CySure

Virtual Online Security Officer

Manage your business safely and avoid cyber threats

Challenges for Large Organisations

Recent experience for large enterprises shows that security breaches result in high costs of remediation, loss of customers and future business.

Where a loss of personal data results the ICO is now regularly imposing significant fines generating the publicity that generates reputation damage. Similar fines are levied by authorities in regulated industries.

Effective Cyber Security requires continuous effort as the nature of threats is evolving, so it is vital that key activities such as regular risk reviews, staff training and awareness and basic cyber hygiene such as software patching are part of "business as normal" activity. The board also needs to monitor risk, ensure that board directives are being followed and take action when they are not.

An organisation that puts in place appropriate protections, follows its process and maintains audit records to show that it is doing the right thing can significantly reduce the likelihood of a breach and fines or reputation damage if a breach occurs.

Security Controls

No technology will provide security for a business without the involvement of people. The recommended approach is to use a set of security controls implemented by people that complement deployed technology to maintain an appropriate level of security.

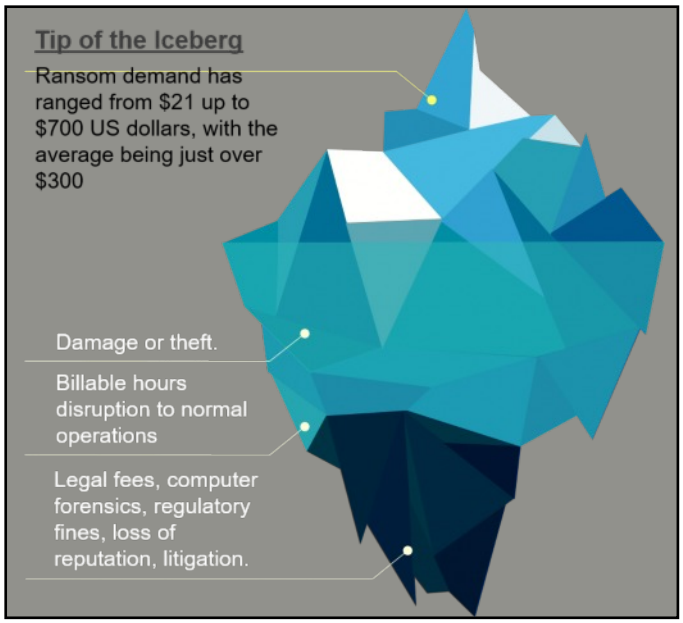
There is much misinformation about GDPR. It is seen as creating additional processes that add cost and deliver no business benefit. In many cases its implementation has created unnecessary cost, for example around the subject of consent which is not required if holding data is necessary to meet contract obligations. GDPR was forced on business because of the cavalier attitude to holding third party's data and the damage to those third parties that resulting from loss.

An organisation that can demonstrate it manages data securely and therefore minimises the risks to a customer should win more business. Using technology effectively increases efficiency and drives down cost for the business creating further benefit.

Minimising complexity

The key points of GDPR are can be summarised as CIA: Confidentiality, Integrity and Availability. Personal data must be protected from unauthorised access, particularly sensitive data, it must be correct so that any decisions taken based on it are robust and must be available so that people are not denied a service on which they depend.

The implications are far reaching and must be considered for all systems that handle data and throughout the lifetime of holding data, starting with "secure by design" principles.
The relationship with Data Subjects imposes specific responsibilities on organisations: the requirement to obtain consent, to respond to data subject access requests, to ensure data is accurate and to delete data when requested balanced against obligations to retain data for lawful purposes.



An organisation's policies must state precisely what data is being collected, what it will be used for and how long the company will store that data. GDPR gives customers more control over their data is and what it's being used for. It also gives an organisation more contact with its customers. The issue is whether it can benefit from this.

What does VOSO do?

There is a wealth of information publicly available from recognised bodies that explains the principles of cyber security and for those that have the time an inclination to read it the underlying detail. Searching via Google can hide this amid the vast amount of product information that does not have the same level of reliability.

VOSO is points customers to the information they need to understand cyber security such as Cyber Essentials, GDPR, IASME, NIST, ISO 20071 and HIPPA.

VOSO provides a series of workflows that implement these standards, provides example policies they refer to and communicates to you in simple terms what your business needs to be doing and when, to protect your online equipment and stored information. These workflows can be modified to meet the needs of individual businesses depending on the size and type of the business and the level of risk that it faces. You do what is appropriate to your business.

For customers seeking accreditation to a standard such as Cyber Essentials, VOSO steps you through the questions helping you to understand its meaning and the actions that you need to take to answer the question positively. It also provides you boiler plate text in plain English as example answers which you can edit to reflect what you actually do, or adopt and change what you do accordingly to be compliant.

There can be a challenge for customers who simply do not understand the basic terms of IT and for them we can provide access to consultancy to help them understand these terms. Most customers actually do understand many of the terms but not all. VOSO is designed to help those customers do the simple things themselves, then identify just those set of tasks where they require help limiting the cost of external consultancy they need.

A key element of cyber security is maintaining the level of staff training and awareness so that employees can recognise when an attack is taking place and take the necessary action. VOSO makes available simple training that is publicly available and then ensures people are tasks to undertake this training.

VOSO provides to managers and the board a dashboard so that they can see that people are doing what they have been tasked allowing them to take action if people are not carrying out their tasks. This includes the initial staff training and tasks that are to be carried out on a regular basis. VOSO also provides the workflows that implement the organisation's policies when responding to external events and incidents.

Thus, VOSO ensures the board is continually aware of your security status though its dashboard, audit trail and reports so that the organisation can demonstrate its compliance with its policies. Thus, preparing for a security audit should be a trivial exercise to print off a report and provide it to the auditor.

Emerging data breach notification laws are establishing standards on the methods, information, and time frame for notifying parties that have been breached. Penalties exist for ignoring such new laws. Changes to law and regulation can be difficult to communicate across the organisation.

Using VOSO to managed these processes ensures that changes can be introduced across the organisation and followed optimising the ability to remain compliant in the future.

Managing across departments and locations

An effective organisation is able identify a business issue that it faces, share accurate information rapidly between its decision makers, make good decisions based on the involvement of the team and then rapidly implement those decisions to deliver the desired outcome.

VOSO is based on all employees with access to computers being registered users. Each user is allocated roles associated with their job specification. When users are distributed across multiple sites, their actions can be coordinated using VOSO across all business processes associated with Cyber Security increasing the effectiveness of the organisation to respond to threats as they occur in as efficient and low-cost manner.

Single Dashboard

The VOSO dashboard provides details of progress of all tasks currently assigned as well as the ability to monitor Key Performance indicators that show organisation performance as an aggregate of activity. VOSO supports general organisation wide KPIs that are visible to those in authorised groups. Also supported are individual KPIs where users may set specific metrics for themselves. From the KPIs users may drill down into the underlying data to determine the source of metrics so that they can take action.

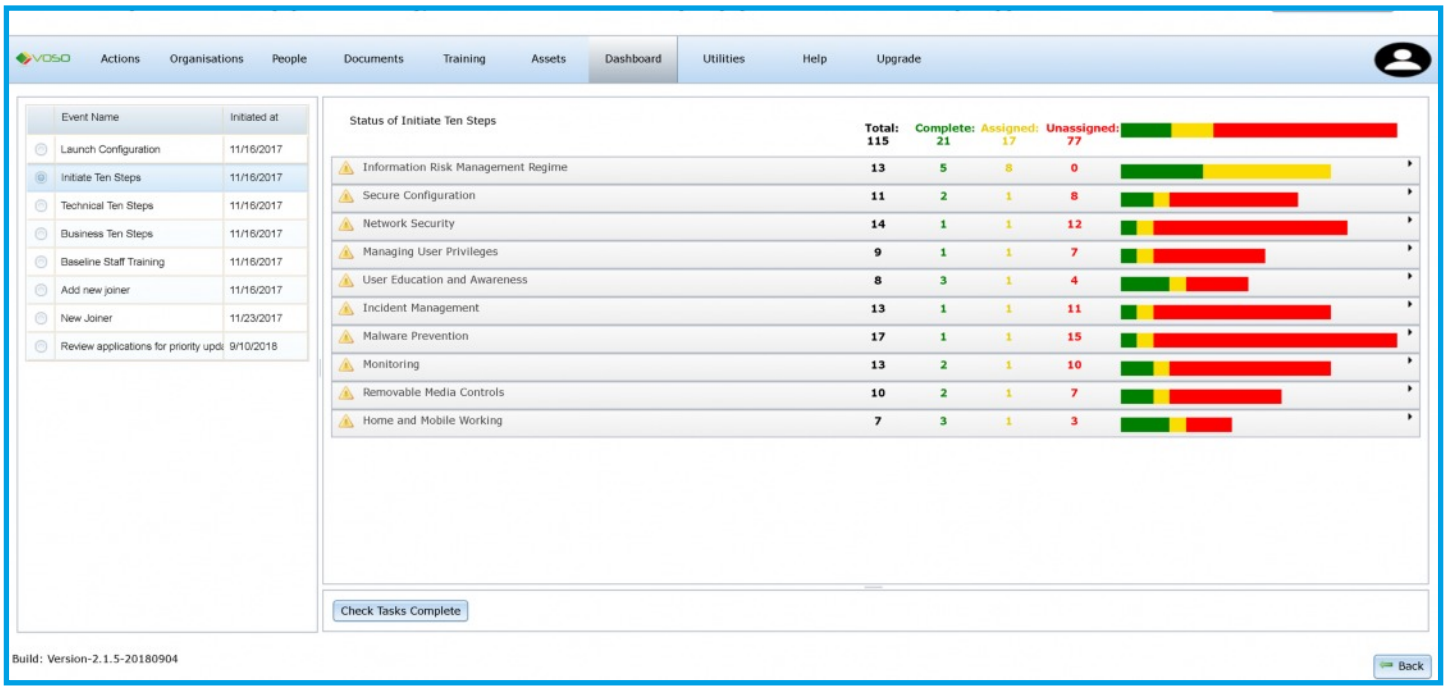
The dashboard also provides access to reports. Users can generate example compliance reports, they can generate reports showing any deviations from what the organisation claims to do and is actually doing, details of tasks being undertaken across the organisation, on KPI performance and more generally on aspects of the audit trail.

The VOSO dashboard is intended to be a single dashboard for all activity that impacts security. Many business-as-normal activities have an impact on security so VOSO has a wide range of simple examples of common business processes, such as new joiner, change of role, Leaver, goods in process to name but a few.

For SME's who do not have asset management systems, HR, CRM or ERP systems these procedures should be good enough. For those that already have other systems and want to integrate with VOSO to benefit from the single dashboard, there are facilities to import data from other systems into VOSO.

Technology Integration

All organisations need to deploy some cyber security defensive technology to implement their policies. VOSO identifies a family of basic products that will enable organisations to provide a minimum, known level of all-round defence suitable for SMEs with a lower level of risk who are cost conscious and may not have assigned a budget. Organisations can then supplement this framework with more functional products to meet additional needs.



VOSO provides integration points so that data from these systems can be propagated into VOSO to provide a single dashboard that includes risks identified through technology.
For example, organisations that use Qualys for vulnerability scanning can generate reports from Qualys and load those into VOSO and see the state of vulnerabilities on the VOSO dashboard.

Breach Management

Disasters do unfortunately happen and when they do an organisation needs to be able to recover rapidly. VOSO is a cloud-based solution so in the event of a serious incident all the information in VOSO should be available to an organisation as soon as it is able to regain the minimum level of electronic access. Thus, VOSO provides an excellent platform for holding all information necessary for managing incidents and recovering from them.

Why VOSO is a benefit not a burden!

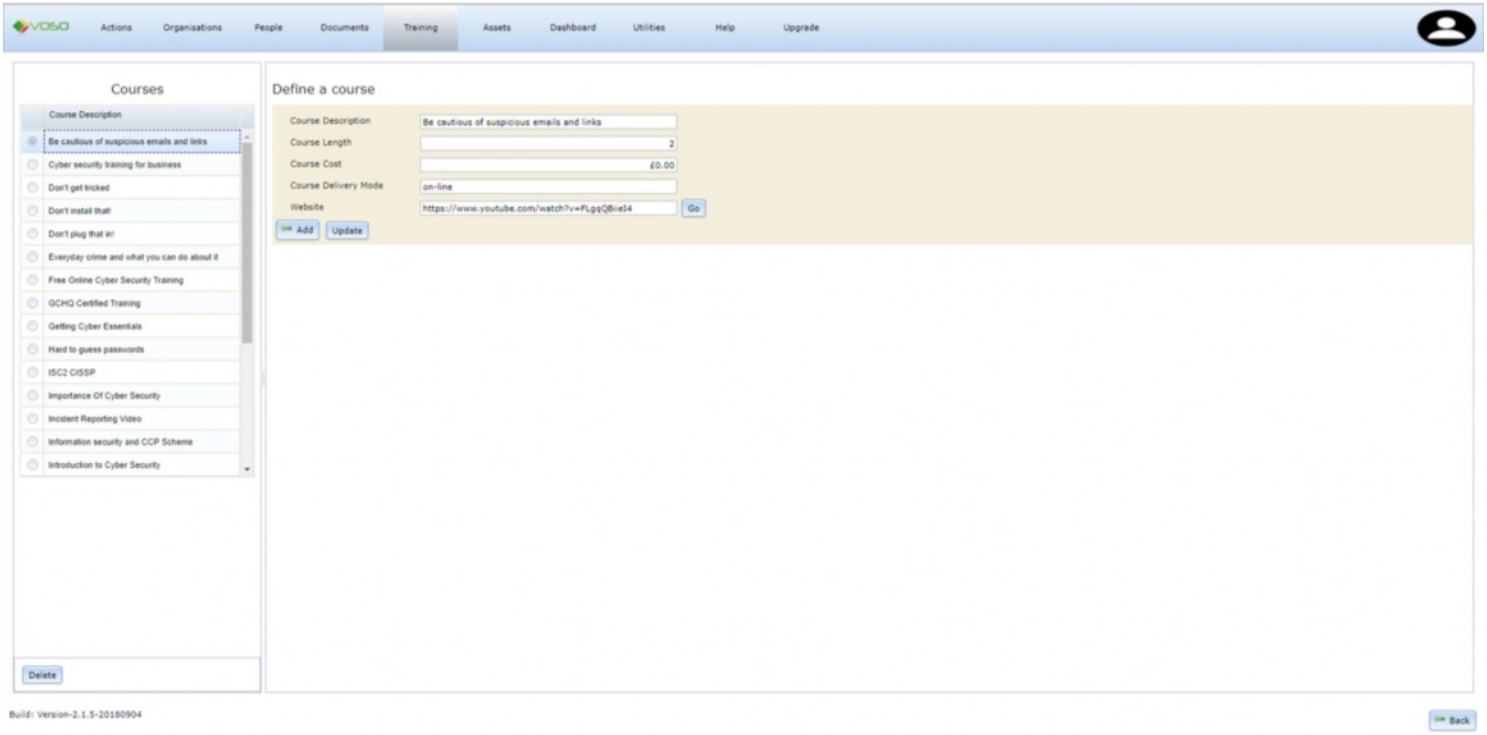
Organisations seeking to manage risk often implement compliance that burdens their staff and "silts up" their organisation with process for no apparent benefit.

Using VOSO the board consider the risks, determines the processes to adopt, task staff in plain English so clear

instructions can be undertaken by staff efficiently, regularly and consistently to ensure that the company's cyber defences are maintained.

The board can identify when the organisation is not following agreed policy, or is in danger of breaching regulation, and can take corrective action.

When a breach occurs the knowledge base and pre-planned tasks in VOSO can also be used to manage the organisation's response and recovery.



CySure provides a virtual cyber security officer that tells you what you should be doing and when, to protect your online equipment and stored data.

CySure

CySure Limited

2, Printer's Yard, 90A The Broadway,
Wimbledon, London, SW19 1RD

D : +44 (0) 20 8412 1106 | W: www.cysure.net

CYBER ESSENTIALS