IDC PERSPECTIVE

Making Strides in Cybersecurity: The Experience of Milton Keynes University Hospital NHS Foundation Trust

Adriana Allocato Jonas Knudsen

EXECUTIVE SNAPSHOT

FIGURE 1

Executive Snapshot: Making Strides in Cybersecurity: The Experience of Milton Keynes University Hospital NHS Foundation Trust

This IDC Perspective analyzes how Milton Keynes University Hospital (MKUH) NHS Foundation Trust in England embarked on a journey to detect and neutralize cyberthreats and subsequently enhance its overall infrastructure. This report highlights the foundational elements of its major action in this journey, which included the adoption of a machine learning technology solution to strengthen its organization against cyberattacks and protect patient data.

Key Takeaways

- The increasing digitalization of NHS services in recent years has driven back-office efficiencies and improved the way medical professionals store and share patient data. However, these developments also increased the risk from disruptive cyberattacks that have the potential to compromise NHS services and patient safety.
- The recent WannaCry attack highlights cybersecurity as a critical patient safety issue requiring urgent solutions. In May 2017, multiple NHS trusts across England were hit by a large-scale ransomware attack, with trusts having to switch off their systems.
- Like other providers, MKUH's key cybersecurity objectives and strategies revolved around its information governance policy principles to ensure confidentiality, integrity, availability, and quality.

Recommended Actions

- Establish a culture of cybersecurity through education and increased training across the organization, emphasizing that every employee (IT, legal, PR and communications, clinical staff, executives, etc.) is responsible for protecting patient data.
- Adopt an integrated security architecture that can span from traditional endpoints to distributed network, mobile devices, and cloud applications to provide automated security.
- Back up data, systems, and configurations periodically.
- Define a risk management plan for cyberthreats. Running risk assessments on a regular basis helps identify vulnerabilities and protect against attacks.
- Consider engaging a well-equipped cybersecurity vendor. Cybersecurity partners can help with detailed analysis through a multilayer defense strategy.

Source: IDC, 2018

May 2018, IDC #EMEA43846818

SITUATION OVERVIEW

This IDC Health Insights case study focuses on Milton Keynes University Hospital (MKUH) NHS Foundation Trust in England, which embarked on a journey to detect and neutralize cyberthreats and subsequently enhance its overall infrastructure. This report highlights the foundational elements of MKUH's major initiatives in this journey, which includes the adoption of artificial intelligence (AI) and machine learning to strengthen the organization against cyberattacks and protect patient data. Furthermore, MKUH required new technology to ensure General Data Protection Regulation (GDPR) compliance by May 2018.

Company Overview

Milton Keynes University Hospital NHS Foundation Trust is a medium-sized district general hospital serving Milton Keynes and its surrounding areas in the U.K. Opened in three phases between 1984 and 1992, it became a NHS Foundation Trust on October 1, 2007, under the National Health Service Act 2006. In 2015, the trust entered into a partnership with the University of Buckingham to establish the first independent medical school in the country.

The hospital has around 548 beds, including acute and neonatal beds. It employs more than 4,000 staff, providing a full range of acute hospital services and an increasing number of specialist services. All inpatient services and most outpatient services are provided at the main hospital site. The trust is organized into four clinical divisions (medicine, surgery, women and children, and core clinical) and a number of corporate directorates. Executive directors and clinical service unit (CSU) leadership teams are responsible for the day-to-day management and running of the hospital's services, with ultimate management accountability resting with the CEO.

Since April 1, 2016, Milton Keynes University Hospital NHS Foundation Trust has been regulated by NHS Improvement (NHSI), which replaced both the regulator for NHS Foundation Trusts (Monitor) and NHS Trusts (NHS Trust Development Agency).

The future for Milton Keynes University Hospital NHS Foundation Trust is likely to be influenced by the work undertaken within the sustainability and transformation plan (STP) for the Bedfordshire, Luton, and Milton Keynes footprint. The STP consists of 16 partner organizations that have a commitment to improve the health and well-being of the local population, while delivering services within the available resources. From April 2017, the STP has been selected to become an accountable care system. This is a system in which the respective NHS organizations (both commissioners and providers), in partnership with local authorities, choose to take on clear collective responsibility for resources and population health. It is anticipated that it will provide joined-up, better-coordinated care. In return, organizations expect to have far more control and freedom over the operations of the healthcare system in the Bedfordshire, Luton, and Milton Keynes areas, and work closely with local government and other partners to keep people healthier for longer, and out of hospital.

However, being part of a healthcare ecosystem (where hospitals, clinics, and medical facilities are being extended beyond their walls with enhanced connected capabilities) has raised privacy and data security concerns. The MKUH is progressively acquiring cybersecurity awareness, policies, and procedures to be security and privacy focused.

Business Needs

Healthcare providers and the MKUH have recently had a deep need to adopt a cybersecurity solution to:

- Prevent possible threats that might stem from the increased digitalization of processes and procedures. The digitalization of NHS services in recent years has improved the way medical professionals store and share patient data. However, these developments have also increased the risk from disruptive cyberattacks that have the potential to compromise NHS services and patient safety. As healthcare organizations transition to digital systems, many are left vulnerable to cybercrime, as health data contains sensitive personal and financial information.
- Meet the regulatory requirements that entered into force through the GDPR, through which the European Commission intends to strengthen and unify data protection for individuals within the EU. The adoption of GDPR requires improved personal digital security, more transparency around how patient data will be used, and greater control over what data can be collected. Therefore, European healthcare providers need to review their existing policies, procedures, and practices to ensure compliance with this new regulation, which aims to bolster privacy rights. At the same time, providers must also ensure a simple clinical workflow that enables fast and secure access to patient data.

However, the vulnerability of healthcare systems to cyberattack mostly stems from:

- Chronic under-investments in information technology infrastructure
- Short supply of cybersecurity experts and cash-strapped healthcare organizations that cannot afford to pay the market rate for their services
- The fragmented governance structure of the application architecture, leading to a lack of clarity over who is responsible for securing systems and data
- The culture of healthcare that understandably focuses on caring for patients, even at the expense of security

Recently, the MKUH experienced deep digital transformation that exposed the hospital to considerable cybersecurity risk. While MKUH has always taken cybersecurity seriously, this digital transformation was not always accompanied by substantial cybersecurity improvements. The real incentive to pursue a more proactive cybersecurity strategy emerged after the WannaCry attack.

The WannaCry attack highlighted cybersecurity as a critical patient safety issue requiring urgent solutions. In May 2017, multiple NHS trusts across England were hit by a large-scale ransomware attack, with trusts having to switch off their systems. The global cyberattack disrupted services at 61 NHS organizations across the U.K., infiltrating more than 200,000 computer systems across 150 countries and forcing the U.K.'s healthcare system to turn away patients.

Following this cyberattack, NHS Digital, the Information Commissioner's Office, and Europol (the European Union's law enforcement agency) announced a list of prevention and recovery tips to help healthcare providers in the future. Additionally, the U.K.'s National Health Service has recently given hospitals and healthcare providers the go-ahead to begin storing confidential patient information in the public cloud. Despite the cyber-risks associated with these adoptions, healthcare organizations are moving forward due to the benefits they can provide. Therefore, digital security has become an NHS priority.

The WannaCry attack served as a warning shot for the MKUH, which decided to strengthen its cybersecurity capabilities. The aim was to avoid more coordinated and more sophisticated ransomware attacks that take advantage of the myriad vulnerabilities across the organization, specifically to inflict more malicious and potentially harmful damage on patient care.

The Approach

Project Background and Objectives

While looking around for a vendor that could help support an innovative cybersecurity approach, MKUH decided to follow the example of West Suffolk (WS) NHS Foundation Trust.

The relationship of the two NHS trusts was developed through the "Global Digital Exemplar" (GDE) initiative. NHS England is currently supporting selected digitally advanced acute trusts that (through funding partnership opportunities) will become "Exemplars" over the next two or three and a half years. The West Suffolk NHS Foundation Trust has already been nominated as a GDE, an internationally recognized NHS provider delivering exceptional care in an efficient manner, using world-class digital technology and information. Each GDE has selected one (or occasionally two) trusts to partner with to accelerate their digital maturity to support the spread of best practices and innovation. In some cases, this will include sharing software or a common IT team. Others will adopt standard methodologies and processes. MKUH has been selected as a fast follower of WS Hospital. This means it can count on NHS England funding and that WS Hospital will continue to share its learnings and experiences to enable MKUH to follow in its footsteps as quickly and effectively as possible.

Therefore, when a cybersecurity need emerged, MKUH decided to explore the cyberdefense technologies that WS already had in place, including an advanced cybersecurity solution offered by Darktrace. After a successful four-week trial period, MKUH selected Darktrace technology to autonomously detect and respond to advanced threats. While Darktrace was the provider of West Suffolk NHS Foundation Trust, and it demonstrated its capabilities and innovations through positive client references, the four-week trial proved the benefits of the technology firsthand.

The technology offered by Darktrace was its Enterprise Immune System (EIS). The solution is modeled on the human immune system and is designed to address the challenge of insider threat and advanced cyberattacks by detecting previously unidentified threats in real time, as manifested in the emerging behavior of an organization's network, people, and devices, including mobile devices and Internet-of-Things (IoT) devices. The system analyzes complex network environments, leveraging advances in machine learning and AI algorithms, to learn the patterns of networks, devices, and users within MKUH information systems. This enables the technology to rapidly detect and respond to subtle deviations indicative of an emerging high-severity threat.

Additionally, the solution was completed with Darktrace Antigena, an automated response capability, enabling MKUH to fight back against cyberthreats without disrupting daily activities. It reduces response time and enables more efficient risk mitigation, regardless of the type of threat encountered. Antigena includes modules for automatically containing malicious activity in network traffic and email communications. John Dyer (Account Director at Darktrace) describes Antigena:

> "…as the antibody. You get infected with a virus, and your immune system fights back. That's what Antigena is. It's an automated response. The Enterprise Immune System says, 'Look over here, there is something potentially malicious happening.' Antigena can kick in and take a number of different responses."

Darktrace's Enterprise Immune System, which addressed MKUH's need to defend its sensitive information, was recognized as a winning platform in terms of self-learning and self-defending technology.

Like many other providers, MKUH's key cybersecurity objectives and strategies revolved around its information governance policy principles to ensure:

- **Confidentiality**, protecting sensitive information from unauthorized access or disclosure
- **Integrity**, safeguarding the accuracy and completeness of information and computer software
- **Availability**, ensuring information and vital services are available to users when required
- **Quality**, ensuring information is of sufficient quality for the intended purpose

Project Description

The project started in September 2017 with a four-week Proof of Value (POV) trial period, for MKUH to evaluate Darktrace's Enterprise Immune System (EIS) at no cost.

The Darktrace team — made up of an Account Director and a Cyber Technologist — installed its flagship technology into an agreed point of the network. The process only took an hour because the system is self-learning and does not require tuning or configuration.

During the four-week trial period, the Darktrace team delivered three threat intelligence reports (TIRs) that detailed the anomalies found, explained the significance of each event, and summarized the findings in an easy-to-understand executive summary. This process helped MKUH to understand the results of the POV and evaluate the benefits of adopting a full network deployment.

The competitive differentiation of Darktrace's solution was immediately evident. It adopted a mathematically oriented self-learning approach that can handle the ever-increasing complexity of healthcare information systems. The Enterprise Immune System thrives in these complex digital environments, as the technology is adaptive and continues to revise its understanding of "normal" in light of new evidence, enabling it to detect and respond to threats that other tools miss, while providing complete visibility across the digital infrastructure.

At MKUH, the IT department was enthusiastic about the benefits of this proactive approach to cybersecurity, and it eventually decided to pursue a full network deployment and signed a three-year contract.

Notably, another aspect that convinced MKUH staff to select Darktrace was the great customer care it provided across the duration of the contract. Darktrace offered continuous online training to inform new employees about the way the system works in addition to updating existing employees regarding new releases. The service offerings also provide access to the cyber-analyst team.

Business Value

The benefits stemming from the adoption of the Darktrace cybersecurity technology were numerous:

- **Network visibility**. The solution includes an intuitive Threat Visualizer user interface, which visualizes the entire network and facilitates the rapid investigation of prioritized alerts.
- **Real-time threat detection and autonomous response.** The system discovers previously unknown threats by detecting deviations from normal behavior. To understand normal behavior, Darktrace employs advanced methods using AI technology.
- **Easy deployment process**. The technology can be installed in an hour, and it doesn't require configuration. Additionally, any step of the process can be followed remotely.

Overall, MKUH succeeded in enhancing its cybersecurity capabilities and significantly reducing the risk of cyberbreaches.

ADVICE FOR THE TECHNOLOGY BUYER

Essential Guidance

Effective cybersecurity must become an integral part of healthcare systems, a pillar of regulation, and the subject of future research strategies. Given the steady rise of more internet-connected devices, healthcare providers must continue to innovate and transform how they approach network security. Therefore, healthcare providers approaching a digital transformation journey should consider the following:

- Establish a culture of cybersecurity through education and increased training across the organization, emphasizing that every employee (IT, legal, PR and communications, clinical staff, executives, etc.) is responsible for protecting patient data.
- Adopt an integrated security architecture that can span across traditional endpoints to distributed network, mobile devices, and cloud applications to provide automated security.
- Back up data, systems, and configurations periodically.
- Define a risk management plan for cyberthreats. Running risk assessments on a regular basis helps to know the vulnerabilities and then protect against attacks.
- Consider engaging a well-equipped cybersecurity vendor. Cybersecurity partners can help with detailed analysis through a multilayer defense strategy.

LEARN MORE

Interviews

- Craig York, Associate Director of IT, Milton Keynes University Hospital NHS Foundation Trust
- John Dyer, Account Director, Darktrace

Related Research

- *IDC Survey: How are European Healthcare Providers Progressing in their Digital Transformation?* (IDC #EMEA43692818, April 2018)
- *The Pulse of IT in the European Healthcare Provider Sector: Key Deals and Initiatives, October-December 2017* (IDC #EMEA43621018, March 2018)
- *Security Strategies for Western European Healthcare Organizations* (IDC #EMEA43530618, February 2018)
- *Does the Healthcare Industry Adopt Cognitive Systems?* (IDC #EMEA43530418, January 2018)
- *The Quest for Value: Key Trends in European Healthcare Digital Transformation* (IDC #EMEA43496817, January 2018)
- *The Power of Information Management for the Healthcare Ecosystem* (IDC #EMEA43493318, January 2018)

Synopsis

This IDC Perspective focuses on Milton Keynes University Hospital (MKUH) NHS Foundation Trust in England, which embarked on a journey to detect and neutralize cybersecurity challenges and subsequently enhance its overall infrastructure. This report highlights the foundational elements of major actions in this journey, which included the adoption of a machine learning technology solution to strengthen the organization against cyberattacks and protect patient data.

"The need to protect sensitive patient data from increasing cybersecurity challenges is putting pressure on most healthcare providers," said Adriana Allocato, senior research analyst, IDC Health Insights. "This case study demonstrates how MKUH benefitted from the adoption of a proactive cybersecurity solution and gained visualization of its entire network.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC Italy

Viale Monza, 14
20127 Milan, Italy
+39.02.28457.1
Twitter: @IDCitaly
idc-insights-community.com
www.idcitalia.com