9. Conclusion

When I was a boy and I would see scary things in the news, my mother would say to me, 'Look for the helpers. You will always find people who are helping.'
– Mister Rogers

The scope of the citizenry affected by cybersecurity vulnerabilities has widened considerably in recent years.

In the past, one might have argued that only computer users were affected by vulnerabilities and their disclosure: this is no longer the case. Affected users now include those who have smartphones, watch smart TVs, use credit cards or ATMs for banking and/or shopping, drive cars, fly in airplanes, go to the hospital for diagnostic imaging or intravenous medicine, live in houses with smart meters, and so forth. The list goes on to include nearly everyone, and "opting out" is not a viable position for most people to take. In an ideal world, software would do exactly what we expect it to do, and nothing we don't want it to do. In an ideal world, vendors would be receptive to finding out about vulnerabilities in their products, and would recognize the service provided to them by those who find and report problems. They would be motivated to place user safety, privacy, and security at the top of their priorities. In an ideal world, human communications would be clear to all parties involved. Well-meaning parties would never misunderstand or misinterpret each other's words or intentions. People would always be polite, patient, humble, calm, without guile, and willing to put aside their own interests for those of others. We do not live in an ideal world. In the world we find ourselves occupying, software-based systems exhibit complex behaviors, increasingly exceeding the limits of human comprehension [1].

As a society, we have become capable of building things we don't fully understand. The difference between what a thing does and what you expect it to do can lead to uncertainty, confusion, fear, and vulnerability. But it's not just the technology that falls short of our ideals. It should come as no surprise that humans have diverse emotions and motives. Values differ. Feelings get hurt, people get frustrated. Words are misinterpreted. Incentives promote individual choices that conflict with each other. What's good for the individual is sometimes bad for the collective, and vice-versa. And so, we're left to muddle through. To confront each day as an opportunity to learn, another chance to improve, and make tomorrow start a little better than yesterday ended. We scan the horizon to reduce surprise. We test for flaws, we probe for weaknesses, and we identify recurring patterns and themes that lead to undesired outcomes. We fix what we can, mitigate what we can't fix, and remain vigilant over what we can't mitigate. We coordinate vulnerability disclosure because we realize we're all in this together.

Thanks for reading.

< 8.2 IoT and CVD | Appendix A - On the Internet of Things and Vulnerability Analysis >

References

1. S. Arbesman, Overcomplicated: Technology at the Limits of Comprehension, Current, 2016.