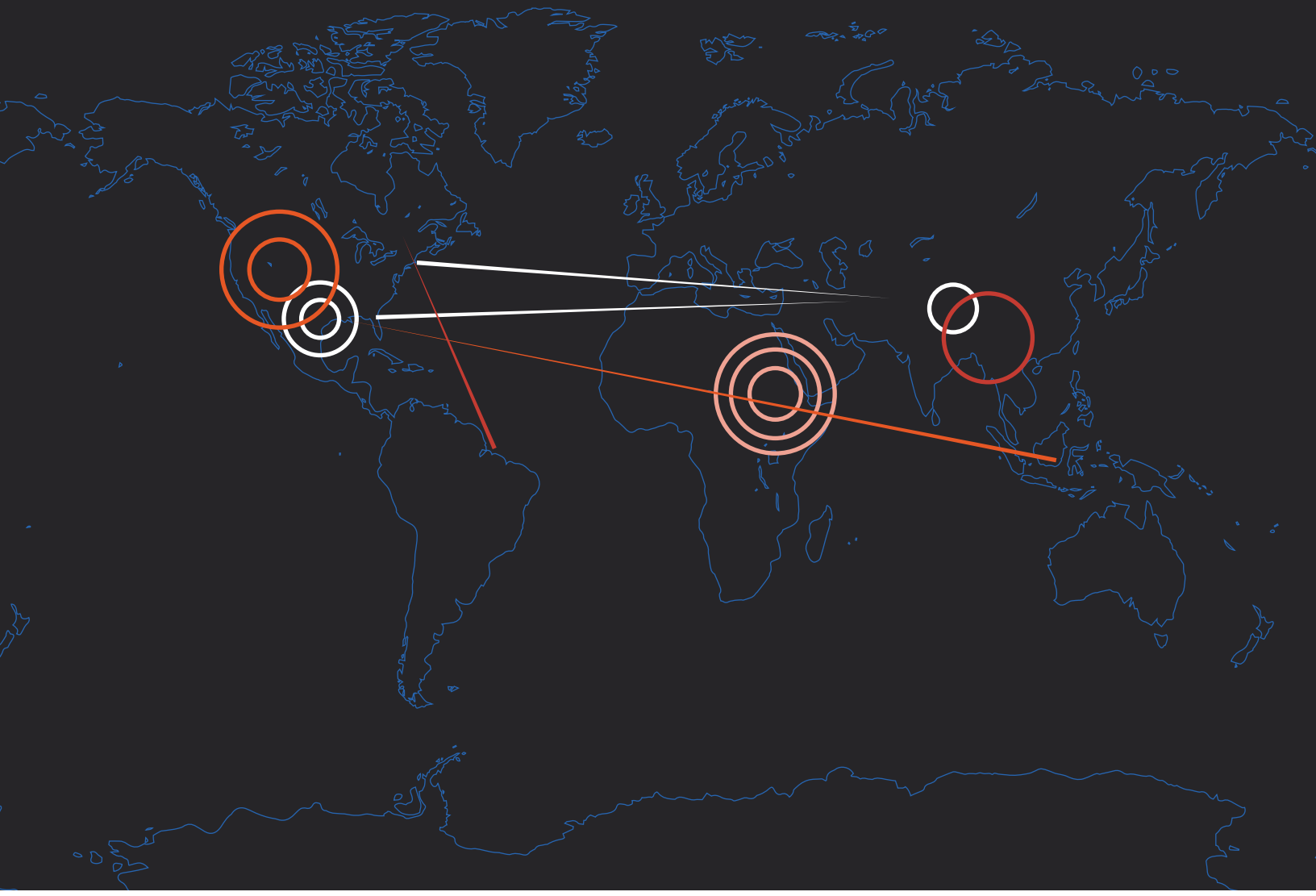
The Cybersecurity Career Guide



UTICA COLLEGE

Table of Contents

Introduction

What used to be the domain of fanciful Hollywood movies and a few extremely talented hackers is now a thriving career field. Thousands of opportunities are available in cybersecurity with government, business, and non-profit organizations. According to NetworkWorld, now is one of the best times to enter the industry.

Cyber weaknesses and issues arise from forces outside the organizations, as well as from internal employees and contractors. These are a few of the types of threats that a cyber security professional work against:

- Trojans designed to get unsuspecting users to run malware that's disguised software
- Phishing attacks through email that trick recipients into providing personal, sensitive information
- Ransomware that locks users' files until the victims pay to free the files
- Point of sale attacks, like the one that targeted retail giant Target in 2013

Even momentary access points with assumed partners can open up defenses enough to cause big problems if not prepared for properly. After all, every system follows the same principle: they are only as strong as the weakest link, and it's the cyber security analyst's job to find and neutralize those weak points as they occur, or to prevent them from happening at all.

Cybersecurity analysts help organizations keep their technology systems running efficiently and without disruption, as well prevent theft of sensitive information. The assets to be protected can range from government and military files to financial records and customer information. Protection is ongoing and continuous in monitoring and identifying weaknesses. Expert cyber security analysts prevent organizational and financial disasters with technology and save time, money and productivity.

According to May 2014 data from the Bureau of Labor Statistics, the average annual salary for information security analysts nationwide was approximately $90,000, with wages for the top 10% exceeding $140,500. Cyber security positions frequently earn a premium over other IT jobs by as much as $10,000 annually. According to Burning Glass Consulting, cyber security job openings have increased three times faster than for IT jobs in general, and cyber security professionals can earn 9% more than non-cyber IT workers.

This guide is for anyone considering a career in cybersecurity. It covers cyber security careers by sector and job type, and it wraps up with an overview on where students might begin their cybersecurity career paths.

Chapter 1: Cybersecurity Careers by Sector

Like many technical fields, cyber security can be broken into a number of specialty areas, and this guide looks at six: government, telecommunications, finance and business, retail, utilities and transportation. Although the industries differ in their scopes, the BLS explains that roles of cyber security professionals are similar across industries. They are responsible for:

- Monitoring an organization's network
- Installation of software (such as firewalls and data encryption programs) to protect the network and to facilitate the monitoring task
- Prepare reports on findings
- Conduct testing that simulates attacks to find vulnerabilities
- Continually conduct research to stay ahead of technology
- Develop the organization's cyber security policy
- Educate all network users and ensure they follow policies and guidelines
- Create and update a disaster recovery plan

Government

Government cybersecurity jobs are predominantly in the areas of intelligence, military, law enforcement, emergency management, and data system protection of sensitive areas, such as nuclear labs. The U.S. Government Accountability Office urges federal agencies to heighten protection of breaches that involve personally identifiable information (PII). Such breaches have increased from 10,481 in 2009 to 25,566 in 2013.

Government databases make ripe targets for stealing information and sabotaging it; therefore, much of the defensive side is focused on system integrity, preventing intrusions, and identifying culprits. The proactive side is aligned with identifying, tracking, and anticipating the motivations of people and entities that are considered risks to government. Positions in civil service come with employment protections and defined benefit packages. High-level analysts may move into political roles.

A good source for career information can be found with the National Initiative for Cybersecurity Careers and Studies. There is also the Resource Center for State Cybersecurity, which is focused more on state and local issues versus federal.

Some of the agencies that are consistently looking for cyber security professionals are: The Department of Homeland Security, Federal Bureau of Investigation, and National Security Agency. Below are links to various federal agencies that are hiring:

- National Security Agency: "Cyber is a team sport." Jobs are available in computer science, computer engineering, electrical engineering, intelligence analysis and mathematics
  - *NSA Careers – Register and search for NSA jobs by keyword.*

- Department of Homeland Security: "...the demand for an experienced and qualified workforce to protect our nation's networks and information systems has never been higher."
  - *Homeland Security Job Search*

- Federal Bureau of Investigation: "As computer and online usage continues to grow, so does the FBI and our responsibilities."
  - *FBI Jobs Search*

- U.S. Army Cyber Command: "We want to recruit, develop and retain the 21st century cyber warrior."
  - *Army Civilian Job Search on USAJobs*

- Defense Cyber Crime Center: "DC3 employees tackle an array of technical and mission challenges."
  - *USAJobs – Search for a job with DC3*

Telecommunication

Telecommunication careers are associated with preserving and protecting communication systems. Cyber security analysts spend much of their time monitoring and guarding systems as well as tracking hackers. Additionally, they are the testers who make sure networks are not compromised.

It's often the case that these positions help law enforcement and government agencies pull together the data needed for evidence and arrests. They spend much of their time watching risk environments to determine what the next new types of threats will be to telecommunication systems. The industry has several associations, which include the National Telecommunications Cooperative Association for rural networks, and the National Cable & Telecommunications Association as well as the Telecommunications Industry of America.

Finance and Business

Financial systems are big targets for attacks, up to 300% more often than other data systems according to a study by commercial cybersecurity company Raytheon|Websense. Financial security analysts spend a good portion of their days looking for risks, responding to potential intrusions, and helping investigations and compliance audits.

The Burning Glass Cybersecurity Jobs report tells us that cyber security jobs that require accounting and finance skills along with IT security knowledge are the hardest jobs to fill. These two skillsets are rarely taught and learned together. Those who are proficient in both would be highly sought after in this industry. The finance and insurance sector accounted for 13% of Burning Glass's cyber security job postings for 2014.

Financial security experts can be involved in investigating a number of issues, including embezzlement, insider trading and outright electronic theft. It's frequently cyber security analysts in the financial field who reconstruct an intrusion and trace it back to the culprit. No surprise, the American Bankers Association has a strong interest in cyber security even though the association is generally affiliated with the overall banking industry. The Association of Financial Professionals also has a section of its efforts dedicated to cyber security issues.

Retail

Retail cyber security analysts are hired to keep merchant pay systems protected from hacking and diversion of transactions. The retail industry works hard to garner and maintain the trust and loyalty of its customers. A breach and subsequent backlash from the often nationally publicized event can be devastating for a company.

Retail analysts are typically in hard positions, as they monitor attacks and work feverishly to shut them down as they occur. They also put a lot of time and effort into design defenses alongside system administrators. The National Retail Federation is an advocate of cyber security and has been pushing for "pin and chip" technology, which adds protection to shoppers who pay for purchases with credit and debit cards. Professionals in retail cyber security are integrally involved with monitoring proposed policy changes and how they might affect their organizations' retail operations.

Utilities and Infrastructure

Utility infrastructure organizations include water, electricity, natural gas, and fuel pipeline systems. Given how much automation and network connection is involved with managing these utility systems, cyber analysts are critical in keeping related networks protected and running smoothly.

Monitoring and looking for anomalies is often the main defense aside from creating programs to identify breaches. The U.S. Department of Energy is one of the biggest influencers of utility cyber security, but the field category is very much in its infancy. That said, utilities are paying attention. The American Gas Association, the American Water Works Association, and the American Public Power Association are making cyber security a priority topic.

Transportation

The American Public Transportation Association's white paper entitled "Cybersecurity Considerations for Public Transit" provides cyber security recommendations for the industry. The association advocates more agility in digital infrastructure in order to fight penetration and recover quickly, whether incidents are from attacks, accidents or natural disasters.

APTA's paper illustrates what the transportation information ecosystem looks like. It is comprised of the following areas, all of which need cyber security protection because vulnerability trickles down throughout systems:

- Operational Systems: Examples include railroads, tracks and signal controls
- Enterprise Information Systems: Examples include third-party software, email systems
- Subscribed Systems: These are managed systems outside of the agency. Examples include Internet service providers, hosting companies, data storage (cloud)

Other organizations highly involved in the protecting and advocating on behalf of public transit safety are Transit Cooperative Research Program and the Intelligent Transportation Society of America.

The International Air Transport Association prepared its second edition of the Cybersecurity Toolkit. As the aviation industry is heavily dependent on computer systems, this toolkit provides extensive information along with 17 training videos.

In October 2014 the U.S. Department of Transportation published A Summary of Cybersecurity Best Practices. The paper discusses how aircraft navigation and communications functions are no longer operating as isolated and independent systems; rather they are part of a new environment of global connectivity. Because of this, the security of these systems must be scrutinized.

Given how much automation and network connection is involved with managing these utility systems, cyber analysts are critical in keeping related networks protected and running smoothly.

Cybersecurity Job Categories

The Burning Glass Cybersecurity Job report indicates seven job categories in the career field:

Job Title	Job Example	Median Annual Salary
Engineer	Network security engineer	$85,000[1]
Manager or administrator	Information security manager	$102,000[1]
Analyst	Cyber intelligence analyst	$75,000[2]
Specialist or technician	IT security specialist	$79,000[3]
Architect	Network security architect	$98,000[4]
Auditor	IT auditor	$65,000[1]
Consultant	Network security consultant	$81,000[1]

Sources:

[1] PayScale
[2] SimplyHired
[3] Glass Door
[4] BLS

Chapter 2 Cybersecurity Careers by Job Type

Cyber security functions are typically classified in functional categories for general description and job placement. These categories include a variety of organizational job types such as operations, policy and management, forensics or investigations, data collection and archiving, emergency management, and intelligence. Clearly, some areas are more specific to certain industries than others. Both intelligence and emergency management, for example, have the most demand in governmental operations. Each category includes description of what is needed for an analyst to succeed in that functional area, according to the National Initiative for Cybersecurity Careers and Studies.

Cyber security analysts with operational experience can move into executive roles. These roles can include CIOs, chief security officers, and chief technical officers.

Operations

The operations area keeps the system running, installs hardware and software, provides maintenance, and is often the first to see major intrusions because they frequently get the first call of trouble, or they catch the variance in monitoring reports. Cyber security analysts in this category have a primary focus of maintaining network efficiency and productivity. They are often the unsung heroes who implement security systems and create and enforce security protocols. They work with the staff that installs new equipment and software to ensure that devices and programs comply with company policies. These professionals look for vulnerabilities when technology companies roll out patches or updates.

Operations are often the function that is relied upon for long-term IT planning and developing proposals for new needs. They are called upon to develop cost/benefit analyses, including security risks, for new projects and expansion of existing systems. They can regularly play the presenter's role in front of executive management as well as provide support to senior managers. Finally, operations frequently provide the legwork for policy development, confirming the technical aspects of policy literature before it is applied to an organization.

Cyber security analysts with operational experience can move into executive roles. These roles can include CIOs, chief security officers, and chief technical officers.

Intelligence

Cyber intelligence analysts working in governmental and law enforcement agencies are responsible for not only collecting data and performing data mining, but also identifying and developing strategies for better network and system protection. Intelligence and law enforcement agencies are large repositories of data, and cyber security professionals use the data to look for weaknesses and predict where risks

might come from. Their efforts help contribute to stopgap measures for instances when security threats are identified.

A critical role of intelligence involves investigation and analysis. It's a field where these professionals spend long hours gathering information and identifying important trends for predictive analysis. That information is compiled quickly and distributed to decision-makers for strategic plans. Without intelligence, an organization is wide open to attack.

Forensics

The preventive work doesn't stop when the attack or damage occurs. Forensics plays a key role in investigative matters, finding and collecting evidence that not only identifies how a weakness and attack occurred but also who is involved and where more attacks might come from. The forensics cyber security analyst is someone who has developed an expertise in both hardware and software, particularly with the ability to extract information from components even when they have been damaged or deleted.

Forensics also plays a field role in evidence gathering and preserving evidence. Both government agencies and private companies have a need for forensics cyber security analysts. The role for government is in the realm of investigation for civil and criminal matters. For private companies, forensics allows a company to spot and neutralize internal and external threats. They work closely with intelligence and operations cyber professionals to prevent the failure from recurring.

Emergency Management

People who work in emergency management cyber security will find themselves predominantly working in government positions for a variety of agencies, reports the National Governors' Association. While law enforcement is the most common, emergency management also includes fire and disaster response, public health, water systems, oil and petroleum infrastructure, and transportation. The analyst's role is to maximize technology tools to assist and make emergency response as quick and efficient as possible. According to FEMA, analysts turn the technology information into critical reports as incidents occur, which become the basis for operational program decisions and resource allocations.

Analysts in the emergency management field have bachelor degrees in justice, fire science, computer science, and public policy. They could also train further with a master's degree in cybersecurity. In many cases, some of the most critical players have significant experience working in uniform positions and have crossed over into IT for additional support and technical training.

Emergency Management magazine reports that the category of emergency response support is growing tremendously, especially as federal and local agencies are beginning to share networks, standards, training, and information. This has opened a key vacuum for cyber security as much of the data sharing is electronic in nature and uses databases with multiple points of input and output.

The forensics cyber security analyst is someone who has developed an expertise in both hardware and software.

Policy

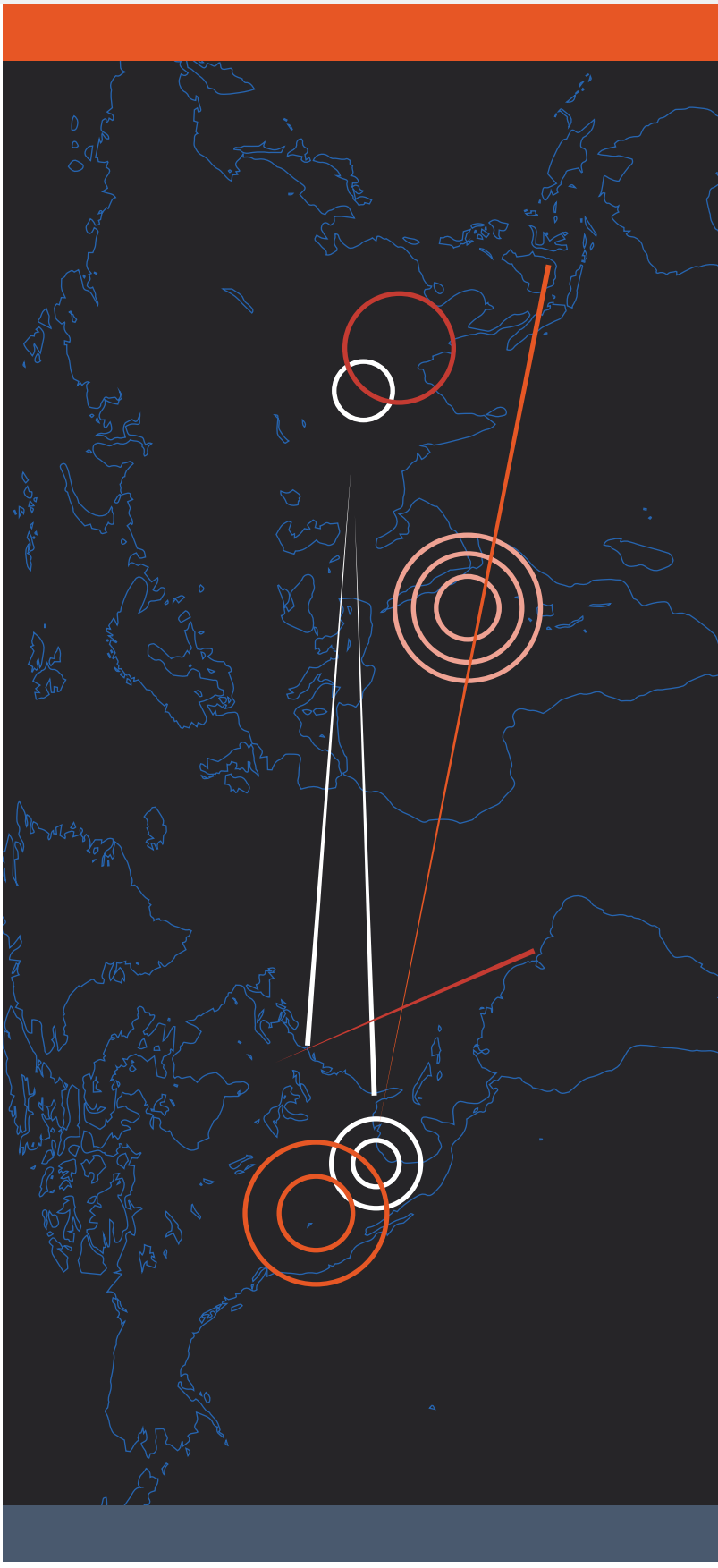
Policy comes in two forms: as directives from management and in response to things that occur in daily operations. Both are important in protecting organizations. One is overt and direct, while the other is indirect and creates functional parameters.

System administrators handle these responsibilities, and they take care of everything from Internet activity to internal and intranet platforms. These are some of the most important sources of information in an organization's computer network system.

The ongoing monitoring works like white blood cells in a human body, constantly roving, reporting and looking for anomalies in a network and related databases. This monitoring is responsible for existing network security testing, patching, and confirming defense systems are working correctly. Many hackers know human error provides the opportune entrances to a system, so it's the administrator's job to make sure this doesn't happen.

Data Collection & Fusion

The review and collection of data may seem like a mundane role, but it is often the foundation of intelligence as well as the protection of operations. Data collection and fusion are frequently about finding unidentified trends and risks to an organization. This requires skill in **data mining** and identifying flaws that might not be obvious to others inside the system. A "second set of eyes" is frequently the needed analysis to point out what gets missed through routine and complacency.



Chapter 3
Graduate Education and Experience in Cybersecurity

Utica College's Master of Science in Cybersecurity

According to the Information Systems Security Association, the cyber security career has a distinct lifecycle. It is at specific phases in that cycle where candidates become valuable to hiring agencies and companies. These phases are:

- Pre-professional
- Entry level
- Mid-career
- Senior level
- Security leader

Academic Excellence

Utica College's Master of Science in Cybersecurity is designed and intended to validate a student's formal training and give him or her credentials from a school with an excellent reputation recognized by the NSA and DHS as a National Center for Academic Excellence. At the same time, the flexible schedule and format of the online program allows working adults to maintain their careers without choosing between the education and work.

Students graduating with Utica's M.S. in Cybersecurity field can seek roles in:

- Intelligence and counter-intelligence for governmental agencies at all levels and jurisdictions
- Security roles that require fast and immediate critical thinking in digital security
- Investigation roles in computer and technology forensics and data recovery
- Liaison positions that bridge the technology administrative side to field operations
- Internal audits and ethics monitoring roles for ensuring protection and adherence to security policies
- Law enforcement roles supporting digital crime prevention and criminal prosecution based on cyber evidence
- Emergency management support and infrastructure protection, ensuring response agencies can function under extreme conditions and threats.

Faculty Network

The faculty at Utica College has deep connections with government and industry professionals, providing references and guidance on career opportunities in the field. This network and real-world faculty know-how is extremely valuable, especially for those who are seeking entry into highly competitive areas.

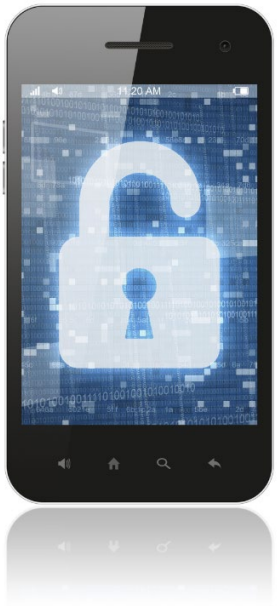
Hands-On Experience

As part of the curriculum, students are provided with fully licensed versions of industry software, such as VMWare, which gives them the familiarity to easily engage with software that is found on the job. Moreover, some courses offer live environments in which students perform actual offensive and defensive attacks. Utica College is one of the few schools that make industry-level software and real-world simulations available to students.

Learn More

Are you a problem-solver? Cyber security requires people and experts who are natural solution finders, who can work on their feet and under ad hoc conditions, who thrive on challenges and can deal with the ambiguous and unknowns every day.

Are you a good communicator? Cyber security involves technical demands that must be communicated to senior managers who might not be well versed in technology. Clear communication channels are important during times of challenge, and cyber security experts maintain those channels when risks are identified.



Reference Guide

Linda Musthaler, "This is a great time to start a career in cybersecurity," NetworkWorld Mar 21, 2014 http://www.networkworld.com/article/2175434/security/this-is-a-great-time-to-start-a-career-in-cybersecurity.html

United States Department of Labor, Bureau of Labor Statistics, 15-1122 Information Security Analysts http://www.bls.gov/oes/current/oes151122.htm

BurningGlass, "Cybersecurity Jobs, 2015," http://burning-glass.com/research/cybersecurity/

US Department of Labor, Bureau of Labor Statistics, "What Information Security Analysts Do," http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-2

U.S. Government Accountability Office, "INFORMATION SECURITY: Federal Agencies Need to Enhance Responses to Data Breaches," http://www.gao.gov/products/GAO-14-487T

National Initiative for Cybersecurity Careers and Studies, "Cybersecurity Careers," http://niccs.us-cert.gov/careers/cybersecurity-careers

NGA Center for Best Practices, "Resource Center for State Cybersecurity," http://www.nga.org/cms/statecyber

National Security Agency, "Cyber Careers," https://www.nsa.gov/careers/cyber/index.shtml

National Security Agency, "NSA Careers," https://www.nsa.gov/psp/applyonline/EMPLOYEE/HRMS/c/HRS_HRAM.HRS_CE.GBL?Page=HRS_CE_JOB_DTL&Action=A&JobOpeningId=1051475&SiteId=1&PostingSeq=1

Department of Homeland Security, "Join DHS Cybersecurity," http://www.dhs.gov/homeland-security-careers/dhs-cybersecurity

Department of Homeland Security, "Homeland Security Jobs," https://dhs.usajobs.gov/

Federal Bureau of Investigation, "The FBI Knows How Easy It Is," https://www.fbijobs.gov/CyberCareers/index.html

Federal Bureau of Investigation, "Jobs Search," https://careers.fbijobs.gov/usajobs/JobSearch.aspx

U.S. Army Cyber Command, "Cyber Warriors Needed," http://www.arcyber.army.mil/g1.html

USAJobs, "army cyber command," https://armycivilianservice.usajobs.gov/JobSearch/Search/GetResults?Keyword=army+cyber+command

Defense Cyber Crime Center, "Employment Opportunities," http://www.dc3.mil/index/employment

USAJobs, https://www.usajobs.gov/

The Rural Broadband Association, http://www.ntca.org/

National Cable & Telecommunications Association, https://www.ncta.com/

Telecommunications Industry of America, http://www.tiaonline.org/

Websense, "2015 Industry Drill-Down Report – Financial Services," http://www.websense.com/content/2015-finance-industry-drilldown.aspx

American Bankers Association, "Cybersecurity/Fraud," http://www.aba.com/Tools/Function/Cyber/Pages/default.aspx

Association for Financial Professionals, "Cybersecurity," http://www.afponline.org/Cybersecurity/

National Retail Federation, "Data Security," https://nrf.com/advocacy/policy-agenda/data-security

U.S. Department of Energy, Electricity Advisory Committee, "Implementing Effective Enterprise Security Governance," http://energy.gov/sites/prod/files/Mar2014EAC_Recs-CyberGovernance.pdf

American Gas Association, "Cybersecurity," https://www.aga.org/cybersecurity

American Water Works Association, "Cybersecurity Guidance & Tool," http://www.awwa.org/resources-tools/water-and-wastewater-utility-management/cybersecurity-guidance.aspx

American Public Power Association, "Grid Security," http://www.publicpower.org/Topics/Landing.cfm?ItemNumber=38507&navItemNumber=37539

American Public Transportation Association, http://www.apta.com/Pages/default.aspx

American Public Transportation Association, "Cybersecurity Considerations for Public Transit," http://www.apta.com/resources/standards/2014%20Q2%20Public%20Comment/RP_cyber_security_considerations_%20PUB_COMMENTS_V10%2012%2019%2013.pdf

Transit Cooperative Research Program, http://www.tcrponline.org/SitePages/Home.aspx

Intelligent Transportation Society of America, http://www.itsa.org/

International Air Transport Association, "Aviation Cybersecurity Toolkit – 2nd edition – July 2015," http://www.iata.org/publications/Pages/cyber-security.aspx

U.S. Department of Transportation, National Highway Traffic Safety Administration, "A Summary of Cybersecurity Best Practices," http://www.nhtsa.gov/DOT/NHTSA/NVS/Crash%20Avoidance/Technical%20Publications/2014/812075_CybersecurityBestPractices.pdf

PayScale, "Network Security Engineer Salary," http://www.payscale.com/research/US/Job=Network_Security_Engineer/Salary

PayScale, "Information Security Manager Salary," http://www.payscale.com/research/US/Job=Information_Security_Manager/Salary

SimplyHired, "Average Cyber Intelligence Analyst Salaries," http://www.simplyhired.com/salaries-k-cyber-intelligence-analyst-jobs.html

Glass Door, "IT Security Specialist Salaries," http://www.glassdoor.com/Salaries/it-security-specialist-salary-SRCH_KO0,22.htm

U.S. Department of Labor, Bureau of Labor Statistics, "Computer Network Architects," http://www.bls.gov/oes/current/oes151143.htm

PayScale, "Information Technology (IT) Auditor Salary," http://www.payscale.com/research/US/Job=Information_Technology_(IT)_Auditor/Salary

PayScale, "Security Consultant, (Computing / Networking / Information Technology) Salary," http://www.payscale.com/research/US/Job=Security_Consultant,_(Computing_%2F_Networking_%2F_Information_Technology)/Salary

National Initiative for Cybersecurity Careers and Studies, "Cybersecurity Careers," http://niccs.us-cert.gov/careers/cybersecurity-careers

National Governors Association, "Hearing Statement – Cybersecurity and Emergency Management," Oct 30, 2013, http://www.nga.org/cms/home/federal-relations/nga-testimony/hsps-testimony/col2-content/main-content-list/hearing-statement--cybersecurity.html

Federal Emergency Management Agency, "Cyber Attack," http://m.fema.gov/cyber-attack

Elaine Pittman, "Cybersecurity: The Most Active, Dynamic and Threatening Area of Risk," Emergency Management, Sep 10, 2012, http://www.emergencymgmt.com/safety/Cybersecurity-The-Most-Active-Dynamic-and-Threatening-Area-of-Risk.html

Information Systems Security Association, "ISSA's Cybersecurity Career Lifecycle (CSCL) Launces, http://www.issa.org/?page=CSCL

George V. Hulme, "Six entry-level cybersecurity job seeker failings," CSO online, Mar 10, 2015, http://www.csoonline.com/article/2894193/infosec-staffing/six-entry-level-cybersecurity-job-seeker-failings.html