ITIC SPECIALIST PROFESSIONAL INDEMNITY INSURANCE

2020 edition

Cyber security wire

Cyber security introduction

Cybercrime unfortunately continues to be a hot topic, with businesses and individuals at risk of becoming potential targets of digital fraud. Any business or individual using electronic communication can be the subject of an attack by hackers. ITIC has issued a number of circulars to warn members and to ensure that they implement robust systems and controls to ensure that they minimise any exposure. However, we are still seeing this type of fraud being regularly committed, particularly where communications are intercepted and bank details changed, whilst the original sender remains unaware.

The result leaves you exposed to a liability as a result of somebody else's dishonesty. Acts of fraud can be varied, and ITIC's experience has shown that fraudsters will often seek to make themselves respectable by associating their actions with reputable companies.

In this special edition of The Wire ITIC outlines some practical tips and checks that you can implement, to ensure that your IT systems and processes are as robust as possible. These suggestions are being shared purely to raise awareness and are not intended to constitute professional IT advice. ITIC is not able to comment on IT security products, individual systems, cyber risk self-assessments or any other element of cyber security. If you require further information, ITIC recommends that you contact an IT professional or cyber risk specialist.

ITIC
IS MANAGED
BY **THOMAS
MILLER**

Social engineering / bank mandate fraud

Bank mandate fraud is when a third party tricks you into sending a payment to a bogus account by impersonating the genuine organisation or individual. This is also known as "social engineering" and "payment diversion fraud".

Sometimes these e-mail scams appear to be an internal request to make a payment; this is known as CEO fraud. In these cases a spoof e-mail is sent from a fraudster, purporting to be the CEO or a company director, to a member of the finance team insisting that an urgent payment transfer is needed for some reason. The member of staff, believing that the message is genuine, does as instructed only to discover later that they have sent funds to a fraudster.

ANY e-mail received from a third party regarding a change to bank details – or setting up new bank details if it is new supplier/payee etc. should be treated with suspicion and checks should be made to ensure that the request is genuine. Fraudulent e-mail addresses are often very similar to the genuine address (perhaps a letter missing or a different top level domain name (i.e. ".com" instead of ".com.sg") making such spoof e-mails hard to spot. ITIC advises that you use the telephone to call the supplier/client and check that they really have changed their bank account. Never seek confirmation of this change to bank account information via e-mail, or by using the phone number provided in the e-mail, as you may end up corresponding with the fraudster.

ITIC have heard of mandate frauds involving cash to master movements, freight payments, supplier invoices and even payment of their insurance premium. Ensure that all staff, not just the finance team, are aware of these types of e-mail fraud.

Internet security – the basics

Antivirus software… Use it and keep it up to date! Use a firewall – Windows has a firewall built in and most antivirus packages also include one.

Keep your system up to date - Not just anti-virus and firewall software, but the system in general. Developers regularly issue updates/patches/fixes. These updates could be released because the developer has discovered a security weakness in their product and should not be ignored. If you are prompted to download an update then you should!

Staff education

Make sure that ALL of your staff are aware of the dangers of clicking links and/ or opening attachments from senders that are not known to them. It could be an attempt to install malware onto your computer network. The malware may be recording keystrokes so that the hacker can learn usernames and passwords for systems, or it may contain ransomware or other nasty payload.

Consider running a phishing simulator within your organisation – this is a method of testing staff security awareness. The simulator sends an e-mail similar to a malicious one with either an e-mail attachment, a link to a website or request for personal credentials and reports the results of how the staff responded to the e-mail. If the results contain a high number of fails (i.e. opened the attachment/ followed the link or provided their credentials) then additional staff training is clearly necessary.

Passwords

Make sure staff do not leave their usernames and passwords on post-it notes on the side of their screen (or in the back page of their notebook!).

If your staff use portable devices (laptops, tablet and phones) which have access to either your work system or e-mail then make sure that they have the password or pin code lock on that device enabled.

Don't use the same password for everything. Try to use complicated passwords such as the name of your favourite film or lyrics from a song. Passwords should be something easy for you to remember but hard for a hacker to guess. Brute force password crackers are readily available on the internet…it doesn't take a mathematician to work out that a computer program could try every single combination of an 8 letter password quicker than it would to crack a 20+ character phrase based password that contains numbers, capitals and special characters.

Consider using a password manager. This is a secure app that stores your credentials and can sync them across multiple devices.

NEVER use "password" as a password. Don't tell anyone else your password.

Simple housekeeping

Regularly check your spam/ junk folder AND deleted files folder on your e-mail system. This is a good habit to get into, not only to check to see if your e-mail system has mistakenly marked a message from a client as spam, but also to make sure that a hacker has not set up an auto spam/ delete function. This happens when a hacker is impersonating your e-mail address in order to defraud another party (as mentioned above) and deleting/ spamming any message from the true third party who is asking to be paid.

Cyber risk assessment

There are cyber security firms who can provide you with a cyber risk assessment. They can look for vulnerabilities in your system through physical attacks, i.e. can a stranger walk in off the street and get into the office as well as penetration tests…these can be internal or external.

An internal attack could be if someone was in the building, say in a meeting room, could they simply plug their laptop into the network and gain unauthorised access to your system?

External testing would be where attempts are made to access your network from outside the physical building. This could be through a weak security measure on the company website or through the online service/ cloud server that employees normally use when working remotely to allow genuine access to their office systems.

An alternative to employing the services of a cyber consultant would be to conduct your own cyber risk assessment. There are some tools available online that allow you to run some of your own vulnerability tests.

If you do look to carry out your own cyber risk assessment obviously make sure that the product being offered online is itself genuine…**after all you do not want to be assisting a cyber criminal by effectively installing their malware on your network thinking that you are installing a free penetration test tool!**

ITIC
IS MANAGED
BY **THOMAS**
MILLER

For further information on any of the products, services or cover provided by ITIC contact Charlotte Kirk at:
International Transport Intermediaries Club Ltd, 90 Fenchurch Street, London EC3M 4ST.
tel + 44 (0)20 7338 0150 e-mail ITIC@thomasmiller.com web www.itic-insure.com