Threat Detection for Manufacturig:

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

e2e assure

Table of contents

Foreword

Cyber security providers are failing Manufacturing organisations; the sector looks to make changes and bring operations in-house if key issues aren't addressed

As organisations across all sectors contend with rapidly evolving extortion techniques such as phishing, ransomware, and supply chain attacks to invade internal networks, it's clear the life of the CISO isn't going to get any easier in 2024.

e2e-assure's recent study* shows there is a genuine cause for concern for the Manufacturing industry, with few describing themselves as resilient (19%).

Given the complexity and breadth of third parties within the supply chain, each with their own attack vectors, the Manufacturing industry will always be highly vulnerable to cyber attacks. A strong relationship with providers is integral to cyber resilience, especially for organisations that are having to get to grips with new forms of smart technology being rapidly deployed across their industry.

When an incident or breach occurs, 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. The sector understands the potential value here, with the majority (54%) of Manufacturing organisations having opted for a fully outsourced cyber security provision, but are they getting the level of service they deserve?

At e2e-assure, we have been working with Manufacturing organisations 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 an attack, to prevent it completely.

So, how are providers failing Manufacturing organisations? And what questions should the industry be asking of their providers, to drive better resilience for an industry forever vulnerable?

Rob Demain
CEO e2e-assure

Introduction

Cyber security has taken centre stage in the operational risk profile of manufacturers, primarily stemming from the increasing integration of digital technologies and the adoption of Industry 4.0 practices. A reliance on a complicated network of partners and suppliers also means the sector is particularly susceptible to attacks within its supply chain.

As production systems become more interconnected, the vulnerability to cyber threats such as ransomware and industrial espionage rises, posing a risk to sensitive intellectual property and operational continuity.

The majority (54%) of Manufacturing organisations are fully outsourced (vs 24% hybrid vs 22% fully in house). This is unique in comparison to other sectors we surveyed as part of this study, such as Financial Services (45% outsourced vs 40% hybrid vs 12% in house), Healthcare (41% outsourced vs 40% hybrid vs 16% in house) and Professional Services (40% outsourced vs 38% hybrid vs 17% fully in house). Clearly, there's been an appetite among CISOs within this sector to gain access to third party specialist expertise, and advanced tools and techniques to detect and respond to threats.

However, although the majority of respondents (57%) say their security posture is much improved, few described themselves as resilient (less than 1 in 5/or 19%) and most have experienced a cyber attack (78%). This begs the question, are outsourced providers up to scratch? Or could they be doing better?

54% are fully outsourced

20% hybrid

24% fully in-house

78% have experienced a cyber attack

19% describe themselves as resilient

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

Chapter 1

How do cyber security providers measure up?

A cyber security provider's aim should be to reduce risk using tactics like threat intelligence to pre-empt and disrupt attackers prior to execution. However, when it comes to our study, the considerable majority (63%) of CISOs in Manufacturing are either unconfident that threat intelligence is being used as it has had no measurable positive impact (48%), or they know that threat intelligence has not been implemented to detect threats within their environment (15%).

With our respondents' top two frustrations being escalating too many false positives (35%), and the need to bolt on new services (34%), closely followed by the provider not being proactive (27%) and poor SLA response times (26%), our CISOs are seemingly unable to get the clarity, speed and flexibility they need. In fact, the vast majority (75%) admitted their provider is either underperforming and they're looking to make changes (27%) or that there's room for improvement (48%).

When asked about what their top frustrations are, CISOs in Manufacturing cited:

Most respondents also said they don't have flexible contracts (53%), transparent pricing (54%) and real-time visibility of dashboards (56%). Worryingly, around half (49%) don't even feel they have client-centric delivery teams who care.

Chapter 2

How do we drive a critical shift?

It's no surprise then that when asked, 'When next procuring cyber security operations what will you be looking for?' the majority (53%) said they'll either be bringing operations back in house (around a third, 31%), or will be taking a hybrid approach (21%). To fill the gaps where their current providers are falling short, a further 29% said they'll now be seeking specialist expertise in specific areas.

With the current level of perceived underperformance and desire to make changes, a critical shift is needed to regain the confidence of CISOs in the Manufacturing sector, with both service and commercial offerings needing to be addressed.

Providers are falling short of offering the speed, proactivity and flexibility they need to tackle the onslaught of cyber attacks within an industry that's vulnerable due to its expansive attack surface. Providers 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 Manufacturing. 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.

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 who may already be over stretched or underfunded struggling to ensure their cyber provision continues to be fit for purpose over time, potentially leaving them vulnerable as new threats emerge.

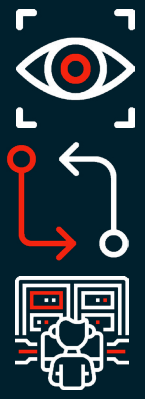
Rigid contracts also appear to cause issues when requirements expand beyond the original statement of work, resulting in a need to bolt on new security options rather than just an evolution of the original contract. In a rapidly changing threat landscape, providers should be offering clear road maps to advance the security posture of the customer overtime.

Chapter 3

Are benefits of SOC-as-a-service being fully realised?

Given the level of outsourcing within this sector (54% fully outsourced, 24% 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 closely matched.

Top three outsourced operations are:



Threat Detection and Response (34%)

End-to-End solution (30%)

SOC-as-a-Service (27%)

Of those utilising SOC-as-a-Service, a considerable majority (65%) said their service is either ok but there's room for improvement (40%) or that their SOC-as-a-Service is underperforming and they're looking to make changes (25%).

Those CISOs utilising SOC-as-a-Service, when asked about their top frustrations, cited:

Continual need to bolt on new service offerings to meet security needs **(50%)**

Provider is not fulfilling their tuning obligations and escalating too many false positives **(35%)**

Long and complex contract terms that make editing the service or switching provider difficult **(35%)**

Where effective, SOC-as-a-Service should bring clarity, but for Manufacturing organisations, too few benefits are currently being felt by those utilising this service.

Chapter 5

Looking Ahead

It's clear there is a need for a critical shift to ensure cyber defence quality meets the needs of Manufacturing 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?

The form and sophistication of today's cyber threats are changing constantly. This means Manufacturing organisations need to be monitoring and ready to respond at a moment's notice. This report shows a desire and need for Manufacturing organisations to work more collaboratively with their providers to achieve this.

There are four clear initial steps organisations can take to drive greater performance from their providers; demanding more proactive reporting to drive quicker decision making, opening an honest conversation about more flexible contracts, scaling down technological investment and pushing for closer integration so providers can better understand an organisation's environment and spearhead plans.

Demand more proactive, up-to-date and accurate reporting to drive quicker decision making

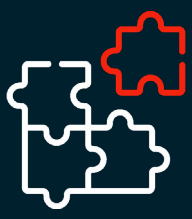
There's an urgent need for providers to take on more of a proactive stance in 2024. As one of Manufacturing CISOs' top frustrations, false positive alerts create a lack of clarity, therefore resulting in a delayed response, potentially adding to the serious nature of an attack and further exasperating the CISO burnout issue. Key processes providers should be carrying out include continually validating analytics to ensure threat data is accurate and tracking emerging threats and vulnerabilities using proactive measures such as Attack Disruption.

Flexibility will play an integral part in a company's cyber defences

Long fixed contract terms without a clear road map will cause organisations to become increasingly vulnerable as threat tactics evolve.

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, i.e. the continuous need to bolt on new services to meet evolving requirements will no longer be tolerated.



Stronger collaboration

Providers should 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 strategies and lead CISOs in the Manufacturing sector through the evolving landscape.

What are the key, critical questions Manufacturing 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 under pressure, 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 contain, 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 95 CISOs and cyber security decision-makers from within Manufacturing companies 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