Peopl e

Best Practice Security

SAEPIO
INFORMATION SECURITY

DATASHEET

Virtual Chief Information Security Officer - vCISO

The first step of a security improvement journey is to establish your **Baseline** – 'where are you today?' Once established, it's advised to define a Target State – 'where do you want to get to?' Now you need a Plan. The creation and implementation of a **Security Improvement Plan** drives forward your risk reduction in a prioritised fashion.

Whilst more organisations than ever are starting to build the in-house teams to deliver this improvement. With the current industry skills gap, security practioners are in short supply, and recruitment is a lengthy and expensive business. This shortage affects all levels, but is particularly felt when someone is needed to communicate the security strategy & progress back to the board.

This is where a Chief Information Security Officer comes in, ideally separate from the IT function they can help to both define and deliver a plan, and make sure the leadership team are kept in the loop with regular updates and insights.

The role of the CISO has never been so important for aligning security and business objectives. It ensures compliance to multiple, at times overlapping, standards and the protection of data and technology.

Using IT to manage security is often the route of least resistance but can also be the least beneficial to the organisation. Not only do IT have many competing requirements for their time, there is also an element of marking your own homework; how do you challenge security policy and practices when you may have been the person that implemented these in the first place?

ABOUT SAEPIO?

Saepio is an Information Security advisor that helps organisations reduce their cyber risk and improve security posture.

Saepio believe Security is more than technology. Best practice policy and process direct a successful security strategy. Products and people help to enforce it

CYBER ESSENTIALS PLUS

If your organisation doesn't currently employ a CISO, then a Virtual one from Saepio could be a great idea. We believe the vCISO approach provides a level of security not previously available or affordable to many organisations. On a retainer basis, the vCISO's time is utilised according to your flexible demands and offers superior access to security knowledge alongside substantial cost savings over a permanent hire.

" A "Virtual CISO" from Saepio has been instrumental in helping us efficiently work towards a vital external compliance requirement, on time and on budget. - Information Security Manager, Leading Personal Services plc "

A vCISO provides on-demand access to an experienced security professional who can provide advice and assistance whenever it is required.
Every organisation is unique, but areas that are likely to require attention are:

- Re-confirming threats and vulnerabilities, and the development of treatment plans
- Raising security awareness and embed within the culture of the organisation
- Introducing and monitoring cyber security operational procedures
- Verifying existing architecture to ensure best security practices are applied
- Reviewing third-parties and service providers
- Providing an internal focus for information security, includi thought leadership

Peopl

Best Practice Security

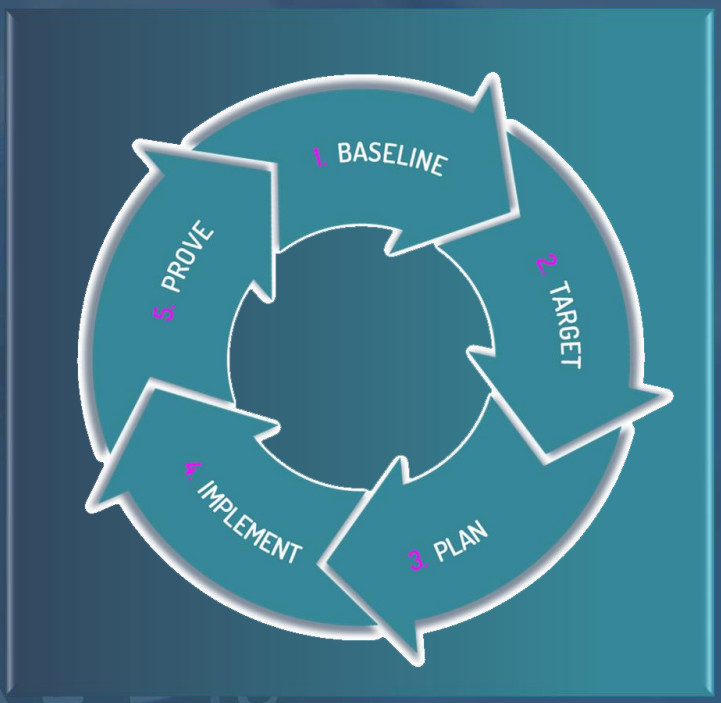
SAEPIO
INFORMATION SECURITY

DATASHEET

vCISO Responsibilities

The **Virtual CISO** would be expected to work across an organisation, reporting at a senior level, with responsibilities that would typically include:

- Creation of a risk register
- Establish and manage an ISMS framework
- Information threat management
- Information on privacy and data protection
- Incident response investigation
- Information security operations
- Establish IT steering committee
- Assess and advice on IT staff skill set and training requirement
- Involve business leaders in IT directives
- Security vendor management
- Oversee regulatory compliance
- Track return on investment on IT security spend



How can a vCISO security help you?

Appointing a CISO may appear unnecessary while systems seem secure, but waiting until a breach occurs could be disastrous. A preventative rather than reactive approach to security issues is by far more sensible. The role is structured to dictate security strategy, an objective that will be hindered if they're fighting fires from the start.

We believe an organisation should focus on its core markets and not allow itself to be distracted. Having a third-party help manage the security risk, and free senior management to focus on the business, in the knowledge that its obligations to secure both information and systems are being looked after.

The virtual role adds to the capability of the organisation and takes nothing away. At the end of the engagement the skills and knowledge remain, either transferred to another individual or encompassed within company policy, process and procedure. The organisation need not be concerned with directly retaining skilled and scarce resource, at a time when the demands on security management are at an all-time high.

Ultimately, the vCISO forms a vital bridge between your internal IT function, your Risk & Compliance teams, and your Board. They give focus, they track progress, and they will help your organisation on its journey of **Continuous Security Improvement.**

According to a 2019 survey, 38% of Fortune 500 companies do not currently have a CISO!