

# Remote Learning of Ethical Decision-Making in Cybersecurity

Gedare Bloom

Assistant Professor

Department of Computer Science  
University of Colorado Colorado Springs

*February 16, 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.

### Cybersecurity

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

## Attacks create ethical situations by causing harm

- 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.
- 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.

# Vulnerabilities also Cause an Ethical Situation

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

# Ethical Situation: Disclosure

Could tell the software product vendor

Private Disclosure

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

Private Disclosure

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

Public/Full Disclosure

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

Private Disclosure

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

Public/Full Disclosure

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

Non-Disclosure

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

Private Disclosure

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

Public/Full Disclosure

Vulnerability disclosure is an **ethical dilemma**

Could tell nobody

Non-Disclosure

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.



# Stacking up disclosure models with DFEI principles

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

# Stacking up disclosure models with DFEI principles

Disclosure Model	Private	Public	Non
Integrity	✓	✓	✗
Trust	✗	✗	✗
Accountability	✗	✓	✗
Transparency	?	✓	✗
Fairness	✗	✓	✗
Respect	✓	✗	?
Rule of Law	✓	?	✓
Viability	✓	✓	✗

# 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.*

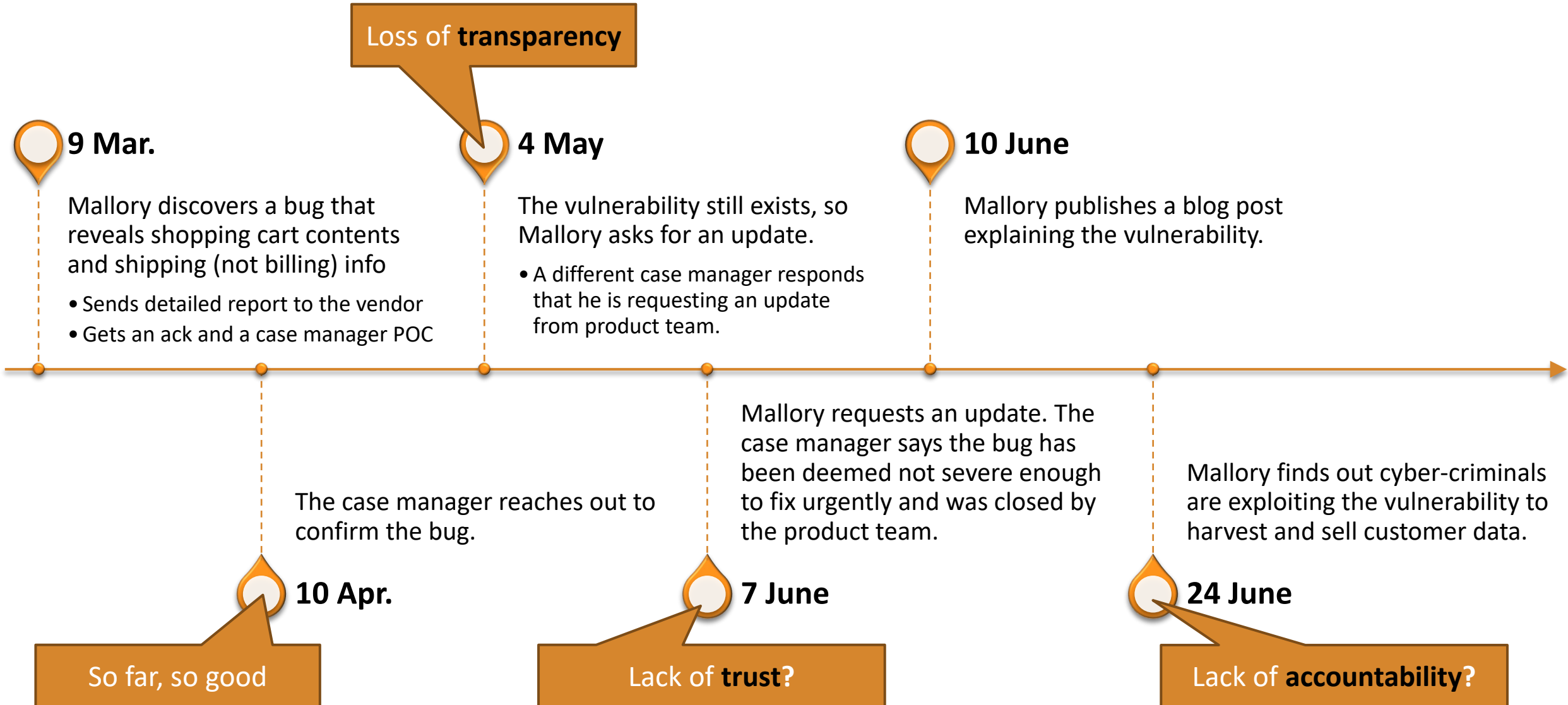
# Responsible Disclosure Can Go Badly (Case)

 **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

# What Went Wrong? Is anyone at fault?



# How fares Responsible (Coordinated) Disclosure?

Disclosure Model	Private	Public	Non	Responsible
Integrity	✓	✓	✗	
Trust	✗	✗	✗	
Accountability	✗	✓	✗	
Transparency	?	✓	✗	
Fairness	✗	✓	✗	
Respect	✓	✗	?	
Rule of Law	✓	?	✓	
Viability	✓	✓	✗	

# How fares Responsible (Coordinated) Disclosure?

Disclosure Model	Private	Public	Non	Responsible
Integrity	✓	✓	✗	✓
Trust	✗	✗	✗	✓
Accountability	✗	✓	✗	✓
Transparency	?	✓	✗	✓
Fairness	✗	✓	✗	✓
Respect	✓	✗	?	✓
Rule of Law	✓	?	✓	?
Viability	✓	✓	✗	✓

# 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>



# DANIELS FUND ETHICS INITIATIVE

## PRINCIPLES

### *Integrity*

Act with honesty in all situations

### *Trust*

Build trust in all stakeholder relationships

### *Accountability*

Accept responsibility for all decisions

### *Transparency*

Maintain open and truthful communications

### *Fairness*

Engage in fair competition and create equitable and just relationships

### *Respect*

Honor the rights, freedoms, views, and property of others

### *Rule of Law*

Comply with the spirit and intent of laws and regulations