The Human Element: Why Cybersecurity Is Never Perfect

Carl Lochstampfor Jr

Department of Cybersecurity, Old Dominion University,

CS 462 — Cybersecurity Fundamentals

April 5, 2026

Watch this TED talk

"The Humanity Behind Cybersecurity Attacks," by Mark Burnette

https://www.youtube.com/watch?v=pnADP41earI

The speaker talks about how he was a kicker for his school football team. He talks about various factors that might affect his kicking and making that score. The same analogy goes to the cybersecurity professionals defending against attackers. These professionals do not always have the perfect conditions to defend against attacks. Provide your opinions on this statement, and ways in which the "Humans Behind cybersecurity" (both attackers and defenders) get around each other.

Reference:

Burnette, M. (2019). *The humanity behind cybersecurity attacks* [TED Talk]. TEDxNashville. https://www.youtube.com/watch?v=pnADP41earI

The Human Element: Why Cybersecurity Is Never Perfect

In his TEDx Nashville talk, Mark Burnette compares his experience as a college football placekicker to that of a cybersecurity professional. Like a kicker faces unforeseen internal and environmental conditions (e.g., wind, crowd noise, pressure), cybersecurity professionals also have to navigate imperfect, uncertain situations (Burnette, 2019).

Burnette stresses that most successful security breaches result from human mistakes, not advanced technical attacks. These mistakes often come from employees outside the IT department and from customers, shifting the discussion's focus from technology to the people who use it. He highlights three key human traits that make people vulnerable to breaches that attackers target (Burnette, 2019). The clearest example is how phishing campaigns, pretexting, and business email compromise all exploit trust, distraction, and habit—rather than software vulnerabilities. Attackers "get around" defenders by targeting the path of least resistance: the human at the keyboard.

In response, defenders create layered security programs (i.e., defense-in-depth). No one can be alert and monitor their systems all the time, 24/7. Therefore, cybersecurity professionals develop tools such as multi-factor authentication, least-privilege access, and security awareness training to help 'bridge' those surveillance gaps. Since the defenders and their programs expect people to make mistakes, cybersecurity professionals understand technology alone is not enough, and that we need multiple safeguards or 'safety-nets' to help overcome human mistakes.

In conclusion, Burnette notes that most cyber-attacks succeed when a person slips up, not the computer. Like Burnette's football analogy, success depends on preparation, resilience, and comprehending human factors on both sides of the spectrum.