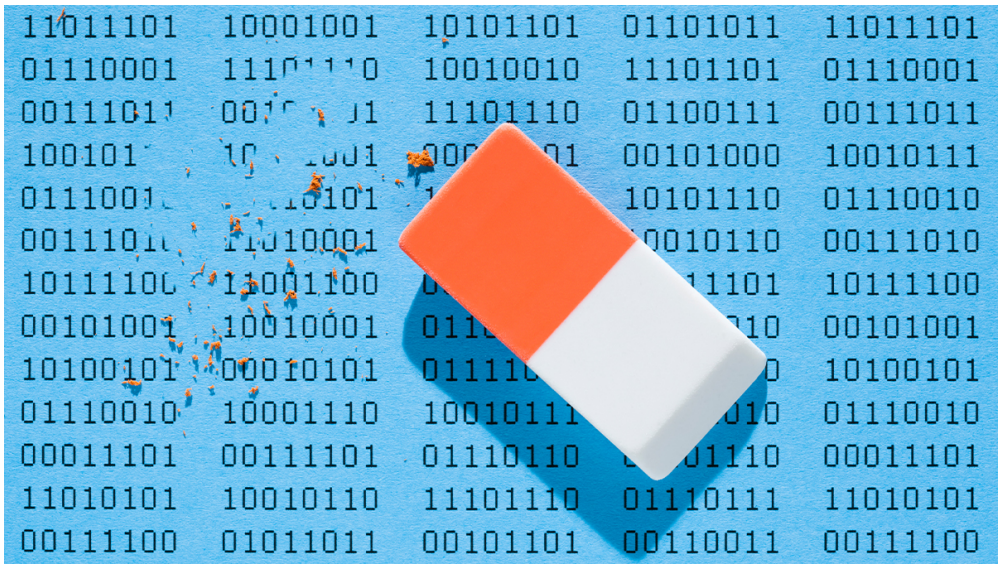
# Every Computer Science Degree Should Require a Course in Cybersecurity

Harvard Business Review

Loading...



JORG GREUEL/GETTY IMAGES

Cybersecurity is eating the software world. In recent years we've seen a rising number of security scares, ranging from Russian interference in the 2016 U.S. presidential election to the 2017 Equifax breach of Americans' private information to Facebook's numerous data woes. What's worse, nothing seems to be getting better. In the past six years over 1,000 data breaches have occurred globally, despite the promises of companies worldwide that "we take your privacy and security seriously."

The problem is that many companies do not have an incentive to care for our personal information when the biggest punishment amounts to nothing more than a slap on the wrist. Companies frequently sacrifice security for other business developments, since investing in it often yields no immediate financial benefits. Further, companies and governments alike will not, and cannot, improve their posture without a pipeline of talented individuals who understand how security works.

As a security researcher who has discovered hundreds of flaws in the systems of companies and governments, I can say the severest issues are often the simplest — an indicator that companies need to go back and review the basics.

Looking through data breaches reveals a remarkable trend: In almost all cases, they stem not from sophisticated hackers' exploiting novel vulnerabilities, but rather from simple errors that any well-trained eye could spot. The Equifax breach, according to its CEO, was due to a single employee's error, and was easily preventable. Dow Jones similarly suffered a data breach because an employee misconfigured a server storing user information, exposing customer data to any public visitor.

The cybersecurity talent shortage is well documented, with one source saying there are roughly 500,000 unfilled jobs in the U.S. alone. While it is clear that these workers are desperately needed, I question if generic cybersecurity roles are all that is needed to combat a future of data breaches and attacks. After all, in a world that is increasingly dominated by the internet, software creators play a crucial role. As connectivity continues to expand from the internet to our wrists, cars, and entire livelihoods, security will continue to become more and more important to real-world safety. Should companies fail to act, the state of security will stay the same while the stakes grow astronomically higher.

If you ask the average software engineer what role security plays in their development process, most responses would likely lie somewhere along the lines of "I don't really think of security" or "I bring in security when I need it." In fact, developers are woefully unprepared and many lack even the most basic security knowledge. In a survey, almost 70% of development and IT professionals described their training in application security as "inadequate" and 86% said their organizations are not investing enough in this kind of training. As a consequence, most developers view security as an afterthought, an extra step that stunts otherwise speedy development. But as data breaches become the norm, this paradigm must change. Why shouldn't software engineers — who are building the code that underpins technological advancements — be responsible for the code's security?

Systematically addressing the problem of security begins with educating software developers at scale. Given that the majority of breaches can be readily prevented using industry best practices, a small amount of knowledge can go a long way. Universities are partly to blame for this lack of preparation. Just one of the U.S.'s top 24 undergraduate programs in computer science lists a security course as a core requirement (I checked). That one exception: UC San Diego. At the other 23 schools, students can obtain a degree without taking a single class in security, and go on to write code that affects the devices on which we increasingly rely.

As an undergraduate student at Stanford, I have the opportunity to see firsthand how the next generation of computer scientists and software developers are incubated. While the curriculum does well at covering computer science fundamentals and hot trends such as machine learning, security is markedly absent from the list of degree requirements. Stanford's only practical security classes for computer science majors are offered as electives for those who might show interest.

Given that Stanford, among other universities, is producing computer scientists who will inevitably be responsible for the impact technology has on our world in the coming decades, it is the duty of colleges to ensure students can not only get a job but also code with the attention and precision that security necessitates. For this reason, universities should overhaul their degree requirements in order to make a security course standard for all students studying computer science. Such a course should teach fundamentals of building secure software, including common security pitfalls, secure coding practices, and application security. Through this course, universities could also explore the implications of technology's being applied to the functioning of society at large, as students learn the technical knowledge needed to build a secure internet.

The security community is at a standstill in making strides to improve global security. Companies must make security experience a priority when hiring developers, and schools must prepare developers by giving them the security skills needed to be well-rounded developers. Until a developer's ability to code securely is valued as much as their ability to write a sorting algorithm, we will continue to face large-scale problems. Give software engineers the basic knowledge needed to build secure code, and the results will pay for themselves.

Jack Cable (aka @Cablej) is a coder turned white hat hacker and Stanford University student, currently ranked within the top 50 on HackerOne. In 2018, Jack became the youngest person to receive security clearance from the Department of Defense through his work on government cybersecurity programs. He is also the founder of Lightning Security. In 2018, Jack was acknowledged by Time Magazine as one of 2018's 25 most influential teens.