

Data theft

I have a problem with data theft; what should I do?

Introduction

Theft of data has reached epidemic proportions in Ireland. The development of ever-higher-capacity portable data storage devices, such as USB pen drives, has made it almost trivially easy to copy large quantities of data from almost any computer. We have also seen users use e-mail and web-mail to transfer key files from their computer systems often in large quantities, and most computers still have CD and DVD burners that provide another potential route for data to be stolen.

Data theft is sufficiently common that, ideally, any organisation should have some kind of incident response plan to deal with it. Most organisations, however, do not. We have prepared the following brief document for IT personnel or other managers who are faced with potential data theft or are thinking of preparing a plan for dealing with it. This document is not a complete incident response plan. We hope, however, that it will provide a useful guide to the key issues in dealing with data theft incidents and may help anyone faced suddenly with dealing with such an event. We think it deals with most of the main issues facing organisations who have encountered this kind of problem.

Grant Thornton has extensive experience helping organisations deal with crises such as these. We have helped many others prepare detailed incident response plans to allow them to quickly react to, control and end incidents that threaten to disrupt or damage their organisations. If you need more advice, or would like to talk to us about our services we would be delighted for you to get in contact with us. Our contact details are at the end of the document.

How is data generally stolen?

We find that in the cases we investigate, the most common method used to steal data is by using a USB “thumb drive” or a similar small data storage device. Indeed, any device with substantial amounts of on-board memory can be employed for data theft. A recent phenomenon, for example, is the use of portable digital music players to remove data from computers, a practice referred to as “podding” by its practitioners. There are however other modes of data theft which we also see on an ever increasing basis:

Common modes of data theft

USB “pen” or “thumb” drive These devices are cheap, easy to hide, and nowadays have large storage capacities. This makes them perfect for data theft.

Portable hard drive While USB pens can store several gigabytes of data (i.e. hundreds of documents) it is possible to purchase small portable hard drives that can store hundreds of gigabytes (tens of thousands of documents.) These devices are often not much larger than an iPod, and can be powered from the USB ports of the computers they are connected to.

MP3 players, digital cameras, memory cards or PDAs Many modern devices now have substantial on-board memory capacities, all of which can be used for removing data. Some of these devices have the additional advantage that their use is more easily explainable by the data thief, and more difficult for an investigator to follow.

CD/DVD Again, using a CD or DVD has the advantage of being more apparently legitimate. Also writable DVD's now have capacities of nearly 9 gigabytes, comparable to the larger USB thumbs.

E-mail Some data thieves simply use e-mail to transfer files out. Often this is done over a long period of time, so organisation IT staff do not notice large messages passing through their servers. It is also common to see such mails sent to private or web-based e-mail addresses, on the pretence that the sender is preparing to work on the data "at home".

Web-mail Similarly, so data thieves use web-mail to send data from their organisation. This has the advantage of greater apparent privacy than conventional e-mails, and often allows for larger attachments to be sent. Fortunately, web mail often leaves significant forensic traces that a skilled investigator can recover.

Printing Some careful data thieves will not make any electronic copies at all, but will print out key documents and steal them in hard-copy form. This, of course, limits the amount of material that can be stolen, but it does not prevent the stolen material being quickly transferred back into electronic form later, through techniques like scanning and Optical Character Recognition.

Remote Access Some organisations make data theft even easier by allowing remote access to their systems from employee's private computers. This makes data theft difficult to trace, and makes it very difficult for investigators to identify the computers and other devices to which the stolen data has been transferred.

Please note that we are only referring in this to data stolen by individuals with legitimate access to it. We have prepared another guide to unauthorised access to data, which can be downloaded from our website.

What can be stolen?

Practically any piece of data stored in a company is potentially of use to somebody. If it weren't of some potential value, it would not be stored in the first place. Over the years, our investigators investigated thefts of almost any kind of data you would care to imagine. However, we believe that the following are most at risk:

Targets for data theft

- customer contact and financial data, including credit card numbers and bank account details;
- software source code and algorithms;
- marketing information including plans, contact lists and media;
- system and user network credentials, such as passwords and certificates;
- proprietary process descriptions and operating methodologies;
- personnel records and private employee data;
- legal data concerning ongoing or planned litigation or contract actions;
- other user's private documents stored on company computers; and
- company strategic data, including the communications of managerial and executive staff.

When does it occur?

It is an unfortunate fact that data theft is done by trusted individuals. If they were not trusted, they would probably not have been given access to the data in the first place.

Circumstances correlated with a higher risk of data theft

- **sudden resignation/departure of staff with access to important data;**
- **departure of staff to commercial competitors;**
- **departure of staff to start their own business or other enterprises;**
- **staff with access to sensitive data involved in disciplinary or relationship issues** It is easier for individuals to rationalise stealing information from organisations they do not like;
- **staff leaving under redundancy**

- **staff in personal relationships with persons in competing organisations;**
- **staff in personal relationships with journalists;**
- **companies undergoing financial or industrial relations problems; and**
- **departure of staff, under any circumstances, with access to business critical data.** While the probability that data will be stolen is not necessarily higher, the potential impact of such a loss is greater, so the overall risk is higher.

Data theft telltales

Virus infections and hacking attempts can cause computer crashes and changes to network performance. These can reveal the presence of an intruder or virus program. Data theft is far less likely to produce effects that allow it to be detected. Consequently data theft is an area where it is often important to call-in computer forensic support early

Many of the cases of data theft we uncover arise when organisations call us in as a precaution, with little or no actual evidence of data theft except, occasionally, a suspicion that current circumstances have increased the chance of a data theft occurring.

Nevertheless, in previous cases we have seen data theft detected in the following ways:

Possible indicators of data theft

- numbers of e-mail "bounces" caused by the data thieves sending excessively large e-mails from their accounts;
- multiple overlarge e-mails being sent from the mail system;
- large scale search activity on the file server system;
- unusual or over-large database dumps from customer management or creditors systems;
- requests for remote access without good reason, or from long-standing employees who have not needed it before;
- purchase of USB storage devices (sometimes data thieves have their victims pay for the devices they use to steal data);
- late night or weekend working by persons suspected of planning to leave the firm. This change in work patterns may only be recognised after the individual has left the organisation;
- change in work patterns by someone about to leave the firm – for example suddenly starting to bring their office laptop home in the evening, after years of leaving it in the office, or a suddenly increased use of USB or other portable devices. Again, this change in behaviour might only be recognised after the person has left the organisation, or submitted their resignation;
- proprietary information or strategies appearing in other organisations or the public domain; and
- competing organisations pre-empting or reacting unusually quickly to your initiatives, or developing competing products or services to ones you have recently introduced, after suspiciously short lead times.

In our experience data thieves often steal data days, weeks or months before they actually decide to leave the organisation (if they leave the organisation at all). This can make it difficult to determine whether data transfers are legitimate or evidence of data theft. In some cases the thief will copy the data for legitimate reasons, but will make a second stolen copy at the same time.

Potential sources of evidence

Fortunately, data theft can leave a great deal of trace evidence behind on computers systems and storage devices. However, it normally takes computer forensic techniques to recover this data in an evidentially useful form, and it takes experience to correlate diverse types of evidence to form a coherent picture. The list of potentially valuable evidence includes:

Potential evidence of data theft

- intact and deleted messages in e-mail accounts;
- remnants of web-mail messages and web-mail inboxes;
- file access histories showing the presence of key files on external devices;
- file and document "metadata" showing recent access;
- file and registry logs showing the presence of external storage devices;
- temporary files and registry entries showing access to key documents;
- temporary files showing documents burned to databases;
- print spooler remnants showing files recently printed;
- recently created Zip files, used to compress the stolen data for copying; and
- remote access logs showing times and dates of access to key servers.

Basic incident response

Priorities

Your priorities in dealing with data theft should be

- to determine the timing and extent of the data compromise;
- to determine the method by which the data was stolen;
- to prevent the data thief distributing the stolen data or making further copies;
- to prevent the data thief making use of the stolen data;
- to assess whether legal or regulatory action may be required; and
- to prevent further data thefts occurring.

It is often necessary to act quickly, because thieves will typically make use of data soon after it is stolen. Also, if legal action is to be taken to prevent the use or dissemination of the stolen data, the Court will need to be persuaded of the urgency of the issue. A rapid response will help persuade the Court of the seriousness of the matter. Conversely a slow response will tend to contradict any claims of urgency.

Other issues you need to consider

Documentation: As with any incident, the first responder should document all significant events, observations and actions taken from when the incident is first detected. If these are not recorded immediately it is very likely that key details will be missed which may delay or reduce the effectiveness of later remedial actions.

Reporting: Managers and key affected stakeholders should be advised of the event:

Considering advising

- General Management;
- IT Management;
- Business/Operational Unit Management;
- Legal;
- HR/Industrial Relations;
- Public Relations; and
- Internal Audit/Fraud Control.

Remediation and reporting

Remediation

Remediation involves putting measures in place to ensure, as far as possible, similar incidents do not reoccur. In the case of data theft we suggest the following precautions, if they are not already in place:

Remediation actions

- consider prohibiting access to web-mail. This needs some consideration, as there are significant advantages and disadvantages of doing so;
- prohibit all private data storage devices from the network. This should include MP3 players, USB pens, digital cameras, Blackberry phones or any other device with mass data storage capabilities;
- restrict and monitor remote access. Do not allow remote access to the network by devices not owned by the organisation;
- perform periodic reviews of leavers' computers, particularly in circumstances of higher risk;
- never let users leave with data storage media, be it a floppy disk, or their old laptop computer;
- remind users of their duty of confidentiality on joining the organisation and regularly thereafter;
- introduce a policy of "least-privilege" across your network. This at least restricts a potential data thief's scope;
- any files or software obtained from outside your organisation must be swept for malware before being used on any of your computers; and
- consider implementing a document management system. This will tell you who has accessed what documents, and when.

Reporting

It is often necessary to prepare a formal report on any incident for senior managers, regulators or other stakeholders. In writing the report on the incident it is probably worthwhile considering the following issues:

Possible report content

- the cause of the data loss (if determined);
- contributory factors to the incident;
- timeline of incident response activities;
- actions taken to recover from the incident;
- assessment of any damages incurred, data lost;
- further remedial actions required; and
- other relevant information.

If you need more advice

Our incident response and computer forensics specialists have helped hundreds of organisations deal with incidents quickly and effectively, helping them resolve their problems with the minimum of loss, disruption or distress.

If you would like to talk to us about computer forensics, incident response planning or any other issue, please feel free to give us a call at the numbers below.

Contact

Paul Jacobs
Partner, Forensic & Investigation Services
D +353 (0)1 6805 835
E paul.jacobs@grantthornton.ie

Andrew Harbison
Director, IT Forensics & Investigation Services
D +353 (0)1 6805 766
M +353 (0)86 040 7211
E andrew.harbison@grantthornton.ie

24-26 City Quay, Dublin 2

Offices also in Limerick and Kildare

This briefing is provided for general information purposes only and is not a comprehensive or complete statement of the issues to which it relates. It should not be used as a substitute for advice on individual cases. Before acting or refraining from acting in particular circumstances, specialist advice should always be obtained. No liability can be accepted by Grant Thornton for any loss occasioned to any person acting or refraining from acting as a result of any material in this briefing. Grant Thornton is authorised by the Institute of Chartered Accountants in Ireland to carry on investment business.