CyberSmart

PROTECTING YOUR ASSETS

The value of cybersecurity in professional services

cybersmart.co.uk

Partner logo

CyberSmart

PROTECTING YOUR ASSETS

The value of cybersecurity in professional services

cybersmart.co.uk

Contents

INTRODUCTION

Big data equals big risk

The professional services industry works with their clients in a more intimate way than most. It deals with vast amounts of sensitive data like IP, financial information, legal documentation, business strategy, and more. There's a great amount of trust in relationships that involve sharing confidential information, and if anything goes wrong, a great risk to that relationship and brand reputation.

With so much at stake, professional services organisations have a doubly difficult job when it comes to cybersecurity. They need to maintain a cybersecurity infrastructure worthy of customer trust, consistently monitor for threats, and educate their employees. It's a lot to manage, but it's crucial for continued success.

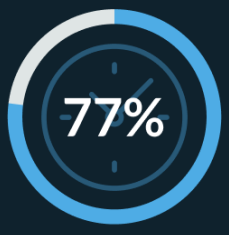
What types of companies do we include in our definition of professional services?

- **Financial**
- **Legal**
- **Consultancies**
- **Agencies**

PROFESSIONAL SERVICES BY NUMBERS

The security landscape

The professional services industry is prone to attack. Cybercriminals target organisations three times a week, on average. Threat actors know there's a lot on the line for their victims, which gives them an incentive to attack. Hackers can use stolen personal data as leverage for ransom payments or sell it on the dark web, for example. Along with the manufacturing industry, finance and professional services face the highest distribution of cyber attacks.

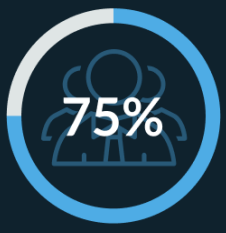


of professional services leaders say they need more time to identify and respond to attacks.[1]

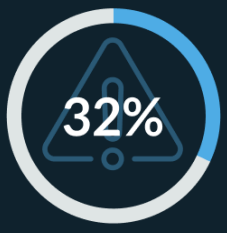
professional services companies are targeted by threat actors.[1]

The value of your fullz data (one person's name, DOB, and social security number) on the dark web.[2]

of financial institutions suffered a ransomware attack in 2021 (up from 34% in 2020).[3]



of law firms the Solicitors Regulation Authority visited in 2020 had been the victim of a cyberattack.[4]



of UK businesses suffered a cyberattack in 2022.[5]

1EB | US banks store one exabyte of data including credit card information, transaction records, interaction logs, and more.[6]

COMMON THREATS

Understand common threats

Know which attacks are most common in your industry, how they occur, what they look like, and what you can do to prevent them. Get a good understanding of your vulnerabilities so you can prioritise how to remedy them to make your business less accessible to threat actors. In professional services, common threats are:

Phishing

Cybercriminals use psychological manipulation in social engineering attacks, like phishing, to trick employees. It's getting harder to recognise and avoid this kind of attack because they're so sophisticated. In 2022, a group called "Crimson Kingsnake" launched a business email compromise (BEC) where they impersonated legal professionals to trick accountants into paying fake invoices.

DID YOU KNOW?

Worldwide, 36% of phishing attacks target financial services companies

Malware

Malware, like ransomware, is common because professional services organisations store so much sensitive data. These attacks can lead to large financial losses as many feel pressured to pay the ransom. According to Veeam's 2023 Ransomware Trends report, in at least 93% of cyber-events, the criminal attempted to attack backup repositories to force victims into paying. And even if companies don't pay the ransom, they'll suffer financially through reputational losses once the breach becomes public knowledge.

Other types of malware, like spyware, adware, worms, and viruses, are also a threat to stay aware of.

Distributed denial of service (DDoS) attacks

Overloading servers with traffic can quickly bring servers offline, causing disruption and frustration for customers. This also casts doubt on an organisation's ability to maintain its IT infrastructure and deliver a consistent service to customers. Cybercriminals can also use the opportunity of a DDoS attack to launch another attack or try to extort money from the victim.

DID YOU KNOW?

25% of cyberattacks submitted to the FCA in the first half of 2022 were DDoS attacks.

Supply chain attacks

If third-party suppliers don't secure their systems, you could be putting your customer data at risk. It's crucial to secure your supply chain so you don't fall victim to poor security protocols from another company. Otherwise, cyber criminals could use your suppliers as a way to get to you and steal your data, install malware, etc.

Nation state attacks

These are particularly risky to professional services companies who work with high-profile figures or companies who might have access to IP or data that's of interest.

DID YOU KNOW?

Cyberattacks against the banking sector have increased by 81% since the beginning of the Russia-Ukraine war.

PROLIFIC ATTACKS

Damages caused by cyber criminals

These examples highlight why it's important to take precautions and stay on top of developing threats. Don't let these concern you. Instead, let them fuel your dedication to building the best possible cybersecurity defences. They're also a good reminder that even the biggest companies with the biggest budgets can fall victim to cybercrime.

1. MOVEit – PwC

Year: 2023
Attack type: Supply chain attack
Scale: Global

Summary: PwC had data stolen through a third-party piece of data transfer software, MOVEit. MOVEit suffered a security incident that affected their customers worldwide. The group behind the attack, Clop, stole data from more than 200 companies and posted PwC data on the dark web and the clear web.

2. Grubman Shire Meiselas & Sacks

Year: 2020
Attack type: Ransomware
Scale: Company

Summary: Cybercriminal group, REvil, launched a ransomware attack on New York law firm, Grubman Shire Meiselas & Sacks. They claimed to have stolen 756 gigabytes of data from their high-profile customer base, including the likes of Madonna, Lady Gaga, and Drake, and demanded a ransom payment of $42 million.

3. WPP

Year: 2017
Attack type: Malware
Scale: Company

Summary: Part of the NotPetya attacks, hackers distributed malware through accounting software, affecting users of the software in multiple countries. The attack was intended to cause disruption to unpatched business systems. Some parts of WPP were badly affected for 10 days and the attack cost the company £10m-£15m.

4. Seven biggest UK banks

Year: 2018
Attack type: DDoS
Scale: National

Summary: Santander, Tesco Bank, RBS, Lloyds, HSBC, Clydesdale and Yorkshire Banking Group, and Barclays suffered a DDoS attack that caused them to close operations. Hackers used rented software that cost just £11 from Webstresser, an online cybercrime market known for enabling large-scale DDoS attacks and responsible for 4 million cyber attacks worldwide.

STAYING SAFE

How to secure your business

Every business is a target for hackers, so it's important to maintain your security. Here are some top tips for securing your business so it's less susceptible to attacks and better at responding to them if they do occur.

1. Protect yourself first

Build a solid foundation based on cybersecurity best practices to keep your processes, systems, data, and employees secure.

Update software regularly

Install patches as soon as they're released to ensure your applications and software are up to date. Only use reputable, verifiable software.

Control access

Limit exposure to sensitive data by ensuring employees can only access the data they need. Set up different access levels to make this easier and give employees user profiles based on their permissions.

Strengthen your password policy

Have an organisation-wide password policy that stipulates what criteria users must meet to set appropriate passwords and how often to change them. Set up multi-factor authentication using tools such as Google Authenticator to add an extra level of security.

Cyber Essentials: a one-stop shop to reduce your cyber risks by 98.5%

A must-have for many legal and finance organisations, a Cyber Essentials accreditation is a simple way to master the fundamentals of security. It includes a set of five controls around firewalls, internet gateways, secure configuration, access control, malware protection, and patch management, with a checklist of criteria you must meet for each. The guidance is clear and will help you get a robust level of cybersecurity across all important areas, rather than tackling things one at a time.

If you want to continue your accreditation journey, there are more complex options to work towards, too. After gaining your Cyber Essentials certificate, you can go for Cyber Essentials Plus and ISO 27001.

These accreditations will help you to maintain a recognised standard of cybersecurity in your business.

Look after your data

Encrypt sensitive data so that, in the event it's stolen, it's unreadable without the encryption key. Install anti-virus software to help monitor any threats, and regularly back up data.

Train your employees

Empower your employees with the knowledge and confidence to protect hardware, software, data, and systems. Have regular refresher sessions to keep security front of mind, and deliver information in digestible chunks. For example, help them to indentify and report suspected phishing emails.

Respond to incidents effectively

Prevention is better than cure, but it helps to be prepared for every eventuality. One way to respond to incidents is through a security operations centre (SoC). For complete peace of mind, it's worth looking at 24/7 SoC options. Third parties can provide this for you to take pressure off your IT team.

2. Secure your supply chain

Because supply chain attacks are so popular with hackers, you need to secure yours. This is a growing trend, with 95% of organisations increasing their focus on third-party risk assessment.

Talk to your suppliers

Understand where your suppliers and partners are with their cybersecurity and share your experiences. Keep an open dialogue so you're front of mind if they suffer an attack.

Assess risks

Find a controlled, detailed way to assess supplier risks. Talking to them is a good start, but having structured risk assessments to measure their approach against your needs is going to speed the process up, especially for manufacturers with thousands of suppliers.

Make good cybersecurity practices contractual

Establish what you expect from your suppliers around cybersecurity and apply those principles to contracts. An agreed level of acceptable cyber hygiene sets expectations and keeps suppliers accountable.

For some businesses, requiring that anyone you work with completes Cyber Essentials certification will be enough. For others, something more comprehensive like ISO 27001 certification might be better.

Follow the NCSC's guidance

If you ever want to find out more about supply chain best practices, the National Cyber Security Centre (NCSC) has some useful guidance and information.

THE BENEFITS OF ROBUST CYBERSECURITY

There’s more to cybersecurity than peace of mind

For objectively little effort and investment compared to that needed if you face an attack, you’ll get a lot back from prioritising security.

1. Preventing disruption

Implementing strong cybersecurity tools and processes, such as regularly backing up data, will help you minimise the impact of cyber-attacks on your operations. Any time you prevent a disruption you’re enabling business continuity, which means more uptime, more profit, and better results for your business.

2. Building trust with partners and customers

You’re reliant on the trust of your customers to stay in business. Leading by example with strong cybersecurity defences will help to maintain your reputation and the trust your customers place in you to deliver your services.

3. Saving money

Far from a cost centre, research shows that investing in cybersecurity pays off in the long run. It costs significantly more to recover from cyber-attacks than it does to protect against them. The average cost of a data breach globally is $4.5 million – a drop in the ocean compared to annual cybersecurity costs.

4. Qualifying for government contracts

Bidding for government contracts is a great way to secure long-term work. But with cybersecurity under greater scrutiny than ever, public sector organisations only allow companies with an active Cyber Essentials certificate to bid for government tenders. Getting accredited will help you expand your portfolio in the public sector and build lasting partnerships.

5. Earlier threat detection

Investing in 24/7 security monitoring gives you the comfort that no matter what time disaster strikes, someone will be on hand to alert you and help stop it, minimising damage.

YOUR CYBERSECURITY JOURNEY

Shape up your cybersecurity

There's a lot of pressure on professional services organisations to do everything perfectly. Unfortunately, it comes with the territory of doing such complex work and managing big data.

Take sensible, steady steps to improve your security, save money, and protect your reputation. It takes time and effort, but you'll feel more confident in the knowledge you're doing all you can to protect your business and customers.

If you don't already have Cyber Essentials and are looking for a straightforward way to cover the fundamentals of security in one go, it's a good place to start. For added peace of mind, invest in 24/7 threat detection. If you don't want to leave threat detection to your already stretched IT team, you can outsource to a dedicated third party. With the fundamentals covered, you can then focus on what to do next to continue your cybersecurity journey.

For support with accreditations, 24/7 threat detection, cyber insurance, and more, get in touch – we're happy to help.

Talk to us

SOURCES

1. 2022 UK Cybersecurity Census Report
2. How much are you worth on the dark web?
3. The State of Ransomeware in Financial Services 2022
4. Cyber Security: A thematic review
5. Cyber security breaches survey 2023
6. How big data enhances banking and financial systems

Back to page 2