Threat Detection for Healthcare:

Rejuvenating Cyber Defence Strategies for a Vulnerable and Fast-Moving Sector

Table of contents

Foreword

Healthcare's need for speed:

Three quarters of cyber security decision makers in the Healthcare space would relinquish some control in exchange for quicker decision making

The life of the CISO isn't going to get any easier in 2024, as organisations across all sectors contend with rapidly evolving extortion techniques such as phishing, ransomware, and supply chain attacks to invade internal networks. e2e-assure's recent study* shows there is a genuine cause for concern for the Healthcare industry, with 77% of Healthcare organisations reporting they've experienced a cyber attack. Despite this huge threat, 31% believe their provider or in-house team is underperforming and are therefore looking to make changes.

Given its access to sensitive information, the industry will always be highly susceptible to cyber attacks. A strong relationship with providers is integral to cyber resilience, especially for fast-moving Healthcare organisations that are often faced with the challenge of legacy systems. The rise of the Internet of Things hasn't helped, providing attackers with new portals to personal medical information in real-time.

When an incident occurs, collaborating with providers can enhance an organisation's response capabilities, offering rapid assistance and plugging gaps that could be missed by an in-house team working alone. This is particularly important to an industry that is time poor and understaffed.

So why are almost a third of Healthcare organisations looking to make a change?

At e2e-assure, we have been working with Healthcare firms to shore up their cyber defences for the past ten years and are repeatedly called upon to help in the aftermath of an attack. But we need to consider the provider's role before the incident, to prevent it completely. Particularly those that are dealing with new forms of technology, and don't have the time or capacity to keep up with ever-evolving threats.

So, how are providers failing Healthcare organisations? And what questions should the industry be asking their cyber security providers, to drive better resilience for a sector forever vulnerable?

Rob Demain
CEO e2e-assure

Introduction

When a data breach and the subsequent downtime has an impact on patient care, catching it and managing it rapidly is imperative. Skills shortages and employee burn out within the Healthcare sector means staff members are time poor, and don't have the capacity to manage the fall out of a cyber attack.

It makes sense therefore, that the majority of Healthcare organisations either fully outsource their cyber security operations (41%) or have a hybrid approach (40%), which is higher than the average across other industries (34%)*.

Unfortunately, only 13% of Healthcare organisations believe their cyber security provider or in-house team is exceeding expectations, which is lower than the average at 16%*. Nearly one in three (31%) believe their provider or in-house team is underperforming and are looking to make changes.

41%

are fully outsourced

40%

hybrid

16%

fully in-house

77%

have experienced a cyber attack

Only **13%**

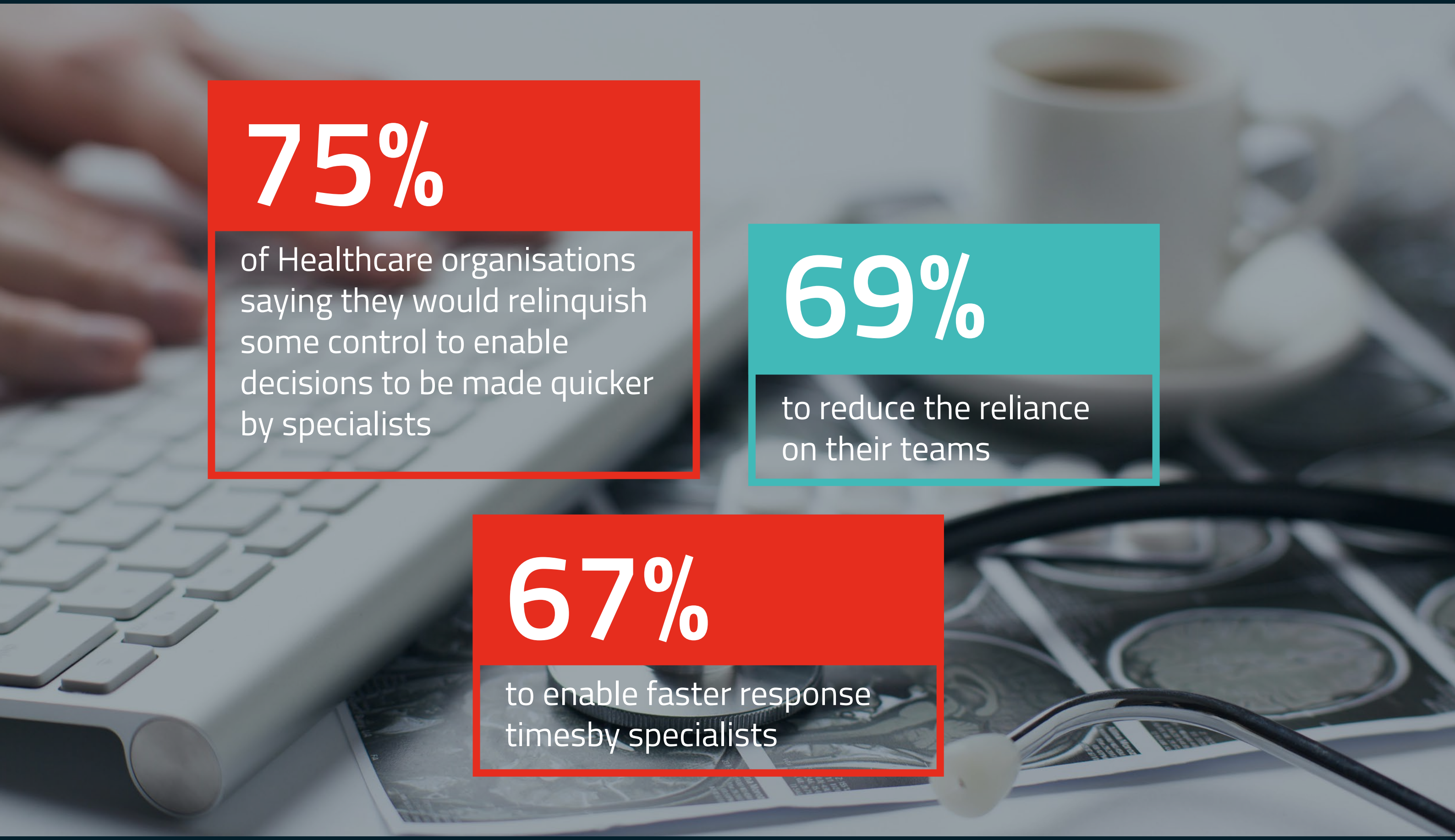
describe their cyber security provider or in-house team as "exceeding expectations"

In this paper we explore the key areas for improvement and how Healthcare organisations can challenge their security provider to create more resilience and provide greater ROI.

Chapter 1

The Healthcare industry is desperate to relinquish control, and lean on providers

The majority of Healthcare organisations either fully outsource their cyber security operations (41%) or take a hybrid approach to cyber security (40%). Over a third (35%) of them are looking for a hybrid solution to extend their current teams. This desire is higher in the Healthcare sector than the average across other industries*, which sits at just 30%. Clearly, those in Healthcare want help because they have other things to worry about.



75%

of Healthcare organisations saying they would relinquish some control to enable decisions to be made quicker by specialists

69%

to reduce the reliance on their teams

67%

to enable faster response timesby specialists

The research repeatedly reflects a strong trend from the Healthcare sector towards relinquishing the responsibility and management of cyber security – with a significant 75% of Healthcare organisations saying they would relinquish some control to enable decisions to be made quicker by specialists, 69% to reduce the reliance on their teams and 67% to enable faster response times.

It comes as no surprise that speed is also essential – with 52% saying it's a priority when it comes to making decisions around their cyber security environment. Control is the least important at 27%, again reflecting the trend that Healthcare organisations want to be able to rely on their providers.

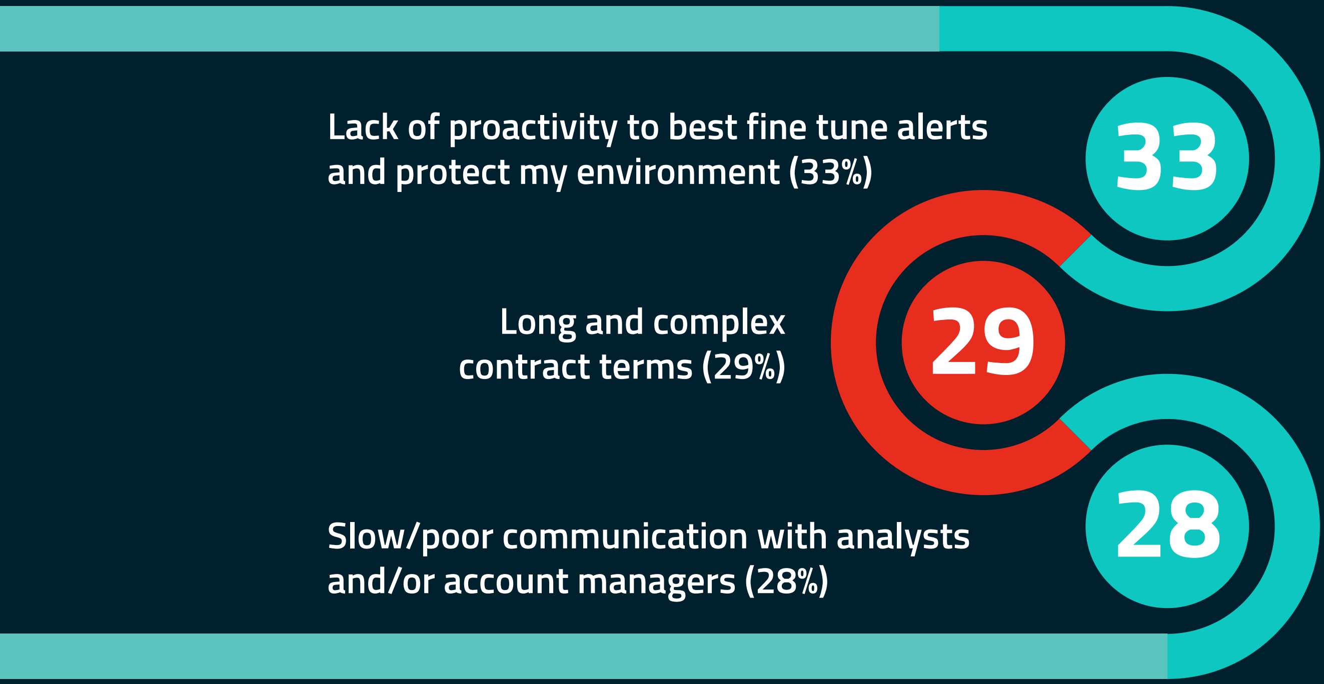
Chapter 2

Why are providers unfit for purpose?

Clearly, there is a huge opportunity for outsourced cyber security providers to support the Healthcare sector. In response to the sector's frustrations around proactivity and speed, a provider's goal should be to reduce risk using tactics like threat intelligence to pre-empt and disrupt attackers prior to execution.

However, 40% are unconfident in their use of threat intelligence to proactively detect threats and 31% are unconfident in their operation's ability to respond to an alert/incident within 30 minutes.

The biggest "don't have but desire" of Healthcare organisations is real-time visibility of reporting dashboards (55%) and around half (49%) don't feel they have client-centric delivery teams who care.



Lack of proactivity to best fine tune alerts and protect my environment (33%)

Long and complex contract terms (29%)

Slow/poor communication with analysts and/or account managers (28%)

There is a way to go before providers are supporting Healthcare organisations with the speed, proactivity and flexibility they need to tackle the onslaught of cyber attacks, exhausting an already over tired workforce.

Chapter 3

SOC-as-a-service is one of the most popular areas to outsource

Given the level of outsourcing within this sector (41% fully outsourced, 40% hybrid) and the exponential growth of SOC-as-a-Service within the marketplace, it remains one of the most popular cyber operations, with the top three all sitting at 28%.

only **5%**
said their service exceeds expectations which is much lower than the average across other industries,

at **14%**

27%
say their SOC is underperforming and they are looking to make changes, which is higher than the average of

25%*

50%
of those in Healthcare that outsource say that providers not implementing proactive measures

Of those utilising SOC-as-a-Service, only 5% said their service exceeds expectations which is much lower than the average across other industries, at 14%*. 27% say their SOC is underperforming and they are looking to make changes, which is higher than the average of 25%*. 50% of those in Healthcare that outsource say that providers not implementing proactive measures, such as threat hunting, is their biggest frustration.

Where effective, SOC-as-a-Service should bring clarity, but for Healthcare organisations, the speed and accuracy currently provided isn't sufficient.

Chapter 4

Navigating the challenges of locked-in cyber contracts

While for some, long contracts allow for predictable costs, they also restrict flexibility and agility over a contract term. This frustration has follow-on consequences, with organisations struggling to ensure that their cyber provision continues to be fit for purpose over time. This is particularly relevant for the Healthcare sector, as the ever-evolving threat landscape becomes increasingly sophisticated and takes advantage of any emerging vulnerabilities, such as an increasingly fraught workforce or inexperienced team members.

Rigid contracts appear to cause issues when requirements expand beyond the original statement of work, resulting in a need to bolt on new security options rather than an evolution of the original contract – considerations that busy Healthcare staff don't have the capacity to ponder.

Instead, providers should be proactively offering clear roadmaps to evolve their customer's security posture.

The provider not fulfilling their tuning obligations and escalating too many false positives will do little to alleviate the issue of CISO burnout for our respondents in Healthcare. Every minute counts when an attack takes place and speed is imperative to prevent serious consequences. Providers need to ensure that only high value signals gain attention, and distracting noise is eliminated.

It's clear that there is a need for a critical shift to ensure cyber defence quality meets the needs of Healthcare organisations in 2024. So, what are the key provider attributes organisations should be looking for when they next procure, to create resilience and drive greater ROI?

Chapter 5

Looking Ahead

The relentless pressure on the Healthcare industry comes from all angles, including from the velocity of cyber attacks. To combat any threat to people's personal health data, detection needs to be accurate and swift. The sector does not have the capacity to manage this, and so they are relying heavily on outsourced or hybrid approaches.

There are three clear initial steps Healthcare organisations can take to drive greater performance from their providers:

Push for closer integration so providers can better understand an organisation's environment and spearhead plans - We've seen a huge desire in the Healthcare sector to either outsource or take a hybrid approach. Providers need to integrate more closely with internal teams, take on more responsibility and accountability, and make the time to truly understand customers' environments. Providers should spearhead cyber defence roadmaps and lead CISOs in the Healthcare sector through the evolving landscape

Demand more proactive, up-to-date and accurate reporting to drive quicker decision making - Speed and accuracy are everything in Healthcare. As one of Healthcare CISOs' top frustrations, false positive alerts create a lack of clarity, therefore resulting in a delayed response, potentially adding to the serious nature of a cyber attack and further exasperating the already dire burnout issue in Healthcare. Key processes that providers should be carrying out include continually validating analytics to ensure that threat data is accurate and tracking emerging threats and vulnerabilities using proactive measures such as Attack Disruption

Scale down technological investment - A growing need to scale down technological investment and consolidate tooling to better enhance cyber resilience, means security decision makers will become more resistant to a key frustration; the continuous need to bolt on new services to meet evolving requirements

What are the key, critical questions Healthcare organisations should be asking their security providers today, to drive improved performance?

How will you demonstrate that you've made our organisation's cyber security provision more resilient?

In a sector where time is everything, providers need to drive down the mean time it takes to respond to a cyber attack, or attempted attack. By responding to emerging threats through an Attack Disruption approach while deploying strong threat intelligence and alert tuning, your provider should be able to eliminate false positives and improve detection and response times. Continuous testing and simulation by your provider will maintain the strength of your cyber security posture.

Can you measure how long it will take to contain a compromised account?

Your provider should be able to give clear KPIs including the mean time to detect and respond and how long it takes to neutralise an incident when threat intelligence is utilised.

How will you provide more visibility of our security stance?

Through closer integration with internal teams, your provider will have a better understanding of your environment and should be able to provide clear reports that allow you to document, respond and learn from attempted breaches. Closer integration addresses the industry desire for real-time visibility of dashboards and the frustration with slow/poor communications.

About e2e-assure's Threat Detection 2024 report: Rejuvenating Cyber Defence Strategies

e2e-assure commissioned this research to find out whether cyber defences are good enough and if they are currently failing UK businesses. It asked pertinent questions around the current offering from cyber security providers and highlights what CISOs and cyber security decision-makers want from their providers in 2024 to ensure they are best protected against the advancing threats.

Research methodology*

The research was conducted by Censuswide, on behalf of e2e-assure, surveying 97 CISOs and cyber security decision-makers from within Healthcare organisations with between 500-5,000 employees. Censuswide abides by and employ members of the Market Research Society which is based on the ESOMAR principles.

The wider research surveyed 506 CISOs and cyber security decision-makers with between 500-5,000 employees across industries including Architecture, Engineering & Building, Arts & Culture, Construction, Higher Education, Financial Services & Insurance, Healthcare, HR, IT & Telecomms, Industrial Manufacturing, Professional Services, Retail & Wholesale, Sales, Media & Marketing, Aviation & Transportation, and more.

Contact Us