Mutual Dependence Demands Mutual Sharing

Unfortunately, interdependence, cooperation, and trust are poorly correlated. This is the fundamental axiom of cybersecurity risks for all of us.

Interdependence makes risk transitive; if A depends on B to function and B depends on C to function, then a failure of either B or C induces a failure for A. By contrast, trust is not transitive; that A trusts B and B trusts C does not impel A to trust C, nor would B’s loss of faith in C impel A to lose faith in B. Worse, the fact that A vitally depends on B and C doesn’t necessarily induce cooperation with either.

In the digital world, our security is as connected as our devices. Your firewall might be strong and your defenses might be active and robust, but if a sophisticated and determined opponent attacks your counterparties, spoofs your legitimate suppliers or customers, or infects your security providers, then that opponent will find a way to undermine your security. Most users don’t even discover their penetration on their own—they learn it from others.¹

In other words, not only is the problem technically and mathematically challenging, but its operational impact has a social component that compounds the complexity; you are probably insecure and you are dependent on others to tell you that.

According to a Wall Street Journal poll of its CEO Council: “9% of the respondents said they would never sufficiently trust the [US] government with information to work with it during a cyberattack . . . . Another 34% said they would cooperate with the government only if their own company was being attacked.”² We don’t think an obligation to share information is simple. Companies have competitive concerns and face legal vulnerabilities when they acknowledge problems. Individuals and companies rightly value their privacy and fear overreaching by an overly intrusive government. But we don’t think it’s viable for nearly half of all CEOs, even in a small sample, to embrace non-cooperation with public authorities.

History shows that nothing unites like a common enemy, and that failure to unite guarantees defeat. Our shared security requires shared defenses.

We need a broad reporting requirement for cyberattacks and increased information sharing among government, private sector actors like ISPs, and private sector attack targets. This imperative can be seen in other contexts. Accident data must be reported when airplanes collide and workers are injured. Beginning in 1912, a diagnosis of plague, cholera, yellow fever, typhus, or smallpox obligated the doctor or clinic to share that information (by telegraph) with public health officials. That list of five communicable diseases has grown to 40, but the same rule applies: prompt, exceptionless disclosure for a limited set of priority conditions irrespective of privacy rules. The principle? Transitive risk above some threshold necessitates information sharing.

The US is stumbling toward coerced information sharing about digital attacks. We do this with different rationales in different contexts, such as when we require prompt and detailed attack information from defense contractors to Pentagon authorities, when state laws force disclosure if customers’ credit card or other personal information is exposed, and when the SEC requires the announcement of security breaches that materially impair corporate operations. But this is piecemeal improvement, and we need to move beyond islands of insight. We should take advantage of opportunities presented to us by digital systems for immediate and comprehensive reporting. To benefit fully from the technical opportunity, we need to complement it with a mandatory reporting system that is comprehensive, inexpensive, adequately protective of confidentiality, and valuable informative about the volume, pattern, and character of digital attacks.
Voluntary systems fill some of the gaps. ISPs and equipment vendors capture attack data and alert their users with varying consistency, speed, and detail. Federal and private Information Sharing and Analysis Centers (ISACs) encourage exchanges between industrial sectors. Utilities representing perhaps two-thirds of America’s customers participate in an automated Cybersecurity Risk Information Sharing Program (CRISP). Companies share information with chosen others, sometimes outside of their own industries to diminish competitive and antitrust concerns. Former colleagues commonly exchange information across industry boundaries.

However, these don’t suffice. Large vulnerabilities remain when a third of the nation’s utilities don’t yet participate in CRISP. In a connected grid, vulnerabilities for some have consequences for all. Though industry-specific data compilation and analysis are commendable, software and hardware attacks cross industries and exploit common vulnerabilities in ways we are not well positioned to understand, never mind remediate. Two of the most recent and insightful assessments have recommended improved voluntary reporting. But why not mandatory?

For its part, the federal government needs to share more systematically. Often the FBI reveals to a surprised company that it has been penetrated, and then doesn’t divulge any more about what it knows or how. Our intelligence establishment understandably guards its secrets, but its highest priority (to protect us) is undervalued in an effort to protect its sources and methods.

We don’t think a regime of broader, compelled sharing is an easy one or without side effects. There is a great deal of thinking still to be done. Biological infections are treated by professionals, but malware infections are treated by amateurs. Diseases spread within jurisdictions before they become global, but malware is global from the get-go. Transmissible diseases can mutate, but they have studied, predictable behaviors, whereas malware comes from sentient opponents who can be intentionally devious.

Of course, our proposal is not the only way to proceed, but one can’t ignore that its cousins have been proven successful in life-and-death matters. We believe the digital domain generates more widely shared vulnerabilities than any other. When dependence is mutual—that is to say when for A to function B must be operational and for B to function A must be operational—the brittleness of the combined system to cascade failure requires other coercive measures if either A or B is critically important to others beyond their mutual embrace.

References

Daniel E. Geer Jr. is the Chief Information Security Officer of In-Q-Tel. Contact him at dan@geer.org.

Richard Danzig is a senior advisor to the Johns Hopkins University Applied Physics Laboratory and former Secretary of the Navy. Contact him at rjdanzig@gmail.com.