

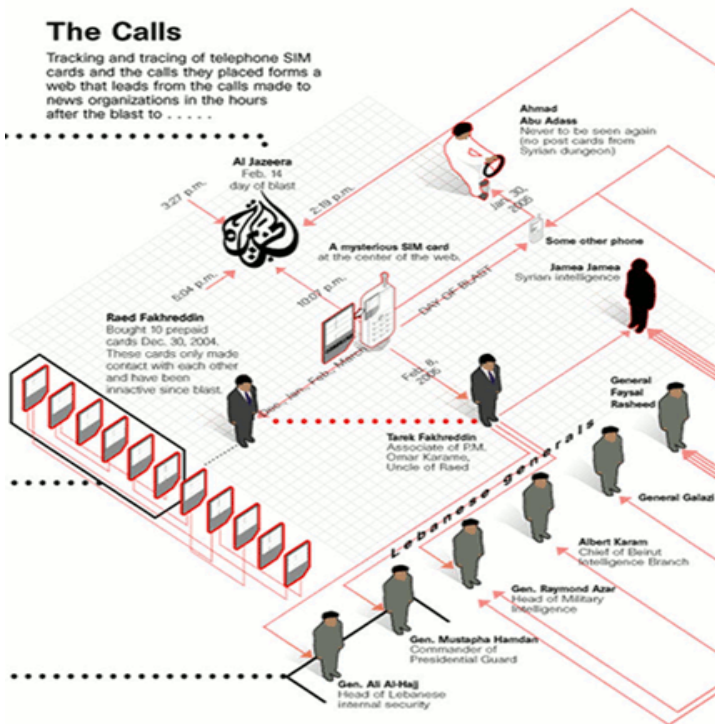
Writing an effective data security procedure in 2 pages or less.

Licensed under the Creative Commons Attribution License
Danny Lieberman
dannyl@controlpolicy.com <http://www.controlpolicy.com/>

Agenda

- Introduction and welcome
- Defining the problem
- Too much choice
- Workplace ethics – the Internet
- AUP
- Enforcement
- Monitoring to reinforce ethical behavior

Defining the problem



- Means
 - Multiple accounts
- Opportunity
 - Multiple channels
- Intent
 - Jérôme Kerviel
 - Albert Gonzales

What employees have

- 1995
 - 1 Company phone
 - 1 Company mail account
 - Mozilla 1.0
- 2009
 - N mobile devices
 - N accounts to M applications
 - Web 2.0

Why too much choice is bad

- Paralysis
- Make worse decisions
- Doing better, feeling worse.



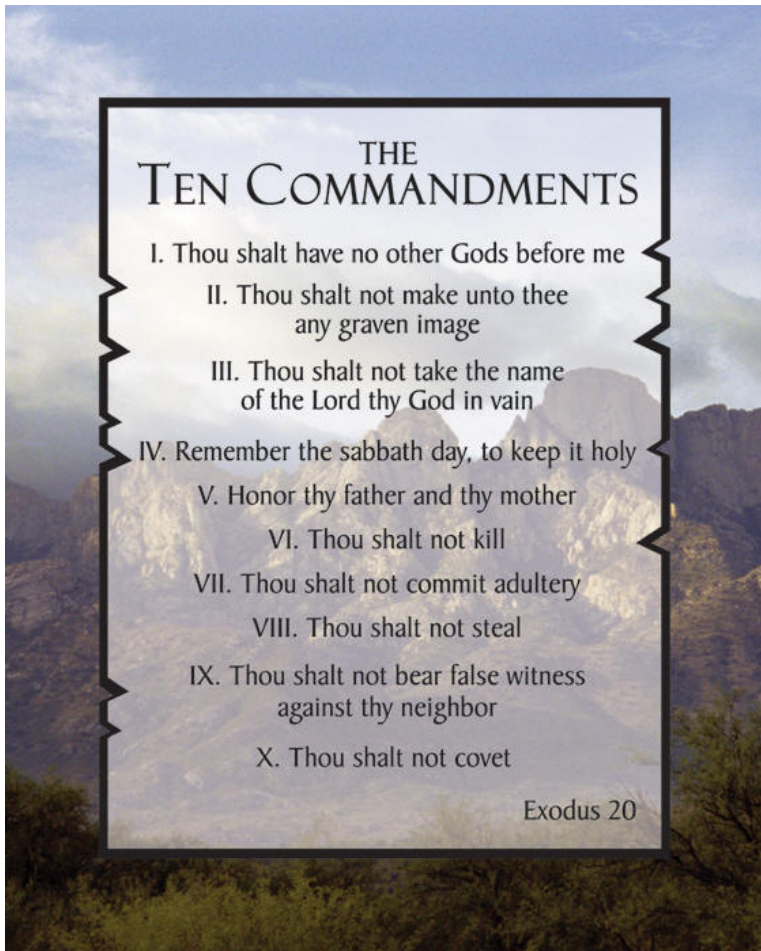
Workplace ethics – the Internet

- **Good**
 - Internet is a great work tool
- **Bad**
 - Time waster
 - Malware
 - Can violate privacy of other employees
 - Sexual harassment suits

Workplace ethics – the Internet

- Ugly
 - Loss of proprietary information
 - Trusted insider theft
 - Mail, Web, IM
 - Smart phones
 - Front-door attacks
 - Lost passwords makes it easy
 - Back-door attacks
 - Spyware, Trojans
 - Piggy back on legit sessions

Acceptable usage policy



- Reduce number of options by default
 - No “opt-in” check box

AUP read and understand agreement

The AUP states that:

- The Internet is to be used to further the company's business and improve customer service and not for personal entertainment or gain
- Protect company assets - physical and digital

Digital Assets

- Any computerized information that the firm uses to compete or accomplish its missions
 - Customer Lists
 - Transaction records
 - Strategic marketing plans
 - Credit cards

Enforcement - management

- Corporate culture
 - *A little fear in the workplace is not a bad idea*
(Andy Grove)
- Everyone signs
- Managers teach

Enforcement – the AUP

- For example:
 - *“The AUP applies to laptops, PDA’s and smart-phones even when you’re out of the office”*
 - No downloads
 - No offensive content
 - Physical, password and email/web security

Enforcement - monitoring

- **Monitoring**
 - Monitor for policy violations
 - To protect staff and customers against unlawful disclosure of personal records
 - Loss/abuse of assets
 - Physical
 - Network

Coming attractions

- Sep 24: Write a 2 page procedure
- Oct 1: Home(land) security
- Oct 8: SME data security
- Oct 15: Business process & security

<http://www.controlpolicy.com/workshops>

Learn more

- Presentation materials and resources
<http://www.controlpolicy.com/workshops/data-security-workshop>
- Includes a sample AUP read and understand agreement in MS Word format.