



Greig Ross Associates  
Connecting your Staff to Security



## Welcome to the January edition of "Oops!"

***"..offering a few People Security New Year's Resolutions".***

### The Secure Line...

Although major fraud scandals such as Madoff, Kerviel or Leeson involve large sums of money and make newspaper headlines small scale fraud is rarely reported but happens more frequently than any of us would care to imagine and is very upsetting for organisations, staff and shareholders. Statistically such events occur more frequently in recessions such as we have at the moment when many people have difficulties with over-extended credit cards, negative equity or even paying the monthly household bills. Wendy Goucher, our lead consultant in the security empowerment team focuses in on fraud and redundancy and what companies, and importantly employees, should be doing at this time.

This month's first article, "[Spring Clean your systems Access](#)" considers how businesses need to increase their awareness at this time and importantly how employees can be helped to reduce the company's risk both for themselves and for others.

In our second feature this month "[For Security's Sake look after your staff](#)" we present our experience with regrettably too many companies who suffer losses and their security is breached at the time of staff departure. Whether an employee is made redundant, resigns or is sacked there are fundamental matters that must be addressed.

**Oops!** from Greig Ross Associates providing the latest case studies and best practice.

Do you know anyone who would benefit from receiving Oops!? [Click here](#) to forward this edition to a colleague or associate.

## Spring Clean your System Access.

In businesses of all sizes one of the big security faults is poor maintenance and monitoring of access to business systems. You would be amazed at the number ex-employees and, even worse, ex-contractors, who still have access to business systems across the world. Most will never realise it, but a few will exploit that access, and use the information they retrieve.

I recently spoke to a consultant who had completed some accounting work for an international media company 7 months ago. When he returned to do another small contract at the beginning of December he was horrified to find that his access to accounting data had not been disabled from his previous contract. Also the e-mail account that had been set up was overflowing with junk mail. This is not an unusual example. In many cases it is the norm.

What could he have done?

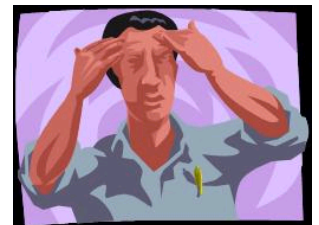
- Copied and used sensitive accounting information.
- Made alterations that could have cost the company money.
- Used his legitimate e-mail account to portray himself as an employee.
- Attacked the business network from inside.
- Stolen money from the business.

[Click here to read the full article.](#)

## Good Management Brings a Security Bonus

As we are now into the start of a new year it can be difficult not to become totally focused on the needs and concerns of the business- at the expense of staff.

That is not to say that staff are being neglected, after all everyone's position depends on the



To immediately unsubscribe to Oops!  
[click here](#)

success of the business. However, it can mean that issues can be missed and that can lead to security concerns.

[Click here to read the full article.](#)

Greig Ross Associates Limited, 1 Trainers Brae, North Berwick, By Edinburgh, EH39 4NR

[enquiries@graltd.co.uk](mailto:enquiries@graltd.co.uk)

T: 0044 8456 444 945 F: 0044 8456 444 943