EVIDEN

Attacks on the system

Boosting security in healthcare

Contents

With cyberattacks increasing in healthcare, we explore the impact of today's targeted attacks, highlight 2023's key investment areas and look at why security is a board level issue, not only an IT responsibility, that constitutes a business challenge.

Analyzing attacks on healthcare systems

In the increasingly digital world of healthcare, few senior leaders are unaware of the broader issues surrounding security and information governance, or the need to effectively secure systems and data to prevent breaches.

Certainly, over the past few years we have seen hospitals and health systems increasing targeted by ‘bad actors’. In the US between January 1 to October 31, 2023, for example, 551 successful data breaches against healthcare providers were reported with more than 82.6 million healthcare records being exposed or stolen[1]. In 2023, 60% of healthcare organizations reported being affected by ransomware[2].

[1] https://www.hipaajournal.com/healthcare-data-breach-statistics/
[2] Sophos study “The State of Ransomware in Healthcare 2023”

Millions of patient records were exposed and healthcare delivery was disrupted in both the US and Europe due to major cyberattacks in 2023. The US saw its largest hospital system, HCA Healthcare, suffer a major data breach in July, exposing the sensitive information of up to 11 million individuals, including names, addresses, dates of birth, and healthcare details.[3]

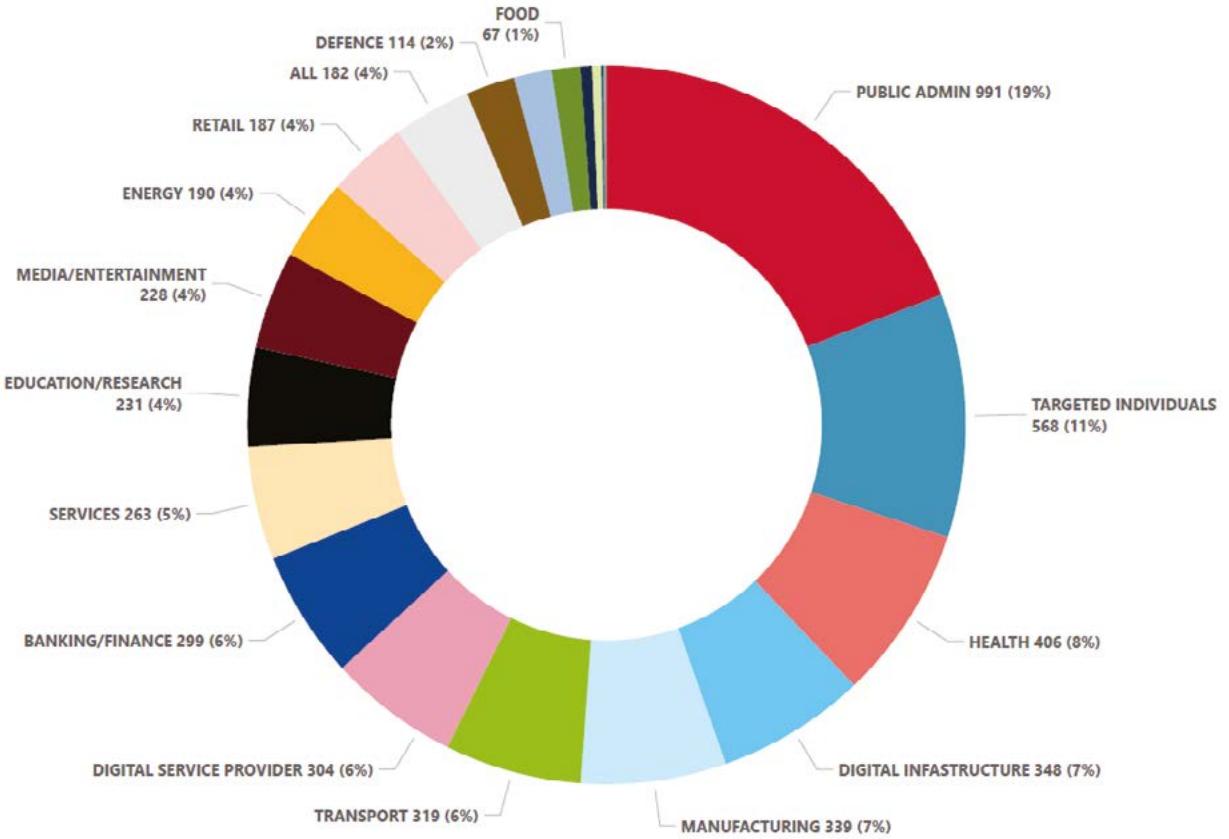
Similarly, a July attack in Europe crippled access to digital health records for several ambulance services across the UK, forcing paramedics back to pen and paper.[4]

Already in 2022, following the Russian invasion of Ukraine, UK health secretary Sajid Javid warned that cyberattacks had become an established form of conflict. This promoted NHS England to advise Trusts to ensure systems were “patched and protected, and that immutable backups are in place”[5]. The US Cybersecurity and Infrastructure Security Agency too issued a similar ‘shields-up’ warning to the healthcare sector.

[3] https://www.cshub.com/attacks/news/hca-healthcare-data-breach-impacts-11-million-patients
[4] https://www.infosecurity-magazine.com/news/supply-chain-attack-hits-nhs/
[5] https://www.healthcareitnews.com/news/emea/nhs-bolster-cybersecurity-following-russian-invasion-ukraine

Geopolitical events aside, there is no doubt that hospitals have been in the firing line for some time – from criminal hackers looking to extort money to well-funded statesponsored hackers bent on creating maximum disruption. And as digital perimeters expand, the threat is heightened and the need for constant vigilance and tougher security measures continues to grow. Indeed, according to the European Union Agency for Cybersecurity, attacks against the healthcare sector surged in 2023 [see figure 1].

Figure 1: Targeted sectors per number of incidents (July 2022 - June 2023)



Source: ENISA Threat Landscape Report 2023

https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

How is the impact of these cyberattacks being measured today?

A security incident in most sectors usually results in financial, legal and reputational damages. A major factor to consider in healthcare is that patients are also more and more affected. According to the Ponemon study “The Impact of Ransomware on Healthcare During COVID-19 and Beyond” published in September 2021, healthcare delivery organizations (HDOs) had to deal with strong impact on patient care after being the victim of successful ransomware attacks.

71% of HDOs reported a longer length of stay for their patients

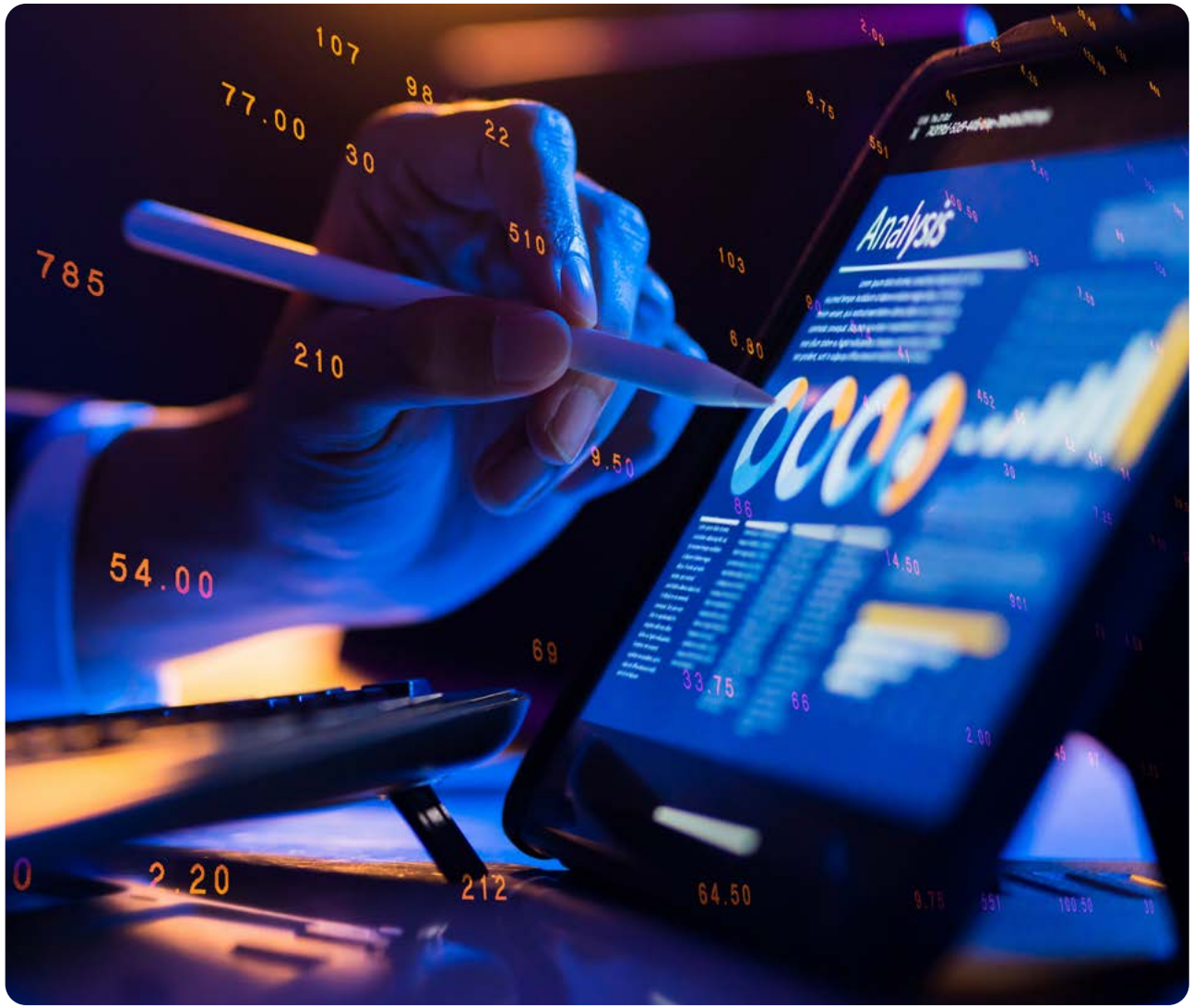
70% of them stated that the attack delayed most procedures and tests

65% of them saw an increase in patients having to be transferred to other facilities

Knowing that attacks are coming is not the same as being in a position to combat them. Similarly, knowing which solutions are needed (regular patching, next-gen firewall, multifactor authentication for access management, penetration testing and so on) isn't the same as having them all deployed across networks.

Security investments need to be balanced against the clinical needs of the organization, the availability of trained IT staff, shared risk approaches with partners, the raft of compliance issues and much more.

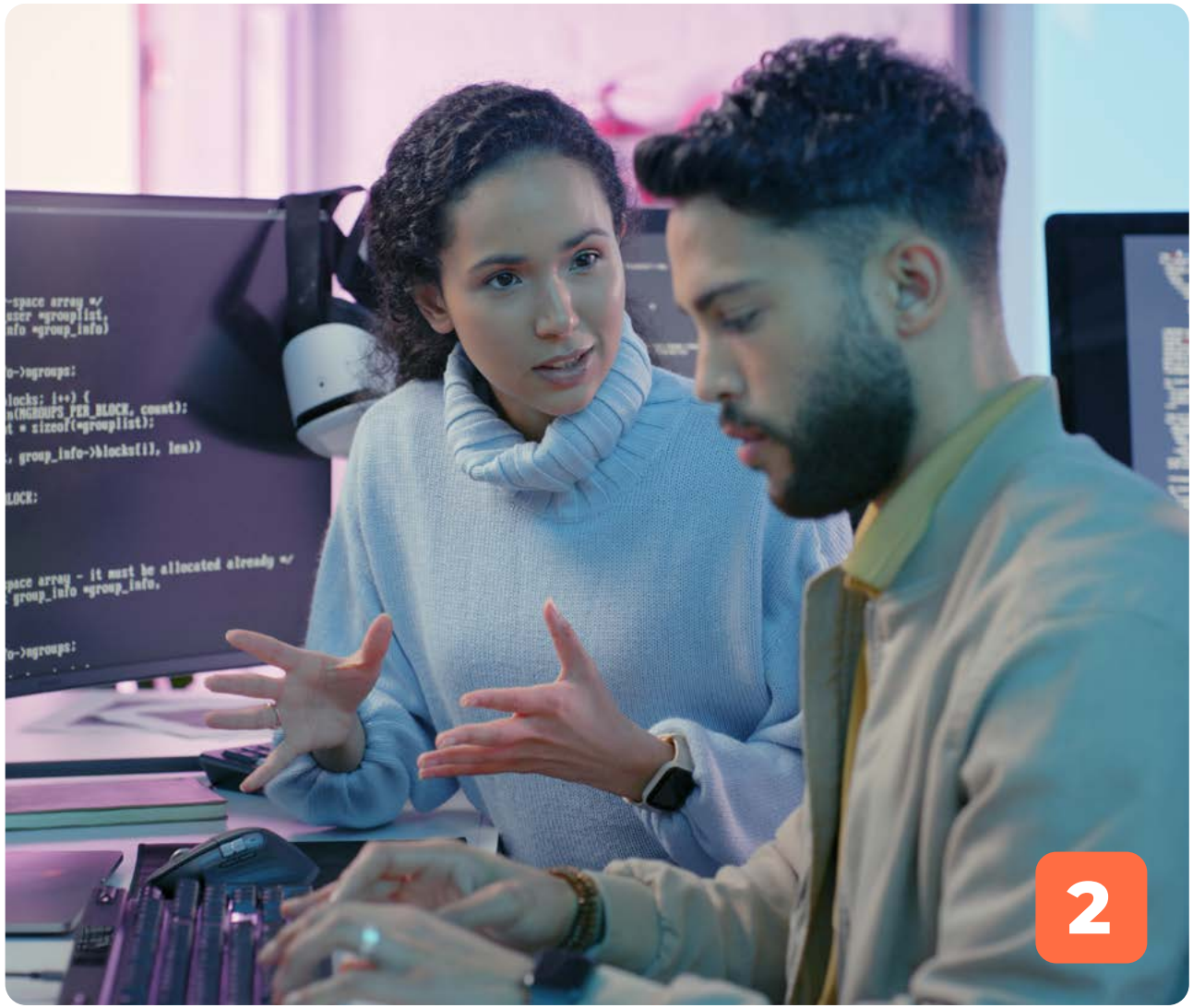
There may be a clear and present danger, but the path to building a stout defence isn't always quite so straightforward.



Cybersecurity: where does responsibility rest?

Ed Duryee, Columbus Regional Healthcare System's Director of Information Systems, stated that security is a board level issue, not an IT responsibility. It's a perceptive point.

While it's the CIO/CISO teams that will certainly be evaluating potential threats, selecting the cybersecurity suppliers and solutions, and managing the IT environments, the impact of a successful attack is much wider than this one department. Indeed, it goes right to the heart of patient delivery, consumer trust and to the continued operation of the facility itself.



Successful cyberattacks are not just a threat to patient care, they're also costing healthcare organizations a lot. Sophos' "The State of Ransomware in Healthcare 2023"[6] report paints a concerning picture. 42% of healthcare providers felt pressured to pay hackers to recover critical data while median ransom skyrocketed: healthcare organizations paid a median ransom of $2.5 million in 2023, a huge increase from $30,000 in 2022.

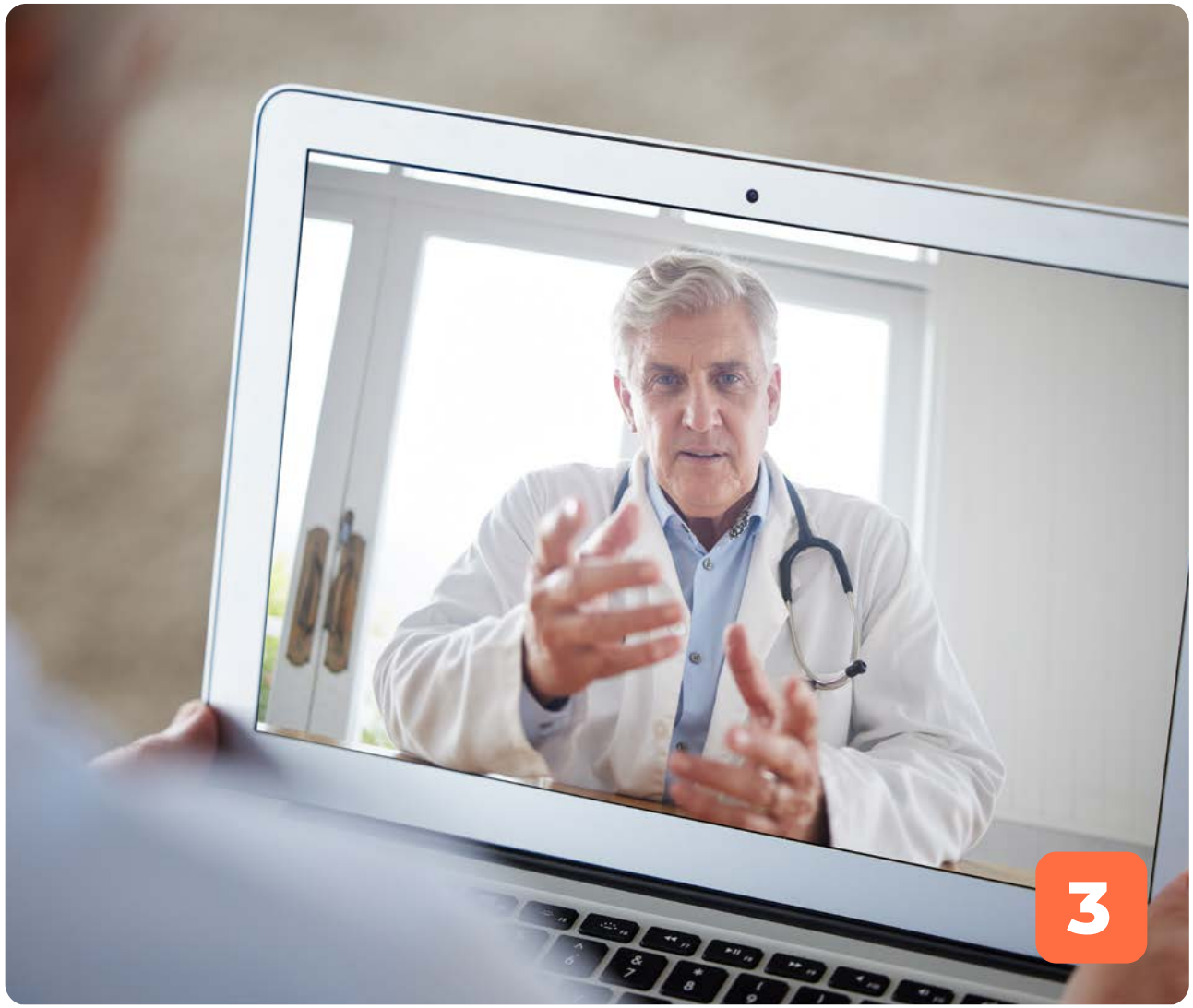
Moreover, ransom payments are just the tip of the iceberg. Recovery costs in healthcare significantly exceed the cross-sector average of $1.82 million, reaching $2,20 million. 85% of private-sector healthcare organizations reported lost business due to attacks. Even more concerning is the slowing recovery rate – only 47% can recover within a week, compared to 54% last year.

Healthcare was the top industry in terms of average total cost of a data breach, with a estimated $10.93 millions in 2023, followed by the financial sector ($5,90 millions) and the pharmaceuticals industry ($4,82 millions). And, in many healthcare markets, the financial costs can also be felt through cancelled procedures and fines for missed targets.[7]

[6] Sophos study "The State of Ransomware in Healthcare 2023"
[7] IBM Cost of a Data Breach Report 2023 https://www.ibm.com/reports/data-breach

Where to focus investments in 2024

There is undoubtably a need for healthcare organizations of all sizes to act, and do so in a holistic way. Increasingly, a risk-driven, zero trust strategy is the 'go-to' approach as healthcare organizations move away from point solutions into a more integrated security model. And, as we move through 2024 and beyond, the following will be the top investment priorities.



Visibility.

You cannot protect what you cannot see.

Organizations will invest in risk-based vulnerability management tools to improve internal visibility and enhance operational efficiency. Many successful cyberattacks exploit known vulnerabilities. Hospitals must therefore improve their vulnerability management programs by adopting vulnerability prioritization technologies and combine them with autonomous pen-testing platforms for better results. It will also be important to invest in technologies that bring external visibility to their assets, such as digital risk protection services, cyber threat intelligence and security risk rating services.

Zero trust.

Never trust, always verify.

Hospitals will embark on (or accelerate) their zero trust journeys to reduce risk and simplify access management for staff. While there's no single path to zero trust, hospitals will focus their approach on their level of maturity. Starting with remote access and identity management of people, devices and objects will provide a solid foundation.

Hybrid cloud security.

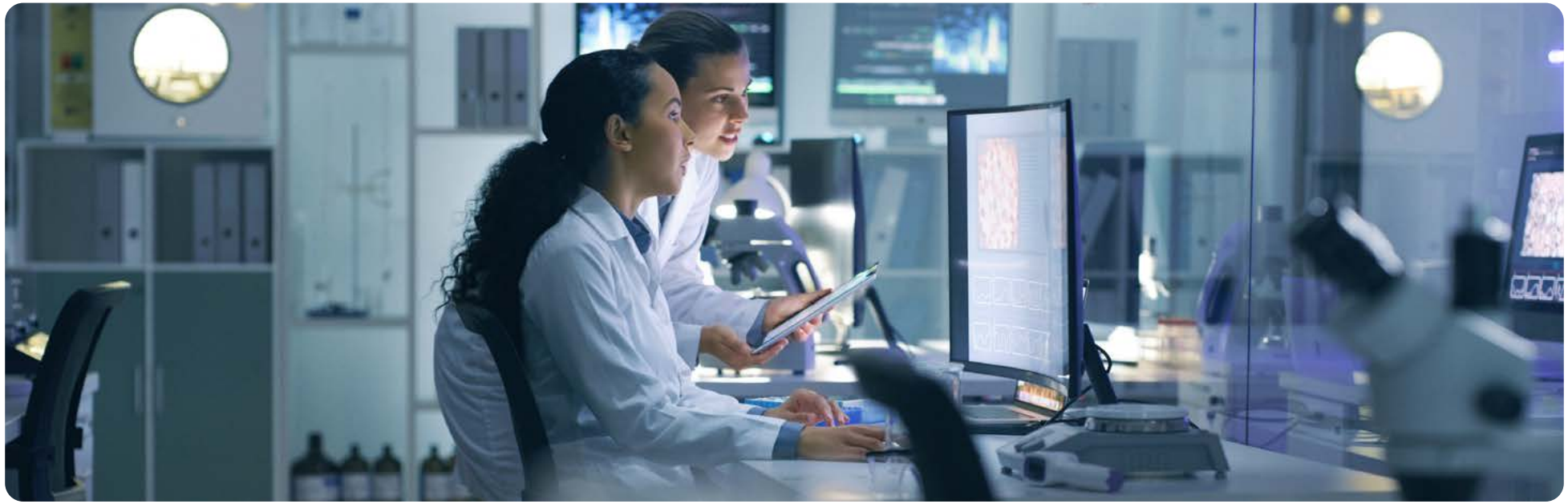
Bring trust to the cloud.

With more patient, personal and operational data in more places, hospitals will need to implement a layer of security control across their systems. Adding a new layer of trust will secure the applications and data across multi-cloud and hybrid cloud environments, and help support compliance.

Connected medical devices protection.

Securing the devices that process your health data.

The Internet of Things (IoT) continues to transform the healthcare industry, providing more innovative solutions for patients and healthcare providers. The average patient bed currently has 10-15 connected medical devices on average and can be an entry door for hackers. It is essential to know what devices are active and inactive within your system through asset discovery and then to actively monitor, manage their lifecycle and secure them.



Managed detection and response.

Turning the tables on cyber criminals.

Managed detection and response (MDR) solutions will help anticipate and detect complex attacks using artificial intelligence algorithms to detect and orchestrate a response in near-real-time. These advanced platforms will integrate a host of applications within a single platform, including security information and event management, security orchestration automation and response, user behavioral analytics, endpoint detection response and more.

Adopt best practices.

Get the basics right

In addition to leveraging state-of-the-art security technologies above, getting the basics right around up-to-date patching, a good security hygiene, a solid backup and recovery program, staff security awareness training and fast incident response will all support a more secure healthcare environment.

Expert support on your journey

In this new healthcare ecosystem, patient sensitive data needs to be protected across a complex network of people, technologies and information.

This cannot be achieved by the CISO function alone and requires education of, and buy-in from, senior hospital budget holders. Similarly, embedding appropriate level of cybersecurity is not an overnight fix or a linear journey. And, of course, it can be complex – particularly as focus shifts to deep learning and artificial intelligence technologies.

It's critical then that security solution keep pace with the healthcare providers and payers' innovation – so they can operate with complete trust. Sensitive data must be protected, but still be easily accessible, and today's increasingly connected medical devices and clinical application access points must also be protected and secured to avoid compromising the wider organization.

With a proven track record of digital compliance and cybersecurity in complex IT healthcare environments, Eviden can help providers and payers do it all – while containing costs.

Find out more: visit our cybersecurity pages **here**

About Eviden[1]

Eviden is a next-gen technology leader in data-driven, trusted and sustainable digital transformation with a strong portfolio of patented technologies. With worldwide leading positions in advanced computing, security, AI, cloud and digital platforms, it provides deep expertise for all industries in more than 47 countries. Bringing together 47,000 world-class talents, Eviden expands the possibilities of data and technology across the digital continuum, now and for generations to come. Eviden is an Atos Group company with an annual revenue of c. € 5 billion.

[1] Eviden business is operated through the following brands: AppCentrica, ATHEA, Cloudamize, Cloudreach, Cryptovision, DataSentics, Edifixio, Energy4U, Engage ESM, Evidian, Forensik, IDEAL GRP, In Fidem, Ipsotek, Maven Wave, Profit4SF, SEC Consult, Visual BI, Worldgrid, X-Perion. Eviden is a registered trademark. © Eviden SAS, 2024.

Connect with us

eviden.com

ECT-240304-JR-EVIDEN ATTACKS ON THE SYSTEM EBOOK