CYBER CONNECTIONS AND DIRECTIONS

Improving Cybersecurity by Upending Presumptions

Raising the Bar

Post by Emily Frye

Eighty years ago, a man named Ronald Coase turned economics on its head by challenging our approach to decision making.

Here's an example. Imagine you move to a pristine rural area. You hang your laundry out to dry, breathe in fresh air, and relish the view of stars at night.

Then a manufacturer builds a heavy industrial factory nearby.

Now your laundry is gray instead of white. The country air induces coughing. And the stars are only visible when the plant shuts down for retooling.

Has a wrong been committed? Most people would say yes and that it was the polluter who committed it. The court would likely hold the factory owner responsible for despoiling the community and make him pay.

> As cyberspace has evolved, we have slipped into an easy, but unexamined, imposition of physical-world presumptions on this very different space.

For Ronald Coase, though, the legal trend toward "polluter pays" illuminates an inverse possibility. What if the law leaned in favor of producer rights, regardless of pollution? Community residents could still address the problem: they could band together and pay the factory to stop polluting. Wouldn't this persuade the owner to change or move?

Consider it for a minute. Are you outraged or intrigued? Either way, the response demonstrates the Coase theorem in action: most of our decisions about right and wrong—and where to place responsibility for fixing problems—are premised on underlying assumptions about where entitlements lie. While you and I might assume that the residents are entitled to fresh air, Coase adherents might hold to the idea that the factory has a right to produce goods and that society gains more by maximizing their production.

The point is this: our assumptions about right and wrong result in rules. Rules become the baseline for norms. Norms, in turn, can become so deeply entrenched that we no longer analyze their reason for being.

With apologies to Socrates, the unexamined norm is not worth following. If we surface, challenge, and change assumptions about where entitlements reside, we might also change the decisions we make about responsibility. Underlying assumptions about entitlements are called "presumptions" in the law.

It is time for some presumption flipping—or at least presumption surfacing—in our approach to cybersecurity. As cyberspace has evolved, we have slipped into an easy, but unexamined, imposition of physical-world presumptions on this very different space. Yet, we are experiencing enough compromise in cyberspace that reexamining these presumptions is merited. A good place to start this process might be looking at how we view network boundaries. The energetic debate over active cyber defense demonstrates that reexamining boundaries is a touchy affair—entrenched presumptions are hard to change. But I believe we must try.

Presumption Flipping 101: Perimeters Do Not Equal Protection

Here's a presumption: Networks have boundaries, and I am secure inside my boundary.

We tend to think of cyberspace in the same way we think of real estate. It's divided into plots called "networks." Because my plot/network has a mapped perimeter, whatever is inside is "mine," and I can be secure within these boundaries.

It is comforting to think this way. It's also wrong—even in the physical world.

Here's an example. Last summer, my garden was consumed by an enormous, flowering plant that I assumed to be Queen Anne's lace. Unfortunately, my horticultural prize turned out to be hogweed, an invasive species that can cause skin irritations and even blindness. For the sake of my neighborhood, I dug out each stem by the roots and discarded the surrounding soil.

I have no idea how the hogweed got there. Clearly, it neither knew nor cared about my boundaries. In the world of cyberspace, finding safety inside boundaries is even more of an illusion. Perimeters don't always equal protection.

If we flip the presumption of boundary-based security, do we end up with a cyber neighborhood watch? What would that look like?

Consider the Target breach. In cyberspace, perhaps a known, repeating supply chain is a kind of neighborhood. Could a neighborhood watch have changed the outcome? Financial institutions backing the stolen credit card numbers are pre-established supply-chain partners to Target's sales, as are some other parties. They all have an interest in seeing that the integrity of the sales process remains intact. If the supply-chain participants all watched out for one another's network health and integrity, would the credit-card financier have caught a suspicious connection from an HVAC contractor account in time to preempt a 40-million-card compromise?

Presumption Flipping 102: Boundaries … Are Disappearing

Even if we begin with the presumption that boundaries equal security, there is another factor to consider: boundaries in cyberspace are fuzzy at best and sometimes don't exist at all. As we move further into the "Internet of Things," in which the entire environment is the network, connections and participants are more fluid than ever.

In a fluid environment where an attack on me is an attack on you as well, perhaps the better presumption is that I am my sister's keeper: if my system spots bad action, it protects us both; yours does the same for me.

So What?

So, what does this mean? That we should be on the lookout for the hidden presumptions that shape our decisions—and the resulting allocations of responsibility—about cybersecurity. Once we spot them, we can determine whether to challenge them.

For instance, if we surface the presumption that every participant in the cyber ecosystem can decide when, whether, and with whom to share security information, we can better assess what is gained and lost through such thinking. If we surface the presumption that users have a right to connect to all manner of resources without any validation of their security posture, we can more honestly assess whether other presumptions are more appropriate in a compromised environment. If we surface the presumption that every defender is on his own, and the attackers outnumber him, then we might see very poor odds. And we might decide to change them.

Questions: email cyber@mitre.org

About MITRE Cybersecurity

MITRE has worked closely with government to strengthen our nation's cyber defenses for more than four decades. We work with our sponsors and industry partners to adopt effective new concepts and apply solutions in awareness, resiliency, and threat–based defense. MITRE advocates a balanced security posture that combines classic cyber defense approaches with a new emphasis on leveraging cyber threat intelligence to respond and adapt quickly to a cyber attack. To accomplish this, we encourage partnerships that promote sharing cyber threat information and effective tools.