THE FINANCIAL SERVICES GROUP OF LIVERY COMPANIES

GUIDANCE NOTE

INFORMATION ASSURANCE GUIDELINES

Introduction

The following is a simple statement of basic principles on Information Assurance.

If more detailed guidance is required it is recommended that professional advice be sought.

Why "Information Assurance"

It is NOT "Cyber-Crime" as such that we should be worried about. It is about protecting the Information that is owned or controlled, as Information is an organisation's and individual's most important asset, second to none. Not even an organisation's most important staff rate are more important than its Information.

Without our Information, we are nothing. In the past, we had guards, gates, secure areas, safes, locked filing-cabinets and plenty of staff to enforce the rules about "documentation" owned or controlled.

Today, we have the equivalent of the M25 running straight into (and, more importantly, out of) all of our most important "documentation" – it is called the Internet. We also have many persons whose life's ambition is to "break" computer systems – sitting somewhere in the world without knowing or caring about most of their targets; they are known as "Hackers". Plus the so-called "Hacktivists", PLUS the viruses, worms, Trojans are all the other ways of compromising Information.

The most common problem area in addressing Information Assurance? **"Human Error"!** Caused almost without exception by a lack of training and a lack of awareness of the issues. by senior management.

For an organisation the responsibility is that of senior management and not to take action is to abrogate responsibilities for the future. We all have to manage our Risks and that means we must understand enough about them.

The message is **"we have to compromise"**. We have to use our data, to access it whenever and wherever we need it, and in so doing we take risks. To understand those risks and to mitigate them by taking basic precautions is a measure of "insurance". We are – all of us – targets in one way or another.

Viruses and worms do not differentiate. Hackers frequently decide their targets on the spur of the moment – and Hacktivists are known to have attacked the wrong target with disastrous consequences.

The Basics Principles to remember

Three words with the mnemonic **CIA**: Confidentiality; Integrity; Availability.

Confidentiality:

Only available to those who should have access;
Having different levels of access authentication depending on sensitivity;
Failsafe is "access denied"!

Integrity:

Information always reliable;
Total change-control in operation both to prevent unauthorised changes and to ensure that no changes are missed;
Failsafe is "don't use any information until verification confirmed"!

Availability:

Always there when you need it;
OR Always there within agreed times/access rights/authentication;
Failsafe is "open to all"!

What might they mean? - Reputational Damage

a. Internal or external persons gaining unauthorised and sensitive data and using it against you

b. Internal or external persons altering data (either by mistake or deliberately) leading to future decisions being taken based on false data or lack of data

c. Internal or external persons causing denial of access to your own Information (temporarily or even permanently if you do not have proper back-up) leading to huge embarrassment (at best)

d. Internal or external persons seeing or receiving inappropriate items on or from your systems (e.g. pornography) and thus rendering you liable for damages – very embarrassing to a Livery Company

e. Internal (or, more likely, external) persons breaking into your database and populating it with a "worm". This will self-propagate and send itself to every address that your system holds, "from you".

Who are the "Enemy"?

Internal non-hostile. Such as simple mistakes due to lack of training or poor systems control (no automatic back-up coupled with the ability to delete at will) or even someone bringing in an infected game software, or pornography, "for fun".

Internal hostile. An employee or anyone with access (especially an ex-employee) who has a score to settle or a grievance (real or imaginary does not matter).

External non-hostile. A mistake – not intended for you – but the result is the same as "friendly fire".

External hostile, random. Hackers, Viruses, Worms – not "aimed" but still lethal.

External hostile, deliberate. Extremely dangerous – an expert targeting your Information for whatever reason, whether to shut you down, expose your "faults", extort money, attack your Membership, etc.

Example: a new employee was given full access rights on day one. Less than two weeks later, she was fired due to her lack of attendance. It took six MONTHS for the IT department to be told of her leaving by the HR department (thus removing her access rights) by which time she had taken her "revenge" in a big way!

Example: a "Trojan" placed pornographic material on a number of computers owned by entirely innocent organisations that were then accessed by the "user community". When an employee discovered – by accident – what was on their organisation's computer system there were several claims made for sexual harassment and these were upheld as there had been a lack of duty of care.

So what can/should be done ?

Implement a number of simple basic Risk Management processes and approaches – to protect your Information such that you will not be as easy a target.

1. Access

Every authorised individual must have a strong password that they have to use before they can log-on. This authorisation must include the level of access permitted – a "temp" should not be given the same level as your Clerk, especially on their first day! Access rights must be removed immediately someone leaves or before that if they are about to be dismissed.

WARNING: the majority of passwords are the word "password"! Every password needs to be at least 8 characters including letters and numbers, upper and lower case and preferably one or more symbols. **WARNING:** the majority of passwords are either written on a post-it note or stuck underneath the keyboard. **WARNING:** people often give out their passwords without thinking, **AND** do not change them (should happen at least every 3 months). Simple rules must be issued, and repeated regularly, to prevent these "obvious" basic mistakes.

2. Back-up

An automatic back-up system – preferably one utilising the Cloud – must always be in place.

WARNING: ensure that everything is included, especially e-mails (frequently they are missed). **WARNING:** regularly check that the back-up system is working and that all data can be re-instated from it – there is no point in having a back-up if it cannot be read. **WARNING:** do not have the back-up in the same office as the computer. What happens if a thief gets in and steals the IT equipment? What happens if there is a fire or a flood or the ceiling falls in – or you are very unlucky and a terrorist attack destroys the building? Back-ups must be "distant" and preferably duplicated in different geographic locations.

3. Firewalls, Anti-Virus Software and Software Updates

They must all be in place, they must be updated constantly and they must be understood!

WARNING: Viruses propagate at the speed of light – from the first report in (say) Australia to the virus arriving in the UK could be measured in seconds. This is why you need to have a general defence in place – a firewall – plus training for all persons using your systems. As soon as the Anti-Virus suppliers spot the new Virus they work to disarm or destroy it – so you must enable the Anti-Virus software to update automatically and check that this is happening. The same applies to the software manufacturers – they are all playing a war-game with the Hackers, who when they identify a "vulnerability" create a nasty programme ("Malware") to exploit it. The manufacturers then identify a "patch" which they will issue to prevent the exploitation – and you had better allow the installation of all such updates automatically.

All "authorised users" must have basic training on all these items – otherwise through ignorance rather than hostility they will make serious mistakes.

4. Use of Laptops and other Devices

Nothing, but nothing, should be allowed to be brought in and connected "inside the firewall". If your staff/other authorised users use such devices at home or for surfing the Net then they are at risk of being contaminated by Viruses, Worms or Trojans. Simple rule – do not allow anything to be connected other than your own, tested, devices and never allow them to be connected to the Internet in any other way.

WARNING: the same applies to a CD-ROM or any other container of electronic data – ensure that they are always screened by your anti-virus software before they are "run". They could be infected by all sorts of "Malware" – but equally they might have pornography or similarly embarrassing data, which you would not want on your system. The rule is – check beforehand.

Example: the head of IT of a very well-known public organisation allowed a family member to use his laptop to play games at home. Despite his "rule" that nothing should be downloaded, the family member went on to a pirate software games site and got hold of unofficial copies – with viruses attached as a non-optional extra. The IT head then used his laptop – breaking his own rules about the firewall protection – and his organisation was without full communications for 6 days.

5. Training, training, training

Every authorised user – and everyone responsible for providing that authorisation whether or not they are themselves a user – must know the basics. Proper training is a necessity – and it needs to be repeated at least annually because most people get careless over time or at least benefit from a timely reminder.

WARNING. Never, NEVER give passwords or any other secure information to someone over the telephone – you have no way to know who they really are. This is known as "Phishing" and is proliferating at a frighteningly fast rate.

Finally, someone has to be responsible for creating the Information Assurance Rules for your organisation – and someone else needs to audit them regularly to ensure that they are being followed. Otherwise, the Rules are just a waste of time.

November 2015