The Recover Report

Mishcon de Reya

It's business. But it's personal.

MISHCON RECOVER

This report examines a sample of 150 data theft cases handled by Mishcon de Reya. Our research has focused on cases involving dishonest employees and industrial competitors. The report aims to help you to identify where you may be vulnerable to employee related data theft, to advise you on the best possible protection and, to ensure you know how to prevent misuse of your information in the event of a theft.

Our sample includes a range of client sectors from large listed companies, to well-established and regulated financial institutions, to privately owned and managed SMEs. We have not included an analysis of our experience advising in relation to cases involving politically-sponsored cyber-attacks by foreign intelligence services or hackers who set about obtaining personal details to clone identities.

THE RECOVER REPORT

A company's competitive edge in the market often derives from the quality of its confidential and proprietary information. Business sensitive data relating to accounts and finances, as well as relationships with employees, suppliers and customers, carries with it significant value. As a result, this data is often considered amongst the most valuable assets of a business. It is therefore vital for the business first to identify this information and then to proactively protect it.

The use of technology is changing the way we do business and the way we manage our business information. Smartphones, tablets, internet-enabled remote access, mobile and Cloud computing and the development of social media have all helped improve efficiency and connectivity. Whilst this has had a positive impact upon profitability, it has rendered businesses more vulnerable to attack than ever before. Yet technology has evolved in a way that means you no longer need to be an IT expert to steal data. You don't even need to be in the building.

When IT systems are compromised, red flags should be raised and alarm bells should start ringing immediately so that the business can quickly take steps to recover data and prevent its misuse. Any failure to address such an incident, or any time lag in taking action, can cause lasting damage to the business, or can even jeopardise the very survival of some businesses.

The U.S. House Small Business Subcommittee on Health and Technology's recent hearing "Protecting Small Businesses Against Emerging and Complex Cyber-Attacks" referenced a report that found that almost 60% of small businesses will close within half a year of being the victim of cybercrime.[1]

The majority of people in business today have a good grasp of IT issues and believe that they can adequately protect information held online. Businesses that have implemented risk management, security and awareness systems and IT protocols are at an advantage, yet this does not mean that they are completely immune from attack. Cyber criminals, hackers, dishonest and disgruntled employees could still break through IT defences and it is important to know how to protect against this risk, and what to do if an attack occurs.

THE PERPETRATORS

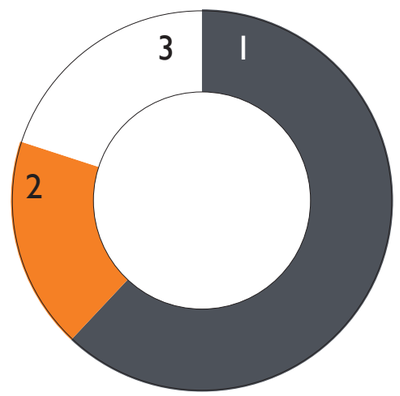
According to our research, lone men aged between 24-35 are most likely to commit data theft. 79% of the data theft incidents we reviewed involved a person acting alone. 77% of these lone perpetrators were male. Our analysis shows that only 20% of the data theft incidents were committed by women or groups of women. As with males, females predominantly acted alone with only 3% of such cases involving a team of women. Only 7% of incidents involved a multi-sex team of men and women.

A business cannot operate without its employees having access to the information they need in order to carry out their jobs. This means that every business owner must place trust in their employees. A recent survey by OnePoll for security company LogRhythm found that 44% of 1000 employers surveyed said that they trusted their employees not to access or steal confidential information and that they perceived external sources to be a greater threat.[2]

Worryingly, however, a survey of 2000 European workers by information management services company Iron Mountain found that one in three employees have taken or forwarded confidential information out of the office on more than one occasion.[3]

This discord between the perceptions of the typical employer and the actions of the typical employee creates a dangerous environment where rogue employees are free to steal from their unsuspecting employers. This can lead to a delay in the discovery of the theft and result in it being too late to prevent the misuse of the stolen information.

Lone men are most likely to commit data theft



1 62% Lone Male
2 18% Lone Female
3 20% Groups/Companies

1. Source: "Protecting Small Businesses Against Emerging and Complex Cyber-Attacks" opening statement http://smallbusiness.house.gov/uploadedfiles/3-21-13_chris_collins_opening_statement.pdf

2. Source: 'UK Insider Threat Survey – employers' by One Poll on behalf of Log Rhythm http://logrhythm.com/Portals/0/resources/LogRhythm_survey_results_4.2013_employers.pdf

3. Source: IronMountain – Taking Data Home. http://img.en25.com/Web/IronMountain/Iron_Mountain-Taking_Data_Home.pdf

INFORMATION THEFT BY ROGUE EMPLOYEES TO SECURE THEIR NEXT MOVE

In 30% of our cases, the thief planned to use the data to set up a competing business. In 65% of cases, the perpetrator planned to use the information in their new role with an existing competitor. Such data often proves to be part of a 'dowry' that a data thief brings to secure employment with a rival. This also raises serious questions about how much a new employer needs to know about the nature, and source, of information that a new employee brings with them, and the extent to which they should be taking steps to protect against obtaining this unfair competitive edge.

If a new joiner is in possession of confidential information, it is vital that you act with integrity, take legal advice and follow the steps set out in the Top Tips section of this report.

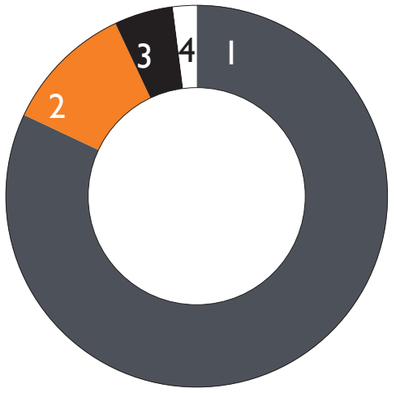
In just 5% of cases considered, the theft was discovered before it was clear what the data thief planned to do with the information. In such cases, the person stealing the data may have taken it in case it had value in the future.

According to Verizon's 2013 Data Breach Investigations Report, which surveyed over 47,000 security breach incidents over 70% of IP theft cases committed by internal people took place within 30 days of them announcing their resignation.[4] Our own case analysis shows that in the vast majority of the data theft cases reviewed, employees had left the employer weeks, and in some instances months, before the leaks were discovered.

WHAT INFORMATION WAS STOLEN?

In the service sectors of the economy, by far the most common data stolen by employees involved customer information. This occurred in 82% of our cases. Internal financial data was taken in 11% of the cases. 5% of cases involved information relating to negotiating or tender positions and in 2% of cases the data stolen related to bespoke back office operations or other business-sensitive information.

1 82% Customer information
2 11% Internal financial information
3 5% Information relating to negotiating or tender positions
4 2% Back office operations or other business-sensitive information.



82% of thieves took just one item, indicating to us that they specifically targeted the most valuable document that would be of most use to them and that, without a wholesale attack on the system, their wrongdoing would be harder to detect.

HOW WAS THE INFORMATION STOLEN?

In 56% of the cases reviewed, the most common method used by employees to obtain and retain the data was via email. In other words, the breach did not involve a sophisticated technique or high level of IT skill and expertise. 26% of the thieves took the data in the most basic of methods by printing out a hard copy and taking it with them. 16% employed more than one method to obtain the information.

Surprisingly, the use of USB memory sticks, data CDs or DVDs was only present in 6% of cases despite their low cost, relative ease of use, and ability to record huge volumes of data very quickly. This may be because businesses have now wised up to the risk posed by these data storage devices and have taken greater steps to restrict their use.

We regularly advise in cases in which the employee has gained remote access to the networks in order to steal data, or has had access to a company laptop in which he or she has stored data for use post-employment. Newer technologies are becoming more prevalent in these cases, such as web apps and cloud computing.

It is clear to us that law and practice are not keeping up with the expansion of social media, in particular, LinkedIn. As a result, we have seen a marked increase in data theft cases involving social media platforms, usually relating to the misuse of client lists following an employee's departure from a company. 90% of our cases in the recruitment sector in the first quarter of 2013 have involved this issue. It is vital to find the correct balance between protecting client contacts and the corresponding revenue this can bring, versus the obvious commercial benefits that can be derived from the use of social media to build relationships and business.

We have also seen an increase in instances of hacking, which can be more difficult to detect but not impossible. Organisations can use forensic tools and techniques to capture digital evidence of such electronic data theft. In 48% of our cases we instructed forensic IT experts to investigate the method of the theft and to undertake IT security audits on our clients' computer networks and systems.

TOP TIPS

1. What to do if a new joiner brings confidential information to your business
You should:
— closely check the provenance of the confidential information and
— ensure that the new joiner confirms in writing that the information is owned by them and able to be utilised in your business.

If you discover the information is not the property of the new joiner:
— Do not use the material. If you do, you could find yourself facing a claim for breach of confidence, conspiracy and inducing breach of contract. You could be found liable for any losses arising from the misuse of the material as well as the legal costs associated with the legal action. In addition, you could find yourself the subject of powerful and intrusive injunctions with the associated legal cost and loss of business time.
— You should seek legal advice and consider notifying the owner of the confidential information that you have the material, are returning it to them and will delete all relevant material from your IT systems.

— You should also consider whether you should continue with the appointment of the new joiner.

If, however, your due diligence establishes that the information does in fact belong to the new joiner, it is important that the contract with him or her expressly states the confidential information becomes the property of the business upon them joining. This eliminates any confusion over ownership in the event the new joiner leaves the business.

2. How to prevent an attack on your business
A preventative approach is vital. Business owners should consider the resources currently deployed to assess and manage the risks to their critical business data. Everyone within the business, from the top down, must understand what information is confidential to the business and how they can help protect it.

Information security policies and guidelines must be up-to-date and communicated clearly to all data users within the business. These should give clear guidance on when, where, how and what data may be moved. Encryption and close control over who has access to data may provide additional lines of defence.

Iron Mountain's Taking Data Home Survey[5] suggested that a lack of appropriate information management policies or their ineffective implementation played an important role in information loss. Only 57 per cent of respondents said it was always clear when information was confidential, and 34% said they were not aware of any company guidelines regarding what information could or could not be removed from the office.

Clearly communicated guidelines and policies reinforce your business rules to your employees and can be relied on in the event of subsequent legal action.

4 Source: Verizon Data Breach Investigations Report 2013 - http://www.verizonenterprise.com/DBIR/2013/

5 Source: IronMountain – Taking Data Home. http://img.en25.com/Web/IronMountain/Iron_Mountain-Taking_Data_Home.pdf

How to prevent an attack on your business

1.
PUT IN PLACE AND ENFORCE BASIC CONTRACTUAL MEASURES SUCH AS:

— a cybercrime policy
— a social network policy
— an internet use policy
— a mobile working policy
— confidentiality clauses which properly identify the information that must be protected and
— restrictive covenants linked to confidentiality clauses in the employment and consultancy contracts.

2.
ENSURE YOU ARE AWARE OF THE OPERATIONAL, LEGAL AND TECHNICAL STEPS YOU CAN DEPLOY IN THE FIRST INSTANCE TO PROTECT YOUR POSITION AND MITIGATE THE BUSINESS IMPACT.

— appoint someone to be in charge of cyber security
— appoint an external consultant to audit your IT security and advise on appropriate systems and steps
— invest in up to date IT security systems that can protect and detect the movement of data
— carry out regular IT security audits and monitoring
— invest in malware protection programmes
— limit or ban the use of data transfer devices such as USB sticks and hard drives, limit and monitor remote access, Cloud and social networking
— make sure you have an incident response plan

3.
EDUCATE AND TRAIN YOUR STAFF TO BE AWARE OF THE RISK, TO UNDERSTAND WHAT IS CONFIDENTIAL TO THE BUSINESS AND THE VALUE OF IT.

4.
CONSIDER OBTAINING INSURANCE TO PROTECT AGAINST BUSINESS INTERRUPTION CAUSED BY CYBER CRIME AND DATA THEFT.

3. What to do if you suspect you have been the victim of a data theft

Even with sophisticated data security controls, you may still fall victim to data theft. Where a data theft is discovered or suspected, a decisive and immediate response is essential. You should seek legal advice immediately. The most effective and decisive action one can take is to obtain a Search Order, Delivery Up Order and / or a Computer Imaging Order to secure and recover the stolen confidential information and the evidence of unlawful use of the material. Of the 150 incidents handled by Mishcon de Reya, the average time from completion of the investigation to obtaining legal relief was just over two and a half weeks. 76% of cases were concluded within a month. The sooner you act in response to a data theft incident, the greater your chances of recovering the data and of minimising any potential loss.

In many situations, where a competing business is being set up, specialist corporate intelligence researchers can provide you with evidence of the timing behind such action, the names and addresses of those involved and even identify others in your business who may continue to pose a risk. Such research can be a key part of building an effective legal case against the wrongdoers.

IN CONCLUSION

Cybercrime and data theft pose a real threat to organisations. Whilst some industries suffer more than others, it is clear that all businesses and all industries in the UK and abroad are at risk.

Businesses should take effective action to minimise the risk of data being stolen. In the event a theft occurs, they should take immediate and decisive action to recover their data and prevent its misuse. Creating effective data protection policies and promoting a climate where employees recognise the value of integrity in handling sensitive commercial data is vital to prevent data theft from taking place.

ABOUT MISHCON

Mishcon de Reya is a law firm with offices in London and New York. Specifically we offer the following legal services: dispute resolution; real estate, corporate; employment; and private client. Mishcon de Reya was named Law Firm of the Year 2012 at the Lawyer Awards and The Legal Business Awards and our Fraud Group is ranked in the first tier in both Legal 500 and Chambers and Partners.

Mishcon Recover

We have 15 years' experience advising on and litigating large and high profile data theft cases for large corporate clients as well as small businesses and individuals across numerous sectors. Using Mishcon Recover we recover and prevent the unlawful use of your stolen data by swiftly obtaining powerful injunctions without notice to the data thief allowing us to search the defendant's premises, recover stolen data, seize evidence of wrong doing and freeze assets. We use this strategy to reach a quick settlement, avoiding protracted and expensive litigation. Visit www.mishcon.com for more information on Mishcon Recover.

Contacts

Robert Wynn Jones
Partner
T: +44 207 440 7443
E: Robert.wynnjones@mishcon.com

Hugo Plowman
Partner
T: +44 207 440 7149
E: hugo.plowman@mishcon.com

Summit House
12 Red Lion Square
London
WC1R 4QD

T +44 20 7440 7000
F +44 20 7404 5982
E contactus@mishcon.com

www.mishcon.com