8 FIELDS THAT NEED MORE CYBERSECURITY PROS

Florida Institute of Technology

High Tech with a Human Touch™

8 FIELDS THAT NEED MORE CYBERSECURITY PROS

FLORIDA INSTITUTE OF TECHNOLOGY

Cybersecurity is the process of protecting computer systems from unauthorized access. As our world has become more interconnected, we have become increasingly dependent on technology. This dependence makes us more vulnerable than ever to cyberattacks.

This vulnerability is growing increasingly apparent. In recent years, the news has been filled with reports of cyber-attacks and data breaches. Criminals, activists and even governments are turning to hacking to perpetrate large-scale criminal activity, interfere with business activities and launch attacks on other countries. This means that individuals, businesses, organizations and governments must protect themselves from cyber-attacks.

NEED FOR CYBERSECURITY EXPERTS

The world needs cybersecurity experts more than ever before. According to Forbes Magazine, there are currently 200,000 vacant cybersecurity jobs in the United States [i] and this shortage is projected to increase. The United States Bureau of Labor Statistics predicts an 18% annual growth in domestic demand for cybersecurity professionals through the year 2024. This demand has driven wages to unprecedented levels as well; in 2015, the median pay for information security analysts was more than $90,000 per year.[ii] **Cyber security ranks among the best fields for tech-savvy students and adults.**

THE AVAILABLE JOBS IN CYBERSECURITY APPEAR IN NEARLY EVERY INDUSTRY. DIFFERENT INDUSTRIES ARE SUSCEPTIBLE TO DIFFERENT ATTACKS. HERE ARE EIGHT INDUSTRIES THAT ARE POTENTIALLY VULNERABLE TO CYBER-ATTACK:

1

SECURITY INDUSTRY

The security industry is the most obvious area that requires cybersecurity professionals. Computer technology changes quickly, and the field is constantly evolving. Not only does new technology lead to new risks, hackers continue to uncover hidden vulnerabilities in historically tried-and-true technologies.

Security is no longer an afterthought. High-profile breaches, hacktivist demonstrations and criminal activity demonstrate the urgent need for security. Now companies that hope to succeed must design security into their products, right from the start. They will need cybersecurity pros in every phase of product development.

Biometric protection is an important technology in the security industry; biometric technology is designed to authenticate users based on fingerprints, retinal scan, voiceprint or other physical characteristics. As security concerns continue to grow, this technology could become the standard for many operating systems.

All of these technologies mean that businesses will require qualified people to implement and manage security.

2

GOVERNMENT

The United States is adopting a more adversarial posture when it comes to foreign cyber-attacks. Aside from any political ramifications of this move, the change will likely place a target on America. Cyber-attacks are one of the most effective ways terrorists organize to attack the United States. Even a single motivated individual can present a serious cybersecurity threat. In the same way that the internet enables an entrepreneur to market a product around the world, it allows anyone bent on creating mischief an avenue for an attack. The United States government is reacting to fears of cyber-attack by implementing new cybersecurity measures.[iii] Only time will tell if the new measures are adequate.

3

RESEARCH

Artificial intelligence ranks among the most revolutionary security technologies of our time. Computers are much more effective than human beings at processing and analyzing big data. Computers can sift through a list of names, known associates, phone and financial records and other data to find connections that could have gone unnoticed. This will give law enforcement and security experts a leg up on criminals.

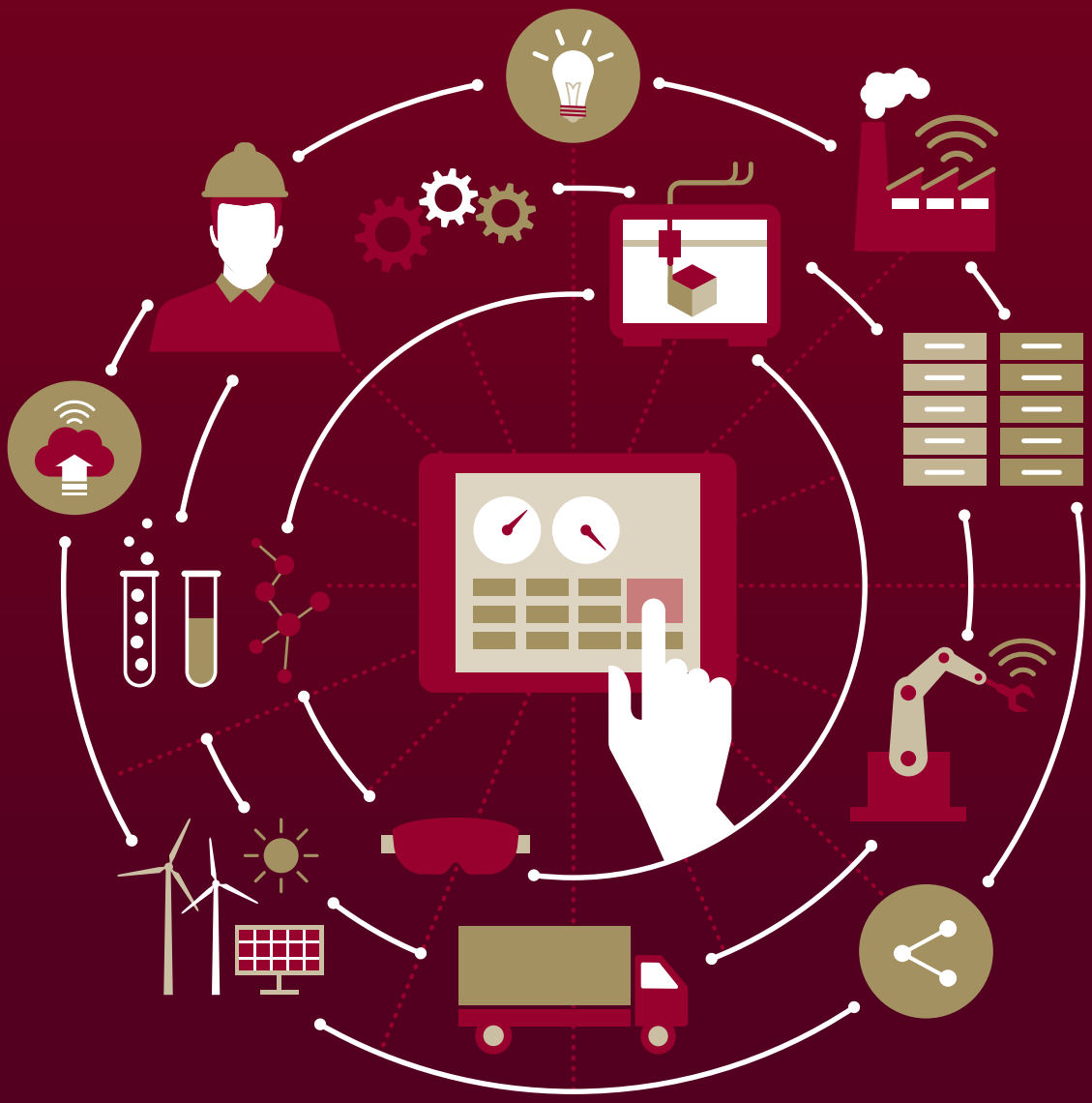
As this technology grows and matures, its widespread adoption is a virtual certainty. One thing that computers do not have is human intuition. Before a business or government takes action on computer derived intelligence, there should always be a human being in the loop. Law enforcement and other organizations will depend on people who can understand and modify artificial intelligence security systems. In addition, there is much research to be done to make the systems more effective. Artificial intelligence applied to security will be an important field of study for many years to come.

4

INFRASTRUCTURE

Most of our infrastructure, including our power grid, water distribution systems and traffic signals, depend on the internet in some way in order to operate. While this has the advantage of making our systems smarter and more powerful, it also opens the door for hackers to attack them. A successful attack on a structure could not only be extremely inconvenient, it could be very dangerous as well.

Without service security specialists to detect and eliminate these threats, we will face a severe threat to national security.



5

CONSULTING

Business leaders in many at-risk industries face a significant knowledge gap in the area of cybersecurity. They need qualified cybersecurity pros to help create solutions to problems they might not even know exist. For many businesses, the answer is cybersecurity consulting. Rather than invest in the resources and build solutions from scratch, cybersecurity consultants can help businesses leverage existing technology to improve security.

6

SMART SENSORS

Connected homes, wearables, appliances and many other devices are now being outfitted with sensors and wireless internet access. Unfortunately, such as with our infrastructure, anything connected to the internet is potentially vulnerable to hackers. In the future, cybersecurity will go far beyond servers, workstations and communications infrastructure. It will expand to include medical devices, utility infrastructure, appliances, vehicles, factory machinery, and the countless other types of devices that will be connected to the internet over the next few years.

The smart sensor market is expected to be worth $57.77 billion by 2022.[iv]

7

MACHINE LEARNING

As our understanding of human health and the surrounding challenges continues to improve, the variety of jobs available in the field of biomedical engineering expands. The possibilities of study are almost endless–careers in the marketing and sales of biomedical products, designing mechanical elements such as prosthetics, even legal careers in the regulation and administration of biomedical engineering practices. The caliber of careers available expands with your education in cybersecurity, making a graduate degree essential to applying yourself in the industry.

8

AUTONOMOUS AUTOS

Self-driving vehicles could potentially revolutionize ground transportation. The vehicles depend on sophisticated computer systems in a network of sensors to navigate our roads with little or no human intervention. One major concern hindering the adoption of self-driving cars is this fear that malicious hackers could hijack the operating system and cause widespread chaos or destruction. Most of the research on self-driving cars to this point has been focused on actually making them a possibility. For the technology to reach widespread adoption, it will require a new focus on security.

Sadly, even traditional, human-operated vehicles are not immune to hacking. Cars are dependent on computers to operate efficiently. Many modern cars have more than 100 electronic control units (ECUs) that control all of the major functions of a car, including brakes, steering and the engine. These units may not be directly connected to the internet, but as researchers have found, they could be vulnerable to hacks that gain access through the entertainment system. Some of these hacks have already been demonstrated, and many more attempted attacks are likely.[v]

[i] http://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/#694f29f87d27
[ii] https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm
[iii] http://www.nbcnews.com/news/us-news/trump-admin-outlines-plan-tighten-government-cybersecurity-n714841
[iv] http://www.marketsandmarkets.com/PressReleases/smart-sensor.asp
[v] https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

EARN A MASTER'S DEGREE IN CYBERSECURITY

With all the attention on cybersecurity and the shortage of available workers, cybersecurity is a hot field. If you have the skills and education, you could position yourself for a lucrative, rewarding career. The best way to gain these skills is with a quality education. As you consider your future career plans, consider whether an advanced master's degree could be a good fit for you.

If you are interested in developing your cybersecurity expertise and want to enhance your career, consider earning a master's degree in information assurance and cybersecurity from Florida Institute of Technology.

Your expertise will only grow as you master valuable skills and competencies that can translate into a rewarding career as a successful cybersecurity professional.

LEARN MORE HERE

Florida Institute of Technology

High Tech with a Human Touch™