axonpartnersgroup.com

Securing healthcare: Navigating cybersecurity threats with Business Continuity

January 2024

Authors

Jesús Carballal
PARTNER

Javier Hervás
MANAGER

Elena Martín
SENIOR ASSOCIATE

AXON CONSULTING

Abstract

As the healthcare industry witnesses an unprecedented surge in cyber threats, this report explores the cyberattack landscape, the latest trends and the evolving tactics that jeopardise the integrity of vital healthcare services, IT systems and most importantly patients' well-being.

The report also highlights that Business Continuity is vital to ensure the seamless and continuous operation of essential healthcare services, a task which is becoming increasingly complex due to the escalating dependency on the digital ecosystem and the still immature readiness of the sector. The report emphasises the need for robust Business Continuity Management (BCM) to prevent, mitigate and minimise the impact and range of cyberattacks targeting core healthcare services. It navigates through the nuances of the healthcare sector and the essential elements of effective Business Continuity Management for this sector. From proactive business impact assessments to developing strong response strategies and solutions, the report provides a summary of the key pillars required to fortify healthcare defences against cyber threats.

With a holistic view, this report will illustrate the synergies between safeguarding critical medical services, understanding the evolving cyber threat arena and developing and maintaining a robust Business Continuity framework to deliver a resilient and proactive foundation for healthcare operations in an increasingly digital landscape.

Contents

1. The escalating wave of cyber threats in healthcare

Healthcare is now more than ever the focus for hackers: the volume and scope of attacks are rapidly rising. According to the United States Department of Health and Human Services, the US has seen an upward trend in the number of data breaches in the last 10 years, and this is expected to continue.

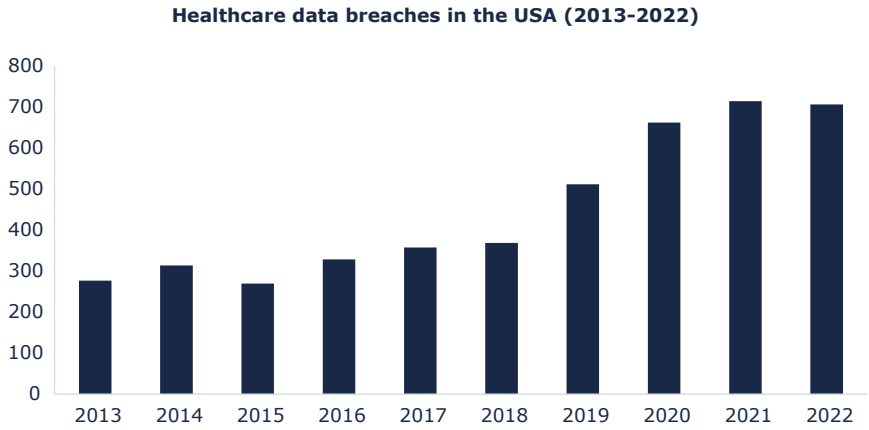

Figure 1: Number of healthcare data breaches in the USA 2013-2022[1]

In terms of the scope of attacks, once limited to accessing a patients' private data, this has escalated to data breaches that have an impact on the continuity of operations, posing a serious risk to healthcare ecosystems, quality of healthcare services and, critically patients' health. According to ENISA, although 43% of European healthcare-targeted attacks only caused breaches or data theft, around 50% of the attacks during the 2021-2023 period disrupted services in the healthcare sector both directly – patient admission, surgery, patient rerouting, hospital IT systems, etc. – or indirectly – web pages, billing systems, internet access, intranet portals, etc.

1 Source: Department of Health and Human Services

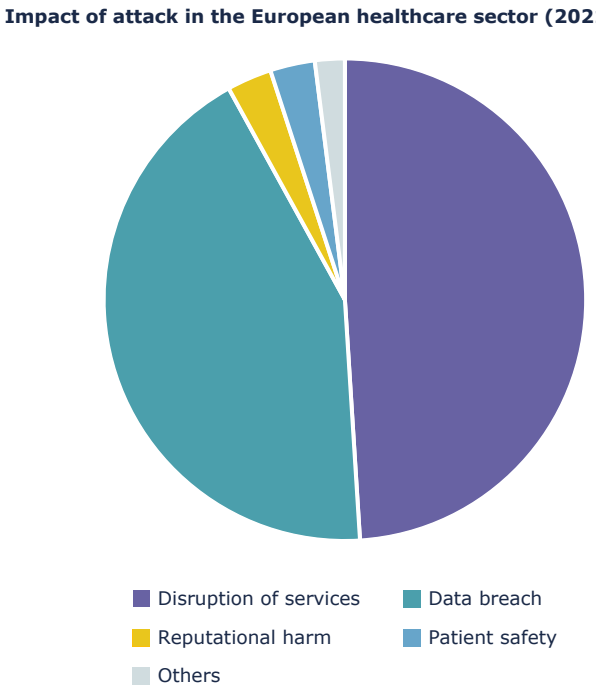

Figure 2: Distribution of impact consequences of healthcare attacks for the period 2021-2023[2]

Nearly 50% of healthcare cyberattacks lead to service disruptions, posing a significant risk to patient safety

Contrary to recent thinking that cyberattacks only target hospitals, hackers are now diversifying their efforts, focusing on the whole healthcare supply chain. While 53% of attacks are targeting healthcare providers, such as hospitals, primary care providers or emergency services, the remaining 47% are targeting health authorities, the pharmaceutical sector, laboratories, supply chain providers, insurance companies, and others. Data breaches are mainly affecting hospitals and primary care centres while cyberattacks that disrupt healthcare services target mainly healthcare entities and healthcare authorities.[2]

2 Source: ENISA, Threat Landscape: Health Sector. https://www.enisa.europa.eu/publications/health-threat-landscape/@@download/fullReport

One of the biggest reported data breaches in the health sector in 2023 was that of HCA Healthcare, one of USA's biggest hospital and clinic operators. It experienced a data breach affecting at least 11 million people and led to several lawsuits against HCA for non-compliance with federal regulation and negligence in safeguarding patients' data.

HCA Heathcare data breach

HCA Healthcare

Year: July 2023

Type of attack: Data breach

Entity: HCA Healthcare

Main objective: Financial gain and identity theft

Timeline of events

- In July 2023, Hospital and clinic operator HCA Healthcare revealed it had suffered **a major cyber attack that put at jeopardy the data of at least 11 million patients**.
- The data accessed included sensitive information such as the **patients' names, partial addresses, contact information and upcoming appointment date**.
- Although the company **disabled user access** to the external affected storage location as an **immediate containment measure**, data had already been extracted and **hackers posted a sample of stolen data online** on July 5. Their main aim was trying to **sell the data and/ or extort HCA**.

Impact and outcome

- HCA reported the event to **law enforcement and retained third-party forensic and threat intelligence advisors**.
- HCA had to **contact affected patients for warning and provision of support**.
- HCA Healthcare was hit with at least **4 class-action lawsuits** days after disclosing massive data breach.

Not only are cyberattacks more complex and damaging, but they are also getting "faster". Ransomware attacks are ones where increased speed and efficiency have been observed during the last couple of years. For instance, since 2019 time-to-encrypt victim's files has been reduced by 94%, and ransomware attacks now need less than four days to encrypt whole systems[3]. An interesting example of this is the ransomware attack on Ireland's Health Service Executive (HSE) systems in 2021, when hackers managed infiltrate the IT systems for at least a week before they were discovered. The attack disrupted services in several Irish hospitals leading to the cancellation of appointments. The scope of the attack was such that it took HSE 6 months to resume normal operations.

3 Source: IBM, Countdown to ransomware: Analysis of ransomware attack timelines. https://securityintelligence.com/x-force/analysis-of-ransomware/

Health Service Executive (HSE) ransomware attack

Feidhmeannacht na Seirbhíse Sláinte
Health Service Executive

Year: May 2021

Type of attack: Ransomware

Entity: Ireland's HSE

Main objective: Disruption of services and financial gain

Timeline of events

- In May 2021, **Health Service Executive (HSE), the entity that provides all of Ireland's public health services** was affected by a cyberattack through the infiltration of their IT systems using a complex ransomware.
- **The attack affected all of HSE's systems, having a significant impact in HSE's services provision:** disruption of HSE's staff operations, cancellations of appointments, etc.
- **Part of the sensitive information stole was published in the dark web.**

Impact and outcome

- The attack forced the **cancellation of up to 80% of appointments** in certain facilities.
- A **High Court order was published** to prevent anyone from sharing, processing, or selling the information stolen during the attack.
- It took HSE approximately **6 months to fully recover** normal operations.

But why is the healthcare sector a focus for hackers? The increasing digital dependency of this industry is attractive and lucrative for hackers for various reasons:

- **Criticality of health operations continuity:** unlike other businesses or sectors, the healthcare industry is directly linked to citizens' care and safety. Ensuring uninterrupted access to networks, digital systems and patients' data is critical and disruption can compromise the quality of healthcare services and patients' health.

  Cybercriminals are aware of these vulnerabilities and how healthcare organisations are willing to respond to their demands to reactivate services as fast as possible. Any lost time will lead to interruption of operations and having to transfer or divert to other facilities, delaying surgeries, and causing cancellations of patient appointments. This is what makes the health industry a clear target for cybercriminals.

  Ransomware attacks have been the prime threat in the healthcare sector for the last three years, accounting for more than half of the cyber incidents and with the most impact on organisations targeted.[2] Mainly because the pressure to reduce any disruption increases the possibility of complying with the criminal's conditions, as has been proved in a recent study that showed that over 60% of health organisations paid a ransom when being hacked, compared to a cross-sector average of 46%.[4]

Healthcare sector is especially attractive to cybercriminals as the pressure to reduce disruption increases the possibility of ransom payments

- **Escalation of digital dependency:** throughout the last decade, and accelerated by Covid-19, digital medicine has an increasingly significant role in healthcare. Continuous access to digital technologies, systems or networks has become not only essential but indispensable which gives hackers plenty of new opportunities.

  The rise of interconnected systems, mHealth, smart monitors, Internet of Things (IoT) medical devices or electronic health records (EHRs) provide cybercriminals with more potential breaching points to gain unauthorised access to medical systems and private data. In addition, healthcare organisations are owners of personally identifiable information (PII) and personal health information (PHI) which is of great value for cybercriminals, particularly on the dark web for identify theft, insurance fraud, etc.

- **Exposure of systems and human capital:** healthcare entities, particularly small-scale settings, such as clinics, usually lack the resources or technical expertise to have adequate IT infrastructure or security protocols. This exposes their systems and networks to cybercriminals, providing them with more points of access, and a wider attack surface making it easier to exploit vulnerabilities.

  According to ENISA, most healthcare organisations state that 61% of cybersecurity incidents are derived from existing vulnerabilities that were exploited. Additionally, there is a general lack of awareness of cyber risks and cybersecurity good practices among healthcare professionals and staff members who easily fall victim to social engineering practices (e.g. phishing emails) aimed at disclosing sensitive data.

The growing reliance on digital systems in healthcare, coupled with infrastructure vulnerabilities, multiplies the opportunities for hackers

4 Source: Portnox, Why Is the Healthcare Industry the Most Likely To Pay Cybercriminals for Ransomware Attacks? https://www.portnox.com/blog/iot-security/healthcare-pay-ransomware-attacks/

Securing healthcare: Navigating cybersecurity threats with Business Continuity

As the healthcare landscape is rapidly evolving towards a digitally dependent ecosystem where technology and IT systems are swiftly acquiring an already vital role in patients' care and safety, organisations are failing to keep up with cybersecurity prevention, protection, and resilience. For instance, according to ENISA, 40% of healthcare organisations have no cybersecurity awareness programme for non-IT staff and almost 50% have never performed a risk assessment.

Any disturbance causing an interruption in service or operational continuity has the potential to result in impacts that extend beyond the purview of ordinary business considerations. In light of this, the implementation of robust procedures and comprehensive plans aimed at fortifying organisational preparedness and resilience becomes imperative. Such measures not only safeguard the continuity of operations but also assume paramount importance in preserving the care and well-being of patients.

2.

Leveraging Business Continuity in healthcare to safeguard against cyberattacks

How can healthcare organisations effectively manage cyberattacks while ensuring an uninterrupted delivery of critical medical services in a complex and digitally dependent ecosystem?

Business Continuity Management (BCM) is a crucial element to solving this intricate puzzle.

Business Continuity (BC) refers to an organisation's ability to maintain critical or essential functions and services during and after a disruptive event or disaster. It encompasses planning, implementing, and coordinating measures, resources, and contingencies to ensure that essential processes and systems can continue to operate or be rapidly restored in the event of a disruption. The main objective of any Business Continuity strategy is to sustain essential operations, protect vital assets, reduce downtime, and strengthen the organisation’s resilience and preparedness.

Although Business Continuity methodologies and frameworks are usually common to all industries or organisations, when deep diving specifically in the healthcare sector, there are areas where special attention should be focused when developing a Business Continuity Plan (BCP). The three main areas are:

- **Emergency response:** during emergencies or crises, it is vital that critical services are maintained with a certain level of quality and that healthcare facilities or organisations have a robust BCP to coordinate resources, communicate and navigate the situation while providing medical coverage to their patients.

- **Data exchange and IT infrastructure:** as the healthcare sector relies heavily on a robust IT infrastructure and on data being exchanged between different systems and entities such as hospitals, pharmacies, insurance providers etc; having processes that enable secure data transmission during incidents or system outages is a primary need. Business Continuity practices aim to ensure healthcare personnel always have access to critical

information and that these are kept confidential and secure, despite a disruption or system unavailability.

- **Supply chain management:** apart from IT systems and infrastructure, the supply chain is one of the key components of a robust medical system. During disruptions or disasters, impacts on medication and shortages of medical supplies can be critical as they can hamper the delivery of vital care services. Business Continuity is required to ensure rapid movement and mobilisation of resources for continuity of medical supplies.

Areas of concern when developing a BCP

Figure 3: Key areas of relevance in Business Continuity management in the healthcare sector

Successful Business Continuity Management demonstrates proactivity and resilience, emphasising both prevention and preparedness

When developing a BCP, although each healthcare organisation should develop a plan tailored to the entity's operating environment and context (e.g. size, objectives, nature, complexity, etc.), there are certain components which are indispensable to all BCPs. These components are the pillars to developing a robust and resilient Business Continuity strategy:

- **Governance:** encompasses the identification of all stakeholders involved in the Business Continuity management across all action layers (e.g. strategic, operational, tactical) as well as their roles and responsibilities in relation to the execution and maintenance of the plan. Governance is the component which interlinks all the procedures, recovery strategies and communication elements of the plan. A fundamental aspect of the governance model is that all parties involved are aware of their responsibilities and are committed to satisfying the requirements of their role.

- **Preparedness operations and communications:** as previously emphasised, Business Continuity is not solely about how an entity reacts during a disruption but also how it prepares and prevents one. Therefore, certain actions need to be performed before any disruptive event of which the following are top priorities:

    - **Business impact analysis (BIA):** the quantification of the impact that potential disruption will have on service delivery and business processes.

      It is also used to define timeframes such as the amount of time when not resuming operations would become unacceptable to the organisation. The target of this procedure is to identify the services or activities that need to be prioritised, the resources they require and interdependencies.

    - **Risk assessment (RA):** through a RA the organisation systematically assesses the potential disruptions to its vital activities and resources.

      This includes identifying risks, analysing their impact, and determining which ones require proactive measures. The primary objective is to strengthen operational resilience and safeguard essential processes from potential threats.

    - **Business Continuity strategies and solutions:** based on the results obtained from the previous two key actions, the entity will develop different strategies and approaches to deal with disruptions and maintain the continuity of service for prioritised pre-identified activities.

      The main objective of these strategies is to:

      i. reduce the possibility of a disruption

      ii. reduce the downtime period of services when disrupted

      iii. minimise the impact if a disruption occurs

All these actions define the methodologies, procedures and specific communication plans and models to communicate results and recovery options to top management and the responsible stakeholders.

- **Response operations and communications:** to be able to efficiently respond and coordinate resources during a disruptive event, organisations need to establish response frameworks and plans to communicate with relevant stakeholders and to effectively navigate the organisation through disruptions.

  Additionally, immediate steps and tasks to manage and minimize disruption through the activation of the applicable business solution/s should be put in place.

- **Testing and training:** once the plans, procedures and methodologies are shared with the responsible teams and stakeholders, the organisation should develop a training and testing programme to ensure teams are confident and have the appropriate level of knowledge and competence.

  This will not only help to assure people's preparedness but also to ensure the BCP is resilient in a non-impactful situation and identify areas of improvement or gaps.

- **Continuous improvement:** the last pillar consists of monitoring and evaluating the overall performance of the plan after a disruptive event, when required by external factors (e.g. regulatory compliance requirements) or through periodic reviews.

Each of these areas plays a crucial role in constructing a comprehensive and robust Business Continuity Plan.

3.

The vital role of Business Continuity in sustaining healthcare operations

Although Business Continuity is relevant across all industries, there is an increasing recognition of the importance of Business Continuity in healthcare, especially after Covid-19 events and the subsequent increase in cyberattacks in the sector, as illustrated previously. But what specific events are triggering healthcare organisations to prioritise Business Continuity Management?

- First, any disruption in the sector can rapidly escalate and lead to a ripple effect on medical services, putting in jeopardy people's wellbeing and safety.
- Unlike other sectors, the healthcare industry holds a unique significance. It is not only about financially contributing to the economy or to a specific business but to fundamental aspects of life such as health and wellbeing.
- Second, Business Continuity is not only about what entities need to do during a disruptive event but what they can do before and after to strengthen their resilience. BC contributes to the identification of risks and vulnerabilities providing the basis of preventive and mitigation strategies and embedding a "continuous improvement" mentality to ways of working.
- Third, governments and international organisations are ramping up their efforts to issue recommendations and guidelines, which are rapidly transforming into mandatory requirements in certain instances.

Figure 4: Key reasons for organisations increasing efforts in Business Continuity management.

Here we explore these in more detail.

Healthcare disruptions: beyond just "financial considerations"

In recent years, customers, regulators, and other stakeholders have become less forgiving of less resilient organisations that, in the event of an incident, dim their quality of service or even collapse due to a lack of preparation and mitigation.

The repercussions of cyberattacks extend well beyond mere damage to reputation or financial losses; they directly jeopardize people's lives

Specifically, in healthcare, the significance of Business Continuity goes far beyond just financial considerations or reputational damage. Business Continuity provides a clear blueprint for the skills to acquire, actions to do, and processes to set to ensure that healthcare services delivery is maintained. It ensures the continuity of critical services and accessibility to medical resources.

Peoples' wellbeing and lives depend on the seamless operation of healthcare services and, with a proper Business Continuity plan in place, the impact of any disruption or disaster is limited or eliminated by avoiding miscommunications, unwanted delays, service interruptions, etc.

Business Continuity: actionable before, during and after disruptions

Business Continuity must be understood as a proactive approach to maintain business-critical services or functions including the actions or steps that must be taken prior to any event to ensure the healthcare-related systems are well enough prepared to face any disruption. This preparation, which must be achieved from an operational, financial, and human point of view, relies on procedures that are defined, planned and actioned before any disruption has occurred.

Although there are several pre-disruption components within Business Continuity Management, a common well-known fundamental pillar is identifying specific threats that can affect the organisation's systems, IT infrastructure, processes, supply chain, etc. It is essential to fully understand the potential consequences of security incidents to ensure that Business Continuity Plans and strategies are adapted to maintain the continuity of critical activities at acceptable levels. Another relevant component of BCM is the training and testing of the Business Continuity Plan. It involves, not only putting in practice the procedures and methodologies but also testing the capabilities of the stakeholders and owners of the plan. It allows identification any gaps, bottlenecks, and misconfigurations. It allows for a flexible BCP to be implemented which can be updated and improved when needed.

In terms of post-disruption components, performing self-evaluations and holding discussions on the timeline of events and the actions taken can motivate organisations to identify lessons-learnt and embed in their operations a "continuous improvement" mindset.

Therefore, Business Continuity is not only about "what needs to be done" during events or disasters, but also about having a clear view on the most critical aspects for the business and what procedures or resources need to be in place for the organisation to have certain success when dealing with a disruption.

Regulatory trend: aligning with international best practices to ensure Business Continuity

Apart from the operational and financial benefits from having a BCP, an increasing number of countries are developing specific standards and specifications related to business resilience and continuity. This suggests that countries and governments are realising the importance of promoting BCM practices across sectors.

Although these are still in an early phase and usually in the form of standards or good practices, the truth is that the Business Continuity practice is evolving fast and will soon become a "must" in all sectors, particularly in the healthcare industry.

For instance, in the UK according to the Civil Contingencies Act 2004[5] and the Health and Care Act 2022[6] it is mandatory for all NHS (National Health Service) entities to establish continuity plans. Simliarly, although not specific for the healthcare industry, in mid-2023 Germany published the updated BSI Standard 200-4 Business Continuity Management which provides organisations with guidance on how to set up and establish a Business Continuity management system.[7] Saudi Arabia, has gone one step further with the DGA (Digital Government Authority) publishing in 2021 a set of guidelines for Business Continuity particularly for government entities.

International organisations are also directing their efforts to strengthen organisations' resilience and security through the publication of different standards and guidelines. The International Standardisation Organsation (ISO) has established ISO 22301:2019 certification which requires organisations wanting to achieve certification to implement, maintain and improve a Business Continuity management system.[8]

The regulatory arena around Business Continuity is rapidly evolving and compliance with national and international policies will soon become a necessity

5 Source: UK Government, Civil Contingencies Act 2004. https://www.legislation.gov.uk/ukpga/2004/36/contents

6 Source: UK Government, Health and Care Act 2022. https://www.legislation.gov.uk/ukpga/2022/31/contents/enacted

7 Source: Germany's Federal Office for Information Security (BSI), BSI Standard 200-4 Business Continuity Management. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-4-Business-Continuity-Management/bsi-standard-200-4_Business_Continuity_Management_node.html

8 Source: ISO, ISO 22301:2019. https://www.iso.org/standard/75106.html

Country/Entity	Sample	Explanation
UK	Civil Contingencies Act 2004 & Health and Care Act 2022	Under these acts, all NHS organisations must put in place continuity arrangements and other emergency preparedness, resilience and response requirements.
Germany	BSI Standard 200-4 Business Continuity Management	Defines practical guidelines for setting up and establishing a business continuity management system in an organisation.
Saudi Arabia	Standards Of Business Continuity For Digital Government Management	Sets standards and plans to prepare for incidents, ensure the existence of effective controls and capabilities to manage incidents or crises, and ensure the continuity of operations and procedures.
ISO	ISO 22301:2019	Specifies standards to implement, maintain and improve a business continuity management system to protect against, prepare for, respond to and recover from disruptions.

Figure 5: International sample of resilience and Business Continuity standards and regulations

Continuity planning regulations and standards have flourished in recent years due to the strategic imperative of ensuring uninterrupted delivery of healthcare services. In an era where disruptions are inevitable, a robust Business Continuity Management strategy aligned with regulatory expectations is a cornerstone for the sustained wellbeing of the healthcare sector and, ultimately, patients.

AXON CONSULTING

About
Axon Consulting

Axon is an international firm founded in 2006 that provides investment and advisory services to a broad client base in the ICT and digital space in more than 70 countries across the world.

Axon's cybersecurity practice is central to its business and an increasingly important service area for clients. Its work in this field includes strategy, policy and regulation, governance and research at business and governmental level. Axon works closely with government representatives and other clients to help them understand their cybersecurity needs and challenges in their territories, and to define actionable recommendations aimed at improving their cybersecurity ecosystems.

Tel: +34 913 102 894
Email: marketing@axonpartnersgroup.com

The views and opinions expressed in this article are those of the authors and do not necessarily reflect the view of Axon Consulting.

AxonPG
axon-partners-group