YOUR COLLEGE
DECISION
Florida Institute of Technology

WHY CYBERSECURITY IS A GROWING CAREER FIELD

All anyone has to do is watch the news these days to know the threats that individuals, businesses and governments face from cyberattacks. Aimed at obtaining personal, financial and proprietary information, these attacks aren't going away, but rather continue to advance rapidly as cybercriminals become smarter and more sophisticated. Security professionals agree that it is not a matter of if there will be a breach, but rather it's a matter of when.

Issues In Cybersecurity

The digital age has put everyone in a battle to fight a constantly growing environment of potential security threats. The challenge has grown from protecting access to a building or outside attacks on a computer network to the myriad of vulnerable facets of daily life and business, including how to control the damage once a breach is made.

Cybercrime is happening just about everywhere including mobile and cloud services, computerized appliances, connected automobiles, credit cards, and health and financial systems, to name a few. New technologies enter the market regularly, bringing with them unforeseen vulnerabilities that can easily translate into data breaches that result in setbacks for businesses and their customers. When just about everything in our daily lives is connected to the internet, an app or a social media platform, lax security knowledge and threat protocols puts personal and business information, finances and livelihoods at risk.

But it doesn't end there. Human nature is one of the biggest threats to good security procedures. Employees may ignore policies or overlook procedures for any number of reasons that then make a company and its information ripe for a security breach. Fact is, most companies don't have a comprehensive awareness of the security threats and risks they face from both inside and outside their company, particularly with so many employees working on mobile, at home or on vulnerable networks in airports and coffee shops. Because corporations are relying on software developed by outside companies, legacy systems and a staff with a range of expertise, it's critical for managers to be aware of the myriad of issues related to cybersecurity and how best to protect their company's assets.

Consumers also fall victim to cybercrime outside of their exposure from the companies they deal with.

The 2016 Norton Cybersecurity *Insight Report* found that despite the threat and awareness of cybercrime, consumers remain complacent about protecting their personal information and often engage in risky behaviors such as:

- sharing passwords
- clicking on links in emails
- using the same login parameters for all their accounts

In fact, victims of cybercrime often continue their unsafe behavior thinking there's just too many people connected in the world for it to affect them again.

Cybercrime Targets Everyone

One of the biggest misnomers when it comes to cybercrime is that large companies are the most likely targets. According to security software company Symantec, 74% of small and medium-sized businesses have recently been targeted and attacks should continue to rise as the environment for breaches and phishing attacks escalates. In fact, *Forbes* recently reported on a survey by IBM and Ponemon of 2,400 security and IT professionals, which found that 75% of the respondents did not have a formal cybersecurity incident response plan across their organization. And 66% of those who replied weren't confident in their organization's ability to recover from an attack. Cybercriminals are using social media to sell and share data as well, according to a whitepaper by RSA (2016: Current State of Cybercrime). In a six-month study, RSA uncovered more than 500 fraud-dedicated social media groups with more than 220,000 members, and 60% of those on Facebook.

According to CSO Online, cybercrime damage costs will be nearly $6 trillion annually by 2021. As a result, cybersecurity spending on products and services was more than $80 billion in 2016. While this is all disconcerting for individuals and tough for businesses and governments to tackle in their budgets, cybercrime will more than triple the number of unfilled cybersecurity jobs.

76%

of consumers know they should protect their information online, but they continue to engage in risky behaviors like sharing passwords.

CYBERCRIME ISSUES ON THE RISE

- Sophisticated Phishing Campaigns
- Ransom Ware
- Fraud Dedicated Social Media Groups
- Dependence on Third Party Vendors
- Lack of Internal Network Protections/ Procedures
- Mobile & Cloud Network Vulnerabilities
- Internet of Things Malware
- Machine Learning & Artificial Intelligence Advances
- Escalation of Espionage

Cybersecurity Professionals Are In High Demand

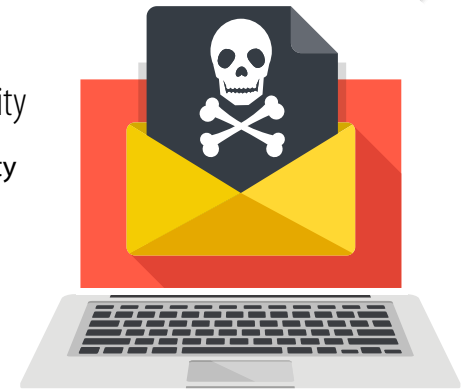
This volatile climate has created a demand for knowledgeable professionals who can help businesses, governments and consumers be better aware and better protected from cybercrime.

Educators from high school through secondary and post-secondary institutions are creating courses and degree programs to prepare individuals for this fast-growing industry and its huge demand for employees. Students entering computing and cybersecurity fields are gaining expertise in computer science, software engineering and mathematics as the basis for any additional expertise with emerging technologies.

Individuals who specialize in cybersecurity conduct threat assessments and remain vigilant about the ever-changing security landscape as well as perform duties such as:

- design and implement security solutions
- perform vulnerability testing
- conduct risk analysis
- train staff and employees on security policies
- respond to incidents and conduct investigations
- update security systems
- support software updates and network needs

DEFENSIVE Cybersecurity



A defensive cybersecurity specialist employs security practices that safeguard computer systems to avoid dangerous computing activity and prevent cyberattacks. These tactics are aimed at overcoming any risky behaviors happening by a computer user and include:

- Patching Software: an attacker may exploit areas of software code that offers an entry point for them to infuse malicious code like viruses and malware. A defensive specialist analyzes software code for weaknesses, fixes any areas of concern and scans for vulnerabilities.
- Firewall Protection: this collection of security measures protects a network from harmful traffic and prevents unauthorized access. A defensive specialist strives to create an impenetrable firewall that blocks potentially harmful traffic and allows safe communication.
- Data Backup: A safety net for any system in case of a malicious attack, data breach or other malicious behavior.

OFFENSIVE Cybersecurity

Offensive cybersecurity specialists take a proactive approach to protecting computer systems by testing attacks on their own systems in order to discover vulnerabilities and prepare for their response during a real attack. This can include:

- Attempts to disrupt and, if possible, disable an attacker's operations.
- Actions that seek out and identify an attacker to stop a current attack and prevent a future one.
- Analysis of all attacks to help better prepare for future ones. Understanding the circumstances of an attack gives important information to strengthen security.

TOP 10 SIGNS YOU HAVE WHAT IT TAKES FOR A CYBERSECURITY CAREER

1. You are curious and perceptive
2. You are persistent and determined
3. You are good at problem solving
4. You aren't overwhelmed by complexity
5. You have an enthusiastic imagination
6. You are an effective listener
7. You are ethical and reliable
8. You can think like a "bad guy" and anticipate incidents
9. You are a team player
10. You can work under the gun and pay attention to detail

What a
Bachelor's Degree
Can Do

JOB STABILITY:

53% of all U.S.-based businesses have been attacked.

ABOVE AVERAGE EARNINGS:

The median annual salary for cybersecurity analysts in 2016 was $92,600.

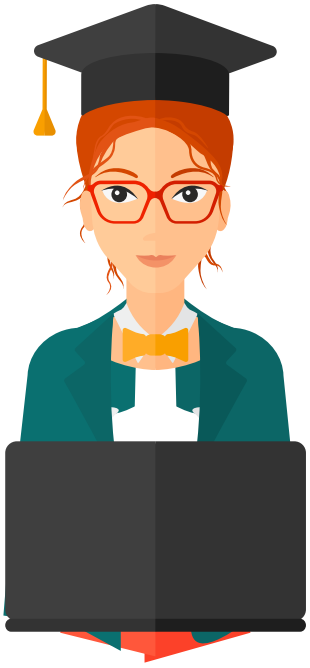
JOB GROWTH:

Demand for cybersecurity experts has grown twice as fast as the overall IT job market.

JOB PROTECTION:

Cybersecurity jobs are not vulnerable to the rise of automation and robots which pose a threat to some jobs.

Sources: *Hartford Business, U.S. News & World Report*



What a
Master's Degree
Can Do

JOB STABILITY:

23% of cybersecurity job postings require at least a master's degree.

ABOVE AVERAGE EARNINGS:

The median annual wages for cybersecurity professionals ranges from $70,000 to $118,000+.

JOB GROWTH:

The Pentagon is one job sector planning to triple its cybersecurity staff.

JOB PROTECTION:

Cybersecurity job postings grew 91% between 2010 and 2015, and the field is projected to grow by 37% over the next 10 years.

Sources: CSO Online, Burning Glass Technologies, U.S. Dept. of Labor O*Net Online

CYBERSECURITY JOBS

- Chief Information Security Officer
- Security Engineer
- Security Architect
- Incident Responder
- Computer Forensics Expert
- Penetration Tester
- Security Analyst
- Security Software Developer
- Security Auditor

Job Availability

In 2017, the U.S. employs nearly 780,000 people in cybersecurity positions, with approximately 350,000 current cybersecurity openings, according to CyberSeek, a project supported by the National Initiative for Cybersecurity Education (NICE), a program of the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce.

The current number of U.S. cybersecurity job openings is up from 209,000 in 2015. At that time, job postings were already up 74% over the previous five years, according to a Peninsula Press analysis of numbers from the Bureau of Labor Statistics.

The Bureau of Labor Statistics also reports that employment is projected to grow 18 percent through 2024.

The federal government, health care and cloud service companies are areas that will have job openings. Because the demand for this expertise touches nearly every business, organization and nonprofit agency, jobs should be prevalent in nearly any industry.

Cybersecurity professionals report an average salary of $116,000, or approximately $55.77 per hour. That's nearly three times the national median income for full-time wage and salary workers, according to the Bureau of Labor Statistics.

Florida Institute of Technology

MK-613-1017