LIS 510
Human Factors in Information Security

Information School
University of Wisconsin-Madison
Spring 2022

Instructor: Dorothea Salo (please call me "Dorothea")
salo@wisc.edu
Student hours: 10:45-12:45 Thursdays, or by appointment
Canvas: https://canvas.wisc.edu/courses/244252
Special course attributes: Intermediate, Graduate, Digital Studies P, Social Science breadth (after Summer 2022)
Instructional mode: Online asynchronous

Introduction

Course description

Introduction to personal, social, and organizational concepts, skills, and processes related to the information security of individuals and organizations. Preparation to help individuals and organizations enhance their own security and privacy, especially but not exclusively online.

Phenomena to be examined include:

- individual and societal need for security
- infosec-related law; infosec ethics (including ethical hacking)
  - common ethical dilemmas in infosec: backdoors, censorship, vulnerability hoarding, vulnerability reporting, "hacking back"
- individual and organizational behavior with regard to infosec:
  - the psychology of human approaches to infosec
  - usability of infosec measures,
  - impact of (lack of) usability on infosec
  - incentives (and lack thereof) for good security practices
- infosec for marginalized populations
- common attack types against specifically human/organizational weaknesses
- risk assessment, risk mitigation, and incident response as human processes
- infosec training and communication
- penetration testing, virtual and physical

Assignments in this course offer repeated practice in *communicating* about privacy and security. Why? Because communication skills (such as incident reporting, composing training materials, communicating with people in power, and technical communication aimed at layfolk) are commonly noted as *absolutely required* in information-security job contexts—as well as commonly noted as lacking in too many information security professionals.

Course Policies

I aim to make this course as accessible as possible to all students. Students seeking accommodations for lecture or assignments must obtain a McBurney Center Faculty Notification Letter. For more information, see https://mcburney.wisc.edu/apply-for-accommodations/**.**

Preferred name/pronouns: Your name or gender may have been reported to me incorrectly. Please let me know your pronouns and preferred given name or nickname as you are comfortable. My pronouns are she/her/hers. UW-Madison lets students indicate a preferred name: https://registrar.wisc.edu/preferred_name.htm Canvas does as well, adding pronoun specification: https://kb.wisc.edu/luwmad/page.php?id=108069

Contacting me

READ THE SYLLABUS before asking a question, please; the syllabus may answer it! For any difficulty with the course that is not private or confidential, please use the Canvas questions and problems forum; I *will not answer such questions by email*. Should you see dead links (it does happen, usually with no notice), weird due dates, or other syllabus problems, please bring them up in the Canvas questions and problems forum. Please also do your best to assist your classmates there.

Textbooks and software

REQUIRED:

- Schneier, Bruce. *Secrets and Lies*. Wiley, 2000 (updated edition 2015). Library ebook: https://search.library.wisc.edu/catalog/9912219160102121 I encourage you to purchase your own; though its examples are admittedly dated, its explanations are classic. Any edition is fine; we will be reading whole chapters at a time, not page-specific segments.
- Andress, Jason. *Foundations of Information Security: A Straightforward Introduction*. No Starch Press: 2019. Library ebook: https://search.library.wisc.edu/catalog/9912897557802121

Assignments

Grading scale

All final grades will be based on this scale:

A: 93.5-100, AB: 89.5-93.4, B: 83.5-89.4, BC: 79.5-83.4, C: 73.5-79.4, D: 64-73.4, F: anything below 64.

Due dates below are specified by module (mostly for my reference); exact due dates are in the Canvas calendar.

	Final-grade %	Due date
Weekly assignments	21%	Each module (some modules worth 1 point, some 2)
In the News items	12%	Any time before the end of Module 7
Each one teach one!	10%	End of Module 11
Book review(s)	15%	Module 7; end of course for graduates' second review
Incident analysis		
Weekly deliverables	12%	Each module through module 12
Written public notice	5%	End of Module 4
Communication artifact	5%	End of Module 8
Presentation	10%	End of Module 12
Journalistic incident report	10%	Final day of course

Weekly assignments

Each course module will contain short surveys, reflections, experiments, investigations, or the like — analogous to tasks and discussions during the in-person class meetings we're not having — worth one or two final-grade points depending on their complexity or time cost. If you do the work conscientiously, you get the points; usually there will not be a specific "right answer" that I expect from you.

In the News

There is an "In the News" discussion forum on Canvas. Before the end of Module 7, post links and *brief* (3-5 sentence) summaries of *the human angle on* at least (undergraduates: two; graduates: four) just-published news items about privacy and/or security. Stories can come from:

- mainstream general news outlets (such as the *Wisconsin State Journal*, the *New York Times*),
- information-technology or information-security news outlets (such as *Ars Technica*, *The Verge*, *Hacker News*),
- higher-education news outlets (such as *Chronicle of Higher Education*, *Inside Higher Ed*, *Educause Review*),
- well-known and respected information-security weblogs (such as Troy Hunt's or Malwarebytes's), or
- (**MA/LIS students only**) library/archives news outlets (such as *American Libraries*, *Library Journal*)

By "the human angle" I mean that many news stories about information security focus on technology and technical issues. I want you to do the opposite: focus on *who*, not what, keeping in mind that "who" may be organizations of people as well as individual people. Who was affected here, in what way, and how severely (actually or potentially)? Who was responsible? Did someone mess up somewhere? What should we learn or do differently because of this? Beyond the summary, you are also welcome (but not required) to post your own reactions to and questions about the story.

By all means use Twitter to look for stories to post (I'll happily suggest accounts to follow!), but a tweet or tweet thread does not count for this assignment; same for a Facebook or LinkedIn post. (Don't rules-lawyer, please. The spirit of this rule is "social media can lead you to stories, but can't be the story.") You may post news stories covering novel academic research, but please do not post new research publications directly — stick to news. To make finding stories easier, I have set up an RSS feedreader with a public page you can consult; the link is on Canvas. Feel free to suggest sources I should add to it!

Book review(s)

Read and review a book! A good book review is no more (ideally much less) than 1000 words long (I am giving you a breather here; many review venues insist on half that or less, and *shorter does not mean easier to write*) and engagingly written. It often includes (but need not be limited to!) a BRIEF summary of the book's argument(s)/plot, a summary of the book's strengths and weaknesses, and a recommendation (or not) for reading or purchase along with a statement of appropriate audiences for the book.

I would specifically like you to evaluate how well the book *communicates its arguments* about security: for whom is it written? is it clear to that audience? understandable to them? persuasive? dismissive or otherwise offputting? scaremongering? hype-y? complete, or suspiciously incomplete? accurate (though consider publication date; things do change)? How might it improve its approach? Do you agree with its arguments?

For more reviewing advice, I strongly suggest perusing the "First-Time Reviewer" suggestions at the *LSE Review* website: http://blogs.lse.ac.uk/lsereviewofbooks/guidelines-and-examples/

UNDERGRADUATES: One book review, written as for a newspaper, magazine, or news website. You may, if you wish, specify the targeted publication.

GRADUATES: Two book reviews, each book from a different category in the categorized list below, written as for a scholarly or professional journal. (*College and Research Libraries* has a review section, as do quite a few other LIS journals.) You may, if you wish, specify the targeted publication, and I encourage you to contact journals that carry relevant reviews to volunteer to review one of the more recent publications on the list, or a new relevant book that does not appear on it.

Post your review to the Book Reviews forum on Canvas by the day it is due. The forum is open throughout the course; you are welcome and encouraged to post reviews early. Do NOT attach your review as a Word file or PDF, please; this will mean an automatic zero! You are not required to read all posted reviews, but I do recommend that you read reviews for as many of the different books/collections as possible.

BOOK LIST:

N.b. I don't approve of all the books below; I haven't even *read* all of them! Don't write a positive review just because you think I want one. You can be honest! I want to know what I should and shouldn't read.

Fiction and graphic novels

- Cory Doctorow, *Attack Surface*
- Annie Jacobsen, *First Platoon*
- Bruce Sterling, *The Zenith Angle*
- G. Willow Wilson, *Alif the Unseen*
- Hari Kunzru, *Transmission*
- Vaughn, Martin, and Vicente, *The Private Eye* (available for paid download from http://panelsyndicate.com/comics/tpeye)

Individual privacy and security

- Brian Kernighan, *Understanding the Digital World*
- Bruce Schneier, *Beyond Fear*
- Jacqueline Ryan Vickery, *Worried about the Wrong Things*
- Leron Zinatullin, *The Psychology of Information Security*

Society and security

- Bruce Schneier, *Data and Goliath* or *Click Here to Kill Everybody* or *Liars and Outliers* or *We Have Root*
- Nicole Perlroth, *This Is How They Tell Me The World Ends* (Recommended for business majors.)
- Jane Frankland, *InSecurity*
- Geoff White, *CrimeDotCom*
- Susan Landau, *Listening In*

Several books on the list are available electronically: on the open web, via UW-Madison library subscription, or for relatively-inexpensive purchase. You may be able to find some in local public libraries, but please observe all COVID-19-related

precautions if you avail yourself of a print library book. If you would like to review a relevant book I haven't listed (one excellent source is Cybersecurity Canon at https://icdt.osu.edu/cybercanon), tell me about it by the end of the first week of class, so I can decide whether to allow it. (Usually I say yes, but one constraint: I don't want you reviewing tool/technology-specific books, e.g. *Metasploit Unleashed*. It's a terrific book and I recommend it highly—but I want you to review books that take a *human-centric* view of information security.)

Grading criteria: Writing suitable for the specified outlet (use the Writing Center if you need it!), appropriate structure, depth of analysis and critique of the book's arguments, savvy reading/purchase recommendations.

Each one teach one!

Write an email that teaches someone you care about (your choice: family member, friend, acquaintance, roommate, classmate, work colleague, fellow volunteer...) as kindly, clearly, and briefly as you can *why* and *how* to avoid falling prey to a specific privacy or security threat (again, your choice; list below, but you are not limited to it). Definitely consider threats that the person has already experienced or is at high risk of experiencing. Honor system: pick a threat that's new to you, please. You may pretend that the person has already asked you for advice.

If you would like a classmate to teach you something, that's great! Request it in the Canvas forum for this assignment. To pick up a request from a classmate, simply reply with your email's subject line and text before the due date.

Briefly tell us about the tech-savviness level of, known risks to, and privacy/security habits of the person you chose — if it's not a classmate, *do not give us their name or any other directly identifying information without obtaining their explicit and unforced consent*, though — and post your subject line and email text to the designated Canvas discussion forum. HTML-style is fine (so you may use screenshots or other images if that's helpful). Plain-text posts may include attachments (which you attach via the paper-clip icon at bottom left of Canvas's text-input field).

Glance at a few of Bruce Schneier's analogies/explanations in *Secrets & Lies,* or posts on Troy Hunt's blog (e.g. https://www.troyhunt.com/fixing-data-breaches-part-2-data-ownership-minimisation/), for excellent examples of written explanations. Make it clear, make it kind, make it FUN, okay?

Some dangers you might warn the person you're teaching against (not an exhaustive list!):

- Phishing (choose ONE modality: email, SMS/texting, or social media)
- Identity theft (choose a specific form of it, e.g. financial-account impersonation or social-media account theft)
- Credential stuffing and/or password spraying (that is, attacks based on password reuse across accounts)
- Account theft (choose a specific account or account type you know the person has)
- Romance scams / catfishing
- 419 scams (choose a pretext relevant to the person you're teaching)
- Surreptitious workplace surveillance
- Bad passwords
- Ransomware
- Stalkerware
- Account compromise via "secret questions"
- Social engineering (choose a context plausibly relevant to the person you're teaching)

It's tempting to infodump. Don't. You're not writing this email to impress me, but to help the person you're writing to. You will lose points if I decide (and I've been teaching for over a decade) that you've lost or overwhelmed or shamed this person. Remember BLUF also: Bottom Line Up Front. Start with what the person should do right away, then explain why.

Incident report

Over the course of the class, you will study a real-world security incident and explain as clearly as possible what happened before, during, and after it. Your major deliverables will be a **journalistic incident report** (such as an information-security-focused journalist would write) **a written public notice and explanation** (such as an organization would release to journalists and the broader public), **the slides and script for an incident presentation** of no more than ten minutes, as though explaining the incident to **non-technical** leadership, and a **communication artifact** that urges people to protect themselves from this or similar incidents in future.

For examples of journalistic incident reports of the type I'd like to see from you, look at some of The Markup's writeups, e.g. on VPN privacy https://themarkup.org/ask-the-markup/2021/08/12/how-private-is-my-vpn and anti-doxing legislation https://themarkup.org/ask-the-markup/2021/08/17/should-doxxing-be-illegal

You must choose the subject of your incident report no later than the end of the second class module (so, in spring/fall, the end of week 2; in summer's eight-week session, the end of week 1).

UNDERGRADUATES: you may choose from the following list of specific incidents:

- US Office of Personnel Management employee-record breach ("OPM breach")
- Grinnell/Hamilton/Oberlin Colleges admissions files breach (2019)
- Proctortrack face-scan breach (2021)
- Edward Snowden NSA breach
- Facebook user-data breaches (most recent reported in 2021, but that's not the only one there's been!)
- Sony Pictures email and server breach
- SolarWinds supply-chain breach
- Breaches in India's Aadhaar government-services system (there have been several)

GRADUATES, please choose from the following list of *classes* of incident. Please research *at least two* real-world case studies (more is fine! word to the wise: information does disappear from the web, so recent incidents are easier to research) and in your journalistic report, compare and contrast the quality of prevention efforts and incident response:

- Internet of Things toy data breaches
- Internet of Things personal-assistant breaches (Alexa, Siri, Echo, etc)
- Student data breaches at colleges/universities (it's fine if employees were also affected, but please focus on students)
- Stalkerware incidents
- Student data breaches at K-12 schools (see `https://www.edtechstrategies.com/k-12-cyber-incident-map/` for help locating examples and coverage)
- Major ransomware attacks (choose an industry to focus on: I suggest K-12 education, health care, or government)

If you wish to analyze a different incident or (for graduates) class of incident, please clear it with me first. (Word to the wise: bigger, more complex, and more difficult failures are better! I will refuse simple obvious failures.) Keep a running list in a shareable online fashion (e.g. Google doc, Pinboard list, public Zotero list are all fine) of every source you discover about your subject, whether or not you use it in your deliverables; **add a link to your list to each deliverable you turn in**.

Deliverables:

- (End of each module through Module 12) A brief (one page or less, typically) narrative or set of notes responding to a weekly prompt about the incident (class) you chose. The prompt is in each module before its reading list. These are graded pass/fail (you get the weekly point or you don't, basically). They do not have to be polished prose or contain formal citations — an outline-style set of notes with URLs/links to sources is just fine. I recommend keeping all of these in the same document, with sections labeled by module (to help me grade); think of it as a master list of information you can pull from for your other deliverables.
- (Module 4) A press-release–style **public notice and explanation** of the incident. (**GRADUATES**: choose *one* of the actual incidents you are researching to write the notice about.) An excellent example you may base yours on: https://www.venafi.com/update-on-cybersecurity-incident Mention actual actions the organization took as often as possible.
- (Module 8) A *polished, persuasive, professional-quality* **communication artifact** about the (class of) incident, targeted to a group of people harmed by it and encouraging them to protect themselves from harm caused by it — consciousness-raising, changes in technology use, organizational activism, and political/legislative activism are all acceptable things to advocate for (but choose one, please). Adroit use of memes and tropes encouraged! The communication artifact may be any one of:
  - an online infographic (a bit more than a meme retread, please, though you may incorporate or riff off memes),
  - a physical flyer for posting to kiosks etc. (turn this in as a PDF)
  - a web page (ONE page, please, and no infinite scroll),
  - a short (three minutes maximum!) well-produced podcast or song,
  - a very short (one minute maximum!) public-service announcement (imagine it playing at WSUM),
  - a short (three minutes maximum!) well-produced video/screencast (think TikTok, and yes, you may use it), or
  - a newsy blog post OR news editorial (think Daily Cardinal, Badger Herald, or news.wisc.edu).

  I will grade and offer feedback on the quality and effectiveness of your communication as well as appropriate audience targeting. The exact action you choose to advocate for will not, however, be graded; that's up to you.
- (Module 12) An **incident presentation** comprising a well-designed, well-organized, compelling **slide deck** and **speaking script** with *no more than eight slides* (cover and concluding slide excluded; fewer slides is fine) explaining *as clearly and concisely as possible* to non-technical organizational leadership what happened before, during, and after the incident. **GRADUATES**: You may treat the incidents as a class, explaining how such incidents typically proceed. Also explain *how to avoid such incidents in future*. (No, you do not have more slides to do this in! That absolutely makes this assignment more challenging for you!)

- You are welcome to use the UW-Madison-branded slide templates (ugly though I find them), as using organizational branding would be perfectly reasonable in a real-life situation like this: https://brand.wisc.edu/multimedia/powerpoint/ If you would prefer to use a different template, that also is fine; do keep in mind that slide design influences how an audience receives and responds to a presentation.
- Place your speaking script in the "presentation notes" section of your slides. Remember that reading Old High Academese aloud is *absolutely deadly boring*; try to write the way you would naturally speak. (Yes, this means that sentence fragments, ending sentences with prepositions, and other English-writing solecisms are actually perfectly okay here!) Check out some of my talk scripts on my Speakerdeck to get a sense of what I mean by "write the way you talk:" https://speakerdeck.com/dsalo. I am aware that you are not me, however; write the way *you* talk, which is not necessarily the way I do.
- I will evaluate the slides for:
  - script appropriate to a workplace presentation for high-ranking people that should run *ten minutes or less*, and (crucially) *will not put them to sleep*
  - text and image legibility at a distance (i.e. don't try to get around the number-of-slides limit with teensy-tiny text; please also keep accessibility considerations in mind — my own eyes are aging!)
  - clarity of narrative (that is, the whole presentation needs to make sense as more than just a collection of random tidbits of information)
  - inclusion ONLY of clearly relevant, appropriate details (yes, this means infodumps will be penalized; I expect you to use good judgment about what organization leadership needs to know!)
  - work-appropriate impassivity (blame-and-shame is inappropriate)

- (End of course) A fully-compiled, well-written, well-structured, well-edited, well-designed *journalistic-style* **report** on your findings and your reaction to them. Yes, you are not only allowed but *expected* to editorialize and make recommendations. You will lose points if you turn in a bloodless, boring, infodumpy term paper. That's not what I want to read, or want you to write.

COURSE SCHEDULE AND READINGS

The quotes in module titles are from Broadway and TV/movie/web musicals. Have fun tracking them down, if you like!

Unit 1: Context

Module 1: "Look, I made a hat where there never was a hat." Setting the stage

Topics: Why individuals and organizations need security. Personal, social, financial, and reputational risks of poor security practices. Jobs in infosec. Stereotypes of infosec work and workers. DEI in infosec.

Incident report: Choose a ***breach/breach-class-and-examples*** *to work with. Build a* ***bibliography/webliography/linklist*** *(a GDoc is fine, or you may turn in a running document each week if you prefer) with as many sources as you can find about the breach. Skim your sources and make* ***a list of people/groups involved****, with* ***job titles*** *wherever possible, and quick notes about their role(s) in the incident (class) or the response(s) to it.*

In your image search engine of choice (which should of course be DuckDuckGo), search for "hacker." On the first page of results, count the number of images containing all of an actual human face. Now count the number of images containing a mask (other than a COVID-19 mask; typically you'll see the one from *V for Vendetta*). Now count the number of images with what I call an "undead hoodie with a laptop" (images that use the hoodie to conceal the upper part of the face count here too).

Schneier. *Secrets & Lies* chapter 5 "Security needs."

Rasch. "The symbiotic, parasitic relationship between privacy, security." https://securityboulevard.com/2020/01/the-symbiotic-parasitic-relationship-between-privacy-security/

Grauer. "Cybersecurity expert careers: skills to embrace, pitfalls to avoid." https://insights.dice.com/2020/08/04/cybersecurity-expert-careers-skills-embrace-pitfalls-avoid/

Sheridan. "Burnout, culture drive security talent out the door." https://www.darkreading.com/careers-and-people/burnout-culture-drive-security-talent-out-the-door

"What does it take to be a cybersecurity researcher?" https://thehackernews.com/2021/04/what-does-it-take-to-be-cybersecurity.html

Poster. "Cybersecurity needs women." https://www.nature.com/articles/d41586-018-03327-w

Spitzner. "Getting started in cybersecurity with a non-technical background." https://www.sans.org/security-awareness-training/blog/getting-started-cybersecurity-non-technical-background

NICCS. "NICE cybersecurity workforce framework." https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework (Click on each category and skim the subcategories. There's a lot!)

Module 2: "Everything is legal in New Jersey." Infosec ethics, law, and policy

Topics: Basic ethics; ethical hacking. The unsettled state of security law; why legal compliance is not the same as ethical treatment of the security of others. GDPR and infosec; US state laws and breach disclosure; BIPA. PCI, HIPAA, and other laws, regulations, and standards that involve security; "sectoral" vs. broad-based security/privacy/data-protection law. "Compliance mentality" and how it can be a problem. Attorney-client privilege and incident response.

Incident report: Investigate and list law and policy relevant to your chosen incident (class); note where regulation would apply today that did not apply (or possibly exist) at the time. As best you can, answer the questions in sections 3 (p. 17) and 8 (p. 19) of Part One of the Vallor/Rewak piece with respect to your chosen incident (class).

Vallor and Rewak. "An introduction to cybersecurity ethics." https://www.scu.edu/media/ethics-center/technology-ethics/IntroToCybersecurityEthics.pdf (Parts One, Four, and Five.)

Digital Forensics Certification Board. "Code of ethics and standards of professional conduct." https://dfcb.org/code-of-ethics-and-standards-of-professional-conduct/

Slayton. "The paradoxical authority of the Certified Ethical Hacker." https://limn.it/articles/the-paradoxical-authority-of-the-certified-ethical-hacker/

Jones and Kaminski. "An American's guide to the GDPR." https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3620198 (Introduction, Section II, and Conclusion only. This is a typical law review article: half footnotes. Ignore the footnotes!)

Schwarcz et al. "Do the legal rules governing the confidentiality of cyber incident response undermine cybersecurity?" https://www.lawfareblog.com/do-legal-rules-governing-confidentiality-cyber-incident-response-undermine-cybersecurity?mid=1

Bilyk. "Class action: Northwestern's online test proctoring wrongly collected face scans, other biometric identifiers." https://cookcountyrecord.com/stories/573732589-class-action-northwestern-s-online-test-proctoring-wrongly-collected-face-scans-other-biometric-identifiers (We use Honorlock, Proctorio, and Respondus on campus. What do they collect? If you don't know, whose responsibility was it to tell you?)

"The state of consumer data privacy law in the US (and why it matters)." https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/

Berens. "One US state stands out in restricting corporate use of biometrics: Illinois." https://www.reuters.com/technology/one-us-state-stands-out-restricting-corporate-use-biometrics-illinois-2021-09-16/

Disterer. "ISO/IEC 27000, 27001, and 27002 for information security management." https://serwiss.bib.hs-hannover.de/frontdoor/deliver/index/docId/938/file/ISOIEC_27000_27001_and_27002_for_Information_Security_Management.pdf

Unit 2: Adversaries and attacks

Module 3: "The history of the world, my sweet… is who gets eaten, and who gets to eat!" How adversaries think about (individuals') infosec

Topics: Types of attacks, and the human qualities they leverage. Phishing attacks; catfishing; smishing. Social engineering. SWATting. Revenge porn. Intimate-partner abuse, and how online and mobile enable attackers; defenses. Identity theft. Mobbing; Zoombombing.

Incident report: List and briefly describe any techniques discussed this module used in your (class of) breach. Create a timeline of the breach and responses to it (a bulleted list is fine; I don't need a visual-style timeline unless you really want to do it). Graduates: timeline at least two incidents, please.

Levy and Schneier. "Privacy threats in intimate relationships." https://doi.org/10.1093/cybsec/tyaa006 (Content alert: non-graphic domestic abuse, elder abuse, and child abuse.)

Cole. "How to tell if your partner is spying on your phone." https://www.vice.com/en_us/article/bjepkm/how-to-tell-if-partner-is-spying-on-your-phone-stalkerware

Pompon. "Phishing for your information: how phishers bait their hooks." https://www.darkreading.com/partner-perspectives/f5/phishing-for-your-information-how-phishers-bait-their-hooks-/a/d-id/1329753

Malwarebytes. "Child identity theft." https://blog.malwarebytes.com/awareness/2020/03/child-identity-theft-part-1-on-familiar-fraud/ and https://blog.malwarebytes.com/awareness/2020/03/child-identity-theft-part-2-how-to-reclaim-your-childs-identity/ (Please protect the young people in your life! They aren't usually given the tools to protect themselves!)

Cross. "From catfish to romance fraud." https://theconversation.com/from-catfish-to-romance-fraud-how-to-avoid-getting-caught-in-any-online-scam-115227

Fagone. "The serial SWATter." https://www.nytimes.com/2015/11/29/magazine/the-serial-swatter.html

Elmer, Burton, and Neville. "Zoom-bombings disrupt online events with racist and misogynist attacks." https://theconversation.com/zoom-bombings-disrupt-online-events-with-racist-and-misogynist-attacks-138389

Module 4: "Such tragedy to finally make the kill…" Attacks as human processes

(the above lyric is especially obscure: kudos to anyone who actually recognizes it without searching!)

Topics: How attacks often proceed; attack models and vocabularies such as MITRE ATT&CK, Cyber Kill Chain, VERIS Framework. Adversarial thinking. Tactics, techniques, and procedures (TTPs). Attribution, and why it is difficult. Nation-state hacking. CVE and CVSS.

Incident report: Add TTPs discussed this module to your list from last module. Do a VERIS-style actors/actions/assets/attributes analysis; you may use the VERIS webapp for this if it's useful, or if you wish to get acquainted with it. Also suggest appropriate risk mitigation strategies.

Schneier. *Secrets & Lies* chapter 2 "Digital threats," chapter 4 "Adversaries."

Winchester. "What's in a name? TTPs in infosec." https://posts.specterops.io/whats-in-a-name-ttps-in-info-sec-14f24480ddcc

"Common Vulnerabilities and Exposures. "Overview" https://www.cve.org/About/Overview and "Process" https://www.cve.org/About/Process

Muncaster. "Twitter mentions more effective than C[ommon] V[ulnerability] S[coring] S[ystem] at reducing exploitability." https://www.infosecurity-magazine.com/news/twitter-effective-cvss/

Hospelhorn. "What is the Cyber Kill Chain." https://www.varonis.com/blog/cyber-kill-chain/

Strom. "ATT&CK 101." https://medium.com/mitre-attack/att-ck-101-17074d3bc62

"VERIS." http://veriscommunity.net/ (Read down the left-hand navigation; stop after the four "Incident Details" pages.)

Stamos. "Tech's adversaries vs enemies." https://medium.com/@alexstamos/techs-adversaries-vs-enemies-a5ca09e09aca

Aucsmith. "The technology and policy of attribution." https://web.archive.org/web/20160729201915/https://cyberbelli.com/papers/attribution/

"Nation-states are taking their supply-chain attack strategy from the cybercriminal underground." https://intel471.com/blog/solarwinds-supply-chain-attack-iran-russia-north-korea (Pay attention to the hacking groups discussed here, and their origins and goals; they are examples of so-called "advanced persistent threats.")

Zetter. "Masquerading hackers are forcing a rethink of how attacks are traced." https://theintercept.com/2017/10/04/masquerading-hackers-are-forcing-a-rethink-of-how-attacks-are-traced/

Module 5: "He's the bafflement of Scotland Yard." How infosec professionals think about attacks and attackers

Topics: Threat modeling. Types of adversaries; routine surveillance creating new types of adversaries. "Advanced persistent threats." OSINT, opsec. Security for activists, journalists, and students.

Incident report: What is known about threat models for the data in your chosen (class of) incident? What is known about likely adversaries for this class of data? What is known (if anything) about specific adversaries responsible for your chosen (class of) incident? Do a quick OSINT sweep on the organization(s) in your (class of) incident; what can you find that might be useful in an attack?

Foundations chapter 7 (This chapter isn't entitled "Threat Modeling" but arguably should be!)

EFF. "Your security plan." https://ssd.eff.org/en/module/your-security-plan

"Open source intelligence." https://www.thecybersecurityexpert.com/open-source-intelligence-what-is-it-and-how-can-you-use-it-to-defend-your-organisation/

Hayden. "A guide to open source intelligence (OSINT)." https://www.cjr.org/tow_center_reports/guide-to-osint-and-hostile-communities.php

Krebs. "Who is the network access broker 'Wazawaka'?" https://krebsonsecurity.com/2022/01/who-is-the-network-access-broker-wazawaka/ (Read this for how the criminal in question left followable traces in his computer and internet use, then think about the traces YOU leave. That's opsec in a nutshell!)

Marino and Mitchell. "How activists should be thinking about cybersecurity." https://www.theverge.com/21298915/cybersecuirty-activism-tech-matt-mitchell-interview-vergecast (Either reading the transcript or listening to the podcast is fine, whichever you prefer.)

Berdan. "An evaluation of online security guides for journalists." https://cltc.berkeley.edu/wp-content/uploads/2021/01/Online_Security_Guides_for_Journalists.pdf (Undergraduates: just the executive summary.)

Satariano. "How my boss monitors me while I work from home." https://www.nytimes.com/2020/05/06/technology/employee-monitoring-work-from-home-virus.html?smid=tw-share (This boss is an adversary!)

Swauger. "Leaving surveillance tech behind in higher education." https://belonging.berkeley.edu/sites/default/files/tech_equity_leaving_surveillance_proof_1.pdf (Find the adversaries!)

Doyle. "Why don't you trust us?" https://jitp.commons.gc.cuny.edu/why-dont-you-trust-us/ (Find the adversaries, again!)

Park and Vance. "Higher education voices: college students' attitudes toward data privacy." https://studentprivacycompass.org/resource/higheredvoices2021/ (Based on what you now know... are students worried enough, do you think?)

"Finding McAfee: a case study on geoprofiling and imagery analysis." https://medium.com/@benjamindbrown/finding-mcafee-a-case-study-on-geoprofiling-and-imagery-analysis-6f16bbd5c219

Unit 3: Individuals and infosec

Module 6: "Why do you do these things you do?" The psychology of security

Topics: Heuristics. Habituation; security fatigue. Error messages. "Folk models" of security. Usability and security; the importance of defaults. Passwords as paradigm example of individual approaches to infosec, and (un)productive responses to them; password managers; authentication apps.

Incident report: Read coverage of your chosen incident (class) for examples of any of the psychological phenomena discussed in the readings and lecture; list those you find, quoting evidence.

Foundations chapters 3 and 8

Schneier. *Secrets & Lies* chapter 17, "The human factor."

Check a few of your favorite passwords in Troy Hunt's https://haveibeenpwned.com/Passwords. IMMEDIATELY CHANGE ANY THAT HAVE BEEN PWNED. Also check your email addresses in https://haveibeenpwned.com/ and change passwords on any accounts that come up that you didn't already know about and change the password for. Can I interest you in a password manager now? I can? Good. Ask in the Jargon File forum if you would like recommendations.

Take the quiz at http://www.pewinternet.org/quiz/cybersecurity-knowledge/ and then read Olmstead and Smith "What Americans know about cybersecurity." http://www.pewinternet.org/2017/03/22/what-the-public-knows-about-cybersecurity/

Parsons et al. "Human factors and information security: individual, culture, and security environment." https://apps.dtic.mil/sti/pdfs/ADA535944.pdf (Parts 1, 2, and 3.)

Wash. "Folk models of home computer security." https://www.rickwash.com/papers/rwash-homesec-soups10-final.pdf

Cram. "When enough is enough: investigating the antecedents and consequences of information security fatigue." https://doi.org/10.1111/isj.12319 (Undergraduates: skip the Methods section. Graduates: don't you dare skip it.)

Francis. "Vendors approve of NIST password draft." https://www.csoonline.com/article/3195181/data-protection/vendors-approve-of-nist-password-draft.html

McGregor et al. "Investigating the computer security practices and needs of journalists." https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-mcgregor.pdf

Greenberg. "High-stakes security setups are making remote work impossible." https://arstechnica.com/information-technology/2020/03/high-stakes-security-setups-are-making-remote-work-impossible/

Module 7: "For there's nothing I enjoy like a horrible muddle!" Individual device security

Topics: Computer, tablet, and phone security. Network-equipment security. Firmware security. Internet of Things security and privacy. Side-channel attacks. Remote-desktop protocols; RATs. Botnets and staying out of them. Adware, spyware, stalkerware, ransomware, keyloggers. Defenses: antimalware software, device firewalls. Authentication and authorization; multi-factor authentication; physical security keys. Biometric authentication and its security failings.

Incident report: Were any individually-used devices (not servers!!!) compromised in your (class of) incident? Did they belong to the organization or to an individual? How were they compromised, and how was the compromise discovered?

Foundations chapter 12

Schneier. *Secrets & Lies* "Identification and authentication," chapter 14 "Secure hardware"

CCSI. "Authentication, authorization, accounting, and identity management." https://www.ccsinet.com/blog/aaa-identity-management/

Davies. "The rise of biometric data technology." https://www.theguardian.com/technology/2021/oct/26/conditioning-an-entire-society-the-rise-of-biometric-data-technology

Krakenfx. "Your fingerprint can be hacked for $5." https://blog.kraken.com/post/11905/your-fingerprint-can-be-hacked-for-5-heres-how/

Cox. "The NSA and CIA use ad blockers because online advertising is so dangerous." https://www.vice.com/en/article/93ypke/the-nsa-and-cia-use-ad-blockers-because-online-advertising-is-so-dangerous (You should too. I suggest uBlock Origin.)

Fairfield. "The 'internet of things' is sending us back to the Middle Ages." https://theconversation.com/the-internet-of-things-is-sending-us-back-to-the-middle-ages-81435

"IoT [Internet of Things] security for policymakers." https://www.internetsociety.org/resources/2018/iot-security-for-policymakers/

Korolov. "What is a botnet?" https://www.csoonline.com/article/3240364/what-is-a-botnet.html

Horowitz. "Router security." https://www.routersecurity.org/ (At least the short list and "Ongoing Care and Feeding.")

Roberts. "Huge survey of firmware finds no security gains in 15 years." https://securityledger.com/2019/08/huge-survey-of-firmware-finds-no-security-gains-in-15-years/

Cunningham. "Phone and laptop encryption guide." https://arstechnica.com/gadgets/2015/08/phone-and-laptop-encryption-guide-protect-your-stuff-and-yourself/ (Do these things. Do them!)

Hornby. "Side-channel attacks." http://www.cryptofails.com/post/70097430253/crypto-noobs-2-side-channel-attacks

Module 8: "'Till the clouds roll by…" Online and cloud account security

Topics: PKI, digital signatures, certificates, and their pitfalls. Common attacks on online accounts; address-book attacks. Cloud storage and its security models; "zero knowledge." Social media and other online accounts (including online source control such as git) as grist for OSINT and social-engineering attackers. Why anonymity is a pipe dream; data brokers as attackers; reidentification.

Incident report: What can you discover about how authentication and authorization were handled at the organization(s) breached? Can you identify any attacks contributing to the incident via online accounts at third-party services?

Schneier. *Secrets & Lies* chapter 15 "Certificates and credentials."

Newman. "Why the password isn't dead quite yet." https://arstechnica.com/information-technology/2021/07/why-the-password-isnt-dead-quite-yet/

Wiefling et al. "More than just good passwords? A study on usability and security perceptions of risk-based authentication." https://riskbasedauthentication.org/usability/perceptions/ (Graduates: click through to read the actual paper.)

King. "Chicago cops use social media to track grieving families of gunshot victims." https://onezero.medium.com/chicago-cops-use-social-media-to-track-grieving-families-of-gunshot-victims-e68e5a6dc40c

Botticello. "Subtle information hackers find in the background of your social media photos." https://medium.com/digital-marketing-lab/subtle-information-hackers-find-in-the-background-of-your-social-media-photos-938ec1876246

Alvarenga. "Cloud security: 12 myths vs. facts." https://blog.checkpoint.com/2020/09/28/cloud-security-12-myths-vs-facts/

Green. "iCloud: who holds the key?" https://blog.cryptographyengineering.com/2012/04/05/icloud-who-holds-key/ (Moral: iCloud is not zero-knowledge. Cloud providers that are exist, and include SpiderOak and Tresorit.)

Whittaker. "Hundreds of exposed Amazon cloud backups found leaking sensitive data." https://techcrunch.com/2019/08/09/aws-ebs-cloud-backups-leak/

Unit 4: Organizational behavior and infosec

Module 9: "We dare not leave him to his own devices." Threats to organizations

Topics: Insider threat. Contractor threat. Supply-chain threat. Business-email compromise. Ransomware. Business email compromise. How social engineering contributes to organizational hacks. Spearphishing. BYOD. Cloud (in)security. Defenses; perimeter defenses (firewalls, DMZs) and their inadequacies; zero-trust security.

Incident report: As with prior modules, discuss the applicability of phenomena from this module to your chosen (class of) incident.

O'Donnell. "Silent Librarian retools phishing emails to hook student credentials." https://threatpost.com/silent-librarian-phishing-student-credentials/149249/

Cohney et al. "Virtual classrooms and real harms." https://arxiv.org/pdf/2012.05867.pdf (This is basically a supply-chain analysis of educational technology.)

Leyden. "Who's hacking into UK unis?" https://www.theregister.com/2018/09/17/cyber_attack_uk_universities/ (I am 100% sure it's no different here…)

Weise. "A hacker's best friend is a nice employee." https://www.usatoday.com/story/tech/news/2016/08/15/hacker-social-engineering-defcon-black-hat/88621412/

Gallagher. "Why you can't bank on backups to fight ransomware anymore." https://arstechnica.com/information-technology/2020/02/why-you-cant-bank-on-backups-to-fight-ransomware-anymore/

Vaas. "Florida city sends $742K to fraudsters as it bites the BEC hook." https://nakedsecurity.sophos.com/2019/11/05/florida-city-sends-742k-to-fraudsters-as-it-bites-the-bec-hook/

Scheier. "Understanding the dissolving network perimeter." https://www.csoonline.com/article/3243272/understanding-the-dissolving-network-perimeter.html#jump

Shackelford. "Zero-trust security." https://theconversation.com/zero-trust-security-assume-that-everyone-and-everything-on-the-internet-is-out-to-get-you-and-maybe-already-has-160969

Module 10: "Frenzy and frolic, strictly symbolic…" Organizational infosec behavior

Topics: Security practices within businesses; reporting lines. "Shadow IT," BYOD. Relationships between IT and information-security professionals. Security practices in software development. Why security is often ignored until a crisis happens. "The market" and security incentives. Vulnerability disclosure practices, vulnerability hoarding, CVEs, CISA, bug-bounty programs. Blaming security researchers and bug-hunters; abuse of CFAA and DMCA.

Incident report: Outline (or draw an org chart of) the security people in the organization(s); to whom in the larger organization(s) did they report? If security was outsourced, give what details you can about the outsourcing arrangement. How long had the organization(s) had dedicated security people (if they even did)? How did the organization(s) targeted in your (class of) breach fail ***as organizations****? Do you notice any of the pitfalls discussed in this module?*

Foundations chapters 4 and 12

Singer and Perlroth. "Zoom's security woes were no secret to business partners like Dropbox." https://www.nytimes.com/2020/04/20/technology/zoom-security-dropbox-hackers.html

Anderson and Moore. "The economics of information security." http://science.sciencemag.org/content/314/5799/610.full

Magee. "Who owns cybersecurity risk management?" https://blog.gigamon.com/2017/05/26/owns-cybersecurity-risk-management/

Baxter. "The risk of shadow IT to business continuity." https://www.csoonline.com/article/3237226/business-continuity/the-risk-of-shadow-it-to-business-continuity.html

Carhart. "About cybersecurity management and expectations." https://tisiphone.net/2020/10/27/about-cybersecurity-management-and-expectations/

Nather. "Four reasons why organizations can't 'just patch.'" https://duo.com/blog/opinion-4-reasons-why-organizations-cant-just-patch

Ellis and Stevens. "Bounty everything: hackers and the making of the global bug marketplace." https://datasociety.net/wp-content/uploads/2022/01/BountyEverythingFinal01052022.pdf (Undergraduates may skip parts II and III.)

Bluestein. "The lock-picker, the lockmaker, and the odyssey to expose a major security flaw." https://www.bloomberg.com/news/features/2021-12-22/ethical-lock-pickers-team-up-with-manufacturers-to-solve-major-security-flaws

Brodkin. "Emails show what happened before Missouri governor falsely called journalist a 'hacker.'" https://arstechnica.com/tech-policy/2021/12/missouri-planned-to-thank-security-journalist-before-governor-called-him-a-hacker/

Pfefferkorn. "America's anti-hacking laws pose a risk to national security." https://www.brookings.edu/techstream/americas-anti-hacking-laws-pose-a-risk-to-national-security/

Module 11: "Beware, you'll scuttle the ship!" Programming practices and infosec; the "infosec market" and the attackers' market

Topics: Infosec in CS and software-engineering education. Infosec practices in open source; how open-source sustainability complicates the issue. Infosec and QA/QC practices; why standard QA/QC will not detect many vulnerabilities. Infosec and end-user programmers. Infosec and choice of programming language. Infosec blue-team tooling: log analyzers, SIEMs, etc. Snake oil in infosec; how to detect and avoid it.

Incident report: What went wrong with the technical infrastructures leveraged during your chosen (class of) incident? How much of it was under the targeted organization's direct control?

Schneier. *Secrets & Lies* chapter 13 "Software reliability" and chapter 22 "Product testing and verification."

Hunt. "The effectiveness of publicly shaming bad security." https://www.troyhunt.com/the-effectiveness-of-publicly-shaming-bad-security/ (Contrast this with my repeated "no blame" exhortations. Which is useful or appropriate in which situations?)

Tahaei et al. "'I don't know too much about it': on the security mindsets of computer science students." https://doi.org/10.1007/978-3-030-55958-8_2 (CS majors: TAKE CS 642. TAAAAAAAKE IIIIIIIIIIIIT.)

Vaas. "Study throws security shade on freelance and student programmers." https://nakedsecurity.sophos.com/2019/03/12/study-throws-security-shade-on-freelance-and-student-programmers/

Robinson. "You fired your top talent. I hope you're happy." https://startupsventurecapital.com/you-fired-your-top-talent-i-hope-youre-happy-cf57c41183dd

O'Neill. "The internet runs on free open-source software. Who pays to fix it?" https://www.technologyreview.com/2021/12/17/1042692/log4j-internet-open-source-hacking/

Hughes. "Open-source developers say securing their code is a soul-withering waste of time." https://www.techrepublic.com/article/open-source-developers-say-securing-their-code-is-a-soul-withering-waste-of-time/

Roth. "Open source developer corrupts widely-used libraries, affecting tons of projects." https://www.theverge.com/2022/1/9/22874949/developer-corrupts-open-source-libraries-projects-affected

Muncaster. "Organizations now have 76 security tools to manage." https://www.infosecurity-magazine.com/news/organizations-76-security-tools/

Stockley. "Stop. Do you really need another security tool?" https://blog.malwarebytes.com/malwarebytes-news/2021/10/stop-do-you-really-need-another-security-tool/

Module 12: "The day needs my saving expertise!" Incident response

Topics: Good and bad incident-response practices. Incident reports, root-cause analysis, "blameless post-mortems". Planning for good incident response. Incident-response teams.

Incident report: Had there been successful attacks against the organization(s) before? How (and how well) were they handled? What, if anything, did the organization(s) do to prevent further attacks? Explain as best you can attacker motives and TTPs. Describe what you can of the incident response, and assess its quality.

Whittaker. "How to decode a data breach notice." https://techcrunch.com/2020/05/19/decoding-data-breach-notice/

"Best practices for victim response and reporting of cyber incidents." https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/04/30/04272015reporting-cyber-incidents-final.pdf

Hunt. "Data breach disclosure 101: How to succeed after you've failed." https://www.troyhunt.com/data-breach-disclosure-101-how-to-succeed-after-youve-failed/

Ruefle. "Defining computer security incident response teams." https://www.us-cert.gov/bsi/articles/best-practices/incident-management/defining-computer-security-incident-response-teams

Muncaster. "CTOs keeping quiet on breaches to avoid cyber blame game." https://www.infosecurity-magazine.com/news/ctos-keeping-quiet-breaches-blame

Cooper. "The day after: your first response to a security breach." https://technet.microsoft.com/en-us/library/2005.01.incidentresponse.aspx

McLaughlin. "Post Mortem: Death Star data breach by ROGUE ONE." https://www.threatstack.com/blog/post-mortem-death-star-data-breach-by-rogue-one/ (Humor, but also a solid, if brief, example of an incident report!)

Tilbury. "How not to build a digital archive: lessons from the dark side of the force." https://preservica.com/blog/how-not-to-build-a-digital-archive-lessons-from-the-dark-side-of-the-force/ (Likewise.)

Module 13: "They've got to be carefully taught…" Infosec training and auditing

Topics: Training, why it often doesn't work, and how it can. Considering training audiences. Controversies over phishing tests. Penetration testing: pretexts, OSINT, physical pentests; the tricky legalities involved.

Incident report: no new material; concentrate on final deliverables.

Pacific Library Partnership. "Data privacy and cybersecurity best practices training: train-the-trainers handbook." https://1gp3bd3nt4aa1f5uv53pfuu3-wpengine.netdna-ssl.com/wp-content/uploads/2021/09/PLP-Cybersecurity-Handbook_508-Compliant.pdf

Education Development Center. "Teaching middle schoolers about cybersecurity." https://www.edc.org/teaching-middle-schoolers-about-cybersecurity

Kohen. "How managers can best communicate the importance of cybersecurity to employees." https://www.csoonline.com/article/3261430/how-managers-can-best-communicate-the-importance-of-cybersecurity-to-employees.html

McKenzie. "Getting personal about cybersecurity." https://www.insidehighered.com/news/2017/11/22/university-gets-personal-its-students-about-cybersecurity

Wright and Thatcher. "Phishing tests are necessary [sic]. But they don't have to be evil." https://hbr.org/2021/04/phishing-tests-are-necessary-but-they-dont-need-to-be-evil (I disagree that they're necessary, myself...)

McHenry. "Deciphering security assessment jargon." https://informationsecuritybuzz.com/articles/deciphering-security-assessment-jargon/

"Inside the courthouse break-in spree that landed two white hat hackers in jail." https://www.wired.com/story/inside-courthouse-break-in-spree-that-landed-two-white-hat-hackers-in-jail/

Module 14: "You're responsible! You're the one to blame! It's your fault!" Finding and analyzing human traces in systems: logging, auditing, digital forensics

Topics: Logs and auditing. Storage-device forensics; filesystems and forensics. Memory forensics. Network forensics; Wireshark. Remanence. Ethics, the Fourth Amendment, and forensics. Sunshine laws; FOIA requests.

Incident report: no new material; concentrate on final deliverables.

Rautner. "Evaluating evidence and information sources." https://kit.exposingtheinvisible.org/en/how/evaluate-evidence.html

Strickland. "How computer forensics works." http://computer.howstuffworks.com/computer-forensic.htm (Pages 1-6.)

US Department of Justice. "Digital forensic analysis methodology." https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/03/26/forensics_chart.pdf

Wade. "Memory forensics: where to start." https://www.forensicmag.com/article/2011/06/memory-forensics-where-start

Sartin. "Network postmortem: forensic analysis after a compromise." https://www.computerworld.com/article/2573728/security0/network-postmortem--forensic-analysis-after-a-compromise.html

Wilson. "Legal issues with cloud forensics." https://www.forensicmag.com/article/2015/05/legal-issues-cloud-forensics

Bureaucratic garbage you don't care about that the Powers that Be make me put in my syllabi

This course requires Junior standing.

Credit hours and regular and substantive student-instructor interaction

Students completing this course will earn three credit hours. The credit standard for the course is met by an expectation of a total of 135 hours of student engagement with the course learning activities (at least 45 hours per credit). Students should expect 150 minutes per week (in Canvas video) of lecture, full-class and small-group discussion on Canvas moderated by the instructor, and individual or small-group activities with outcomes reportable to (and assessed by) the instructor. Students should expect to work on course learning activities (reading, writing, studying, etc) for about three hours out of the classroom for each class period, doing readings, individual assignments and projects and other student work as described in the syllabus.

This course will provide regular and substantive student-instructor interaction in the following ways:

- The instructor provides direct instruction weekly in lecture;
- The instructor will assess and provide substantive feedback on student coursework regularly as assignments are due;
- The instructor will regularly provide information and respond to questions about the content of a course through weekly instruction in lecture, regular office hours, and communication through email and Canvas;
- The instructor will facilitate group discussions and group critiques related to course content through weekly direct instruction on Canvas.

Course learning outcomes

1. Communicate clearly and effectively to non-expert audiences about security vulnerabilities and security-related incidents (both grad and undergrad).
2. Mitigate common human-centered risks to information security and privacy (both grad and undergrad).
3. Develop awareness of the structure of the information security field, and career opportunities within it (both grad and undergrad).
4. Build strategies and sources for current awareness of security issues (both grad and undergrad).
5. Demonstrate understanding of professional competencies important for management of information organizations (graduate).
6. Demonstrate understanding of societal, legal, policy or ethical information issues (graduate).

7. Demonstrate understanding of issues surrounding marginalized communities and information (graduate).

MA/LIS: This course is designed to assess the following program-level learning outcomes: 4, 6, 7

iSchool learning outcomes

MA/LIS learning outcomes	Assignments measuring outcomes
1. Students demonstrate understanding of societal, legal, policy, or ethical information issues.	
4. Students demonstrate understanding of professional competencies important for management of information organizations.	
7. Students demonstrate understanding of issues surrounding marginalized communities and information.	

Digital Studies Learning Outcomes

For Digital Studies students, this course fulfills the P requirement, and is designed to develop masteries related to the following program learning objectives:

Digital Studies Program Learning Objective	Course Material that Addresses LO
To understand key theories and concepts related to digital studies and the historical context surrounding the creation of digital technologies	Conceptual models of security (CIA model, CyberKillChain, MITRE ATT&CK) discussed and employed in the campus data report. Standards creation discussed.
To gain familiarity with methods, concepts and tools needed to research and evaluate information related to digital studies	OSINT as a research method employed throughout course.
To think critically about how digital technologies work and their impact on society	Each-one-teach-one assignment, breach report require critical thinking about security.
To be able to create strategic communication content and self-expression using digital tools	One campus data report deliverable is a persuasive communication aimed at targets of a data breach.
To understand the professional and ethical principles related to the field of digital studies	Ethics introduced explicitly in first course module, referred to throughout rest of course.