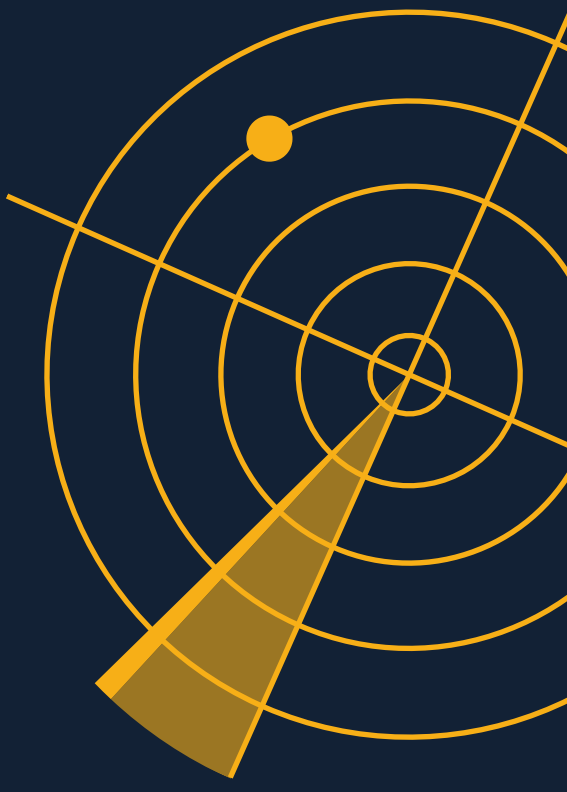
# Under Attack and Under Your Radar

## Cyber security threats: to your business and to your brand reputation



falanxcyber.com

falanx Cyber

**Your brand reputation will be one of the first casualties of a cyber attack.**

**And nothing can be more important than reputation and trust to your business.**

Businesses are only too aware of the regulatory, financial and reputational threats posed by unauthorised access to the data they hold.

Yet, time and again, the latest breach reveals that they are still not taking enough action to ensure they are protected.

The regulatory threats include the stringent breach detection and reporting protocols of the Security of Network & Information Systems Regulations (NIS Regulations) and the EU General Data Protection Regulation (GDPR) requirements.

As for the financial and reputational costs, here are a couple of recent high-profile examples:

Hospitality group Marriott was hit by a major data breach recently in which the guest records of 339 million customers had been accessed.

It was fined £99 million by the Information Commissioner's Office (ICO) and suffered weeks of operational disruption. Travel giant British Airways was issued with a record £183 million fine last year by the ICO after hackers gained access to the personal data of about half a million customers.

Even more concerning here, is that consumer watchdog Which? circled back to websites owned by these brands only to detect 500 security issues on Marriott's sites and 115 vulnerabilities on BA's.

Shocking as these specific examples are, the overview provided by statistics paints an even more concerning picture.

- UK businesses were among those worst hit financially by the fallout from cyber attacks during 2020, according to research from insurance provider Hiscox. This shows the median cost is $57,000, a near six-fold increase on the previous year's $10,000.

- Almost half of UK businesses suffered a cyber security breach or attack during the past 12 months, rising to 68% of medium-sized firms and 75% of large enterprises, according to statistics released by the Department for Digital, Culture, Media and Sport (DCMS).

- DCMS also reports that, despite the threat, many businesses are still not taking the high-stake risks seriously. Only half of UK businesses have undertaken an internal and external security audit in the past 12 months.

All businesses are custodians of highly sensitive information, and therefore an inviting target for hackers. There remains a major liability threat, financial cost and risk of lasting damage to your brand should you take this responsibility lightly.

# The main threats facing your business

It's clear that the stakes are incredibly high for businesses with a duty to protect sensitive data. But where are the main threats coming from?

**The top three tactics used are:**

**Phishing**
An attempt to obtain information by sending fraudulent emails to people in your firm.

**Spoofing**
An attempt to obtain information from third parties by impersonating your firm by sending emails or hosting a fake website.

**Viruses, spyware or malware attacks**
These are types of malicious software designed to perform damaging operations on your computers and networks.

Increasingly threats are coming from 'weak links in the chain' offered by the numerous third-party suppliers your business contracts work out to – and, even further down the line, the extended network of suppliers who supply them.

These people are concentrating solely on their jobs, not necessarily on your security – how secure are their passwords or the devices they use to access your information?

You may not know, but sophisticated hackers will be able to very quickly find out.



falanx Cyber

## Managed Detection and Response (MDR): the ultimate in cyber security protection

Many businesses have realised that their internal IT teams cannot provide the investment in resources or technology that is needed to maintain the prevention, rapid detection and immediate response to increasingly sophisticated and diffuse attacks.

Partnering with Falanx Cyber offers you the benefit of continuous protective monitoring of your network by the latest techology and a team of UK security-cleared analysts.

We can investigate and prioritise risks, and use proactive hunting to discover existing threats or weaknesses to your network, including identifying threats from your third-party network.

## What exactly is MDR and how does it protect your data and reputation by minimising risk?

MDR offers a 24/7 monitoring and eradication of threats across your entire environment and endpoints. It rapidly identifies and obtains clarity about any security issues threatening the integrity of your organisation.

It goes beyond traditional techniques, which only analyse your networks' and devices' endpoints. MDR also analyses your servers, apps and Cloud services.

It is seeing massive growth because it saves your business from needing to invest in expensive talent and tools, and protects their entire organisation, not just aspects of it.

## The benefits of Falanx Cyber MDR

Your business – and the data it holds – is increasingly being targeted by cybercriminals. And as your network of suppliers grows, the risk just gets greater.



### Identify and eradicate the real security issues threatening the integrity of your organisation

We continuously analyse your entire environment including, Cloud, network, servers, firewalls, and endpoints, for indications of targeted attacks – 24x7x365.

Our MDR service rapidly evaluates severity and impact and we can take appropriate action on your behalf.

By using our service you can prevent breaches, reduce cyber risk, support compliance, and help address the stringent breach detection and reporting requirements required by The Security of Network & Information Systems Regulations (NIS Regulations), the EU General Data Protection Regulation (GDPR) and GPG-13.



### Detection in depth

Our detection in depth approach is achieved by leveraging multiple protective and analytical capabilities to provide a multi-layered defensive security posture. The service combines capabilities such as Endpoint Detection & Response (EDR), SIEM, Security Configuration Assessment, Suspicious Email Analysis and External IP Monitoring as standard.



falanx Cyber

## Reducing the time to respond

Reducing the time to respond is critical when it comes to a security breach or a cyber-attack.

Reducing the time taken to detect and respond to an incident (known as the Mean Time To Detect, or MTTD, and Mean Time To Respond, or MTTR) is a significant factor in reducing the time, effort and cost involved with a security incident. Put simply, the sooner an incident can be detected and dealt with, the easier and cheaper it is to ensure the business continues to operate.

Our service has been designed to reduce MTTR. With our Detection in Depth approach we can act on suspicious activity within seconds and take immediate action by terminating processes or isolating machines.

Our cost-effective and fully-managed MDR service works as an extension of your IT team. It provides you with highly skilled security experts, leading-edge technology and rapid cyber incident response, delivered from our UK-based Security Operations Centre (SOC).

Of course, you have access to our dashboards and we will communicate threats posed and actions taken. But, on the whole, you can focus on other tasks, rather than fighting cyber security fires.

**To find out more about how Falanx Cyber's MDR can give you full visibility of threats and rapid responses to eliminate them, call our team on +44 (0) 20 7856 9450 or visit us at falanxcyber.com/managed-detection-response.**

Falanx Cyber holds, operates to, and delivers its cybersecurity services in accordance with the following certifications and accreditations:

ISO 9001 CERTIFICATION EUROPE™

ISO 20000 CERTIFICATION EUROPE™

ISO 27001 CERTIFICATION EUROPE™

CYBER ESSENTIALS CERTIFIED

CREST

falanx Cyber

Crown Commercial Service Supplier

falanxcyber.com
020 7856 9450

falanx Cyber