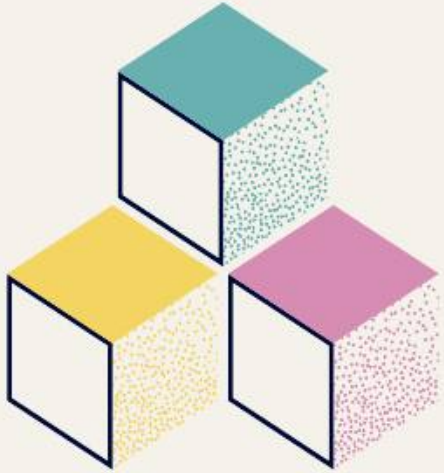


People, Policy, and Security

Cybersecurity through a social science lens: the theories, the people, and the structures

Briannah Greene · Old Dominion University

Security Is a Human Problem First

Tech alone doesn't stop breaches

Firewalls and encryption matter, but most incidents trace back to a decision someone made, a password reused, a link clicked, a policy ignored.



Criminology explains behavior

Routine activity theory and deterrence theory, borrowed from criminology, describe why offenders act and what discourages them.



Policy decides who's protected

Who gets security resources, who gets left out of the research, and who responds to an incident are social and political choices.



Two Theories That Explain Cyber Offending

Routine Activity Theory

A crime happens when a motivated offender, a suitable target, and no capable guardian happen at once

Online, the "guardian" is patching, monitoring, and access control, and a lot of breaches happen simply because no one was watching. .





Deterrence Theory

People avoid crime when the cost of getting caught outweighs the benefit of the act.

Weak cross-border prosecution is why deterrence breaks down online, offenders can act from almost anywhere consequences can't easily reach.

Same Pattern, two different incidents

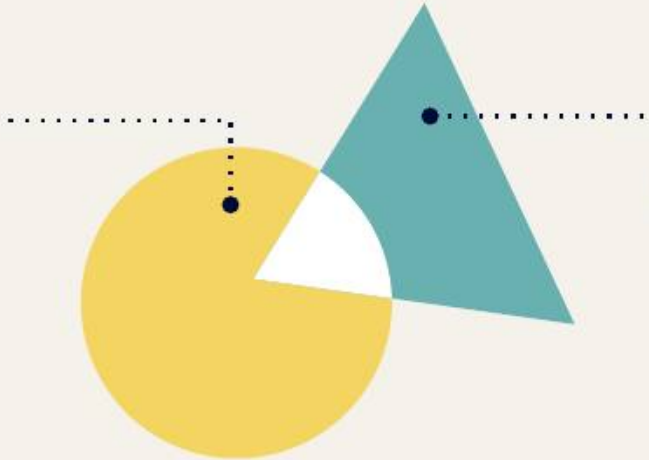
Incident	What Failed	Human/Social Factor	Theory It Illustrates
Target (2013)	Third-party HVAC vendor credentials reused into the main network	Weak vendor oversight and no segmentation between systems	Routine activity: no capable guardian watching third-party access
Colonial Pipeline (2021)	A single reused password on an old VPN account	No multi-factor authentication, low cost for the attacker to try	Deterrence: low risk of being caught made the attempt worth it

Both breaches started with a human or organizational gap, not a sophisticated technical exploit, which is what routine activity and deterrence theory predict.

Two Sides of the Same System

The CISO

Describes an organization built to detect and contain a breach on its own, long before police get involved, since most departments don't have the technical bandwidth to investigate one.



The Convicted Hacker

Shows how punishment, once it happens, tends to come through harsh federal sentencing rather than rehabilitation, even when that same skill set could be redirected toward defense.

Together, they point to a response system that is reactive, under-resourced at the local level, and more focused on deterrence than on turning offenders into defenders.

Who Gets Left Out the Data



Elderly & non-English Speakers

More difficulty reporting fraud or navigating recovery after it happens.



Lower Income Homes

Older, unpatched devices make them exactly the suitable target routine activity theory predicts.



Under resourced communities

Least access to credit monitoring, legal help, or recovery support once they're victimized

Policy and Geography Shape Jobs



Virginia leads the country largely because of its proximity to federal agencies and defense contractors in the D.C. metro area, national security policy, not just population, drives where the jobs are.

My Takeaways

Security Is Never Just Technical

- Criminology theory explains cyber offending better than any purely technical framework I've studied so far.
- Who gets protected, and who gets studied, is a policy choice.
- Where I choose to work after graduation is shaped by these same structural forces, and I want to be very aware of that as I pick what I want to do