Teaching Resources for Cybersecurity Code of Honor

Discussion Questions and Additional Case Studies

Dr. James Tippey

Contents

[Chapter 1 3](#_Toc151389551)

[**Discussion Questions** 3](#_Toc151389552)

[Chapter 2 6](#_Toc151389553)

[**Discussion Questions** 6](#_Toc151389554)

[**Case Study** 8](#_Toc151389555)

[Chapter 3 10](#_Toc151389556)

[**Discussion Questions** 10](#_Toc151389557)

[**Case Study** 12](#_Toc151389558)

[Chapter 4 14](#_Toc151389559)

[**Discussion Questions** 14](#_Toc151389560)

[**Case Study** 17](#_Toc151389561)

[Chapter 5 19](#_Toc151389562)

[**Discussion Questions** 19](#_Toc151389563)

[**Case Study** 22](#_Toc151389564)

[Chapter 6 24](#_Toc151389565)

[**Discussion Questions** 24](#_Toc151389566)

[**Case Study** 27](#_Toc151389567)

[Chapter 7 29](#_Toc151389568)

[**Discussion Questions** 29](#_Toc151389569)

[**Case Study** 32](#_Toc151389570)

[Chapter 8 34](#_Toc151389571)

[**Discussion Questions** 34](#_Toc151389572)

[**Case Study** 37](#_Toc151389573)

[Chapter 9 39](#_Toc151389574)

[**Discussion Questions** 39](#_Toc151389575)

[**Case Study** 42](#_Toc151389576)

# Chapter 1

“The time is always right to do what is right.”

* Dr. Martin Luther King Jr

This chapter starts with an exploration of why cybersecurity is needed. And more importantly, why we need to be a people of character. This book presents a case for the Cybersecurity Code of Honor. The world needs cybersecurity professionals who can be trusted. The Cybersecurity Oath is one of the ways we can begin to make sure we are a group others can trust.

Cybersecurity is needed everywhere, in all industries. Furthermore, there is a need to establish trust among those who ask us to protect their data. Thus, the start of formalizing an ethical standard for cybersecurity professionals. This is because cybersecurity is a human problem. Yes, it is surrounded by technology and uses technology. But to win the battle, we must look to the human aspect of cybersecurity. Again, there is a need to establish an ethical standard. The Cybersecurity Oath is that standard.

As medicine, law, and warfare have established ethical standards, cybersecurity needs a standard. This book presents the Cybersecurity Oath, this piece of ethical standard. The time is now to adopt such a standard. This book explores why each element is a part of the oath and how the oath can impact cybersecurity at all levels.

Below are some discussion questions to help explore this chapter with your students.

## **Discussion Questions**

1. State of Cybersecurity

Cybercrime continues to rise year after year. The numbers are staggering: the cost of cybercrime, the amount spent on cybersecurity, and the individual cost to a company for a data breach – all are ever-increasing and staggering to consider. As your students review the numbers in the book or look to current headlines about the cost of cybersecurity, what can be done to reduce these costs and their impact? This is not a simple problem with easy answers. But take time to consider the options. We are in an arms race against cybercriminals.

What role do ethics and trust play in the overall arms race? At this time, where do your students see the solution to the issue of cybercrime coming from? Do we need more technology? Is AI the solution? Or is this the human problem that needs to be addressed?

1. “Why you should care.”

If you read the news, cybercrime and cyber-attacks are in the news daily. No target is either too big or too small to be affected by cybersecurity. How do we address a global cybersecurity crisis? How can we bring a stop to this crisis? Do you think that companies you buy from are concerned about cybersecurity?

Choosing a recent major hack should not be hard to find one to discuss. Do you think this company was concerned about cybersecurity before the breach occurred? How about after the breach? Cybersecurity needs to be everyone's concern.

Do you think the average person is concerned about cybersecurity? How can we raise awareness of the impact of cyber-attacks?

1. Ethics in Cybersecurity

The high-stress, high-stakes nature of cybersecurity leads to the saying that cyber ethics is essential. Much as other professions have codes of ethics, cybersecurity needs to be developed and adopted. This book proposes a code of ethics to be adopted. But before you read the whole book, what are some aspects of ethics that you think should be covered in the Cybersecurity Oath? You may not have the wording, but what areas need to be addressed by such an oath?

A couple of stories in the book paint a familiar picture of happenings in cybersecurity. The book proposes that behind all cybersecurity is people making decisions. Do you think this is a correct view of cybersecurity? If humans are a vital part of cybersecurity, how do we develop the needed skills and frameworks?

The idea of a code of conduct in cybersecurity is not new. This book proposes a unified approach across cybersecurity. The book wants to present you with a framework for making ethical decisions in cybersecurity, regardless of what is happening. Do you find having a framework and guidelines to be helpful? Does this seem like a beneficial approach to addressing human issues within cybersecurity?

1. Long-standing models

Medical, law, and war have developed codes of conduct (ethics) over the years of human development. This book proposes that cybersecurity is now where we must adopt a similar code of ethics. Is cybersecurity at a place where A Cybersecurity Oath is needed?

Consider the Hippocratic Oath and the impact it has had on modern medicine. The goal of the Cybersecurity Oath is similar in scope and goal. How can a bind set of standards benefit cybersecurity? Do you see any drawbacks to having a binding, uniform Code of Conduct?

1. Why Now

Why do you think that we need an Ethical Code of Conduct now? The goal is to create an unchanging code that can guide an ever-changing world of technology. As you prepare to enter the field of cybersecurity, do you see value in adopting a Cybersecurity Code of Honor, an Ethical Code of Conduct?

In what ways is the Code of Conduct valuable to the field of Cybersecurity at large? As you explore this book, we will find more ways this can influence the overall cybersecurity industry. How can a Code of Conduct benefit you personally, both now and in your future career?

# Chapter 2

“I will treat all people with value and dignity.”

* The Cybersecurity Oath

As we consider the Cybersecurity Oath, the first statement concerns treating people with value and dignity. Below is a set of discussion questions to help lead the class in discussing how to treat people with value and dignity and how this intersects with Cybersecurity. Also included is a story (case study) and questions to guide a further conversation. These resources aim to help you, the instructor, in talking with students about how to treat people with value and dignity while working in Cybersecurity. While Cybersecurity is a highly technical field, it exists to serve and protect people.

## **Discussion Questions**

1. Cybersecurity Is a Human Business

When a cybersecurity breach occurs, who are the people that are affected?

You can use the case study in the book or another cyber-attack in the news.

While there is no answer to this question, the goal is to get students to talk about the people impacted by a significant or minor cyber-attack. Cyber breaches affect more than 1’s and 0’s more than businesses. Cyber-attacks and breaches impact people. Considering human value and integrity is a start to considering the human aspect of Cybersecurity.

1. Humans Have Inherent Value

Outside of Cybersecurity, consider when someone showed value to another person throughout your life. What does offering value to another human look like? How do you know when someone is treating others with dignity and worth? Can you think of times when people did not value people?

The goal is to get students to think about what it looks like to value others in life. What does treating people with dignity look like throughout life? These examples could come from the news but are more likely examples from their personal lives. Give them a chance to explore what valuing and treating people with dignity looks like and why it matters. This can lead them to think about how they can treat others with value and dignity. While this might not always be easy, it is imperative to develop these skills. The more we improve these skills, the better cybersecurity professionals we will have in the field.

1. The Solution to the Problem of Cybersecurity is Principle a Human Solution

The people doing the work. The book mentions DIY projects that have failed due to lack of experience. Can your students think of a project they have either been a part of or seen that failed – not for lack of tools, but due to lack of experience? Talk about what could have been done differently, primarily needing someone who knew how to do the task. How does this apply to cybersecurity? There is a place for learning skills in cybersecurity.

Yet this book wants us to go beyond technical skills. How does being a person of integrity affect our ability to do the job of cybersecurity? Consider the ethical skills that might be good for a cybersecurity professional. As you build this list, how do these skills impact cybersecurity? This book has boiled this down to a relatively short list of ideas. Keep your list in mind as you work through the book, where do your ideas fit into the book? Is there something that you missed or something that the book missed? Is there anything that surprises you?

1. Character Costs and Character Pays

Cyber professionals are tasked with protecting data and systems. How does protecting data and systems work to defend human value and dignity?

The goal here is to again think about how the technical tasks we, cyber professionals, perform daily are involved in defending the value and dignity of people. It is easy to focus on the 1’s and 0’s, the technical aspects of the job. Yet, focusing on the human elements is essential in talking with professionals and students. Many pursue cyber defense to help people. Getting students to understand the importance of protecting the value and integrity of people as part of cyber will allow them to see what they are doing through another lens.

## **Case Study**

Cyber-attacks come in lots of different forms and sizes. The book provides an excellent example of treating people with value and dignity in a significant cyber-attack. Yet, even in minor cyber incidents, treating people with value and dignity is vital. This case study will explore a smaller-scale, daily cyber incident.

Sally works for a symphony in the finance department. Over the years, she has been through the cyber training programs offered and required by the organization. Sally strongly desires to help everyone; Sally is always ready to do whatever is needed in the office. She is friendly and helpful on the phone. She always responds to emails and is prepared to help. She has learned that not everyone is as friendly as she is and that cyber-attacks are a real threat – even at their symphony. She has even reported several simulated phishing attacks in the past six months.

On Monday morning, Sally received an urgent email. The email appears from the CFO requesting an urgent bank transfer to pay a deposit for an upcoming visiting artist. The amount is an average amount of money to transfer for an artist ($50,000). It is unusual for the request to come by email – Sally can never remember getting an email like this from the CFO. But it is urgent. There is a risk of losing the artist, so it needs to be done immediately. So, Sally contacts the bank and starts the transfer. She then calls the CFO to confirm the work is done. The CFO is surprised and has no idea what she is talking about. They quickly realize that someone has sent a cyber-attack against the organization. However, they are not immediately sure how. Their next stop is to contact their internal IT department.

After realizing she had made a mistake, Sally and the CFO called the IT department to see what could be done. An immediate meeting is held to evaluate the situation and determine a plan.

This study is not about the response. So, we will leave them to deal with the cyber incident. We will pick back up with the IT department after the meeting as they break for lunch and discuss the incident. One of the members starts to talk about how Sally always seems to be falling for phishing attacks. After all, including simulated attacks, this is the fifth phishing attack that she has fallen for in the past year. The talk quickly turns to the challenges of supporting users and what Sally and others have done; they seem unbelievable to the technical staff.

In contrast, the staff is always polite and professional around others at the symphony. But when it is just the technical group, they often commiserate about their experiences with others. So, in many ways, this is just another lunch with the IT staff.

**Case Study Questions**

1. Who was impacted by this attack?
2. How was the value and dignity of people either protected, exploited, or devalued in the story?
3. What steps can be taken to improve human value and dignity treatment?
4. What steps could have been taken by what roles to improve the treatment of human value and dignity?

# Chapter 3

“I will seek the best interests of others.”

* Cybersecurity Oath

When I started teaching cybersecurity, I wondered whether students would choose to major in cybersecurity. Students could have lots of motivation, but I suspected that at the top of the list would be money and a love of technology. Hacking sounds cool, something they saw on TV or in a movie. While some students fit these thoughts, I was surprised to find many students who chose cybersecurity to serve others and give back to society. This motivation was familiar to me, but I did not expect this to be a leading reason for choosing cybersecurity among my students. While this might or might not match your experience, it is essential to know that people choose cybersecurity as an act of service.

               Chapter three is focused on seeking the best interest of others in cybersecurity. Below are some discussion questions to help you discuss this material with your students. It will also include a case study (story) to help highlight what serving others through cybersecurity might look like. These materials are provided to further the conversation around cybersecurity as a way to look to the interests of others. This looks different in different circumstances.

## **Discussion Questions**

1. We Need You on that Wall.

People are needed on the Wall to quote the book. This is not always an easy task, and this is not always a task that others will acknowledge or even appreciate, but this is a needed place. To get the class talking about serving on the Wall and in cybersecurity, what are some ways that working in cybersecurity is being on the Wall? The reference to serving on the Wall, the image of A Few Good Men, brings up the image of a military. So does the talk about Protect and Serve. Talk about how cybersecurity is like serving in the military. What is the mission of cybersecurity? How is each of us fitting in a global cyberwar?

This question aims to start students thinking about cybersecurity as a service to others, even if they have yet to think this way in the past. Much as we need soldiers, sailors, and airmen in the military, we need people to choose to serve through the work in the global cyber war. The chapter covers the importance of cybersecurity to serve the interests of others. Use this question as a possible way to challenge the why of choosing a career in cybersecurity. It is not that there is not a love for tech that is needed, it is not that there is no money to be made, and it is not that cybersecurity is not a place to learn and be creative, but cybersecurity is a way to serve.

1. Know Your Why – Purpose and People

Knowing that people have value and need to be treated with dignity, see Chapter 2; this builds on that concept – we guard the value and dignity of people by seeking the best interest of people and society. How is seeking the best interest tied to the value and dignity of people? Can you think of a story or a time (not necessarily cyber-related) that someone demonstrated seeking the interest of others? How do these stories affect you and others? How can you apply this concept in your future work in cybersecurity?

Finding stories around an idea is a great way to help students identify with the theme. The idea of cybersecurity to seek the interest of others might be new to many people. These questions aim to get them thinking about what seeking the interest of others looks like and how they can accomplish this in their future career.

1. Service Means Sharing: Sharing Starts with Good Communication

If we are going to look to the best interests of others, we must learn to communicate and communicate well. The first question for your students is how well they can communicate with others (peers, professors, bosses, non-technical friends, etc.). How does stress affect the ability to communicate? Can the students think of times when they or others have communicated well? What allowed them to communicate well in that situation? Explore aspects of treating others with dignity paired with the students’ feeling of knowledge on the topic.

The goal is to explore the value of good communication when looking at the best interests of others. Communication comes in many forms, and all are necessary for cybersecurity. Students must consider how to communicate well. It is also crucial for students to begin to understand how they can work to improve their communication skills. This is a critical piece of looking to the best interests of others.

1. Sharing with the Broader Cyber Community: We are all on the Same Wall

As the chapter points out, we share the Wall with others. You are not in this cyber conflict alone. We are all sharing the defense of the Wall. Sharing in the cyber defense of the Wall is a challenging concept. How do we work well as a team in cybersecurity? This is about working well as a member of the corporate team you find yourself a part of, but there is more. First, how do you work as a team? How do you share your perspective while respecting the views of others? Another aspect is how we share cybersecurity information outside of the organization. This involves sharing cyber defense and attack information with law enforcement, competitors, partners, and other groups to make cybersecurity better and stronger for all. This task is challenging; keeping cyber-attacks close to the vest is general practice. Do not share anything that is not legally compelled. Nevertheless, secrecy aids the attackers; what worked in one attack will likely work in another. The question is, how do we share cyber information with others? How do we do this without compromising company data and secrets?

For some organizations, this is easier than others. Education and nonprofits sometimes have an easier time-sharing information with their peers about what is happening and what they are struggling with; for most companies, sharing is hard. Between not wanting to share confidential information and not wanting to look weak to customers and investors – companies tend to keep things quiet. Can your students think of ways to share vital cyber elements while maintaining confidential data? Solutions are being explored, but this is an ongoing issue.

## **Case Study**

We live in a world where Ransomware attacks are everyday occurrences. This story will talk about an attack that occurred a few years ago. While this is based on an event that happened, it has been modified to help tell the story of this study.

Everything started as a typical day at the organization. The Helpdesk support staff, Sam, came into the office a few minutes early and started checking his email. Sam is one of many employees who was in early; James was also in early. James works in the marketing department. But when he logs onto his computer, he is met with a screen he has never seen before. The screen shows something about encrypted, cryptocurrency, and a timer counting down. James is still determining what the screen means and what to do about it. So, he decides to ignore it for now. After quickly scanning his email, he decided to open an Excel file to look over a spreadsheet he was working on yesterday. It fails to open and again gives a message about being encrypted. At this time, Sue is also trying to access files from her computer in the marketing department and also gets a message about encryption.

After a quick conversation, Sue and James decide to make two calls. First, they call the Helpdesk. Then they call their supervisor to let her know what is happening in the department, even though all they know is the files cannot be accessed.

This started the process of the Executive Team talking about the Ransomware Attack. It was quickly discovered that all the network-shared files are encrypted, and no one can access any files to get work done. The calls start flooding the Helpdesk; the IT staff is working to determine the cause and plan a recovery.

Thanks to the first call to Sam at the Helpdesk, IT started looking into the breadth of the issue. When the calls started flooding the Helpdesk, the team had been assembled and was working on identifying the scope of the encryption. Due to an error in the account permissions, James had more permission than was required for his current role in the company. Thus, the reach of the attack was more significant than expected. The team begins to follow their Disaster Recovery Plan.

**Case Study Questions**

* From what is shared in the case study, some communication is happening. Calls are being made, and teams are being assembled. What communication do you see in the scenario? Is there alluded to communication in the scenario that most likely happened? What groups, people, and teams are communicating?
* Now think beyond the story that is told. Who should the IT/Cyber Team be communicating with about this event? What internal Communications need to be taken? What external Communications? Is there a need to involve Legal Counsel? What could be shared with Law enforcement? What can be shared with other fields and/or area organizations?
* What other types of communication can you think the company should consider using in the case of a Ransomware Attack?

# Chapter 4

“I will strive to recognize, take ownership, appropriately communicate my mistakes, and exercise patience toward others who make errors.”

-The Cybersecurity Oath

Taking ownership of one’s mistakes is never easy – this is especially true when you have been trusted to do a job, and your mistakes might make it look like the wrong decision was made. Yet, it is vital as people of integrity that we are honest about our accomplishments and our mistakes. This chapter provides a great story about trying to hide one’s mistakes. Matt and his team could have taken a different approach, and the story could have had a very different outcome. Yet Matt is not alone in his choice to try and hide/fix the mistake before others notice.

Beyond looking at integrity, the chapter explores how we, as cybersecurity professionals and people in general, can live lives of integrity. This includes exploring humility, curiosity, and teamwork. In this study guide for Chapter 4, we will explore each of these areas through discussion questions and an additional case study. The goal is to get the students thinking about how they can live lives of integrity now and in their future careers.

## **Discussion Questions**

1. Bad Decisions and Multiplication

The story in the chapter presents several challenges as we work to be the best we can and make decisions based on the information at hand. Yet, as is seen, Matt chose poorly, and the results were of significant impact. Yet, each team member also chose this experience. They were trying to fix the bug but did not report it up the chain.

1. Is it better to be a part of the team or to go around your boss and report a concern to further up the chain of command?
2. How do you know when to report further up the chain of command? Sometimes, this makes sense, but it is a challenging choice.
3. This story is a series of small choices. Can you think of a time when a small choice has led to bigger problems in your life or a story you are familiar with? Assuming that you can, can you think of a way it could have been done differently? Would the outcome have been different?
4. How could this story have been different? When could someone have chosen to report this to the CISO? How would telling the CISO change the approach the team and the company could have taken to address the issue?
5. Humans are Flawed.

As we begin to explore the idea of integrity and living a life of integrity – the first place for students to consider integrity as students. As we consider the “zero-day vulnerability” in humans. In what situations have they seen their own or other imperfections and poor decision-making? This could be an example from their own life or even something they have witnessed elsewhere. What was the “zero-day” impact on the person and the others involved in the event?

1. Turning Vulnerability into Strength: It Begins with Humility

Humility is an essential aspect of developing as a person. Humility is not easy, a skill we all work to develop, yet humility is vital to developing an open and healthy culture. When the students are considering a situation/ a decision that needs to be made, use the story about Matt from the book. Now, have them take a few minutes and consider the following questions from the book:

1. Why am I pursuing this approach?
2. Is this all for my benefit?
3. Who else could potentially be hurt by this approach?
4. What’s best for my organization overall? What’s best for my employees? What’s best for my boss? What’s best for my family?
5. How does this approach benefit or hurt our customers (teammates, friends) and other stakeholders?
6. Are there other options that I’ve overlooked that might be more optimal for everyone involved?
7. Being a Lifetime Learner

Your students are entering a career in cybersecurity; curiosity and life-long learning are essential to a successful cyber career. As most students are aware, technology is continuously changing and evolving. In this field, there is always something new to learn. What new technology/cyber-attack have your students heard about that could impact cybersecurity? What do they know about this technology? What can they think of that they should learn about it? What are some ways they can go about learning more on a given topic?

Have students list ten sources that can be used to stay current on cybersecurity. Have them summarize how they believe each source can be used in life-long learning.

1. Handling the Mistakes of Others

Dealing with our own “zero-day vulnerabilities” is the first step in being a team player. However, we all must go further; we must work with others as well. Even more importantly, we must remember that we all fail. Thus, we must work with others who also fail – dealing with these failures is how we can be great team players. Extending grace and patience is a vital tool. Can your students think of a time when someone else failed that impacted them? Did the student extend patience? If so, how were patience and grace shown? If not, how could grace and patience be shown in the situation?

Is showing grace and patience always about avoiding the consequences of another’s actions? If not, how do you show grace and patience while still having consequences for one’s actions?

1. Let’s try to Avoid “Breaking Bad”

An essential step in taking ownership of our actions and working with others is knowing that we can and do all make mistakes. We all make unethical decisions. It is always just an easy step to make those bad decisions.

As you read the book, the authors shared several small decisions in the grey area. These are unethical decisions minor unethical decisions. Yet these small decisions can lead to big problems. Can your students think of a time when they made a small, unethical decision? Or a case where someone else made a small unethical decision? How did or could this slight decision lead to more significant ethical issues? What different decision could have been made?

1. How to Develop a Reflective Practice

Building good habits is an essential aspect of life. We are all working to develop good habits. This is true in all aspects of life, from exercise to lifelong learning. This is also true for making sound ethical decisions. As the book indicates, one of the steps in this is reflecting on our choices.

The book includes some suggestions for being reflective about our decisions. What benefits can your students see in being reflective about our decisions? How can we work to be better tomorrow than we are today?

1. Chapter review

This chapter has been working through the concepts of taking ownership of our mistakes and giving patience to others. What lesson is most impactful to your students? Have them consider the chapter and how this can help them become better cybersecurity professionals. Once they have identified which element of the chapter speaks to them most, how will this aspect make them a better cybersecurity professional? Will this also make them better people?

## **Case Study**

As a professor, grace and consequences are every semester's occurrence. Students make decisions on doing or not doing assignments. Students either do or do not come to class. Students either communicate well with the professor or they do not. In one of my early semesters, I had a brilliant student who made terrible decisions regarding his assignments. He did not do many of the assignments for the semester. Over the semester, he communicated well with the professor and asked for extensions. The student was granted several extensions. Yet the student continued not to turn them in. At the end of the semester, the student was missing multiple assignments. The student was missing enough that he had a failing grade. The student came again to ask what he could do to pass the class.

So, this is not a cyber incident, but it does show bad decisions and grace that you can understand. Take a few minutes and consider the decisions made by both parties. What bad decisions were made? What patience and grace were shown? How would you have responded to the student's request for what can be done to pass the class?

In the end, the student was informed that there was nothing left he could do to pass the class. Bad decisions have consequences even when there is grace and patience shown.

**Case Study Questions**

1. How does this case demonstrate patience and grace with other's bad decisions?
2. Does this show that even when patience is extended, consequences still happen?
3. Can you think of times in your experience that this is also true?
4. What are some ways you can think of that patience and consequences can happen in the life of a cybersecurity professional?

# Chapter 5

“I will be honest, trustworthy, and above reproach in my actions and communications.”

-The Cybersecurity Oath

As the opening narrative demonstrates, trust takes time and effort. At the same time, some level of trust indeed comes with the hiring process. Real trust must be earned and maintained. Just as Xiang took time and effort to build a high level of trust, so must we take our time to make the trust of those around us. Further, it is essential to understand that trust does not require technical skills. Yes, if in a technical role, technical skills are necessary, but trust must all be built.

The challenge is to learn how to build relationships with people so that they can trust you, even when the situation is challenging. Trust is easily lost and takes time to build. All the technical skills in the world will only be enough with trust.

Take the time to build trust. Put the work in building trust. With that trust, you can accomplish great things. Consider the narrative in this chapter and what else you know about trust and building trust. Below are discussion questions to help students consider the value of trust, followed by another case study that can be used to explore the virtue of trust building.

## **Discussion Questions**

1. The Secret of Success

“Meaningful, trust-based relationships are essential to most successful careers.” This is especially true in the world of cybersecurity. As a cybersecurity professional, you will often have great access to files and data the company values. Sometimes, you might have access to all the company's digital resources. This means that the company needs to trust you. This might be a new concept, the idea that companies trust them with access to information.

1. How does having access to data and information require trust?
2. How does a young, new employee gain the trust of a company?
3. While you need technical skills, you must also ensure trust is built. What steps will build trust? What actions will erode trust? Consider arrival, lunch, and departure times – how do these affect trust? Consider how you talk about your work – both at and away from work; how might his impact company trust?
4. When you look at your own experiences, what are some areas where you have built trust with others? Have you acted in a way that reduces another's trust in you? Or did someone else's action cause you to not trust them anymore? Now, consider how you can apply these events to your future career in cybersecurity.
5. Trust is the Currency of Cybersecurity

If we are willing to see that cybersecurity is primarily a human problem, trust is at the center of the problem and the solution to the problem. Cybersecurity professionals must be trustworthy. The fact is that companies trust cyber professionals – because they must trust. How can we, the cyber professionals, build and continue to earn this trust?

Consider your life experiences to this point; you have had people who trusted you and people you have trusted. You are on the path to becoming a cyber professional with access to critical and private information. What can you take from your current experience with trust and apply it to your future cyber career?

1. Building Trust Requires Courage

Trust is not easy to build. It takes effort and time. The book points out that it also takes courage to build trust. In cybersecurity, trust is the coin of the realm. We are giving great access and are expected to maintain the trust of the employer. But what is the role of courage in building and maintaining trust?

1. What role do you think courage has in the building of trust?
2. Can you think of someone that has shown courage? Did this demonstration of courage increase trust in the situation or not?
3. Why does it take courage to build trust?
4. Applying this to cybersecurity, in what circumstances does it take courage to act? How might this action affect the trust relationship you have?
5. The Role of Leadership in Building a Culture of Trust

Cybersecurity is a rapidly growing industry, which has led to rapid advancements of those that show technical ability. The challenge compared to other business areas is that this does not mean the young individuals have had the time to develop the trust and responsibility for the management role.

1. How can cybersecurity leaders help young cyber-professionals understand the importance of ethical decision making?
2. How can cybersecurity leaders help to demonstrate the process of ethical decision making (transparency)?
3. How does the handling of small decisions demonstrate your ability to handle more important decisions?
4. Have you experienced a time where learning to be trusted with small things has led to great privilege and responsibility?
5. A Checklist for Building Trust

Trust is not about perfection – we all make mistakes, and we make bad decisions. What are the three elements that are needed to build trust? Honesty, Accountability, and transparency.

Trust can be built and damaged. What are some examples of ways trust can be damaged as a cyber professional?

Some trust is lost, even when the situation is outside one's control. For example, when there is a security breach, the company will lose some of the public's and customers' trust. Security breaches happen – yes, we take steps to avoid them, yet a security breach is still possible. What steps can be taken to restore trust due to a security breach? What steps can be taken that might damage trust further?

Can you find examples of companies that have lost trust due to a security breach? Find an example of a company that handled a security breach well and worked to restore trust. Find an example of a company that handled a security breach poorly. What differences exist between how these companies acted and how the public and customers responded?

1. Honesty

Honesty and truthfulness are vital for trust to exist. There are many times to tell the truth in cybersecurity, but not all are easy. The book mentions reporting a vulnerability in code before going to production. While this sounds simple, consider why this might be difficult for junior team members. What is some reasons reporting could be a challenge? Consider increased cost, missing deadlines, and questioning others' work.

What are some other situations that might be hard to report? Why would these be difficult?

1. Accountability

Once you have discovered a breach or an issue, you must report it. This is accountability. How does accountability affect trust?

If you discovered a breach at your company, what would you do?

What steps would you take if you discovered an unknown vulnerability in your company's new software, which is about to be released?

1. Transparency

In the world of cybersecurity, transparency does not mean that you need to tell everyone everything. So, we talk about transparency with discretion.

How do you know what to share with whom when you are trying to follow transparency with discretion?

Your company just experienced a breach that you discovered and were instrumental in helping to contain. Your friends ask what has been happening at work. What do you share with them?

What role does legal counsel play in knowing what to share with whom and when? Consider this in the case of cybersecurity.

## **Case Study**

It was exciting when a Network Manager, John, started at a new organization. Starting a new job with new challenges and opportunities is a great time. As John gets settled into the new position, it becomes clear that the IT team he is a part of has some conflict with other departments at the organization. There is a lack of trust, especially with the Physical Plant that cares for facilities. The two groups often need to be in the same space, especially during the summer when projects are happening. Both groups feel the other group is trying to control the calendar and are always in the way.

John decides this is not the optimal way for either team to function and begins to try to find ways to build bridges between the two teams. This starts slowly. It starts with a talk with the physical plant employees. Trying to find some common ground – Both teams work for one company. This made little progress.

Next, the campus experienced a power outage, and John noticed the phys plant team gathering. So, he walked over to see if he could help. They assigned people to check various buildings and turn off breakers to key equipment to avoid damage due to low power (brownout). Having master keys to some buildings, John offered to be another set of hands. They accepted, and progress in building trust started to grow. Over the next year – anytime there was a power issue on campus, John was there ready to help. Any time there was a project, John was making sure to communicate with the other team to make sure everyone was on the same page.

Over time, trust was built in both directions. By the end of the year, John called the lead electrician to ask if he knew about power issues in various buildings at different times. The electrician asked how John knew about it before anyone else. It turns out the installation of smart UPS that alerted the network team was allowing for quick notifications, and the electrician asked to be added to the paging list. John was glad to do this. The two teams continued to build trust and work together for the organization's good.

When John left the company, the CIO mentioned that the trust between the two teams was a great accomplishment that was unforeseen in coming. But the CIO knew John was at the center of this trust building. This trust helped in several cases, not only during project time. But also with mechanical failures in the IT server room and closets.

**Case Study Questions**

Why was this building of trust necessary?

What was done to build the trust?

How do you think this trust impacted the overall organization?

# Chapter 6

“I will not be a lone wolf but will instead work collaboratively with my peers and superiors.”

-The Cybersecurity Oath

This chapter suggests that we cannot be an excellent cybersecurity team alone. The Cybersecurity Oath refers to the idea of not being a lone wolf. This is the picture of a lone animal trying to live in the wild. While the wolf can do this for a time, the wolf is always the most potent in a pack. The same is true for cyber professionals; you might be able to make it on your own for a time, but you are always most robust with a good team.

The chapter opens with the story of a promising young cyber professional who tries to do it alone. Even though he knows he has a solid team to support him, he tries to solve the problem alone. His lack of experience and knowledge leads to failure. Failure for him, failure for the team, and failure for the company. Had he had the courage or insight to mention the initial findings to another of the team? It could have been contained, and the failure avoided.

The chapter continues to explore aspects of working as a team. Below are some discussion questions and a case study to further explore the concept of teamwork – the goal is to ensure we are not trying to be a lone wolf.

## **Discussion Questions**

1. The value of teamwork

Consider the quote from the Jungle Book: - “For the strength of the pack is the wolf, and the strength of the wolf is the pack.” How can you, the cyber professionals, both be the team's strength and find strength in the team?

Ask the students to consider a time in their life when a team/group has accomplished something no one member could have done on their own. After finding this story in their life, have them consider individuals' impact on the event. The hope is for them to begin to see that as a team, they could do something individuals could not – but without each team member's strength, the event would also have failed.

How can teamwork make the sum of the parts more significant than the individuals?

What are some reasons that teamwork is vital in Cybersecurity?

Give some time to consider how the team's makeup can impact the team's overall strength. When building a team, what are some elements that should be considered?

1. No Room for Know-it-Alls

Two elements about you can never know it all. First, you need others that know things you do not know. Second, you do need to be a life-long learner. There is always the opportunity to learn something from someone else. Do not let pride lead to you failing to talk to the rest of the team – even when you think it is all under control.

Looking at the first story of the Chapter, what could Jonah have learned by talking to the rest of his team? How could a conversation with the team impact his chance for promotion? Why do you think that Jonah did not ask for help?

Have the students think about a time they learned something from a classmate, a friend, or a teammate. Was this a good experience for them? What was the response from others? Was there a negative aspect to learning from a peer? Have them talk about how this could be applied in a cybersecurity team.

1. Making Informed Ethical Decisions with Input

It is always a great idea to talk with others when deciding. This is especially true in the face of ethical decisions. Making decisions in a vacuum can be dangerous. This is demonstrated in our opening story. When Johan found confusing information about the malware, bouncing ideas off another trusted teammate could have saved the day and his job.

Can your students think of a time when they bounced an idea off a peer or boss? Or can they think of a time when they decided that, in hindsight, they would have benefited from talking about it beforehand with someone else?

How does talking through a decision help to make better decisions?

How do you choose who to bounce ideas off when facing a decision?

Reflecting on earlier chapters, how do you retain confidentiality while using others as sounding boards?

1. Why Teamwork Really Does Make the Dream Work

From the book – “Collaborative work surrounds us with people who bring different perspectives and experiences to each task, creating a more informed, well-rounded foundation for critical thinking and decision-making and better ethical choices.”

When putting together a team, what part or value does diversity play?

How can we ensure diversity and that the team has the best members?

How has diversity played a role in teams you have participated in?

1. When Collaboration Breaks Down – Seeking Allies In Your Organization

As the book mentions, teamwork and open communication sometimes fail – remember, others are also human. Sometimes, this is intentional, asking you to ignore what you might have seen. Other times, others do not see your sense of urgency, which might exist.

How should you respond when the team does not support an issue you see?

How do you raise the issue with a senior leader outside your direct reporting line?

How do you raise a legal issue outside of your company if necessary?

What are the potential consequences of reporting outside of your typical reporting structure?

Who could you talk to about making this decision? How do you maintain confidentiality during this process?

1. The Power of Mentors

A good mentor can be crucial to your overall success in your career. This also falls into the always learning parts we have considered earlier.

Have any of your students experienced a good mentor?

Have them consider the steps in Chapter 6 of the book. Now is an excellent time to start looking for a mentor if they do not yet have one.

While it might not be the right time for all students to find a lasting mentor, meeting with a mentor, if only for this class, will be a good exercise that will serve the students well.

1. Beware of Rattlesnakes

We only succeed with the help of others. Looking back on our lives, we can see those who helped us along the way. Take a few minutes and think of those who helped you to gain the victories and successes you have accomplished. What can you see about those who helped you along the way? Is it easy to accept help? How do you accept help gracefully?

There are also those that you have helped. It is good to realize that you are receiving help and helping others. How have you helped others? Are there other ways that you can help others?

We are all climbing a mountain. We all need help. How do we identify those who can best help us? How do we identify those that we can best help? As you are climbing remember to accept help when it is needed and to offer help to those you can help.

## **Case Study**

In the world of IT and cybersecurity it is impossible to know it all. Further, this becomes truer all the time, as new technology continues to be created and distributed. Knowing where your limits of knowledge are at is vital to a successful career in cybersecurity. This also means needing to work as a team – not as an individual. Below is a tale of teamwork.

Sue had been hired as a Network Administrator at a mid-sized manufacturing company. During her time there, most network challenges were easily managed within her knowledge. Her knowledge even continued to grow as new challenges arose. There were many new challenges, and the learning was exciting. Yet, Sue also learned there are areas that others know better and are able do better work than she might ever be able to accomplish.

Her boss, Fred, would periodically call Sue to his office and ask a random technical question. Sue often knew the answer or would soon be able to find the answer for Fred. It felt great to be of such an outstanding level of service. During this time, Sue came to know and occasionally worked with a contractor, Bob. Bob was a truly outstanding Network Engineer. Able to accomplish more than Sue knew.

One day a challenge came to the company network. Fred asked Sue if she could accomplish the changes that needed to be made to the network. Sue began to consider what needed to be done and concluded that she might be able to eventually solve the challenge – but know that Bob could probably do this in 15 minutes.

Sue went to her boss and owned that although she was the senior network admin at the company, she did not know everything that was needed for this challenge. She asked Fred to use Bob to solve this issue. It was using an outside contractor, not her the internal expert. After speaking about the options. Fred agreed that asking Bob to assist would be the best solution for this case.

Bob was happy to help. He even went further and took time to explain what he was doing to Sue, in case she ever needed to know this in the future. By knowing her limits and using an extended team, the company was able to get the needed work done correctly and Sue was able to learn some advanced networking.

**Discussion Questions**

1. Do you think it was easy for Sue to acknowledge her lack of knowledge in the field she as the company expert?
2. How have you asked for help? Was it easy to ask for help?
3. How does this story demonstrate the power to teamwork?
4. Does Bob assisting with Sue’s learning fit the model of teamwork?
5. How can you see mentoring happening between the lines of the story?

# Chapter 7

“I will endeavor to exercise patience, wisdom, and self-control in all situations.”

-The Cybersecurity Oath

This chapter looks at what it means to remain in a stressful situation. There are lots of ways this can be described; in the end, it is about having patience, wisdom, and self-control to function when everything and possibly everyone is going wrong.

The chapter starts with a great story of a cyber incident and provides some insight into how various people might respond. The truth is that people do respond when bad things happen, especially when the bad things are highly public and disruptive. Below, I will provide some discussion questions about dealing with these hard situations and a case study to help. Always remember different people react differently to stress. But having a plan and practicing the plan will help everyone respond better.

## **Discussion Questions**

1. Dealing with chaos

Cybersecurity can have chaotic times when everything seems to be going wrong. These times truly test the people who work in the field. These are the times of challenge to you and your character. Take some time and think about your life; some of you have experienced chaotic times of challenge. If you cannot think of a personal time of chaos, think of a story about a time of chaos. How did people respond in those moments? Describe those that seemed to fall apart, even if they seemed in control minutes before the chaos struck. Who were the ones that stepped up and brought order to the chaos? What made them different? Did they have all the answers? Probably not. Yet what gave them the presence of mind, the peace in chaos to succeed in challenging times?

1. Essential to success: Patience, wisdom, and self-control

Part of being calm in the face of chaos is developing patience and self-control. These are skills and traits that you must develop, like any skill. Some people have more patience, wisdom, and self-control, but all of us can work to develop these skills. When asked if a junior administrator could handle the job of being a senior administrator – I once responded that from a technical perspective, the answer is yes. But from an if something goes wrong perspective, I was not sure he could handle the pressure. He had not taken the time to develop the patience, wisdom, and self-control to remain calm in the face of fire. Technical skills are not enough.

Now is the time for some personal reflection. If you are not there – it is okay. We are all still working on building patience, wisdom, and self-control. When you consider yourself – what level of each do you feel you have (patience, wisdom, self-control)? If you were to find yourself in a cyber-attack, how do you feel that you would respond? Are you able to stay calm when life throws the unexpected at you? As the book points out, cybersecurity often goes from enjoying coffee to fighting a cyber-attack in the blink of an eye. Are you ready for the ever-changing nature of cybersecurity? How can you work to develop the patience, wisdom, and self-control that you will need now and in the future? What steps are you taking currently to make you a better person tomorrow?

1. Remember the Titanic

As stated before, we are all trying to improve patience, wisdom, and self-control. We are also practicing responding when something does not go as planned. The book tells us to remember the Titanic. While the Titanic failure was significant, boats sank. The greater failure was not having a plan for what to do if the unthinkable happened. Today, from a cybersecurity perspective, we talk about various levels of being attacked or hacked. For many, this is unthinkable. After all, we are in the work of cyber-defense. Who wants to consider what happens when we fail? We are supposed to defend – the attack should never be successful. Yet the reality is that cyber breaches are a daily occurrence. Defenses fail. So, what can be done to help ensure your company has a plan for when the ‘ship sinks’? What ways can you think of that can help a company practice for the unthinkable? How do you prepare for that which you might not have even considered? What role do patience, wisdom, and self-control play in preparing for the unexpected?

1. A few Principles for Emergency Planning

Consider the quote, “Failing to plan is planning to fail.” Do you think there is truth in this statement? Again, how do you plan for what you do not think can happen? What skills do you think need to be developed in you and your team to allow for this level of planning?

The book lists four steps to Emergency Planning

1. Understand the chain of command.
2. Be clear about the sequence of the steps.
3. Know your role.
4. Practice makes you more perfect.

Consider again how to plan for the unexpected. What do these steps have to do with the ability to respond to the unexpected? How could the crew of the Titanic use these four steps to improve the chances of survivors of an unsinkable ship sinking?

1. Stay Clam, Cool and Collected

As a cyber professional, it is crucial to know yourself well and to be able to stay calm under pressure. Looking at the quote from Haidt – “What does not kill you makes you weaker; always trust your feelings.” How do you respond to this quote? Do you believe that this is a good description of life?

I grew up with a different saying – “What doesn’t kill you makes you stronger.” The difference between the two sayings is only one word weaker or stronger. Yet, the difference has a significant effect on our view of events in life. Chaos will happen, bad things will happen, and the unexpected will happen. How are you going to view these concerning your growth and life? Will you break, or will you learn to remain calm under pressure?

Again, it's time to think about yourself. We have all experienced times of stress, crisis, and chaos. Are we using these as a chance to train for the next event? How do you handle the stresses of life? Have you considered tips for handling high-pressure situations? How can you better use these tips to improve handling the chaos that is to come?

1. Our Job is Not Revenge

We don't usually handle it in the civilian world to seek vengeance. We are not to return hack for hack. Yes, you will develop the skills that could allow you to exact revenge. The time is now to decide how you will respond when you find yourself in a situation where revenge is possible. How will you respond? How will you act to defend others? We are in cyber-defense, not in the life of revenge.

Are there organizations and agencies that hunt cyber-criminals? Who are these organizations? Think and talk about the difference between cyber-defenders and those that are cyber offensive.

## **Case Study**

A cyber incident can be a stressful experience. Yet remaining calm in the face of stress and the unknown can result in positive results and not in further failure. Below is a exploration of a incident that occurred, while not an attack, it was a stressful experience with a chance to either enter into panic or find a solution. The primary actor in the story remains calm and finds a solution to a stressful and difficult situation.

One story of a stressful situation is told here. A manager named Ted was working for a small ISP. The ISP owners are in the process of selling the ISP, and all the senior management has been given severance packages. Ted is one of the senior technicians who is trying to keep the call center and the technology working, until the full cut over to the new owners can take place.

On Monday morning Ted was the first at work in the office. As he walks into the office, he notices that the phone on the first desk is not powered on. While this is strange, things are being unplugged and moved as part of the transition. When he reaches his desk, he notices that his phone is not working either. Ok, so the call center is to open in a few minutes and a quick check confirms that none of the phones in the company are working.

Staying calm, Ted calls his supervisor who is off site, on personal business. Salley walks through the steps of checking the phone system and trying to reboot it. None of this works. Upon further investigation, the phone system will not boot up at all. Although it is getting power, there is no response from the system. Other staff are starting to show up for the day, and stress levels are rising.

Ted calls his other supervisor at the company that purchased them to see what steps they should take. Ted is informed to try to get the phone system functioning in some format, but that the data call center is being moved in less than a month and to keep costs near zero as possible. Stress is continuing to rise around the office. How can they do their job of answering customer calls with no phone system?

Staying calm, Ted begins thinking of what they need. What they need first is a functional phone to answer calls. Are any phones in the company working? Some quick testing finds that the fax machine is still working. This is a simple phone line. Thinking quickly, Ted figures out that it is possible to transfer the main line to an analog phone line, and they have a single functioning line for handling customer calls. Not enough, but a start.

Over the next couple of hours Ted, is on his cell phone with the phone company and is setting up roll-over lines to the various analog lines the company has. He then is buying and connecting a series of analog lines and answering machines. With the help of some paper clips, and creative wiring, by lunch they have a half a dozen phones set up that will pass through until answered or handed to an answering machine.

While not ideal, it did solve the immediate problem. Staying calm and thinking through the issue allowed Ted to solve a stressful and complex situation while still spending very little money. His makeshift system keeps servicing customers until the call center is transferred three weeks later.

**Case Study Questions**

1. How does this case demonstrate the skill of staying calm in a stressful situation?
2. Can you think of a time that you or someone you know has stayed calm in a stressful situation? How did this impact the outcome of the situation?
3. Can you think of a time when you or someone did not remain calm under stress? How did it impact the situation?
4. What is the outcome of remaining calm under pressure?
5. How do you think you can learn the ability to remain calm in the face of stress?

# Chapter 8

“I will not steal and will do everything within my power to prevent theft in all its forms.”

-The Cybersecurity Oath

This chapter looks at the ethics of stealing. In comparison, it is simple to say that you should not steal or that I will not steal. It is often clearer and more straightforward than one might think. This chapter begins to explore some of those challenges and where they impact technology and cybersecurity.

The chapter starts with a story of James copying a file he wrote at work and getting sued for Intellectual Property theft. This chapter continues by looking at instances of what theft might look like. It concludes with “Everything that I need to know I learned in kindergarten.” This chapter considers the ethical challenges and how we all might face them. Below is a set of discussion questions and a further case study to help students explore these issues and how to respond to them.

## **Discussion Questions**

1. If it’s free, it’s for me?

Ask your students to consider if they have ever downloaded anything shared illegally over the internet. Why the days of Napster and peer-to-peer file sharing are not in the high use that they once were, the idea of “if it is free, it’s for me” still exists throughout the internet. Bringing up the idea of downloading songs, movies, games, and other software from the Internet might, on its own, start the conversation.

Challenge students to consider the ethical and economic consequences of Internet Piracy. What is the problem if everyone downloads illegal copies of a product? What is the incentive for an artist or a company to continue to produce their products?

How does “if it’s free, it’s for me” extend beyond Copyright Property? What are the implications of stolen data from a company leaked online? If the data is stolen from a Nation and leaked? What are the possible consequences? If it is leaked emails from a company CEO?

The idea of information wanting to be free has excellent implications. As cybersecurity professionals, it is our job to defend information. We need to be careful that we are not stealing it as well.

1. Avoid a “Robin Hood” Narrative

This section resonated with me as the instructor who teaches our Penetration Testing courses. Not only do some cybersecurity professionals have offensive skills, but I am also the one teaching my students to hack systems and networks.

Ask your students to consider their thoughts on making a copy of a file – especially if that file does not belong to them. It is very easy to copy a file, yet some files have great value to the company or person they belong to – this is stealing. Is there a way to help everyone realize the implications of this type of theft? Can your students think of ways to help everyone to remember the value of intellectual property? As stated, we are defending data; our currency is trust, so we must take theft seriously.

Is there a place where stealing is ethically correct? The idea of Robin Hood draws many people in to consider there could be a time to steal – stealing with the right motives. Realizing this is likely. Who gets to decide when stealing is a good thing? Consider the ethical implications of deciding this time but not that time.

Another consideration is the legal. Are you willing to pay the legal price for what you are stealing? Even if you can find an ethical time to steal – it is still illegal, and you could face fines and jail time. Further stealing could damage the level of trust others place in you. This loss of trust will impact your current and future career.

1. A Tragedy of “Free Information”

Aaron Swartz is an excellent example of the legal consequences of being Robin Hood. Again, I am not commenting on who was right or wrong in this case. However, that could be an excellent discussion for the class. Have them read more about Aaron Swartz and discuss his actions and those of the courts.

In other thoughts, consider people like Edward Snowden or Harold Martin III. Each of these men had reasons for stealing data. In the cases of Snowden and Martin, it was from the US government. Did they think of themselves as Robin Hood? Were they correct in stealing this data? Again, who gets to decide when it is right to steal? What legal consequences did each of these faces and continue to face? What choice might you make in these situations?

Again, consider if you have made or downloaded an illegal copy of a file. Were you the right person to decide it was okay to steal this data? What legal consequences does this carry? What consequences does it carry for the trust you ask others to have in you?

1. Property is Property

The book makes it clear – the standard the line not to cross is that intellectual property (IP) is property. The discussion questions above have focused on the idea of stealing or not stealing data or IP. We can shift the conversation a little. Is it ever ethically correct to steal a car? Some may have argued that it is okay to steal 1s and 0s, but if property is property – a car should be the same as data. Is it the case that data and a car are equally wrong to steal? What if we ask about bank robbery? Even if I am going to give all the money away? (after all, I am Robin Hood 😉)

Stealing data could do more damage than auto theft. How can this be true?

Consider how you can avoid theft or even the appearance of theft as a cybersecurity professional. Given the case studies in the book, what are some ways that theft happens that perhaps you have not considered? How can you plan to protect yourself and your future employer?

1. Choices have Consequences.

As has been discussed through the above questions and the chapter in the book, choices have consequences. Theft is theft regardless of what one is stealing. The book states that the line between good and evil in cybersecurity is as simple as bad actors steal and good actors do not. Please discuss with your students their perspective on this.

Again, take time to consider the consequences of stealing Intellectual Property. I have heard it said often that data piracy is a crime with no victim. This is not true, yet it continues to permeate people's thoughts. What are the consequences of stealing Intellectual Property? Who suffers from this type of theft? What are the consequences to the various parties?

1. All I Really Need to Know I Learned in Kindergarten

“All I really need to know I learned in Kindergarten.” While this might not be true in every aspect of life, it is valid for theft, even intellectual property theft. “Do not take things that aren’t yours.” As a parent, I can say that many fights and bad actions would be avoided if my children would not take what belongs to their siblings.

As a student and future cybersecurity professional, how can you apply this principle to your life and professional career? Does this make it simple to remember?

How does a minor theft impact the trust others have in you? Remember, trust is the commodity that cybersecurity is built on. How will you maintain the trust of others and employers in your career?

## **Case Study**

When considering stories of employees stealing from the company and the consequences, one of the stories that comes to mind is an employee who misused company email. This is a tale of not only violating the Company's acceptable use policy but also of theft. Let’s take a few minutes and see what you, the student, think.

One day, Sam, the Head of IT, was approached by one of the company Vice Presidents and the Head of Human Resources. They requested a meeting in the HR department offices. Upon arriving at the meeting, Sam was presented with a request. The team suspected something was happening with one of the employees under the Vice President. They were unsure of the details of what the employee, Bob, was doing but believed there was a violation of the Acceptable Use Policy. They called the meeting to request Sam’s assistance investigating Bob’s computer activities.

The investigation began, exploring files and internet sites visited by company computers. The initial pass did not find anything out of the ordinary. Then, the HR Director asked for help examining Bob’s email. What was discovered in the email box was surprising. About a year earlier, Bob had begun to run a business, using company email as a primary form of communication. A history of correspondence that had grown over the year. With this information, files were found on the company computer and server that were also tied to Bob’s new business. Using time stamps on the emails by the end shows that Bob was spending most of his time at work, not working for the company, but running his own business. Further, this business appeared to have gained growth using the company email address since it was in a related field. So, Bob was also leveraging the company's reputation to grow his business.

Questions

1. What theft do you find in this case study?
2. Was Bob’s actions justified at any level?
3. Consider again whether Intellectual Property theft is victimless.
4. How do you think the company should respond in this case?

# Chapter 9

“I will protect and respect the privacy of others.”

-The Cybersecurity Oath

The chapter starts with a story about a privacy violation in the digital world. Privacy matters and is constantly threatened in our new digital world. While there are many different views on privacy, and different individuals view their level of privacy differently – it is still vital to defend the privacy of others. It is their lives and information to share or not to share. Remember, the chapter starts with a quote stating that privacy is a human right that must be maintained.

The chapter then continues to explore the concept of privacy and that cybersecurity professionals must work to defend the privacy of others. This includes not violating it ourselves or allowing others to violate this human right. The sections below will provide discussion questions and thoughts to help you and your students explore the idea of privacy. It will conclude with another case study to explore when talking about privacy.

## **Discussion Questions**

1. Curiosity Can Kill the Cat

Privacy is so important that it has been identified as a human right by the United Nations. If you have not considered this before, consider what this says about privacy. Why is privacy so crucial that the UN identifies it as a fundamental human right? What challenges to privacy have occurred in the past century that the UN was concerned about by declaring Article 12? What is the connection between privacy and dignity? How does protecting human dignity and value translate into protecting privacy?

In cybersecurity and Information Technology, curiosity is considered a good trait and essential to accomplish great things in your career. Yet this same curiosity can get you in trouble. This final chapter of the Code of Honor draws the various elements of the oath together. Here is where self-control is essential as well. How can curiosity get you in trouble concerning privacy? What might you have access to that could violate a person's privacy? If you are looking for some ideas, look first at the opening story of this chapter. How did our system administrators allow his curiosity to violate another's privacy? How else can one with access to another's data allow curiosity to violate privacy? Does having access mean that you should do an action?

1. The Golden Rule Applied to Cybersecurity

Preston’s story in this section is an all too familiar story. Young system administrators have lots of access and sometimes have seemingly dull jobs. Curiosity left unchecked can lead them down the wrong path. Can you think of ways Preston stepped past the privacy line in the story? Now, it did not end his career, but it could have. What types of checks should be in place to help prevent this type of invasion from happening? What types of checks do you think Preston might have in place now to help prevent his employees from going down a similar path?

How does treating others as you want to be treated translate into a digital world?

Most people want to be treated with respect and dignity. Therefore, we should make sure we are treating others with dignity and respect. When you consider working as a cybersecurity professional, what steps do you take to ensure that others are treated with respect and dignity? How can you work to protect the privacy of others?

1. Stay in Your Lane

When you hear stay in your lane what comes to mind? Staying in your lane is a great way to avoid violating another’s privacy. As a cybersecurity professional, you might have access to vast amounts of company data and develop the skills to access other data sets. Staying in your lane means focusing on the job/task you have been given and not simply looking at other data because you have access. How can you help to control yourself? Again, remember that self-control is also an essential part of the oath.

What type of controls can a company put in place to help protect the privacy of its employees and customers?

Is viewing confidential information without permission a violation of privacy? How can viewing information hurt other people? Consider the implications of viewing health information. What about financial information? Again, what are the consequences of viewing information without permission? These are important questions as you can access information you should not be viewing. Part of our job is to protect the privacy of others.

A follow-up question: what do you do when you see private information? Look at the last little story in the section. Did the system admin act ethically? Why or why not?

1. Four Questions to Help Avoid Impropriety

The book offers four questions to help us stay in our lane, stay focused, and not violate the privacy of others—it is time to consider these questions with your students.

1. Is the information essential to what I am working to investigate or trying to accomplish?
2. Is this information something that I would want others to see or know about if they were working on my system?
3. Am I getting into information here that was not intended for me?
4. Is this something that I need to be investigating alone?

How does each of these questions help to focus the intention of the cybersecurity professional? Sometimes, you might be tasked with digging through information not intended for you, for example, investigating a violation of acceptable use policy or some system compromise. How can these four simple questions still help keep you focused? How can having someone else join in the investigation assist in protecting privacy (question 4)?

What role do these questions play in protecting the privacy of others? Are there other questions that you think might also be helpful>

1. Each time You Cross the Line it Becomes Easier

We need to build the habit of making ethical decisions. We must make it commonplace that we choose to protect others' privacy and dignity. How can we help to avoid crossing the line? How can we work to ensure that we are above reproach?

What can you learn from Butch, the family dog? Do we learn to ignore the shock of violating privacy? Do we need to build walls around privacy? If so what does this look like?

1. We Hurt Real Human Beings

When privacy is violated, it is real people who are hurt. The chapter includes numerous examples of privacy violations in various industries. These violations do happen daily, but that does not make it okay. Can your students think of incidents of privacy violation that have occurred either personally or in the news? What is the impact of these violations? Just because privacy is broken daily does not make it acceptable. How do we, as cybersecurity professionals, work to protect the privacy of others?

Have you ever considered that cybersecurity is tasked with protecting the dignity of people? We are tasked, even called, to protect the privacy, dignity, and respect of people close and far. How does this call affect your view of your future career? You are not tasked with only protecting the 1s and 0s but with protecting the human rights and the privacy of those whose data you protect. How does this affect your view of being a cybersecurity professional?

1. Remember: We Are the Shield

Protecting others is the core of our mission. It does not matter where you work in cybersecurity; you are called to protect others. Depending on your specific job, this looks different, but you are tasked with and expected to help defend others. Remember, these are real people we are protecting, but just 1s and 0s. This is a protection of fundamental human rights. You have embarked on a mission with great significance. Does this change your view of the job you will be doing?

How will you maintain integrity and trust now and in the future? How can you help others to understand the importance of trust? How can you build and strengthen the trust that is granted to you?

You have read through the Code of Honor. Take time to reflect on the various points. How will these points help shape your ethical approach to cybersecurity? How do you plan to remain consistent with the trust given to you?

Remember, we are the shield that protects others. Stand firm, remember you are not alone – we stand together. We all make mistakes. Yet we work to stand. We work to shield others. Now, stand together and protect the human rights of others.

## **Case Study**

Protecting privacy sometimes means that we must help others protect themselves. This might be the most challenging part of protecting privacy: how do we help others ensure they do not violate privacy through their actions or actions? There are lots of stories and tales about people failing to protect their privacy. Listen to this tale and consider how you might have responded in similar or different ways.

A Vice President, Sue, brought her laptop and cell phone into IT for an upgrade of the cell phone. This was a normal process. The Company was working through cell phone users and upgrading one after another for users. The technician sat down at the table with the VP to begin the process. Opening Sue’s laptop, it was locked. This is good. The tech asks Sue to log in to the laptop so the upgrade can proceed as planned. Part of the process is to produce a local backup of the phone and restore it to the new phone.

Sue looks at the tech and says my password is … The technician, thinking quickly, politely stops Sue, saying we do not share passwords. Sue explains that she assumes IT can access all her data anyway – so why not share her password with them? This started a conversation about privacy and logging to track who is accessing what in a system – if there is a problem.

**Case Study Questions**

1. How is sharing a password a violation of one’s privacy?
2. Is this true even if the person receiving the password already has access?
3. What other ways can you think of that a user can violate their privacy?
4. Was Sue right in being willing to share her password with the IT team?
5. What damage could have resulted in Sue sharing her password?