SALUS

CYBER

CYBER SECURITY CONSULTANCY SERVICES

WWW.SALUSCYBER.COM

CYBER SECURITY CONSULTANCY

Organisations typically use consultancy to obtain expert advice on how they can maximise strategy, increase profits, add value, and resolve issues. Cyber Security consultancy supports all those key elements and acts as a critical friend to a business dealing with complex issues where they lack internal capacity.

Our consultants bring many decades of experience with them from various industry sectors so that we can adapt to your specific needs. Salus Cyber consultants apply critical thinking to problem-solving and supporting our clients to get the maximum value out of an engagement.

Why use our consultant services?

COST REDUCTION

Your bottom line is a critical factor in any business decision you make. However, the Cyber Security Skills gap has made it challenging to get the right hire for your business need. In addition, the growing trend towards remote working opens the opportunity to think differently about what your fixed workforce should look like.

RISK REDUCTION

Cyber threats are constantly evolving, and security is becoming a significant concern for businesses whether you have 10 or 200 clients. Equally, your 3rd party suppliers present risks directly to you as well. Bringing in fresh eyes to help you manage those risks using an experienced cyber security consultant means you can be assured that you are receiving a high-quality review of your existing people, process, and technology risks.

EXPERIENCE WITH NEW TECHNOLOGIES

As cyber-attacks occur more frequently and hacker capabilities have improved, new safety technologies are rolling out to protect businesses from these threats. Therefore, having the right advice on how best to use limited funding is critical. External consultants bring a deep understanding of the pros and cons of products and services. The best part of this is that they are not salespeople.

One of the best financial decisions you can make is investing in the right people, whether that's a single cyber security expert or training employees. Unsure of where to start? Working with a Salus Cyber security consultant can take the guesswork out of the process and help ensure you're on the right path.

ENHANCING YOUR STAFF WITH CYBER SECURITY CONSULTANTS

When you work with Salus, we can help educate your current employees on the latest information on cyber security and technology risk. Additionally, we can help them implement better cyber security in the workplace practices each day and broaden their horizons. Once the consultant(s) have completed their job, your employees will continue to implement the new security practices that were established.

APPLICATION SECURITY SERVICES

Cyber Security Improvement

Salus Cyber provides a consultancy presence from our Senior Team to identify areas of weakness in the operational and technical space. Our Senior Team will work with your organisation to ensure observations can be translated into a shift in strategy that will directly improve the cyber security maturity.

Salus Cyber evaluates all elements of the current cyber security landscape to identify gaps in capability or improvements that could be made.

The evaluated areas of an organisation include:

- Technical controls.
- Technologies in use.
- Policies.
- People.
- Current auditing.
- Standards or certifications achieved.

The service is designed for organisations of all shapes and sizes looking to make gains over extended periods where marginal operational and tactical improvements significantly impact the overall cyber maturity.

Our senior team is composed of experienced cyber and security risk consultants with a minimum of five years of experience advising organisations on technical and procedural changes to improve their cyber security posture and strategy, including:

- Cyber Essentials and Cyber Essentials Plus Assessors.
- IASME Governance Assessors.
- CHECK Team Leader Assessors.
- ISO 27001 Lead Auditors.

CYBER SECURITY CONSULTANCY

Cyber Incident Exercising

All strategies and plans need to be exercised within a business. Cyber security incident response has become an essential component of Information Technology systems. Cyber security-related attacks have become more numerous, diverse, damaging, and disruptive. Understanding how resilient your business is to such attacks is now a critical business requirement.

New types of cybersecurity-related incidents emerge frequently. Whilst preventative activities based on the result of risk assessments can lower the likelihood of incidents; not all incidents can be prevented.

INTERNAL VS EXTERNALLY FACILITATED EXERCISING

Exercising helps organisations evaluate their Incident Response and Disaster Recovery Plans and assumptions around resilience within their 3rd party supply chain. Internally facilitated exercises are helpful but often mean that key people who would generally be at the forefront of incident management are not being evaluated realistically.

Salus Cyber facilitated exercising allows all key decision-makers to fully participate in the exercise in their real-world roles to ensure the full organisational response capabilities are tested.

Externally facilitated exercising allows all the key individuals within the business to practice their responses in a safe and managed environment. This approach helps refine your people, process, and technology strategies. In addition, it acts as a valuable check of your people's skills, highlighting areas where further training and development might be needed. Salus can develop custom exercises to fit the business need and bring its significant experience in Cyber Security vulnerability testing and management to the task.

CYBER SECURITY CONSULTANCY

DPA18, GDPR and Privacy Gap Assessment

Data Protection Impact Assessment (DPIA) is a process to help you understand and minimise the data protection risks your company may well be exposed to without knowing.

The Information Commissioners Office (ICO) sets a mandatory requirement for impact assessments in any case where a Cyber incident is 'likely to result in a high risk' to individuals.

Whilst organisations come in all shapes and sizes, undertaking a data privacy assessment is a way for you to analyse your processing and data retention and help you identify and minimise data protection risks systematically and comprehensively. Those core principles can also be applied to digital Intellectual property held within your systems.

DPIAs should consider compliance risks and broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm – to individuals or society at large, whether physical, material, or non-material. It is also the case that not all such privacy risks will be Cyber Security related.

Salus Cyber can conduct assessments to identify where privacy risks exist in your business processes and help support the development of a more formal DPIA which must consider both the likelihood and the severity of any impact on individuals.

Salus Cyber can also work with you to align your privacy management polices with the NIST Privacy Framework.

https://www.nist.gov/privacy-framework

CYBER SECURITY CONSULTANCY

Virtual Chief Information Security Officer (vCISO)

The pressures on organisations in the connected world to manage legal/regulatory obligations and maintain an effective information security program are significant and changing daily.

A CISO is a senior-level manager/executive responsible for developing and implementing an information security program, which includes procedures and policies designed to protect enterprise communications, systems, and assets from internal and external threats.

The CISO has a lead role in ensuring that the organisation's incident response plans are maintained and effective and liaises with other key business leaders on the structure of business continuity plans and disaster recovery.

The CISO will often own the strategy and policies that cover:

IDENTIFY – PROTECT – DETECT
RESPOND - RECOVER

The CISO must align security initiatives with the broader business objectives and outcomes to do this effectively. However, a full-time CISO is not necessarily the most cost-effective approach to these challenges.

WHY CONSIDER A SALUS VIRTUAL CISO?

A vCISO is a cost-effective option for having a CISO, enabling your organisation to benefit from board-level expertise in the cyber security domain. If your organisation has a transformation agenda, vCISO's can help architect the security strategy and, in many cases, help manage its implementation. They often provide a cost-effective alternative to a full-time CISO. They support:

- Information security planning and management activities.
- Organisational and management structure.
- Initiatives affecting information practices.
- Security risk management activities.
- Evaluation of third parties with access to organisational data.
- Coordination of audits by regulators or customers.

Why are vCISO becoming more popular? The idea of a virtual CISO has grown in demand with organisations for several reasons:

CISOs are in high demand – Cybersecurity has moved to the forefront of business risk thinking with the rise in cyberattacks, data breaches, sophistication in attacks, and the focus on an organisation's information. It is understandable for an organisation to want to put a comprehensive set of controls and technologies in place and needs a CISO. A vCISO allows an organisation to quickly fill a CISO role without going through the hiring process.

Continued on next page...

CYBER SECURITY CONSULTANCY

Virtual Chief Information Security Officer (vCISO) (continued)

Full-time CISOs can be expensive and hard to find – A business might need the skills but cannot afford the permeant salary costs in the current market. A vCISO allows organisations to avoid the expense of employing one in-house full-time, only paying for the services and time used.

- **vCISO can be more experienced** – A vCISO has implemented information security programs for many clients in various industries and sizes, giving them a broad range of expertise that can be applied to your organisation.
- **vCISO can be anywhere** – The growing trend of remote working allows a business to think differently about its workforce strategies and optimise the time needed to fulfil a role.
- **vCISO are a consumption-based option** – We can perform the tasks based on an agreed scope of work. So, you're paying for the services you want.

OTHER BENEFITS WE CAN BRING

- **Bridging and Hiring a New Full-Time CISO** – The departure of a business's existing CISO may be untimely regarding current security initiatives. A seasoned vCISO can come in, provide value in reviewing the current cybersecurity strategy and help recruit, select, and transition to a full-time CISO.

- **Developing a Mature Cybersecurity program for a Smaller Organisation.** When a full-time CISO is too costly for an SME, a vCISO works part time to provide enterprise-calibre expertise to craft a security program. The organisation would, otherwise, not be capable of developing.

- **Creating a Compliance Program** – Organisations with or without a current CISO do not have the expertise on a specific compliance mandate and how it translates to develop policy and processes to secure protected information.

- **Re-aligning Cyber Spend** – Whatever the organisation did six months ago to protect against cyber risk is likely not as effective today. A vCISO can help organisations of every size by looking at the current budget and spending to help identify ways to spend it more effectively and efficiently on improving security and reducing risk.

CYBER SECURITY CONSULTANCY

Supplier Assurance

The advent of 'Just in time' and 'agile supply chain' methodologies have been tested significantly during the COVID pandemic. A growing trend for Cybercriminals to focus more actively on the supply chain space for financial gain. As a result, supply chain disruption can create significant business damage (reputationally and fiscally).

Salus Cyber works with clients to review supplier assurance and improve internal processes (and supports its clients with remediation of supplier security weaknesses).

Any business must have a well-defined 3rd party management strategy. Your business needs to follow the National Cyber Security Centre's best practice:

Understand the risks
- Understand what needs to be protected and why
- Know who your suppliers are and build an understanding of their security.
- Understand the security risk posed by your supply chain.

Establish Control
- Communicate your view of security needs to your suppliers.
- Set and communicate minimum security requirements for your suppliers.
- Build security considerations into your contracting processes and require your suppliers to do the same.
- Meet your security responsibilities as a supplier and consumer.
- Raise awareness of security within your supply chain.
- Provide support for security incidents.

Check your arrangements
- Build assurance activities into your supply chain.

Continuous improvement
- Encourage the continuous improvement of security within your supply chain.
- Build trust with suppliers.

Salus Cyber can work with you to address all the above.

CYBER SECURITY CONSULTANCY

Remote Working Security Assessment

COVID-19 saw many organisations being forced to adopt a remote working practice. As a result, it has become essential to ensure security is a priority. Remote workers that access the systems and data they need from home can create a wide range of cyber risks that attackers can quickly exploit.

This service assesses the essential controls of the IT infrastructure, ensuring that a secure configuration is in place for remote access. It also ensures adherence to policies and governance whilst working remotely.

Additionally, Salus identifies that adequate capacity planning is in place. The security challenges faced by most organisations when adopting remote working include:

- Larger attack surface.
- Undefined Perimeters.
- Identity and access management challenges.
- Reduced endpoint visibility.
- Employee-owned device usage.
- Managing cloud applications.

A remote working security assessment from Salus Cyber is an audit designed to help comprehensively identify risks from employees working outside the office. A remote working security assessment includes the following:

- Policies and procedures.
- Remote access technologies.
- BYOD and device management.
- Existing remote working practices.
- Data controls and flows.
- Logging and monitoring.
- Review employee training and education.
- Device configuration.

CYBER SECURITY CONSULTANCY

Cyber Essentials Basic (CE)

Cyber Essentials Basic consists of a self-assessed questionnaire (SAQ). First, applicants must affirm and describe their systems' compliance with the Cyber Essentials specification. This SAQ is then marked according to Cyber Essentials marking criteria.

The Cyber Essentials Basics is designed to cover several cyber security concerns affecting enterprises in today's highly networked world. The SAQ covers the following five (5) security controls:

- Boundary firewalls and internet gateways.
- Secure configuration.
- Access control.
- Malware protection.
- Patch management.

SELF-ASSESSMENT QUESTIONNAIRE (SAQ)

Applicants are expected to answer honestly and provide supporting details for their answers. Example responses are provided at every stage of the questionnaire. A Salus Cyber consultant can optionally guide clients through the process to ensure appropriate responses have been provided and lower the potential for resubmissions in the event of a failure.

Cyber Essentials Plus (CE+)

Cyber Essentials Plus is the audited element of Cyber Essentials and extends the assurance provided by Cyber Essentials Basic. The five controls are the same as Cyber Essentials Basic; however, they are only tested against a subset of IT assets.

The first element involved will be a review of the Cyber Essentials report; this certificate must have been issued in the past three months to the Cyber Essentials Plus audit. Next, the consultant will use this report to define the scope of work for the Cyber Essentials Plus audit, namely, which assets require testing.

The testing comprises multiple elements, an external vulnerability scan, an internal credentialed patch audit and vulnerability scan, a review of the anti-malware security features in use, and a review of the browser and email protections in place.

SALUS

CYBER

CYBER SECURITY
CONSULTANCY SERVICES

WWW.SALUSCYBER.COM
01242 374087

CYBER ESSENTIALS CERTIFIED PLUS

THE CYBER SCHEME

Assured Service Provider
in association with National Cyber Security Centre

CHECK
IT Health Check Service

Crown Commercial Service Supplier

ISOQAR REGISTERED 0026
UKAS MANAGEMENT SYSTEMS
Certificate Number 18737
ISO 9001