Identity Theft

- by Dr John Russell BSc, MSc, PhD, CEng, MIET

Identity theft occurs when someone steals and misuses an individual's personal data such as their name, address or passport number. Whilst this theft of identity is, by itself, not a crime under UK law, misusing the identity information to fraudulently obtain goods or services is. Identity theft has most commonly arisen from physical attacks such as burglary or pick-pocketing where identifying information is stolen from credit cards, passports or driving licences. More recently, though, identity theft has enveloped the online world as a result of:

- Increasing numbers of consumers surfing or shopping on-line
- More online sources of personal information often derived from the Electoral Register
- Increased use of credit and information exchanged with banks and retailers.

This white paper is primarily aimed at corporate audiences and examines identity theft in relation to the risks associated with eCommerce and the Internet. It also covers issues relating to personal identity theft and will, therefore, be of interest to individuals themselves as well as organisations that offer online services to such individuals. Impact to individuals and businesses Identity theft has become the fastest growing type of fraud in the UK and already costs Britain over £1.3bn a year. For individuals, the main impact of identity theft is likely to be unauthorised use of one or more of their existing credit card accounts. Such crimes can normally be detected by the identity owner within a matter of weeks following receipt of their next statement – assuming that the individual regularly checks it. However, in the event that the stolen identity information is used to create a new account, it may not be possible for the identity owner to detect any offence for some time. In many such cases, account statements will have been redirected to an address selected by the thief. The owner will only become aware of the activity when either the credit card company debtors or bailiffs contact them to settle the debt-ridden account – or when legitimate future credit applications made by person fail. Whilst credit card customers are generally only liable for the first £50 of unauthorised transactions, the harm to person's credit reputation, their inability to carry out domestic business – as well as efforts to put things right – can be far more damaging and long lasting to the individual. The cost of identity theft – in terms of paying for fraudulently obtained goods – is most likely to be claimed against the relevant retailers by the credit card issuer. Indirect costs to business include reduced levels of sales through eCommerce channels due to continuing concerns over security and privacy of the Internet and, when news about identity thefts are published, any named company may have its reputation damaged as a result.

In the UK, the Home Office reported identity theft statistics that included over 3000 driving tests which were terminated due to concern over the identity of candidates, 1500 fraudulent passport applications, and over 500 cases of identity fraud identified by the Benefits Agency.

In more extreme cases of identity theft, such as identity cloning, the importer uses the victim's information to establish a new life. Examples include illegal immigrants,

criminals avoiding warrants, people hiding from abusive situations or other instances where becoming a 'new individual' would be advantageous to them.
Corporate identity theft allows criminals to order goods or obtain services from suppliers on company accounts or to conduct industrial sabotage. For the company that becomes the target of this activity, there would be an impact of direct financial losses of misappropriated services or goods, possible fines resulting from breach of regulatory rules and, significantly, loss of actual and potential customers resulting from harm to the company's reputation. Company directors have a duty to exercise control and, in the event they breach their responsibilities, they may be liable for disqualification from being a director. In the case of stolen corporate identity being used to obtain confidential company information, there could be a loss of competitive or marketing advantage, loss of staff morale and also public confidence. It's important to note that 'insiders' carry out the majority of identity theft and fraud involving companies.

Threats and vulnerabilities

There are a number of threats and vulnerabilities to systems that have given rise to the increase in significance of identity theft. Internal attacks on systems
The storage of large numbers of individual's personal records on eCommerce sites presents a clear risk to the identity of the customers or subscribers involved. Credit card details – including expiry dates which can allow 'card not present' purchases to be undertaken – as well as passwords and other personal identifying information offer the identity thief a variety of opportunities for misuse.

Earlier this year, bulk disclosure of personal information from the computer system of a North American insurance company followed the theft of a computer disk drive. The drive went missing from the organisation's secure computing facility, and was recovered but the data it contained has been overwritten. Police believe an employee of the company stole the drive for personal use. One of the largest known and published incidents of identity theft involved an employee of a US company that supplied banks with credit reports from many of the large credit agencies. He used confidential computer passwords and subscriber codes to access and download the credit reports of over 30,000 consumers during a three year period. The employee provided the stolen codes to external co-conspirators who were willing to pay up to $60 per credit report.

Increased use of mobile devices

Many millions of people now rely on PDAs for electronic scheduling and address books as well as storing passwords and codes for their online banking accounts. However, very few individuals carry sufficient security protection to prevent identity theft if the hand held device is lost or stolen – and such loss is commonplace. Of the users who store their bank account details on a PDA, it has been estimated that around two thirds do not encrypt this information, with just under a quarter failing even to implement password protection. Further revealing statistics indicate that around 6 per cent of users have lost PDAs in the past, but 32 per cent of those still continue to use them without a password.

Online scams

There have been a great many reported cases where individuals have been enticed, by email, into disclosing sensitive information such as passwords by using clever social engineering trickery. The substantial torrent of spam now produced worldwide has included a number of such scams. In a recent case, a teenager was charged with using spam emails and a fake web page from a well-known ISP to trick people into divulging credit card information. The emails told recipients they needed to update their ISP billing information and instructed them to click on a hyperlink connected to a billing centre. In fact, the link diverted people to a fake web site - similar in appearance to the legitimate one - containing the company's logo and links to real ISP web pages. The targets of the scam were instructed to enter their credit card numbers, along with mothers' maiden names, billing addresses, social security numbers, personal identification numbers and ISP logon names and passwords. The information that was derived was subsequently used to steal thousands of dollars.

Poor password management

A username and password required to access a free website, such as an online news site, is of limited immediate value in itself. But many users tend to re-use passwords, and those same credentials may be valid for giving access to confidential, web-based email and providing access to information at electronic banking and other eCommerce sites. There's even a good chance that the password is identical to the user's corporate network login. So, identity information obtained from one source may provide a much bigger impact to its owner when used in different circumstances.

Loss of privacy online

Individuals who register or subscribe to services from web sites, or who run file or plug-in downloads run the risk of giving away more personal information than they realise - and to parties that they are not even aware of. Any activity in which identity information is shared or made available to others creates an opportunity for identity theft. The majority of these risks relate to loss of privacy - revealing interests and purchasing trends for the benefit of marketing organisations. In some cases, however, theft of identity can result when information submitted to a web site run by an unscrupulous organisation is passed on to a dishonest third party. Web mechanisms including cookies, adware and web bugs may all be misused to achieve this loss of privacy, and ultimately identity theft. For more information on this subject, see Insight's white paper entitled Spyware – The Risks Facing Businesses.

Confidential documentation theft Dumpster diving – involving the searching of waste for confidential information that has been discarded – has been identified in a recent survey to be a major source of identity theft. The survey, which interviewed local councils in the UK, revealed a significant number of incidents involving the practice and which specifically targets individuals at home where the use of paper shredders, for example, is still relatively uncommon and where awareness of the associated risk is similarly low. The survey also identified many cases of information that could be used to instigate identity theft such as utility bills, bank statements and blank cheques together with household documentation that included samples of

individual's signatures.

Corporate security measures

A number of regulatory requirements that affect organisations now encompass risks such as corporate identity theft. The guidance contained in the Turnbull Report, for instance, states that a board of directors is responsible for a company's system of internal controls, and that they consider the nature, extent and likelihood of the risks faced by their company. It also requires that a company's annual report includes a statement on the effectiveness of internal controls and non-compliance with the Turnbull code.
Whilst this guidance is mandatory for companies listed on the London Stock Exchange, it does also provide sound business advice for smaller organisations as well.

Some of the controls that specifically address corporate identity theft and the risks described above include:

- Recruitment security checks on new staff
- A clear desk policy and use of secure storage for sensitive documentation
- Ensuring personal data is adequately secured with access limited to named Individuals
- Secure disposal of confidential information
- Segregation of duties, ensuring that not one person is solely depended upon to carry out a business process
- Secure procedures for exchange of personal information
- Ensuring the personal and sensitive data stored on websites and other vulnerable systems is encrypted for additional protection
- Documented procedures for verifying the identity of individuals
- Effective access control measures for password management, user registration and de-registration procedures (with the ability to examine historical data access records)
- Restricting corporate desktop configurations such as browser settings for accepting cookies or downloading active code.

Tips for individuals

It is impossible to completely eliminate your chances of becoming a victim of identity theft; however, you can effectively reduce your risk by following these basic recommendations.

In daily life

- **Guard your personal information**. Do not provide personal data on the phone or via mail, unless you've initiated the contact. Clever identity thieves might pose as bank agents, phone companies, and even government agencies. Before sharing personal information, confirm the organization is

legitimate by calling directly using the number listed on your account statement or telephone directory

- **Protect your mail**. Promptly remove mail from your mailbox, and when travelling, contact the Postal Service to request a vacation hold

- **Monitor your credit**. Regularly review your credit report with major credit services, and follow up with creditors if bills do not arrive on time. Federal law requires credit reporting agencies to provide you a free copy, upon request, of your credit report every 12 months

- **Monitor your accounts**. Review the balances of your financial accounts, and carefully check for any unexplained charges or withdrawals

- **Carry only necessary information**. Don't carry extra credit cards, a passport, or Social Security card in your purse or wallet unless you need it that day

- **Protect your trash**. Never discard a credit card or ATM receipt in a public place. Always shred personal information including credit card numbers, bank statements, charge receipts, and credit card applications

- **Minimize unsolicited credit offers**. To opt out of these offers in the mail, call the major credit reporting agencies at 888-5-OPTOUT

On your computer

Your computer can be a gold mine of personal information to an identity thief. The following are some tips to keep your computer—and the personal information stored within it—safe.

- **Phishing scams**. These use fraudulent emails and web sites to impersonate legitimate businesses, in hopes of getting you to disclose your personal information

- **Emails requesting personal information**. Reputable businesses will never ask for your user name, password, or credit card or Social Security numbers via email. If you are concerned about your account, contact the organization directly by phone

- **Web links in emails**. Never cut and paste the link from the message into your Internet browser. Phishers can make links appear as if they go to one place, while actually sending you to a different site. Instead, open a new Internet browser session and manually type the company's correct web address

- **Keep security software up to date**. Some email messages contain harmful software that can damage your computer or track your Internet activities without your knowledge. Anti-virus and antispyware software and a firewall

will protect you from inadvertently accepting such unwanted files. Anti-virus software scans incoming communications that contain these malicious files, while a firewall protects both the inbound and outbound connections to your computer. A firewall is particularly crucial if you have a broadband or DSL connection that leaves your computer connected to the Internet 24 hours a day

- **Use caution when opening email attachments— regardless of who sent them**. These files might contain viruses or other malicious software that could capture your passwords or other information you enter on your computer. If you download files, make sure your security software is enabled and pay close attention to any warnings

- **Be selective when sharing your email address**. Only family and friends should have your personal email address. Do not post your address on web sites, forums, or in chat rooms. If you post your address, you are vulnerable to receiving spam or having your email passed on to others. If you would like to subscribe to a newsletter, consider using a generic email address not linked to any of your personal information

- **Using email**. It's an excellent way to stay in touch with friends and family, but be selective when emailing them your personal information. Although you might have security software on your PC, your friends and family might not be protected

- **Before disposing of a computer, permanently erase personal information**. Erasing files using the delete command or reformatting your hard drive is not sufficient because files remain on the computer's hard drive, and can be retrieved later by any tech-savvy criminals. Use a trusted utility to permanently erase your sensitive, personal information, or consult a professional

- **Web site security**. When providing your personal information to a business web site, check for signs that the site is secure: a lock icon on the browser's status bar or a URL for a site that begins with "https:" (The "s" indicates "secure"). However, these signs are not 100 percent foolproof, since even security icons might be forged

- **Web site privacy policies**. Trustworthy businesses will publish how they maintain the security of personal information collected by the site, how the information will be used, and whether it will be provided to third parties. If no privacy policy is available or if the policy is hard to understand, consider doing business elsewhere

- **Use strong passwords**. Security experts recommend creating passwords that combine letters (both uppercase and lowercase), numbers, special

characters, and are more than six characters in length. For instance, a strong password would be: Go1dM!n3

- **Use caution when instant messaging (IM)**. If you use IM to communicate with friends and family, be careful when sending personal information. Protect yourself by using a nickname for your IM screen name, and never accept strangers into your IM groups

Tips for businesses

Absolute protection does not exist; however, tight security makes it possible to discourage significant attacks and to minimize the consequences of mistakes.

The following are key points that ensure the best security to help businesses avoid identity theft:

- Name a person and a backup to be responsible for information systems security
- Have policies for human resources administration—as well as for trusted vendors and partners—that are consistent with the level of security you choose for your information systems
- Take action to reduce risky behaviour—downloading programs, accepting email without discretion, responding to email concerning confidential information—through education and by creating documents detailing the rules of hardware usage or listing user responsibilities
- Build the network and define the parameters for hardware and software so that it is impossible to bypass the system
- Adopt manageable solutions for the people in charge of security who must support the system
- Create an inventory of hardware and software, and maintain message boards for users
- Manage the corporate network by formalizing its use (adding and deleting users, for example) and by documenting the actions performed on the information system (installing, restoring, troubleshooting, testing)
- Maintain a single gateway to the Internet with a firewall and an intrusion detection/prevention system to detect and block suspicious data exchanges
- Install security software (anti-virus, anti-spyware, antispam, and anti-Trojan) on all of the workstations as well as on any servers connected to the network
- Regularly apply official security patches and update the anti-virus, anti-spyware, and anti-Trojan definition files on workstations and servers
- If necessary, contact an external consultant who can assess the security of your system, and reconfigure, administer, and modernize it. Don’t jump at offers for free remote security audits
- Protect your data backup devices

In addition to these general measures:

- Tighten security around your system’s most sensitive information. Don’t allow crucial data onto a laptop computer

- Analyze in detail the wireless networks within the company. A laptop may be stolen solely to gain access to its wireless network
- Protect the information system's surroundings.

The simplest method is to restrict physical access to the computers

- Supervising job mobility to minimize the risks and the consequences of a theft or a copy
- Controlling the circulation of information beyond electronic communication. Exchanges in public or private locations, presentations at conferences, seemingly personal solicitations, responses to questionnaires, invitations to tender, and interviews are opportunities to expose information that should not be made public or to present a bad image of the company through poor performance

Conclusion

We must first admit that every one of us—individuals and businesses—are threatened and potentially vulnerable to identity theft; this is not something that happens only to others. Despite the seriousness of current incidents and the increasing threat, some basic principles allow us to significantly reduce the risk. Awareness is the best defence. Through awareness, we develop our senses to spot identity theft and to protect personal and corporate information, while maintaining the benefits of information technology.