

Arguably an organisations' most vital asset is its databases, often containing sensitive financial information, customer and employee data and intellectual property.

There have been many articles written that examine the risks posed of data being exposed and the potential damage caused. External threats have long been recognised, with billions of pounds spent strengthening defences to mitigate against them - yet there is little acknowledgement of the very real threat from within.

The statement 'don't leave your valuables on show' is a simple principle so why is it often ignored by Corporate UK?

It has been proven to be relatively easy to bribe someone on the inside - or even plant a rogue employee in the organisation - to gain access to sensitive data - but even if we leave this well-documented risk aside, how often has someone left your organisation taking company stationary with them? Do you know what else has been taken? Could they have sneaked out with sensitive material? What about a copy of the entire corporate database? Would you even know if they had?

Below, I've identified the most common techniques individuals will employ to copy sensitive data:

LEGITIMATE ACCESS, YET INAPPROPRIATE USE

Let's be realistic, employees need to have access to corporate data in the normal course of their duties. Increasingly today, this need is 24 hours a day - 7 days a week and is not restricted to within the corporate walls or to company owned devices.

It is this need that is opening up one of the biggest and growing weak points for Corporate UK as data is seeping out via unprotected end-points, a significant number of which the company is unaware exist, or they are simply outside the company's domain, such as private USB sticks, iPods and a complete generation of smartphones such as iPhones, BlackBerrys and Android mobiles.

To illustrate, an employee in sales may need to legitimately access customer records whilst on or off site and during a normal day may do so up to 100 times.

Another employee in R&D may need access to the secret formula for a product that's in development, whilst another employee in the marketing department may need to access the marketing plans for this new product's launch and email them to the various agencies tasked with delivering the plan.

However, there is no viable reason for all of these different employees and departments to be able to access all of this information in the same way, and do the same things with it.

In many instances, in fact, the company may be legally obligated to limit access to information on a need-to-know basis.

Access must be restricted to just the records that are needed to perform the task, with control over which bits of each record can be viewed, combined with limiting what can be done with the record.

If there is no obvious explanation why an employee should need to be able to access confidential and sensitive data, whilst off site, then they shouldn't be able to.

This is especially true now that we have the Information Commissioner's Office able to impose penalties of up to £500,000 for a data breach or loss, which could have been avoided.

Against this backdrop, it would be prudent to employ a solution that can detect and monitor devices connecting to the enterprise and sync'ing up with corporate data.

Additionally, if there is no reason why they should need to make an electronic copy of these records - be it to a corporate or personal endpoint such as a CD, a USB/Memory stick, an iPod or aforementioned smartphone, then there should be an enforceable means of ensuring they not be able to do so.

If there is a valid reason why they need to make a copy then it should be force-encrypted with a solution that does not impede the system, regardless of the device it is stored to, to ensure the integrity of the data is protected once away from the safe corporate environment.



By the same token, if an employee does not need to print a copy of the data then they should not be able to do so and even if they do, this should be regulated as our experience suggests that there can be no genuine reason for complete records to be printed.

Perhaps an alarm system should be sounded if someone does print the entire database and a means deployed to ensure that it is not removed from the premises.

Another way to identify if an employee is abusing their access rights is if their usual behaviour alters and they suddenly start accessing a greater number of records than usual for longer, or even shorter, periods of time.

This could indicate that they are writing the records down in some format to by-pass any security restrictions in place.

In the case of a disgruntled employee determined to cause mischief, records could be altered, or perhaps worse deleted, thereby damaging the reliability of the data.

Another danger is if an employee wishes to steal a copy of a database and may attach it to an email and send it out legitimately through the corporate gateway.

A savvy employee, worried at leaving a trail, may try to by-pass this by uploading the file to an external system, such as Yahoo, Hotmail or a hosted document storage and management solution.

As already noted, there have even been a few instances of people seeking employment to steal data, or of an employee persuaded to divulge corporate secrets for financial gain.

OPPORTUNISTIC ACCESS IS STILL A REAL RISK

There are some risks that aren't high-tech and therefore harder to detect - and even harder to protect against. For example, the business case for a printed hard copy of sensitive records needs to be strong as an opportunist may access this and make a photocopy of it, completely undetected!

Another increasingly recognised threat is the mobile employee, justifiably working while travelling; either on

the train, in a service station or another location, with someone looking over their shoulder and making a note of material displayed on the screen.

One further, really obvious, risk is writing down and/or sharing passwords. This is a truly naive practice, with no justification, yet it is still widely abused today.

ILLEGITIMATE ACCESS - SO OF COURSE THEY'RE UP TO NO GOOD

The easiest, yet inexcusable, way for data to be violated is by an ex-employee whose access rights have not been revoked in a timely manner, and who is accessing the network remotely, perhaps initially just to see if they can, and then tempted into taking liberties with this oversight.

Another potentially soft target is a portable endpoint; such as, but not limited to, a laptop, a USB/Memory stick, or a smartphone that is misplaced or stolen. Should the device be unprotected then any data stored on it is exposed.

Additionally, in the case of a laptop or smartphone, it may provide a back door to the corporate network.

SO WHAT CAN CORPORATE UK DO?

It may seem like a nightmare with so many trusted employees intentionally, or even inadvertently putting your most vital asset – your data – in jeopardy, yet there are ways to mitigate against these risks:

- 1.** Restrict data access to only those employees who need it and limit what they can see, and what they can do, with the records
- 2.** Appropriately monitor employees' behaviour, ideally setting control mechanisms to flag any significant deviations from the norm
- 3.** Employ a solution that can detect devices trying to connect to the enterprise and sync up with corporate data and force-encrypt information when it is removed, legitimately or illegitimately, from the safe environment of the corporate network
- 4.** Do not make unnecessary hardcopies of records or leave them unsecured
- 5.** Educate the mobile workforce to the risks posed by their activities and the devices that they use



ARTICLE:

20 Ways to Lose Your Database

Tim Pollard, VP EMEA for CREDANT Technologies

6. When an employee leaves, ensure all access rights are revoked immediately
7. Never leave a written record of passwords
8. Perform background checks on new employees, including contractors and any periodic workers. It may be prudent for these checks to be conducted at regular intervals to ensure that nothing has changed, as is the case for those working with children via the criminal records bureau
9. Never leave data security up to the end user. It is imperative that this is controlled and managed centrally - which can also reduce TCO (total cost of ownership) as machines don't need to be locked down or brought in to the office to update them
10. Corporate governance - especially with the arrival of rules such as PCI DSS and the Companies Act - requires you now to have security and to be able to prove it. Use a solution that includes a central management console - that way every endpoint is protected and can be tracked.

20 WAYS TO LOSE YOUR DATABASE

1. Employees able to access a database regardless of their need to do so, with sight of complete records including information that they do not necessarily need to see
2. Unrestricted downloading of the database to removable media
3. Employees able to print individual records, or even the full database, in hard copy format
4. Employees able to access records, in undefined quantities or for unlimited periods of time, providing the opportunity to make a written copy
5. Records, or even the entire database, altered or deleted

6. The full database, or individual files, emailed as an attachment
7. The full database, or individual files, uploaded to an external storage facility/website or a hosted document storage and management solution
8. Loss of external or portable media (memory sticks, CDs, laptops, etc) that contain unencrypted information, often during travel
9. Misplaced, or stolen, devices (laptops, blackberries, etc) used as a back door to the corporate network
10. Secure employment for the purpose of having unrestricted access to confidential data with criminal intent
11. Existing employees being coerced into removing data for financial gain
12. Ex-employees who have not had their access rights revoked
13. Photocopy hard copies
14. Over the shoulder screen theft from mobile workforce
15. Writing down, or even sharing, passwords
16. Hacked WiFi networks - even with passwords
17. Use of non-alphanumeric passphrases and passphrases of eight or less characters - which can be cracked in a few hours
18. Use of unvetted external contractors or companies
19. Use of vetted external companies on contracts without remediation/penalty clauses on responsibilities for when things go pear-shaped on the data security front
20. Failure to use encrypted back-up storage media

For more information contact www.credant.com