

# Computer misuse

I have a problem with computer misuse; what should I do?

## Introduction

Employees have been misusing the computers assigned to them for as long as they have been used in organisations. We have seen computers used to download pornographic and illegal material, bully other employees, to threaten or defame colleagues and clients, to access gambling and other questionable and other inappropriate uses. There is also the ever present problem of excessive personal use of computers – employees spending hours each day surfing the net instead of doing what they are paid to do.

Computer misuse is so common that organisations should really have some plan in place to respond to it. Many organisations have HR procedures for dealing with misconduct by staff but, in our experience, few of these consider the preservation and analysis of computer evidence. We have prepared the following brief document for IT personnel or other managers who are faced with dealing with a case of computer misuse or who 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 computer misuse and may help anyone faced suddenly with dealing with such an incident. 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.

## What kinds of computer misuse do I need to worry about?

With the exception of accessing illegal (usually child pornographic) material, none of these activities are necessarily illegal. All, however, expose any organisation that permits them to civil actions, and consequently all must be controlled. The problem is that because they are not illegal many must be explicitly prohibited in the organisations own acceptable use policies if they are to be investigated and pursued aggressively. It is essential, therefore, that companies have comprehensive acceptable use policies in place before any such events occur.

### Common types of computer misuse

**Accessing illegal material.** In most cases, illegal material on computers means child pornography. Child pornography is contraband, and should be immediately reported to police. Some organisations worry that, if they report child pornography and the suspect is later cleared, they will be susceptible to being sued to defamation. In practice, if the report is made in good faith, this never happens. If you find yourself in such circumstances, Grant Thornton or other reputable IT forensics providers can advise you whether or not the material found is likely to fall under the category of illegal material.

**Accessing pornographic material.** This kind of behaviour appears to have become less common in recent years, but still occurs regularly enough to remain a significant issue for companies. The problem is that while this activity can be interpreted as a form of sexual harassment, and failing to deal with it can place an organisation at risk of legal action by its employees, it is not in any way illegal. This means it must be expressly prohibited by the acceptable use policy. In any case, where conventional pornography is tolerated, use can very often escalate into illegal material.

**Accessing grossly inappropriate material.** Pornographic material is not the only kind of graphical material that can cause problems in an organisation. In the past we have seen scatological, racist, sexist and discriminatory material, or other material meant deliberately to cause disgust or shock circulated in organisations. Again this material is not likely to be illegal, but might very easily lead to a legal claim if not actively suppressed.

**Bullying/defamation.** Bullying is increasingly carried out over the internet, often using bulletin boards, social networking sites and anonymous e-mail accounts. Defamatory material can be sent in similar ways. This kind of material is traceable using internet computer forensics, but it requires specialist skills which may not be present in most organisations.

**Copyright theft.** Illegal copying of music MP3s and other media is becoming more of a problem, not only because it is becoming more prevalent, but also because media companies and organisations are increasingly likely to take action against organisations, whose networks are used to download, store or distribute such materials.

**Access to restricted sites.** Some organisations prohibit access to web-mail, gambling, sports and other sites, usually for very good reasons. Some users insist on visiting them, by means of visiting "proxy" sites, bypassing web-filtering programs or using independent internet connections. Action needs to be taken against such users for any acceptable use policy to remain in force.

**Possession of inappropriate software.** It is not unusual for anti-virus software to detect the presence of hacking or network scanning software on user computers. While some of these have legitimate use in network administration, the presence of such software at the very least raises concerns about the possibility that they may be used for hacking. Worse still some of this software is rigged by its writers to load backdoors and other malicious software to the computers it is installed on. Another problem is the presence of media modifying or "ripping" software. This software is used to remove the copyright protections on media, and its presence can represent a significant legal threat to the organisation that permits it.

**Installation of computer games/media.** Obviously, games movies and other time wasting applications stored on computers are a major threat to productivity and need to be acted upon as soon as they are found. More extreme cases may require IT forensic analysis to establish a case for disciplinary action.

**Other breaches of acceptable use policies.** Acceptable use policies need to be enforced for all users or the organisation runs the risk of the policy being considered "tacitly not in force". In such an event, the policy would be effectively unenforceable. In the past we have investigated problems such as deliberate sharing of network privileges, culpable mishandling of customer data, theft of company-licensed software and many other serious problems. All can be dealt with quickly and effectively through the use of computer forensics.

**Excessive use.** In our experience it generally takes hours of daily use over an extended period of time. Also, it needs to be demonstrated that the browsing was unrelated to the individual's role and that the individual had other duties that were not performed.

If you do not have an acceptable use policy yet, we have included some guidelines to writing one below. The absence of an acceptable use policy does not preclude responding to computer misuse. It does mean, however, that you need to be more careful in dealing with private material on computers, and it may affect how your legal advisors recommend pursuing the matter through administrative or disciplinary proceedings.

## Misuse telltales

Computer misuse can be uncovered in many ways. It is most commonly found when other computer users report it, but there are many other ways it can be revealed. The one thing most misuse incidents have in common is that they come as a surprise and catch the organisations they affect off their guard. It is important therefore that there be some kind of plan in place to react to computer misuse when it occurs.

### Computer misuse indicators

- complaints by other staff;
- lowered employee productivity - failure by employees to carry out instructions or meet objectives;
- heavy internet or web-mail access (identifiable at the proxy);
- repeated malware infections on single users' computers or subnets;
- repeated web-filter blocks on the user's account;
- the same user account used on many different computers;
- increase in spam received by a single user or small group of users;
- large numbers of large e-mails sent between users;
- use of "anonymisation" or "proxy" web-sites on the computer;
- excessive out of hours working without a reasonable explanation;
- use of non-standard communications protocols such as Internet Relay Chat, Internet Newsgroup Protocol or unauthorised encrypted protocols; and
- use of non-standard file transfer-protocols such as Bittorrent, Limewire and TFTP.

## Basic incident response

### Priorities

Your priorities in dealing with data theft should be:

- to determine the nature, timing and extent of the misuse;
- to determine the means by which the misuse was carried out;
- to determine if others are complicit in the misuse;
- to assess whether disciplinary, legal or regulatory action may be required;
- to determine if the misuse may have affected other users, clients, or other stakeholders;
- and
- to prevent further misuse of a similar nature occurring.

It is advisable to use computer forensic techniques to secure and analyse evidence in misuse cases. Organisations sometimes avoid using sophisticated investigative techniques in so-called "administrative cases" on grounds of cost, when they would be perfectly willing to use such methods in fraud, data theft or other cases. This is regrettable because administrative cases can easily become civil actions, where the validity of evidence becomes much more important, and also because administrative investigations often uncover far more serious misconduct than is first suspected. Grant Thornton always recover evidence to the highest legal standard for just this reason.

### Other issues you need to consider

**Documentation:** As with any incident, the person to whom the misuse is first reported 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:

#### Consider 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 action

- if no IT acceptable use policy is in place, implement one as a high priority;
- ensure you reserve the right to examine all data on all computers and other devices connected to your network;
- prohibit privately held data storage devices from your network. Never allow anything to be connected to your network and computer systems that you do not own;
- monitor e-mail traffic for large files passing back and forth;
- monitor spam traffic on the e-mail system. Note if any users are receiving unusual amounts of spam;
- ensure that all users are regularly reminded of their duties and obligations under the acceptable use policies;
- implement web-filtering software, and make sure the databases are kept up to date;
- ensure web-filtering and proxy logs are checked regularly for signs of inappropriate use;
- consider performing periodic spot checks of users' computers for signs of misuse; and
- periodically check the network for signs of bittorrent, limewire or other peer-to-peer file transfer programs.

#### 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 nature of the computer misuse;
- contributory factors to the misuse;
- 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.

Be careful to avoid defaming the subject(s) of the investigation.

#### Acceptable use policy

It is important to have an effective computer acceptable use policy in place in any organisation, regardless of size. Without such a policy, circulated to all users, it can be difficult or impossible to investigate computer misuse (or any other form of computer based incident). Users are permitted to use their work computers to store personal information and to have their privacy respected unless they are warned in advance not to do so, or that if they do so the organisation reserves the right to inspect the contents of all computers on their network.

Grant Thornton have helped many organisations develop comprehensive and effective computer Acceptable Use Policies (APU). We have found that good AUPs should at the very least include:

#### Key components of acceptable use policies

- a statement that the policy applies to all employees, regardless of position, and to all devices owned by the organisation whether on or off the premises;
- a section reserving the right of the organisation to inspect all computers and devices on the organisation's computer infrastructure, regardless of type;
- a statement making clear that no employee should store personal or private material on the organisations computer systems;
- a description of the user's rights and obligations with respect to the organisation's computer systems;
- a description of what is prohibited on the organisation's computer systems. This should include a prohibition on pornographic, discriminatory or hateful material;
- a description of the conditions under which private use of the internet is permitted as well as specifying material that cannot be viewed or copied. These conditions and limitations must be explained to users;
- a requirement that users keep password, keys, certificates and other computer system credentials secure, and that they not be shared with others inside or outside the organisation;
- a requirement that users do not use their company e-mail addresses for private uses (as this tend to greatly increase the amount of spam received);
- a requirement that users do not use or attempt to use computer resources to which they have not been given permission;
- a statement of the penalties to be imposed in cases where the acceptable use policy is not followed;
- a description of the kind of monitoring of use users can expect on the organisations computer systems; and
- a reporting procedure in case they observe breach of the acceptable use policy.

#### 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.