You've been hacked!

Ken Witt explains the growing role of the management accountant when it comes to protecting against cyber attacks

The recent global WannaCry and Petya cyber attacks were a wake-up call for many organisations. The extent of Petya is not known yet, but according to reports there were around 2,000 attacks on a single day, crippling businesses and government agencies around the world. WannaCry is estimated to have affected more than 200,000 computers and, with the NHS being one of the victims in the UK, it meant that even operations had to be cancelled.

Cyber threats can have severe consequences: lost business, fines, lawsuit costs and settlements, and reputational damage, among other things. There are predictions that the financial loss from WannaCry could be hundreds of millions of pounds.

Who's in control?

According to a 2017 Deloitte report, only 5% of FTSE 100 boards appear to have a director with specific cybersecurity expertise – a clear cybersecurity weak spot. Management accountants and finance professionals can play a big role in helping organisations identify and mitigate cyber security risks. Chief financial officers work at the heart of an organisation, and usually have ownership of risk management, asset protection and control, and business continuity. All of this is affected by cybersecurity, so it's only logical that finance professionals take care of this area as well. Risk management is also a core competency of management accountants, making them the ideal partner to help organisations develop their cybersecurity strategies.

You cannot protect your company without knowing what the threats are. To help management accountants understand security risks, approaches and responses to cyber threats, the AICPA has introduced the CGMA cybersecurity tool. This new resource provides a practical guide to combatting cybersecurity intrusions to help ensure the success of organisations.

Understanding cybersecurity

To win the war you need to know who your enemy is – and what weapons they use. While you've got your 'basic' cyber criminals, cyber attacks can also be carried out by business competitors, insiders such as former employees or even other countries. Cyber criminals often use malicious software – malware – to steal data and money or cause denial of service. The most common malware types are:

- Ransomware used for denial-of-access attacks, which lock computer systems until a ransom is paid.
- Botnets, a network of infected computers controlled by the attacker.
- Malvertising, where online advertisements are used to spread malwarePhishing, usually in the form of an e-mail made to look like it comes from a trustworthy or legitimate source. By clicking on a link in the mail or by opening an attachment, the user installs malware on their computer.

Another threat is application attacks via phone apps or home devices connected to the internet.

What makes your systems vulnerable?

Weaknesses can be traced back to technical, procedural or human flaws. Among technical problems are software defects or not using adequate security protections. Procedural vulnerabilities can be caused by system configuration mistakes or if staff ignore software security updates. Nevertheless, many problems and vulnerabilities are caused by users themselves, for example, by using weak passwords or clicking on links or attachments from unknown parties.

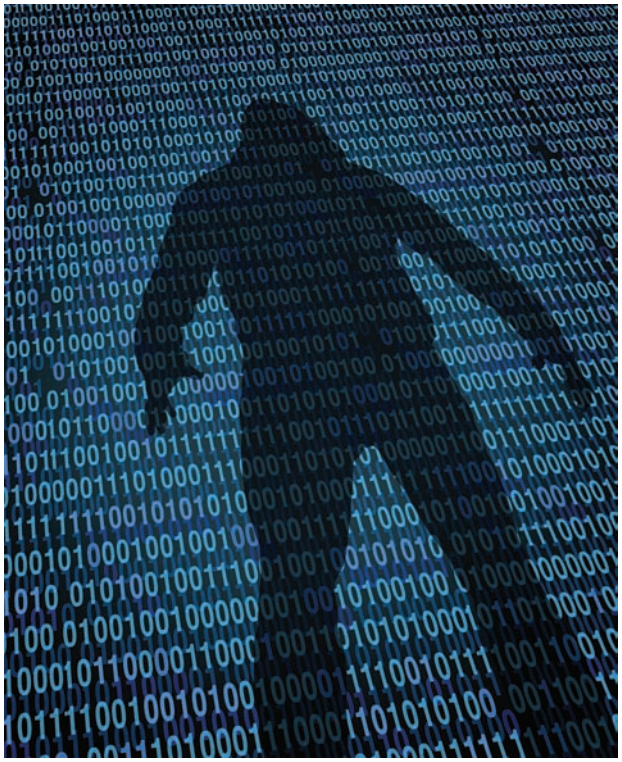
Cybersecurity objectives

Organisations should define their key cybersecurity objectives. Key objectives include:

- Enabling continuous access to and use of information and systems.
- Protecting information from unauthorised access and disclosure.
- Guiding against data modification or destruction.
- Guarding against the improper use, modification or destruction of systems.

To achieve these objectives, businesses need to implement security mechanisms to protect information assets, detect malicious activity and be able to respond effectively when these attacks happen. These measures could include:

- Requiring identification, such as usernames, to make sure that there is accountability.
- Authenticating this identification via passwords, fingerprints, etc.
- Only allowing particular types of access or transaction for users with verified level of authority.



- Protecting sensitive data such as credit card information, for example, through encryption.

Responding to cyber breaches

Centralisation is an important element of cybersecurity, especially for big firms with large numbers of computers, laptops and mobile devices. The ability to manage software updates or security protocols through a centralised management ensures better control. Centralised management is also an option for mobile devices as third-party mobile device management (MDM) products are now available. For laptops, whole disk encryption is vital as it prevents unauthorised access in case laptops are stolen or lost.

Further security features are network configuration and firewalls; application firewalls; and antivirus and endpoint products.

What can you do?

Finance professionals have a responsibility to understand and mitigate the business risks associated with a cybersecurity attack. Our CGMA cybersecurity tool will help you guide your organisation to develop an organisation-wide approach to protecting against cyber attacks, ensuring the continued success of organisations.

The CGMA cybersecurity tool can be downloaded – go to www.cgma.org/resources/tools/cgma-cybersecurity-tool.html PQ

• Ken Witt, Technical Manager – Management Accounting, Association of International Certified Professional Accountants