Business challenge

NHS Digital sought to broaden the breadth and scale of its offerings and support to the health and care system, and increase its cybersecurity preparedness and resilience.

Transformation

For NHS Digital, cybersecurity isn't just an IT concern—it's also a clinical safety issue. To better protect England's healthcare system from cyberattacks, it engaged IBM as its strategic Cyber Security Operations Centre (CSOC) partner to provide enhanced security services and support and enable it to predictably and precisely block would-be threats.

Results

Expedites stakeholder-driven security innovation
by developing a joint Cyber Security Innovation Factory

Increases ability to manage and respond to threats
by industrializing processes that enable more effective monitoring of assets

Provides a central source of cybersecurity intelligence
and a single point of coordination for the healthcare system and partners

NHS Digital

Boosting cybersecurity preparedness and resilience for the sake of patient care

Founded in April 2013, NHS Digital is the national provider of information, data and IT systems for England's National Health Service (NHS) healthcare system. Its primary responsibility is to ensure the reliability, performance and security of NHS's IT infrastructure and platforms that enable data collection, sharing and exchange. NHS Digital also develops digital services, such as electronic referrals and electronic prescriptions, to a wide range of customers and stakeholders, including NHS trusts, pharmacies and patient groups. NHS Digital is based in Leeds, England and employs 6,000 people.

"IBM is not simply a supplier—it is one of NHS Digital's main strategic security partners supporting our Data Security Centre to help the wider NHS."

—Rob Shaw, Former Deputy Chief Executive Officer and Senior Information Risk Owner, NHS Digital

Share this

Cyberthreats jeopardize healthcare

The National Health Service (NHS) is the UK's system of public healthcare providers. Like many other healthcare systems, it is not a technology organization but has patient-facing tools and services that are enabled by technology. Like others, it is in the midst of a digital revolution and looking to serve patients better by integrating data, processes and technologies. And like others, it debates where best to spend its money: on IT and security or patient services.

But unlike others, the NHS has NHS Digital. NHS Digital is the healthcare system's digital, data and technology delivery partner specializing in designing, developing and operating complex, national-scale IT and data systems. Everything it does, from building innovative tools and services for citizens to facilitating access to data for clinicians, is aimed at enhancing the lives of patients and improving health and care outcomes.

The breadth of NHS Digital's role and responsibility is massive: it supports over 200 NHS trusts in England, plus a host of national organizations, general practitioners, pharmacies and patient groups. It runs more than 80 core national systems, including the NHS Spine, an information exchange platform that handled one billion messages in October 2018.

It also designs public-facing tools and nationwide services that facilitate and speed care. Its NHS 111 service for online emergency care has helped more than one million people. Its electronic referrals service handles over 70,000 referrals daily, and its electronic prescriptions service processed more than 690 million prescription items in 2018.

The job of protecting these tools and services from security threats falls to NHS Digital's DSC. The mission of the DSC is to support the delivery of digital patient outcomes by protecting the health and care system from preventable cyberattacks and proactively detecting threats. It also helps health and care organizations, such as NHS trusts and hospitals groups, respond to security incidents through a wide range of services, including designing cybersecurity support models, providing data security training, issuing cybersecurity threat notifications, and more.

Recognizing that the volume, variety and severity of security threats to healthcare are on the rise, the DSC sought to boost its cybersecurity preparedness and resilience. This need was highlighted in May 2017 when the global ransomware cyberattack, WannaCry, disrupted or infected 80 hospital trusts and 603 affiliate NHS organizations. Although the NHS was not the specific target, the incident ultimately cost the service an estimated GBP 92 million and 19,000 cancelled appointments. Worse, it jeopardized patient care.

For NHS Digital, cyberthreats aren't IT risks; they're risks to patient-facing services that can affect clinical safety and the ability to deliver timely care to citizens. To help ensure the safety and health of patients, it wanted to broaden its support and increase the number and type of services it offered to the NHS. It sought to use technologies that integrate and automate processes. And it looked to harden and evolve its operational capability, technical solutions and security operations model to support a greater number of health and care services.

But it couldn't do it alone.

Stronger, more resilient security defenses

In 2018, NHS Digital appointed IBM as its strategic security partner. Under a three-year contract, IBM® Cybersecurity Services is providing a wide range of enhanced data security services. It is also supporting the enhancement of NHS Digital's CSOC and the development of DSC services, such as the Business Intelligence and Risk Platform and the NHS Security Innovation Factory.

"The partnership with IBM allows NHS Digital's Data Security Centre to develop and grow faster to help keep patient information and services safe and secure," says Rob Shaw, Former Deputy Chief Executive Officer and Senior Information Risk Owner at NHS Digital. "It gives us access to specialist resources in times of increased need and allows us to grow our security capability in line with the evolving cyberthreat landscape, enabling NHS staff and patients to have confidence in the security of our system."

Of the large number of organizations bidding on the tender, IBM was chosen for its global presence in security operation centers (SOCs) and for its skill sets and expertise. In particular, IBM stood out for its clinical point of view and approach to developing solutions that focus on patient and health outcomes, versus a technical approach to solution development.

NHS Digital is transforming its security operating model (SOM) in stages. IBM organized the journey into four phases and a significant number of work packages designed to sustainably improve security capabilities over the term.

To begin, IBM Security Intelligence Operations and Consulting Services conducted a high-level, as-is assessment of NHS Digital's security capabilities and maturity levels using discovery activities such as workshops, interviews and documentation analysis. The team also conducted a gap analysis to identify areas of good practice and improvement using IBM methodologies and applied the IBM Digital Transformation Maturity Model to rate the importance and relevance of each of the evaluation criteria.

To support the DSC in its goal to becoming the most effective, mature and capable CSOC of its kind globally, relevant teams from IBM Security Strategy, Risk and Compliance Services defined the future-state SOM. This involved mapping the findings of the discovery process to capture eight specific views requirements: customer, risk, service, governance, organization, process, information and infrastructure.

IBM also developed the digital transformation roadmap, aimed at enhancing maturity level and driving improvement in 18 – 24 months by grouping the identified improvements into work packages. The work packages are prioritized to address critical areas first, and will be executed and re-evaluated across the four phases using agile methodologies.

For example, IBM worked with the DSC to optimize its in-house orchestration and security information and event management (SIEM) solution to more efficiently onboard new services, enhance the scale and pace of its security analytics capability, and increase the use cases to widen the malicious activity being monitored.

IBM also augmented the DSC CSOC with seasoned security analysts who work side-by-side with DSC analysts to gain a better understanding of the NHS and its threat landscape. The analysts also share IBM response best practices to enhance the maturity of the collective NHS security operation.

Threats are thwarted, faster

With support from IBM, the NHS Digital's DSC has matured the capability, scale and functionality of its CSOC consistent with that of an industry-leading service provider. In addition to providing a central source of cybersecurity intelligence and incident support to the NHS system, the CSOC acts as a single point of coordination with NHS and external partners.

Today, the CSOC can proactively detect, respond to and remediate security events more quickly, effectively and efficiently. It live monitors more than 1.2 million NHS devices for cyberthreats and vulnerabilities. On average, it blocks more than two billion malicious emails a year through targeted filtering. Since September 2018, it has stopped a number of zero-day attacks, and has blocked tens of millions of suspicious transactions on NHS and social care assets, including networks and computers.

According to NHS Digital, one of the key strategic benefits of working with IBM is the ability to take advantage of IBM's research insights, products and services, and partner network. "IBM brings the best of breed from the marketplace and its vast partner network to improve and enhance the capabilities of the DSC," says Shaw.

IBM also augmented NHS Digital's handling processes by providing threat intelligence capabilities and services, including the deployment of a new and tailored threat intelligence operating model.

In one instance, these enhancements supported the CSOC in detecting a large amount of suspicious traffic on the national NHS network. After identifying the Ramnit trojan as the source, the center immediately issued mitigation advice to affected local health and care organizations. NHS Digital also tested the trojan in a secure environment and used the insight to develop a rule preventing the malware from spreading further. In the end, the CSOC completed its response to the attack in less than 72 hours.

To help organizations and local partners identify and address potential threats quickly and effectively, the DSC provides articles on threat intelligence, creates custom alerts and offers threat scanning tools. As part of a wider training initiative for its 1,000-plus member Cyber Associates Network, NHS Digital also provides online training licenses for 500 IT and security staff in the NHS. In addition, it is part of the cybersecurity ecosystem in the UK, working closely with the National Cyber Security Centre.

> ***"The partnership with IBM allows NHS Digital's Data Security Centre to develop and grow faster to help keep patient information and services safe and secure."***
>
> —Rob Shaw, Former Deputy Chief Executive Officer and Senior Information Risk Owner, NHS Digital

Looking forward, NHS Digital continues to innovate, adapt and improve its services to meet the changing needs of its constituents and enhance its resilience against emerging security threats. For example, to gain real-time analysis of security alerts, it is moving critical national applications and services onto its SIEM system.

With support from IBM, NHS Digital is also developing its automated threat-hunting and machine learning capabilities. For example, the Data Security and Protection Toolkit, operated by the DSC, helps organizations identify their current security and compliance baseline and provides a roadmap for local improvement. To date, more than 27,800 health and care organizations have signed up for the toolkit. NHS Digital also supports organizations' adherence to NHS-specific standards, such as the 10 Data Security Standards prescribed by the National Data Guardian.

Recently, IBM and NHS Digital jointly developed the Cyber Security Innovation Factory, a place where people come to collaboratively identify cybersecurity threats and find solutions. The staff consists of employees with different skill sets within the NHS, NHS Digital and IBM, ensuring that everyone can contribute and innovate. Early successes of the Innovation Factory include a Cyber Policy Toolkit and the delivery of a Business, Intelligence and Risk platform, designed to help local organizations make informed and accurate decisions based on their local security risk exposure.

"IBM is not simply a supplier—it is one of NHS Digital's main strategic security partners supporting our Data Security Centre to help the wider NHS," concludes Shaw. "In partnership we are taking the best of both organizations to build resilience and response across health and care."

Solution components

- IBM® Cybersecurity Services
- IBM Digital Transformation Maturity Model
- IBM Security Intelligence Operations and Consulting Services
- IBM Security Strategy, Risk and Compliance Services

Take the next step

To learn more about the IBM solutions featured in this story, please contact your IBM representative or IBM Business Partner.

Please Recycle

10031010USEN-00