Ethics and Information Security

BSAD 141
Dave Novak
BDIS 4.1

Topics Covered
- Information ethics
- Information management policies
  - Ethical computer use policy
  - Information privacy policy
  - Acceptable use policy
  - Email privacy policy
  - Social media policy
  - Workplace monitoring policy

“Ethical Dilemmas in this area usually arise not as simple, clear-cut situations but as clashes among competing goals, responsibilities and loyalties.”
BDIS 4.1 Pg 141

“Unfortunately, few hard and fast rules exist for always determining what is ethical”
Pg. 142 BDIS 4.1

Recommendations from Text
- “When in Doubt, Leave it Out”
- Don’t share your Password Hints
- Don’t share your Passwords
- Don’t share info about your finances
- Don’t share your address or phone number
- Don’t share photos of your children
- Don’t share company info
- Don’t share personal conversations

Questions
- Is my email private? Is it the same as a US Mail First Class envelope?
- Can my boss read my email? Can I read my employee’s email?
  - What about after you leave? Who owns the email?
- Can I use Facebook on my work Computer?
- Should I ‘friend’ my boss, co-workers and direct reports?
- Can I access my work files on my home computers?
- Can I use a work web server for a small hobby site to sell works of art?
- What right do I have to edit or filter user generated content on my platform?
- How do I manage my digital reputation?

Ethics and Information
- Individuals form the only ethical component of MIS
  - Software and hardware do not engage in ethical or unethical behavior
  - Information does not care how it is used
    - Will not stop itself from sending spam, viruses, or highly-sensitive information
- Information-based ethical policies therefore focus on the behavior and choices of individuals using various technologies
**Ethics and Information**

- **Ethics** – The principles and standards that guide our behavior toward other people
- **Information ethics** – Govern the ethical and moral issues arising from the development and use of information technologies, as well as the creation, collection, duplication, distribution, and processing of information

**What makes it an Ethical Issue?**

- If an interested party deems a decision or behavior as not conforming to acceptable behavioral principles or standards, it is an ethical issue.
  - This doesn’t tell you what to do...
  - It should motivate you to clarify, codify and disseminate a rationale for the decision or behavior
- Transparency, Clarity and Communication

**Ethics and Information**

- **Ethical Issues**
  - Copying, using, and distributing software
  - Searching organizational databases for sensitive and personal information
  - Creating and/or spreading viruses or other malicious programs
  - Viewing and/or stealing confidential information
  - Destroying information

**Ethics and Information**

- Some business issues related to information ethics
  - Intellectual property
  - Copyright
  - Pirated software
  - Counterfeit software
- Are ethical standards the same across cultures?

**Ethics and Information**

- **Privacy** is a major ethical issue in the US
  - **Privacy** – The right to be left alone when you want to be, to have control over your own personal possessions, and not to be observed without your consent
  - **Confidentiality** – the assurance that messages and information are available only to those who are authorized to view them

**Legal versus Ethical**

<table>
<thead>
<tr>
<th></th>
<th>Ethical</th>
<th>Not Ethical</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal</td>
<td>![Legal]</td>
<td>![Unknown]</td>
</tr>
<tr>
<td>Not Legal</td>
<td>![Unknown]</td>
<td>![Ethical]</td>
</tr>
</tbody>
</table>
Can companies resist wrongdoing in a digital world?

Executive Summary

Rapidly advancing technologies such as big data analytics offer potentially great benefits to companies and consumers, but experts warn that modern technology also has a downside: It can give companies seeking a competitive edge the tools to engage in illegal or unethical practices. Because digital devices—from the sensors and computers that control the inner workings of automobiles to code that tracks individuals’ activities on the Internet—are powered by software that is inherently invisible, consumers and regulators are often in the dark about the data that companies are collecting and how they are using it. Industry groups and outside observers disagree about what should be done. The former argues self-regulation is sufficient while the latter seeks tough regulation and increased ethics training in business schools and companies. Among the questions being debated: Should the uses of big data be more tightly controlled? Should there be limits on employers’ monitoring of employees? Is software too open to abuse?

UVM’s Code of Conduct and Ethical Standards


Organizational Information Management Policies

- Organizations strive to build a corporate culture based on ethical principles that employees can understand and implement
  - 1) Computer use policy
  - 2) Information privacy policy
  - 3) Acceptable use policy
  - 4) Email privacy policy
  - 5) Social media policy
  - 6) Workplace monitoring policy

1) Computer Use Policy

- General principles to guide computer user behavior
- The ethical computer user policy ensures:
  - all users are informed of the rules, and
  - by agreeing to use the system on that basis, consent to abide by the rules

Computer Use Policy

- Important to understand that when you sign a computer use policy, you are verifying (from a legal standpoint) that you UNDERSTAND the policy and agree to abide by that policy (CONSENT)

Articles


2) Information Privacy Policy

- General principles regarding information privacy
- The unethical use of information typically occurs "unintentionally" when it is used for new purposes
- Who decides how an organization uses information and exactly what information they use?

3) Acceptable Use Policy

- Set of rules that restrict how a particular technological resource may be used
- Requires a user to agree to follow the policy to access to the resource (corporate email, information systems, and the Internet)
- Nonrepubidation — A contractual stipulation to ensure that ebusiness participants do not deny their online actions

UVM Computer, Communication, and Network Technology Acceptable Use

- Can you use your UVM account, webspace, email, or any UVM resource for private enterprise or private (non-uvm) fund raising?
  - No Personal Financial Gain: Users agree not to use computers, network connections and accounts, or other information and communication technology services for the operation of private enterprises or the private fund-raising.
  - What consequences are there to violating any of this policy?
  - Enforcement: Users understand that violations of this Policy may result in suspension or termination of access to UVM’s network or to services available through that network and may result in disciplinary action including academic expulsion, employment termination, or criminal prosecution.
  - When did you agree to this policy?

4) Email Privacy Policy

- Details the extent to which email messages may be read by others
- Organizations can mitigate the risks of email and instant messaging communication tools by implementing and adhering to an email privacy policy
- Extends well beyond spam…
4) Email Privacy Policy


Email Disclaimers

- Applicability – “On the Whole, they ain’t worth much.”
  - There are Exceptions …
  
  http://fortune.com/2013/10/15/the-short-history-of-email-disclaimers/
  
  A better analogy might be suspenders with no pants. Many disclaimers — particularly of the “This is confidential. Do not forward. Delete and return to sender” variety — are simply one-sided contracts. Without prior agreement from the other side, they’re unenforceable.

5) Social Media Policy

- Guidelines or principles governing employee online communications — extends beyond email
- There is no such thing as a private or truly restricted social media site

Facebook Policy at UVM

- Is it acceptable for me to be on Facebook in my office during work hours using UVM computing equipment and UVMs network?
- What options do organizations have to institute and enforce policies around issues like this?
- Am I allowed to use Facebook for UVM related purposes?
- Should I ‘friend’ students taking my classes?
5) Social Media Policy

1. “Some subjects can invite a flame war. Be careful discussing things where emotions run high (e.g. politics and religion) and show respect for others’ opinions.”
2. “Your job comes first. Unless you are an authorized Social Media Manager, don’t let social media affect your job performance.”
3. “If you #!%#@# up? Correct it immediately and be clear about what you’ve done to fix it. Contact the social media team if it’s a real doozy.”
4. “Don’t even think about it…. Talking about financial information, sales trends, strategies, forecasts, legal issues, future promotional activities. Giving out personal information about customers or employees. Posting confidential or non-public information. Responding to an offensive or negative post by a customer. There’s no winner in that game.”

Source: http://blog.hirerabbit.com/5-terrific-examples-of-company-social-media-policies/

---

5) Social Media Policy

1. HP promotes healthy and honest discourse with its readers.
2. The company reserves the right to edit or amend any misleading or inaccurate content depicted in blog posts. The company also reserves the right to delete blog posts violating the code of conduct.
3. HP values, respects, and upholds the intellectual property rights of its bloggers.

Source: http://blog.hirerabbit.com/5-terrific-examples-of-company-social-media-policies/

---

6) Workplace Monitoring Policy

- Addresses organization’s policies regarding monitoring employee behavior both in and out of work
- The dilemma surrounding employee monitoring in the workplace is that an organization is placing itself at risk if it fails to monitor its employees; however, some people feel that monitoring employees is unethical or goes “too far”

---

6) Workplace Monitoring Policy

- Employee monitoring policy – Explicitly state how, when, and where the company monitors its employees
  - Key logger or key trapper software
  - Cookie
  - Adware
  - Spyware
  - Web log
  - Clickstream

---

6) Workplace Monitoring Policy

According to new data, nearly 80 percent of major companies now monitor employees’ use of e-mail, Internet or phone. That’s per the American Management Association, which conducts an annual survey of workplace

The figure represents a sharp rise from 1997 when only 35 percent of companies kept tabs on their workers. And the increase comes while the percentage of workers with access to office e-mail and Internet remained virtually unchanged.

The AMA study, while not representative of all workplaces, focused on 1,627 large and mid-sized firms among its members and clients which together employ over a quarter of the U.S. work force.
6) Workplace Monitoring Policy

- What can my employer monitor?
  - [https://www.privacyrights.org/fs/fs7-work.html#2a](https://www.privacyrights.org/fs/fs7-work.html#2a)

Summary

- Overview of information ethics
- Information management policies
  - Ethical computer use policy
  - Information privacy policy
  - Acceptable use policy
  - Email privacy policy
  - Social media policy
  - Workplace monitoring policy