NEWS

THE IMPORTANCE OF CYBERSECURITY AND ITS BOOMING JOB MARKET

Cybersecurity is one of the most in-demand job markets in the U.S. in 2022

October 5, 2022 | Author: Logan Pellegrom | Media Contact: Logan Pellegrom

Share

Since 2004, the President of the United States and Congress have declared October to be Cybersecurity Awareness Month to help individuals protect themselves online as threats to technology and confidential data become more commonplace.

While the word "cybersecurity" may cause you to envision a hacker on a computer in a dark room in a far-off land, cybersecurity is actually something that you're likely involved in every single day whether you realize it or not.

The annual proclamation released by President Biden on Monday, Oct. 3 declares that Cybersecurity Awareness Month aims to "highlight the importance of safeguarding our Nation's critical infrastructure from malicious cyber activity" as well as raise awareness for "simple steps Americans can take to secure their sensitive data and stay safe online."

Qi Liao, computer science faculty member and professor for Central Michigan University's College of Science and Engineering, shared his expertise on cybersecurity, what is being done to combat it and how CMU is educating future cybersecurity professionals.

Since it is Cybersecurity Awareness Month, why is cybersecurity so important? Why should most people care?

Thirty years ago, we computer scientists only focused on making things work, such as early versions of Windows, emails and websites. Security was only an afterthought. Nowadays, there is no need to convince anyone security is important. Security is in everyone's daily life. For example, if one falls for a phishing scam they may suffer major financial loss, malware infections may cause major business interruptions and huge financial loss. On a larger scale, security breaches in national infrastructures could cause large-scale power outages, water poisoning, nuclear disasters or more issues.

What are cybersecurity professionals doing to combat issues?

Traditionally, cybersecurity industries come up with malware signatures, like a vaccine in medicine, whenever a new computer virus comes out. To combat with the vulnerabilities, professionals adopt behavioral-based mechanisms utilizing artificial intelligence and machine learnings techniques. While AI/ML-based automations are important, researchers have also used data visualizations to bring humans into the loop for better decision making in terms of cybersecurity situation awareness and investigations. Viewing cybersecurity as a purely technological problem sometimes results in a never-ending arms race between the good and bad sides. Often, economic principles and game theoretical modeling may be helpful to analyze the dynamic interactions between attackers and defenders, ultimately removing the root cause (i.e., financial incentives) of many cybersecurity criminal activities.

Why is cybersecurity education important?

Cybersecurity education is important for both professionals and the general public. On the one hand, we need to train professionals to build safe, secure, and dependable systems, and to trace and fight cyber-criminals. On the other hand, we cannot win the war if we only rely on military soldiers. The vast majority of security incidents are not overly technical but are performed on unaware users so we need people to have security built into their mind. Even simple security education such as: don't click on links on suspicious emails, don't type in passwords on phishing websites, don't set up a Wi-Fi router without a password, etc., can help. A heavily fortified front door is meaningless if the backdoor is left open. Security always depends on the weakest link.

How can people get educated on cybersecurity?

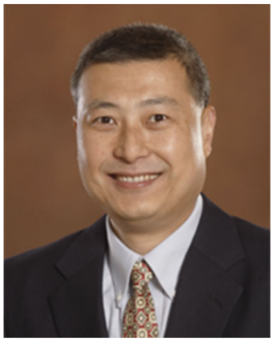
Cybersecurity is one of the fastest growing and in-demand job markets in the world. The worldwide cybersecurity market was valued at $156.24 billion in 2020 and is expected to reach $352.25 billion by 2026. According to Cyberseek, there was an annual talent shortfall of 39,000 information security analysists from May 2021 through April 2022. There are currently 534,548 additional openings requesting cybersecurity-related skills, and employers are struggling to find workers who possess them.

This fall, CMU introduced a new cybersecurity bachelor's degree program through the Department of Computer Science, which compliments the university's cybersecurity graduate program and cybersecurity graduate and undergraduate certificates. The cybersecurity major is interdisciplinary, involving mathematics, management of information systems, computer science and information technology, and integrates closely with the computer science curriculum so students are trained with security in mind. The cybersecurity major prepares students for a variety of in-demand cybersecurity careers, dedicated to securing vulnerable data and information infrastructure and stopping cyberattacks in the digital environment.

Cybersecurity public awareness, education and training opportunities at local community levels and K-12 students at schools also have broad impact on public cybersecurity education.

What can we expect in the future of cybersecurity?

While I wish I had a crystal ball to predict the future of cybersecurity, I do not, but my research in cybersecurity will focus on the following areas. First, while we are more and more relying on AI/ML-based defense mechanisms, the security of AI/ML is largely unknown. As we move to Internet of Things and autonomous vehicles, research on adversarial attacks on AI/ML-based mechanisms is promising. Second, as we are transitioning to quantum computing, we need to design new security protocols and cryptographic framework. Our current cybersecurity curriculums also need to be rewritten under this revolutionary change. Lastly, data-selling ransomware is inevitable so my near-term research will focus on building prototypes of preventive encryption and deception to defend against it. We must always prepare to be one step ahead of potential attacks.



About Qi Liao

Qi Liao is a Professor in the Department of Computer Science at Central Michigan University. He received his M.S. and Ph.D. in Computer Science and Engineering from the University of Notre Dame and his B.S. and departmental distinction in Computer Science from Hartwick College in New York, with a minor concentration in Mathematics.

Liao's research interests include computer security, anomaly detection, machine learning, visual analytics, and economics/game theory at the intersection of network usage and cybersecurity. Learn more about Liao's work and research interests through his profile.

Share

f 🐦 in

Related News

1200 S. Franklin St.
Mount Pleasant, Mich. 48859
989-774-4000

FACULTY & STAFF DIRECTORY

NEWS

DEPARTMENTS A-Z

EVENTS

MAPS & DIRECTIONS

GIVING

CAREERS AT CMU

BUDGET & TRANSPARENCY

Nondiscrimination Statement

Privacy Policy

Website Accessibility

Website Feedback

Consumer Information

Campus Safety Information and Resources