A close-up of a stack of black plates

Description automatically generated with medium confidenceA green letter on a black background

Description automatically generated with low confidence



Money-makers – Cyber Security

Partner Positioning & Deal Examples

Date: 20 July 2023

Contents

[What is “cyber security”, “CSOC” and “SIEM”? 3](#_Toc142464933)

[Definition 3](#_Toc142464934)

[The UK Market 3](#_Toc142464935)

[Key Stats 3](#_Toc142464936)

[Why partner with us? 4](#_Toc142464937)

[What we offer 4](#_Toc142464938)

[Benefits to our Channel Partners 4](#_Toc142464939)

[Results for your customers 4](#_Toc142464940)

[What questions should you ask about cyber security? 5](#_Toc142464941)

[Sales examples: “What’s in it for me?” 6](#_Toc142464942)

[Example 1: Professional Services – 120 users 6](#_Toc142464943)

[Example 2: Private Healthcare – 150 users 7](#_Toc142464944)

[Example 3: Manufacturing – 200 users 8](#_Toc142464945)

[Example 4: Retail – 250 users 9](#_Toc142464946)

[Example 5: Global Distributor – 550 users 10](#_Toc142464947)

# What is “cyber security”, “CSOC” and “SIEM”?

## Definition

Cyber security is the application of technologies, processes, and controls to protect systems, networks, programs, devices, and data from cyber-attacks.

A Cyber Security Operations Centre (CSOC) and a Security Incident and Event Management (SIEM) platform are different strategies for monitoring network environments. Together, they help businesses prevent data breaches and alert them to potential ongoing cyber events.

## The UK Market

A report published by Mordor Intelligence predicted massive spend will continue across the UK cyber security market. In 2023, the estimated spend will be £12bn, growing to a whopping £19bn by 2028, with a CAGR growth rate of over 10% during this forecast period.

## Key Stats

The stats below illustrate why the cyber security market is a growth area in the UK:

A blue and white infographic

Description automatically generated

# Why partner with us?

Cyber security is a critical consideration for all businesses, particularly at C-level. The potential impacts of cybercrime are expansive, reaching far beyond fraud on a public or private company level. Pauses in productivity, lawsuits triggered by compromised data, and the long-term effects of stolen business intelligence, not to mention reputational harm, all add up.

From our in-house investment in cyber security, we can offer you a wide range of basic to complex services that you can resell to your customers, enhancing your own offerings and – in turn – boosting your profits and brand reputation.

In the last 3-4 years alone, our cyber security ecosystem has evolved from basic security products to today’s more complex portfolio, including the launch of our own CSOC. In this area of our business alone, we’ve gone from zero to £10M+ turnover in this short period of time, with exponential growth forecast for the future.

We have the resources, the tools, and the expertise to provide a full suite of world-class cyber security services for you and your customers.

## What we offer

* 24x7 real-time monitoring, analytics, alerting, and reporting.
* Hands-on support from our own cyber security experts.
* Purpose-built CSOC system.
* Simple and customisable management platform.
* Proactive BI, based on analytics.

## Benefits to our Channel Partners

* We offer an extended and wide-ranging portfolio of cyber security services.
* Peace of mind: we are highly accredited, so your customers are in skilled and reliable hands.
* Extension of resources to your business and in-house skill set.
* Exploit higher margins on this EXPO.e Money-maker.

## Results for your customers

* Effortless integration with existing systems.
* Visibility of the entire estate.
* Higher level of proactive cyber security monitoring = lower risk to business.
* Simple operating model and increased automation.
* Reduced operational expenditure.
* Demonstrable accountability through analytics.
* Streamlined compliance, through simplified management and reporting.

# What questions should you ask about cyber security?

Firstly, it is important to establish how your customer currently manages their cyber security posture and what plans they have for the future (i.e. current projects, plans, and future aspirations).

Some opening questions we use regularly are:

* *“What is your cyber security strategy?”*
* *“Who is responsible for cyber security within the business?”*
  + *A dedicated team, e.g. a cyber security operations team*
  + *A single person, such as a CISO*
  + *The Board/C-level*
* *“What concerns and challenges do you currently face around cyber security and how do you currently deal with these?”*
* *“What security systems do you have in place today?”*
* *“Do you have a team monitoring cyber security threats or do you outsource this to another partner (or a mix of both)?”*
* *“What regulations and standards apply to you?”*
* *“Is all of your sensitive data identified and encrypted?”*
* *“What are your high-risk systems and platforms?”*
* *“Do you provide security awareness training for staff?”*
* *“Are you regularly scanning all the data on your network – including backups and archives – for malware?”*
* *“Have you created and maintained a comprehensive incident response plan?”*
* *“How would a security breach affect your business, including your company's morale and your customer relationships?”*
* *“Do you have to ask your MSP to advise on improvements needed in your security posture, or are they providing that to you as standard?”*
* *“Do you have cyber security insurance? If so, are you experiencing issues with renewing it, due to – for example – changing compliance requirements?”*

These basic questions can help to spark the initial conversation and gauge whether there is an appetite to introduce a cyber security specialist on a follow-up call or meeting.

You can access further information (including templates) on our website, under our Partner Hub > Marketing section: <https://expo-e.uk/partner-login>

References:

\*[https://www.mordorintelligence.com/industry-reports/uk-Cyber security-market](https://www.mordorintelligence.com/industry-reports/uk-cybersecurity-market)

# Sales examples: “What’s in it for me?”

### Example 1: Professional Services – 120 users

**Total Contract Value: £159k**

**Business driver**

One driver was the customer’s cyber security insurance. The insurance broker was requesting further, mandatory provisions to be in place before they would provide a quote.

The other factor was they only had two people running IT across the business, and cyber security was not a strong skillset they had in-house. The customer was worried about the resulting risk and gaps within the business, particularly after receiving some direct phishing emails.

**Approach**

After an initial consultation meeting, it was agreed that the customer needed a partner with security experience to call upon – one who had the ability to monitor the business for threats and also to help meet their cyber security insurance requirements (i.e. testing, end point protection, logging, and monitoring).

**Solution**

EXPO.e provided an outline plan of the services and tools required to meet the objectives set out by the insurance broker. These included a penetration test. to identify any initial gaps. After undertaking scoping, high-level commercials, and a solution demonstration, it was also agreed to provide a CSOC service, as well as upgrading their current endpoint protection service (anti-virus) to protect against ransomware.

With these services in place, the customer was able to demonstrate to their insurance broker that then now had advanced protection in place, which allowed them to gain the insurance cover they required.

In addition to the above, it was agreed to provide several additional services, including vulnerability scanning and a phishing service. We are also providing the customer with support throughout the assessment process for their Cyber Essentials accreditation.

**Services sold**

* CSOC
* Pen testing
* Phishing service
* Vulnerability scanning
* Cyber Essentials accreditation support

**Additional services and future requirements**

* Support moving from Cyber Essentials to Cyber Essentials Plus
* Upgrade and improve the security posture of the customer’s firewalls
* Incident Response Service (IRS)

### Example 2: Private Healthcare – 150 users

**Total Contract Value: £97k**

**Business driver**

This customer was required by their compliance obligations and a recent audit to conduct pen testing on a regular basis, and to ensure that their network traffic logs were monitored, collected, and stored securely for several years – as is the norm across this sector. Their IT team were concerned, as they were a small team of just three people, who did not have the right skill sets to cover cyber security within their business.

**Approach**

After further conversation, EXPO.e arranged for a one-off pen test to take place to give the customer a view of where they stood. Alongside this, we scoped out the CSOC service to meet the logging and monitoring aspect of their compliance requirements. Once the pen test was completed, the customer was able to remediate the high risks and use this as a starting point, showing the board what had been corrected and so providing a way forward to shape their cyber security strategy. This then led to a contract being signed to continue the pen testing for a three-year period, which mirrored the contract we won for the CSOC service.

**Solution**

The initial one-off pen testing elements of this service covered the customer’s internal and external infrastructure, as well as the on-site Wi-Fi estate. This scope was mirrored for the longer-term contract, with an agreement for any further testing to be purchased ad-hoc.

The CSOC service covered all the customer’s endpoints, servers, Cloud environments and additional cyber security tools that were in place (including firewalls, and pre-existing security tools).

**Services sold**

* Pen testing
* CSOC

**Additional services and future requirements**

* Improved endpoint protection (a project due to be rolled-out in later 2023, once the current solution expires)
* User awareness training

### Example 3: Manufacturing – 200 users

**Total Contract Value: £234k**

**Business driver**

The customer experienced a ransomware attack which affected their IT infrastructure across the business and left staff unable to access data or critical systems. This left the customer and its users offline for many days, with the resulting loss of business having a negative impact on the company as a whole. After several weeks, the customer still did not have all data and systems fully restored, resulting in a complete loss of certain services.

**Approach**

At the outset, an IRS was implemented for a short-term period. Further investigation helped identify the source of the ransomware attacks, after which measures were put in place to strengthen the business’ cyber security posture. This included firewall upgrades, an endpoint protection service, and Multi-Factor Authentication (MFA).

**Solution**

In addition to the initial IRS requirement, we included multiple improvements to increase the customer’s overall cyber security maturity, with a phased approach to deployment. This included a Managed Detection and Response (MDR) service, along with upgrades and improvements to the firewalls.

Further improvements are ongoing and planned to take place throughout the next 2-3 years.

**Services sold**

* IRS
* MDR service
* Firewalls
* MFA

**Additional services and future requirements**

* CSOC
* IRS training
* Pen testing
* User awareness training

### Example 4: Retail – 250 users

**Total Contract Value: £297k**

**Business Driver**

This customer was victim of a cyberattack which affected the majority of their IT infrastructure. In principle, the issues the customer experienced were similar to the example cited above in the manufacturing example, whereby, the customer was attacked over a Bank Holiday weekend and so it took longer for anyone to respond to and begin investigations into the attack that occurred.

**Approach**

There was no IRS plan in place and nobody monitoring the business for these types of threats and attacks. When the cyberattack was discovered after the Bank Holiday, EXPO.e mobilised our resources to restore the customer to a position where they could continue to trade.

It took several weeks to get the customer back up and running, after which further measures were put in place to help prevent further, similar incidents occurring.

**Solution**

Building on the above a slightly wider scope of service was required. This not only included MDR and CSOC, but also included further cyber security forensic work.

**Services sold**

* Consultancy
* IRS and forensics
* Firewalls
* MFA
* MDR
* CSOC

**Additional services and future requirements**

* TBC – this will form part of the longer-term strategy into 2024 and beyond

### Example 5: Global Distributor – 550 users

**Total Contract Value: £244k**

**Business driver**

The customer was looking to outsource cyber security due to two factors: 1) The small size of their IT team in-house and, 2) lack of in-house cyber skills and knowledge. The threat landscape was the biggest concern to them, after seeing another business in the same sector suffer a cyberattack. The customer wanted to increase their visibility on cyber security as a whole to proactively identify and prevent any form of cyberattack that might threaten their business.

**Approach**

A meeting was held to understand what they had in-scope for the cyber security service and if any additional aspects were to be identified upfront. After the initial meeting, it was agreed that the best initial solution to their requirements was a CSOC. Once this was up and running, we agreed to review further security services, which would complement what they already had and add additional security layers, as and when required.

**Solution**

The customer outlined what they were looking for from a CSOC perspective and EXPO.e were able to meet all these requirements. We then provided a run-through of the service and presented commercials, following a demonstration session.

The CSOC service covered all of the customer’s endpoints, servers, Cloud environments and additional security tools that were in place (including email security, firewalls, etc.).

**Services sold**

* CSOC

**Additional services and future requirements**

* Cyber security assessment for a new company they recently acquired (£5,000 one-off cost)
* Email security upgrade (£20,000 on-off cost)
* IRS (c.£123,000 TCV)
* Firewall upgrade (£10,000 one-off cost)