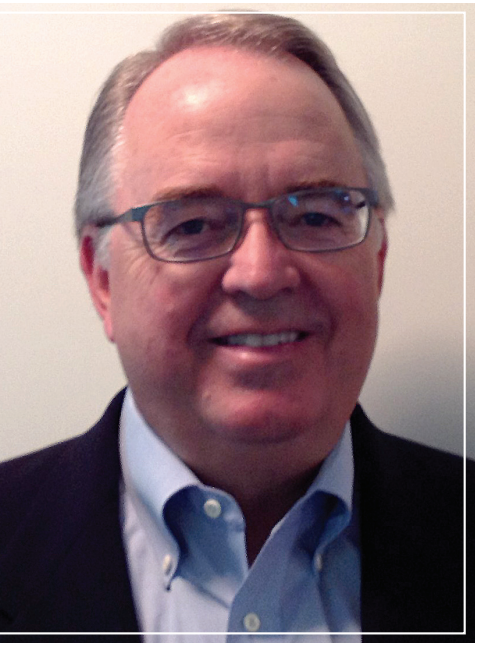
Stand Your Ground

Daniel E. Geer Jr.
In-Q-Tel



Jerry Archer
Sallie Mae

When you get to a fork in the road, take it.
—Yogi Berra

Protection from the risks of Internet use comes down to a choice: blind faith or self-defense. All versions of "trust us, and you'll be okay" are probabilistic falsities.

In your heart, you know the answer. The very definition of "trust" is this: a state of trust is where you have sufficient capacity for effective recourse that you can disregard self-protection. Recourse of that sort is not yours.

It is said that the true purpose of the state is to hold a monopoly on the use of force. But when a state can no longer protect its citizens, its last duty is to arm them. Fat chance of that—states of every stripe and virtue are arming themselves with cyberweaponry, ipso facto, you have no choice but to do the same. Remember, in no other arena of warfare than cyberwarfare is collateral damage so assured yet so unpredictable a priori and dirt simple enough for a bulleted list:

- The A in APT now stands for average.
- Blended is the norm: cross-channel, cross-domain, cross-functional.
- Defense against known threats is necessary but insufficient.
- Adversaries have significant technical means funded by cybercrime profits and/or nation-state taxation.
- Current defense techniques are obliterated by accelerating growth in technology.
- Third-party risk continues to increase.
- Imposition of dramatically increased compliance burden does not accrete to improved security.
- Resource constraints continually challenge security program sustainability.

Risk is proportional to dependence. Ergo, to decrease risk, curtail dependence. Start with the obvious: identify and minimize likely targets and threats. Limiting criminal objectives means that defense becomes more tractable, well-defined, and economically feasible. As in Washington, expansion of the enterprise's catalog of essential technologies creates unfunded liabilities such that one truly must run faster and faster to stay in the same place.

The better the attack, the higher the need for intelligence. The better the opponent, the more that intelligence is not what you get by passively listening. You will cross the line between defense and offense or you will fail.

And, resilience is essential. Operationalize, treat the inside like the outside—trust nothing that is not continuously verifiable; believe nothing that is not corroborable. You need both inbound and outbound defense, which means exfiltration prevention, choke points, and compartmentalization. Reduce the threat plane with strong governance practices, aggressive patching, and anomaly detection. Fortify your courage to say "NO" with data. Survive.

(A state of) security is the absence of unmitigatable surprise. Your design task is not perfection; assume that you'll fail, and pick tolerable failure modes. Pair robust application and network security with rapid and effective incident response. If replacing something low tech and dear with something high tech and cheap, retain your ability to fall back to low tech, or put the greater part of the savings into your security program.

Automate your compliance burdens faster than those professional utopians can impose them. Automate to eliminate the greater fraction of first-level support, and reduce false positives to a manageable roar. Drive your availability metrics by zeroing your mean time to repair, not by infinitizing your mean time between failures. Build your own cyberdrones and stand your ground, but reserve the kill decision to a sentient human. ■

Daniel E. Geer Jr. is CISO for In-Q-Tel and past president of the Usenix Association. Contact him at dan@geer.org.

Jerry Archer is chief security officer at Sallie Mae and founding member of the Cloud Security Alliance. Contact him at Jerry.Archer@salliemae.com.

Copublished by the IEEE Computer and Reliability Societies