CYBERWHITE™
DIGITAL SECURITY CONSULTANTS

CyberWhite Support Service

Overview.

Today, organisations are expected to be agile and dynamic, delivering increased value and of course, unparalleled levels of customer service.

In the background, the cyber threat landscape continues to evolve, presenting increasingly complex challenges. These threats are designed to limit the effectiveness of organisations through either interruption of service, exfiltration of data and financial or reputational harm.

The CyberWhite Support Service (CSS) helps you to address these challenges. Our experience in developing bespoke risk mitigation strategies, enable us to work in partnership with you, supporting you to secure your most critical information assets.

The CSS is suitable for all organisations, irrespective of size. Each engagement is tailored to suit your specific, organisational requirements. This delivers a cost-effective way of increasing and broadening your organisational security knowledge base without the need for investment in additional staff.

It's reassuring to know that you can rely on the team of highly qualified security experts at CyberWhite. Each team member is a subject matter expert in their respective fields, holding security clearance to BPSS or SC levels. In addition, some team members also hold enhanced DBS certificates.

This allows the CyberWhite team to become a trusted, integral, and invaluable part of your team.

This combination of experience, security clearance and industry leading customer service is what makes the CyberWhite difference.

CYBERWHITE™
DIGITAL SECURITY CONSULTANTS

Background.

The Best practice states that organisations and executive management teams should have access to security advice and expertise.

A major challenge that many organisations face, is sourcing and securing this advisory support.

This challenge is often further exacerbated as governance, risk and Compliance often falls outside of the skills and remit of many trational IT Teams.

The CSS solves this problem by providing a wide range of valuable benefits. It provides assurance that the team of experts at CyberWhite are available to support your organisation wherever information security expertise and resource may be required.

This is all available for a simple, fixed monthly cost. This includes providing access to subject matter experts and technical experts in the fields of information security, data security and cyber security.

Available Services
Incident Response.
Governance, Risk & Compliance Advice.
vCISO – (virtual Chief Information Security Officer).
Dark Web and Company Profile Reports.
Security Scans & Penetration Testing.
Access to the CyberWhite Technical Security Helpdesk.

So, whether you require strategic advice at board level, operational planning with senior leaders or perhaps project implementation support, testing or validation of security protocols or security awareness and training programs, CyberWhite is here to support your journey.

CYBERWHITE™
DIGITAL SECURITY CONSULTANTS

Incident Response.

An incident response plan helps organisations identify, respond to, recover from and most importantly, learn from incidents.

The team at CyberWhite can assist in reviewing, building or supporting a CIRT (Cyber Incident Response Team) within your organisation.

Core elements include creating a new plan if you don't have one or reviewing, and where appropriate updating your existing incident response plan. In addition, we can assist with identifying, assessing and analysing incidents and co-ordinating and communicating response efforts. Post incident, we provide comprehensive technical advice and support to help with remediation and reporting.

To complement this, we can also develop and manage audits through rigorous test plans. Of course, each element should be supported with clear and concise documentation. CyberWhite can create new policies or review existing policies for relevance to ensure that they are aligned with and support the organisational strategic plan and risk appetite. Post incident we also provide recommendations from lessons learned and support with implementation.

The final, and often overlooked element of incident response is staff awareness and training. CyberWhite support this with bespoke, on premise learning sessions which involve role play and are based on real life scenarios.

Due to the variety of potential incident types and complexity of scenarios, the training element will be scoped separately.

"CyberWhite has become an important part of our cyber support eco system. They have become an integral part of our training and awareness program, creating bespoke scenarios to support staff of all abilities. They are also a trusted partner for the provision of our internal and external penetration testing, delivering clear and concise reports with superb remediation support".

IT Director: Legal Services.

CYBERWHITE™
DIGITAL SECURITY CONSULTANTS

Virtual CISO.
(Chief Information Security Officer).

The CyberWhite virtual Chief Information Security Officer (vCISO) takes a hands-on approach that goes beyond just a technical engagement.

Our approach will take the time to understand your organisational culture, your compliance requirements, risk tolerance and internal processes.

Our team of experts has decades of experience, building information security programs that work alongside your business objectives and show measurable improvements to your security posture.

To achieve this, we combine risk assessment results and remediation efforts.

The key is for us to gain an initial understanding of the strengths and weaknesses of your existing security program.

Based on the results, the CyberWhite vCISO lead consultant will work with your executive leadership to understand goals, budget and capacity.
This allows us to provide actionable recommendations and a roadmap based on the findings of the risk assessment.

With the roadmap agreed and in place, we then work with the operational security team to train staff and make the recommended improvements. This enhances the ability of your organisation to protect sensitive information and increase operational efficiencies.

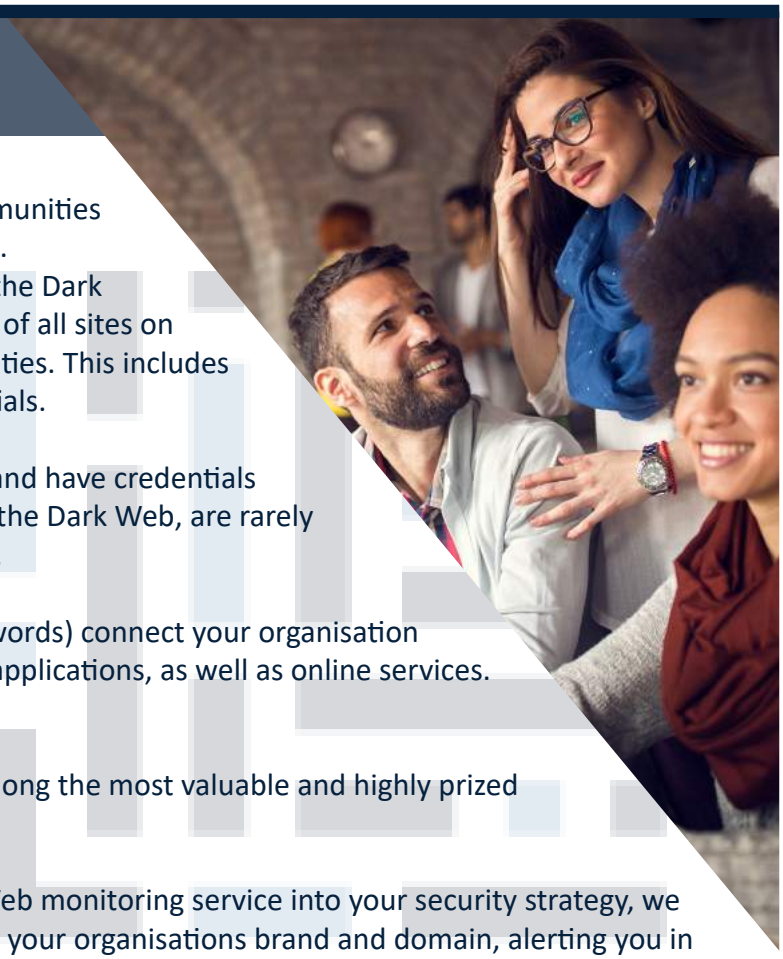
Whether you need high level guidance on a monthly or quarterly basis or require hands on help several days per week, our vCISO's are able to build a solution for you.

"The advice and support I have received from the vCISO team at CyberWhite have been enormously helpful. They have brought experience and order to an increasingly important area of our business and really augmented our existing skills".

Managing Director: Facilities Management.

CYBERWHITE™
DIGITAL SECURITY CONSULTANTS

The Dark Web.



The Dark Web is made up of digital communities that sit below the surface of the Internet.
While there are legitimate purposes for the Dark Web, it is estimated that more than 50% of all sites on the Dark Web are used for criminal activities. This includes the disclosure and sale of digital credentials.

Organisations that suffer data incidents and have credentials compromised and subsequently sold on the Dark Web, are rarely aware, and often only when it is too late.

Digital credentials (usernames and passwords) connect your organisation and your employees to critical business applications, as well as online services. Cyber-criminals are aware of this.

This is why this type of information is among the most valuable and highly prized across Dark Web marketplaces.

By incorporating the CyberWhite Dark Web monitoring service into your security strategy, we identify, analyse and proactively monitor your organisations brand and domain, alerting you in real time the moment any data appears for sale.

This aspect of the CSS produces a detailed quarterly report, highlighting any exposed information available on the Dark Web, information which may leave your organisation vulnerable to cyber-attacks and reputational harm if not addressed.

"CyberWhite have been a pleasure to deal with by repeatedly demonstrating their professionalism and technical knowledge throughout the procurement and execution of our project. From initially exploring our goals to a consultant working with us on-site and remotely, we've enjoyed a positive experience that has ultimately benefited our organisation and helped to improve our Cyber Security posture."

Cyber Security Manager: Housing Association.

CYBERWHITE™
DIGITAL SECURITY CONSULTANTS

Security Scans and Penetration Testing.

Assessing the robustness of your environment through regular scans, vulnerability assessments and penetration tests is a key element of all good security programs.

Knowing your vulnerabilities and how attackers might exploit them provides tremendous insight that you can use to improve your security posture.

We recognise that no two applications are the same, so we bring just the right combination of skills, performance and experience to you based on your requirements.

All our team are certified security professionals with deep domain expertise and a passion for finding vulnerabilities.

Of course, identifying a vulnerability is just one part of the process.
At CyberWhite, we take great care in checking for false positives and false negatives.
This robust process ensures that the final report contains only issues that you need to address.

In addition, as part of the reporting process we like to meet with you.
This proves invaluable in allowing you to ask questions and apply context to the findings.

Once testing is complete, PX Limited will have access to the CyberWhite helpdesk who will be on hand to provide support and guidance throughout the remediation stage.

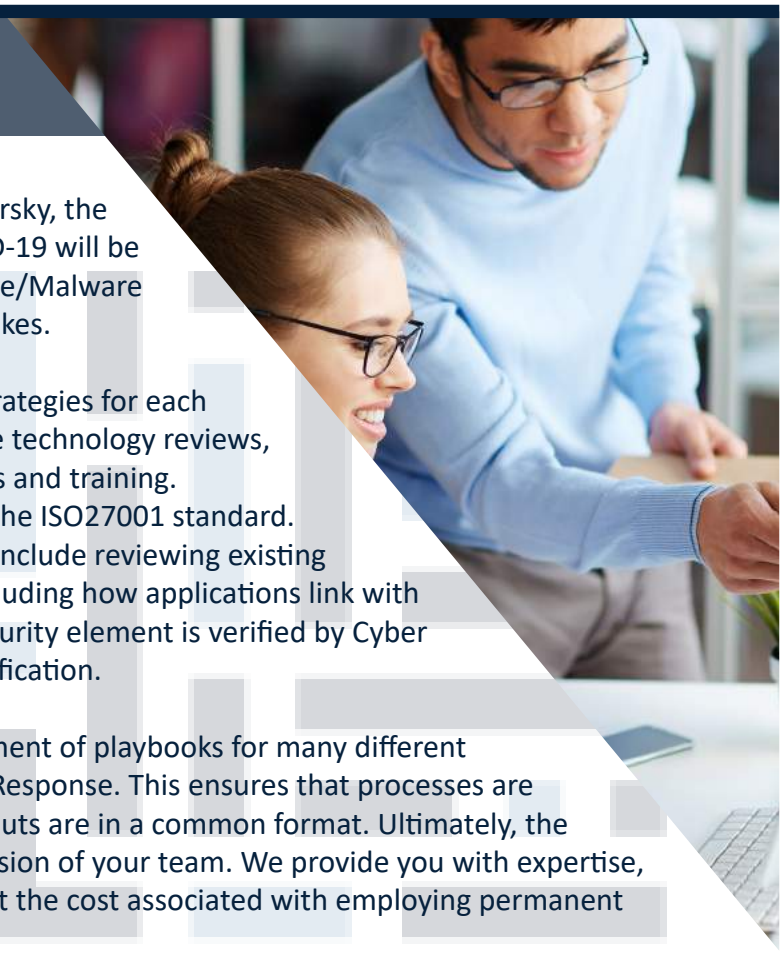
Finally, once all the recommendations have been actioned, we carry out a final scan to ensure that no legacy issues remain.

“Regular security testing of our applications and infrastructure provides assurance that our security program is working. The skills and knowledge from the team at CyberWhite provides real peace of mind for the board”.

Head of Governance: Third Sector

CYBERWHITE™
DIGITAL SECURITY CONSULTANTS

Why CyberWhite?



According to recent research from Kaspersky, the three most persistent threats post COVID-19 will be Phishing/Social Engineering, Ransomware/Malware and Lack of Awareness or end user mistakes.

At CyberWhite, we provide mitigation strategies for each of these threats. These strategies include technology reviews, process flow reviews and user awareness and training. Several of these are key components of the ISO27001 standard. Comprehensive technology reviews can include reviewing existing solutions for robustness and security including how applications link with other applications and of course, the security element is verified by Cyber Essentials and Cyber Essentials plus certification.

Our expertise also includes the development of playbooks for many different operational activities including Incident Response. This ensures that processes are repeatable across departments and outputs are in a common format. Ultimately, the team at CyberWhite operate as an extension of your team. We provide you with expertise, experience, agility and scalability without the cost associated with employing permanent members of staff.

“One of the reasons I chose to partner with CyberWhite was their reputation for customer service and technical support. I haven’t been disappointed. The team at CyberWhite, will remain my partner of choice for all my information and cyber security requirements”

IT & Service Manager - Financial.

CYBERWHITE™
DIGITAL SECURITY CONSULTANTS

Helpdesk Support.

Effective support is critical.
At the start of our engagement, we will agree the definitions of what constitutes HIGH, MEDIUM and LOW priorities.
This removes the potential for confusion, provides assurance and sets clear expectations

	HIGH Severity	MEDIUM Severity	LOW Severity
HIGH Impact	Priority 1	Priority 2	Priority 3
MEDIUM Impact	Priority 2	Priority 3	Priority 4
LOW Impact	Priority 3	Priority 4	Priority 5

We monitor each support case with three maxims: Respond Within, Plan Within and Resolve Within.

Respond Within: This is the maximum amount of time that it will take to get back you and confirm who is dealing with your request.

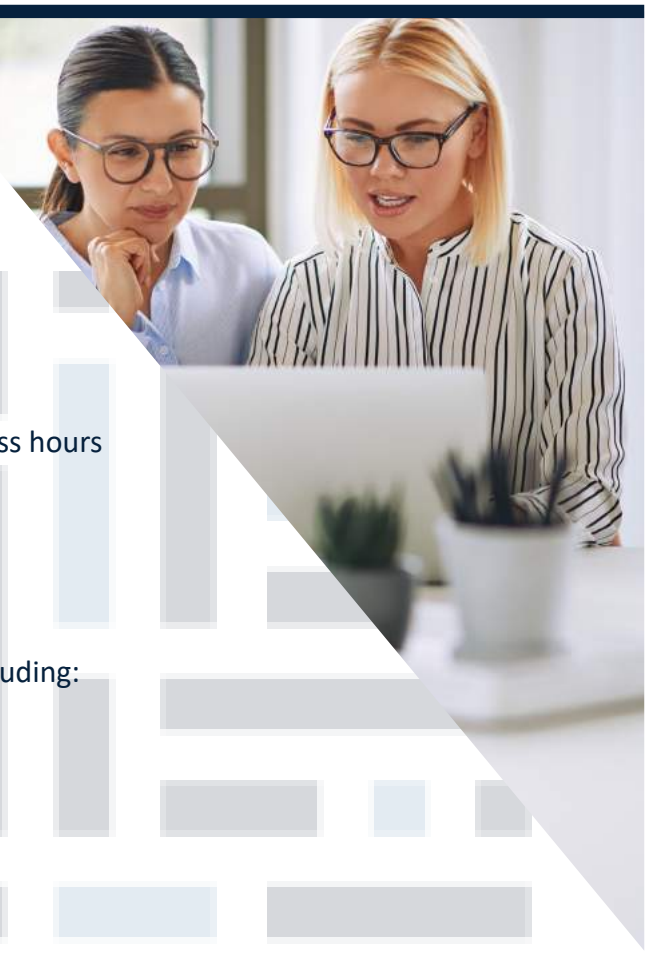
Plan Within: This is for our own use, to ensure that we are on track to resolve your challenge on time.

Resolve Within: The maximum amount of time required to close your ticket.

Priority Type:	Respond Within:	Plan Within:	Respond Within:	Goal %
Priority 1	1 hour	4 hours	8 hours	95%
Priority 2	1 hour	4 hours	8 hours	95%
Priority 3	1 hour	8 Hours	16 hours	95%
Priority 4	2 hours	8 hours	16 hours	95%
Priority 5	8 hours	16 hours	40 hours	95%

CYBERWHITE™
DIGITAL SECURITY CONSULTANTS

Contacting Us.



Advice and support is provided in various ways including email and telephone.

Tel: 0191 562 3228
Email: CSS.helpdesk@cyberwhite.co.uk

Standard support is available during normal business hours (excluding public holidays in England).

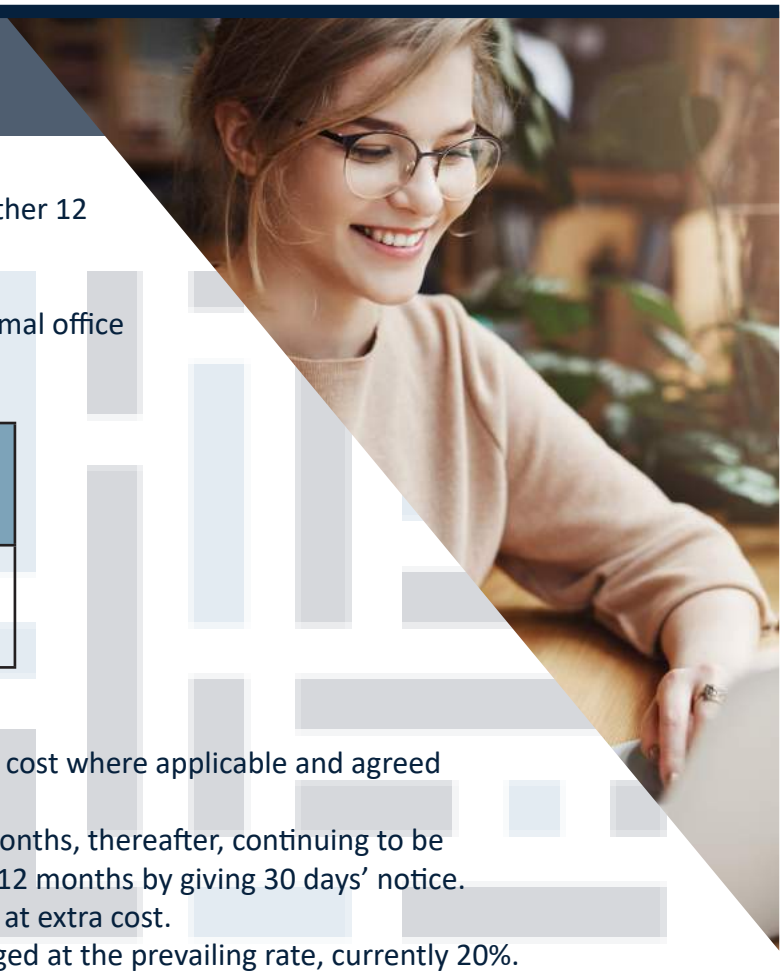
Monday – Friday
9:00am – 5:00pm

CyberWhite offer a range of additional services including:

Simulated Phishing.
Penetration Testing.
Business Email Compromise Protection.
Tailored End User Training.
Artificial Intelligence Virtual Security Analyst.
Ransomware Prevention.
Social Engineering.
Password Review and Management (NIST SP 800-63B compliant).
Cloud Protection.
Authentication.

CYBERWHITE™
DIGITAL SECURITY CONSULTANTS

Commercials.



The CSS may be procured for terms of either 12 months, 24 months or 36 months.

Standard support is delivered during normal office hours.

Description
CSS Mon. – Fri. 9.00am - 5.00pm (Excluding Bank Holidays)

Please note:
Travel and expenses are charged extra at cost where applicable and agreed in advance.
The CSS is for a minimum period of 12 months, thereafter, continuing to be invoiced monthly. It may be ended after 12 months by giving 30 days' notice.
24/7 x 365 extended support is available at extra cost.
All prices exclude VAT which will be charged at the prevailing rate, currently 20%.
Subject to our standard terms and conditions, a copy is available upon request.

CYBERWHITE™
DIGITAL SECURITY CONSULTANTS

Our Technologies.

CyberWhite partner with a range of trusted vendors.

Please visit our website for further information.

ALERT LOGIC
AppCheck ACCURACY IS EVERYTHING
appgate
arcserve
Authlogics
bitglass
Check Point SOFTWARE TECHNOLOGIES LTD
Cymulate
deepinstinct BEFORE YOU KNOW IT
egress
galaxkey
GURUCUL
HEIMDAL™ SECURITY
IRONSCALES
KnowBe4 Human error. Conquered.
netconsent
RAPID7
solarwinds
thycotic
VECTRA
yubico

CYBERWHITE™
DIGITAL SECURITY CONSULTANTS

Information.

For more information on our CSS, please fill in your details below and return to Phil Anwyll at phil.anwyll@cyberwhite.co.uk:

Name: _____

Company: _____

Email: _____

Tel: _____

CyberWhite Ltd

T: 0191 562 3228 **W:** www.cyberwhite.co.uk **E:** info@cyberwhite.co.uk

Registered Office
Portland House
Belmont Business Park
Durham
DH1 1TW

Head Office
Mulberry House
3 Defender Court
Sunderland
SR5 3PE

Regional Office
Boho 5
Bridge Street East
Middlesbrough
TS2 1NY

Follow us on social media

Facebook
YouTube
LinkedIn
Twitter
Instagram