Lessons from 'Star Trek: Picard'—A cybersecurity expert explains how a sci-fi series illuminates today's threats

May 12 2023, by Richard Forno

This orbiting museum in the show ‘Star Trek: Picard’ plays a key role in fending off a futuristic form of cyberattack. Credit: Paramount

(Editor's note: This article contains plot spoilers.) Society's understanding of technology and cybersecurity often is based on simple stereotypes and sensational portrayals in the entertainment media. I've written about how certain scenarios are entertaining but misleading. Think of black-clad teenage hackers prowling megacities challenging

corporate villains. Or think of counterintelligence specialists repositioning a satellite from the back of a surveillance van via a phone call.

But sometimes Hollywood gets it right by depicting reality in ways that both entertain and educate. And that's important, because whether it's a large company, government or your personal information, we all share many of the same cybersecurity threats and vulnerabilities. As a former cybersecurity industry practitioner and current cybersecurity researcher, I believe the final season of "Star Trek: Picard" is the latest example of entertainment media providing useful lessons about cybersecurity and the nature of the modern world.

So how does "Star Trek: Picard" relate to cybersecurity?

The nature of the threat

The show's protagonist is Jean-Luc Picard, a retired Starfleet admiral who commanded the starship Enterprise-D in a previous series. Starfleet is the military wing of the United Federation of Planets, of which Earth is a member. In Season 3, the final season, Picard's ultimate enemy, the Borg, returns to try conquering humanity again. The Borg is a cybernetic collective of half-human, half-machine "drones" led by a cyborg queen.

The Borg has partnered with other villains and worked for over a decade to deploy hidden agents able to compromise the DNA data contained in the software underpinning the transporter—a teleportation device used regularly by Starfleet personnel. Over many years, a certain subgroup of Starfleet personnel had their DNA altered by using the transporter.

Thus, in launching their final attack, the Borg is able to instantly activate thousands of "drones" to do its bidding in the form of altered, compromised Starfleet personnel. As Geordi La Forge, the Enterprise-

D's engineer, notes, "They've been assimilating the entire fleet this whole time, without anyone ever knowing it."

The Borg's prolonged, stealthy infiltration of the federation is indicative of how today's most effective cyberattackers work. While it's relatively easy to detect when hackers attempt to breach a system from the outside, experts worry about the effects of an enemy infiltrating critical systems from within. Attackers can put malicious code in software during manufacturing or in software updates, both of which are avenues of attack that do not arouse suspicion until the compromised systems are activated or targeted.

This underscores the importance of ensuring the security and integrity of digital supply chains from product development at the vendor through product deployment at client sites to ensure no silent "drones," such as malware, are waiting to be activated by an adversary.

Equally important, "Star Trek: Picard" presents the very real and insidious nature of the insider threat faced by today's organizations. While not infected with a cybernetic virus, recently arrested Massachusetts Air National Guard airman Jack Teixeira shows the damage that can occur when a trusted employee has malicious intent or becomes co-opted and inflicts significant damage on an employer.

In some cases, these compromised or malicious individuals can remain undiscovered for years. And some global adversaries of the U.S., such as China and Russia, are known for taking a long-term perspective when it comes to planning and conducting espionage activities—or cyberattacks.

Humans remain the weakest link

"Synchronistic technology that allows every ship in Starfleet to operate as one. An impenetrable armada. Unity and defense. The ultimate

safeguard."

With these words, humanity's military defenders activated a feature that linked every Starfleet vessel together under one unified automated command system. While intended to serve as an emergency capability, this system—called Fleet Formation—was quickly hijacked by the Borg as part of its attack on Earth. In essence, Starfleet created a Borg-like defense system that the Borg itself used to attack the federation.

Here, the most well-intentioned plans for security were thwarted by enemies who used humanity's own technologies against them. In the real world, capabilities such as on-demand real-time software updates, ChatGPT and centrally administered systems sound enticing and offer conveniences, cost savings or new capabilities. However, the lesson here is that organizations should not put them into widespread use without carefully considering as many of the potential risks or vulnerabilities as practical.

But even then, technology alone can't protect humans from ourselves—after all, it's people who develop, design, select, administer and use technology, which means human flaws are present in these systems, too. Such failings frequently lead to a stream of high-profile cybersecurity incidents.

Resiliency is not futile

To counter the Borg's final assault on Earth, Picard's crew borrows its old starship, Enterprise-D, from a fleet museum. The rationale is that its ship is the only major combat vessel not connected to the Borg collective via Starfleet's compromised Fleet Formation protocol and therefore is able to operate independently during the crisis. As La Forge notes, "Something older, analog. Offline from the others."

From a cybersecurity perspective, ensuring the availability of information resources is one of the industry's guiding principles. Here, the Enterprise-D represents defenders in response to a cyber incident using assets that are outside of an adversary's reach. Perhaps more important, the vessel symbolizes the need to think carefully before embracing a completely networked computing environment or relying on any single company or provider of services and connectivity for daily operations.

From natural disasters to cyberattack, what's your plan if your IT environment becomes corrupted or inaccessible? Can your organization stay operational and still provide necessary services? For critical public messaging, do governments and corporations have their own uncorruptible Enterprise-D capabilities to fall back on, such as the fediverse, the decentralized microblogging platform that is immune to the impulsive manipulations of Twitter's ownership?

Prepare for the unknown

The "Star Trek" universe explores the unknown in both the universe and contemporary society. How the crews deal with these experiences relies on their training, the appreciation of broad perspectives and ability to devise innovative solutions to the crisis of the week. Often, such solutions are derived from characters' interests in music, painting, archaeology, history, sports and other nontechnical areas of study, recreation or expertise.

Similarly, as modern digital defenders, to successfully confront our own cyber unknowns we need a broad appreciation of things beyond just cybersecurity and technology. It's one thing to understand at a technical level how a cyberattack occurs and how to respond. But it's another thing to understand the broader, perhaps more systemic, nuanced, organizational or international factors that may be causes or solutions,

too.

Lessons from literature, history, psychology, philosophy, law, management and other nontechnical disciplines can inform how organizations plan for and respond to cybersecurity challenges of all types. Balancing solid technical knowledge with foundations in the liberal arts and humanities allows people to adapt comfortably to constantly evolving technologies and shifting threats.

Dystopic metaphors in fiction often reflect current social concerns, and the "Star Trek" universe is no different. Although rooted in a science fiction fantasy, "Star Trek: Picard" provides some accurate, practical and understandable cybersecurity reminders for today.

Season 3, in particular, offers viewers both entertainment and education—indeed, the best of both worlds.

Provided by The Conversation