Privacy and Information Security

What's in it for me?

Fabian Andre Perez
fapv.xc@gmail.com

Agenda

I. Focus on security principles rather than specifics

II. Use common sense rather than technical terms

III. If information is in digital format, it is shockingly easy to reproduce - willingly or not

IV. Regulations, frameworks, standards, ...

V. Information security vs. Risk Management

VI. Risk and value assessment of our activities

VII. Mitigate our risks

VIII. Monitor our controls

IX. Base our decisions on security principles

X. Follow well recognized guidelines

XI. Practical examples

I. Focus on security principles rather than specifics

- Security applies to every individual in a society.

- Security might be seen as an inconvenience...
  - until proven helpful,

    OR
  - until we have to pay for the consequences.
- Security principles and concepts to apply in everyday activities.

II. Use common sense rather than technical terms

- Golden rule:

<u>"always use common sense"</u>

What are the risks and vulnerabilities?

III. If information is in digital format, it is shockingly easy to reproduce

original (analog)

digital versions

III. If information is in digital format, it is shockingly easy to reproduce

		INFORMATION FORMAT	
		ANALOG	**DIGITAL**
INFORMATION CHARACTERISTICS	**ACCESSIBILITY**	extremely hard (usually one at a time)	easy (technical details)
	PRESERVABILITY	extremely hard (ages with time)	easy (technical details)
	REPRODUCIBILITY	not possible (replicas usually expensive)	extremely easy (usually very cheap)
	MODIFIABLE	extremely hard (usually not possible)	easy (technical details)
	SECURABLE	easy (there might be financial considerations)	hard (extremely hard without affecting usability)

NOTE: The more important the information, the more difficult it is to protect it.

IV. Regulations, frameworks, standards, laws...

REGULATION	**FOCUS**	**COMMENT**
COSO	Internal Control	Committee of Sponsoring Organizations of the Treadway Commission
CobiT	IT Governance	Control Objectives for Information and related Technology
ISO 17799/27001	Information Security	International Organization for Standardization
SOX	Financial reporting	Sarbanes & Oxley
HIPAA	Health care information	Health Insurance Portability and Accountability Act
FERPA	student education records	Family Educational Rights and Privacy Act
PCI	Credit Card Information	Payment Card Industry Data Security Standard
BASEL	International banking regulations	
State laws		
Federal laws		

V. Information Security vs. Risk Management

- Perfect security is not achievable
- Instead focus on a:

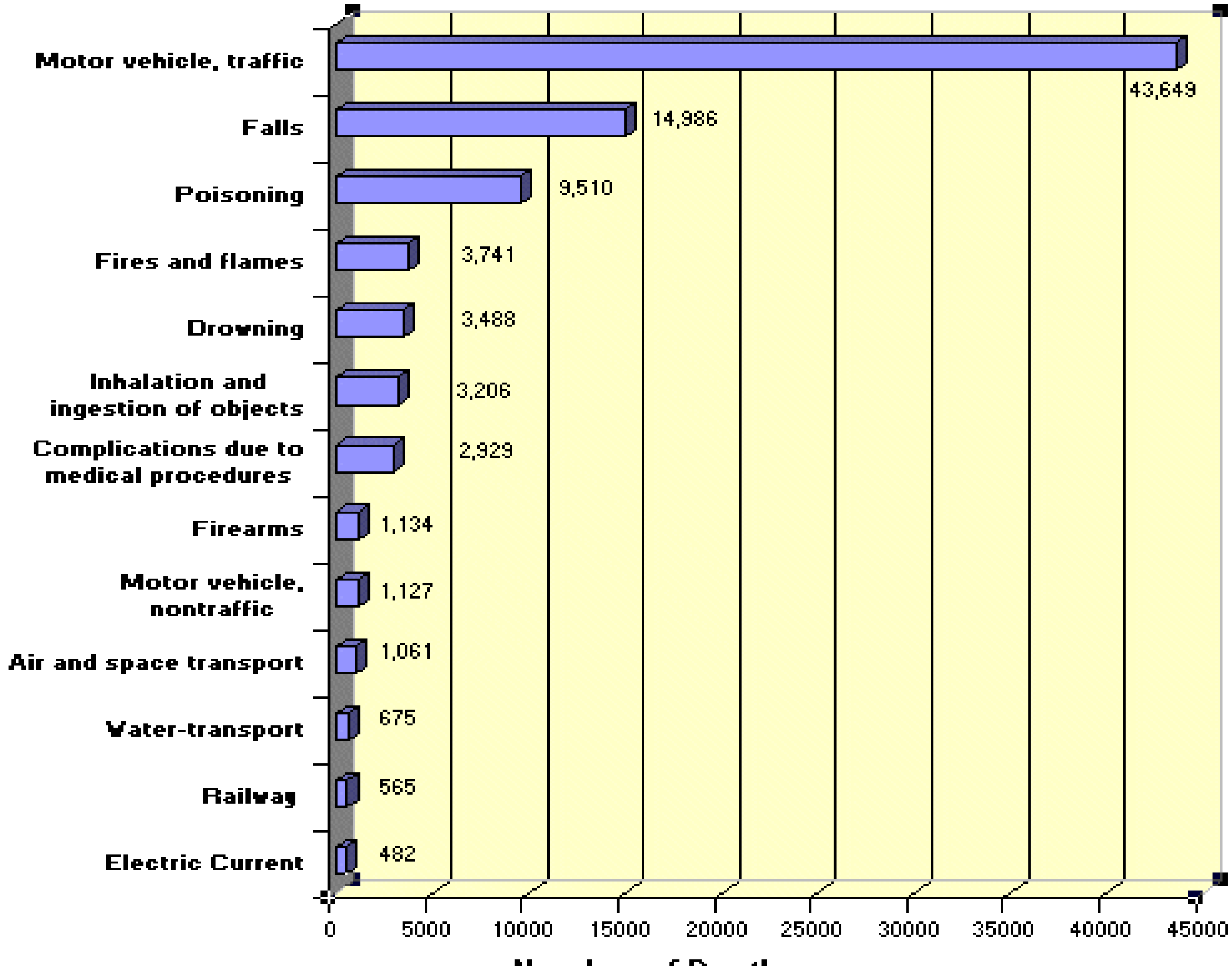
"Reasonable level of security that mitigates the risks to an acceptable level, to a level that we are comfortable to live with"

- How does this apply to our examples...?

VI. Risk and value assessment of our activities

- What is the value of the activities we perform?
- What are the risks of these activities?
- Of these risks:
  - What is their potential impact?
  - and more importantly, what is their probability of occurrence?
- These analyses are critical in order to properly prioritize our activities.

VI. Risk and value assessment of our activities

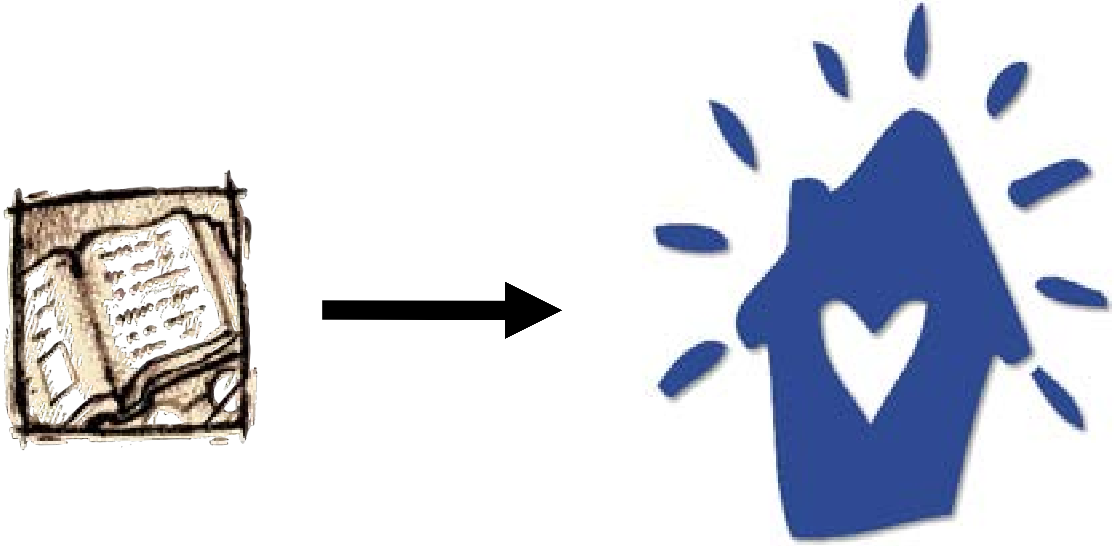


Deaths from Accidents, by Type

Source: U. S. Census Bureau, Statistical Abstract of the United States: 1999, Page 106, table 146. Figures are for 1996, the latest year appearing in the table.

VII. Mitigate our risks

- Apply resources to the activities with highest priority.
- To handle the risk we could:
    - avoid
    - mitigate
    - transfer
    - accept
    - eliminate



VIII. Monitor our controls

“**Control:** The policies, procedures, practices and organizational structures designed to provide reasonable assurance that the business objectives will be achieved and undesired events will be prevented or detected”

Definition by cobitonline

- The success of the controls depends in the ability to “monitor” and learn from them.

VIII. Monitor our controls

Let's review what we have learned:

- Everyday we have to perform a number of activities to comply with our responsibilities.
- These activities always face risks where each risk has a potential impact and a probability of occurrence.
- Based on the value and the risk of the activity we can single out the activities that need attention and we should invest resources in order to mitigate these risks.
- We can accept, avoid, transfer or mitigate the risks, and the actions we perform to mitigate the risks are known as controls.
- The important point about controls is that they should be continuously monitored to get information on how they are performing and what to do to keep the risks at an acceptable level.

IX. Base our decisions on security principles

- Design principles from “The Protection of Information in Computer Systems” by J. Salter and M. Schroeder:
  - *principle of least privilege*
  - *principle of fail-safe defaults*
  - *economy of mechanism*
  - *complete mediation*
  - *open design*
  - *separation of privilege*
  - *least common mechanism*
  - *psychological acceptability*

IX. Base our decisions on security principles

1. The ***principle of least privilege*** states that a subject should be given only those privileges necessary to complete the assigned activity and nothing else.

IX. Base our decisions on security principles

2. The ***principle of fail-safe defaults*** states that a subject should be given only those privileges necessary to complete the assigned activity and nothing else

IX. Base our decisions on security principles

3. The ***principle of economy of mechanism*** states that the activity should be kept as simple as possible. Simpler means less can go wrong, and if anything goes wrong the problems are easier to understand and fix.

IX. Base our decisions on security principles

4. The ***principle of complete mediation*** states that in any activity every action should be checked for proper permission. If permissions change after the first check, unauthorized access might occur.

IX. Base our decisions on security principles

5. The ***principle of open design*** states that security of an activity should not depend on the secrecy of its design or implementation. It should depend on the strength of its design.

IX. Base our decisions on security principles

6. The ***principle of separation of privilege*** states that critical activities must require multiple conditions to grant privilege. This is also known as separation of duty.

IX. Base our decisions on security principles

7. The ***principle of least common mechanism*** states that mechanisms that handle critical information should not be shared.

IX. Base our decisions on security principles

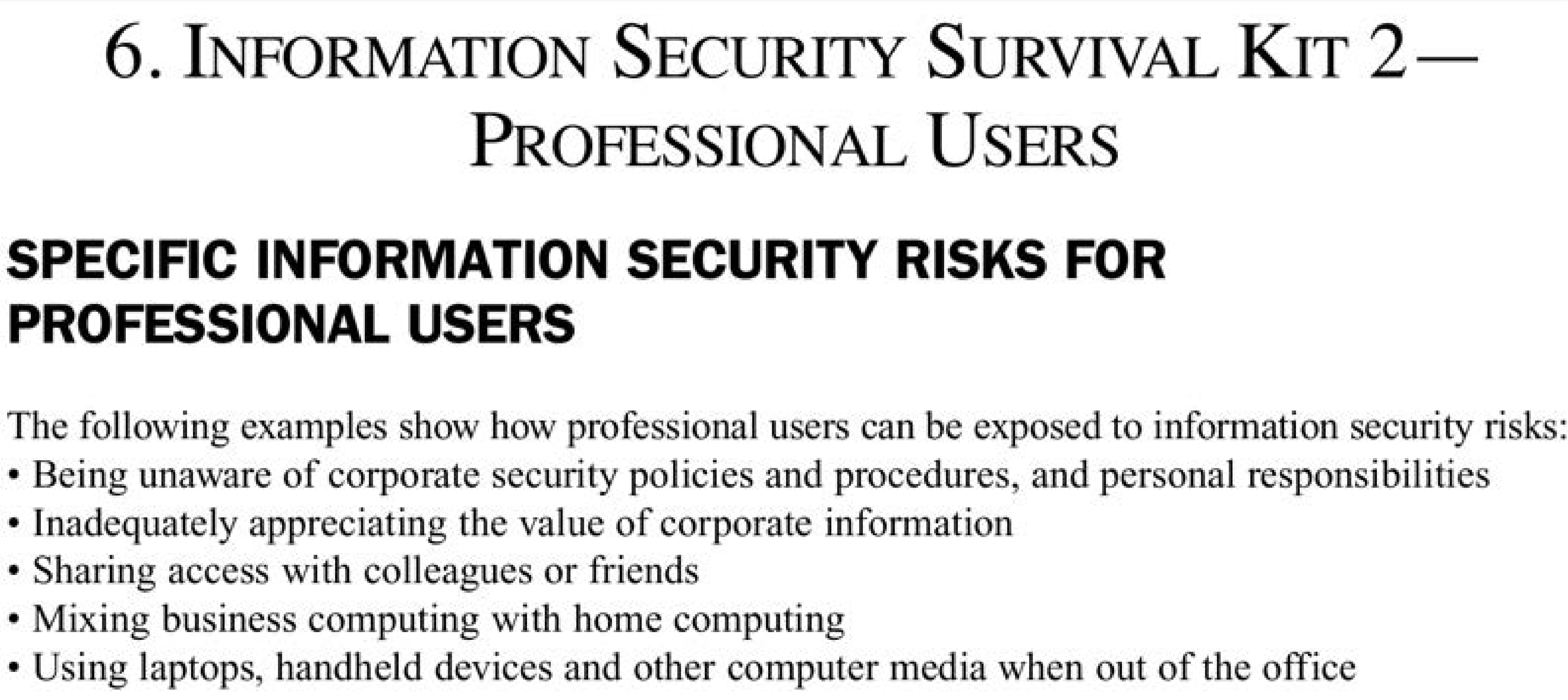
8. The ***principle of psychological acceptability*** states that secure activities should not add difficulty to the actions to access the information.

X. Follow well recognized guidelines

- CobiT security baseline
  - Information Security Survival Kit for:
    - Home Users
    - Professional Users
    - Managers
    - Executives
    - Senior Executives
    - Board of Directors/Trustees

http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=36883&TEMPLATE=/ContentManagement/ContentDisplay.cfm

X. Follow well recognized guidelines



6. Information Security Survival Kit 2—Professional Users

SPECIFIC INFORMATION SECURITY RISKS FOR PROFESSIONAL USERS

The following examples show how professional users can be exposed to information security risks:

- Being unaware of corporate security policies and procedures, and personal responsibilities
- Inadequately appreciating the value of corporate information
- Sharing access with colleagues or friends
- Mixing business computing with home computing
- Using laptops, handheld devices and other computer media when out of the office

http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=36883&TEMPLATE=/ContentManagement/ContentDisplay.cfm

X. Follow well recognized guidelines

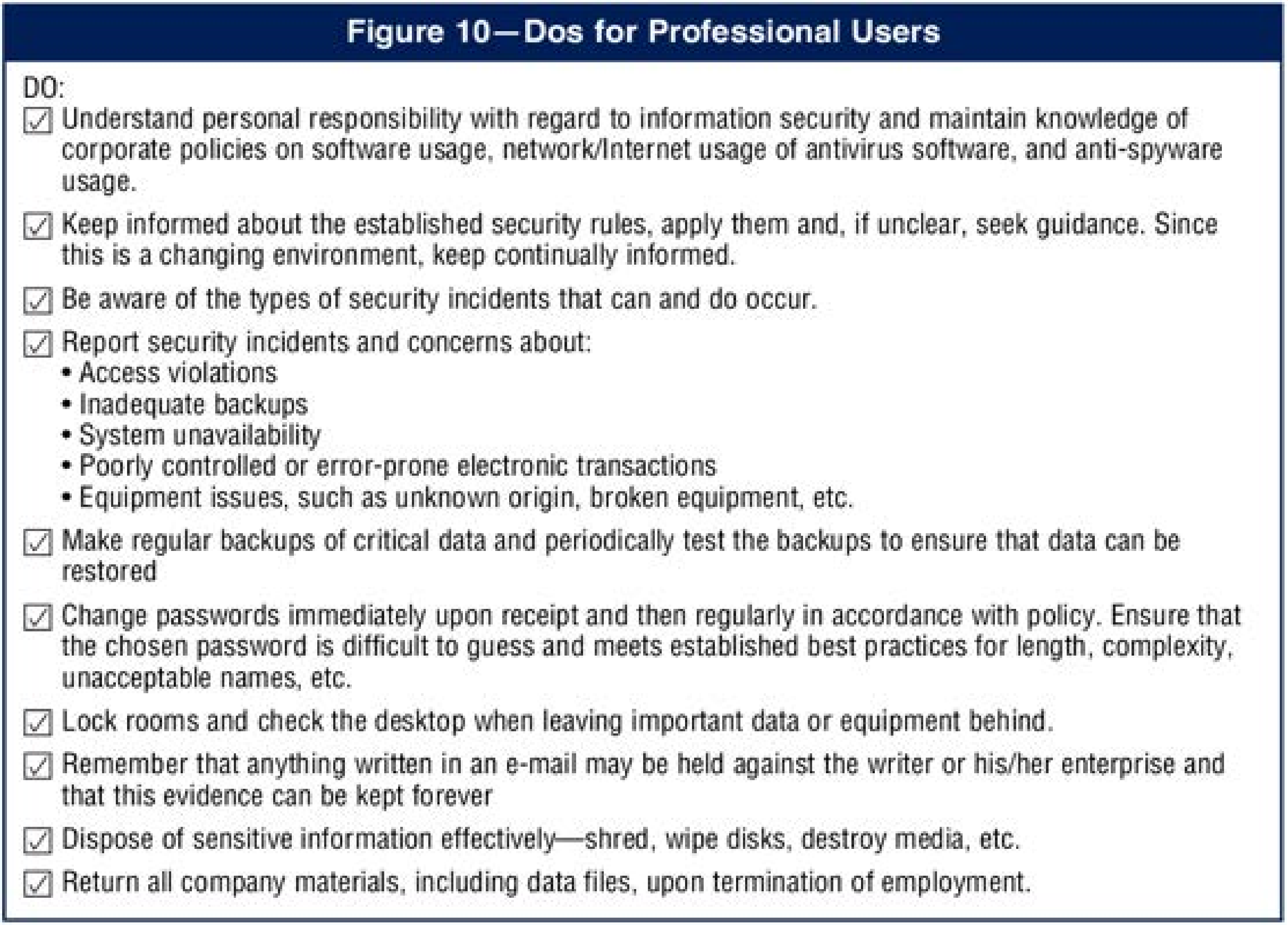


Figure 10—Dos for Professional Users

DO:

☑ Understand personal responsibility with regard to information security and maintain knowledge of corporate policies on software usage, network/Internet usage of antivirus software, and anti-spyware usage.

☑ Keep informed about the established security rules, apply them and, if unclear, seek guidance. Since this is a changing environment, keep continually informed.

☑ Be aware of the types of security incidents that can and do occur.

☑ Report security incidents and concerns about:
- Access violations
- Inadequate backups
- System unavailability
- Poorly controlled or error-prone electronic transactions
- Equipment issues, such as unknown origin, broken equipment, etc.

☑ Make regular backups of critical data and periodically test the backups to ensure that data can be restored

☑ Change passwords immediately upon receipt and then regularly in accordance with policy. Ensure that the chosen password is difficult to guess and meets established best practices for length, complexity, unacceptable names, etc.

☑ Lock rooms and check the desktop when leaving important data or equipment behind.

☑ Remember that anything written in an e-mail may be held against the writer or his/her enterprise and that this evidence can be kept forever

☑ Dispose of sensitive information effectively—shred, wipe disks, destroy media, etc.

☑ Return all company materials, including data files, upon termination of employment.

http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=36883&TEMPLATE=/ContentManagement/ContentDisplay.cfm

X. Follow well recognized guidelines

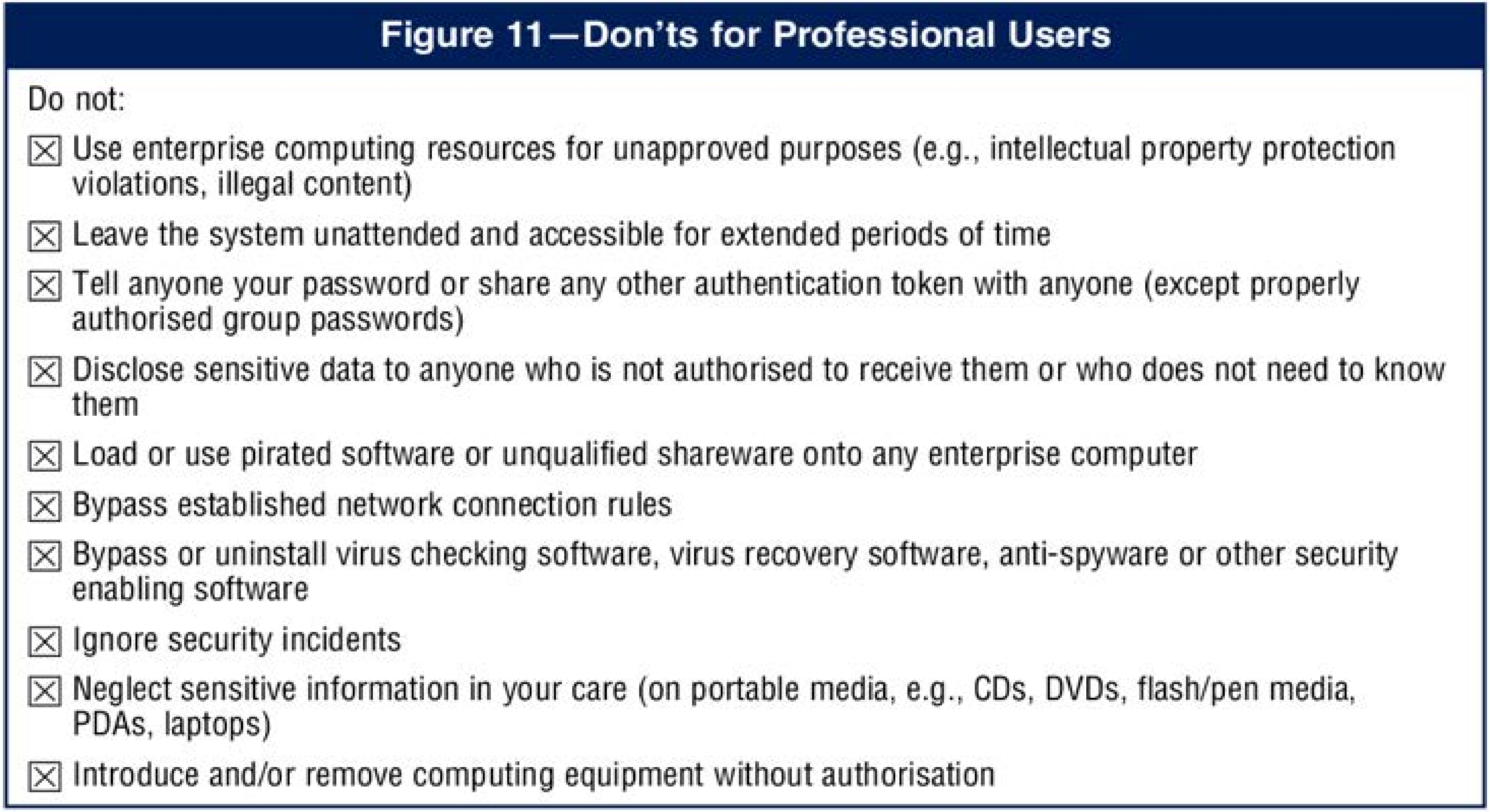


Figure 11—Don’ts for Professional Users

Do not:

☒ Use enterprise computing resources for unapproved purposes (e.g., intellectual property protection violations, illegal content)

☒ Leave the system unattended and accessible for extended periods of time

☒ Tell anyone your password or share any other authentication token with anyone (except properly authorised group passwords)

☒ Disclose sensitive data to anyone who is not authorised to receive them or who does not need to know them

☒ Load or use pirated software or unqualified shareware onto any enterprise computer

☒ Bypass established network connection rules

☒ Bypass or uninstall virus checking software, virus recovery software, anti-spyware or other security enabling software

☒ Ignore security incidents

☒ Neglect sensitive information in your care (on portable media, e.g., CDs, DVDs, flash/pen media, PDAs, laptops)

☒ Introduce and/or remove computing equipment without authorisation

http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=36883&TEMPLATE=/ContentManagement/ContentDisplay.cfm

XI. Practical examples

Example I:

What is the value?

What are the risks?

Potential impact, probability of occurrence

How do we mitigate the risks?

XI. Practical examples

Example II:

What is the value?

What are the risks?

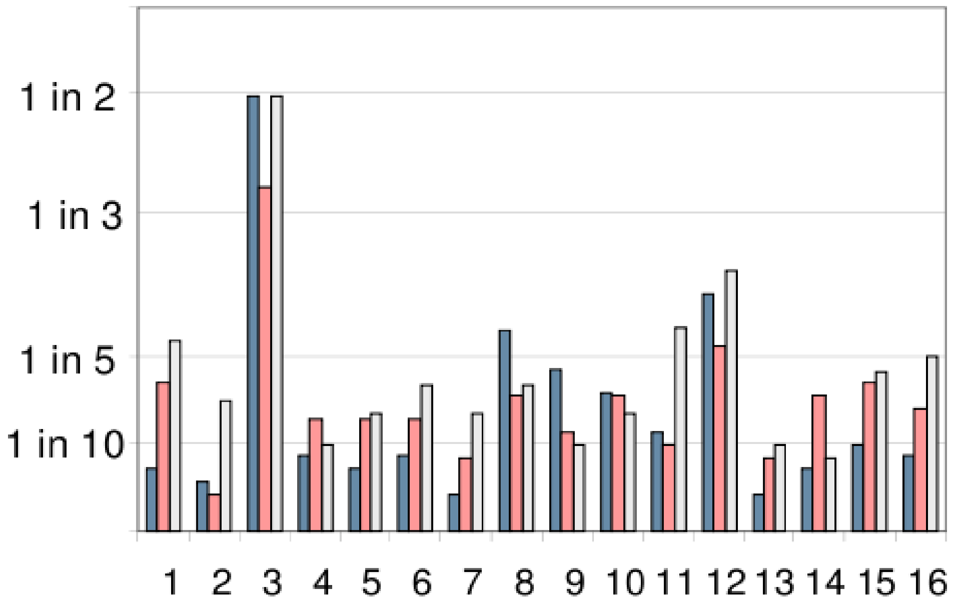
- Potential impact, probability of occurrence

How do we mitigate the risks?

XI. Practical examples

Leading causes of sensitive data loss/theft

- #1: User errors (1 in 2)
- #2: Policy violations (1 in 4)
- #3: Internet threats attacks, hacks (1 in 5)
- #4: Lost or stolen laptops (1 in 7)
- #5: IT vulnerabilities and insufficient IT controls (1 in 7)



🟦 Less than $50 million

🟥 $50 million to $999 million

⬜ $1 billion or more

1: Lost or stolen laptops
2: Improperly disposed computer equipment
3: User errors
4: Transferred backup media
5: Inappropriate access to IT
6: Insufficient controls: business procedures
7: Insufficient controls: IT procedures
8: Internet threats, attacks, hacks
9: Employee fraud
10: Accidental damage to computing equipment
11: Inappropriate use of IT
12: Violation of policies
13: Unauthorized access to IT
14: Insufficient auditing, monitoring, reporting
15: IT vulnerabilities
16: Insufficient IT controls

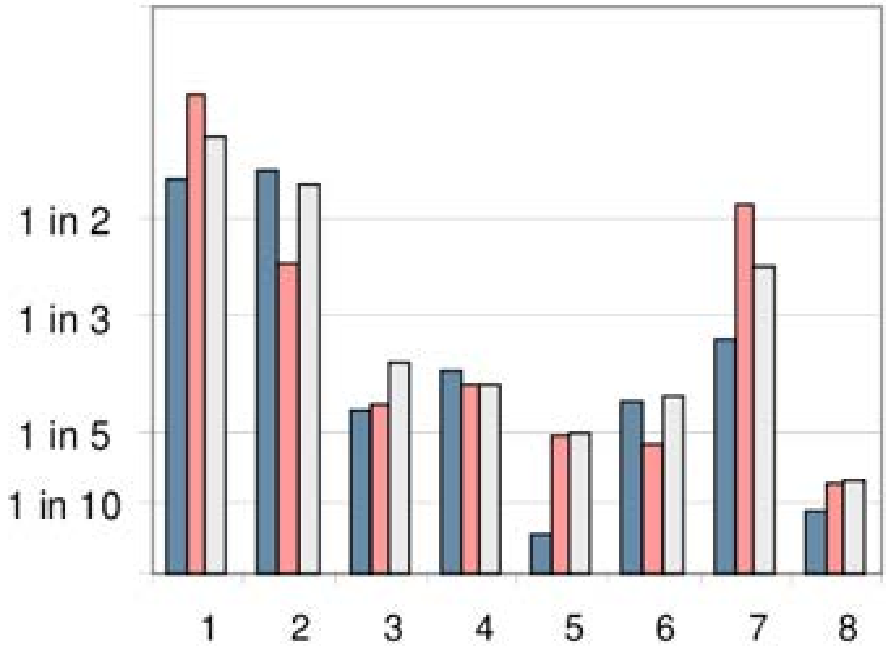
© IT Policy Compliance Group, 2007

Source: IT PCG, 2007 N: 860

XI. Practical examples

Leading conduits for sensitive data loss/theft

- #1: Data residing on PCs, laptops and mobile devices
- #2: Data leaking through Email, Instant Messaging and other electronic channels
- #3: Data accessible through applications and databases



🟦 Less than $50 million

🟥 $50 million to $999 million

⬜ $1 billion or more

1: Data residing on PCs, laptops and other mobile devices
2: Data leaking through Email, IM, and other electronic channels
3: Data residing in centralized storage facilities and devices
4: Data transferred to backup and archive sites
5: Data that has been off-shored or outsourced
6: Data in the hands of business partners and suppliers
7: Data accessible through applications and databases
8: Data in the hands of sales channel partners

© IT Policy Compliance Group, 2007

Source: IT PCG, 2007 N: 860

XI. Practical examples

- In August 2006 Unisys, a subcontractor of the Veterans Affairs, lost a laptop with personal information pertaining to veterans. It included SSN and personal identifiable information; enough information to apply for credit cards, wireless phone accounts, etc. The White House was considering spending $160 million just to monitor whether the lost information would be used for fraud.

http://www.privacyrights.org/ar/VABreach.htm

XI. Practical examples

- T. J. Maxx had a security fiasco that is being estimated to cost $4.5 billion to fix, which will probably increase because T. J. Maxx is the subject of a class action law suit because of this problem.

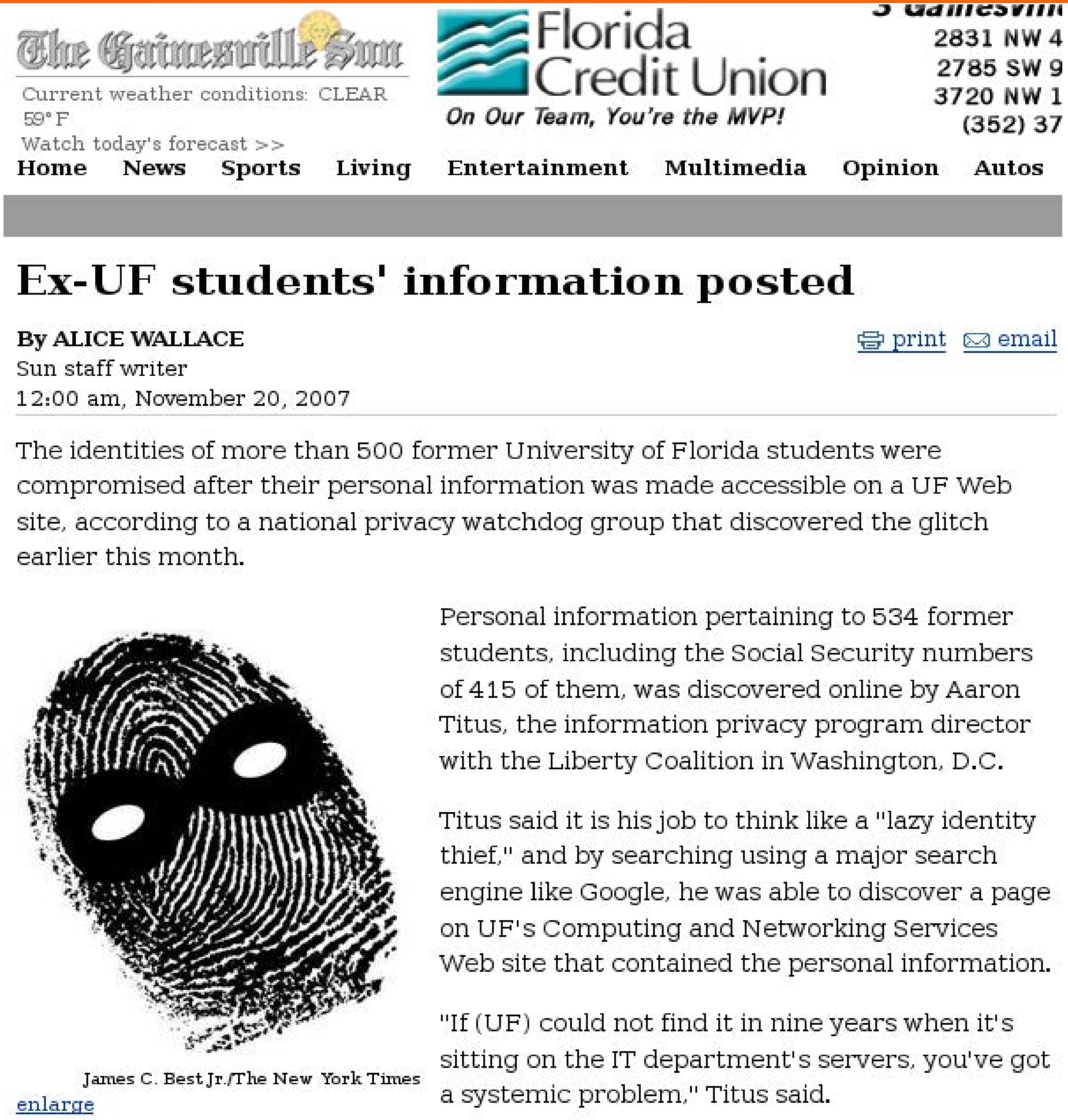
http://www.informationweek.com/news/showArticle

XI. Practical examples

- CardSystems Solutions, a credit card processing company, exposed 40 million debit and credit card accounts; this information could be used for fraud. How much did it cost to fix the problem? Well, let’s answer that saying that CardSystems does not exist anymore.

http://www.wired.com/science/discoveries/news/2(

XI. Practical examples



The Gainesville Sun

Current weather conditions: CLEAR
59° F
Watch today's forecast >>

Ex-UF students' information posted

By ALICE WALLACE
Sun staff writer
12:00 am, November 20, 2007

The identities of more than 500 former University of Florida students were compromised after their personal information was made accessible on a UF Web site, according to a national privacy watchdog group that discovered the glitch earlier this month.

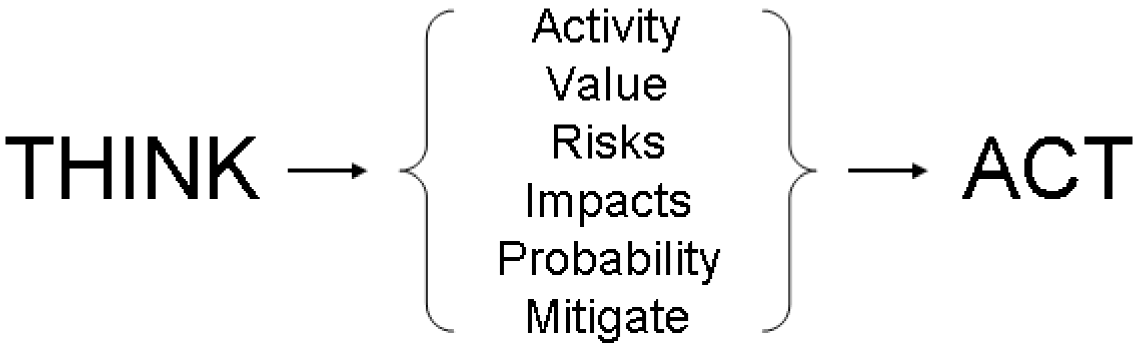
James C. Best Jr./The New York Times

Personal information pertaining to 534 former students, including the Social Security numbers of 415 of them, was discovered online by Aaron Titus, the information privacy program director with the Liberty Coalition in Washington, D.C.

Titus said it is his job to think like a "lazy identity thief," and by searching using a major search engine like Google, he was able to discover a page on UF's Computing and Networking Services Web site that contained the personal information.

"If (UF) could not find it in nine years when it's sitting on the IT department's servers, you've got a systemic problem," Titus said.

Privacy and Information Security, what's in it for me?



THINK →

Activity
Value
Risks
Impacts
Probability
Mitigate

→ ACT

Privacy and Information Security, what's in it for me?

- FERPA Training

http://privacy.health.ufl.edu/training/FERPA/

- HIPAA Training

http://privacy.health.ufl.edu/training/

- UF Information Technology Security Regulations

http://www.it.ufl.edu/policies/security/drafts.html

Privacy and Information Security, what's in it for me?

Q & A

Fabian Andre Perez
fapv.xc@gmail.com
(352)339-4489