Virtual CISO (vCISO) Datasheet

Who do you turn to when you need to improve your organisation's cyber security?

What a vCISO provides:

- ☑ Benchmark maturity level
- ☑ Conduct a risk assessment
- ☑ Implement a risk register
- ☑ Create & implement security policies
- ☑ Evangelise security policies throughout the organisation
- ☑ Build out key procedures (BCP/IR)
- ☑ Ensure processes in place to enforce policies/procedures
- ☑ Implement & manage ISMS
- ☑ Build a roadmap of continuous security improvements
- ☑ Remediate priority issues
- ☑ Report to C-Level stakeholders
- ☑ Provide senior leadership & guidance

Autodata's vCISO Service

Many organisations lack strategic cyber security leadership and hence overlook the fundamentals required to create a solid security baseline to build upon.

Beyond this, a worrying number of companies of varying sizes - both small and large - have no discernible cyber security programme in place whatsoever. This can be attributed to a lack of time, resource or budget but typically, it's due to the fact there's simply no one in the organisation with the necessary experience to take responsibility for implementing and managing an effective cyber security strategy.

What they need is an experienced individual within the organisation charged with ensuring that continuous security improvements are being discussed, agreed, implemented and reported to the senior leadership team. Appointed on a retainer basis, Autodata's vCISO service adds tremendous value by providing access to a highly experienced, CISSP-certified CISO, who can work with your senior leadership and IT teams, to dramatically improve security and reduce risk within your business.

We can structure a flexible service to meet the demand and budget of your organisation at a fraction of the cost of a permanent hire.

When would you use a Virtual CISO?

- When you don't have the budget or need for a fulltime CISO
- When you have a roadmap to recruit a permanent CISO but are still some way off hiring
- When someone in your InfoSec team has left the organisation leaving you with a skills gap
- When you have an IT security/IT operations team but no CISO
- When you only have a general IT team with no IT security specialists

Crucially there has to be an appetite to improve IT security within your organisation and this has to come from the top down, so buy-in from your CEO/MD/FD is essential.

CISSP

CIS SecureSuite® Membership

CYBER ESSENTIALS PLUS

bsi ISO/IEC 27001 Information Security Management CERTIFIED

256-260 Old Street, London, EC1V 9DD
t. +44 (0) 20 7749 7949 | e. salesteam@autodata.co.uk

Our vCISO Process

IDENTIFY THE GAPS

Our vCISO service deliverables will depend on your overall level of cyber security maturity, hence we would recommend undertaking a maturity assessment at the beginning of an engagement, to fully understand where your organisation is in relation to security.

As a CIS SecureSuite member, Autodata subscribes to the globally recognised CIS Controls. One of our CISSP certified security consultants will run an assessment of your organisation against these, providing a detailed report across all 18 Controls, with recommendations on which areas are a priority for your specific organisation to address.

CIS Controls are unique in providing Implementation Groups (IGs 1-3) which enable cyber security maturity to be tailored to your business risk and exposure, and built up incrementally over time. Using our vCISO service and the CIS Framework you can ensure a relevant and effective security strategy can be implemented.

RUN AN IT RISK ASSESSMENT WORKSHOP

It's important to identify security risks, assess the threat they pose and understand the appetite for accepting risk within the senior leadership team. The purpose of this assessment is to mitigate risks to prevent security incidents and compliance failures, focussing resource on the most pressing issues within the business.

We will run a workshop with your internal IT team to demonstrate how a risk matrix works and show you how to prioritise assets and identify risks. If there is no risk treatment plan in place, we can provide template risk registers and guidance on how to quantify, record and discuss any existing or future risk.

IMPLEMENT FOUNDATIONAL ELEMENTS

Organisations often overlook the fundamental elements of IT security, none more so than creating, implementing and communicating both IT and company user security policies and procedures such as:

- IT SECURITY POLICY
- ACCEPTABLE USE POLICY
- BUSINESS CONTINUITY PLAN
- INCIDENT RESPONSE PLAN

We run a workshop to help you create relevant security policies and procedures, providing templates to document them and guidance to implement and communicate to existing and future employees.

CISSP

CIS SecureSuite® Membership

CYBER ESSENTIALS PLUS

bsi ISO/IEC 27001 Information Security Management CERTIFIED

256-260 Old Street, London, EC1V 9DD
t. +44 (0) 20 7749 7949 | e. salesteam@autodata.co.uk

Our vCISO Process

REMEDIATE ISSUES

Once you understand your security gaps and which risks to address first, you can progress to remediation. With Autodata's vCISO service, you can start to address issues in a number of key areas, such as:

- Inventory and Control of Enterprise Assets
- Inventory and Control of Software Assets
- Data Protection
- Secure Configuration of Enterprise Assets and Software
- Account Management
- Access Control Management
- Continuous Vulnerability Management
- Audit Log Management
- Email Web Browser and Protections
- Malware Defenses
- Data Recovery
- Network Infrastructure Management
- Network Monitoring and Defence
- Security Awareness and Skills Training
- Service Provider Management
- Application Software Security
- Incident Response Management
- Penetration Testing

ONGOING STRATEGY, LEADERSHIP & GUIDANCE

IT security is a journey, and an ongoing roadmap of continuous improvement is essential for your business to stand the best chance of weathering the increasingly hostile threat landscape.

It is also important that your internal IT team have a point of reference to guide them and that progress is recorded and reported to senior management, to ensure that the necessary changes are being made.

Having a retained vCISO service from Autodata ensures that you have the leadership in place to maintain an effective strategy.

INCIDENT RESPONSE MANAGEMENT

Clearly the aim is to prevent any security incident from occurring; but in the event that your company is breached, it is incredibly important to know what to do and who to turn to. Having a detailed Incident Response plan in place ensures your company knows what steps to follow.

It is equally important to have access to the necessary expertise to respond to a breach in order to lessen the impact of a cyber incident via triage, analysis, containment, remediation and recovery.

Autodata can provide assistance in the unfortunate event of a breach via an additional retained service.

CISSP

CIS SecureSuite® Membership

CYBER ESSENTIALS PLUS

bsi ISO/IEC 27001 Information Security Management CERTIFIED

256-260 Old Street, London, EC1V 9DD
t. +44 (0) 20 7749 7949 | e. salesteam@autodata.co.uk