1 Ethics in Cybersecurity

When the Watcher Gets Watched

2 Welcome!

- Thank you for attending this workshop!
- We will be looking at the field as a whole, how it has developed and how ethics has become important to build, maintain and display.
- We hope that this will help you on your path to becoming an ethical, professional cybersecurity professional!

3 The Days of Firewalls…

- Yes, there was a time where firewalls were all that you need!
- Before cybersecurity it was the days of assurance
  - 1960s – Era of password protection
  - 1970s – ARPANET
  - 1980s – The Internet grows
  - 1990s – The Days of Firewalls
  - 2000s – Digitization, the mass movements
  - 2010s – Errors of our ways (era of breaches, vulnerabilities, etc.)
  - 2020s – AI?
- Technology has progressed exponentially!
-

4 The First Virus – Pandora's Box

- Let's look at the 70s a bit more in-depth
  - The Creeper Program (1971)
    - Created by Bob Thomas
      - Experimental Program
    - Ray Tomlinson, wrote a new version (that same year)
      - Which replicated itself as it moved across the network (ARPANET; the first worm)
      - The Reaper (the first antivirus) would detect and remove the Creeper
  - Zeus (Created 2005, discovered in 2007)
    - The first information stealer used with an intent-to-harvest-data
- Today
  - GameOver Zeus – One of the variants of Zeus
  - Mindware – Ransomware targeting government, healthcare, engineering, & finance sectors
  - Onyx – Ransomware that destroys files larger than 2MB
  - Custom malware

5 Building Walls, Securing the Village

- Personal security
  - Security attacks are a trickle down economy
    - Meaning, most of the attacks that the personal consumer deals with, started as attacks on enterprise
- Cybersecurity is a personal effort
  - It is something that should impact our personal lives
    - Why? Because we share data and give data willingly/unwillingly

This Careers Preparation National Center product was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-22-1-0329), which is part of the National Security Agency.

    - Cybersecurity is also a personal responsibility
        - It’s our village, we have to build the walls for it
- Attackers understand this, as their efforts have shifted from attacking companies to attacking individuals
    - This is in an effort to minimize capture and increase profits/success
- That doesn’t mean that you are in this alone
    - Ethics help in building strong/solid walls

6 Building Systems, Securing the Nation

- Enterprise Cybersecurity
    - There are still challenges for companies and organizations
        - Advanced Persistent Threats (APTs) are a constant threat to organizations as a whole
        - APTs – are typically attacks that are carried out by groups (nation-states, fringe groups, activists, etc.)
- Organizations, like the nation, rely on ethical cybersecurity professionals to build these systems
    - To bolster defenses
    - To keep them and their customers secure
- Companies have had to make the transition from an assurance mindset to a Cybersecurity mindset
    - Information vs Data
    - Strategy vs Practice
    - Attack Vector
    - Risk Management
    - Offensive & Defensive
-
-

7 Legislation

- Security Initiatives
    - National Cybersecurity Strategies
    - Cybersecurity Awareness Campaigns
    - Corporate Cybersecurity Policies
    - Regulation & Compliance
        - GDPR – Comprehensive data protection law (EU), that sets guidelines for the collection and processing of personal information of individuals within the EU. It is intended to give individuals more control over their personal data.
        - COPPA – US Federal law that aims to protect the privacy of children under the age of 13 through placing restrictions on the online collection of their personal information.
        - HIPPA – Sets the standards for the protection of sensitive patient health information, restricting how information can be used by healthcare providers, insurance companies, and others, while also giving patients more control over their health information.
        - HITECH – Intended to address privacy and security concerns associated with electronic use and transmission of health information, it expanded the HIPAA rules.
- Legislation is typically the slowest to adapt to cybersecurity, as it has it’s own processes it has to go to etc. get something passed

8 The Rise of Defenders

- Blue Team

    - Term commonly used for defenders
        - Security Analyst
        - Information Security Officer
        - Incident Responder
    - Blue team typically defends, hardens, and strengthens a system or network
- CIA Triad
    - Confidentiality
    - Integrity
    - Availability
- Best Practices
    - NIST Framework
    - ISO (27001)
    - CISA

9 The Arms Race

- Red Team
    - Offense is still the best defense
        - Mentally, a defender should be able to think like the Red Team
        - Pen Tester
        - Ethical Hacker
        - Social Engineer Specialist
- Certifications
    - Cybersecurity Career Certifications (cyberseek.org)
- Ethical Practices
    - Become a requirement and not just a benefit
- Insiders/Rouge
    - What happens when someone with valuable knowledge or information goes rouge?

10 Development of Ethics

- Script Kiddies
    - Those starting out
- Hats
    - White – Good Guys
    - Grey – Ambiguous Guys
    - Black – Bad Guys
    - Blue – Revenge Guys
    - Green - Newbies
    - Red – Targets Black Hats
- Our Work Today
    - Development of the Cybersecurity Professional
    - Creation of the Cyber Defense Force

11 Ethics in the Field

- Accountability
    - Is necessary for any professional, but arguably more so in Cybersecurity
    - Trust is gained in drops and lost in buckets

        - It could result in a lost of career in cybersecurity
    - You will make mistakes, but will you own them?
- Professionalism
    - Goes hand-in-hand with ethics
    - Professionalism is more of your display/practice of your ethics and ability to perform within the role
- Life Skills
    - Helps in developing ethics and professionalism in all that you do
-

12 Activity: Company Ethics

- Have you ever read the Terms & Conditions on a service or software that you'd like to use?
- No?
    - Why?
        - Too long?
- Well, visit this site:

https://tosdr.org/

- In the next 10-15 minutes, document 3 points that surprised you for any of the services (feel free to mix and match)
- We will discuss them

13 Welcome Back!

- We hope your lunch was enjoyable!
- Did you share any of the interesting information you found?
- Did you look deeper into what you agreed to with these platforms?
- Ethics has an undeniable impact on our industry

14 Watching the Watchers

- Who are the watchers?
    - Data custodians
    - Analysts
    - Data Owners
    - Most in a cybersecurity role
- How do we watch the watchers?
    - Monitoring
    - Rotation of Duties
    - Mandatory Vacations
    - Reporting
- What are they Watching?
    - Our Networks
    - Systems
    - Data
- The relationship between the ones we trust with data and the ones we don't is…trust
- No matter your role in Cybersecurity you must be someone that the organization can trust and depend on

15 The Growth of the Cybersecurity Industry

- “Everyman…a phone?”
  - Consumerism & Devices
    - The average US household has 25 connected devices (telecompetitor)
    - Young people are most likely to be digitally connected (pewresearch)
      - To a Red Team, these are vectors. To a Blue team, these are places to defend
  - Security & Convenience
    - Finding the sweet spot is the goal of Cybersecurity
    - How do we keep systems, networks, people secure without compromising their convenience? Or at least meeting halfway in business and personal life
- The Rise of Viruses
  - Advance Persistent Threats & AI
    - While AI is an important tool to learn how to use, it will be used maliciously and companies have to prepare for this (They prepare by looking to hire ethical people like you ☺)
- Guidelines & Cyber Hygiene
  - CIS Controls
  - OWASP Top 10

16 The Needs of Today

- Professionalism & Ethics
  - And the ability to consistently display and abide by them
- Wild West is Over
  - Privacy
    - Is a debatable topic
  - Anonymity
    - Is another debatable topic
  - Systems should not be treated as inherently private and your online presence should not be treated as inherently anonymous
- On Professionalism
  - Essential Life Skills
  - Behind a Screen Doesn’t Mean Can’t Be Seen
  - Competencies
  - IT Roles – Understanding the job requirements and what is expected of you

17 Activity: Equifax Breach, A Company’s Duty to Others

- Take 10-15 minutes to read (and research further) over the Equifax Data Breach Case Study
- Consider the following:
  - What would you say the ethical responsibility to report should be for a company as large as Equifax?
  - How should time to notify be handled for a case such as this? Should a company as large as Equifax has special requirements?
  - How should the company deal with the long-term fallout? How should they deal with the impact on consumers short-term? What about long-term?
  - Given the magnitude of the incident, should we see governmental response? Any suggestion on legislation?
- We will take time to discuss this as a group!

18 Conclusion

- Thank you for attending this workshop!
- We hope that this helps you in your journey to becoming an ethical cybersecurity professional!
  - Remember it is about what you do when no one is watching
  - It is about standing for what is right
  - It is about doing the right thing, even if they give you a blank check
    - Money will run out, but your character never will
- No one’s path is the same
  - This is a community focused field
  - Participate! Reach out! Get involved!
- You’ll be happy you did