LORCA NEEDS ACCELERATOR: HEALTHCARE

LORCA

Healthcare is evolving into a new era of interconnectivity where organisations, professionals and patients will be connected through digital technology to make healthcare more personalised and predictive.

This will likely be driven by increased data sharing and the predictive power of advanced analytics and AI, leveraged in near real time to deliver tangible clinical outcomes.

As healthcare organisations (HCOs) pursue these initiatives, the use of the Internet of Things (IoT) and connected medical devices in healthcare settings will increase, while remote and virtual healthcare will become widespread.

Covid-19 greatly accelerated change in some of these areas and changed risk appetites almost overnight.

Electronic health records were shared across new regions and infrastructures, while telemedicine, remote working and remote monitoring devices became the norm. At the same time, the threat landscape intensified as bad actors exploited the pandemic to conduct pandemic-related scams and attacks against healthcare organisations.

LORCA brought together a group of cyber industry leaders, policymakers and innovators to explore how these shifts will affect the security landscape of the healthcare sector.

HELD UNDER THE CHATHAM HOUSE RULE, OUR VIRTUAL DISCUSSION UNVEILED THE FOLLOWING NEEDS AND PRIORITIES

1. Protecting confidentiality and privacy in data sharing initiatives
2. Protecting the confidentiality and integrity of data when it’s shared
3. Data availability during ransomware attacks
4. Frictionless security solutions and prioritising patient care
5. Securing a hybrid IT infrastructure that includes the cloud and legacy IT
6. Managing heightened security risks with few available resources during the pandemic

PROTECTING CONFIDENTIALITY AND PRIVACY IN DATA SHARING INITIATIVES

Protecting the confidentiality of patient data is key to the success of data sharing initiatives in the healthcare sector. HCOs often implement privacy solutions like data anonymisation techniques to protect the confidentiality of people's medical data. But data anonymisation is an ongoing research area and no existing privacy solution currently ensures that data can be used as intended while remaining 100% secure.

Attendees noted that past data sharing initiatives like Care.data (a programme that aimed to extract data from GP surgeries into a central database) have failed because the public was concerned that their data wasn't secure. HCOs have found that implementing rigorous data protection and privacy controls isn't sufficient. They must also communicate these privacy controls to the public to get their buy-in.

Policy-related barriers and operational siloes can also prevent data being shared securely and efficiently. HCOs can overcome these challenges by developing secure data sharing models that take all parties involved – and the context in which data is being shared – into consideration. For example, medical data shared with vaccine developers during the pandemic will require different privacy controls depending on whether the data in the hands of a clinician or a researcher.

Innovators can support the healthcare sector by developing data protection and privacy solutions that enable data to be shared securely. Innovations in the area of data anonymisation that allow for least-privilege Identity and Access Management (IAM) controls to be implemented could bring real benefits to HCOs.

And when developing these solutions, innovators should remember to communicate the privacy benefits of their solutions in a way that's transparent and accessible to the general public.

PROTECTING THE INTEGRITY OF DATA WHEN USING AI

Modernising and digitising healthcare services could have unintended consequences for patient health. For example, there may be ethical considerations around combining data with AI.

People can't always see the underlying computational processes behind these technologies, so the user can't know if the data or technology has been compromised. Attendees stated that there's a need to make sure that the computational processes of these tools are transparent, easy to explain and verifiable.

Attendees thought that AI could change the emphasis from protecting the confidentiality of data to protecting the integrity of data. If the accuracy or integrity of data is compromised, it could lead to significant and direct negative healthcare outcomes.

Threats to data integrity could come from bad actors or from a lack of governance over tools. One attendee described a situation where the US declared a cholera outbreak because an analytics tool identified a surge in the number of people searching for the term "cholera", for example. This surge was later attributed to a book club suggestion made by Oprah Winfrey. Examples like these show how assuming the accuracy of data used by analytics tools and AI could lead to unforeseen consequences that affect patient health or the delivery of healthcare services.

HCOs are looking to regulators to develop guidelines around the governance of these tools. Meanwhile, innovators can support HCOs by developing tools that detect and prevent data integrity attacks.

DATA AVAILABILITY DURING RANSOMWARE ATTACKS

Attendees told us that the healthcare sector is protected from physical attacks (deliberate acts of violence against healthcare facilities are prohibited under international humanitarian law, for example) but there are no similar protections when it comes to cyber attacks. This means that bad actors are not dissuaded from attacking the healthcare sector during times of crisis.

As a result, HCOs have experienced an increase in ransomware attacks during the pandemic. Sophisticated threat actors (including nation state actors) are targeting healthcare, life sciences and pharmaceutical companies to gain information about vaccine production.

But even though these attacks are coming from sophisticated threat actors, they're currently exploiting known vulnerabilities like end-of-life or unpatched legacy hardware, systems and applications. Many HCOs have sought external help to mitigate the risks from legacy IT and manage ransomware attacks, but they lack the financial resources to address the problem.

Attendees stated that their priority during a ransomware attack is to maintain the availability of patient data so that healthcare services can continue. HCOs can achieve this by assessing their business continuity and disaster recovery processes.

Innovators can help HCOs to prevent ransomware attacks from propagating through the network. For example, network segmentation solutions that are built on zero trust principles may provide security benefits to HCOs.

FRICTIONLESS SECURITY SOLUTIONS AND PRIORITISING PATIENT CARE

Insiders who attempt to bypass security protocols can compromise the security of data or digital infrastructures. The threat from insiders has increased during the pandemic due to the rise of remote working and remote healthcare services. Attendees described situations where clinicians bypassed cumbersome remote security controls like Virtual Private Networks (VPNs) and Software-as-a-Service (SaaS) platforms by using shadow systems and IT.

Attendees also described examples where clinicians were uploading information to medical forums to access a second opinion when they didn't have the tools to communicate with and consult with colleagues remotely.

Clinicians and general practitioners use shadow IT and systems rather than more secure but cumbersome systems because this makes providing patient more easy. One attendee said that if they asked a clinician why they were using shadow IT, they may respond with "I'm trying to save a life". IT departments can't simply reject the use of shadow IT or systems.

Instead, they need to streamline their current security processes and solutions to make it easier for healthcare professionals to deliver patient care. Where this is not possible, security professionals will need to find a way to secure shadow IT and protect data wherever it resides.

HCOs can address this issue by assessing their current security processes and systems and evaluating their effect on healthcare delivery.

Innovators can help HCOs to manage the risks of shadow IT and systems by developing security solutions like endpoint management tools that are frictionless, easy to use and don't get in thew way of delivering patient care.

SECURING A HYBRID IT INFRASTRUCTURE THAT INCLUDES THE CLOUD AND LEGACY IT

Historically, the healthcare sector has used on-premises data centres, developed bespoke applications and relied on medical devices with a long shelf life. As a result, many HCOs have a lot of legacy IT in their infrastructure. This reliance on legacy makes HCOs vulnerable to attacks, but they also have a low tolerance for downtime.

Many HCOs have turned to the cloud to modernise their infrastructure, but even cloud companies have built in security and privacy as an afterthought rather than by design. At the same time, the lack of funding in the sector means that not all legacy systems and IT can be replaced. This means that the end-state infrastructure for many HCOs will be a hybrid cloud model that includes legacy devices.

Greater connectivity across the healthcare ecosystem – due to the rise of IoT, data sharing initiatives and remote healthcare applications – makes this hybrid infrastructure model more vulnerable. For instance, new remote healthcare customers could potentially connect to applications hosted in the cloud using compromised personal devices, allowing sophisticated attackers to move laterally through the network to compromise on-premises applications and devices.

HCOs can gain a thorough understanding of the risks and vulnerabilities associated with a hybrid, IT environment by understanding what's hosted on premises and how it connects and interacts with the cloud. No single solution can secure this infrastructure. Instead, multiple security concepts will be required, such as network segmentation, identity solutions, endpoint management and end-to-end visibility.

Innovators should be mindful of HCOs' need to maintain and secure legacy IT by developing tools that directly secure legacy IT or protect the wider infrastructure.

MANAGING HEIGHTENED SECURITY RISKS WITH FEW AVAILABLE RESOURCES DURING THE PANDEMIC

The threat landscape for the healthcare sector intensified during the pandemic. Cyber criminals who usually focused on the finance sector switched to conducting Covid-19 related scams, and sophisticated nation state actors began to target research institutes and hospitals.

Meanwhile, to ensure the continuity of healthcare services during lockdown, HCOs changed their risk appetite. IT and security professionals were tasked with rapidly implementing and scaling new remote working and healthcare services, often without adequate security controls in place.

Traditionally, IT and security departments in the healthcare sector are small and experience a high turnover rate. These departments don’t always have the in-house capability to manage emerging threats. As a result, security professionals in the healthcare sector are struggling to manage sophisticated cyber threats at a time when their digital infrastructure is vulnerable.

Attendees told us they will need to address the security decisions made during the pandemic by reviewing the security weaknesses and processes in the remote healthcare solutions that were implemented quickly and at scale.

Innovators should be mindful of the pressures that the healthcare sector is currently experiencing. Solutions should be cost-effective and easy to implement.

THE INNOVATION OPPORTUNITY: ENABLING EFFICIENCY, SECURING DATA AND PRIORITISING PATIENTS

The future of digital health is arriving – and soon.

The rise of data sharing, analytics, AI and IoT in healthcare environments is transforming the security landscape.

But many HCOs feel they're still trying to address the same security issues they were facing 10 years ago, such as protecting data shared across the ecosystem, securing legacy devices and defending against ransomware attacks.

Security professionals are also having to manage these issues during a crisis. They're trying to secure their infrastructure against a new threat landscape, and cyber startups can support the healthcare sector by offering innovations in areas such as:

- data protection and privacy
- securing data to enable the use of data analytics and AI
- network segmentation and endpoint management

When designing security products and services for the healthcare industry, innovators should keep industry-specific challenges in mind. Innovators should clearly communicate how their solution can improve patient care and the efficiency of healthcare services.

CONNECT WITH US

lorca.co.uk
info@lorca.co.uk

Twitter: @LORCACyber
LinkedIn: LORCA Cyber

FIND US

Plexal, The Press Centre Here
East, 14 East Bay Lane
Queen Elizabeth Olympic Park
London, E20 3BS

LORCA BY plexal