

Dealing with electronic harassment in the workplace

As figures show a startling level of workplace bullying and harassment, Mark Larson from CCL-Forensics looks at how digital forensics can help companies investigate this growing menace.

One in five employees has been the victim of bullying or harassment in the last two years according to a survey from the Chartered Institute of Personnel and Development.

Bullying and harassment can take a number of forms but the spread of electronic communications into the workplace, and the ease with which messages can be sent with relative anonymity, mean that the age of the cyber-bully has well and truly arrived.



Research by one of the UK's leading legal firms shows 20 per cent of employers still turn a blind eye to inappropriate emails from colleagues. This is despite new guidance from the Equal Opportunities Commission (EOC) confirming they can constitute harassment and, therefore, cost companies dearly.

Statistics from the EOC suggest there is, on average, one successful sexual harassment claim each week in the UK, but only a small proportion of people affected make a claim, hiding the true extent of the problem.

A few minutes on the BBC News website reveals a number of cyber-bullying stories, among them are these headlines:

PA's £10,000 for obscene e-mails 'shock'

Stalker guilty of e-mail campaign

E-mail stalker jailed

The fact that employees can send abusive, harassing and offensive material electronically can have serious consequences for a company because they may have a vicarious liability if they haven't taken effective steps to prevent such activities. This can be compounded by the fact that many victims complain that they did not feel that the employer took the matter seriously or that the action taken was sufficient.

The incident that the first headline refers to is a case in point. The victim said "When my complaint didn't seem to be taken seriously I lost confidence in my employer and felt I couldn't carry on working for them."

Julie Mellor, chairwoman of the Equal Opportunities Commission, which supported the case, said: "All employers should make their staff aware that sexual harassment can take many forms and can be deeply distressing for the person on the receiving end. The fact that comments are made by e-mail doesn't mean they should be treated any less seriously than if they were spoken or written down."

"One in five employees has been the victim of harassment in the last two years"

The message for employers must be - deal with it. Don't hope the problem will just go away. It is not unusual for harassment to be conducted over periods measured in years. Remember too that even when an offensive email is not sent directly to a member of staff, but circulated to others within the same workplace, it can be recognised as harassment.

So what form does cyber-harassment take? While statistics are difficult to come by,

anecdotal evidence suggests that email is by far the most common form. This has almost certainly been greatly facilitated by the advent of free, apparently anonymous web mail.

“Comments by e-mail shouldn't be treated less seriously”

The mobile phone is another common means of harassment and this often takes the form of SMS (text) messages. The relative anonymity of this is perhaps once again a factor. Cheap, anonymous pay-as-you-go phones make hiding the attacker's identity even easier.

Cyber-harassment can also take place on web forums, chat rooms, blogs and social networking sites.

What can you do to combat electronic harassment in your workplace? One key factor is having effective policy in place; although policy, no matter how comprehensive, cannot ultimately prevent harassment from taking place, it can provide the context for subsequent disciplinary action.

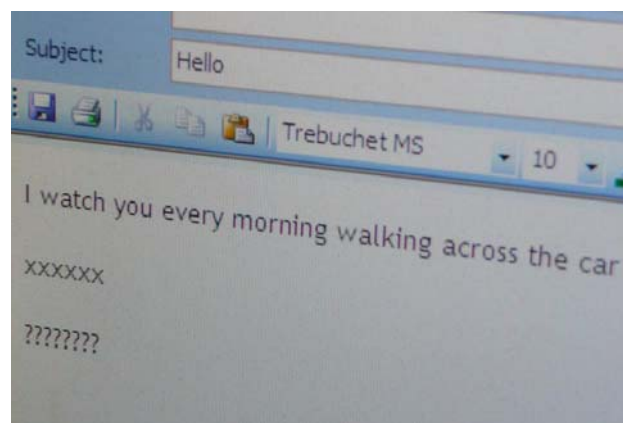
Consider backing up your policy with training. Installing content filtering can also help prevent some offensive messages passing through the network. In the end, though, it is extremely difficult to prevent harassment from taking place and it is crucial that you are prepared for it so that when it happens you act promptly and treat it with the seriousness it requires.

So, what can you do when someone in your company is the victim of electronic harassment? First and foremost it is essential to preserve the evidence. While it must be tempting to any victim to delete offensive messages they should not do this. While no harm can come from printing and preserving offensive messages this should not be relied on as the sole source of evidence; firstly because some of the most important evidence may be hidden in the message header and also because a print is not best evidence, they would be easy to manufacture and on that basis may not necessarily be admitted or given full weight by a tribunal or court.

In some cases the victim may previously have deleted offensive email messages before bringing them to management's attention. If this is the case the evidence may not be lost - copies may be retained on a backup of the email system.

One key issue in harassment cases is identifying the perpetrator where they have taken steps to protect their identity. Statistically most (in fact about two thirds) are known to the victim. Indeed a common profile for attacks is that the victim has had some sort of relationship with the attacker.

Establishing a trust relationship with the victim can potentially provide the strongest evidence of the attacker's identity. It is ironic considering how many attackers are known to the victims just how often they get away with it. One fundamental property of electronic harassment is that it will leave evidence on both the sending and receiving computers or mobile phones as well as on the respective network infrastructures.



Where any of these belong to the company, getting access should not be a problem and you should, at an early stage, consider collecting the available electronic evidence. The best way to do this in the case of computers is to use a digital forensics process known as imaging. The hard disk drive is accessed through a piece of specialist hardware that prevents changes being made to the disk and the image is created by digital forensics software. The image is effectively a byte for byte copy of the computer's hard disk drive. This is extremely powerful in that it captures the entire data present on the disk, not simply that visible to the user, and therefore includes all the deleted data that has not been subsequently overwritten

and any other data written to the disk. Similar forensic techniques are used to capture data from mobile phone handsets and SIM cards.

Digital evidence is fragile and can be lost if action is not taken promptly. You should consider securing the digital evidence at the earliest opportunity. Seek specialist advice to help you through this process. Once the data is secured you needn't necessarily proceed to analysis but it is impossible to forensically analyse data that is no longer there.

“Digital evidence is fragile and can be lost if action is not taken promptly”

Ideally you will forensically examine both the victim and the attacker's computers or mobile telephones. This will provide the most comprehensive view of the evidence. In practice you may not always be able to do this - perhaps because you cannot compel someone to grant access to their personal computer or mobile phone however you should not assume that such a case must fail, judges may have the power to make an order granting access. You should consult your solicitor about this. In practice the most compelling evidence will always come from the attacker's computer or mobile phone but this doesn't mean a case is hopeless without it.

The following case studies show how digital forensics has successfully been used in cyber-harassment cases.

**Case study:
Anonymous web mail harassment**

This case involved the victim being subject to sexual harassment by email. The attacker used a free web mail account set up under a false identity.

In this case there was a clear suspect - the victim had an office romance with a co-worker that she had subsequently ended. When challenged however the suspect denied he was responsible for the emails. The timings of the messages showed they were sent while the suspect was at work and so the suspect's computer was forensically imaged and

analysed. Although the suspect had never consciously stored any of the messages on his computer the computer itself had caused the web mail pages to be written to the computer's hard disk drive as temporary internet files.

Although these had automatically been deleted subsequently, by using techniques such as keyword searching for some of the offensive message text and the originating web mail address CCL-Forensics were able to recover many of the offensive messages - proving that they had been sent from the suspect's office computer while he was logged on. When confronted with the evidence the suspect made a full admission.

**Case study:
Anonymous web mail harassment
(no suspect)**

This case involved the victim being subject to racist abuse sent via email. Once again the messages originated from an anonymous web mail account. In this case there was no specific suspect although it was suspected that the sender was a colleague. As a further complication the victim shared an office with fourteen co-workers.

Forensically imaging all fourteen computers was not viable both on grounds of cost and proportionality. We used a more selective approach to narrow down the field of potential suspects. A small team of forensic analysts went to the company's office at the weekend. Using forensic write-blocking hardware that prevented any changes being made to the data on the computers' hard disk drives we conducted keyword searches for the offensive terms used in the original emails.

After only a few hours on site we were able to identify traces of the email messages on a co-worker's computer. Subsequent forensic analysis of that computer recovered enough traces of the messages to show that they had been sent from that computer and who was the logged-on user at that time. Analysis also showed that no other user had ever logged-on to that computer.

**Case study:
Deleted SMS text messages**

This case concerned sexual harassment in the workplace. The victim had received a number of sexually offensive text messages from a co-worker. At the time the victim had not considered the matter especially serious and had deleted the messages.

This is an understandable reaction and, although we recommend that evidence is always preserved, it isn't always clear at the outset that a particular matter is that serious. The harassment proceeded from the sending of text messages to face to face verbal harassment and it at this point the victim reported the matter to management.

Management were sympathetic and reacted quickly but had no means to compel the suspect to allow his personal mobile phone to be examined. Without this they had no real tangible evidence and the situation was stalled in a 'my word versus their word' situation. In an attempt to break the deadlock the victim's mobile phone was forensically examined. One piece of potentially useful evidence was found immediately - the victim had replied to one of the text messages insisting the sender stop. This message was stored in the 'sent messages' store. While not conclusive it was of some help in confirming the victim's account of events.

Recovering deleted information from mobile phones can be technically challenging and it is not always possible.

In this case the victim's mobile phone was of a type that we were able to recover deleted messages from. We used a raw dump of the entire phone memory, analysed this and were subsequently able to recover some of the original messages - substantially confirming the victim's account. ■

Mark Larson is Forensics Manager at CCL-Forensics - a leading supplier of digital forensics services. Our law enforcement clients include the Metropolitan Police and H.M. Revenue & Customs. We have a range of legal and corporate clients and also have significant experience undertaking criminal defence work. If you would like any help or advice relating to securing and analysing evidence of cyber-harassment or similar activities please contact us on 01789 261 200 or info@ccl-forensics.com