MY TAKE

DAVID HECHLER

Cybersecurity has certainly arrived. Everyone knows that word. You want proof? CrowdStrike ran Super Bowl ads in **2024** and **2023**. This was confirmation that the company has made it. And CrowdStrike obviously had confidence that viewers knew what the ads were talking about.

But what do most people know about cybersecurity? That is, people who do not make their living trying to prevent, mitigate, or respond to cyberattacks. It's an important question because for years research has shown that people are the weak link in cyber defense. We get fooled by phishing emails and we click on links that endanger our companies. And it's not just lower-level employees who are the problem.

The recent book TAG published on cybersecurity, called **Guiding Cybersecurity from the Boardroom** (which can be downloaded for free), was designed to address a dangerous gap in cyber defense that many companies suffer from.

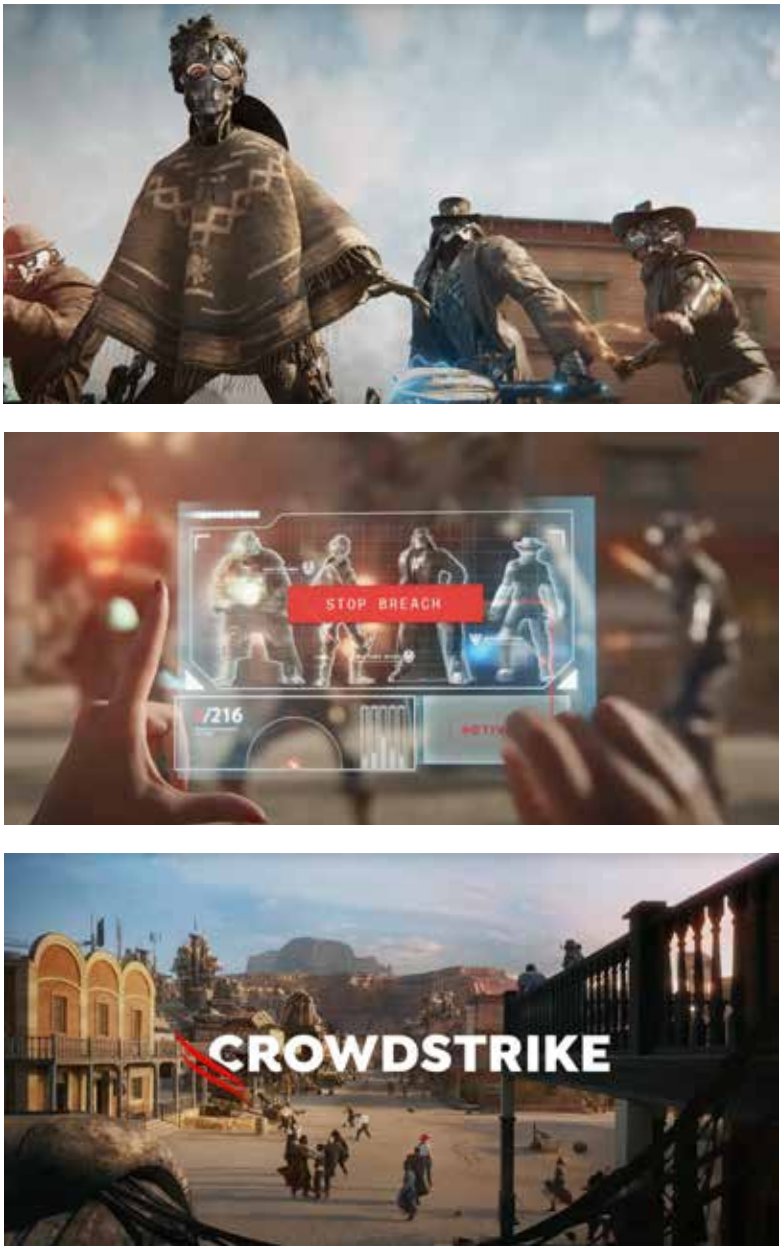
Their boards of directors are not necessarily better prepared to help prevent cyberattacks than the employees.

The more I think about it, the more I think that cybersecurity is a black box to nearly everybody in this country. We hear about it. We know it does damage and costs money. We know we're supposed to be careful to avoid being fooled into clicking on a dangerous link. But beyond that, what do most people really know?

WHAT MAKES CYBERSECURITY DIFFERENT

There's one way in which these attacks are at odds with the way we generally think about crime. It's the absence of perpetrators—or rather, perpetrators we can see. It's hard to think about crime without thinking about criminals. But we rarely see the criminals behind the attacks. If they are identified at all, it's often by the name of a gang or their nation of origin. And those nations rarely have extradition treaties with the United States.

For the vast majority of us, cybersecurity is the invisible crime. We don't see it happening. Companies and individuals who are victimized rarely want to report it or talk about it. As for the criminals, we've come to assume that they're all far away and they work for, or are protected by, nation-states. No pictures appear on the front pages of newspapers to show the world the latest big hack. It's almost as if the danger is beyond perception—like Covid-19.



Stills from CrowdStrike's 2024 Super Bowl ad

One of the biggest attacks in recent years that received a lot of media attention was SolarWinds. Recently it was in the news again, but it was because the company itself faces an SEC enforcement action, along with its chief information security officer (CISO). But still we see nothing about the criminals responsible—just the attribution that it came from Russia.

Maybe it's no coincidence that in CrowdStrike's most recent Super Bowl ad, the bad guys are aliens who look as though they just stepped out of one of those weird bars in Star Wars.

THE EXCEPTION

There is one case I can think of that was an exception to this rule. It happened here in the United States. There were charges filed. Several defendants pleaded guilty and testified in court. One man who seemed to be on the side of the good guys—he was responsible for security in the company that had been hacked—stood trial.

The case, of course, involved Uber and has proved highly controversial. Many professionals who work in security supported and continue to support Joe Sullivan, who in October 2022 was convicted by a jury of obstructing justice and covering up a felony. Sullivan was not charged with the hack. Two men pleaded guilty to that, and one testified against Sullivan, as did a former Uber in-house lawyer. (In the interest of full disclosure, Sullivan now works as a TAG senior analyst.)

Was this the case designed to open the public's eyes about cyberattacks? Hardly. The focus was not on the hack; it was on the effort prosecutors said was designed to conceal anything resembling a crime by calling the hack research and the $100,000 payment to the hackers a bug bounty. These were the issues the testimony highlighted. For friends and former colleagues of Joe Sullivan (and there are many), it was just another effort to blame the chief security officer when things go wrong.

NO PICTURES APPEAR ON THE FRONT PAGES OF NEWSPAPERS TO SHOW THE WORLD THE LATEST BIG HACK. IT'S ALMOST AS IF THE DANGER IS BEYOND PERCEPTION—LIKE COVID-19.

When SolarWinds' CISO, Tim Brown, was included in the SEC's enforcement action against his company in October 2023, a year after Sullivan's conviction, it struck some people in the field as yet another tightening of the screws. In this instance the problem wasn't breaches. The SEC charged that Brown and his company had failed to let shareholders know about security vulnerabilities he and his colleagues were aware of and concerned about.

THE TAKEAWAY

But let's set aside the specifics for a moment. Let's not try to prelitigate or relitigate these two cases. If the nation were determined to learn lessons about cybersecurity that would help us all better understand the challenges we face, what can they teach us? What do they tell us about the nature of cybersecurity?

The short answer: Companies don't like to be hacked. And when it happens, or when they fear it might happen, they seem highly motivated to keep the details to themselves.

Law enforcement, Congress, and the Cybersecurity and Infrastucture Security Agency (CISA) have been trying for years to convince companies to share with the authorities, and with each other, the dangers they hear about or encounter. The goal is to help build defenses against the virulence, the way vaccines aimed to counter Covid-19. The government seems to think this approach would shine more light on these invisible crimes and bolster the nation's defense.

It's hard to see how recent events have advanced that cause. A number of angry CISOs have argued that heavy-handed enforcement has spurred veteran security professionals to consider moving on—and aspiring ones to reconsider their options. It's hard to see any way in which the public is now enlightened and better prepared to deal with future cyber threats.

If only the criminals looked like bad sci-fi characters, and CrowdStrike could chase them back to their home planets.

(Reprinted from the TAG Security Annual, 2nd Quarter 2024.)