Every Day is D-Day on Data-Breach Beaches

Hackers attack when they're ready, not when we're ready.

By Mark Gerard

In his recent keynote at the West 2018 defense conference, Deputy Defense Secretary Patrick Shanahan put defense-industry CEOs on notice: protect computer networks and data or lose government business.

"I think of things like safety, and cyber falls into that category—whether it's safety or security, as being one of those things that should be uncompromising," he said.

Shanahan's remarks were timely and forceful. Creating an "uncompromising" network security environment is a good place to start, as is insisting on accountability and bottom-line consequences. But even all of that doesn't go far enough.

To be blunt: We are at war. We need to recognize that fact and act accordingly. Government agencies, defense contractors, health care companies and all the rest of us who deal with data protection, need to take this war very seriously. That means changing our attitude and our behavior.

We are being hunted by invisible predators who feed on data. But this is no Hollywood movie, where Arnold Schwarzenegger and a team of commandos hunt an alien monster through some steamy jungle. This is a 24/7 reality in which hackers work constantly to breach networks and gain access to our digital life-blood.

We need to understand the enemy. Like biological viruses, hackers are opportunistic and go after hosts that unwittingly help them thrive. Cultural and legal boundaries between public sector and private sector are meaningless to them. They attack when they're ready, not when we're ready. On this battlefield, they observe no moral code and give no quarter. And we can't change hackers' hearts and minds.

We need to think and act differently than we have in the past. Human nature, unfortunately, tends to make us complacent and leads us to do things or fail to do things even when we know better. We're all human, but that's no excuse for sticking our heads in the sand. "That will never happen to me" syndrome must be countered daily. We can't play the odds and hope our data will be overlooked.

We need to ensure that data center infrastructure is kept safe from direct hits by Mother Nature and has both physical and cybersecurity that truly prevents intrusion—including certifications that maintain the high bar called for by Shanahan. We have to think like the enemy and anticipate vulnerabilities.

In the colocation industry, we know hurricanes will strike, earthquakes will shake, and dense brush will burn. The smart money looks at those risks before committing to a site and avoids locating on the coast or near a fault line or in a wildfire-prone landscape. Similarly, the data security war demands that we think holistically, asymmetrically, with 360-degree awareness.

Whether we are a data center, an agency, or a contractor, we cannot be lazy, we cannot accept window-dressing in place of real security, and we cannot fall into a bureaucratic, check-the-boxes mentality.

Every day is D-Day in this battle against data breaches and network compromises. We have to start every day recognizing the stakes we face, knowing what winning and losing means to us and to those who depend on us. It's not about us, our careers, or any agency's or company's reputation. It's about protecting our country and our fellow citizens.

Mark Gerard is the president of DP Facilities, Inc.