Deloitte.

Mobile devices
Secure or security risk?

Leading business advisers

Contents

Introduction

“There is no doubt that mobile devices are a convenient portal to the online world, allowing us to stay connected while on the move. It is important however to consider the potential risks of the data on your device getting into the wrong hands and in the case of corporate data, any reputational or legal implications this may have.

If you are a corporate body allowing employees access to corporate data from mobile devices consider the potential implications of device loss in the same way as you would treat a company laptop. There is no clause in Irish data protection legislation exempting corporate or employee mobile devices.

If you are one of the hundreds of thousands of users who have no passcode lock setup on your phone now might be a good time to reconsider this choice. If you think that your data might be valuable to someone else think about employing a complex passcode. If your mobile device supports encryption and it is not enabled by default consider implementing it.

Keep your phone model and the operating system on it up to date. The older a phone is the more likely it is that someone will have worked out how to hack into it.

A bit of time invested now in considering what level of security is right for you or your organisation could save a lot of time, effort and money in dealing with the repercussions of lost data.

Colm McDonnell
Partner
Deloitte

Overview

Online fraud. Identity theft. Cybercrime. All threats that are becoming increasingly prevalent and indeed increasingly sophisticated. There is much talk regarding how to protect our information and protect our data, yet perhaps one of the most significant sources of personal information is the smartphone.

What happens to this information when smartphones are lost or stolen?

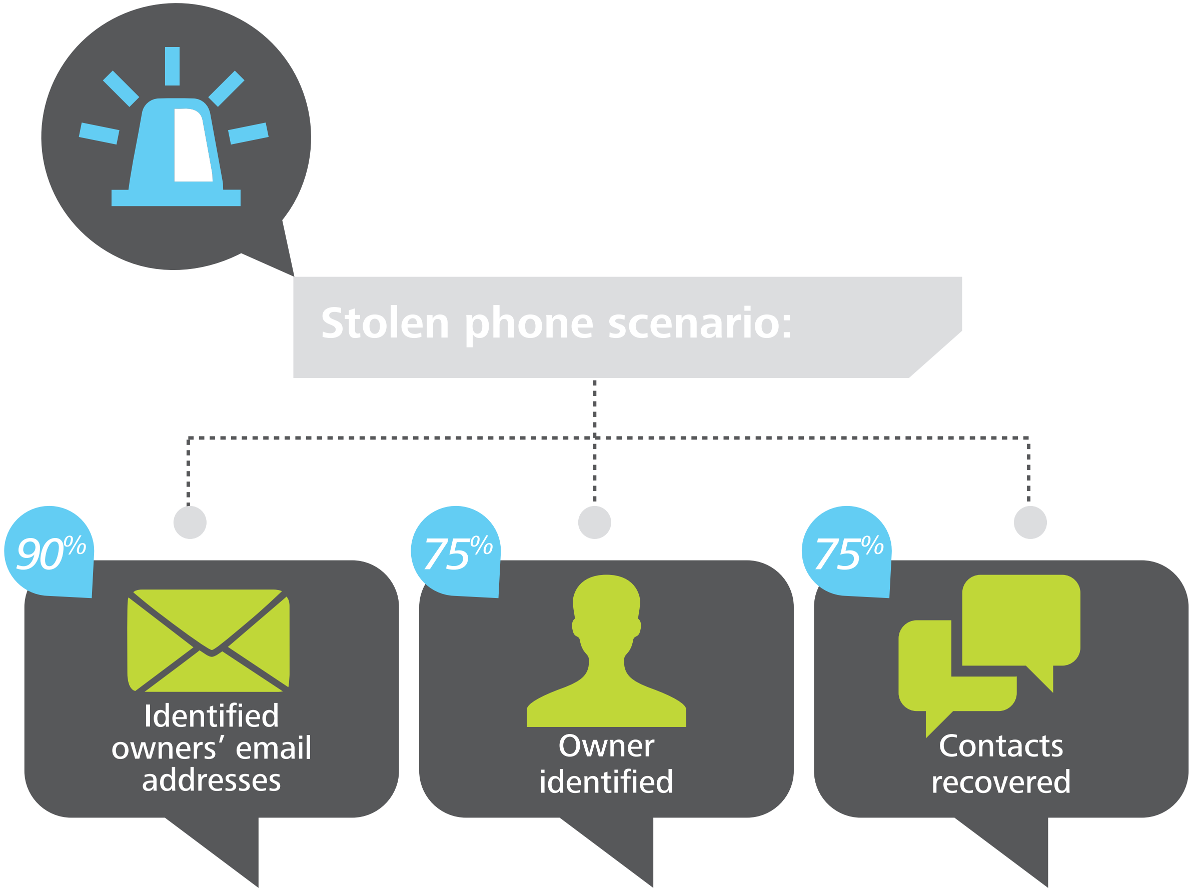
In order to investigate how much information is essentially 'left behind' the Deloitte forensics team recently undertook a research project to see what, if any data, could be accessed on second hand or 'stolen' mobile devices.

We managed to access a significant amount of data. We retrieved data identifying the original owner including social media profiles, PayPal login details, PPS numbers, Amazon account details, corporate and personal emails, SMS messages, call logs, internet browsing history, photos, location data, Skype chats, contact lists and more.

The findings clearly reinforce the need to protect your data. Think about the value of the data on your mobile device and protect it appropriately. Consider putting strong access restrictions in place, encrypt your device, provide additional barriers for corporate data, avoid malware by evaluating apps carefully before installing them and dispose of your old devices carefully.

In this report, we'll provide an overview on how accessible this data is and details on the types of data we found. Most importantly, we'll provide guidance on what can be done to protect data on mobile devices from unauthorised access.

Snapshot of key findings



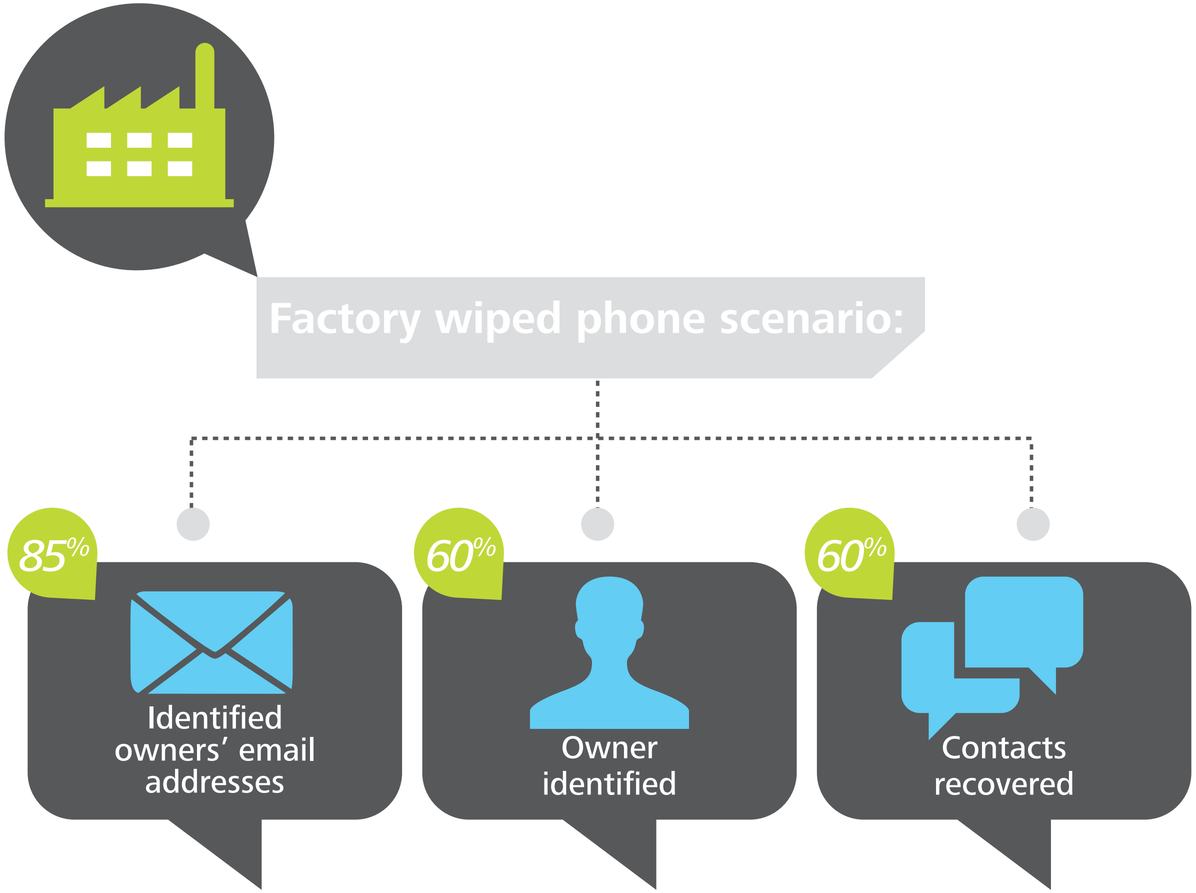
Stolen phone scenario:

90% Identified owners' email addresses

75% Owner identified

75% Contacts recovered

Snapshot of key findings



Factory wiped phone scenario:

85% Identified owners' email addresses

60% Owner identified

60% Contacts recovered

Background and research objectives

The core objective of this research project was to see what data can be retrieved from smartphones. We chose two scenarios – phones that had been lost or stolen and second hand phones.

Recent Garda figures report that 12,000 phones were reported as stolen in 2013, the unreported figure is not quantified. Similarly, when you consider that many mobile phones are upgraded every 18 or 24 months there is an abundance of second hand phones in circulation. For example, on one Irish classifieds website there are over 5,000 phones listed for sale.

What is the risk? The first reaction to loss of a mobile device might be annoyance at the inconvenience, concern about unauthorised calls, irritation at the replacement cost of the device and regret at not backing up the contacts and photos more frequently.

There is a presumption that mobile phones are stolen for use or resale. While this is probably the case in most instances, with the broadening usage of such devices for mobile payments and other cash like transactions and for work purposes in BYOD scenarios, data theft is a serious risk which is often not considered when a device is lost or stolen. This research aimed to discover what types of commercial and private data was accessible on other people's mobile devices.

Most businesses are aware of the potential repercussions of a lost laptop and understand their legal obligations with regard to protecting the data held on them. Now that mobile devices have become so powerful, is their loss and the protection of any corporate data held on them treated with the same gravity? Employees often need access to corporate data off premise, for example access to corporate email, but it is important to strike a balance between the accessibility and the security requirements of that data. Blocking all external access is extremely secure but not very conducive to the mobile office. Putting minor restrictions, for example simple passcodes in place makes it easy for employees to get access to the data but may not provide adequate protection given the commercial sensitivity of the data or any legal or compliance obligations a company might have to keep that information private. Organisations that allow external access to corporate data from mobile devices need to balance ease of access with confidentiality requirements.

Given that it is commonplace for mobile devices to be used to access corporate data, the question we wanted to raise is what, if any, residual corporate data might exist on lost, stolen or second hand mobile devices. Furthermore, could we get access to any of it? For example, could we locate any commercially sensitive data that an organisation would not want to make publicly available or data that a company was legally obliged to protect under data protection legislation.

From a private individual's perspective it is common knowledge that credit card fraud and other forms of identity theft are a fact of life in today's world. A mobile phone typically stores a wealth of personal data, and while each piece of data on its own may not pose a noteworthy risk, the cumulative effect of all the data can be significant. For example, if you were stopped in the street and asked for your name, home address, email address and home phone number, would you give it to a stranger? This would all be valuable starting information for an identity thief trying to impersonate you. That's before you start thinking about user account names, passwords, credit card numbers, PPS details and so on. These details can be stored on a mobile phone without your explicit instructions. Helpful features like personal dictionaries and keyboard caches can store words or character sequences that you have used on the phone in the past to assist you when typing them in the future. Substitute the words "character sequences" with "passwords" or "credit card number" in the previous sentence and the potential risk becomes more and more apparent.

Method

For the purposes of this review the term mobile devices incorporates smartphones and tablets.

A range of mobile devices were selected including Apple iPhones, Blackberries, Android devices, Windows phones and a number of tablets. Two scenarios were tested: a simulation of lost or stolen devices and a set of second hand phones that had been wiped. In order to get a real picture of the potential risks faced by mobile device users in Ireland we devised a set of experiments to establish what could potentially be found on devices typically in use today.

We simulated lost/stolen devices by borrowing phones from consenting participants and trying to retrieve data with no knowledge of the PIN codes or passwords. We also purchased a sample of second hand phones that had been "wiped" with the phones own in built reset or factory wipe facility. Using the sample phones we attempted to retrieve both personal and corporate data.

This research was conducted by a group of digital forensic investigators using a range of specialist techniques and tools. All but one of the devices in the research was protected by a passcode, meaning that the data we collected would not have been accessible by using the handset itself. However, even if data is not directly accessible, it may still be present.

We deliberately have not associated any of the findings with the specific devices models. The purpose of this research was not to provide a device specific vulnerability list but to raise the awareness of the potential risks associated with unauthorised access to mobile devices.

Phone access

The first step in this research project was to get access to data on the devices. All phones tested, with the exception of one tablet, were either protected by a passcode or had been factory reset to wipe any data stored on them. In other words the device owner or previous owner had some level of belief that the device had been wiped or that there was a block in place to restrict access to the data. The two main barriers to access in place were data encryption and passcodes.

Data encryption means that data is not stored in plain text and needs to be passed through complex mathematical algorithms to be read. It should be noted that while the encryption algorithms typically employed on mobile devices are strong and have not currently been cracked, the manner in which they are implemented is also relevant. In non-technical terms, you could have a door which requires ten separate keys and codes to open it but if you leave them all under the mat then someone might still be able to get inside. In the case of some of the older phones we were able to access the phone data even though the device was encrypted. On the newer devices this was typically not the case. Approximately 45% of the sample devices examined were encrypted.

The second barrier was a passcode. A variety of methods were used to lock the phones analysed, ranging from four character PIN codes, more complex longer codes, PIN patterns and biometric authentication (fingerprints). The success for bypassing the codes was mixed and very specific to the phone model, operating system version and complexity of the code. We did not manage to crack any biometric restrictions, but we did crack the complex password on one unencrypted device and we cracked more than 50% of the four character PINs in the sample set using software tools in less than 30 minutes.

> We cracked more than 50% of the four character PINs in the sample set using software tools in less than 30 minutes.

Findings – ‘stolen’ phones scenario

On the “stolen” phones, no attempt had been made to wipe any of the data prior to our examination. Where we were able to access the phone we could see what the original owner could see. If the device was encrypted we were not typically able to get access to items that had been previously deleted by the user. On unencrypted devices we were able to retrieve considerable deleted data, in addition to what was currently accessible from the device.

STOLEN PHONES SCENARIO (50% ENCRYPTED, 90% PASSCODE LOCKED)

75%

OWNER IDENTIFIED

Full names and partial contact details identified from numerous references; SMS text messages, e-mail addresses, email content, Facebook details and photos. On one phone we were able to identify the current owner and the previous owner prior to a factory reset.

75%

CONTACTS RECOVERED

An average of 300 contacts per phone were recovered detailing names, telephone numbers and email addresses.

90%

IDENTIFIED OWNERS’ EMAIL ADDRESSES

References to email addresses associated with the owner’s name; some phones had multiple email account details including business and personal.

60%

PERSONAL EMAIL CONTENT

Some phones had data from more than one webmail account. Email content and metadata showing who the mail was sent to/from and the time and date stamps were available.

25%

CORPORATE EMAIL CONTENT

Business related email was recovered with content, incoming and outgoing addresses and timestamps.

STOLEN PHONES SCENARIO (50% ENCRYPTED, 90% PASSCODE LOCKED)

75%

BROWSING HISTORY

A large amount of data was recovered including details of websites visited, favourite sites recorded, cookies from sites visited, google map and YouTube searches, social media sites visited including Facebook and Twitter with status updates and tweets.

40%

LOCATION DATA

The amount of data stored for this varied hugely depending on whether locations services were turned on or off on the device. Typically location data was available from cell towers that the device connected to, Wi-Fi access points that were in close proximity, regardless of whether a connection was made and photos. With the data from one of the devices we were able to generate a graphical representation of the owner's movements for the last couple of months. Another device held nearly 9,000 locations.

60%

INTERESTS AND HOBBIES

This varied from device to device depending on the type of usage; typically if web browsing history was accessible you could gather a lot of information on favourite sports, teams and general interests that might assist with targeted information gathering or guessing account passwords.

40%

ACCOUNT PASSWORDS

A variety of passwords were recovered including Wi-Fi access point passwords which could potentially allow access to your home or work networks and website access credentials which although generally innocuous, can give hints as to how an individual typically forms. On one device the user had saved login credentials for PayPal and Amazon on their PC, inadvertently synchronised them to the cloud and then these were transferred in plain text to their smartphone.

60%

PHOTOS

We managed to get access to thousands of images. These were typically photos taken from the device or social media/profile images from Facebook, WhatsApp and Viber. These were both from the phone owner and their contacts.

0%

CREDIT CARD DETAILS

We did not manage to scrape credit card details from any of the devices in the sample set.

25%

PPS NUMBERS

A number of devices had PPS numbers stored in contacts or SMS messages.

60%

TEXT AND CHAT LOGS CONTENT

This included whole and partial texts with sent and received identifiers and timestamps. They were from a variety of sources including SMS, Viber, Skype and WhatsApp.

Findings – ‘wiped’ phone scenario

These phones had all had a reset or factory wipe performed on them. Most were purchased as second hand and some came from individuals known to us who had wiped the phone before giving it to us. The phones had no passcode protection in place. No residual data was visible from using the handset in the usual way. However, when we made specialist images of the devices we were able to collect some data from 70% of the devices. The devices with inbuilt encryption were the least likely to have any retrievable data.

FACTORY WIPED PHONES SCENARIO (40% ENCRYPTED, 0% PASSCODE LOCKED)

70%

OWNER IDENTIFIED

Full names and partial contact details identified from numerous references; SMS text messages, emails addresses, email content, Facebook profile. One phone had details of two previous owners.

60%

CONTACTS RECOVERED

A small amount of contacts were retrieved from SMS messages, call logs and email fragments.

60%

IDENTIFIED OWNERS’ EMAIL ADDRESSES

Email accounts associated with the owner’s name were identified, both personal and to a lesser degree corporate addresses.

30%

PERSONAL EMAIL CONTENT

A small amount of personal webmail data was recovered.

15%

CORPORATE EMAIL CONTENT

Fragments of business related email were recovered with email addresses and content.

40%

BROWSING HISTORY

Facebook chat fragments and twitter account details were recovered along with data and images from websites visited.

FACTORY WIPED PHONES SCENARIO (40% ENCRYPTED, 0% PASSCODE LOCKED)

0%

LOCATION DATA

There was no location data found on these devices.

30%

INTERESTS AND HOBBIES

The career of some of the previous mobile device owners was apparent.

30%

ACCOUNT PASSWORDS

Passwords and SSIDs for all Wi-Fi networks that one device had connected to were recovered. Login names were retrieved alongside their passwords. Passwords appeared to be stored in close proximity to webmail account details.

30%

PHOTOS

We were able to match images from one device with a current Facebook profile to confirm the old user's identity. Numerous photos were recovered; one device had more than 8,000 recoverable images, many of which were personal photos.

0%

CREDIT CARD DETAILS

We did not manage to scrape credit card details from any of these devices

15%

PPS NUMBERS

PPS numbers were recovered from SMS messages.

85%

TEXT AND CHAT LOGS CONTENT

This included whole and partial texts with sent and received identifiers and timestamps. We recovered over 2,500 texts from one device.

30%

CALENDAR EVENTS AND CALL LOGS

We recovered a log detailing 500 calls on one device, calendar events were also found.

What measures can individuals and organisations take to protect your data and maximise privacy?

The findings from both scenarios show that an accurate personal profile of previous owners can be retrieved, emphasising the very real need for both organisations and individuals alike to protect their data and maximise privacy.

Put a passcode on your phone

There is little point having the latest encrypted mobile device if you don't put some kind of passcode on it. Simple four digit passcodes are typically easy to remember, easy to guess, easy to observe by shoulder surfing and in a lot of cases easy to crack using brute force automated or manual retries. Most phones can be setup to require a more sophisticated or complex password setup, for example allowing more than four digits or allowing a wider selection of alphanumeric or special characters. The worst case scenario is that this will slow down attempted unauthorised access as the potential number of key combinations increases dramatically by the length of the code and the selection of characters. Some mobile devices will automatically wipe after a preselected number of incorrect attempts or enforce an increasing wait time between attempts.

Biometric locks are now emerging and are predicted to become more common over the course of 2014. The Chaos Computer Club claims to have forged a dampened latex finger model, created from a high resolution image of a fingerprint that successfully authenticated and granted access to a device. This is probably not a procedure that an amateur hacker or thief could perform, however it may be within the reach of a determined criminal following on from a targeted theft.

You should always protect your PIN code from prying eyes when using your phone in public. It is also worth noting that a PIN code that is easy to remember for you (for example your date of birth) can also be easy to guess. Some mobile devices support a pattern lock to restrict access. As with the four digit passcodes, some hacks or bypasses exist for particular models and they are also vulnerable to shoulder surfing.

While passcodes are not perfect they will, at minimum, slow down access to your device, potentially giving you the option to remote wipe your device before a thief can access your data.

If your phone supports it, enable encryption

Of the four brands of products we analysed the current models of Windows, iOS and Blackberry phones are encrypted by default. Encryption can also be enabled on Android devices but it is not enabled by default. Of the older phones we examined fewer had encryption enabled and there were known hacks to bypass the implementation of the encryption in some cases. While it can be argued that some implementations of encryption are better than others there is no doubt that it sets up a barrier that, at a minimum, makes it harder to gain unauthorised access to data and in a best case scenario blocks unauthorised access completely.

Protect your corporate data

There are many options for enforcing minimum security standards and restricting what is downloaded to a mobile device. Mobile Device Management options support features such as containerisation, where a section of a phone is portioned off and remains encrypted and under corporate control. Minimum requirements for BYOD or corporate phones can be enforced, limiting access to corporate data to registered devices with specific security requirements. These might include complex passwords or device encryption. Each organisation should consider the options and decide what is right for them.

Wipe your old phones

All phones we tested had some kind of factory reset or wipe facility. In all cases running this reset made it impossible to access residual data from the handset itself. However, in some cases using specialist methods and tools we were able to access considerable amounts of old data from "wiped" phones. On the newer encrypted mobile device models we were unable to retrieve any data post wipe. On some of the older encrypted devices we did get some data post wipe. It remains to be seen if the older devices had poorly implemented encryption or if it just takes time for someone to find a vulnerability on a device.

Ironically, on one unencrypted device where the history was known, the residual data appeared to be data that had been deleted by the user prior to the factory reset.

Again while not perfect on every device, a factory reset is still worth performing on your old phones before you retire them or pass them on.

Enable the remote wipe facility if it exists

Unless you can put your hand on your heart and say that you have no sensitive personal or corporate data on your phone it is a good idea to enable the remote wipe facility on your mobile device. Each manufacturer has slightly different implementations of remote wiping. The devices we looked at had various combinations of an excessive incorrect PIN code attempt wipe or a network based wipe. The former will wipe the phone's contents if more than a pre-set number (typically 10) incorrect PINs are entered on the device. To utilise a network based wipe the device needs to be preconfigured to accept a remote wipe request that may be instigated via the phone network or over Wi-Fi. If the SIM has been removed from the device or disconnected from the cell network and the phone is not connected to a Wi-Fi network the remote wipe facility will not work.

Record the IMEI number

Keep a record of your IMEI number somewhere safe so that you can report your phone stolen and ensure that the unique identifier is blocked from being re-connected to the public phone network. This hugely reduces the value of the phone hardware.

.

Protect your phone backups

If you value your data, perform regular backups of your mobile device. A backup of your phone on a PC doesn't suffer from the same risk of loss as your mobile device. However, home PCs do get stolen. If you synchronise your phone onto your home PC you should either encrypt the PC or encrypt the phone backup. Getting unauthorised access into a backup of your phone's data can be easier to accomplish than getting into the device itself.

Vet your apps

Mobile malware is becoming more prevalent. Where possible, only download reputable apps from reputable sources. Some common aims of mobile malware would be to collect data or run up bills. Data that is stored on the phone or data from normal communications can be intercepted and transmitted to another source, potentially account credentials or online banking details. Credit cards can be used or bills can be accumulated, for example by getting a device to send premium rate texts.

The practice of "rooting" phones may make them more susceptible to malware.

Safe disposal

At the very least you should wipe your old phone before you put it in a cupboard, sell it or give it away. If a private mobile device potentially holds corporate data, device disposal issues should be addressed and agreed with the data owner.

> “At the very least you should wipe your old phone before you put it in a cupboard, sell it or give it away. If a private mobile device potentially holds corporate data, device disposal issues should be addressed and agreed with the data owner.

Contacts

For more information please contact:

Colm McDonnell
Partner
T: +353 1 417 2348
E: cmcdonnell@deloitte.ie

Jacky Fox
IT Forensic Lead
T: +353 1 417 2208
E: jacfox@deloitte.ie

Martin Moroney
T: +353 1 4173000

Sean Wills
T: +353 1 4173000

The Deloitte Security and Forensic team operates an incident response hotline for companies that require timely assistance in the event of a cyber security incident. A typical incident might be an ongoing data breach, a website defacement or a denial of service attack.

Contact the team on (01) 4173000 to reach a security professional in our state of the art forensic lab.

For more details please contact:

Dublin
Deloitte & Touche
Deloitte & Touche House
Earlsfort Terrace
Dublin 2
T: +353 1 417 2200
F: +353 1 417 2300

Cork
Deloitte & Touche
No.6 Lapp's Quay
Cork
T: +353 21 490 7000
F: +353 21 490 7001

Limerick
Deloitte & Touche
Deloitte & Touche House
Charlotte Quay
Limerick
T: +353 61 435500
F: +353 61 418310

www.deloitte.com/ie

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/ie/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte has in the region of 200,000 professionals, all committed to becoming the standard of excellence.

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, Deloitte Global Services Limited, Deloitte Global Services Holdings Limited, the Deloitte Touche Tohmatsu Verein, any of their member firms, or any of the foregoing's affiliates (collectively the "Deloitte Network") are, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this publication.