PROTOCOL POLICY SYSTEMS

Socitm
Delivering digital leadership

Cyber security:

Why your people are your most effective defence.

— October 2017

Cyber security culture is a collective effort

Responsibility for protecting businesses and local authorities from cyber attacks should be a corporate responsibility in which IT, HR and others play a significant joint role, says a cyber security expert.

Martin Ferguson, Director of Policy & Research at Socitm, says many public sector organisations take a technological approach to the problem, which ironically can make them more vulnerable to attack.

"While technological solutions are an important line of defence, technology should not be the only safeguard. Cyber criminals have moved on and are increasingly taking a social engineering approach rather than exploiting technology vulnerabilities," he says.

This has resulted in a shift away from phishing type attacks, whereby cyber criminals masquerade as trustworthy entities, such as banks, to trick people into providing passwords.

Instead, criminals are moving up the organisational food chain, with so-called 'whaling' attacks.

This sophisticated type of attack, which aims to catch an organisation's 'big fish', targets C-suite members by hijacking senior executives' computers. Cyber criminals will monitor emails and quietly gather information for many months before emailing their target. Typically, this email will be a seemingly legitimate request for funds that is purportedly from a colleague or executive-level supplier, such as the company's lawyer or accountant.

Ferguson says organisations need to take a big step back when reviewing their cyber security protection and first of all ensure that they have the right accountability structures and policies in place.

"Cyber security should be a corporate responsibility to include enterprise risk personnel and human resources managers as key players, alongside IT and service managers. This is because organisations need to design 'cyber resilience' into their normal ways of working, if they are to keep themselves safe.

"It's not enough simply to email employees about the issue; businesses and local authorities need to understand cyber security awareness levels and gaps at all levels of their organisation and that's where the HR team comes into the picture."

"When designing 'cyber resilience' into normal ways of working it's good practice to establish and maintain a set of comprehensive IT securities policies that can easily be accessed and referenced by all staff. This creates an awareness level and also promotes a common and safe 'highway code' of operation for users, reducing the human factors that can lead to cyber security breaches."

Developing a cyber security culture will involve ongoing education, communication, assessment and evaluation, so as to continuously raise all employees' awareness, improve skills, close gaps and ensure accountabilities.

Ferguson says everyone from members of the board and management teams, through to frontline employees should be engaged and contribute to protecting the organisation from attack.

"Achieving this requires specialist skills and insight into the human factors side of the equation.

That is why it is vital to engage the HR team in helping to develop a strong cyber security culture and reinforcing that everyone in an organisation has a role to play.

Cyber criminals succeed when it's easy to identify and exploit the weakest links within the organisation," he says. "It presents HR professionals with a valuable opportunity to lead the way in working with all levels of the organisation to identify and address vulnerabilities at all levels."

Six ways to develop a cyber security culture

Local authorities and other public sector organisations can protect themselves in the following ways:

1. **Involve all parts of the organisation** in developing and regularly reviewing cyber security policies. Policies help define the expectations you have of everyone that works with your organisation's IT systems and data – "everyone" is defined as users, the board, managers and IT people. For example: What is an acceptable use of systems? What are the expectations for employees who need to connect to internal systems remotely? How should technical staff administer technical controls such as a firewall?

2. I**nvolve employees** in reviewing the processes and procedures they follow so as to increase their engagement and vigilance, and build security in day-to-day operations. This review will help increase the understanding of what vulnerabilities exist in the current environment. The pace of technological adoption is increasing so, when new business initiatives are launched with different technology, ensure that security is a key consideration in the design phase. Building cyber security in from the outset will enable the organisation to become more robust and be able to adopt technology with more confidence.

3. **Change the organisation's mind-set** from regarding cyber security as an overhead, to seeing it as a business enabler. The cultural, process, procedure and engagement required for good cyber security practice are also good for business as a whole.

4. **Implement the organisation's cyber security policies and procedures** (they are no use just sitting in a folder!) and align organisational accountabilities to ensure this happens. Improving or changing cyber security culture requires ongoing work to ensure the policies and procedural information are understood and complied with.

   A good starting point is to make the information available on the intranet. Also, undertake simple testing to validate team members' comprehension of the material. Some companies provide phishing and whaling attack simulation services that can send out fake test emails and measure how many people take the bait.

5. **Look beyond what your own organisation is doing** to protect itself and also take all aspects of the supply chain into account so as to ensure your supply partners also have adequate protection against attack.

   If the organisation contracts or outsources business functions or part of its supply chain, then be sure to assess the sensitivity and value of the company information that is provided to these third parties. They should handle and store that information securely and ensure it is deleted when no longer required.

6. **Don't just communicate to employees** – communicate with them. Be sure to check their understanding when advising them of steps they can take to protect the company against attack. Engaging employees to discuss threats and options to minimise them very likely will see them provide some useful insights and ideas.

For additional cyber security information for Director or C-Level and Manager roles please see the Socitm Cyber Guide at *https://cyberguide.socitm.net*

Further information on IT security policy management is available from Protocol Policy Systems, a joint venture with Socitm, at:

web: *www.protocolpolicy.com*
email: *sue.lal@protocolpolicy.com*

PROTOCOL POLICY SYSTEMS

Socitm Delivering digital leadership