Small doesn’t mean safe - 5 Steps to Cyber Security for SMEs

CySure

Virtual Online Security Officer

Manage your business safely and avoid cyber threats

With new threats appearing daily cyber security is becoming increasingly important and complex, yet many small business owners don’t have the bandwidth to take the trend seriously. Most news stories have focused on security breaches in large organisations however small businesses are especially vulnerable to security threats as they often lack the resources and expertise to implement operational and risk management policies.

Cyber criminals are preying on this lack of expertise and target small and medium sized enterprises (SMEs) as they are easy victims and can be used as a backdoor to larger companies.

The Cyber security breaches survey 2017 conducted by Ipsos Mori on behalf of the UK Government revealed that 52% of small businesses identified a cyber breach or attack in the past 12 months. The most common types of breaches identified were related to staff receiving fraudulent emails (72%), followed by viruses, spyware and malware (33%), people impersonating the organisation in emails or online (27%) and ransomware (17%). For small companies with limited budgets, cyber security can be a tricky job, however, getting “your ducks in a row” with an information security management system is a good place to start.

Here are 5 Steps to Cyber Security for SMEs.

1. Leadership is vital –

Cyber security starts at the top of the organisation, if management leads by example taking an active approach to the mitigation of cyber risk, this attitude will prevail throughout the organisation. Understandably, leaders in SMEs are focused on building their business and not inwardly looking at complex organisational policies. However, adopting a systematic approach to processes and procedures promoted by a virtual online security officer, as part of an information security management system takes away much of the time-consuming administration burden.

Even organisations that cannot afford a full time inhouse security specialist can seek the services of an online service to guide them through the complex, emerging safety procedures and protocols to improve their online security and reduce the risk of cyber threats.

2. Education and awareness training –

As revealed in the Cyber security breaches survey 2017, phishing emails and malware are the two biggest threats to organisations. Both of these exploit human behaviour so it’s vital that staff are trained to recognise the threat and respond appropriately.

Similarly, accidental breaches, privilege misuse and data loss are all the result of employees not understanding their information security obligations. Educating staff on the ways they could put data at risk helps organisations turn one of their biggest vulnerabilities (people) into an area of strength.

3. Identify your risks -

A risk assessment is one of the first tasks an organisation should complete when preparing its cyber security programme. Identifying the risks that can affect the confidentiality, integrity and availability of information is a time-consuming process. However, by identifying threats and vulnerabilities organisations can take steps to mitigate by prioritising which risks need to be addressed in which order.

4. Regular reviews -

Policies and procedures are the documents that establish an organisation's rules for handling data. Policies provide a broad outline of the organisations principles, whereas procedures detail the how, what and when things should be done. Together they provide a framework of do's and don'ts for the organisation's workforce on how data should be managed and trains employees to offset social engineering campaigns that are one of the main causes of a data breach.

A good information security management system will provide policies and procedures that ensure regular reviews are conducted with all employees to ensure they are up to date and policies remain effective. If a procedure isn't working, it needs to be rewritten.

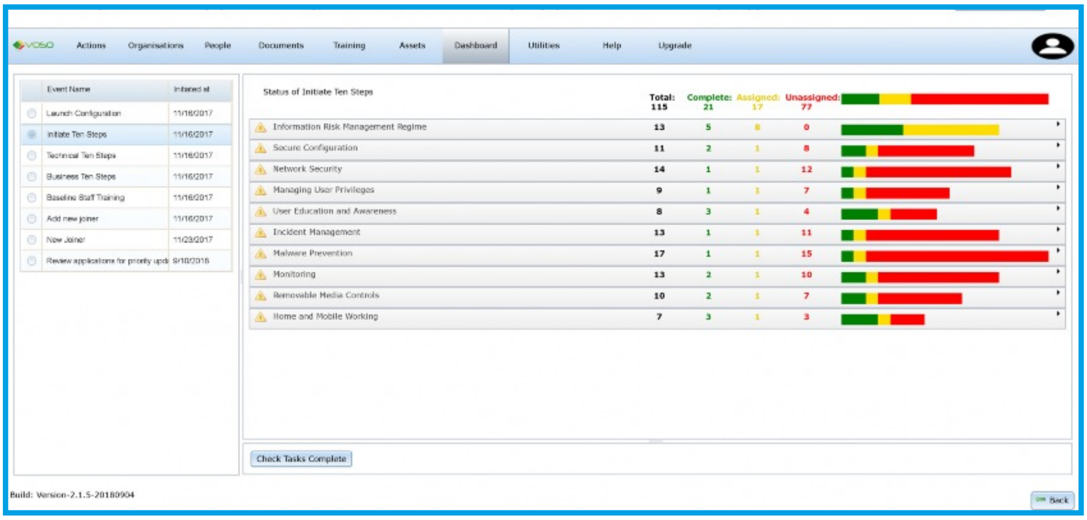
5. The wonders of a dashboard –

Assessing progress and monitoring improvements is essential to maintaining an organisation's security posture. A dashboard simplifies the process by providing a central location for all plans, policies, best practice advice and employee training information. Good dashboard software should guide companies through complex safety procedures and protocols, display compliance progress against selected standards including GDPR as well as online security training videos for continual staff training. A visual traffic light system soon lets business leaders know just how well prepared their organisation is to prevent a data breach or cyber attack.

It's time for SMEs to act

By underestimating the true impact a cyber attack can have on their reputation and the disruption caused while management remediate the situation, small businesses are putting themselves at significant commercial risk. Now more than ever it is essential for SMEs to take action and reduce the risk of cyber threats. Without adequate protection they are risking their future business growth and development.

Managing risk from inside the organisation is vital and relies upon the application of a consistent set of policies and processes, backed up by continual employee training. By utilising an information security management system that incorporates leading cyber security standards, SMEs can benefit from the expertise of online cyber security consultants at a fraction of the cost, enabling them to create robust, best-practice policies to help keep their organisations safe.



	Event Name	Initiated at
○	Launch Configuration	11/16/2017
●	Initiate Ten Steps	11/16/2017
○	Technical Ten Steps	11/16/2017
○	Business Ten Steps	11/16/2017
○	Baseline Staff Training	11/16/2017
○	Add new joiner	11/16/2017
○	New Joiner	11/23/2017
○	Review applications for priority upd	9/10/2018

Status of Initiate Ten Steps

	Total: 115	Complete: 21	Assigned: 17	Unassigned: 77
⚠ Information Risk Management Regime	13	5	8	0
⚠ Secure Configuration	11	2	1	8
⚠ Network Security	14	1	1	12
⚠ Managing User Privileges	9	1	1	7
⚠ User Education and Awareness	8	3	1	4
⚠ Incident Management	13	1	1	11
⚠ Malware Prevention	17	1	1	15
⚠ Monitoring	13	2	1	10
⚠ Removable Media Controls	10	2	1	7
⚠ Home and Mobile Working	7	3	1	3

Build: Version-2.1.5-20180904

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 Limited

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

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