UC SANTA BARBARA
THE Current

October 23, 2024
By Lindsey Terra

UCSB’s cybersecurity chief on protecting digital spaces and the role of AI

Jackson Muhirwe, UC Santa Barbara’s chief information security officer and director of information assurance, is a seasoned higher education leader with over two decades of experience in information technology (IT) and security.

For Cybersecurity Awareness Month, he reflects on his journey into the field, offers practical advice for safeguarding personal information online, and discusses the challenges and evolving landscape of modern cybersecurity and the future of protecting digital spaces. From insights on massive data breaches to reflections on the role of artificial intelligence in security, this Q&A offers valuable takeaways for the campus community and beyond.

How did you get started in the field of information security?

I have worked in IT for about 25 years, with most of that time spent in higher education. About 20 years ago, I participated in my first security class as a graduate student. This class was an eye opener and got my attention on cybersecurity.

Are there any particularly defining moments in your life that solidified your interest in researching and pursuing cybersecurity as a career path?

After my graduate studies, I got an opportunity to serve as the chief information officer for a major intergovernmental organization. This role presented many security challenges due to the confidential nature of the organization's work. I collaborated with my leadership team, colleagues and service providers to establish a robust security program for the organization. This experience was a turning point in my professional life and marked the beginning of my security career.

Our personal and professional lives are intersected by cybersecurity more than ever. From online shopping to government services to our employers, it's almost impossible to live in the modern world without sharing personal or financial information on a website. What are some steps everyone should be taking to protect their information online?

Cybersecurity threats are becoming increasingly sophisticated and prevalent, but there are critical steps everyone should take to protect their information online:

1. **Strong Passwords:** Create strong passwords that are a combination of uppercase and lowercase letters, numbers and symbols. Avoid using easily guessable information like birthdays or pet names.
2. **Password Managers:** Since we all have many passwords, it's advised to use a password manager to securely store and generate strong, unique passwords for each account.
3. **Multi-Factor Authentication (MFA)**: Enable MFA for all online accounts that support it. This typically involves providing a second form of verification, such as a code sent to your phone or email.
4. **Phishing Attempts**: Be cautious of suspicious emails, especially those asking for personal information or containing unexpected links. Always verify the sender's address and avoid clicking on links from unknown sources.

By following these steps, you can significantly reduce your risk of falling victim to cyberattacks and protect your personal information online.

We've gone from using the same simple password for all our accounts to needing complex passwords, entire phrases, MFA, security questions, password managers, etc. What would you say to people who find all of this too inconvenient and unnecessary?

If you lived in a neighborhood where your home was constantly under attack from criminals wishing to harm you and steal your valuables, you'd probably consider

increasing security for your home to stop the criminals, right? UCSB systems and all of our accounts are under constant and unrelenting attacks from cyber criminals wanting to steal our information, disable our operations and cause havoc to our lives. The goal is to balance security with usability — making it possible for authorized users to access the information they need to access when they need it.

Massive organizations and businesses are experiencing data breaches from hackers, resulting in our personal information being leaked. Is this happening more often than before and if so, why? What security measures should we expect from organizations that we're sharing our personal information with?

In today's online environment, it is no longer a question of *if* you fall victim to a breach, but *when.* Data breaches have increased exponentially in the last few years due to a number of factors. Externally, there continue to be more highly-motivated and well-funded criminal organizations that are constantly scanning and searching for organizations to breach.

Many organizations struggle to keep up with this growing trend and still have unpatched systems and weak internal security controls. Improving the security posture of an organization requires a combination of strategies and tactics that include administrative, technical and physical safeguards. One form of protection is never enough to provide robust security for an organization.

At an organizational level, the first step is making security everyone's responsibility. Each and every member of the UCSB community has a role to play. At some point, security measures might fail and if they do, each individual in the organization has an obligation to detect and mitigate threats. People have less reason to worry if they are acting in ways that reduce the probability of falling victim to a breach.

For the last several years, campus leadership has invested in security technologies and resources to enable a comprehensive, centrally-managed security program. At UCSB, we are currently implementing Secure UCSB, a cybersecurity investment program that addresses a new security mandate from the UC Office of the President. This initiative will help to bolster our overall security by enhancing protections for our campus network and university-owned devices.

What do you think the future of cybersecurity looks like 20 years from now?

It’s hard to imagine what the future of cybersecurity looks like considering how much technology has evolved over the last two decades. Organizations utilize the most advanced technology available to implement solutions and solve problems that were considered impossible in the past, but cyber attacks continue to become more sophisticated as a result, so it’s hard to be optimistic. This is why it’s critical for both people and organizations to follow best practices and prioritize cybersecurity investments, before it’s too late.

With the advancement of artificial intelligence (AI) technologies, organizations are scrambling to respond to the growing number of use cases for AI to replace humans and make some organizations and departments obsolete. These AI advancements present challenges in the higher education landscape, including bias, ethical use, abuse of intellectual property rights, uncontrolled sharing of sensitive institutional information and more.

To address these challenges, state governments and large intergovernmental organizations are creating regulations to guide the development of AI models, sharing of data, acceptable use cases, and responsibilities of AI owners. At UCSB, we are working to develop and publicize our own set of guidelines for implementing AI, including the establishment of governance structures to support responsible development and use of AI models.

What’s some of the most interesting research you’re seeing in the cybersecurity space recently?

Some of the most fascinating research in cybersecurity right now involves artificial intelligence (AI) and quantum computing, both of which present unique opportunities and challenges. In AI, advancements in machine learning are enhancing automated threat detection, helping security teams identify and respond to cyber threats more efficiently — this has direct implications for our work in UCSB’s Security Operations Center. Generative adversarial networks (GANs) are also being used to create synthetic datasets and test security systems with realistic adversarial examples.

On the quantum computing side, researchers are focusing on post-quantum cryptography, which aims to develop algorithms resistant to quantum attacks, and quantum key distribution, a secure method for sharing cryptographic keys that could transform secure communications.

Is there a film, book or pop-culture reference with an interesting take on technology that you find memorable or thought-provoking?

I love movies and I am always fascinated with how cybersecurity is depicted in them. One of the most memorable and, in my opinion, one of the best cyber-related movies of all time is “War Games” from 1983. It was the first cybersecurity-related movie that I watched many years ago, and I have rewatched it many times since then and still find it fascinating.

Recent global events have demonstrated that there is a very thin line between cyber and physical warfare, a key concept depicted in this film. The movie’s portrayal of how technology can inadvertently escalate tensions highlights the growing importance of cybersecurity in maintaining national and global stability, as today’s interconnected systems make it easier for cyber incidents to have far-reaching physical consequences.

Tags
Artificial Intelligence

Media Contact
Lindsey Terra
(805) 893-2191
lindsey_terra@ucsb.edu

About UC Santa Barbara

The University of California, Santa Barbara is a leading research institution that also provides a comprehensive liberal arts learning experience. Our academic community of faculty, students, and staff is characterized by a culture of interdisciplinary collaboration that is responsive to the needs of our multicultural and global society. All of this takes place within a living and learning environment like no other, as we draw inspiration from the beauty and resources of our extraordinary location at the edge of the Pacific Ocean.