Risk Management: Tackling Fraud & the Impact on your Business

Introduction

There are many forms of attacks that take place under the heading of cybercrime and we urge all firms to be vigilant.

Firms holding client information and funds are vulnerable to the risk of theft of confidential data, which could lead to the targeting of client money held in client accounts. Irrespective of your size, your firm can be targeted and the effect on the scammed firm and its clients can be extremely serious. Only through remaining vigilant and taking swift action following a successful attack, can you avoid catastrophe.

Types of fraud

These can include the following:

- Impersonating clients or known contacts e.g. bank fraud team.
- Requests to change sort code and account number.
- Other systems that are compromised e.g. clients.
- Spearfishing and hacking.
- Bailiff scam: impersonation and ‘court number’ to call on court papers.
- Bogus Law firms: cloning websites, firm letterheads, emails.
- Impersonating lawyers, such as using closed genuine firms.
- Mortgage fraud.
- Investment fraud: too good to be true

However, criminals use a variety of ever-changing and increasingly sophisticated means to obtain confidential financial information and data. Also, some may be targeted at particular areas of law.

In the majority of cases, the best defence against them is the ability of the staff dealing

with the matter to question what is being put in front of them. All staff should keep their knowledge current by regularly following guidance issued by CILEx Regulation, their insurers, and the government. It's also a good idea to sign up to alerts from Action Fraud at the National Fraud Intelligence Bureau.

VOICE PHISHING (VISHING)

One such technique used to gain information for malicious purposes is vishing and the issues that this raises is relevant to a large number of the frauds listed above. Fraudsters, who ring people to try and trick them into disclosing information, are carrying out 'vishing'. Those fraudsters who use email to trick people into providing confidential information are 'phishing'.

If someone makes contact purporting to be a bank, building society, or the police, for example, **stop and think**:

- Is the information being asked for sensible;
- Is there a sense of unnecessary urgency;
- Are you being asked to move quickly; and
- Does it feel right?

These are all red warning signs and care is needed. Do not assume a call (or email) is genuine despite how it appears. Fraudsters often clone the telephone number of the firm they want to impersonate (and the appearance of an email) to make it appear that they are the firm.

A bank or lender is not going to ask you to move money to prevent fraud. They have their own actions to protect their clients' funds, so this should put you on alert.

If the call (or email) is unexpected and unusual requests are made, contact the bank/building society using an independently verified telephone number and from another phone other than the one the call has been received on. Fraudsters can stay on the line and make it appear that the call has been disconnected but when you make an outgoing call thinking you're calling the firm, the fraudster may still be on the line.

If you are unsure who you are talking to you should not continue with the call.

PROTECTING YOURSELF AND YOUR CLIENTS FROM AN ATTACK

Useful starting points for protecting your business from cybercrime are the government's Cyber Security Guidance and Cyber Essentials Scheme. That presents requirements for mitigating the most common Internet-based threats to cyber security under the five key areas of:

- boundary firewalls and Internet gateways
- secure configuration
- access control
- malware protection
- patch management.

Using the controls recommended will assist in defending against the most common forms of cyberattack. However, no system is invulnerable to all types of crime and you should regularly review all preventative measures to ensure that they reflect current best practice, are applied consistently across the firm, and are effective.

What to do if you are a victim of an attack

It is essential that in the immediate aftermath of the incident you do everything that you can to contain the situation as quickly as possible, limit the damage and maximise the chances of rectifying it.

If you find or suspect that your firm has been the victim of a scam you should, as soon as possible:

- Inform your bank.
- Inform the police at Action Fraud on 0300 123 2040.
- Inform your professional indemnity insurer.
- Inform CILEx Regulation by telephone on 01234 845770.

Swift actions could help safeguard your clients' money and data, and also your firm's reputation and viability. As your regulator we will do everything we can to assist you should the worst happen but as ever, prevention is better than cure.

There are a number of organisations that provide support and guidance on how to prevent fraud. Some of these are listed on our Risk Management: Resources and Links information sheet.

Business continuity management

You should ensure that you have effective business continuity management so that you can continue to handle your clients' business if something goes wrong.

If say, a potentially catastrophic incident occurred which would take three to six months or more to resolve, would you know how to cope?

Research has shown that many people just view business continuity management as what to do when your IT systems don't work. Emergencies can vary widely but they all cause disruption to a business. Strangely loss of key people does not tend to rank that high in people's perceptions.

However, some incidents are fairly common and can be mitigated by sensible continuity planning.

What is business continuity management?

What it should be is a process that identifies the possible threats and impacts to your entity and considers how you can make an effective response if they happen.

Its objective is to protect:

- stakeholders
- reputation
- brand
- value-creating activities.

What should you do?

The following are the types of actions and processes that you should carry out:

- Ensure someone with sufficient seniority within your entity has responsibility for business continuity.
- Conduct a risk assessment to identify those risks that require improvement and then put the necessary actions in place.
- Produce a written business continuity plan fully supported by necessary recovery provisions appropriate to the size of your firm.
- Ensure that you maintain and test your plan regularly.
- Ensure everyone is aware of the plan.

CILEx Regulation Limited
Endeavour House, Wrest Park, Silsoe, Bedford
MK45 4HS Tel +44 (0)1234 845770
E info@cilexregulation.org.uk www.cilexregulation.org.uk | @CILExRegulation