MAN IN THE MACHINE

Context is key for Dhillon, whose recent work includes an exploration of cyberstalking in the Journal of Business Ethics. That focus has also led him to critical work on the uses of information systems theories. "If we come up with a theory in North Carolina," he asks, "how well does that apply in Hong Kong?"

When it comes to cybersecurity, everyone has skin in the game.

Individuals worry that their financial data and social media identities won't remain private and secure. Corporations spend millions to shield their computer systems against hackers and intellectual property thieves. Governments may play both sides of the issue, seeking to spy on the computer systems of friend and foe alike while struggling to protect their own data systems from unauthorized entry.

Long before cybersecurity was the stuff of daily headlines, long before average citizens worried about protecting their Facebook data, Professor Gurpreet Dhillon was focused on nuanced security factors not usually considered in information systems curricula.

Dhillon, head of the Bryan School's Department of Information Systems and Supply Chain Management, theorized early in his career that human factors – social and behavioral aspects – are as critical to cybersecurity as technical elements.

"The nature of the technology is that we get consumed in the knowledge and the technical controls," he says, "and we ignore everything else."

But no computer, he wrote in a textbook over 20 years ago, has ever been arrested for a computer crime.

The gray area between technology and people continues to drive his research. It's an increasingly challenging field, he explains, as data platforms with global reach – such as Facebook and LinkedIn – grow ever larger. Swimming in this giant data ocean are hundreds of millions of individuals, as well as the businesses that want to connect with them. Though international borders disappear in this cyber universe, different cultures, societies, and people bring their own values, standards, and assumptions to the mix.

The result, Dhillon observes, is a digital world fraught with chasms, places where security provisions of digital service providers and corporations don't intersect with expectations of individuals. Dhillon calls these chasms "value gaps."

Much of his current research involves identifying value gaps, determining methods to measure them, and offering alternatives. In 2002, Dhillon introduced the concept of value-focused thinking to the field of information systems research. It provided the foundation for his research into social identity threat assessment. One of his most recent publications, for the journal Decision Sciences, offers policy makers guidance on assessing value gaps.

"What information do users want publicly available? What information are companies making available? How well does intent compare to reality?"

Businesses and governments are human constructs, Dhillon points out. They are by nature imperfect and fluid. Cybersecurity challenges, he notes, often result from misinterpretations and missteps by the organizations entrusted with handling information.

Dhillon, who earned his Ph.D. from the London School of Economics and Political Science, seems to be both behavioral scientist and statistician, analyzing patterns of seemingly unrelated data to make statistically accurate predictions. During the Arab Spring, he was among the experts tapped to predict where North African rebels would move and strike next.

Governments still seek Dhillon's counsel on security issues. Just don't ask which ones. That information is secure.

By Tom Lassiter • Learn more at go.uncg.edu/isscm