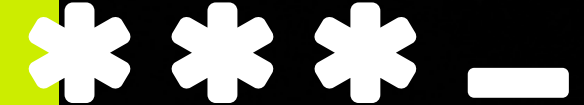


Technology Services Group

tsg.com | 0333 220 0777



# TSG CYBERSECURITY SERVICES





# ONE COMPROMISED CREDENTIAL

---

Are you really aware of the risks to your company's data? Are you sure that your employees, both new and existing are clued up on how to spot threats to your company's data?

Remember, it only takes one compromised credential to have a devastating effect on your organisation and, in some cases, even take it down.

It's becoming clearer that we need to do more as we move into the new world, especially as cyberattacks become more sophisticated.

# What will a cybersecurity attack cost your business?

---

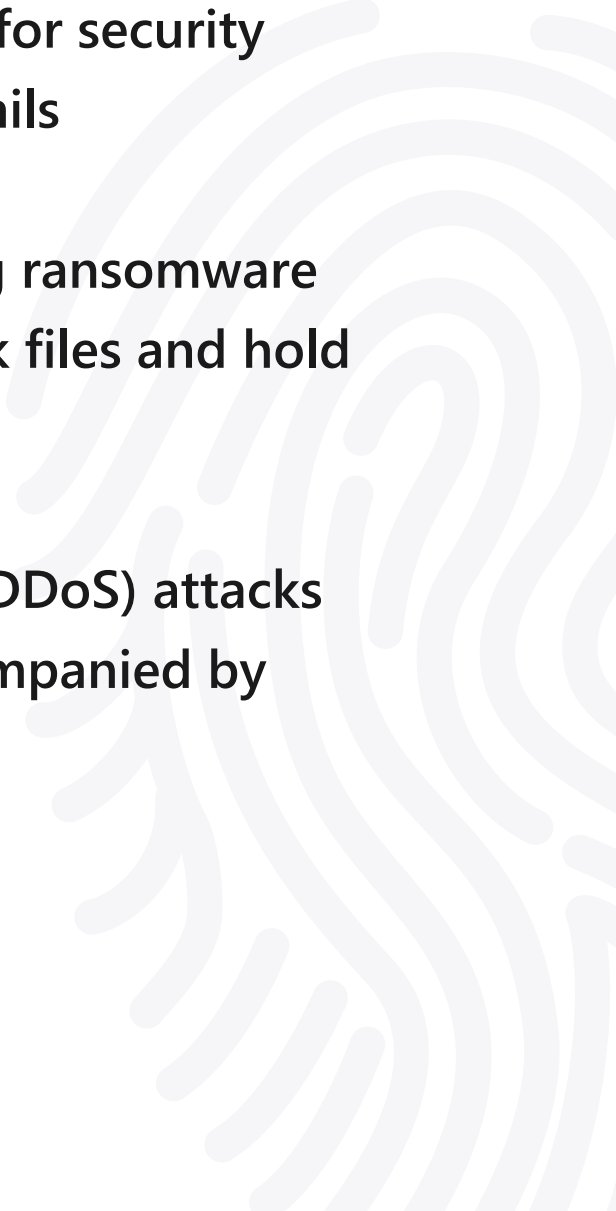
In 2018, British Airways (BA) faced a devastating cyberattack affecting more than 400,000 of their customers. As a result, the Information Commissioner's Office (ICO) fined the airline £20m for failing to protect the personal and financial details of its customers. BA did not detect the cyberattack for more than two months, a failure that broke data protection law.

(2020, ICO fines British Airways £20m for data breach affecting more than 400,000 customers)

As well as the financial implications of the breach, a cyberattack like this can cause massive damage to a company's reputation and a loss of customers and their confidence.

These are the serious consequences of not only having poor cybersecurity, but also failing to recognise a breach in the first place.

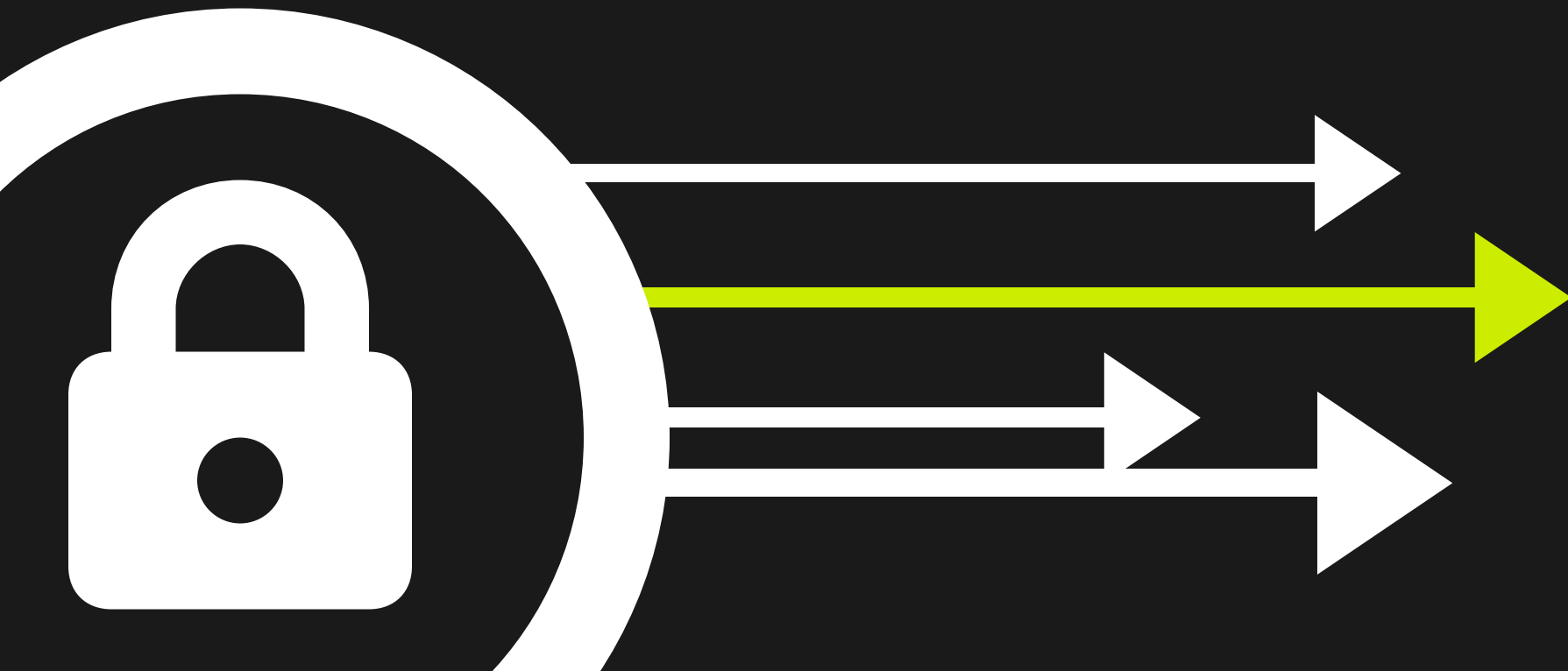
It's important to remember that the most common cyber threats to your organisation include:

- Hacking – including social media and email passwords
  - Phishing – fake emails asking for security information and personal details
  - Malicious software – including ransomware through which criminals hijack files and hold them to ransom
  - Distributed denial of service (DDoS) attacks against websites – often accompanied by extortion
- 



# TSG's Cybersecurity Offerings

At TSG we've streamlined our cybersecurity offerings to ensure that your organisation receives the right level of protection it needs. Our aim is to help you build and strengthen your cyber defence using a collection of services tailored to your needs.



## Basic Security Review

In our basic review we carry out an 18-point assessment of your organisation. Once complete, you will receive a simple report where our experts will highlight areas for remediation. This provides, at a foundational level, areas where your organisation has potential weaknesses towards cyberattacks and discover what else you require to secure your data further.

## Multi-point Security Assessment

Areas covered include the likes of hardware, software (Operating Systems, Applications, Anti-Virus) and user privilege review.

## Advanced Security Review: Certification Pathway

To mitigate the risk to your data, we carry out a much more extensive audit. We use sophisticated tools to delve deep into your network and discover issues and vulnerabilities. We also carry out internal and external port scanning to identify known vulnerabilities. Reviews are completed on policies to make sure they are up to today's standards, for example Microsoft recommends you ban common passwords.

You will receive a detailed report and the outcome directs your business into a position to gain Cyber Essentials accreditation. Cyber Essentials helps you to guard against the most common cyber threats and demonstrate your commitment to cybersecurity. More detail can be found on Cyber Essentials on the 'Recommended additional services' page of this brochure.

# Security as a Service

TSG employs numerous certified cybersecurity engineers and the best tools on the market so you don't need to. Our Security as a Service offering is designed to help you identify, visualise and then proactively remediate risks before they are exploited

## Security as a Service

Even well resourced IT departments struggle to manage the diverse range of technologies, tasks and risks involved in protecting their users 24/7.

TSG's Security as a Service offering aims to support your existing teams, identifying and reducing cyber risks so that you can focus on what you do best - running your business.

### Service Components

We aim to tailor our Security as a Service programs to your unique needs and priorities. A typical program will usually comprise the following elements:

- Detailed vulnerability scanning and posture reviews
- Targeted remediation of top 25 risks and vulnerabilities
- Regular trend analysis and detailed reporting on risk reduction
- Disaster recovery testing
- External penetration testing
- Managed user awareness training



# Vulnerability Management

---

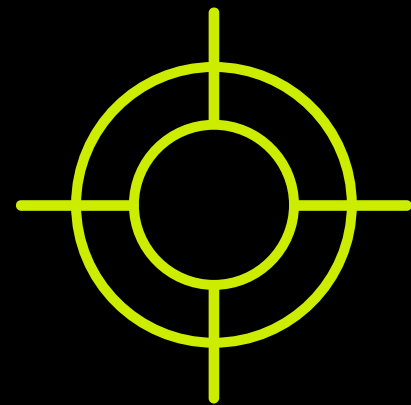
Very few businesses truly understand how their defences stack up against increasingly well resourced and motivated adversaries. Unfortunately, most are poorly prepared to defend against even relatively routine malware and email borne attacks.

TSG's Vulnerability Management service uses award winning scanning tools to help customers visualise their most critical vulnerabilities. Unlike most Vulnerability Management services, we will actively intervene to reduce or eliminate these risks wherever possible. Where it is not possible to fully eliminate a risk, our specialists will work with you to reduce the risk to an acceptable level.

- Unpatched Operating Systems and Software
- Unpatched Hardware (Wifi, Switches, CCTV etc)
- Insecure System Configuration
- Legacy/unused systems and services



Scheduled and on-demand scanning



Targeted remediation



Risk trend analysis



Top 10 vulnerability reporting



Tailored security reports



# User Awareness Training

---

Help your users become key assets in keeping your business safe from constantly emerging threats.

Our managed awareness training programs will deliver award-winning content straight to your users inboxes at a frequency of your choosing.

Training can be completed in only a few minutes per month and takes the form of funny, engaging videos and quizzes that are enjoyable and provocative in equal measure.



# Penetration Testing

We also offer a range of comprehensive penetration testing services that help you identify potentially exploitable vulnerabilities within your infrastructure, critical applications and physical security measures.

Our CREST certified analysts use a variety of tools and techniques to expose weakness and provide clear reporting and actionable intelligence that help remediate risks.



## Infrastructure Penetration Testing (Ethical Hacking)

Infrastructure penetration testing, also called ethical hacking, is the practice of testing an organisation's internal or perimeter network devices to identify vulnerabilities that an attacker could potentially exploit. Penetration testing typically involves a mix of automated software scanning for discovery and manual manipulation and attempts of known or common exploits.

## Social Engineering Testing (Human Error Testing)

Social engineering typically involves tricking employees into making mistakes and exploiting weaknesses or gaps in your workforce security knowledge or physical security arrangements. Social engineering comes in many different forms: it can be performed via email, over the phone, or in person at your office and facilities. TSG will test your organisation's ability to identify and prevent these sorts of attacks, then provide guidance on how to prevent/reduce their impact.

## Application Penetration Testing

Similar to infrastructure testing, application testing seeks to identify exploitable vulnerabilities in an organisation's internal or public facing applications and their interaction with other technologies or systems. Application testing is commonly used to answer questions such as: what vulnerabilities exist, what is their severity, how they should be addressed what is the root cause and what business change is required.



# 24/7 Managed Detection and Response (MDR)

---

Few organisations have the skills or appetite to mount a manned cyber-defence operation 24/7. With TSG's Managed Detection and Response service you can rest assured that our engineers will be available at all hours to help identify and defend against emerging threats.

We use specialised software to actively monitor your environment for Indicators of Compromise (IoCs) and will work to intervene wherever threats or anomalous behaviour is detected.

As well as offering both lead-based and lead-less threat hunting we also maintain a team of dedicated incident responders that will work to rapidly neutralise threats as they are detected.



# Recommended additional services

## ● Cyber Essentials

---

As well as the extensive advanced security review, we also encourage you to acquire the Cyber Essentials accreditation for your business.

Cyber Essentials is a simple but effective, Government backed scheme that will help you to protect your organisation, whatever its size, against a whole range of the most common cyberattacks. This is important because vulnerability to simple attacks can mark you out as target for more in-depth unwanted attention from cyber criminals and others.

Certification gives you peace of mind that your defences will protect against the large percentage of common cyberattacks simply because these attacks are looking for targets which do not have the Cyber Essentials technical controls in place.

For in depth information on Cyber Essentials visit:  
<https://www.ncsc.gov.uk/cyberessentials/overview>

## ● Cyber Essentials Plus

---

Cyber Essentials Plus is a more rigorous test of your organisation's cybersecurity systems. It requires a more in-depth analysis by TSG's Cyber Essentials partner who carries out a formal assessment.

## ● ISO 27001 and PCI Compliance

---

For customers that require independent validation of their security posture we can offer tailored programs to help you achieve ISO 27001 and PCI Certification.

# Overview of TSG's Cybersecurity Offerings

## Security Audit

- Point in time security assessment and report
- Can be tailored to be aligned with Cyber Essentials or CyberEssentials+

### Benefits

- Point in time understanding of risk
- Can give a roadmap to CyberEssentials compliance

### Limitations

- Security is not a point-in-time problem. Whilst audits and security assessments are helpful they do not replace a constant proactive approach to managing risk.

## Vulnerability Management as a Service

- Dedicated vulnerability management of both internal and external networks
- Rank orders risks to maximise remediation efforts against highest impact concerns
- Can provide regular reporting on vulnerability trend lines – providing assurance to senior managers
- Unlike other Vulnerability Management providers we will work with you to remediate issues directly

### Benefits

- Rank ordering of threats and remediations ensuring maximum ROI
- Easy visualisation of risks and ongoing trend lines as issues are resolved
- Addresses some of the most common attack vectors for ransomware

### Limitations

- Focuses largely on the patching and security of hardware, operating systems and end user applications
- User awareness training, external penetration tests and regular review of security logs via proactive services are still recommended



## Security Proactive Services

- Dedicated time to review key security KPIs and logs
- Will review security logs, expired logins, antivirus status, backup status etc
- Can be used to manage the patching of high risk platforms such as firewalls, clusters, wifi services etc

### Benefits

- Regular, tailored checks around most common failures in an organisations security posture
- Provides regular assurance of posture
- Proactively looks for anomalies

### Limitations

- Does not include advanced vulnerability scanning but could be combined into a consolidated security program

## User Awareness Training

- A managed program that employs award winning videos and phishing training delivered direct to user inboxes
- Test results and click through rates can be reported back to provide evidence of effectiveness over time

### Benefits

- Helps users become security assets rather than security risks
- Essential way of helping minimise the principal risk to security in most organisations – email attack/phishing

### Limitations

- Important but limited in scope
- Does not address technical risks

## Penetration Testing

- External or Internal Penetration testing of a network of the customers choice

### Benefits

- Provides point in time assurance of external perimeter

### Limitations

- Important but usually limited in scope to external company perimeter
- Usually point in time assessment



## Business Continuity and DR

- Quarterly disaster recovery or business continuity testing

### Benefits

- Provides regular assurance that key systems can be recovered

### Limitations

- Gaps can still exist between DR tests
- Full coverage of customer environment can be difficult to guarantee

## Compliance Services

- Support in achieving Cyber Essentials or ISO 27001

### Benefits

- Can provide customers with a clear roadmap to external certification
- Combined with Security Proactive Services can help achieve and retain compliance in a short period of time





# THE NEXT STEP

If you feel like your company's data could be at risk or would like more information on how TSG can help with your current cybersecurity defence measures, please get in touch with us today.

---

[tsg.com](https://tsg.com) | [0333 220 0777](tel:03332200777) | [info@tsg.com](mailto:info@tsg.com)

