Remote Learning of Ethical Decision-Making in Cybersecurity

Gedare Bloom
Assistant Professor
Department of Computer Science
University of Colorado Colorado Springs

February 16, 2021

This material was developed by Gedare Bloom, Ph.D., and is intended for classroom discussion rather than to illustrate effective or ineffective handling of administrative, ethical, or legal decisions by management. No permission or compensation is needed for classroom use as long as it is acknowledged to be the creative work of the author and the UCCS Daniels Fund Ethics Initiative. For public action or electronic posting, please contact the UCCS Daniels Fund Ethics Initiative Collegiate Program at UCCS College of Business at 1-719-255-5168. (2021)
Connecting the dots...

**Ethics**

Ethics are the principles you hold that guide your behavior and decisions.

- Strong ethics help make good decisions in new situations.
- An **ethical situation** occurs when a decision’s outcome may cause harm to someone or something.
  - An **ethical dilemma** is when no decision is harmless.

**Cybersecurity**

Cybersecurity is the field of practice that protects computer system data, information, and functionality from harm.

- A **harm** is a negative consequence to an asset: information/resource with value.
- An **attack** is the act of causing harm by exploiting a vulnerability.
- A **vulnerability** is an aspect of a system that can cause it to behave incorrectly.
Connecting the dots...
Ethics and Cybersecurity are Strongly Related

Ethics

Ethics are the principles you hold that guide your behavior and decisions.

• Strong ethics help make good decisions in new situations.

An ethical situation occurs when a decision’s outcome may cause harm to someone or something.

• An ethical dilemma is when no decision is harmless.

Cybersecurity

Cybersecurity is the field of practice that protects computer system data, information, and functionality from harm.

• An attack is the act of causing harm by exploiting a vulnerability.

• A vulnerability is an aspect of a system that can cause it to behave incorrectly.

Attacks create ethical situations by causing harm
Suppose Penny discovers a vulnerability in a software product used in many computer systems.

Penny has an *obligation* not to exploit that vulnerability

- Could face legal consequences

Penny also has a *decision* whether or not to *disclose* that vulnerability

- Could tell the software product vendor
- Could tell the world
- Could tell nobody

**Vulnerabilities also Cause an Ethical Situation**
Ethical Situation: Disclosure

Could tell the software product vendor

The vendor may fix it, and thereby prevent harm from coming.
The vendor may do nothing about it, and thereby allow harm to come.
Ethical Situation: Disclosure

Could tell the software product vendor
The vendor may fix it, and thereby prevent harm from coming.
The vendor may do nothing about it, and thereby allow harm to come.

Could tell the world
Raise awareness of it; may encourage the vendor/others to fix it and prevent harm.
Facilitates adversaries to exploit it and allow harm.
Ethical Situation: Disclosure

Could tell the software product vendor
The vendor may fix it, and thereby prevent harm from coming.
The vendor may do nothing about it, and thereby allow harm to come.

Could tell the world
Raise awareness of it; may encourage the vendor/others to fix it and prevent harm.
Facilitates adversaries to exploit it and allow harm.

Could tell nobody
If no one knows about it, no one can exploit it, so may avoid harm.
Adversaries may already know it or find it independently, so may allow harm.
Ethical Situation: Disclosure

Could tell the software product vendor

- The vendor may fix it, and thereby prevent harm from coming.
- The vendor may do nothing about it, and thereby allow harm to come.

Could tell the world

- Raise awareness of it; may encourage the vendor/others to fix it and prevent harm.
- Facilitates adversaries to exploit it and allow harm.

Could tell nobody

- If no one knows about it, no one can exploit it, so may avoid harm.
- Adversaries may already know it or find it independently, so may allow harm.

Vulnerability disclosure is an ethical dilemma
## Stacking up disclosure models with DFEI principles

<table>
<thead>
<tr>
<th>Disclosure Model</th>
<th>Private</th>
<th>Public</th>
<th>Non</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Integrity</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Act with honesty in all situations</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Trust</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Build trust in all stakeholder relationships</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Accountability</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accept responsibility for all decisions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Transparency</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maintain open and truthful communications</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Fairness</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Engage in fair competition and create equitable and just relationships</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Respect</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Honor the rights, freedoms, views, and property of others</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Rule of Law</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comply with the spirit and intent of laws and regulations</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Viability</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create long-term value for all relevant stakeholders</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Stacking up disclosure models with DFEI principles

<table>
<thead>
<tr>
<th>Disclosure Model</th>
<th>Private</th>
<th>Public</th>
<th>Non</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrity</td>
<td>✓</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>Trust</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Accountability</td>
<td>x</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>Transparency</td>
<td>?</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>Fairness</td>
<td>x</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>Respect</td>
<td>✓</td>
<td>x</td>
<td>?</td>
</tr>
<tr>
<td>Rule of Law</td>
<td>✓</td>
<td>?</td>
<td>✓</td>
</tr>
<tr>
<td>Viability</td>
<td>✓</td>
<td>✓</td>
<td>x</td>
</tr>
</tbody>
</table>
Responsible (Coordinated) Disclosure

Model for cybersecurity researchers (aka ethical hackers*) to engage with vendors:

1. Independent researcher discovers a vulnerability

2. The researcher privately discloses the vulnerability to the vendor, with a timeline
   Allows vendor time to address a security vulnerability
   Often between 3-6 months from date of disclosure

3. If not fixed in time, the researcher publicly discloses the vulnerability.

Premise is to hold vendors accountable for security problems.

*You may see ethical hackers referred to as “white hat” or “gray hat” hackers. These terms should be avoided as they connote a negative color-based association that has racial overtones. [https://www.acm.org/diversity-inclusion/words-matter](https://www.acm.org/diversity-inclusion/words-matter)
Mallory discovers a bug that reveals shopping cart contents and shipping (not billing) info

- Sends detailed report to the vendor
- Gets an ack and a case manager POC
What Went Wrong? Is anyone at fault?

9 Mar.
Mallory discovers a bug that reveals shopping cart contents and shipping (not billing) info
- Sends detailed report to the vendor
- Gets an ack and a case manager POC

4 May
The vulnerability still exists, so Mallory asks for an update.
- A different case manager responds that he is requesting an update from product team.

10 Apr.
The case manager reaches out to confirm the bug.

10 June
Mallory requests an update. The case manager says the bug has been deemed not severe enough to fix urgently and was closed by the product team.

7 June
Mallory publishes a blog post explaining the vulnerability.

24 June
Mallory finds out cyber-criminals are exploiting the vulnerability to harvest and sell customer data.

So far, so good
Lack of trust?
Lack of accountability?

Loss of transparency
<table>
<thead>
<tr>
<th>Disclosure Model</th>
<th>Private</th>
<th>Public</th>
<th>Non</th>
<th>Responsible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrity</td>
<td>✅️</td>
<td>✅️</td>
<td>✗</td>
<td>✗️</td>
</tr>
<tr>
<td>Trust</td>
<td>✗️</td>
<td>✗️</td>
<td>✗️</td>
<td>✗️</td>
</tr>
<tr>
<td>Accountability</td>
<td>✗️</td>
<td>✅️</td>
<td>✗️</td>
<td>✗️</td>
</tr>
<tr>
<td>Transparency</td>
<td>✗️?</td>
<td>✅️</td>
<td>✗️</td>
<td>✗️</td>
</tr>
<tr>
<td>Fairness</td>
<td>✗️</td>
<td>✅️</td>
<td>✗️</td>
<td>✗️</td>
</tr>
<tr>
<td>Respect</td>
<td>✅️</td>
<td>✗️</td>
<td>✗️</td>
<td>✗️</td>
</tr>
<tr>
<td>Rule of Law</td>
<td>✅️</td>
<td>✗️?</td>
<td>✗️</td>
<td>✅️</td>
</tr>
<tr>
<td>Viability</td>
<td>✅️</td>
<td>✅️</td>
<td>✗️</td>
<td>✗️</td>
</tr>
</tbody>
</table>
### How fares Responsible (Coordinated) Disclosure?

<table>
<thead>
<tr>
<th>Disclosure Model</th>
<th>Private</th>
<th>Public</th>
<th>Non</th>
<th>Responsible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrity</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Trust</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Accountability</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Transparency</td>
<td>?</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Fairness</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Respect</td>
<td>✓</td>
<td>✗</td>
<td>?</td>
<td>✓</td>
</tr>
<tr>
<td>Rule of Law</td>
<td>✓</td>
<td>?</td>
<td>✓</td>
<td>?</td>
</tr>
<tr>
<td>Viability</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
</tr>
</tbody>
</table>
Online Learning of Ethical Cybersecurity

Platform Design
Cloud-based Own Moodle LMS
   Like Canvas/Blackboard, but free
   Allow students to self-enroll
Model after online training software
   CITI, Skillsoft, etc.
Responsible Disclosure “Course”
   Overview, Case Studies, Quizzes
Other courses possible in future
   Certified Ethical Hacker curriculum?

Implementation Progress
Moodle installed in local VM
   Linux, Apache, mySQL, PHP (LAMP)
Basic site created
   1 admin, 1 instructor, 2 “students”
   No external access yet
   After content created, will migrate to cloud
Disclosure course design in progress
   Expect to test in late March when my class (CS 4980/5980: System Security) covers responsible disclosure
Demo

Video next slide
Learn More

Daniels Fund Ethics Initiative
https://www.danielsfund.org/ethics/overview
https://business.uccs.edu/resources/ethics

Disclosure
https://iamthecavalry.org/about/disclosure/
https://googleprojectzero.blogspot.com/

About Me
https://gedare.github.io