Cyber Security for Key Decision Makers

Claire Vandenbroecke – Cyber Security Specialist

7th February 2023

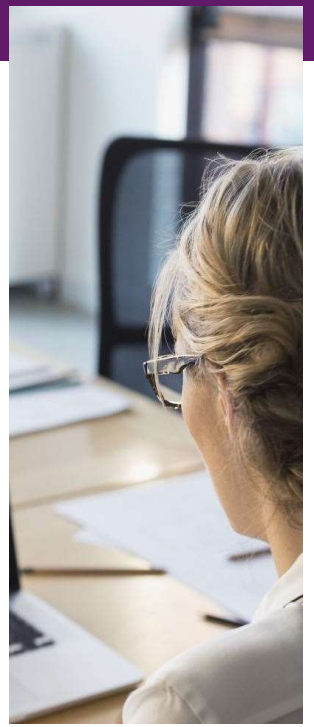
claire.vandenbroecke@tsg.com

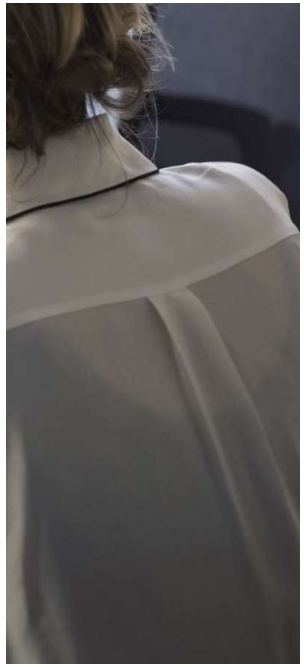
Objectives

- The role you play in supporting your client's cyber security journey.
- How cyber security applies to business security and risk as a whole.
- The important conversations to have with your clients around cyber security.

Agenda

- Threat Landscape
- The real world impact of a cyber attack
- What does this mean to me?
- Key Takeaways
- Q&A





Threat Landscape

TSG®
TECHNOLOGY SERVICES GROUP

Poll

Which threat are you or your clients most concerned about?

1. Email phishing attacks
2. Malware attacks
3. Ransomware attacks
4. Insider threat

Cyber Security Breaches Survey: 2022

All businesses

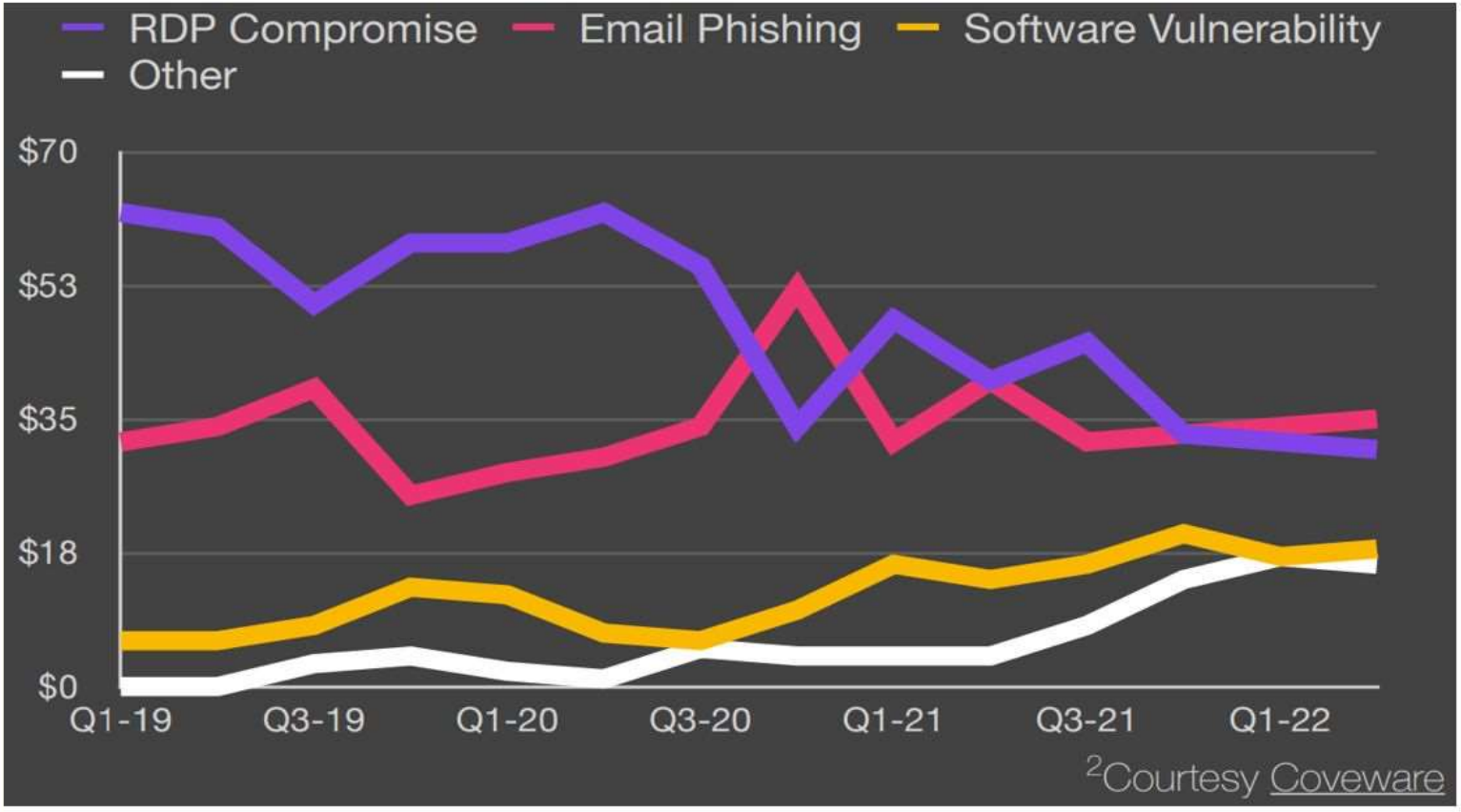
The Cyber Security Breaches Survey is an official statistic. Since 2016, it has measured the policies and processes organisations have for cyber security, and the impact of breaches and attacks. This infographic shows the key findings for UK businesses.

Cyber attack

A cyber-attack is a malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization. **39%** of UK businesses identified a cyber-attack in the last 12 months, with **83%** of these businesses reporting phishing attempts and **26%** identifying a more sophisticated attack type such as a denial of service, malware or ransomware attack.

Cyber Attack Vectors

Email Phishing now most successful for hackers



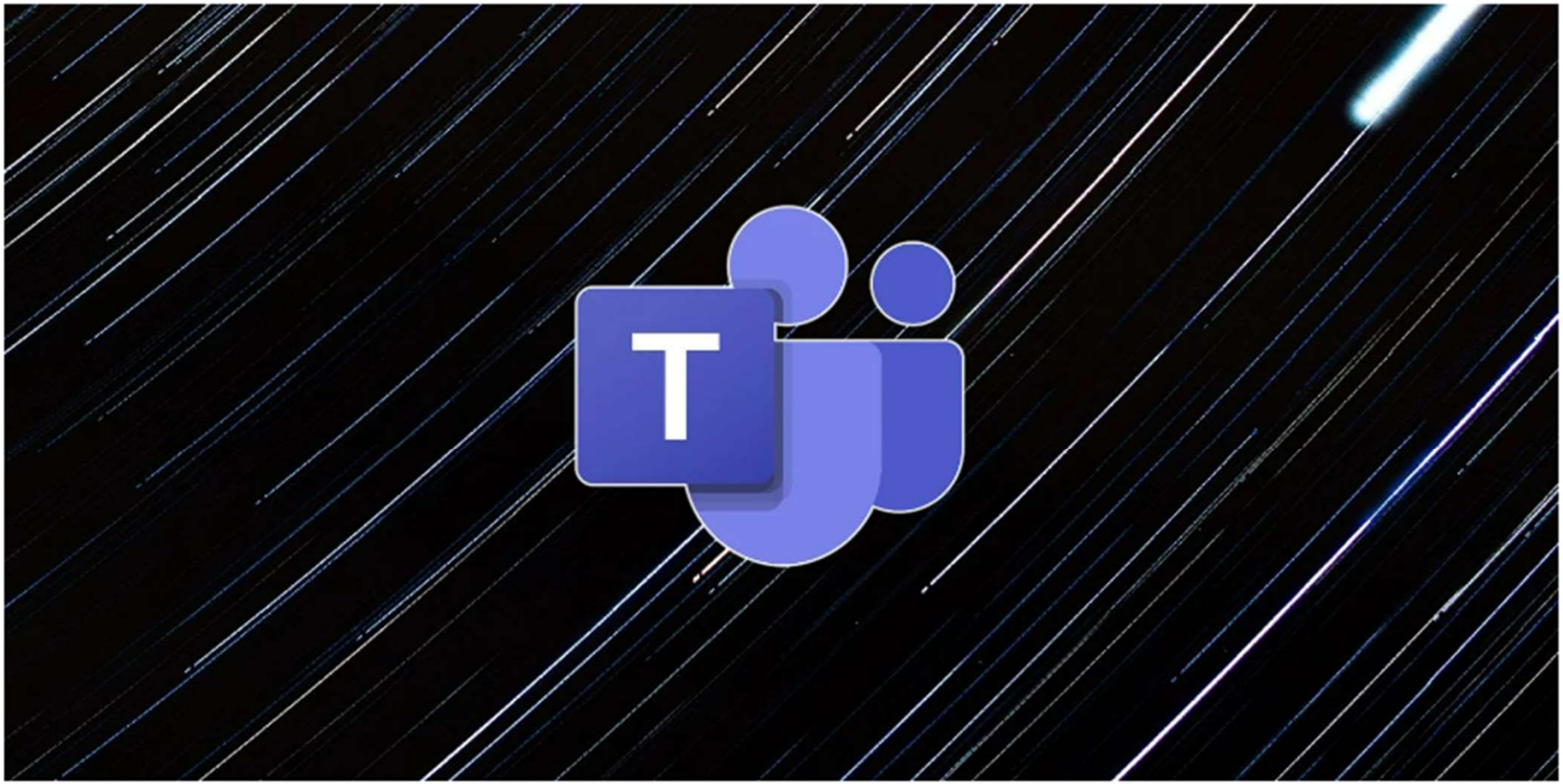
BLACKFOG™
Privacy. Security. Prevention.

Published September 2022

GIFShell attack creates reverse shell using Microsoft Teams GIFs

By Lawrence Abrams

September 8, 2022 03:28 PM 4



Source: https://www.bleepingcomputer.com/news/security/gifshell-attack-creates-reverse-shell-using-microsoft-teams-gifs

Ransomware became the most significant cyber threat facing the UK in 2021.

Due to the likely impact of a successful attack on essential services or critical national infrastructure the NCSC assessed ransomware as potentially as harmful as state-sponsored espionage.

Source: National Cyber Strategy 2022

The real-world impact of a cyber attack

TSG
TECHNOLOGY SERVICES GROUP

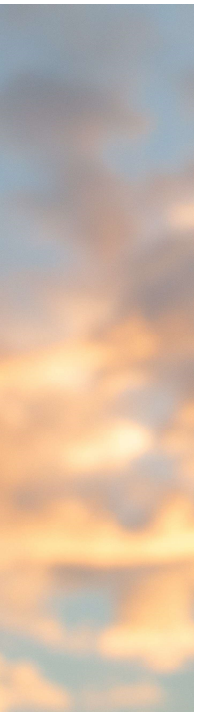
- Reputational Damage
- Emotional Impact
- Restoration Costs

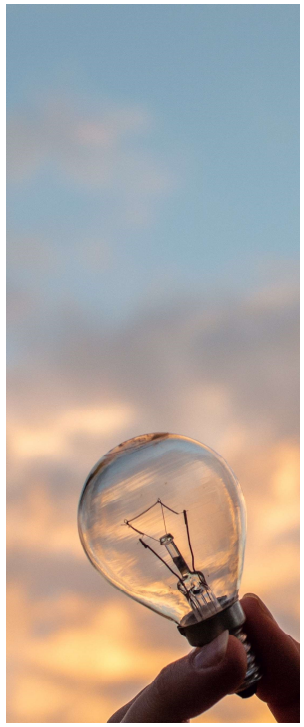
£19,400

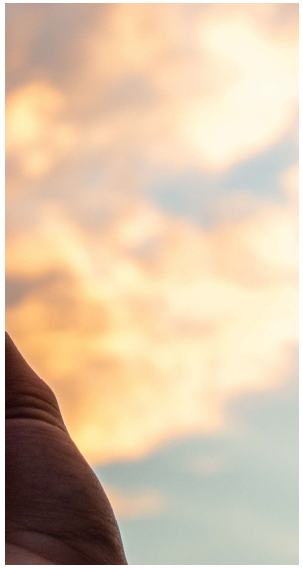
Average cost for SMEs following a cyber attack

Source: UK Government Cyber Security Breaches Survey 2022

The real-world impact of a cyber attack



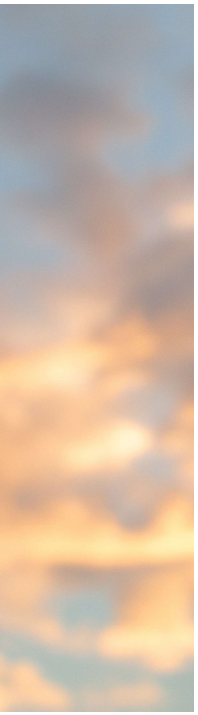


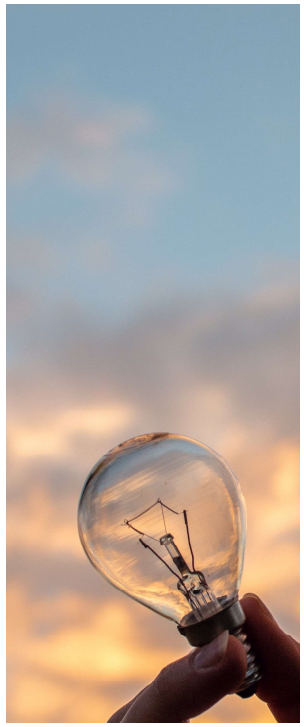


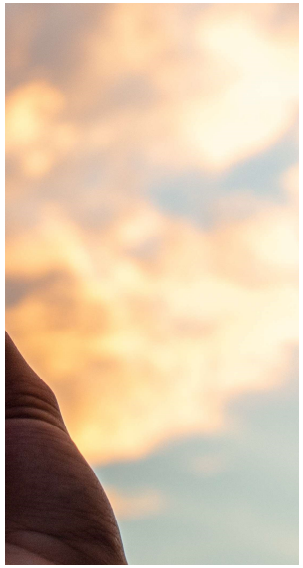
"found the experience 'devastating' and akin to an assault"

Source: Exploring Organisational Experiences of Cyber Security Breaches (publishing.service.gov.uk)

The real-world impact of a cyber attack







"It had a real impact as then I started to question everything that I did… it really got me down"

Source: Exploring Organisational Experiences of Cyber Security Breaches (publishing.service.gov.uk)

What does this mean to me?

TSG
TECHNOLOGY SERVICES GROUP

By 2025, 70% of CEOs will mandate a culture of organisational resilience to survive coinciding threats from cybercrime, severe weather events, civil unrest and political instabilities.

Source: The Gartner Top Cybersecurity Predictions for 2023

TSG
TECHNOLOGY SERVICES GROUP

Cyber security impacts on *every* aspect of an organisation and so needs to be integrated for it to be successful.

Source: Board Toolkit - NCSC.GOV.UK

It's not just about reporting...

To scale fast, increase valuation and escape the routine of day-to-day operations you need to consider each of the 12 building blocks of a world class finance function. These include:

Sell/Exit

Identify Risks

Review Business Plan

Source Funding

Improve Systems & Controls

Implement KPI Reporting

Increase Profit

Improve Cash Flow

Tighten Up Compliance

Optimise Tax & Legal

Audit Outsourcers

Build Strong Banking Relationships

Review Business Plan

Cyber Security is no longer just a conversation for the technical experts, it needs buy-in from the top level.

Key Question

Does my client's business plan address any of the following in relation to a cyber attack or serious incident?

1. Business Continuity
2. Incident Response
3. Disaster Recovery
4. Don't know
5. No

Identify Risks

Having a robust risk management process in place is key when addressing cyber security, it helps you to identify your most vulnerable and valuable assets and decide how to best protect these assets in the event of a cyber attack.

Key Question

Does my client have any of the following in place and documented?

1. Security Audit / Threat assessment
2. Risk Assessment, Risk Register and Risk Matrix
3. Joiners, Movers and Leavers (JML) policy
4. Minimum security standard for third parties / supply chain
5. Don’t know
6. No

Tighten Up Compliance

- Established cyber and information security frameworks can help with a client's cyber security journey.
- Government contracts require Cyber Essentials certification.
- Cyber Insurance is demanding more in order to be eligible for cover.
- Improving your cyber security also assists businesses in complying with Data Protection Laws / GDPR.
- ICO is issuing more fines.

Cyber and Information Security Frameworks

- Network and Information Systems Regulations 2018 (NIS)
- Cyber Essentials & Cyber Essentials Plus (NCSC & IASME)
- Cyber Assurance Level 1 & Level 2 (NCSC & IASME)
- ISO27001

Network and Information Systems Regulations 2018 (NIS)

Established legal requirements on providers of:

- Essential services
- Digital service providers
- Managed Service Providers

Source: www.gov.uk/government/collections

Cyber Essentials & Cyber Essentials Plus (NCSC & IASME)

Cyber Essentials

- Firewalls
- Anti-virus / Malware protection
- User Access Control
- Secure Configuration
- Patch Management

Cyber Essentials Plus

- CE certification required
- Technical audit by a qualified assessor.
- Advised for government contracts

Source: https://www.ncsc.gov.uk/cyberessentials/overview

Cyber Assurance Level 1 and Level 2 (NCSC & IASME)

Cyber Assurance Level 1

- NCSC's Ten Steps to Cyber Security
- Policies and Processes
- More affordable and achievable for SMEs
- CE certification required

Cyber Assurance Level 2

- Level 1 certification required
- Technical audit by a qualified assessor.

Source: https://iasme.co.uk/iasme-cyber-assurance

International Organization for Standardization (ISO27001)

ISO27001

- Worldwide federation of national standards bodies (160+ countries)
- International standard on how to manage information security
- Advised for enterprises with an international reach

Key Question

Does my client fall in to any of these categories?

1. Provider of essentials services / digital service provider / managed service provider
2. Supplier to or customer of any of the above?
3. Applying for a UK government contract (or considering)
4. International client-base
5. No
6. Don’t know

Improve Systems & Controls

With Microsoft planning to enforce MFA for all users this year, technology is becoming increasingly demanding of businesses and how they secure their infrastructure.

Addressing the basic security controls outlined in the Cyber Essentials framework can help a business defend against around 80% of the most common cyber attacks.

Key Question

Does my client have any of the following in place?

1. Managed Security
2. Managed Detection and Response (MDR)
3. Incident Response and Support
4. Don’t know
5. No

TSG
TECHNOLOGY SERVICES GROUP

Cyber security should be seen as an *enabler*: something that supports an organisation's overall objectives rather than a standalone issue.

Source: Board Toolkit - NCSC.GOV.UK

Implement KPI Reporting

"Cyber security should be seen as an enabler: something that supports an organisation's overall objectives rather than a standalone issue."

Integrating cyber security into business KPIs is a way to ensure all employees are aware of their responsibility when it comes to protecting the business from cyber attack.

Source: Board Toolkit - NCSC.GOV.UK

Key Question

Has my client carried out either of the following in the last 6 months?

1. Staff training
2. Phishing campaigns
3. Vulnerability assessment
4. Penetration test
5. Don’t know
6. No

Good cyber security isn't just about having good *technology*: it's also about people having a good relationship with security and having the right *processes* in place across the organisation to manage it.

Source: Board Toolkit - NCSC.GOV.UK

Sell / Exit

"Good cyber security isn't just about having good technology: it's also about people having a good relationship with security and having the right processes in place across the organisation to manage it."

Demonstrating to a potential buyer that your business' *technology, people* and *processes* meet industry-standard requirements for cyber security makes it a much more appealing asset.

Source: Board Toolkit - NCSC.GOV.UK

Key Questions

Q1. Do they have a process that ensures cyber risk is integrated with business risk??

- ✓ How do they assess this risk?
- ✓ How do they manage this risk?
- ✓ How do they balance this risk against others?

Key Questions

Q2. How do they assure themselves that the organisation's approach to cyber security is effective?

- ✓ Do they have an up to date threat assessment?
- ✓ Are their defensive priorities regularly reviewed?
- ✓ Do they test their defences?

Key Takeaways

- The threat of a cyber attack is real, it's not a case of 'if' but 'when'.
- Legislation and compliance means cyber security can no longer be left to the IT experts.
- Addressing the basic security controls outlined in the Cyber Essentials framework can help a business defend against around 80% of the most common cyber attacks.

Poll

Key Takeaways

Q&A

claire.vandenbroecke@tsg.com

TECHNOLOGY SERVICES GROUP

We contribute to our customers' success through partnership, passion and knowledge.