HALSTON GROUP X DIGITALXRAID

MEDTECH COLLABORATION SERIES

HALSTON GROUP

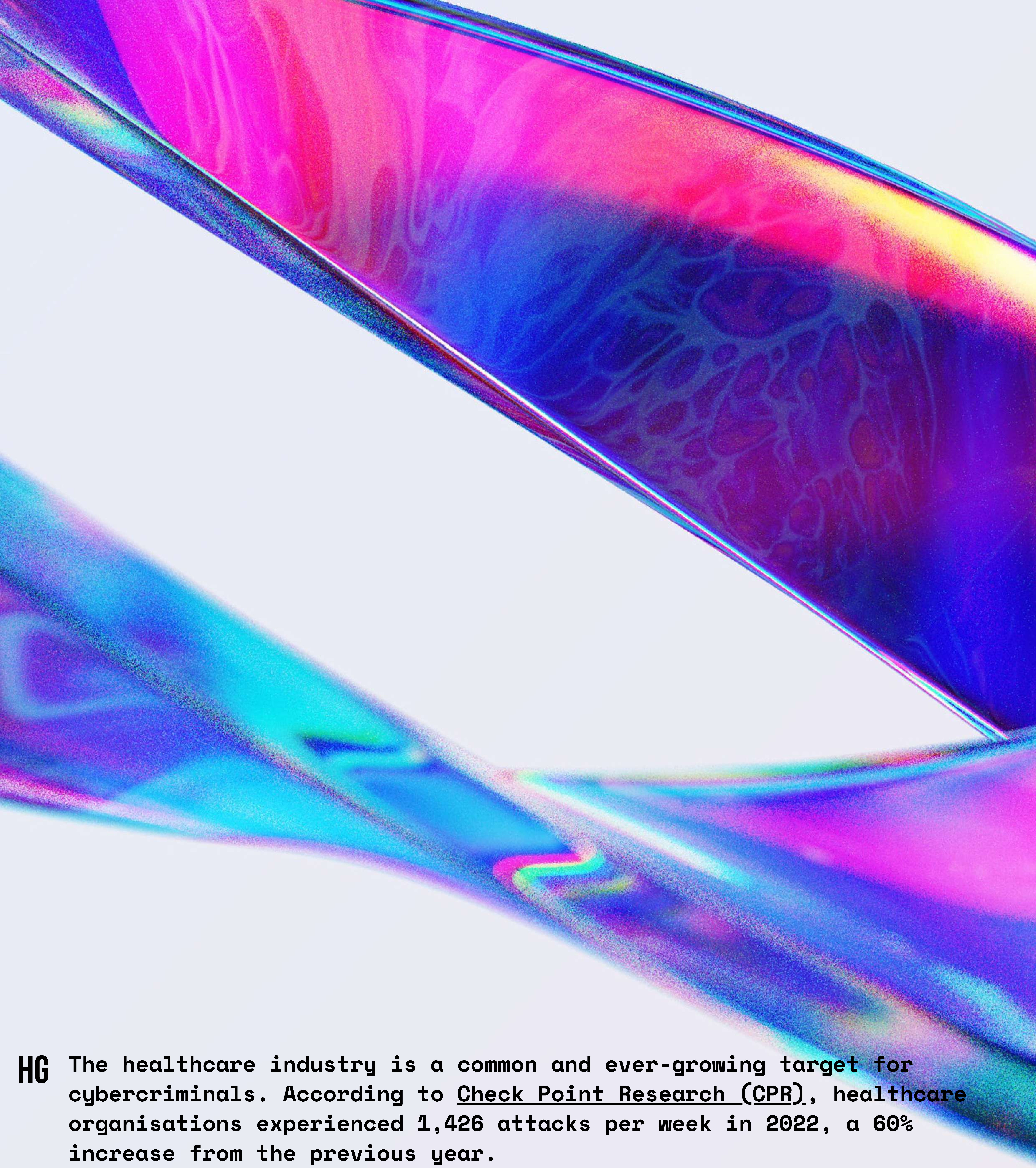
DigitalXRAID

THE MINEFIELD OF MEDTECH CYBERSECURITY

EXPLORING THE CYBER RISK IN HEALTHCARE WITH DIGTALXRAID

WHAT TO EXPECT

1. DIGITALXRAID X HEALTHCARE
2. THE PRIMARY TARGET
3. CASE STUDY: MEDICAL RESEARCH INSTITUTE
4. CHALLANGES IN HEALTHCARE CYBERSECRUITY
5. THE RISK BEHIND THE RISE OF WEARABLES
6. SECURING THE HEALTHCARE INDUSTRY: EXPERT ADVICE
7. THE FUTURE OF HEALTHCARE



The healthcare industry is a common and ever-growing target for cybercriminals. According to Check Point Research (CPR), healthcare organisations experienced 1,426 attacks per week in 2022, a 60% increase from the previous year.

The attacks are continuous, increasing in size and complexity, and for those in the sector, it is a case of when, not if. Whilst not all of these attacks will be made public, there are growing news stories around cyber attacks causing catastrophe in healthcare organisations. For example, just last month a cyber attack closed down emergency rooms in three US states, due to an attack on Ardent Health's IT infrastructure.

DIGITALXRAID X HEALTHCARE

HG To understand more about this stemming issue, we collaborated with DigitalXRAID which is at the epicentre of the cyber crime challenge.

DigitalXRAID is an award-winning managed security services provider with 25+ years' experience, dedicated to providing their clients with state-of-the-art cyber security solutions. They specialise in Vulnerability Management, Threat Intelligence, Information Security, PCI-DSS, Penetration Testing, Managed Security Services, Security Consultancy, and offer a fully managed Security Operations Centre (SOC) for complete cyber security protection.

Their company includes some of the highest qualified professionals in the country ready to safeguard your security. They are one of the elite few who hold both CHECK and CREST certifications alongside Cyber Essentials Plus, IASME Gold Standard, ISO 27001, and ISO 9001 accreditations.

With cutting-edge tools and techniques, they shield healthcare organisations from cyber threats, safeguard digital assets and ensure businesses stay two steps ahead of criminals.
We spoke with Rick Jones, CEO and Co-founder of DigitalXRAID, who has an impressive career spanning 25 years of delivering cybersecurity strategies and network security architecture to large corporates, to explore the security challenge facing the healthcare industry and what organisations can do to prepare.

THE PRIMARY TARGET

HG As discussed earlier on, the healthcare industry is a common target for cyber-attacks, but it is often considered the primary target amongst all industries. The reasoning behind it being the primary target stems from a number of places, one of the main ones being the sensitivity of the patient data that is held.

DX Healthcare is a prime target for cyber attacks because of the sensitive nature of the data it handles. Medical records are valuable on the black market due to their comprehensive personal information. Security is paramount in handling patient data due to the highly personal and sensitive information involved. A breach can lead to identity theft and medical identity fraud. Maintaining trust is critical; without it, patients might withhold crucial health information. Additionally, the sector often lags in updating cybersecurity practices and technologies, creating exploitable vulnerabilities. Aside from this, the NHS doesn’t necessarily have the resource or budget to put the right protection in place.

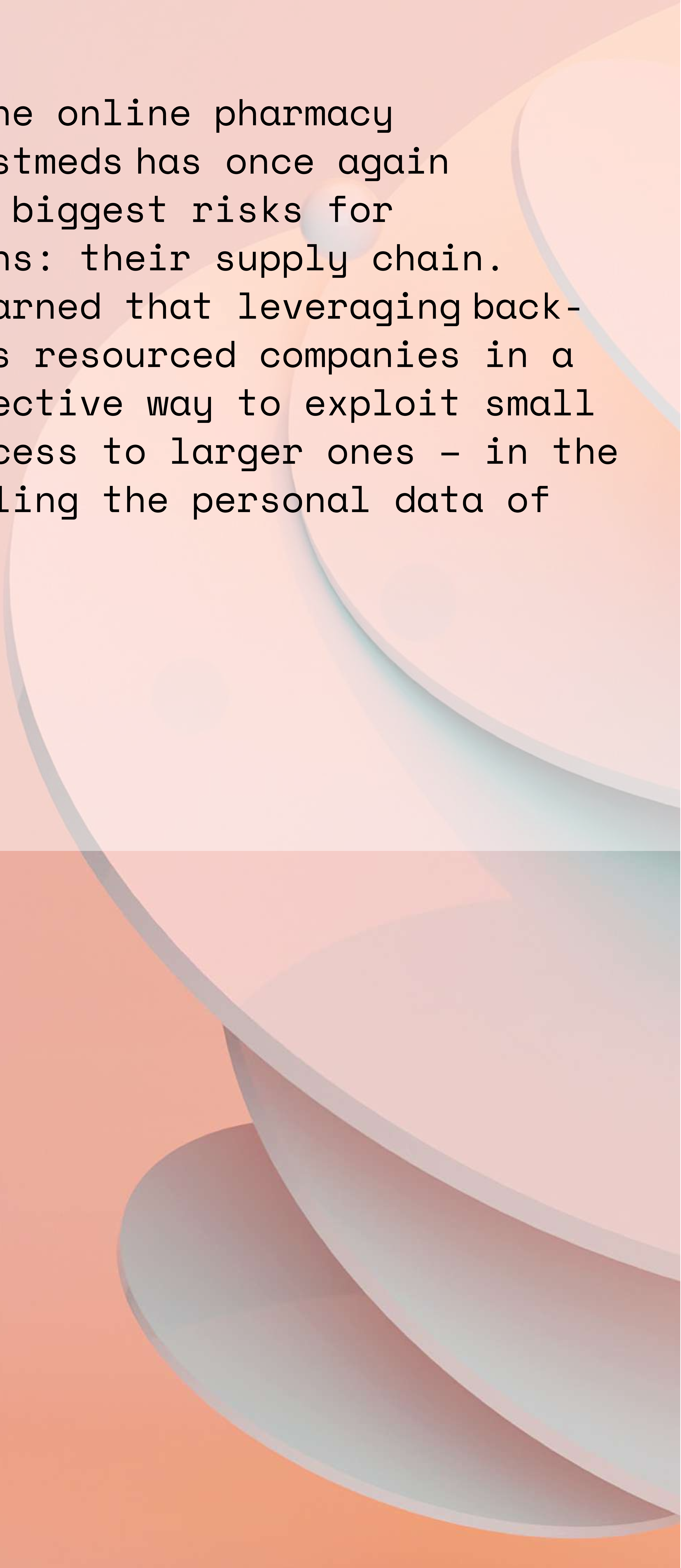
Cyber attacks have increased since Covid due to the accelerated digital transformation in healthcare. Remote work and telehealth services expanded attack surfaces. The urgency of the pandemic often led to rapid digital solutions deployment without thorough security checks.

HG Whilst the pandemic was a few years ago now, the ripple effects of those digital systems that are lacking proper cybersecurity measures are still causing vulnerabilities for healthcare organisations worldwide today, and we must continue our mission to rectify and protect these organisations.

THE PRIMARY TARGET

It's crucial that we continue to dedicate time and resource to boosting cybersecurity in healthcare. More so than other industries, breaches in healthcare can have a knock-on effect on reputation, even impacting the quality of care and confidentiality that healthcare providers can offer.

The recent breach of the online pharmacy fulfilment provider Postmeds has once again highlighted one of the biggest risks for healthcare organisations: their supply chain. Cybercriminals have learned that leveraging back-door entry through less resourced companies in a supply chain is an effective way to exploit small businesses and gain access to larger ones – in the case of Postmeds, stealing the personal data of 2.3 million patients.



CASE STUDY:

MEDICAL RESEARCH INSTITUTE

A UK based medical research institute, that specialised in Phase 1 and Phase 2 of medical trials, was supporting the Government by providing a no-cost Covid-19 testing service for NHS staff.
The research institute was also on standby to perform live trials of coronavirus vaccines for the Government.
The medical research institute operated with a highly diverse and dispersed infrastructure that included a hybrid cloud environment.

Succeeding a highly publicised breach by MAZE group during the COVID-19 outbreak, the research institute needed to secure its digital assets urgently.
Following a comprehensive impact assessment, DigitalXRAID were able to identify and agree a security action plan, which commenced immediately. Penetration testing was used to ascertain the research institute's current security posture and potential exposure to further attack.

DigitalXRAID's 24/7 Security Operations Centre (SOC) service, which is powered by Extended Detection & Response tooling, and is one of only a handful of its kind in the world due to its CREST accreditation, was implemented within a matter of weeks. A thorough incident response plan and investigation was conducted with the reports presented to government agencies both on and offshore.

CHALLANGES IN HEALTHCARE CYBERSECRUITY

HG The approach to cybersecurity is not a one size fits all - each system and architecture is unique, and as healthcare organisations grow and connect with emergent medical technologies, the network of systems grows in complexity but also vulnerability. Rick explains the challenges that are faced sector-wide, but homes in on those especially prevalent to the NHS.

DX The healthcare sector struggles with cyber security due to legacy systems, a lack of standardised protocols, budgetary constraints, and a talent gap. The primary focus on patient care sometimes leads to cyber security being a secondary concern.

In terms of legacy systems, in the NHS many of the medical systems were very expensive to purchase initially, but are either built on an old PC or will not be built for such a fast-moving industry and yet will be around for a considerable amount of time. Where within the private sector, it'll be seen as deprecated, no longer supported ,and thereby removed. So, the way the world works is not necessarily how MedTech or the NHS work. The sensitivity of these systems means that once breached, the attackers could even change medical records, which is devastating. In the NHS and with your doctor there is an inherent trust, but if people are worried about their data being stolen, the trust has gone, and patients may hold back on providing crucial information.

HG The healthcare sector is presented with so many challenges that are unique to the industry, but the threat landscape is tense. With the growing occurrences of cyber-attacks being felt across a multitude of industries, this can be partly attributed to the fact there are more criminals entering the hacker field.

CHALLANGES IN HEALTHCARE CYBERSECRUITY

DX Historically, there used to be strong barriers to entry in terms of becoming a hacker. It used to require someone with expertise and a certain skill set, which there is still, but what we're seeing now is organisations running as businesses that are building tools and hiring expert criminals to run phishing or hacking attacks, and it is becoming less complex to run an attack. AI-based tools are also making it easier for someone to orchestrate a cyber attack.

THE RISK BEHIND

THE RISE OF WEARABLES

HG Wearable medical devices are reshaping healthcare, but as the technology evolves rapidly, the speed of cybersecurity embedded within hasn't always kept pace. Therefore opened the door to vulnerabilities as a weak end point for hackers to target.

DX Wearables and IoT devices in healthcare introduce risks due to their extensive data collection and connectivity. Wearables are at the bleeding edge of technology in terms of IoT, and these devices are often designed with a focus on functionality, not security, and connect to various networks, increasing the risk of breaches. A security approach really needs to be indoctrinated into the design process of IoT wearables because they are creating vulnerabilities that may not necessarily be considered. The Security Act is a step forward in terms of introducing regulations and making sure that cybersecurity is within the hardware or architecture of wearables. There was a period where IoT devices were effectively open to DDoS (distributed denial-of-service) attacks by overwhelming the target with requests. So, there have been positive changes, but the space is moving so fast that you are inherently open to vulnerabilities.

For MedTech wearable developers, incorporating robust security measures is crucial to protect patient data and comply with regulatory standards. Healthcare facilities must ensure the security of connected wearables to protect their networks and prevent cyberattacks.

MedTech companies should embed security from the start, conduct comprehensive risk assessments, stay updated with regulations, invest in continuous monitoring, partner with cybersecurity experts, educate staff, focus on data encryption, and regularly conduct penetration tests and security audits.

SECURING THE HEALTHCARE INDUSTRY

EXPERT ADVICE

HG **The devasting consequences of a cyber attack are front and centre right now, with the increasing frequency and public announcements of hospital breaches. But as the risk is looming, protection against attacks is very achievable. Rick gives his advice to those healthcare organisations looking to strengthen their cybersecurity protocols and protect against those inevitable attacks.**

DX To mitigate this risk, healthcare organisations need to be proactive and demand more from their suppliers and partners. At a minimum, these organisations should contractually agree data breach liability with third parties, but they should also build out security defences that prepare for the worst. Regular cybersecurity awareness training alongside implementing a Zero Trust architecture will also reduce risk and halt lateral movement of attackers inside a network. Given the highly sensitive data held by healthcare organisations and the growing threat landscape, investing in extended detection and response by outsourcing to a Security Operations Centre, or SOC, is becoming increasingly essential.

EXPERT ADVICE

DX The bigger the organisation, the more complex and harder it is to manage from a security perspective. Incorporating security measures must be a central consideration and those in healthcare IT departments need to be:

- Regularly conducting risk assessments, be that through penetration testing or standard policy procedures.
- Making sure the data held abides by the regulations in the sector, such as GDPR, HIPAA, DSP.
- Investing in monitoring solutions so that when the inevitable happens it can be remediated quickly and effectively.
- Partnering with cybersecurity experts; focus on quick wins internally and then utilise the expertise of sector specialists for more complex activities.
- Conducting awareness and training programmes for all employees and ensuring to create a culture of openness.
- Ensuring data is encrypted, both at rest and in transit.
- Exploring PEN testing audits to provide assurance that any new systems being developed are tested before they are released.

Those in cybersecurity need to be at the forefront of technology and leading the way in terms of identifying new emerging threats. DigitalXRAID is comprised of cybersecurity specialists who are able to understand your assets and how they are exposed through potential vulnerabilities. We stay ahead of this evolving market, both from a risk and regulation perspective. We live and breathe it every day, and see threats across multiple industries, and anticipate what could be emerging in the healthcare sector.

THE FUTURE OF HEALTHCARE

HG The healthcare industry will continue to innovate, adopt, and evolve with digital technologies, and will need to prioritise security to protect patient data. Rick gives his perspective on what the cybersecurity landscape could look like in the coming years.

DX I think cybersecurity will become more and more embedded, alongside the fact that the knowledge around IT, IoT, and cybersecurity is increasing. Therefore, people are understanding from a budgetary perspective that they need to separate cybersecurity as its own standalone cost, which is very important to deliver adequate budgets for the tasks that are needed.

DIGITALXRAID IS SAFEGUARDING THE HEALTHCARE INDUSTRY AGAINST IMMINENT CYBER ATTACKS.

THE MINEFIELD OF MEDTECH CYBERSECURITY

EXPLORING THE CYBER RISK IN HEALTHCARE WITH DIGTALXRAID

Published by Halston Group

halstongroup.co