YOBAH

CYBER SECURITY SOLUTIONS THAT JUST ADD UP

A Guide to Cyber Security for the Financial Services Industry

It’s Time to Multiply Your Cyber Defences

As the threat landscape continues to evolve and become more mature, cyber security has become important for businesses in every sector. However, for financial services (FS) companies, establishing the right cyber security posture is paramount. The finance industry handles high volumes of extremely sensitive data, making FS businesses extremely attractive targets for cyber crime. Falling victim to a cyber attack could result in unrecoverable reputational, financial and legal damages.

As a result, it is essential that you establish the right protections to protect your business from the negative consequences of a cyber attack. In this guide, we arm you with the knowledge you need to tackle financial services-targeted cyber threats head-on.

We will explore

- The importance of cyber security for financial services businesses
- The top five cyber threats currently facing the finance business
- How to defend your financial services company
- Why Zero Trust Security is important for finance businesse
- How Yobah can help strengthen your protections

The Importance of Cyber Security for Financial Services Businesses

It's a simple equation: your financial services business + the right cyber security posture = stronger operations, robust data protection and business success. However, if you fail to invest time and forethought into your cyber security, the consequences could be catastrophic.

Simply assessing your security posture and making small changes could save you a lot of time, money and hassle in the long run.

300 x

Businesses in the financial sector fall victim to cyber security incidents approximately 300x more than other industries.

40%

The average cost of cyber crime for the financial services sector is 40% higher than all other industries.

15.6 m

The average cost of a cyber attack on a financial services provider is £15.6 million

The Importance of Cyber Security for Financial Services Businesses

Although these statistics are shocking, the cost of a cyber attack is more than just financial. As financial services, businesses need to adhere to strict data security regulations, including GDPR, FCA and ISO/IEC 27001, if your confidential data is compromised, you could face significant legal repercussions. For instance, failing to comply with GDPR could result in a maximum fine of £17.5 million or 4% of your annual global turnover – whichever is greater.

Fundamentally, if you suffer from a data breach, you are compromising your clients' trust. When your customers choose to work with you, they allow you to handle their sensitive, confidential and valuable information. If this is then exposed or exploited during an attack, then the faith they placed in you will prove unfounded. You should not underestimate the negative effects this could have on your reputation as an organisation. You could be risking your profitability as a business – losing clients in the short term, sacrificing referrals and failing to attract new customers.

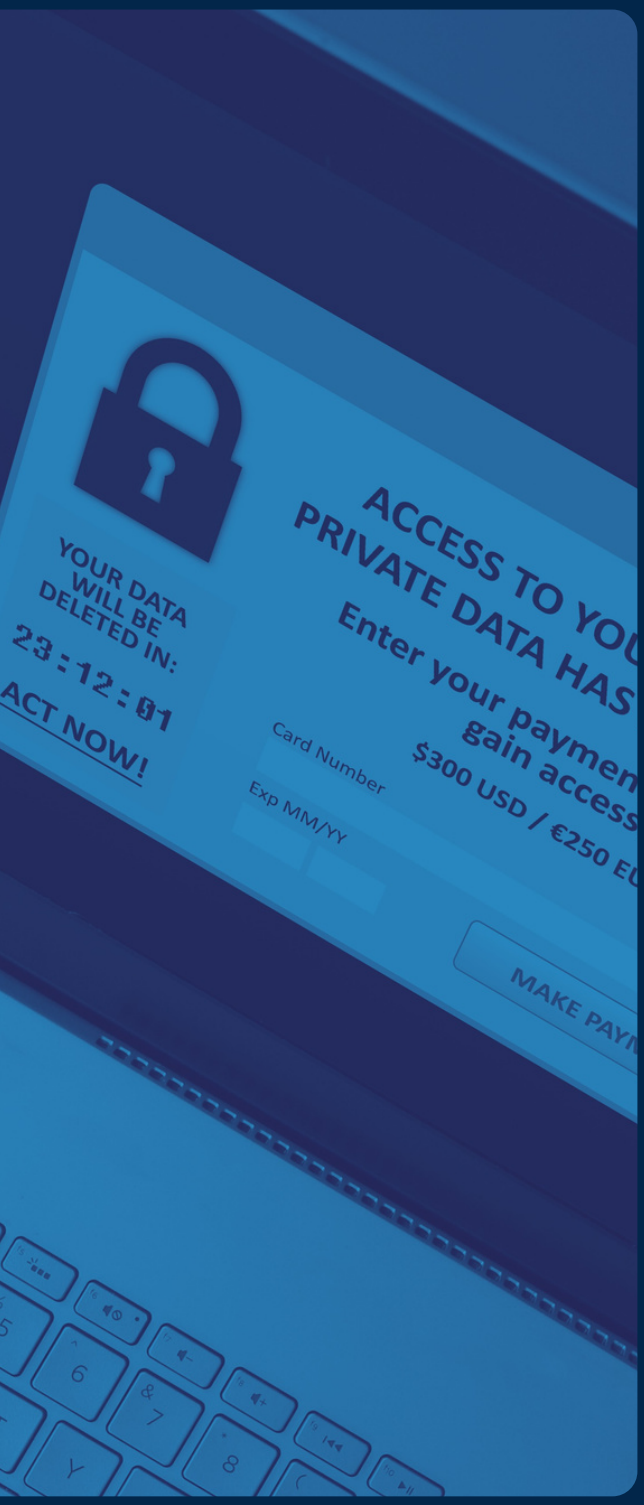
Top 5 Cyber Threats Facing the Finance Sector

The first step to effectively defending your financial services business is knowing what you're up against. Understanding the most prevalent, pervasive and pressing threats is essential to strengthening your protections in the right way. With that in mind, let's take a look at the top five cyber threats currently facing the financial sector.

Phishing

During phishing attacks, cyber criminals use social engineering tactics to pose as legitimate or trusted correspondents and send targeted messages to trick recipients into downloading malware or revealing sensitive information. Phishing is a pervasive cyber attack across sectors, accounting for around 90% of all data breaches. The finance industry is no exception. Reports from Akamai found that almost 50% of observed phishing attacks were linked to the financial services sector. In 2021, phishing attacks against the finance industry increased by 22%, with attackers using phishing to gain initial access in 46% of attacks against the financial services sector.

Top 5 Cyber Threats Facing the Finance Sector



Ransomware

Ransomware is a form of malware that exploits the value of a company's data, encrypting it until the victim pays a ransom to retrieve it. Ransomware attacks on financial services businesses have increased in recent years, with 55% of organisations being hit in 2021 - up from 34% in 2020.

Additionally, 52% of financial services organisations paid the ransom to restore their data, which is higher than the global average of 46%. There are even specific strains of ransomware that have developed specifically to target the financial industry, including Sodinokibi, Lockbit and Darkside.

Top 5 Cyber Threats Facing the Finance Sector

SQL Injections

SQL injection is a form of attack which uses malicious code to access private information and compromise your database. This technique is commonly used to attack data-driven applications. Financial services businesses frequently use end-user-facing applications that allow customers to submit sensitive data. As it is easier for cyber criminals to gain access to these applications than the company's network directly, they are a powerful threat vector for SQL injections. According to Akamai, 94% of observed cyber attacks in the financial sector were facilitated by SQL injections, cross-site scripting, local file inclusion and OGNL java injections.

Crypto jacking

As cryptocurrencies have risen in popularity, they have become a significant security challenge for financial services businesses. Cryptocurrency can be used to launder money or transfers can be used as entry points for data theft. It is now estimated that 25% of all businesses have encountered cryptojackers on their devices. This can cause legal, financial and security issues for the financial industry.

Top 5 Cyber Threats Facing the Finance Sector

Account Takeover

SIn an account takeover, cyber criminals use stolen employee credentials to impersonate users, steal data or plant malware. If a cyber criminal can gain access to a privileged account within a financial services business, then they will be able to wield a significant amount of power. In recent years, this threat has seen a significant increase, with high-profile companies like Uber and Twitter being targeted. Improperly managing user identities and account access increases the potential of exposure to account takeover attacks.

For instance, identity sprawl, where users have numerous accounts and identities managed by multiple unsynchronised systems, maintaining the same access permissions across Cloud applications and on-premises environments and failing to implement least privilege policies can all increase your chance of account takeover.

How to Defend Your Financial Services Business

Fortunately, there are some relatively simple preventative measures you can implement to protect your business from cyber-attacks. These include:

Data Encryption

Data encryption is a security method which encodes information until a user with the correct encryption key decrypts it – rendering it incomprehensible should an unauthorised user try to access it. You can also tokenise your data, replacing it with a generated number or token until it is decrypted by a token vault. For further protection, you can even encrypt your tokens.

Role-based access control (RBAC)

RBAC is an identity-management process which restricts access to your company's network, applications or data depending on the user's elationship to the organisation. This means that only specific users will be able to access sensitive information or systems – reducing both internal and external threats.

Intelligent threat detection

Threat detection is the practice of continually analysing a company's system to identify malicious activity that could compromise the network. AI harnesses knowledge of previous threats to allow you to respond to and mitigate encroaching attacks more quickly.

Endpoint protection

TImplementing endpoint detection and response solutions and carrying out centralised logging across your estate helps detect and remediate incidents faster. By collecting insights from networks, infrastructure, endpoints and applications into a single location, you can gain a consolidated view of all activity, making it easier to identify and resolve issues.

Using all of these controls together will help your business work towards achieving a Zero Trust security architecture.

Zero: The True Magic Number

The Importance of Zero Trust Security for the Financial Sector

Zero Trust eliminates the idea of implicit trust from your cyber security strategy, requiring anyone attempting to connect to your business' system to be continually verified at every stage of the digital interaction. This makes it more difficult for malicious actors to gain access to your data and valuable assets.

Zero Trust security is one of the most important cyber security strategies for the financial services sector, helping to define who can access your network, applications and data and protect your assets from unwanted users. You should adopt a Zero Trust approach to security across your entire infrastructure, including routers, switches, cloud, IoT, and supply chain.

Identity Led Security

Zero Trust allows you to create specific user access policies at the individual application and file level, reducing your dependence on passwords which can be compromised. It is no longer safe to validate a user based on their physical location, such as whether they are on the corporate network. Instead, identity-led security validates who the user is, what they should have access to and their security posture at the time of access. This allows you to implement privilege escalation, providing employees with access exclusively to the sensitive materials required to do a specific task for a limited period of time.

By implementing RBAC, you can assign access to resources and information based solely on their position in the company. This means that as employees join, move roles or leave the organisation, their permissions can be efficiently altered or disabled. Joiner, Mover Leaver identity governance can even be automated, making the whole process more seamless.

Consistent Monitoring

Zero Trust security solutions allow you to monitor the activity of users on their systems. You can use a central management dashboard to monitor activity and funnel data to other processing tools to look for deeper insights. Through behavioural analytics, the process of collecting and analysing data collected from the actions of users on your systems, you can see exactly how users typically behave and be able to define a baseline of what ‘normal’ or ‘good’ looks like. As a result, suspicious activity will be highlighted more efficiently, allowing you to assess threats and take mitigating action more easily. This has the additional benefit of aiding compliance reporting, helping you to adhere to security regulations within the industry. By continually evaluating your security strategy and controls to ensure that the insights from your analytics are still correct, you can remain notified of issues and protect your business more comprehensively.

Secure network access

A Zero Trust security architecture is centred around removing the network boundary and using the user's identity as the security enforcement point instead. By securely protecting the identity, the platform, the endpoint and the data, you can achieve true Zero Trust.

By implementing the right security strategies and solutions, you can now access applications from any device, from any location. Secure Sockets Layer (SSL) is an encryption-based security protocol that offers privacy, authentication and integrity to Internet connections. SSL initiates an authentication process, known as a handshake, between two devices attempting to communicate with each other via the web, to ensure that both devices are legitimate. SSL then encrypts the data transmitted across the web, so any malicious actor who tries to intercept the data will not be able to understand it.

Your Business + Yobah's Innovative Cyber Security Solutions = Comprehensive Protection

At Yobah, we deliver comprehensive security solutions specifically designed to defend the financial services industry. With our expertise and support, you can seamlessly protect your systems, applications and network.

Our approach to security services is completely partner-led. We understand that every organisation is on their own journey and will be at different stages of security development. That's why we offer a cyber security consultancy service that will help you define your specific goals and create a bespoke roadmap that will help you get there.

Following initial consultation, we design, implement and manage a security strategy that will move you towards a 'Zero Trust' architecture. We deliver this through the following key practices:

- Endpoint protection
- Identity and access management
- Platform and application landing zones
- Data protection and loss prevention

Your Business + Yobah's Innovative Cyber Security Solutions = Comprehensive Protection

Endpoint protection

As Bring Your Own Device (BYOD) policies have become commonplace, your employees' endpoints may not benefit from your organisation's security policies and are therefore more vulnerable and exposed. As a result, endpoint protection is more important than ever before. At Yobah, we can help you secure your devices with innovative endpoint protection services.

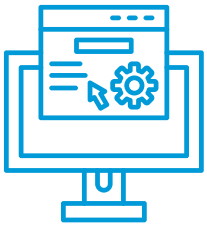
We continually monitor your endpoints and offer advanced threat detection, investigation and response capabilities to help you identify and contain potential threats before they become problematic.

Identity and Access Management

By leveraging Azure Active Directory, we help you control and manage who can access your valuable resources. Azure Active Directory integrates into over 4,500 SaaS apps for Single Sign-On, providing you with one source of truth. Additionally, with Conditional Access, you can establish strict criteria for application log ins and set up adaptive access policies which prevent unknown devices, security setups or connections from accessing your apps. This helps to keep bad actors away from your sensitive data.

Your Business + Yobah's Innovative Cyber Security Solutions = Comprehensive Protection

Platform and application landing zones



Through a centralised management system, we protect your business' platform and application landing zones.

We apply controls and platform tools to the platform and application landing zones and establish behavioural and environmental constraints and policies. We also securely configure and deploy resources and fully manage and support the landing zone environment.

Data protection and loss prevention

At Yobah, we understand the importance of your data and we want to help you manage it, control it and protect it.

We use best-in-class industry solutions to back up your data, both in the Cloud and on-premises. Additionally, using Microsoft Purview, we offer you a unified data governance solution to manage and govern your on-premises, multi-Cloud and SaaS data. We can provide valuable insights into the management of sensitive data across your entire estate and help you easily provision data access.

Cyber Security to the Power of Yobah

Is your cyber security as strong as it should be? Are your current protective solutions up to scratch? In an industry like finance, where data is so valuable and the cost of compromise is catastrophic, there's no room for error.

At Yobah, we specialise in delivering optimal IT solutions to financial services businesses.

Through years of experience assisting the financial sector with their technical troubles, we have become specialists in FinTech and security for financial services companies.

We know that the threats facing your industry are developing at a rapid pace and we want to help you not only keep up, but stay ahead of the game.

Ready to get started?

Get in touch to begin optimising your security solutions today.

0161 457 1375
info@yobah.co.uk
www.yobah.co.uk