare-specific cybersecurity strategy to defend healthcare institutions against cyberattacks. From a national perspective, Dutch and European legislation, standards, and information protection authorities form the defensive layer.

Cyber Intelligence and Cybersecurity Awareness

In an effort to combat cyber threats and make organizations more aware of the risks, both Israel and the Netherlands focus on cyber intelligence and cybersecurity awareness in their critical infrastructure, as both nations have started to understand the objectives and effects of sophisticated and damaging attacks on the critical infrastructure.

Cyber Intelligence and Cybersecurity Awareness in Israel

The healthcare industry has not reached an optimized level of situational awareness in terms of the dangers for its networks and medical devices. In essence, negligence in addressing vulnerabilities and updating software makes healthcare institutions the perfect target.[63] Cyber intelligence for the healthcare industry is mainly delivered through government institutions, while the Ministry of Health collects cybersecurity information through a multitude of sources (i.e., government bodies, civic organizations, and international organizations).[64] The Ministry of Health has encouraged healthcare institutions to connect to its cyber intelligence services, free of charge, for extra protection.

Israel's MedSOC was created by the National Cyber Directorate and the Ministry of Health to provide information about cyberattacks in the healthcare industry and share information through the MedSOC network. Currently, MedSOC is connected only to hospitals, although it is expected

[62] Interview with Tom S., December 19, 2018.

[63] Patricia Williams and Andrew Woodward, "Cybersecurity Vulnerabilities in Medical Devices: A Complex Environment and Multifaceted Problem," *Dove Press Journal*, no. 8 (2015): 305–316.

[64] Interview with Yaniv P., January 6, 2019.

to be connected to all healthcare institutions within the next five years.[65] Additionally, the Israeli government commits to fostering resources and efforts across educational institutions and to reinforcing cybersecurity efforts in the technology sector.

Cyber Intelligence and Cybersecurity Awareness in the Netherlands

Large organizations in the private sector in general are adequately focused on cybersecurity awareness, and most are aware that cyberattacks can cause damage to property; however, they can also damage the organization's image. The Dutch government has held meetings with other nations in the European Union to discuss if it should be mandatory for organizations to address cybersecurity for hardware and software.[66] Although the government has invested much in raising awareness for digital threats, a renewed approach is needed, focused more on stimulating and facilitating organizations to take action to improve online security. At the end of 2017, the Ministry of Economic Affairs and Climate Policy and the Ministry of Justice and Security jointly launched the "Digital Trust Center" (DTC) program. The DTC's mission is to increase the resilience of businesses to cyber threats with a focus on two key tasks. Its first task is to provide businesses with reliable and independent information on digital vulnerabilities and concrete advice on the action they should take. Its second task is to foster cybersecurity alliances between businesses.[67]

Comparative Findings

Both the national cybersecurity strategies of Israel and the Netherlands have similar aims of protecting cyberspace against their adversaries and enhancing cyber resilience. However, both countries' cyber threat landscape, socio-political conditions, security trends, traditions, the level of cyber awareness, among other components, have caused significant variations in the cybersecurity approaches of the two countries.[68]

[65] Interview with Eliav N., November 25, 2018.

[66] Herna Verhagen*, De economische en maatschappelijke noodzaak van meer cyber security—Nederland digitaal droge voeten* (The Hague: PostNL, September 2016).

[67] Government of the Netherlands: Ministry of Economic Affairs and Climate Policy, "Factsheet Digital Trust Center," (August 6, 2018), 1–4.

[68] Martti Lehto, "The Cyberspace Threats and Cyber Security Objectives in the Cyber Security Strategies," *International Journal of Cyber Warfare and Terrorism* 3, no. 3 (2013): 1–18.

Risk Governance

In terms of risk governance, the approaches of Israel and the Netherlands have many similarities and differences. Both nations have government bodies (in the Netherlands, the Ministry of Health and the NCSC; in Israel, the Ministry of Health, Welfare, and Sport, and the National Cyber Directorate) that organize regular meetings with healthcare institutions, aimed at maintaining industry knowledge and situational awareness, challenges, and relevant processes. However, with the creation of the MedSoc, which specifically supports the medical sector, Israel's government clearly shows it understands the present cyber threats are a potential danger to the business continuity of the healthcare industry. In contrast, the Netherlands has an operational National Cyber Security Operations Center, but there is not one specifically focused on the healthcare industry.

Regulatory Environment

In addition to the risk governance, the governments of Israel and the Netherlands have created similar cyber and information laws, but each country still maintains its unique composition based on the local and current situation. Both nations have developed regulations for appointing a CISO or DPO to an organization. Israel's Privacy Law requires data owners to appoint a data manager; although it is mandatory, it is not always enforced. Despite the similarities, there are some key differences. The Netherlands has a cybersecurity law currently modified to the GDPR, which created a better system for dealing with personal data and created the Data Protection Agency (DPA) as the main authority for this subject. Currently, Israel has no cybersecurity law (still in the drafting stage), making it difficult for government bodies to enforce certain cybersecurity measures or standards in the healthcare industry. Nevertheless, both regulatory environments regarding cybersecurity and information security are similar, since Israel has broadly replicated the European Data Protection Directive to bring about greater harmony with European standards.[69]

Key Stakeholders of the Strategy

Both countries are pioneers in cybersecurity as the Israeli and Dutch governments support cybersecurity cooperation among experts across the

[69] Bourne, *A Guide to Data Protection in Israel.*

government institutions, as well as civil and industry sectors. Despite the fact that Israel's national cybersecurity strategy does not focus on international cooperation in the document, as in the case of the Dutch strategy, the multiple international public-private partnerships clearly indicate the government's interests in engaging international cooperation on this issue.

Definition of Critical Infrastructures and Critical Objects

A significant aspect in the national cybersecurity strategy of both nations is the confidentiality, integrity, and availability (CIA) triad of information. Israel's strategy emphasizes using specific controls to protect systems and organizations against harming the CIA of information and systems, whereas the Dutch document mainly mentions the CIA but does not provide any approaches on how to deal with cybersecurity. Both countries recognize that the critical and secondary assets of the healthcare institutions must be mapped to understand the threats to the processes and to understand the vulnerabilities in the healthcare systems.

Nevertheless, Israel's approach on dealing with the weak points in the supply chain of the healthcare industry is extraordinary in the cybersecurity field. Israel's National Cyber Directorate and the Ministry of Health have created a grade-based system to check how critical the supplier's systems or services are for the healthcare industry and to check the cybersecurity measures at the supplier, based on the criticality of the products and/or services.

Cyber Intelligence and Cybersecurity Awareness

Both Israel and the Netherlands are some of the more developed countries in terms of cyber innovation and cybersecurity measures. Israel's National Cyber Directorate proactively protects the healthcare industry by scanning the dark web on cybercriminals and new cyberattack methods. In the Netherlands, the intelligence service started the Joint SigInt Cyber Unit (JSCU), which provides information and expertise for the entire critical infrastructure. At the same time, the Dutch government has created a program to improve Dutch society's cybersecurity awareness through advertising and media. The initiative targets all Dutch citizens and the government is slowly changing its approach from that of being knowledge-based to having cybersecurity skills.[70] In Israel, there is no such initiative to increase the cybersecurity skills of its citizens. However, the Israel Defense Force's Unit 8200 focuses on cyber warfare, acting as a catalyst for cybersecurity in the "high-tech" nation. Another difference is the MedSOC in Israel, which shares information about cyber threats specifically to the healthcare industry.

Conclusion

The technological changes in the healthcare industry and the ongoing threat of cyberattacks targeting healthcare networks and medical devices—amplified by greater connectivity—has created an expansive target, including IoMT, medical applications, software, information systems, and security devices across healthcare institutions. Given these growing threats across the critical infrastructure sector, many nations have developed strategies and regulations to enhance cybersecurity. The current Israeli and Dutch national cybersecurity strategies and regulations are comprehensive and take into account a multitude of cyber threats; however, both countries need to make some improvement in order to manage the ongoing cyber changes in the healthcare industry.

Risk governance in cybersecurity enables both countries to change and achieve their strategic objectives while risks are minimized. Both risk governance and the responsible ministries in Israel and the Netherlands focus on a bottom-up approach through cybersecurity meetings with directors and IT managers in hospitals. The approach to cybersecurity measures for medical devices differs considerably in both nations since Israel creates a safe environment to test the new medical devices before they are implemented in the healthcare industry, while the Netherlands chooses a more instructive way of advising healthcare operators to check their medical equipment before implementation.

Both countries have created regulations to protect data in organizations, including in healthcare, as well as private data of civilians against cybercriminals. Israel and the Netherlands created regulations for organizations to hire data managers (CISO or DPO) if they handle sensitive information. Another important law in both countries is the data notification breach law, which requires data managers to report data protection incidents. Israel, like the

[70] Government of the Netherlands: Ministry of Justice and Security, *National Cyber Security Agenda: A Cyber Security Netherlands*, April 20, 2018.

Netherlands, eventually will implement a cybersecurity law, which will improve the handling of cybersecurity incidents.

Stakeholders strongly affect a country's national cybersecurity strategy since the operational level has a different view on cybersecurity than the strategic level. When governments want to improve the overall cybersecurity, employees of healthcare institutions benefit more from a respectable balance between cybersecurity and day-to-day work. Both Israel and the Netherlands interact on a regular basis with their stakeholders in the healthcare industry, in order to create effective cyber strategies that result in pro-active and multi-disciplinary commitment.

Alongside the process of formulating the critical infrastructure sector, healthcare institutions need to understand their critical and non-critical assets, so cybersecurity measures can be implemented specifically for safeguarding those assets. Both the national cybersecurity strategies of Israel and the Netherlands are focused on mapping organizations' assets through a process of risk assessment and inspecting current cyber defense systems. The confidentiality, integrity, and availability of information is the main concern for the healthcare industry, and both Israel and the Netherlands emphasize cybersecurity in order to prevent cyberattacks. A big difference between the two nations in supporting the healthcare industry is that Israel's government takes responsibility to help the healthcare industry with the vulnerabilities of the supply chain, while the Netherlands chooses to play a more informative role in the supply-chain security.

Finally, cyber intelligence and cybersecurity awareness are becoming a necessity of the healthcare industry. In Israel, the intelligence services work together with the Ministry of Health to scan the dark web on potential new cyberattacks. The Dutch military and general intelligence services created the National Response Network to detect and deter cyberattacks through new cybersecurity solutions. Furthermore, the Dutch government has designed a security awareness program using advertisements to inform of the dangers of the internet so that civilians will be more resilient. Israel has currently no similar program for cybersecurity awareness, but it increases the cyber knowledge through some IDF units, focused on cyber warfare and intelligence. Cyber intelligence in Israel is also spread through the new MedSOC in Beer Sheva, which allows the Ministry of Health and the National Cyber Directorate to upload information about cyberattacks or vulnerabilities.

Recommendations

This section consists of recommendations for the improvement and ongoing process of national cybersecurity strategies, partly based on the current strengths of the existing Israeli and Dutch strategies. First, the effectiveness of cyber strategies and regulations in both countries depends on the flexibility of the government in adapting to the evolving cyber domain. Future cybersecurity strategies should thus adhere to a basis of regulations in combination with reshaping the regulatory environment and information systems in critical infrastructure organizations in a flexible manner. Governments should update their strategies, policies, and regulations on an annual or bi-annual basis to keep up-to-date with new cyber advances.[71]

Second, an ongoing process of risk assessments is necessary to test and develop new cybersecurity strategies. Israel and the Netherlands should always maintain their cybersecurity approach to protect the healthcare industry against cyberattacks as cybercriminals will never stop trying to break into the information systems of healthcare institutions. Fortunately, both nations systematically test their cybersecurity strategies in national cybersecurity exercises to elevate and strengthen established security procedures. Israel's National Cyber Directorate and the Dutch equivalent, the NCSC, need to take more responsibility in the healthcare industry by encouraging institutions and their CISOs to create Business Continuity Plans and perform exercises to train staff in case of a cyber crisis.[72] In addition, to protect the national medical databases against cyberattacks, the Israeli National Cyber Directorate and Dutch Health and Youth Care Directorate should focus on smaller, less-secured institutions by creating a separate approach for them, as these institutions tend to be less eager or short-staffed to perform system updates or to buy new medical devices.

Third, the Israeli and Dutch governments should reference and explore the cybersecurity strategies of other cyber allies in order to ensure that the international threat landscape is handled as "many hands make light work." Within the cyber domain, this is exactly what is lacking at the moment between governments. Additionally, international consensus on definitions, regulations, and cybersecurity alternatives could alleviate regulatory constraints across nations.

[71] Interview with Yaniv P., January 6, 2019.
[72] Interview with Eliav N., November 25, 2018.

Fourth, more awareness of cybersecurity should be promoted in the healthcare institutions in particular and in the society in general. Part of the guidelines need to focus on cybersecurity awareness for healthcare staff, since healthcare staff is not concerned with it and rather is focused on the patient's health. Organizations and staff need to be aware of the cybersecurity dangers and attack methods.

Finally, although both Israel and the Netherlands have gaps in their cybersecurity approach, they both have a high-end approach to cybersecurity. Hopefully, future cyber research and additional effort in understanding the cyber threats in the healthcare industry will create a more resilient society in both countries. In addition, greater international cooperation with multiple countries across the world can make cyberspace a better and safer place.