



Managing Data & Databases

Session 20
Information Security

Digital Security? Tell me about it...



Giesecke & Devrient



What if these guys get hacked?

Well, they kinda did...

THE // INTERCEPT

[FEATURES](#)

[GREENWALD](#)

[FROOMKIN](#)

[DOCUMENTS](#)

[STAFF](#)

[CONTACT](#)

//



Great retailers?
Well...

10 January 2014 Last updated at 09:26 ET

Share f t

Target data theft affected 70 million customers



The cyber-thieves managed to infiltrate card swipe systems at Target stores

Great retailers?
Well...

MENU

TIME

Subscribe

SIGN IN

Home

U.S.

Politics

World

Business

Tech

Health

Science

Entertainment

Newsfeed

Living

Sports

Data Security

Target Expects \$148 Million Loss from Data Breach

Dan Kedmey

Aug. 6, 2014



The bill comes due for one of the largest security breaches in retail history

Target estimates that losses from a 2013 data breach that compromised credit cards and account information for 40 million shoppers could cost upwards of \$148



Alex Wong—Getty Images

Great retailers?
Well...



The Washington Post

Target data breach victims could get up to \$10,000 each from court settlement



By [Sarah Halzack](#) March 19 at 12:45 PM [Follow @sarahhalzack](#)



How did that happen?

Home Auto Gadgets Hardware Internet IT Science Software Blogs Polls
Submit News



Internet

HVAC Firm at Center of Target Data Breach Also Counts Wal-Mart, Costco as Customers

Jason Mick (Blog) - February 5, 2014 9:35 PM

Print

+1 5

19 comment(s) - last by Samus.. on Feb 8 at 12:16 AM

Access was reportedly given to help power savings, but network wasn't properly isolated from consumer data

It's said that for every \$100 USD spent at retailers via credit card, 5 cents is lost via digital fraud. The [holiday hack of Target Corp. \(TGT\)](#) reminded Americans that this problem was [far from solved](#). And with new details leaking out from the [U.S. Secret Service](#) investigation there's cause for concern that the Target data loss could be just the tip of the iceberg in the attack.



(Source: South Park Studios)

How did that happen?

PCI Data Security Standard – High Level Overview



Build and Maintain a Secure Network and Systems	<ol style="list-style-type: none">1. Install and maintain a firewall configuration to protect cardholder data2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	<ol style="list-style-type: none">3. Protect stored cardholder data4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	<ol style="list-style-type: none">5. Use and regularly update anti-virus software or programs6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	<ol style="list-style-type: none">7. Restrict access to cardholder data by business need-to-know8. Identify and authenticate access to system components9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	<ol style="list-style-type: none">10. Track and monitor all access to network resources and cardholder data11. Regularly test security systems and processes
Maintain an Information Security Policy	<ol style="list-style-type: none">12. Maintain a policy that addresses information security for all personnel

GIZMODO

+ Follow

9

Banks?

Leaked Data From 30,000 Swiss Bank Accounts Reveals Mass Tax Avoidance



Jamie Condliffe

Filed to: LEAKS 2/09/15 6:06am

30 ★



Technology Firms?

nakedsecurity

Award-winning computer security news from **SOPHOS**

malware mac facebook android vulnerability data loss privacy more...

search articles

◀ President Obama orders review of NS... Has Microsoft just PROVED why you s... ▶

Adobe breach THIRTEEN times worse than thought, 38 million users affected

Join thousands of others, and sign up for Naked Security's newsletter


[Don't show me this again](#)

by [Anna Brading](#) on October 30, 2013 | [14 Comments](#)
FILED UNDER: [Adobe](#), [Data loss](#), [Featured](#)

At the start of this month, Adobe [let it slip](#) that it had suffered a data breach.

The attackers had managed to access customers' Adobe IDs, encrypted passwords, names, encrypted debit and credit card numbers, expiry dates and order details.

Brad Arkin, Adobe's Chief Security Officer, [wrote in a blog post](#) at the time:



SOPHOS

60

SECOND COMPLIANCE CHECK

Upcoming EU Data Protection Regulation

See if you are at risk

Governments?

Data lost on 583,000 Canada student loan borrowers

Names, SIN numbers, contact info. missing

The Canadian Press

January 11, 2013

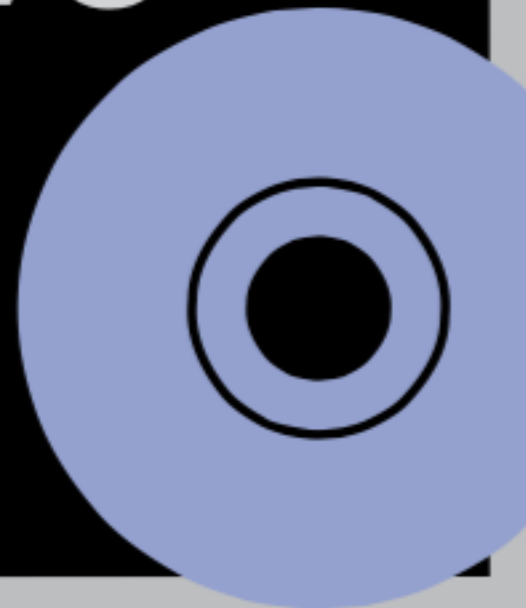
A federal agency has lost a portable hard drive containing personal information about more than half a million people who took out student loans.



Minister Diane Finley (pictured) called the incident "unacceptable and avoidable." (Patrick Doyle/CP)

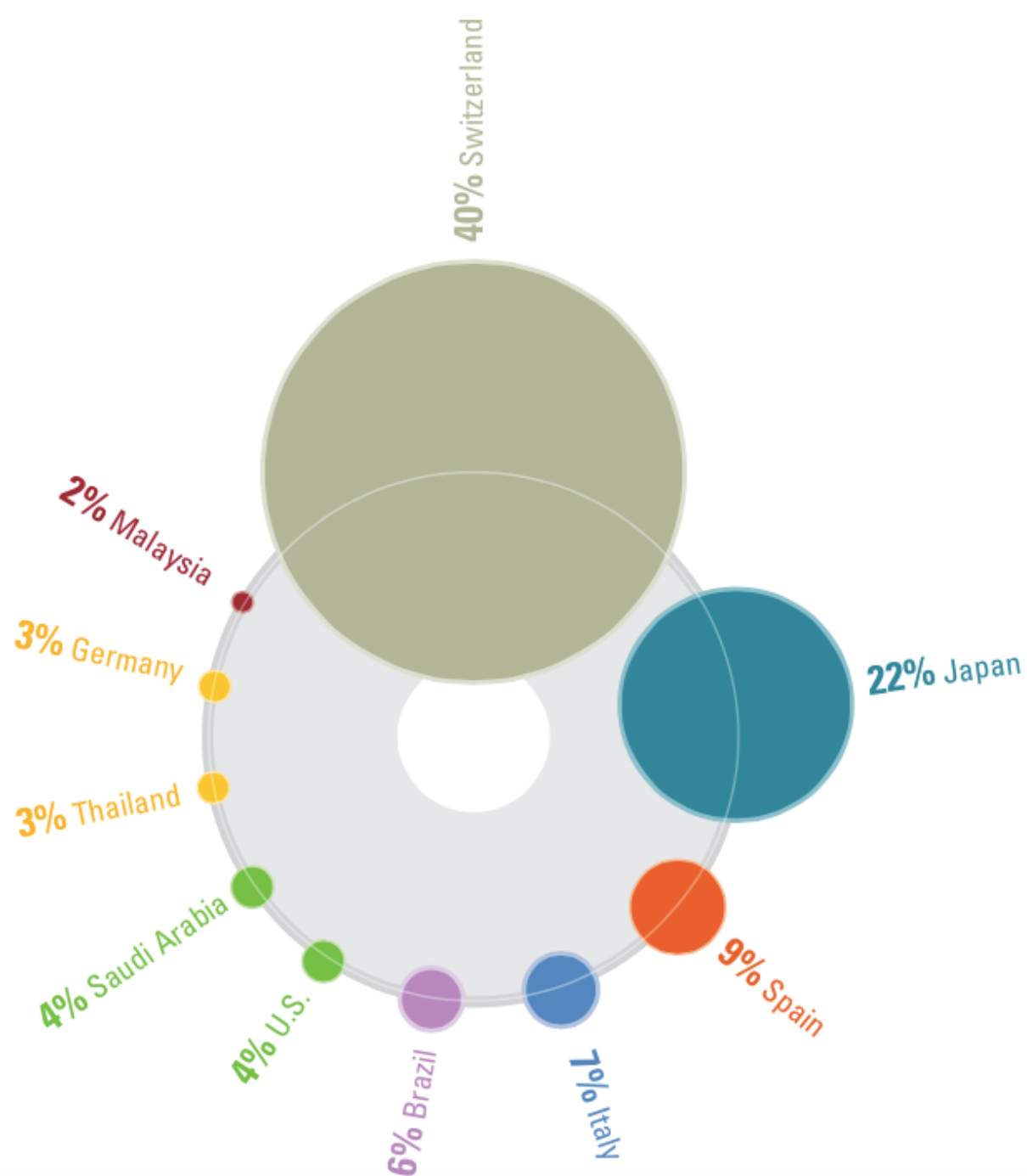
You think it is stupid to lose a hard drive?

Hard Drive
number one
portable media
incident, but a growth
in DVD/CD incidents



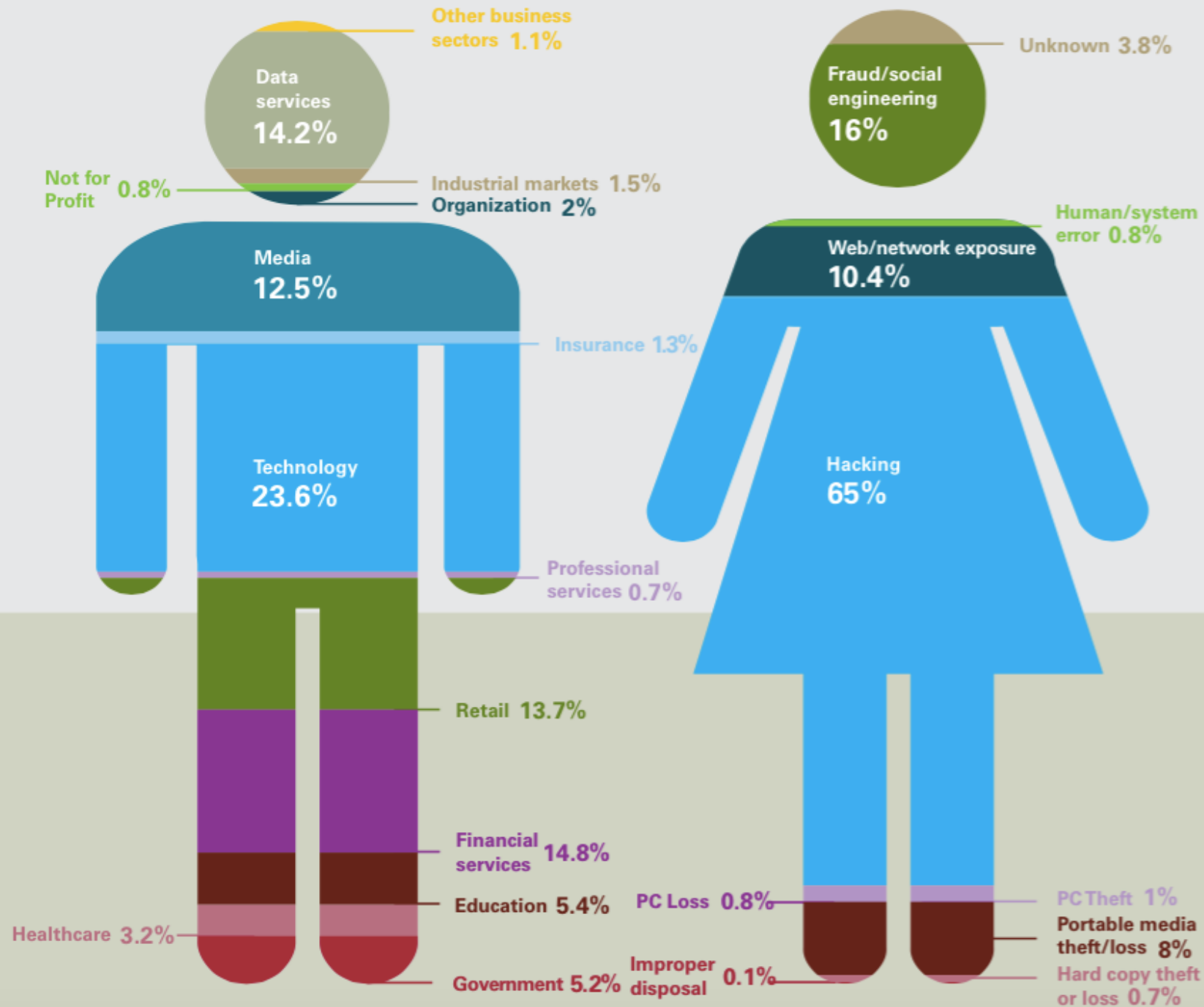
And how bad is the situation?





Where and
how does
that happen?

Where and how does that happen?



How to prevent that?

01

ASSESS

Perform an assessment of your Internet presence.
What data does your organization currently leak to the world?

02

SPRING CLEAN

Where possible, cleanse meta-data from your existing published documents.
Ensure all corporate devices are fully patched, not just your online web servers.

03

EDUCATE “ALL” EMPLOYEES

Everyone in the organization – from the boardroom to the mailroom – must understand the value and sensitivity of the information they possess and, more importantly, how to protect it.

04

ADJUST POLICIES

Instigate a policy to minimize unintentional or undesired corporate information appearing on the Internet.

Does it all come from outside?

Insider attacks: An unappreciated risk

- Why such an increase? (4% in 2007 to 20% in 2010)
 - Increasing complexity of IT
 - Cross-Utilization of computer resources for work and personal matters
 - Social media growth
- And why do they do it?
 - Money? Machivaellianism? Narcissism? Heroism? Whistleblowing?

How to deal with insider threats?

- Adopt a robust insider policy
- Raise awareness.
- Look out for threats when hiring
- Employ rigorous subcontracting processes
- Monitor employees

But companies have
regular information audits,
don't they?

What is the role of the
government?

Some cool insight

[http://www.ted.com/playlists/130/the dark side of data](http://www.ted.com/playlists/130/the_dark_side_of_data)