CLEARSWIFT
ADAPTIVE CYBER PROTECTION

Stop The Leak:
How Data Breaches Happen

Data can leak from the most unexpected places. Here's how it happens.

Stop The Leak:
How Data Breaches Happen

It's time to get serious about data leaking from your organization. The costs of data breaches continue to rise. **The Privacy Rights Clearinghouse reports that since 2005, 607.4 million records have been breached in the US.** In reality, it says, the number should be much larger because many breaches are not reported in the media. But why do these data breaches happen, and how? What are some of the most serious examples?

Why they happen

Data leaks from an organization are for two broad reasons: either someone makes a mistake, or someone intends to leak it.

In the first case, employees can unwittingly put data where they shouldn't.

This was the case at Volunteer State Community College in Gallatin, Tennessee, where staff **posted the personal data of 14,000 students and faculty to an insecure web server,** and then left it there for four years.

The other kind of breach is intentional and malicious.

Insiders or external third parties gain deliberate access to data, with the intent of using it for personal or political gain.

That's the why, but what about the how? Data can leak through any number of holes in an organization's computing infrastructure. Here are some of the worst.

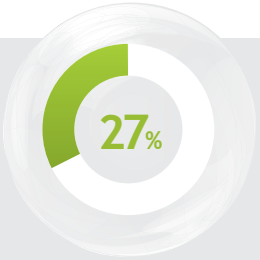
Misuse of Corporate Computers

The **2010 CSI Computer Crime and Security Survey** revealed that 25% of all security incidents reported by organizations involved insider abuse of net access or email. Quite simply, people are doing things that they shouldn't with company computers and data is leaking as a result.

There are many different types of misuse. Everything from

- **peer-to-peer file sharing**
- **inappropriate use of email**
- **non-work web browsing**

can all lead to disaster.



The negative results of a simple miscalculation when using corporate resources can be massive. 27% of data breaches are caused by inadvertent misuse of computing resources by an employee.

Then, there are the intentional breaches resulting from computer misuse. In 2012, an employee working in the Medicaid program was **arrested** after allegedly transferring the personal information of over 228,000 Medicaid recipients to his personal email, and forwarding it to at least one other person. The Department Of Health and Human Services discovered the breach, and contacted police.

Solution: Technology and policy.

- Maintain policies governing acceptable and unacceptable use of corporate computer systems and information.
- Use your data security technologies to enforce these policies.

Unauthorized network access

You can't talk about unauthorized network access and data leaks in the same paragraph without mentioning Albert Gonzalez. This hacker, who was convicted in 2010 and sentenced to 20 years in federal prison, worked with accomplices to **gain access to the computer network operated by Micros Systems,** which makes point-of-sale systems. Once he had access to its network, he was able to read the credit card information whenever a credit card was swiped at a point of sale terminal. He used this technique on organizations including JCPenney, clothing chain Wet Seal, and the Hannaford Bros grocery chain.

Solution: Defense in depth.

- Secure the perimeter to your network.
- Secure the systems within it.
- Secure the data itself, via encryption, access control and DLP.

Unauthorized physical access

Some of the worst data leaks happen because people have unauthorized physical access to devices and media. In 2010, Minneapolis-based Educational Credit Management Corp had the names, addresses, Social Security numbers and birthdates of 3.3 million people nationwide **stolen from its headquarters.**

The thieves **broke into a storage area** in its building that had been secured with card key access, and took two safes containing portable media with them.

Solution: Better physical security.

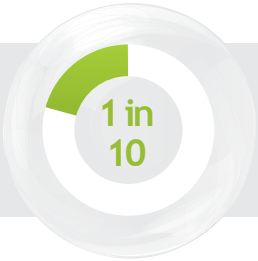
- **This Global Information Assurance Certification paper** details appropriate physical security measures for your computing facility.
- Secure the data itself, via encryption, access control and DLP.

Remote worker security

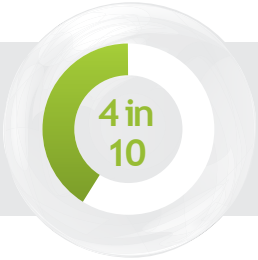
Just because end users know the importance of security when working remotely doesn't mean that they practice it.

According to a **Cisco survey, two thirds of users** said that they were more conscious of security concerns when working remotely, **but 29%** of them used their employers PC for personal ends.

One in 10 users hijacked (borrowed!) a neighbor's wireless Internet connection when working remotely because "they were in a bind", and **18%** of those said that their neighbor didn't know.



Perhaps most alarmingly, almost **4 in 10 users** open emails from unknown senders, with a further **6%** clicking on links and attachments in those emails.



Policies and awareness training should be used to help remote workers work securely.

Unauthorized application usage

The unauthorized use of applications can be a major source of data leakage.

Two thirds of employees use free file sharing platforms to share corporate files, most without alerting their IT departments.

Even when applications have been authorized by an organization, employees may still not be authorized to use them. For example, a low-level worker or a contractor working for a third-party organization should not necessarily have access to sensitive corporate data held on a corporate database.

One of the worst types of unauthorized application use is by former employees.

Companies are often lax in terminating an employee's user account after they leave.

In 2010, former employees at Stens Corporation were **found** to have been using their accounts at the company to access commercial information when working for a competitor.

Ensure that the policy and processes around employees leaving shuts down their account access to all corporate and cloud based applications that the ex-employee would otherwise have access to.

Misuse of passwords

The case highlights yet another data breach vector: misuse of passwords. Walter Puckett and Scott Burgess, the employees indicted for the Stens breach, were able to access their accounts even after managers at the company became suspicious and changed the password. The former employees simply guessed the new ones, which shows just how important proper password management is.

Misusing passwords inside organizations is a key problem for many companies.

Employees will often share passwords for convenience. And up to 45% of people will apparently **give away their password in exchange for a bar of chocolate.**

The Australian arm of Vodafone suffered its own embarrassment, after a journalist **reported** that she was able to log into its customer database using legitimate credentials. The cause? Password sharing among employees.

Solution: Better password management practices, including automation.

This **SANS white paper** on the topic provides some useful pointers.

For every one unfortunate example of data leakage in modern companies, there are tens or even hundreds more. Judicious use of technology and process in an organization will go a long way towards preventing it – but the key is to always be diligent. Unless you keep an eye on them, those data holes have a nasty habit of cropping up.

About Clearswift

Clearswift is an information security company, trusted by thousands of clients worldwide, to provide adaptive cyber solutions that enable their organizations to secure business critical data from internal and external threats.

Built on an innovative Deep Content Inspection engine managed and controlled by a fully integrated policy center, Clearswift's solutions support a comprehensive Information Governance strategy resulting in data being managed and protected effortlessly.

As a global organization, Clearswift operates out of offices in Europe, Australia, Japan and the United States.

Clearswift has a partner network of more than 900 resellers across the globe.

More information is available at **www.clearswift.com**

CLEARSWIFT
ADAPTIVE CYBER PROTECTION

UK - International HQ

Clearswift Ltd
1310 Waterside
Arlington Business Park
Theale
Reading
Berkshire
RG7 4SA

Tel : +44 (0) 118 903 8903
Fax : +44 (0) 118 903 9000
Sales: +44 (0) 118 903 8700
Technical Support:
+44 (0) 118 903 8200
Email: info@clearswift.com

Australia

Clearswift (Asia/Pacific) Pty Ltd
5th Floor
165 Walker Street
North Sydney
New South Wales, 2060
AUSTRALIA

Tel: +61 2 9424 1200
Technical Support:
+61 2 9424 1210
Email: info@clearswift.com.au

Germany

Clearswift GmbH
Landsberger Straße 302
D-80 687 Munich
Germany

Tel: +49 (0)89 904 05 206
Technical Support:
+49 (0)800 1800556
Email: info@clearswift.de

Japan

Clearswift K.K
Shinjuku Park Tower
N30th Floor
3-7-1 Nishi-Shinjuku
Tokyo 163-1030
Japan

Tel: +81 (3)5326 3470
Technical Support:
0066 33 812 501
Email: info.jp@clearswift.com

United States

Clearswift Corporation
309 Fellowship Road, Suite 200
Mount Laurel, NJ 08054
United States

Tel: +1 856-359-2360
Tel (Toll Free): +1 888-937-7938
Technical Support:
+1 856 359 2170
Email: info@us.clearswift.com