HealthManagement.org

LEADERSHIP • CROSS-COLLABORATION • WINNING PRACTICES

VOLUME 23 • ISSUE 1 • € 22

ISSN = 1377-7629

AI & Robotics Implementation and Pitfalls

THE JOURNAL 2023

9 771377 762006 01

Cybersecurity:

Preventing the Worst-Case Scenario

Shifting from Cybersecurity to Cyber Resilience

A paradigm called “Cyber Resilience” includes a long-term defense against cyberattacks. It covers all three phases of a cyberattack, including mitigation techniques, reaction to an incident, and recovery.
An organisation’s cyber resilience attempts to lead it through such challenging circumstances and speed up its recovery. Additionally, it seeks to protect the entire business by considering all potential mistakes, which can range from basic human error to weaknesses in internal and IT controls.
The COVID-19 crisis has highlighted the necessity of making investments in digital health technology in order to improve, for instance, the effectiveness and efficiency of surgical procedures. Even though the unit’s overall performance is currently more than excellent, there is still plenty of opportunity for upgrade and enhancement. It is crucial to increase the Radiology Unit’s resilience and capability to guarantee the effectiveness and scope of care as well.

CHRISTODOULOS PAPADOPOULOS

Founder
geevo® and CPbros Group
Chairman
Cyprus Association of Information Protection and Privacy (CAIPP)
Cyprus

key points

- Cyber Resilience has evolved dramatically since the outbreak of COVID-19.
- eHealth has already started taking place in Cyprus since 2021.
- Artificial Intelligence must be optimised for our patients’ better outcomes.

Cyber Resilience vs Cybersecurity

Cyber resilience can be defined as an organisation’s capacity to consistently execute contracted services, operations, and results in the face of cyber incidents. These occurrences may have a negative influence on facilities, systems, information, people, and technology. What distinguishes cybersecurity from cyber resilience? Endpoint security, network security, and security awareness training are some of the sub-components of cybersecurity, which is a component of cyber resilience. These collectively make up the wide category we refer to as “cybersecurity.”

When data backup and recovery are added to the mix—which in turn includes services like endpoint backup and recovery, backup for Microsoft 365, server backup, migration services, and more—we start to talk about cyber resilience in a broader sense.

When data security plus data backup and recovery come together to keep your business online, we call it cyber resilience.

The Importance of Cyber Resilience

A cyber resilience strategy is vital for business continuity. It can provide benefits beyond increasing an enterprise's security posture and reducing the risk of exposure to its critical infrastructure. Cyber resilience also helps reduce financial loss and reputational damage. And if an organisation receives cyber resilience certification, it can instil trust in its clients and customers. Further, a cyber-resilient company can optimise the value it creates for its customers, increasing its competitive advantage through effective and efficient operations.

To attract customers and gain their business, some organisations comply with international management standards, such as ISO/IEC 27001 provided by the International Organization for Standardization. ISO/IEC 27001 provides conditions for an information security management system (ISMS) to manage assets security such as employee details, financial information, intellectual property or third-party entrusted information. Cyber resilience provides organisations a competitive advantage over companies without it. Enterprises that develop management systems based on best practices, such as Information Technology Infrastructure Library (ITIL), create an effective operation. So, too, do they when developing a management system for cyber resilience. And as a result, these systems create value for their customers.

A true cyber resilience solution can help businesses solve for:

- **An evolving threat landscape** where more than half of small businesses report having suffered a data breach.* To defend against polymorphic malware and malicious, evasive scripts, you need way more than a traditional antivirus.
- **Ubiquitous connectivity** has dissolved the traditional network's edge, stretching IT resources and involving multiple cloud applications. This opens the door to data loss from malicious actors, human error, system failure, network outages, and natural disasters.
- **Market complexities** involving ever-stricter data security and compliance regulations, including GDPR, plus a dire shortage of qualified IT professionals to help manage it all.

> Nowhere is resilience on better display than in nature. Trees are designed to bend but not break under the weight of snow or high winds

Advantages of Cyber Resilience

Protection of Data

Security controls are used to protect the data from cyberattacks and ensure that the work remains unaffected.

Data Recovery

It aids in recovering the most data in the shortest length of time with the least amount of data loss.

Training

The staff of the company receive the necessary instruction on how to handle data safely and what to do in the event that a cyberattack occurs. In addition, the employees are also trained on an organisation's security protocols in protecting the data and help identify their responsibilities during a data breach.

Data Backup

Data and statistics are used to run every organisation. Every business' ability to operate effectively depends on data. Therefore, data backup is crucial during cyberattacks or natural disasters. The data backup also lessens the likelihood of data loss and its associated expenditures.

Blocking

When cyberattacks are made against an organisation, cyber resilience serves as an additional layer of protection. It aids in stopping harmful threats from getting into the system.

Access Control

Regular resource and asset monitoring by the security team aids in preventing unauthorised access to sensitive data. Implementing zero-trust security, which requires multiple-step authentication to stop illegal and unauthenticated data access, is another way to achieve

restricted access. Cyber resilience therefore aids in preventing data loss and in identifying unauthorised users.

Regular Maintenance

Regular maintenance of IT infrastructure and security measures is made easier with the aid of cyber resilience. Conducting routine internal and external audits will help with this. Thus, achieving a proper security architecture against a cyber-attack is made possible by cyber resilience.

Cyber Resilience in eHealth

The word "eHealth" refers to a broad range of Information and Communication Technologies (ICT)-based technologies designed to enhance health and lifestyle management, monitoring, and prevention.

Online collaboration between patients and health service providers, data sharing between various healthcare organizations, and communication between patients or health professionals are all examples of electronic health (eHealth). It also includes telemedicine services, electronic health records, networks of health information, and systems for monitoring and assisting patients.

To identify better solutions and share best practices among Member States, the European Union is pushing a "European eHealth Area" while organising various efforts and facilitating synergies between related policies and stakeholders. The creation of an electronic health record system, information sharing and standardisation, electronic prescription (ePrescription), and other goals are all special to the EU.

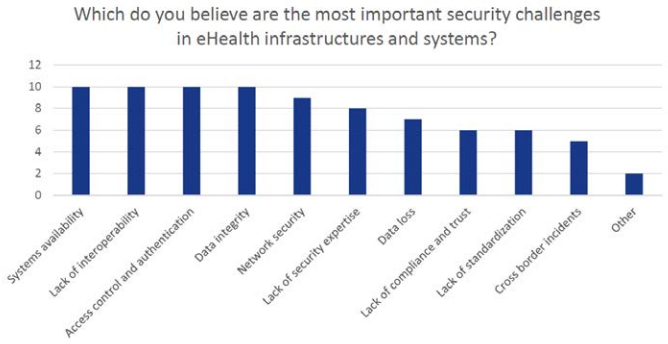

Figure 1

Cyber Resilience in Cyprus and the eHealth Challenge

Cyprus lacks an eHealth-specific strategy and/or policy. In Cyprus, eHealth activities are in the very early stages. The Ministry of Health has started taking advantage of eHealth standardisation processes (to create infrastructure for electronic health records) at two large hospitals (Nicosia General Hospital and Famagusta General Hospital), as well as the effective management of electronic materials and electronic prescription. The Ministry of Health began to implement various projects that contribute to a better approach to cross-border healthcare. Some of the most important projects are the following:

(a) The creation of an Integrated Health Information System, which consists of 13 subsystems that deal with how hospitals operate, such as managing e-prescriptions, electronic patient records, patient billing, laboratory test management, etc. The Integrated Health Information System is designed to encompass the essential aspects of hospital operations, allowing for both quality and cost management of patient care. Both Nicosia General Hospital and Famagusta General Hospital, as well as a few of the Health Centers in the two districts, use the Integrated Health Information System.

(b) Drugs Information management system. This system operates in all hospitals, pharmaceutical stores and many health centers.

(c) Spreading the word of the Makarios Hospital for Children as a single place for complete paediatric care.

(d) Enhancing the image of the Paphos and Limassol General Hospitals

In addition to having a significant impact on the digital shift, the digitalisation of cross-border healthcare and the tracking of infectious illnesses also aims to boost public health policies. With increased accessibility and equal rights for all residents thanks to digital health solutions, social cohesion can be further enhanced.

General cross-border eHealth services are being implemented in Cyprus, including: a) patient summaries; and b) ePrescription/ eDispencing (part of eHealth)

Objectives:

The main objective of this reform is to support Cyprus efforts to be part of a secure peer-to-peer network allowing the exchange of Patient Summaries and ePrescriptions, reaching the following general objectives:

- Facilitate secure access to patient health information and seamless cross-border treatment between European healthcare systems, particularly with regard to the sharing of patient summaries and

ePrescriptions.
- Contribute to patient safety by reducing the frequency of medical errors and by providing quick access to patient health information, as well as by increasing the accessibility of a patient's own prescriptions, also when abroad.
- Reduce the need for repeated diagnostic procedures by giving medical staff life-saving information in emergencies.
- Assist COVID-19 in its ongoing talks about policies and procedures in EU institutions (such as the eHealth Network) pertaining to the necessary eHealth infrastructure for cross-border services.
- Enable the national deployment of cross-border services across all healthcare stakeholders integrated with the currently emerging national eHealth digital infrastructure.
- Allow Cyprus to move more quickly toward developing the European Health Data Space for the exchange and access to various types of health data (electronic health records, genomics data, data from patient registries, etc.), not only to support healthcare delivery (referred to as primary use of data), but also for health research and health policy making purposes (so-called secondary use of data).
- Encourage the incorporation of AI functionality, particularly in relation to patient management, analytics, and decision-making, in cross-border services.

Challenges:
The National Contact Point for eHealth with other Member States is the National eHealth Authority (NeHA), which was established by law. The following are some issues that need to be resolved in this area:
- To build the proper data security and data protection systems in order to adhere to all applicable national regulations as well as cross-border e-services standards.
- To ensure data security by taking all practical precautions, such as maintaining data confidentiality, integrity, authenticity, availability, and non-discouragement.
- Establishing a suitable method for the control of health data entering and leaving Member States, which will enable duly accredited official entities to adequately oversee existing data collecting, processing, translation, and transmission systems.

> Nature is inherently designed for resilience - and we believe it's time for us to take a similar approach to security. This requires a move from a posture of Cybersecurity to one of Cyber Resilience

Conclusion
As countries transition into a post-industrial, knowledge-based economy characterized by dramatic developments in the information technology area, the digital transformation of the healthcare sector is a crucial development. In order to sustain sectoral development and, eventually, its antifragility, the adoption of the newest technologies and their applications in the health and care ecosystem must be managed properly from the perspectives of cyber security and resilience. The fundamental ideas that must define the strategic vision of a robust and sustainable digital transformation of healthcare, however, are yet only partially understood.

Heavy snow and rains will come.
Prepare for the worst - and be the tree that bends but doesn't break.

Conflict of Interest
None. ■

HealthManagement

Promoting Management and Leadership