



# Microsoft Security Insight Report for Professional Services Firms

2022 Edition

Discover why Professional Services Firms should consider a 'Microsoft First' approach towards cybersecurity



#MicrosoftFirst  
For Security & Compliance





# Contents

Executive summary .....	1
The unique challenges for the Professional Services Sector .....	2
Assessing the cyber threat for Professional Services Firms .....	3
Understanding Microsoft security .....	5
A Microsoft First approach in action .....	7
Key findings and recommendations .....	9
About this report .....	12



A 'Microsoft First' approach encourages a better understanding of the latest Microsoft security portfolio. This enables you to leverage your existing investment, resulting in significant commercial gains and an improved security posture.

## Executive summary

The particularly damaging nature of a successful cyber breach for Professional Services Firms is as obvious as it could be catastrophic. By virtue, no other group of industries places such importance and value on the core principles of trust and integrity. For this sector, a cyber breach can pose an existential risk.

The vulnerability of Professional Services Firms is also due to the nature of the data they store. The survey by the UK Government *Cybersecurity Breaches*, for example, reveals that 77% of Finance and Insurance Firms hold personally identifiable information (significantly higher than the 55% average). This makes them more likely targets for cyberattacks in order to exploit that sensitive data.

To learn more about the nature of cyber threats to Professional Services Firms, Softwerx conducted a survey of over 50 senior decision makers in the industry.

Of the participants, 76% thought that their role in managing the cybersecurity threat to their firm was increasing in complexity. Over 80% thought that the marketplace was becoming increasingly difficult to navigate, with one stating that "*there is now significant product-overlap between many security suppliers, often making it difficult to see the wood from the trees.*"

We asked the same cohort what they knew about the current Microsoft security portfolio, and to what extent this formed part of their overall cyber strategy.

Only 20% of participants claimed to be fully conversant with all aspects of the Microsoft 365 and EMS portfolio. 52% stated that there was a lot of scope to leverage a greater value from their existing Microsoft subscription.

Many IT leaders may not be aware that Microsoft is now a bona fide security company. This is despite the fact that Microsoft currently leads in five Gartner Magic Quadrants for security and it tracks more than eight trillion security signals every 24 hours. It is spending \$20BN in security over the next five years. Only Microsoft can offer a completely native and seamless security user experience.

The findings in this report indicate that Professional Services Firms can realise significant security gains by adopting a 'Microsoft First' approach towards cybersecurity.

In practice, this means that your Professional Services Firm should stop overspending on unnecessary, alternate and overlapping security solutions. Instead, you should better utilise your existing Microsoft investment.

# The unique cybersecurity challenges for the Professional Services sector

The Professional Services sector faces a unique, tripartite challenge from a cybersecurity perspective.

Like almost all businesses, **reputation is key**. However, losing it through a cyberattack may have irreversible consequences for your business when **data-integrity is an integral part of your DNA**.

The **highly complex information processing and technology orchestration required** makes the sector very vulnerable to cyberattack. This is especially relevant where significant funds are transacted.

Finally, **the Professional Services sector is highly regulated**. Governance, risk and compliance in this sector is not an isolated discipline, but is intrinsically linked to a strong cybersecurity posture.

Notably, it is mid-market Professional Services Firms that may be most vulnerable, with cyberattacks becoming increasingly complex and sophisticated.

Adopting a Microsoft First approach to security can significantly reduce your firm's risk from sophisticated threats.

## Brand reputation on the line

The effect of a serious breach goes well beyond any immediate financial costs. Nearly a quarter of firms (23%) mentioned that significant bad publicity resulted from an attack.<sup>1</sup>

<sup>1</sup> [www.hiscox.co.uk/sites/default/files/documents/2021-04/21486-Hiscox-Cyber-Readiness-Report-2021-UK.pdf](http://www.hiscox.co.uk/sites/default/files/documents/2021-04/21486-Hiscox-Cyber-Readiness-Report-2021-UK.pdf)

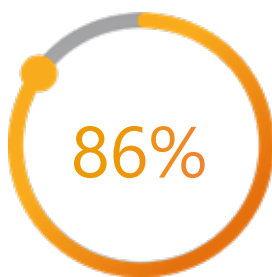




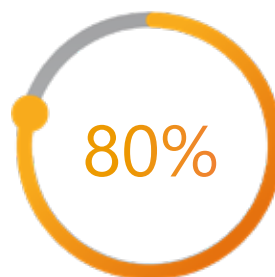
## Assessing the cyber threat for Professional Services Firms

**We asked** to what extent Professional Services Firms are under increasing pressure to protect data and to demonstrate that security measures are in place. We also asked to what extent cybersecurity is becoming more complex.

**You answered** that the likelihood of a successful cyberattack is increasing, and that your own role in terms of trying to manage and mitigate attacks is becoming more difficult.



86% claimed that data integrity is critical for their business

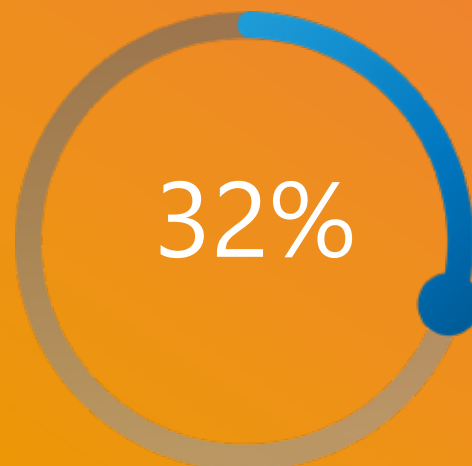


80% explained that the cybersecurity marketplace is becoming more complex



### Pen Testing

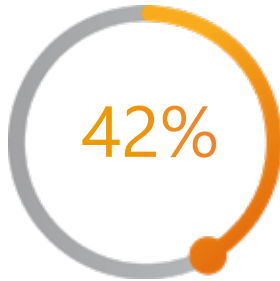
More than 30% did not know whether they undertake regular Penetration Testing



32%

# Meeting the challenge

**We asked** what the major inhibitors were to improving cybersecurity in the Professional Services sector.

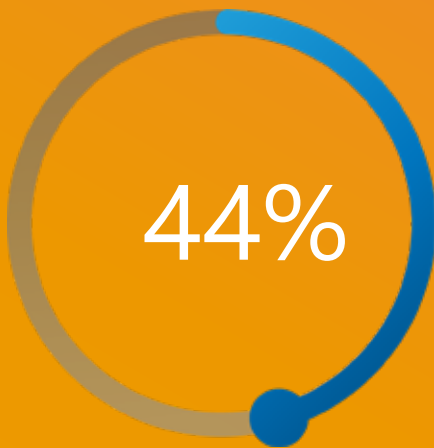


42% felt that budget is a major inhibitor for security

**You answered** that the major challenges involve budget, recruitment and retention as well as certification.



60% stated that skilled resources (recruitment and retention) was a significant limiting factor



44%



## Certification

Less than half subscribe to industry standard Information Security accreditations, e.g. Cyber Essentials & ISO27001



# Understanding Microsoft security

## Microsoft security in 2022



### Global capability

Microsoft monitors more than eight trillion security signals every 24 hours.



### Future-proof investment

Microsoft has committed to invest \$20BN in security over the next five years.



### Best of breed

Microsoft is now leading in five different Gartner Magic Quadrants for security.

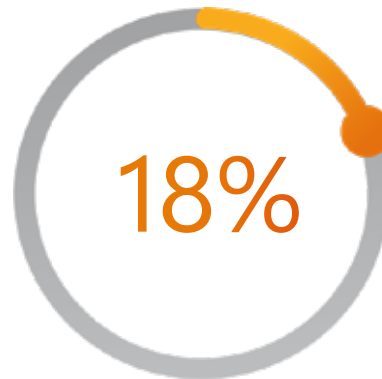


### Seamless security

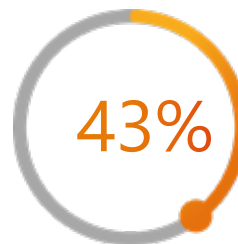
Only Microsoft can offer a uniquely seamless security experience for end-users.

## A Zero Trust approach

A Zero Trust approach is central to the Microsoft Security portfolio.



Just 18% of respondents currently adhere to Zero Trust design principles



43% of participants did not know their Microsoft Secure Score

*“Given Microsoft’s footprint across so many technologies, we’ve been in a unique position to think holistically about the core aspects of security... all coming together as one humming machine with a singular mission.”*



**Vasu Jakkal**  
CVP, Security, Compliance  
and Identity  
Microsoft



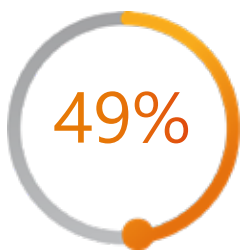


Adopting a Microsoft First approach means not overspending on unnecessary, alternate third-party cyber security solutions, but rather better leveraging your existing Microsoft investment.

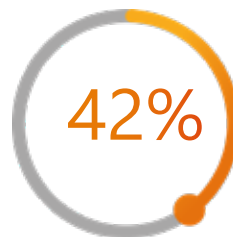
## Adopting a Microsoft First approach

**We asked** to what extent Professional Services Firms were aware of the security features available in Microsoft 365.

**You answered** that 75% were aware of Microsoft MFA but there was a significant lack of awareness about other critical feature sets.



Less than half were aware of Conditional Access and Data Loss Prevention



Only 42% were familiar with Cloud App Discovery



### Scope

52% of participants felt that there is 'a lot' of scope to leverage more value from their existing Microsoft investment



LGL Group

Experience Excellence

## Company

**Company name:** LGL Group

**Incorporated in:** 2000

**Area of operation:** Financial Services

**Office locations:** Jersey, Luxembourg, London

**Who they work with:** Multi-national corporations, high net worth families and private individuals

## Profile



**Peter Messervy-Gross**  
*Chief Information Officer*  
LGL Group

**Peter's bio:** Peter brings 20 years' IT experience to his role at LGL. He has helped modernise LGL's platform and streamline the firm's information security with a Microsoft First approach.

When Peter is not at work, he enjoys taking on endurance challenges. In 2019, he completed a 160km run over a frozen Mongolian lake. Having lost his luggage on route, he completed it anyway - in jeans and a pair of brogues...



Finalist

**Microsoft First Award**  
For Security & Compliance

Professional services



## Q & A with Peter Messervy-Gross

**As the person in charge of LGL's IT security, what is your key concern?**

"As a business, our focus is on quality of client service. Managing anything that puts our data or provision of that service at risk is our ultimate security concern."

**With risk management in mind, what is your understanding of what is now possible with Microsoft from a security perspective?**

"Previously, one had to go to a variety of providers for each of the tools in a security architecture in order to achieve robust risk management. Now, there are very few areas which Microsoft doesn't have covered in its security arsenal (and even those are normally on their published roadmap).

With the Microsoft platform, it is simply a matter of defining our strategy and then selecting the features which suit our needs. This gives us a streamlined approach to our information security."

**So you are saying that Microsoft is now your 'go-to' security provider. What appeals to you about this approach?**

"The simplicity of the solution. As much as taking a practical approach, I wanted to take the simplest one. This solution was the simplest."

Conceptually, Azure infrastructure – Microsoft business systems with a Microsoft security architecture wrapped around them – is the most elegant solution we could design for our business."

**Utilising Microsoft's integrated security stack is what we at Softwerx call adopting a 'Microsoft First' approach to help simplify security. How has adopting a 'Microsoft First' approach to security helped move your business forward?**

"By really committing to the approach, we have seen huge benefits in our capability and our efficiency. The range of security tools available under the higher end licensing is vast. It is far beyond what could be achieved by going to separate suppliers for a similar cost and implementation effort."

Working with Softwerx, we have designed a roadmap to roll-out and utilise those tools, prioritised against our perceived risks.

From an efficiency perspective, we are able to make use of the advisory tools within Azure and 365. Using those tools, we effectively have a team of experts constantly monitoring our environment and informing us of detailed recommendations for improvement."

**Can you give some examples of how this strategy has streamlined your IT security procurement?**

"Overall, we have moved off a number of systems in favour of Microsoft tools with direct cost benefits and at least 'like for like' functionality."

For example, our migration to Azure and Azure Virtual Desktop allowed us to move away from Citrix. We then replaced a third-party SIEM solution with Microsoft Sentinel. Once we had our Azure cloud foundation in place, building on it was straightforward."

**Finally, from your experience, what would be your advice to other businesses?**

"Understand your business, your data landscape and your risks, then enlist the help of specialists."

Unless you have access to a dedicated team of security experts, there is no way you will keep up to speed with the latest threats."

Invest time with security advisors like Softwerx in building a long term roadmap and start ticking items off the list."

*"We have successfully streamlined our risk management with a Microsoft First approach. Previously, you had to go to a variety of providers for world-class security. By working with Softwerx, we've discovered that there are very few areas Microsoft does not effectively cover with its security arsenal."*

**Peter Messervy-Gross  
Chief Information Officer  
LGL Group**





# Key findings & recommendations

## 1. Simplify Security

**If you make security too hard from an end-user perspective, employees will seek to work around it** and your SecOps Team will struggle to manage it.

**Microsoft is the only security company that can offer a truly native and seamless end-to-end user experience** through its holistic 'security by design' philosophy, implicit within Microsoft 365 and Azure. Take advantage of this by streamlining your security from a 'Microsoft First' perspective.

## 3. Get Certified

**A strong cybersecurity posture does more than just mitigate against an attack- it adds value.** Ideally your firm should provide evidence for this through an industry recognised accreditation like Cyber Essentials. Such accreditations increase the likelihood of additional investment and reduce associated costs such as business insurance.

Every Professional Services Firm should as a minimum have a current Cyber Essentials certification in place. **Softwerx strongly recommends a Cyber Essentials Plus certification.**

## 2. Stop Overspending

**Professional Services Firms should stop overspending on unnecessary, alternate third-party security solutions.** These solutions from multiple vendors often overlap, increasing both complexity and cost.

**Your organisation should review what you have already paid for within your Microsoft subscription** and seek to better leverage or augment existing Microsoft solutions.

## 4. Partner Up

Very few respondents claim to have a direct relationship with Microsoft, and **more than half of those surveyed believe they could gain a greater benefit from their Microsoft investment** if they could keep up to date with the constant flow of information and change.

Staying ahead of the Microsoft curve is a full-time job. Your Professional Services Firm should seek to form a trusted partnership with specialist Microsoft security partners whose core business is Microsoft security.



# Take Action



## Book a FREE Microsoft Security Assessment

Understand your Microsoft Secure Score. Build a Road Map with a qualified Microsoft Solutions Architect.

[softwerx.com/secure](https://softwerx.com/secure)



## Get your business formally certified

A Cyber Essentials Plus accreditation is a Government-endorsed certification that forms an ideal security foundation.

[softwerx.com/certify](https://softwerx.com/certify)



## Join the Microsoft Security TechTalks

Join our popular Microsoft Security TechTalk series normally held monthly on the third Tuesday at 11am. #TechTalkTuesday

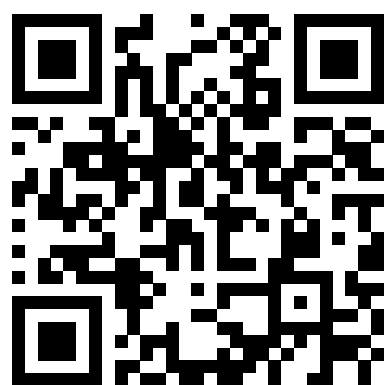
[softwerx.com/techtalks](https://softwerx.com/techtalks)



## Book a FREE Microsoft Licensing Assessment

Take back control of your Microsoft licence spend through the Cloud Service Provider (CSP) platform.

[softwerx.com/licence](https://softwerx.com/licence)



## Get started now

Scan the QR Code on the left or use the link below to access the latest free Microsoft security resources:

[softwerx.com/getstarted](https://softwerx.com/getstarted)

For more information, get in touch:

**+44 (0)1223 834 333**

**info@softwerx.com**

**softwerx.com**

## About this report

This report, published in January 2022, incorporates the first primary research analysis undertaken for the UK Professional Services sector from a Microsoft security perspective. We consulted 64 senior decision makers within financial services, insurance and other Professional Services Firms varying in size from 50 to 1,000 users.

We asked them a set of detailed questions about their overall security posture, as well as their use, adoption, approach and attitude towards their Microsoft 365 investment.

## About Softwerx

Softwerx is a leading Microsoft Cloud Security Practice with specialist knowledge around Microsoft security, infrastructure and compliance.

Our 24x7 Microsoft SOC (Security Operations Centre) is based in Cambridge, UK and provides cutting edge XDR and SIEM-managed services built on the latest Microsoft security stack.

We have been helping to secure the UK's leading Finance, Insurance and other Professional Services Firms for over two decades.

Softwerx holds multiple Gold Microsoft Partner competencies and industry standard accreditations.

## About the Author



Faith Akinbo is a Microsoft Research Analyst at Softwerx, specialising in the empirical research and analysis of Microsoft security.

### Disclaimer:

Information is accurate at time of going to print. Softwerx cannot be held liable for any losses or damages resulting from information provided in this report. The opinions expressed in this report are those of Softwerx Ltd and do not necessarily represent those of Microsoft.

# softwerx

The Microsoft Cloud Security Specialists



✉ [info@softwerx.com](mailto:info@softwerx.com) ☎ [01223 834 333](tel:01223834333) 🌐 [www.softwerx.com](http://www.softwerx.com)

Cambridge Copley Hill Business Park, Babraham, Cambridge, CB22 3GN

London 26 Finsbury Square, London, EC2A 1DS

© Copyright Softwerx 2022. All rights reserved.



#MicrosoftFirst  
#SimplifySecurity

