# CYBERSECURITY TAKES CENTER STAGE

Your company could be vulnerable. And it's everyone's problem.

By Information Systems Professor Patricia McQuaid

Every employee who does not pay attention to cybersecurity potentially puts their company at risk.

Today, students and graduates of all disciplines need to have at least a basic level of cyber awareness. I teach my students that security is not relegated to the technical job titles in an organization but relates to every individual in the organization. I am a firm believer that businesses need to create a culture of security that empowers individuals to safeguard devices and information. My experience and research have suggested those proactive companies will be more resilient in the face of increased hacking, email phishing and ransomware attacks.

While overall spending on cybersecurity has increased, now at approximately $12 billion per year, so have the attacks. No brand wants to be known for an all-caps headline detailing the latest hack. In recent years, there have been significant data breaches at retail stores (think Target) and entertainment companies (think Sony), the latter resulting in the release of executives' private emails. Hackers even found a way into Disney's systems and demanded payment to stop the leak of a new, unreleased film. The ramifications of these attacks go beyond the information that was directly compromised. The effects translate into lost revenue, lowered employee morale and a damaged reputation with consumers.

Not long ago, the ransomware cyberattack known as "WannaCry" infected more than 200,000 users in more than 150 countries through computer networks. As the name suggests, the virus held the infected computer hostage and demanded the victim pay a bitcoin ransom in order to regain access to his or her files. Enterprises, from manufacturers to government agencies, that ran older versions of Windows or had not updated the newest Windows versions were vulnerable. Major institutions — including hospitals — ground to a halt in a matter of hours.

Even at Cal Poly, the threat of hacking is a daily reality. According to our Information Technology Services team, university accounts received 6.4 million emails during the first week of spring quarter. More than 80 percent of those messages were threat emails including spam, viruses or phishing scams.

Prosecuting these crimes is also becoming more complicated as laws and regulations struggle to catch up with advancing technology. While researching my latest article, *Digital Forensics for First Responders*, I found there are very specific procedures that must be followed to ensure that data is preserved in order

**80%+**

**During the first week of spring quarter, more than 80 percent of emails sent to Cal Poly accounts were threat emails including spam and phishing scams.**

→
**On Guard**
Professor Patricia McQuaid says Cal Poly is on the forefront of the cybersecurity discussion.

to prove wrongdoing. In California, the data must be preserved throughout the entire time the perpetrator is incarcerated, not just during the trial. The unexpected burden on companies or professionals to store or maintain devices could make the difference in a case.

Business professionals who expect to succeed can't have an attitude of "it won't happen to me." Rather, forward-thinking leaders can take a proactive role in keeping themselves, their employees and their company a step ahead of constantly evolving threats.

Those in strategic planning roles can make cybersecurity a long-term priority as a form of ongoing sustainability. Professionals in finance and accounting can allocate resources that support low-cost, common-sense solutions such as data backups in the cloud or via external hardware. Human resources professionals can advocate for safety policies that protect colleagues who work remotely or perform work across multiple devices. And employees in all sectors can adopt best practices to protect themselves and the networks they utilize.

I'm proud to say that Cal Poly is on the forefront of the discussion and is committed to educating more students to fill the significant talent shortage in the cybersecurity industry. It has established the Cybersecurity Center, which includes the Northrup Grumman Cyber Lab and infuses technical curriculum into courses, including those in the Orfalea College of Business. Just this year, I became a research and education coordinator at Camp San Luis Obispo's California Cyber Training Complex, which is a partnership between Cal Poly and the National Guard.

As the faculty liaison to the college from Cal Poly's Cybersecurity Center, I often advocate for fusing management education with cybersecurity topics. Inevitably, the business leaders we educate will need to make informed decisions about data security and technology resources. To jumpstart that effort, I'll play an integral role in the course Cybersecurity for Executives offered this fall through Cal Poly Extended Education. The class will help leaders understand potential threats, learn how to position their organization to address threats, and leverage limited budgets.

At the undergraduate level, I've also involved my students in the Cybersecurity Case Study Library, a database of cases that connect technical topics to disciplines like political science, philosophy and agribusiness. Information systems student Lauren Tang recently co-wrote a case that is now being published in the library.

The concept of cybersecurity can feel like a moving target, and in many ways, it is. However, the field is the next frontier of safety we all have to deal with, and the organizations and individuals who confront it head-on will come out on top. With Cal Poly's efforts coming together, we are poised to become a leading supplier of cyber-ready experts, professionals and innovators leading the way.