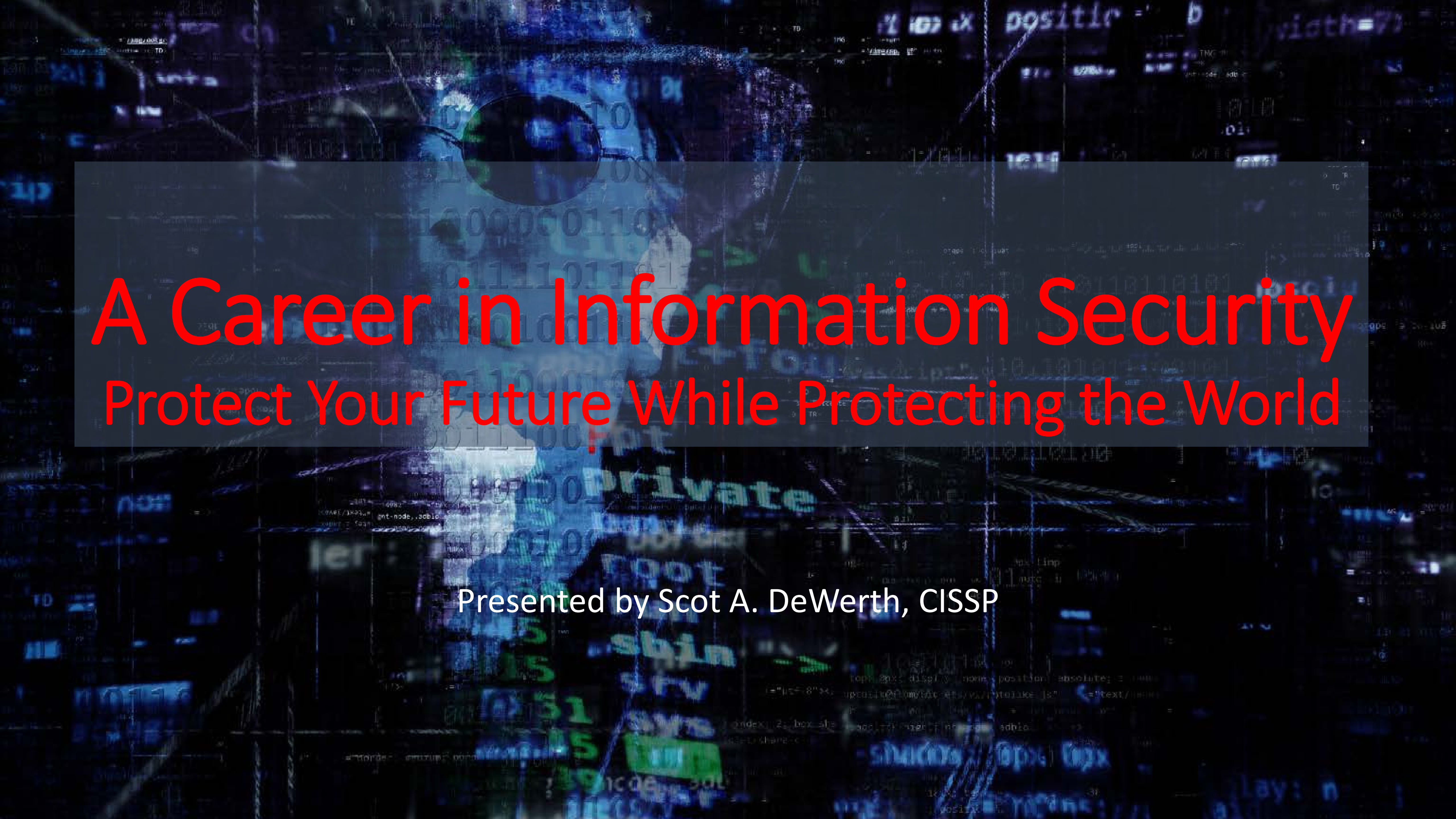
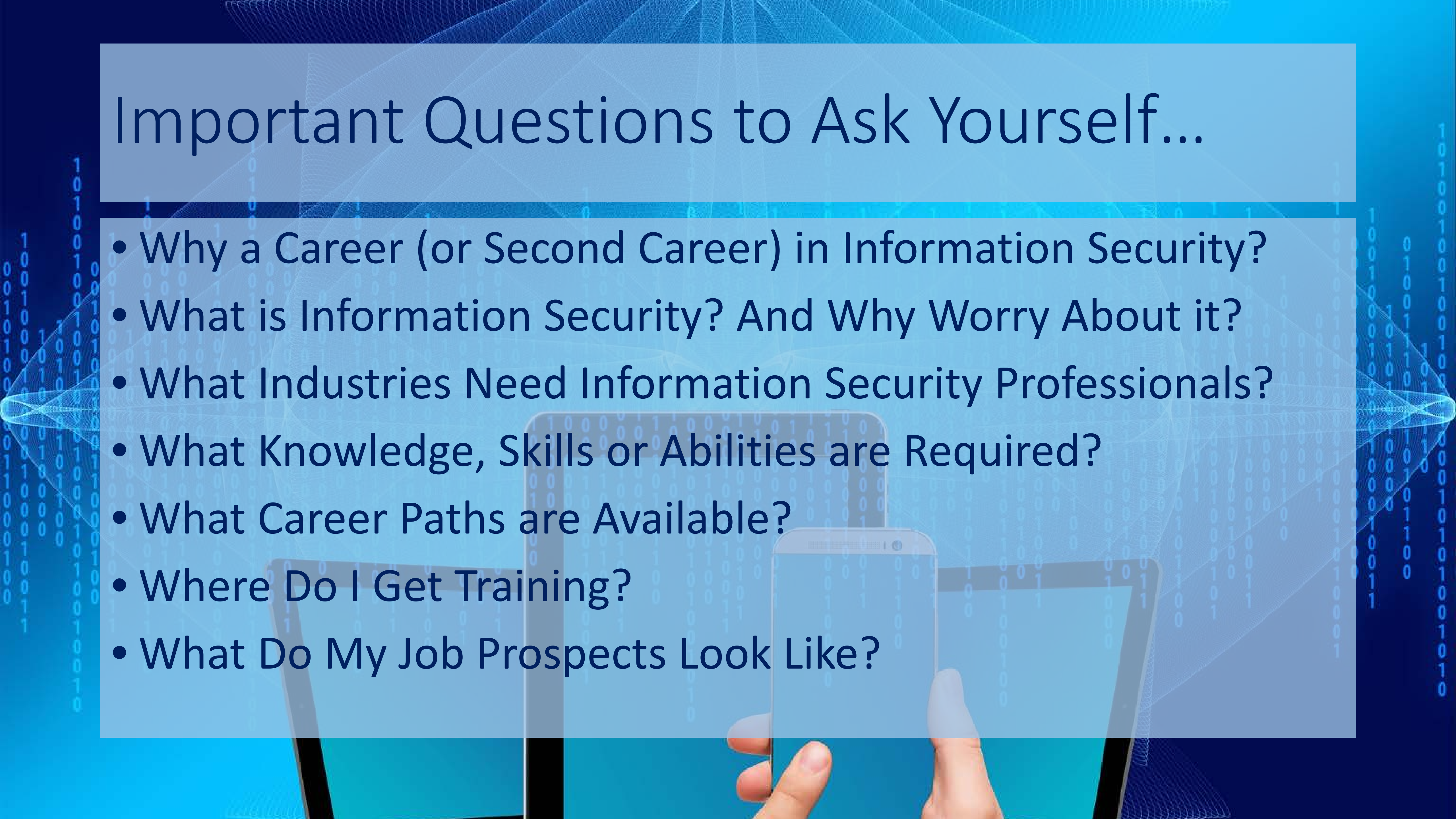


A Career in Information Security

Protect Your Future While Protecting the World

Presented by Scot A. DeWerth, CISSP

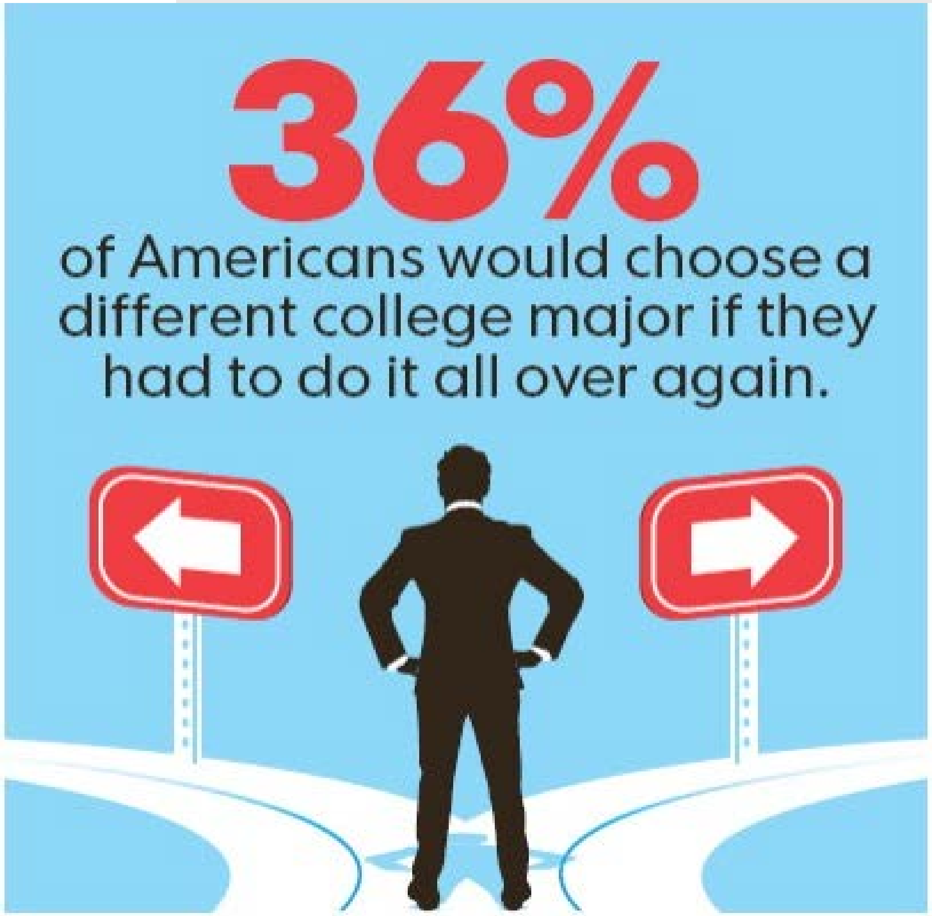
- Over 3.7 billion people worldwide are connected to the internet (with over 2 billion on Facebook alone!)
- Using over 6.4 to 17.6 billion internet connected devices
- Creating 2.5 quintillion bytes of data daily (2.5 x10^18 or 1 million trillion)
- Stored in data centers which have been breach over 7500 times since 2005
- By one of over 390,000 new malware variants created each day
- Revealing over 912 million account records to unauthorized users and cybercriminals
- Resulting in over 2 million cases of identity theft from fraudulent use of stolen account information (2013)
- Causing financial losses due to cybercrime of over $3 trillion dollars (2015)



Important Questions to Ask Yourself…

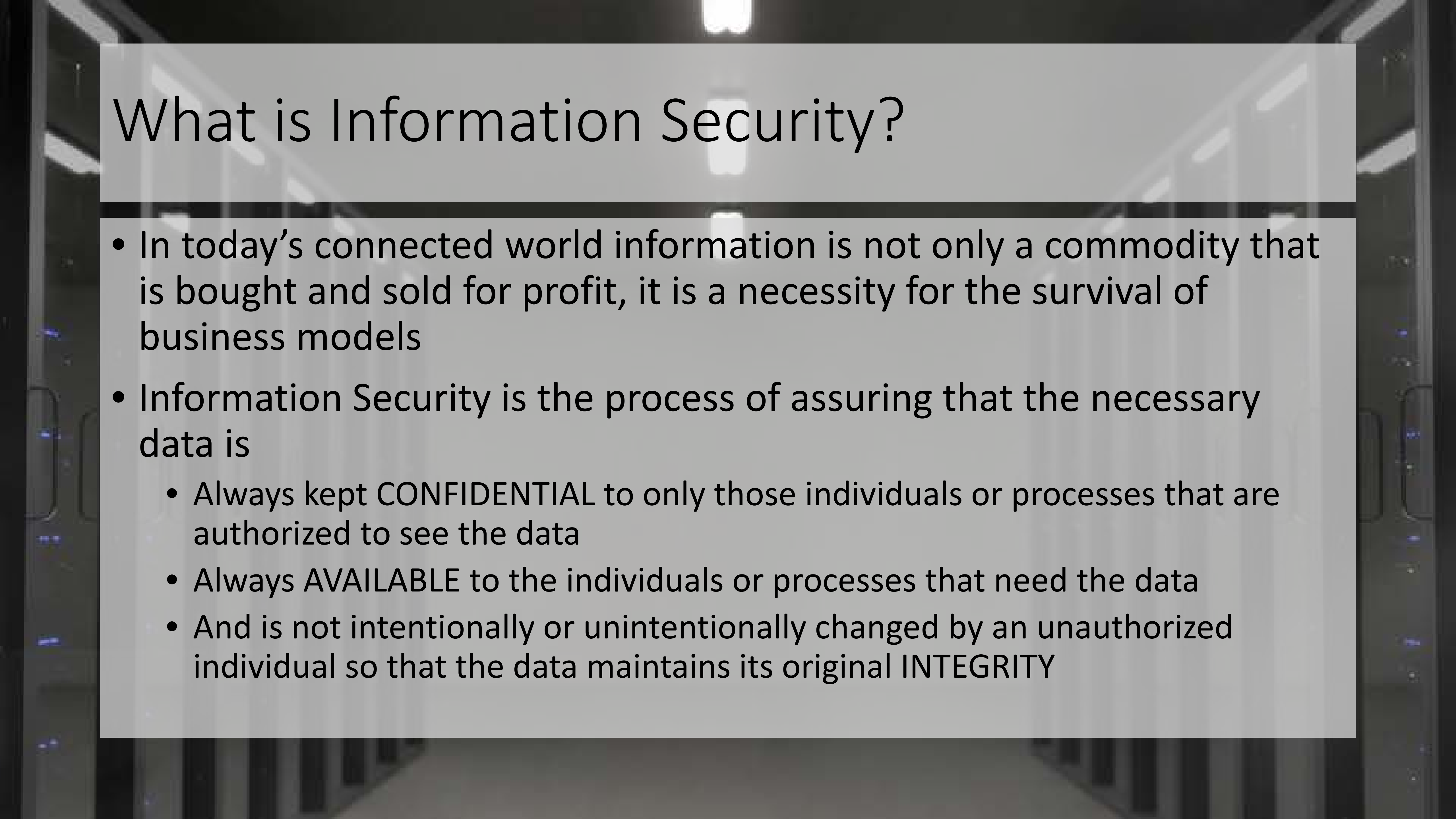
- Why a Career (or Second Career) in Information Security?
- What is Information Security? And Why Worry About it?
- What Industries Need Information Security Professionals?
- What Knowledge, Skills or Abilities are Required?
- What Career Paths are Available?
- Where Do I Get Training?
- What Do My Job Prospects Look Like?

Why A Career in Information Security?


36%
of Americans would choose a different college major if they had to do it all over again.

USA Today Gallup Strada

- It’s a growth industry – projected job growth of 18% thru 2024, with 50% of the jobs in the U.S. unfilled.
- STEM (Science, Technology, Engineering and Mathematics), Health and business majors are the highest paying annual wages with top paying college majors earning $3.4 million more over a lifetime.
- It is a transportable skill across industries and across localities.
- It is an evolving field and people that thrive on learning new skills, solving hard problems and implementing real solutions are perfect matches for this career.



What is Information Security?

- In today's connected world information is not only a commodity that is bought and sold for profit, it is a necessity for the survival of business models
- Information Security is the process of assuring that the necessary data is
  - Always kept CONFIDENTIAL to only those individuals or processes that are authorized to see the data
  - Always AVAILABLE to the individuals or processes that need the data
  - And is not intentionally or unintentionally changed by an unauthorized individual so that the data maintains its original INTEGRITY

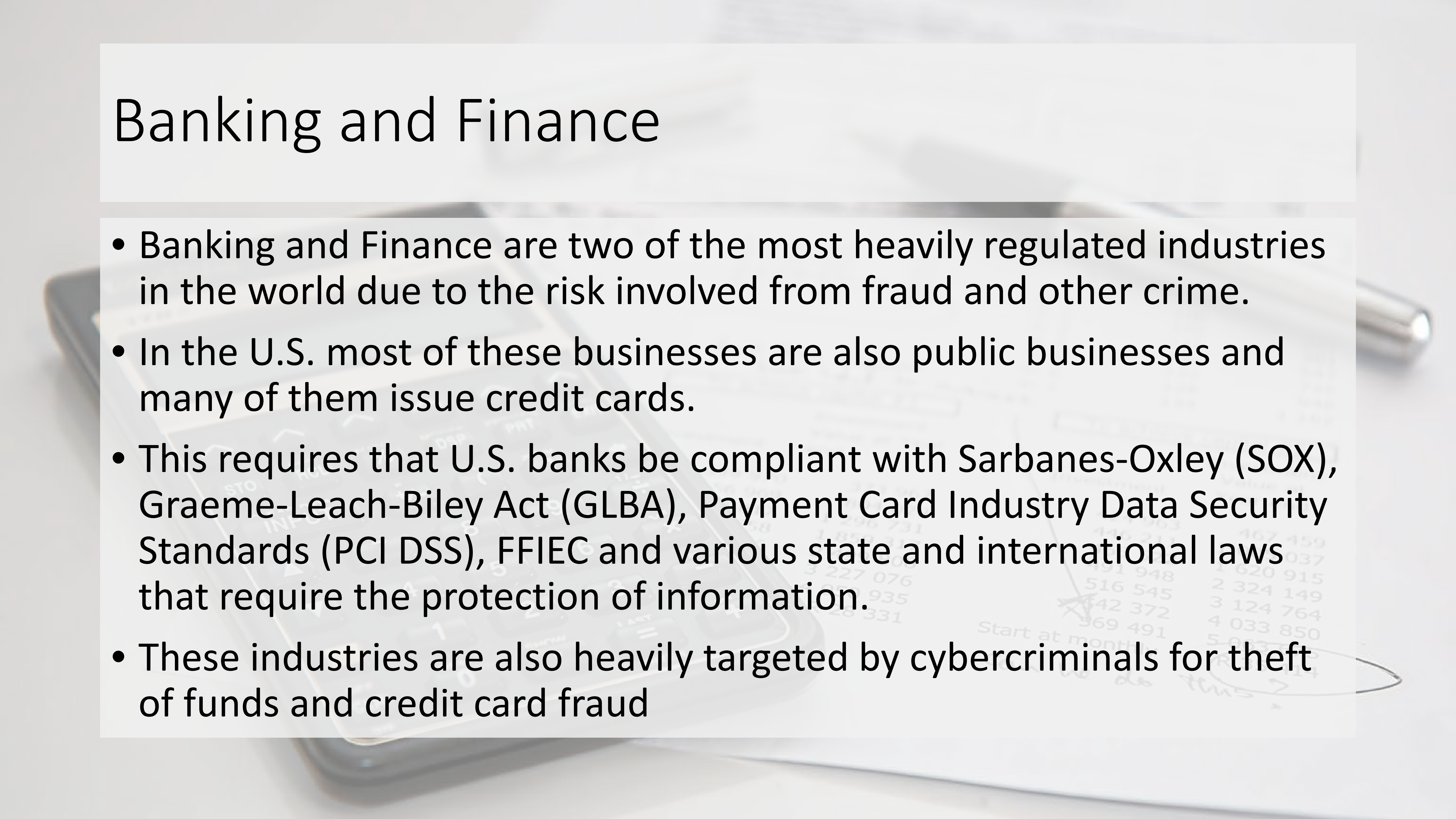
Why Worry About Information Security?

- Cybercrime is a growing problem on the internet.
- Criminals are collecting and aggregating data to make full digital identities for sale to perpetrate fraud. Over $3B in crime was committed last year.
- Regulatory Risk – many governments and some private regulatory organizations have established substantial fines for poor information security practices by organizations.
- Reputation Risk – customers will potential leave due to a breach.
- Loss of Intellectual Property and the value of the R&D efforts.

So What Industries Have a Need for Information Security Professionals?

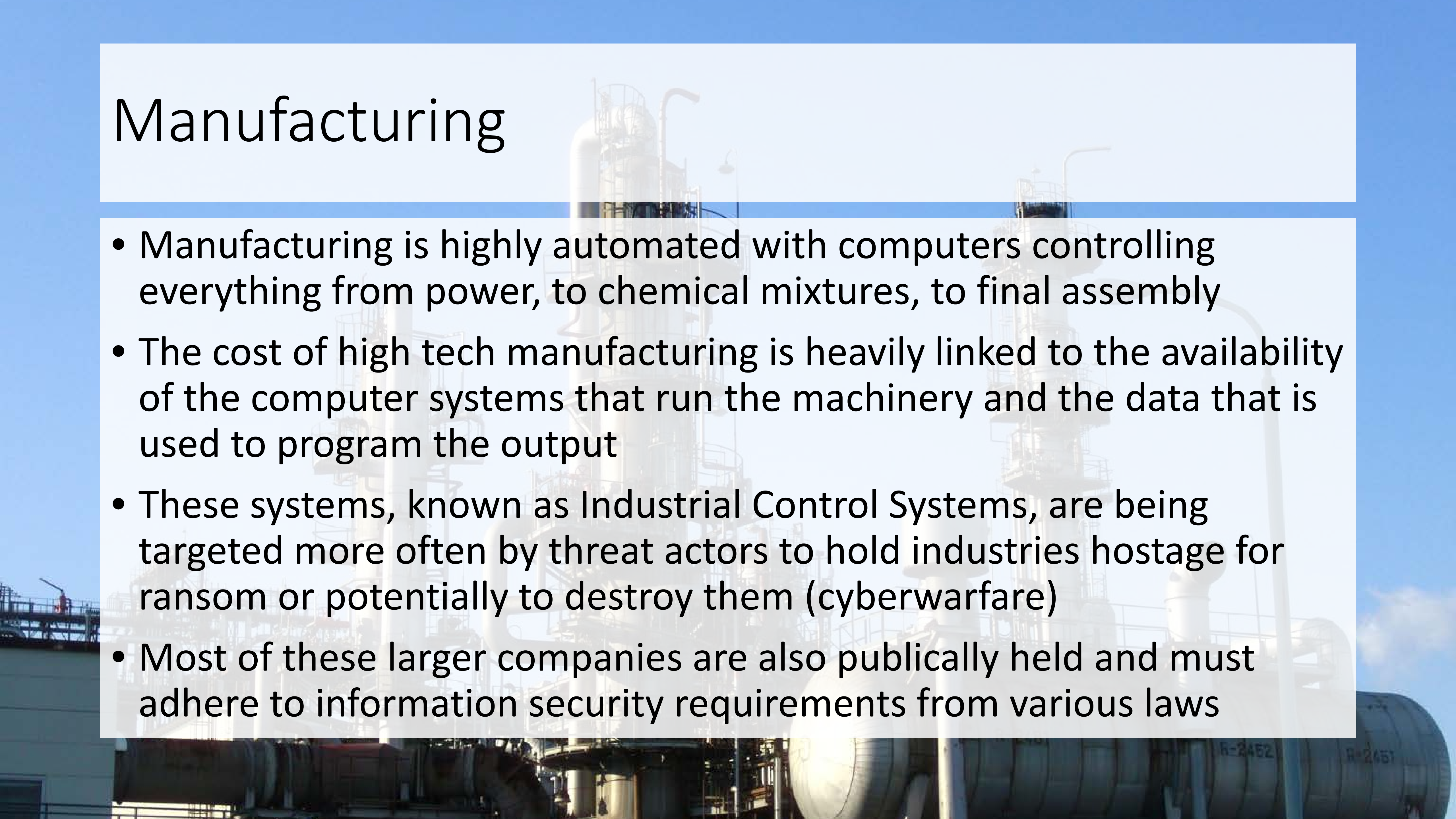
Healthcare

- Healthcare – contains a vast amount of privacy and financial data that must be protected by law and is wanted by criminals
- Healthcare data within the United States is protected by the Health Insurance Portability and Accountability Act of 1996
- This law requires that companies that have data on people’s health, protect it with sufficient Privacy and Security controls
- Failure to protect this data from criminals is harmful to the individual whose data was lost and can cost the company millions in fines
- This information is targeted for identity theft and theft of services



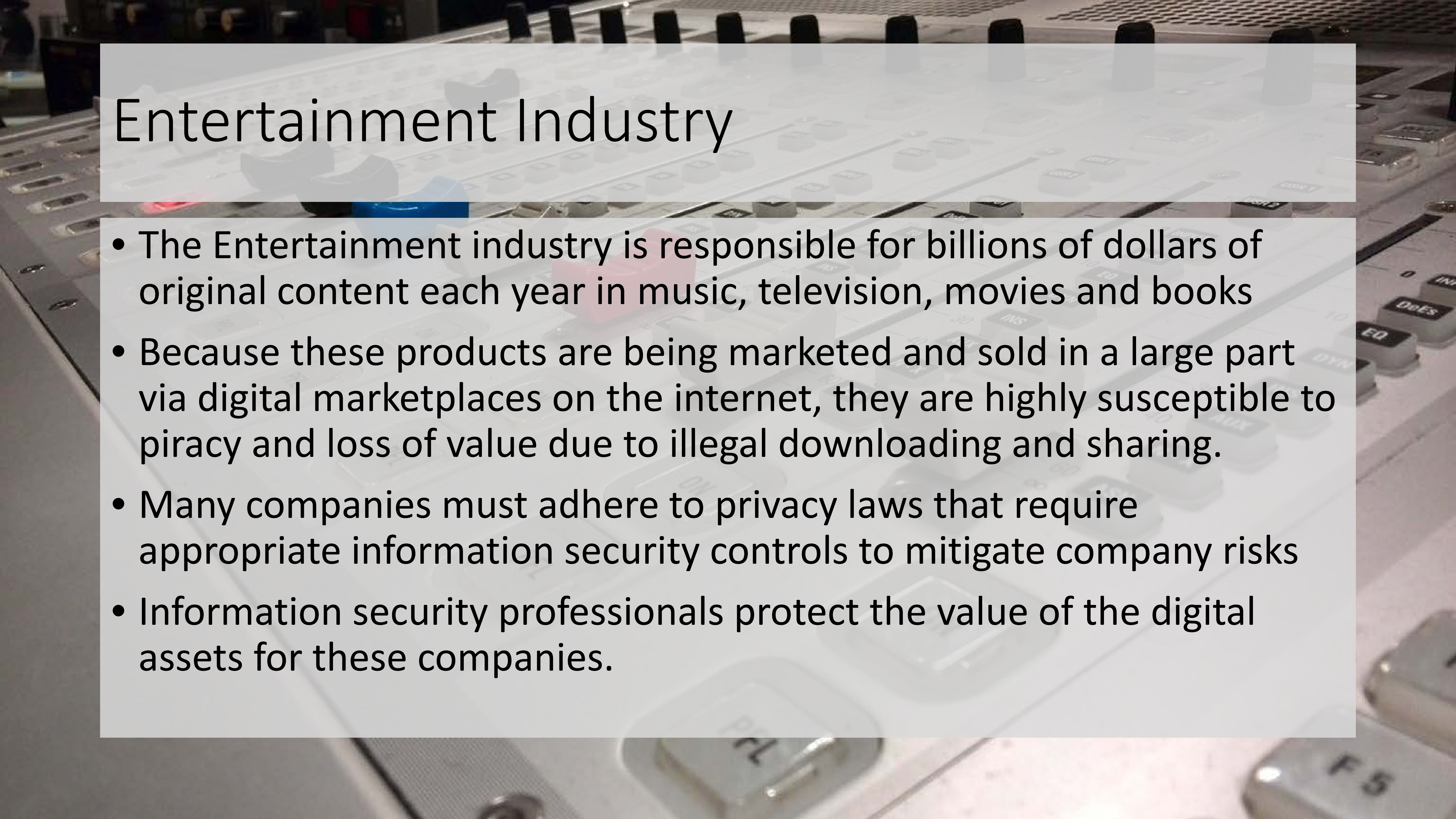
Banking and Finance

- Banking and Finance are two of the most heavily regulated industries in the world due to the risk involved from fraud and other crime.
- In the U.S. most of these businesses are also public businesses and many of them issue credit cards.
- This requires that U.S. banks be compliant with Sarbanes-Oxley (SOX), Graeme-Leach-Biley Act (GLBA), Payment Card Industry Data Security Standards (PCI DSS), FFIEC and various state and international laws that require the protection of information.
- These industries are also heavily targeted by cybercriminals for theft of funds and credit card fraud



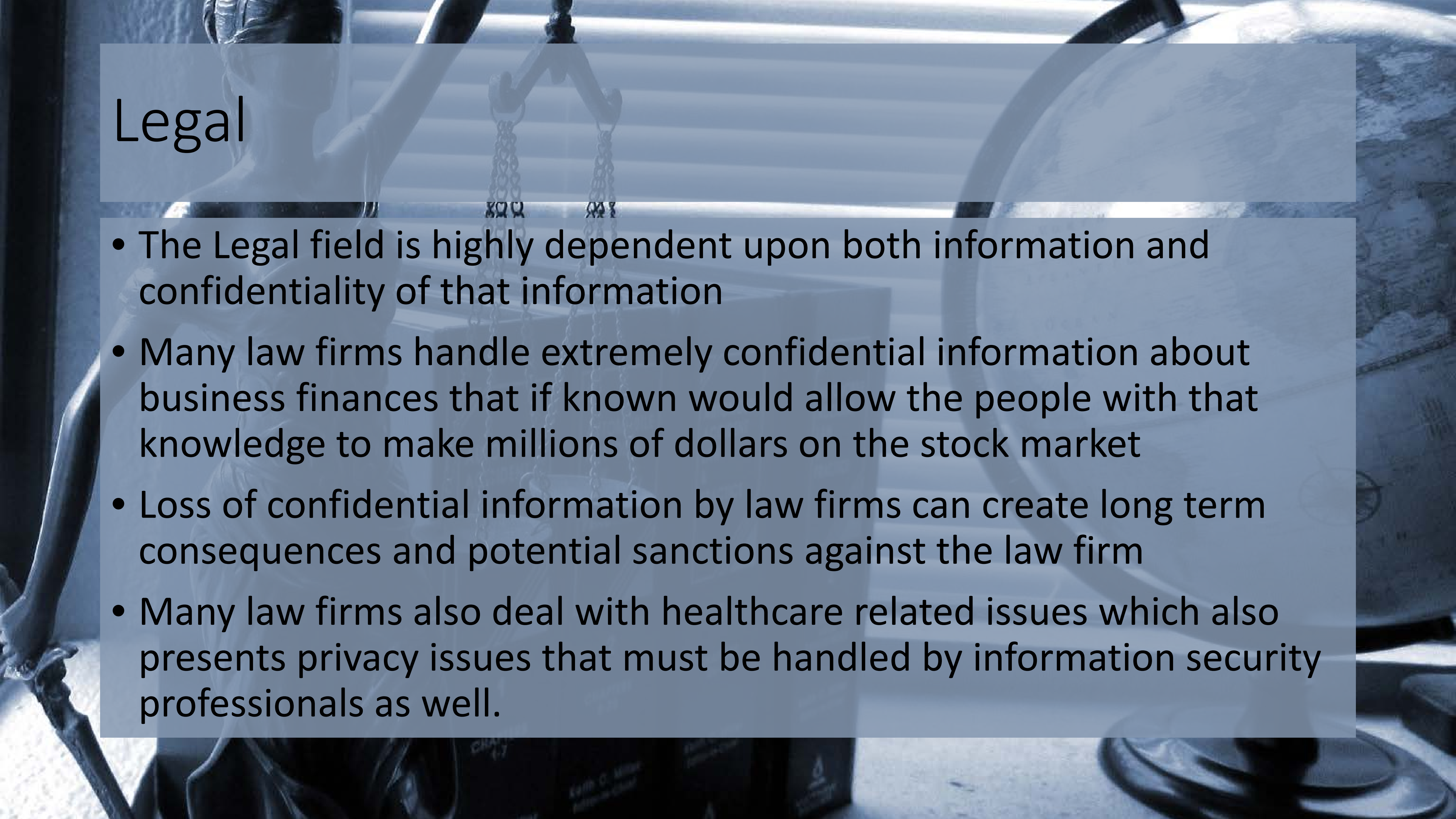
Manufacturing

- Manufacturing is highly automated with computers controlling everything from power, to chemical mixtures, to final assembly
- The cost of high tech manufacturing is heavily linked to the availability of the computer systems that run the machinery and the data that is used to program the output
- These systems, known as Industrial Control Systems, are being targeted more often by threat actors to hold industries hostage for ransom or potentially to destroy them (cyberwarfare)
- Most of these larger companies are also publically held and must adhere to information security requirements from various laws



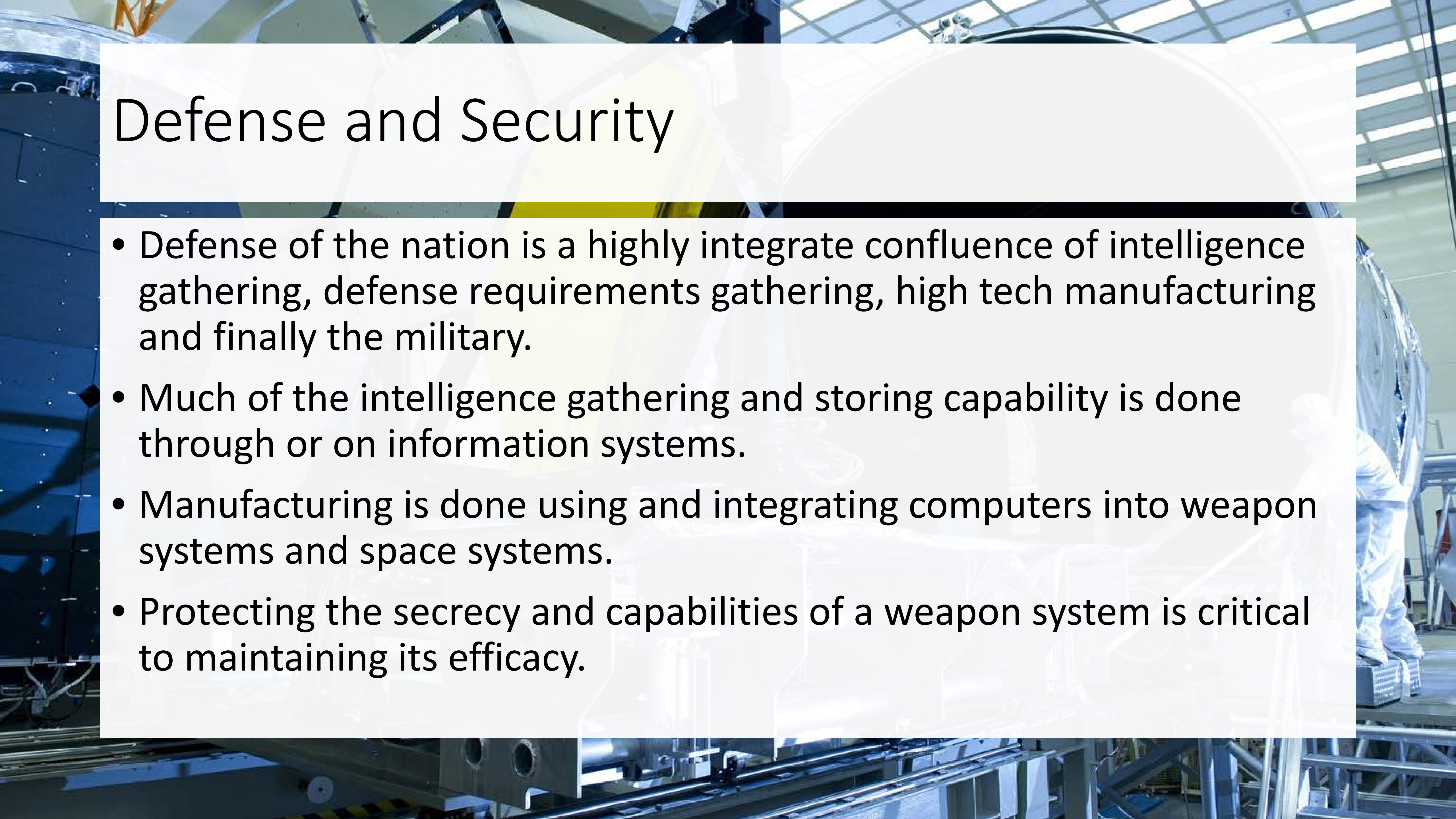
Entertainment Industry

- The Entertainment industry is responsible for billions of dollars of original content each year in music, television, movies and books
- Because these products are being marketed and sold in a large part via digital marketplaces on the internet, they are highly susceptible to piracy and loss of value due to illegal downloading and sharing.
- Many companies must adhere to privacy laws that require appropriate information security controls to mitigate company risks
- Information security professionals protect the value of the digital assets for these companies.



Legal

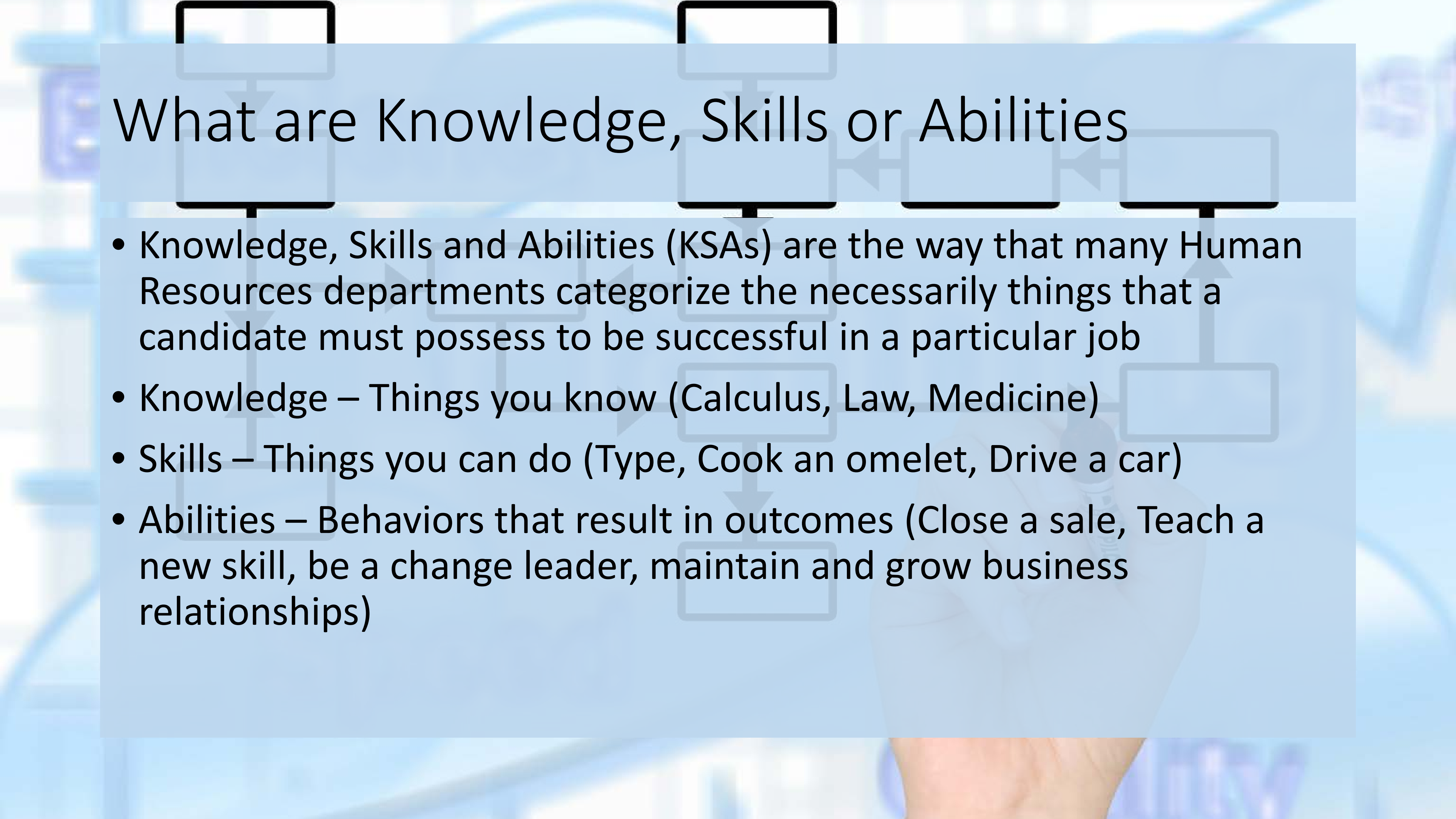
- The Legal field is highly dependent upon both information and confidentiality of that information
- Many law firms handle extremely confidential information about business finances that if known would allow the people with that knowledge to make millions of dollars on the stock market
- Loss of confidential information by law firms can create long term consequences and potential sanctions against the law firm
- Many law firms also deal with healthcare related issues which also presents privacy issues that must be handled by information security professionals as well.



Defense and Security

- Defense of the nation is a highly integrate confluence of intelligence gathering, defense requirements gathering, high tech manufacturing and finally the military.
- Much of the intelligence gathering and storing capability is done through or on information systems.
- Manufacturing is done using and integrating computers into weapon systems and space systems.
- Protecting the secrecy and capabilities of a weapon system is critical to maintaining its efficacy.

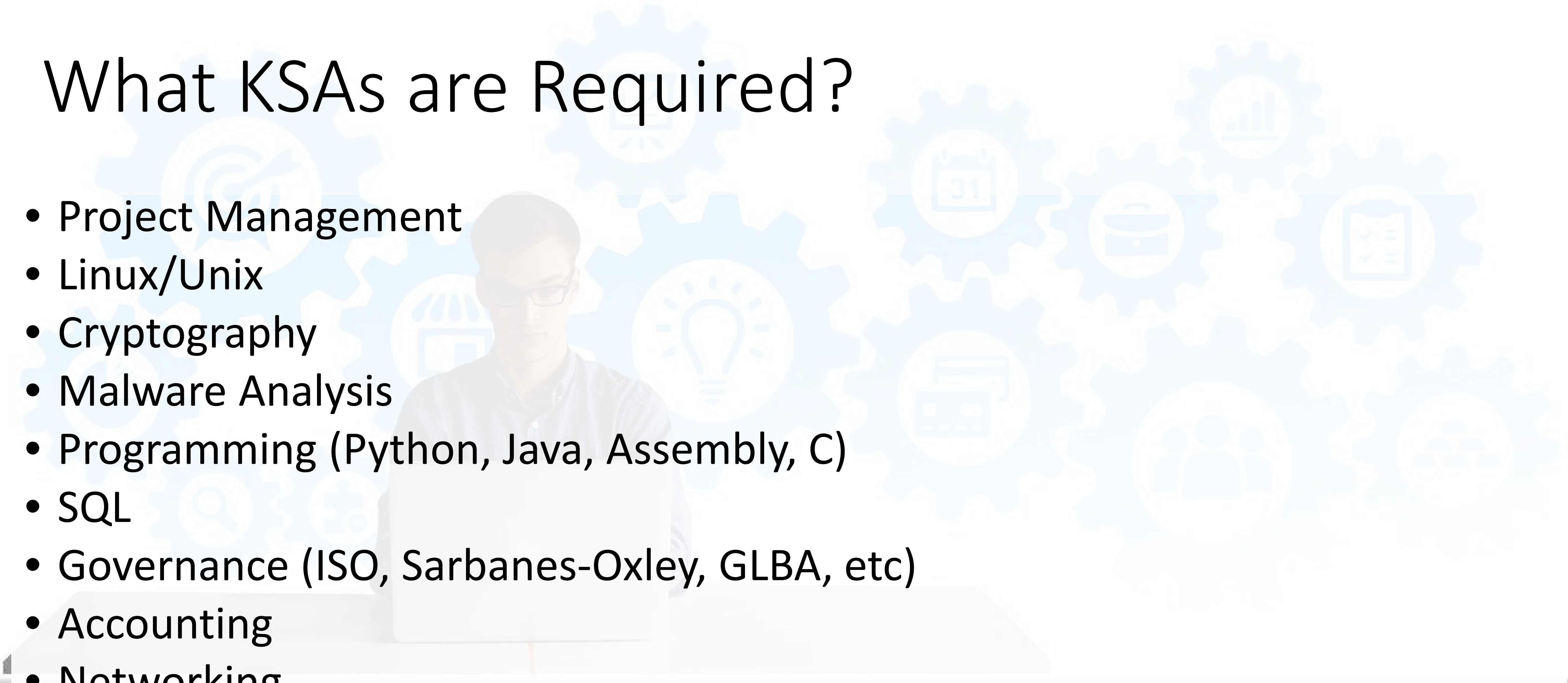
What do you need to be an Information Security Professional?



What are Knowledge, Skills or Abilities

- Knowledge, Skills and Abilities (KSAs) are the way that many Human Resources departments categorize the necessarily things that a candidate must possess to be successful in a particular job
- Knowledge – Things you know (Calculus, Law, Medicine)
- Skills – Things you can do (Type, Cook an omelet, Drive a car)
- Abilities – Behaviors that result in outcomes (Close a sale, Teach a new skill, be a change leader, maintain and grow business relationships)

What KSAs are Required?



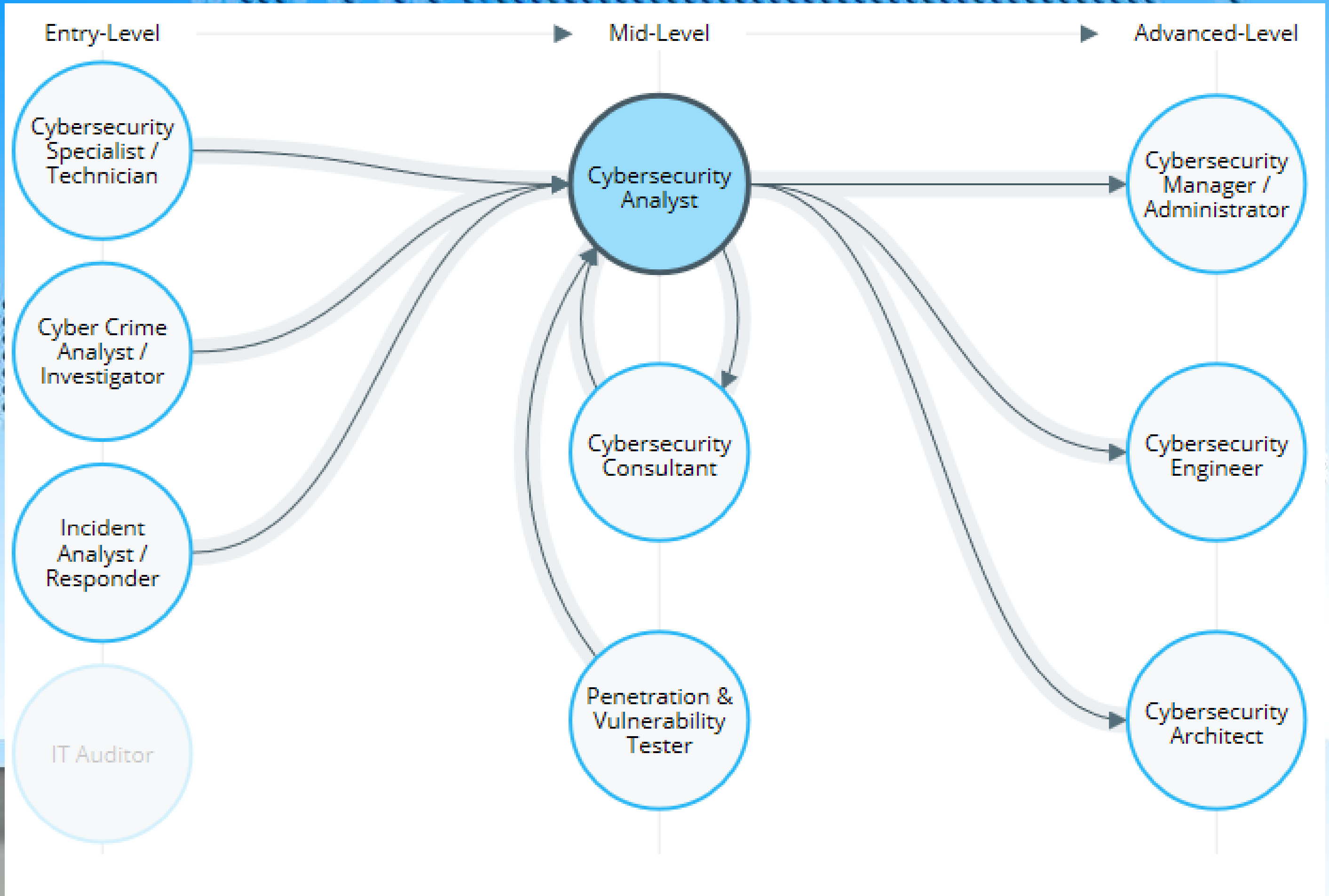
- Project Management
- Linux/Unix
- Cryptography
- Malware Analysis
- Programming (Python, Java, Assembly, C)
- SQL
- Governance (ISO, Sarbanes-Oxley, GLBA, etc)
- Accounting
- Networking
- Information Security certifications (CISSP, CISA, Security+)

What KSAs are Required?

- The National Initiative for Cybersecurity Careers and Studies defined a workforce framework to categorize information security specialty areas. These are:
  - Investigate
  - Operate and Maintain
  - Oversee and Govern
  - Analyze
  - Collect and Operate
  - Protect and Defend
  - Securely Provision

What Career Paths are Available?

- The National Initiative for Cybersecurity Education has defined potential career paths with an interactive tool
- http://cyberseek.org/pathway.html
- It shows expected career progression, required KSAs, average pay and number of job openings



Entry-Level
Mid-Level
Advanced-Level
Cybersecurity Specialist / Technician
Cyber Crime Analyst / Investigator
Incident Analyst / Responder
IT Auditor
Cybersecurity Analyst
Cybersecurity Consultant
Penetration & Vulnerability Tester
Cybersecurity Manager / Administrator
Cybersecurity Engineer
Cybersecurity Architect

Entry Level Careers

- IT Auditor
  - Understand governance (policies, laws, regulations) affecting enterprise information systems and their data.
  - Develops a plan to audit process and system compliance with internal requirements to meet governance objectives.
  - Regularly conducts audits of systems and processes against audit plan and presents findings to internal management.
  - Typically needs a Bachelor’s degree and security certifications.
  - This falls under the SECURELY PROVISION and the OVERSEE AND GOVERN categories of the NICE Cybersecurity Workforce Framework.

Entry Level Careers

- Incident Analyst/Responder
  - Responds to real or probable Information security incidents within the network, including malware, loss of data, outside network intrusions. Investigates evidence of incident.
  - Determines course of action to stop incident and recover from the potential damage caused by the incident.
  - Documents the incident for auditors and senior leadership and helps determine course of action to prevent incident in the future.
  - Typically needs a Bachelor’s degree and security certifications.
  - This falls under the PROTECT AND DEFEND category of the NICE Cybersecurity Workforce Framework.

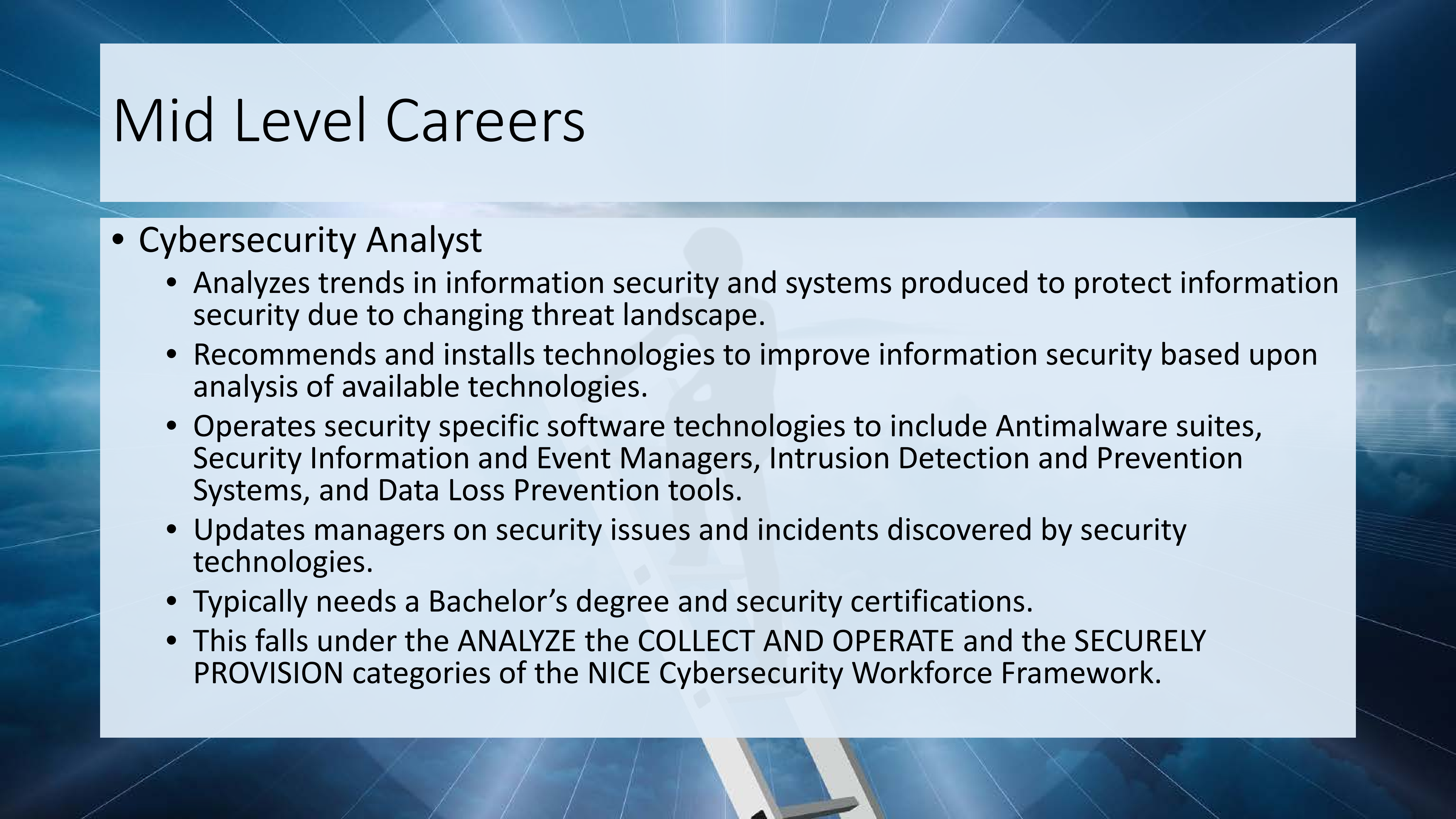
Entry Level Careers

- Cybercrime Analyst/Investigator
  - Investigates computer systems, mobile devices and software systems using digital forensics of hardware and software.
  - Uses proper handling of evidence to maintain legally viable chain of custody. Testifies in court cases and depositions about evidentiary findings and techniques used.
  - Requires deep understanding of platform security, software security and system security.
  - Typically needs a Bachelor’s degree and security certifications.
  - This falls under the INVESTIGATE category of the NICE Cybersecurity Workforce Framework.

Entry Level Careers

- Cybersecurity Specialist/Technician
  - Understands security requirements as defined by enterprise policy and industry best practice.
  - Implements policies into systems and software.
  - Operates security specific software technologies to include Antimalware suites, Security Information and Event Managers, Intrusion Detection and Prevention Systems, and Data Loss Prevention tools.
  - Updates managers on security issues and incidents discovered by security technologies.
  - Typically needs a Bachelor’s degree and security certifications.
  - This falls under the PROTECT AND DEFEND and the OPERATE AND MAINTAIN categories of the NICE Cybersecurity Workforce Framework.

Mid Level Careers



- Cybersecurity Analyst
  - Analyzes trends in information security and systems produced to protect information security due to changing threat landscape.
  - Recommends and installs technologies to improve information security based upon analysis of available technologies.
  - Operates security specific software technologies to include Antimalware suites, Security Information and Event Managers, Intrusion Detection and Prevention Systems, and Data Loss Prevention tools.
  - Updates managers on security issues and incidents discovered by security technologies.
  - Typically needs a Bachelor’s degree and security certifications.
  - This falls under the ANALYZE the COLLECT AND OPERATE and the SECURELY PROVISION categories of the NICE Cybersecurity Workforce Framework.

Mid Level Careers

- Cybersecurity Consultant
  - Understands security requirements as defined by information security frameworks and legal requirements.
  - Recommends governance requirements to meet legal, regulatory and risk requirements of the policies into systems and software.
  - Recommends specific software technologies to include Antimalware suites, Security Information and Event Managers, Intrusion Detection/Prevention Systems, and Fata Loss Prevention tools to meet enterprise risk requirements.
  - Typically needs a Bachelor’s degree and security certifications.
  - This Job must understand all seven categories of the NICE Cybersecurity Workforce Framework.

Mid Level Careers

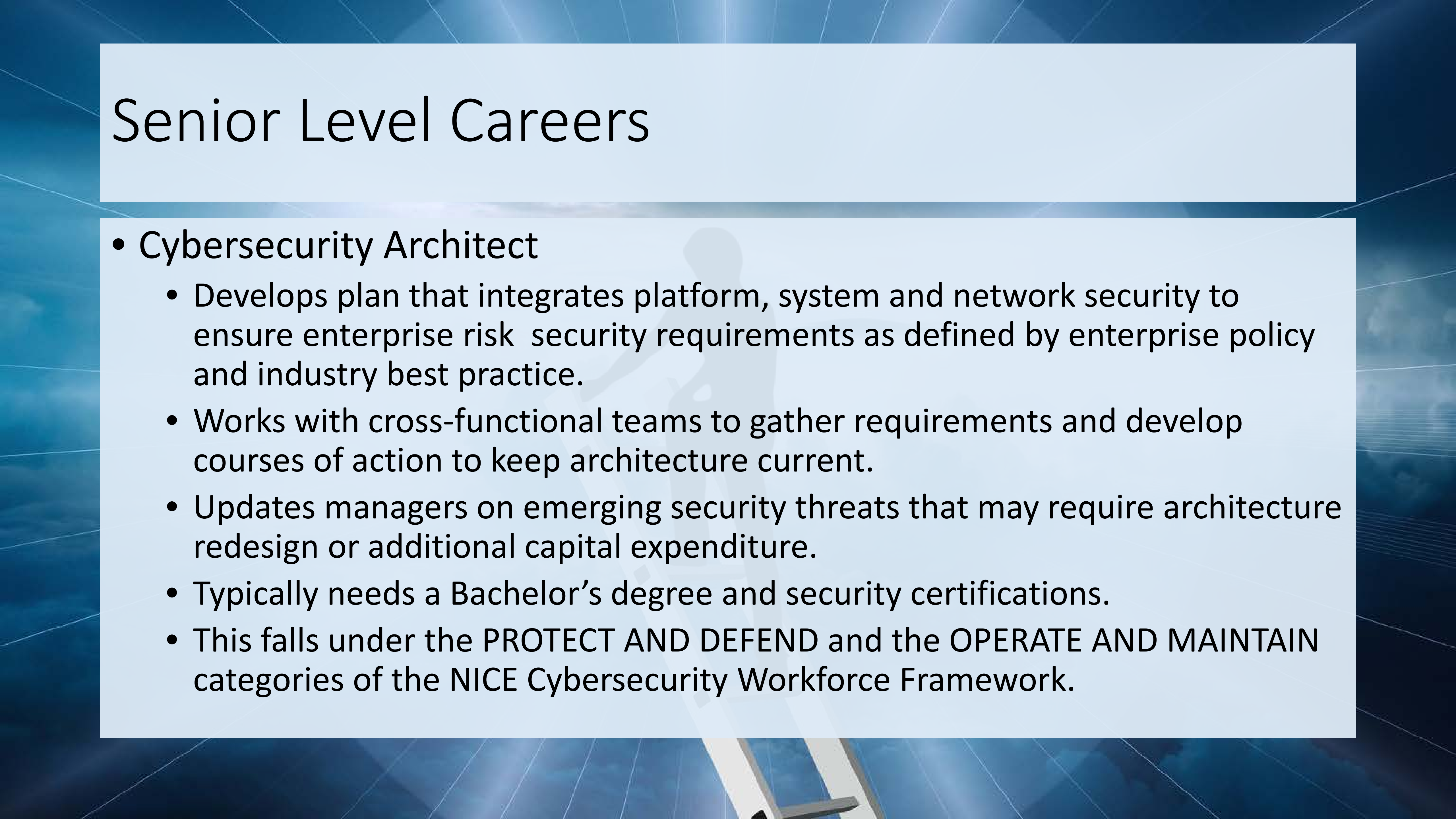
- Penetration and Vulnerability Tester
  - Understands system and platform engineering principles to find flaws in system and network security of an enterprise.
  - Utilizes specific information security tools to test and breach the security of an enterprise network.
  - Develops a comprehensive report on security findings that led to security intrusion and potential fixes that could alleviate issue.
  - Updates enterprise leadership on discovered security issues and the potential risk that they present.
  - Typically needs a Bachelor’s degree and security certifications.
  - This falls under the PROTECT AND DEFEND and the ANALYZE categories of the NICE Cybersecurity Workforce Framework.

Senior Level Careers

- Cybersecurity Manager/Administrator
  - Leads implementation of enterprise governance requirements.
  - Advocates with senior company leadership for funding and budgets for operations and updates to security controls.
  - Understands implications of audit findings and remediates issues with process, procedure or policy to meet governance requirements.
  - Leads team of entry-level and mid-level security professionals to manage enterprise information security program.
  - Typically needs a Bachelor’s degree and security certifications.
  - Works in all categories NICE Cybersecurity Workforce Framework except for INVESTIGATE.

Senior Level Careers

- Cybersecurity Engineer
  - Understands platform, system and network level security at the protocol level to be able to effectively design security solutions.
  - Builds new systems to meet information security needs of the enterprise.
  - Integrates and operates new information security technology in enterprise network to meet new threat requirements.
  - Updates managers on security issues and incidents discovered by security technologies.
  - Typically needs a Bachelor’s degree and security certifications.
  - This falls under the PROTECT AND DEFEND and the OPERATE AND MAINTAIN and SECURELY PROVISION categories of the NICE Cybersecurity Workforce Framework.



Senior Level Careers

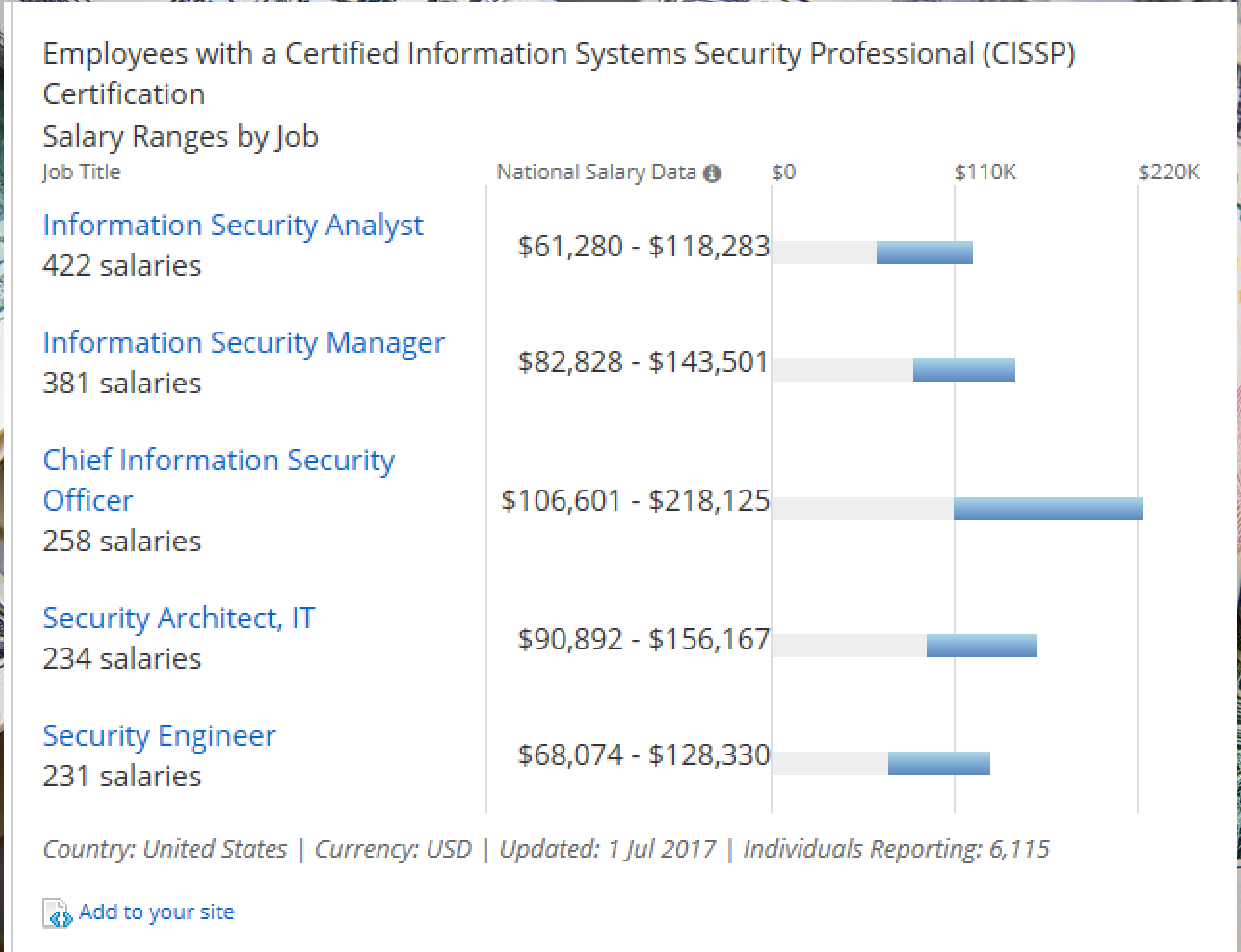
- Cybersecurity Architect
  - Develops plan that integrates platform, system and network security to ensure enterprise risk security requirements as defined by enterprise policy and industry best practice.
  - Works with cross-functional teams to gather requirements and develop courses of action to keep architecture current.
  - Updates managers on emerging security threats that may require architecture redesign or additional capital expenditure.
  - Typically needs a Bachelor’s degree and security certifications.
  - This falls under the PROTECT AND DEFEND and the OPERATE AND MAINTAIN categories of the NICE Cybersecurity Workforce Framework.

Certifications and Professional Organizations

- International Information System Security Certification Consortium
  - ISC(2) is a non-profit organization that specializes in information security training and certification. Their CISSP has become a de facto standard requirement for mid-level (>5 year) security practitioners.
- Information Systems Audit and Control Association (ISACA)
  - A non-profit membership based organization that provides high quality certifications for all phases of an information security career.
- SANS Institute
  - A For-profit organization, SANS certifies individuals under the Global Information Assurance Certification (GIAC) program in various specialties. GIAC certification are considered high quality due to the rigor of training required. SANS also has an online Masters Degree program.
- Computing Technology Industry Association (CompTIA)
  - A non-profit trade organization that issues professional accreditations in various information technology topics including security. Associated with more entry level certifications for entry level positions.

High Stakes Proctored Exams and Experience

- Information Security specific certifications are achieved through at a minimum, a high stakes in person or remotely proctored examination, with the stakes being from $265(CompTIA) to $1699(GIAC) for the cost of the certification attempt.
- Many certifications also have a requirement for verified time spent working within the particular field.
- Time requirements for selected certifications range from 2 years to 5 years. Many allow a substitution of 1 year experience for a college degree in an associated field.

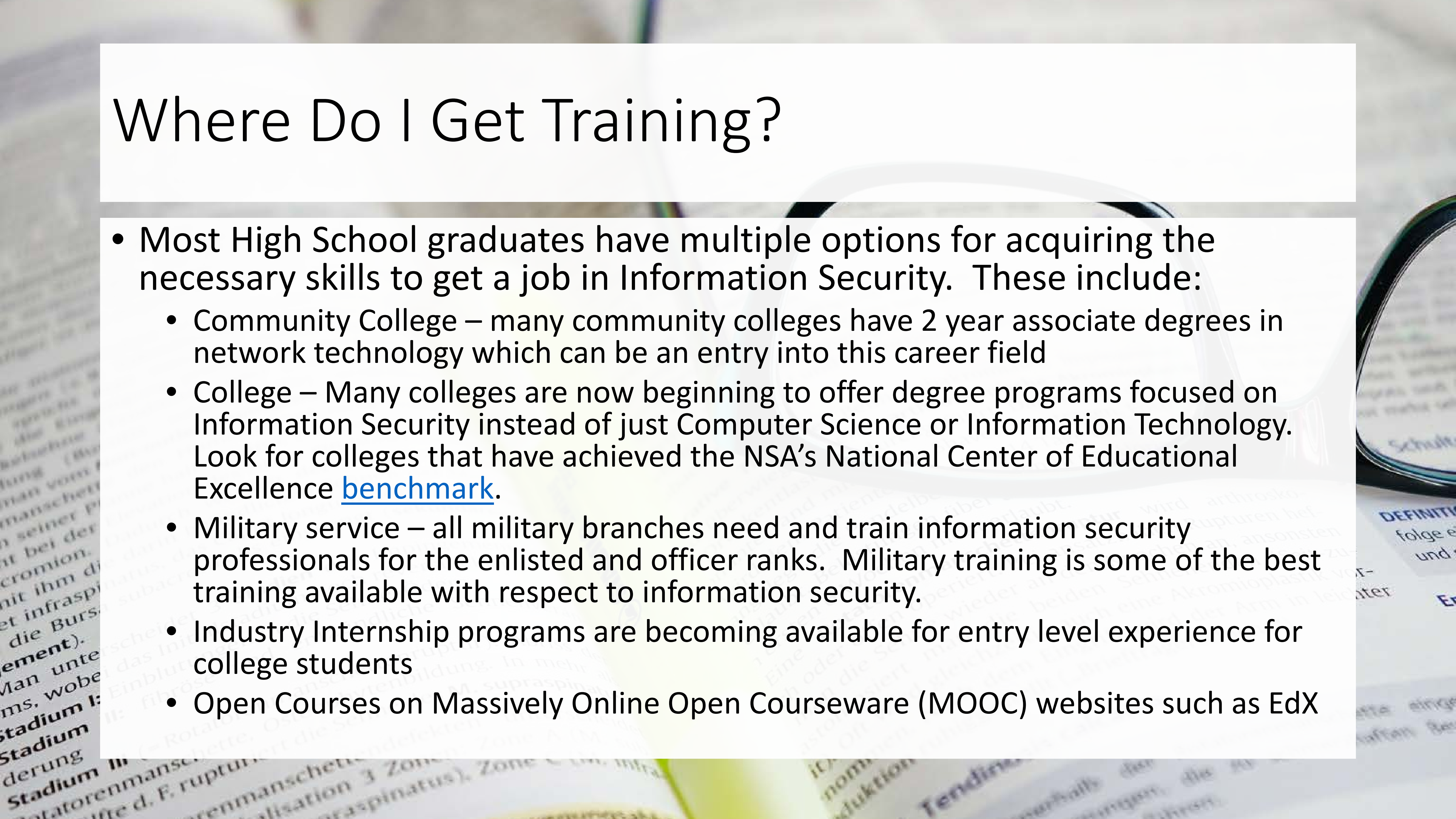


Employees with a Certified Information Systems Security Professional (CISSP) Certification

Salary Ranges by Job

Job Title	National Salary Data
Information Security Analyst 422 salaries	$61,280 - $118,283
Information Security Manager 381 salaries	$82,828 - $143,501
Chief Information Security Officer 258 salaries	$106,601 - $218,125
Security Architect, IT 234 salaries	$90,892 - $156,167
Security Engineer 231 salaries	$68,074 - $128,330

Country: United States | Currency: USD | Updated: 1 Jul 2017 | Individuals Reporting: 6,115



Where Do I Get Training?

- Most High School graduates have multiple options for acquiring the necessary skills to get a job in Information Security. These include:
  - Community College – many community colleges have 2 year associate degrees in network technology which can be an entry into this career field
  - College – Many colleges are now beginning to offer degree programs focused on Information Security instead of just Computer Science or Information Technology. Look for colleges that have achieved the NSA's National Center of Educational Excellence benchmark.
  - Military service – all military branches need and train information security professionals for the enlisted and officer ranks. Military training is some of the best training available with respect to information security.
  - Industry Internship programs are becoming available for entry level experience for college students
  - Open Courses on Massively Online Open Courseware (MOOC) websites such as EdX

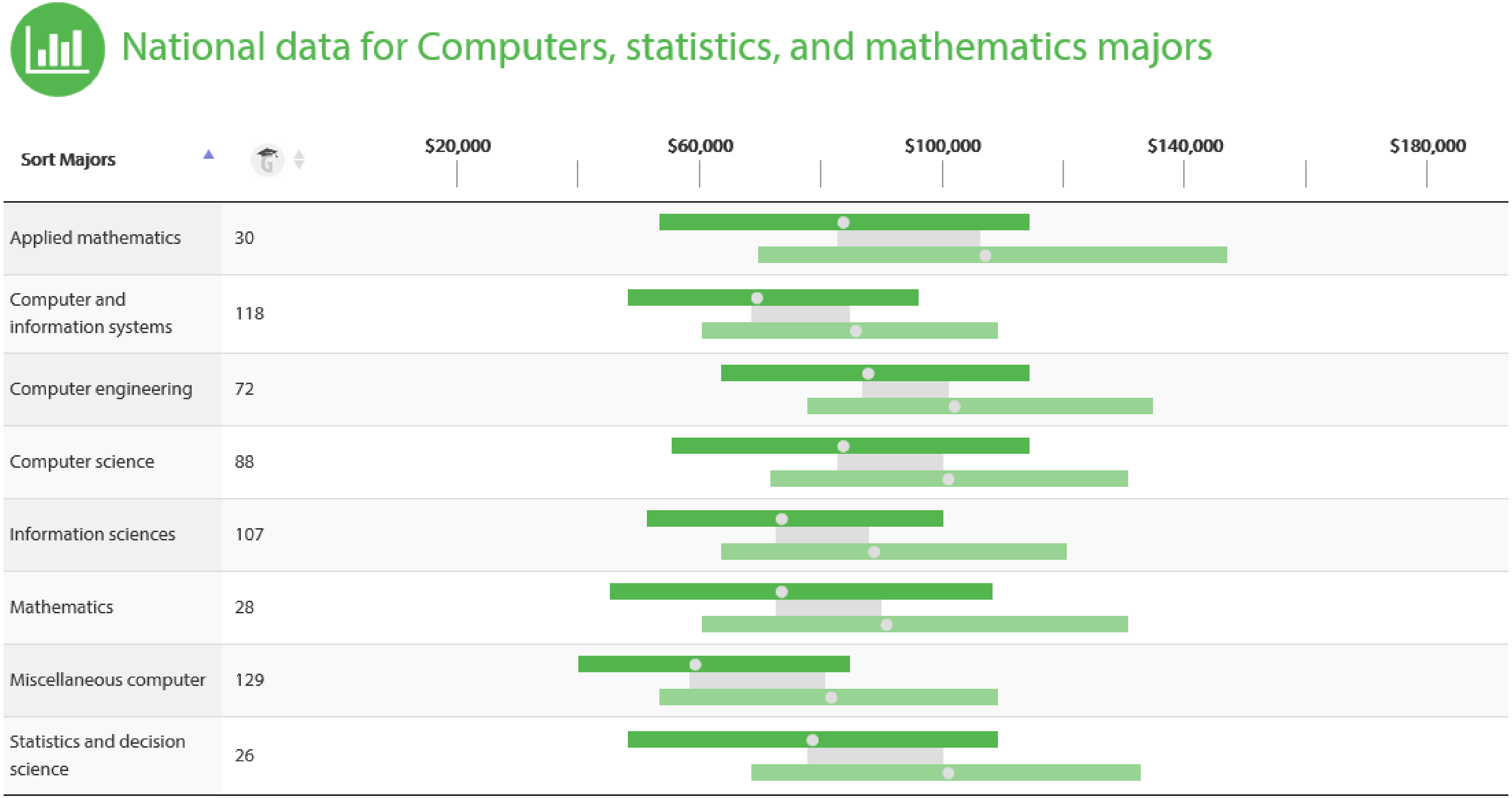
Where Do I Get Training?

- Internship Programs are a way to gain experience in a program while still learning the required skills
- Gallup employs Cybersecurity interns at the High School, Undergraduate and Graduate level
- Department of Homeland Security Internships
  - https://www.dhs.gov/homeland-security-careers/cybersecurity-internship-program-0
- Central Intelligence Agency
  - https://www.cia.gov/careers/student-opportunities/undergrad-info-assurance.html
- National Security Agency
  - https://www.intelligencecareers.gov/icstudents.html?Agency=NSA

Colleges with Cybersecurity Majors

- University of Nebraska – Omaha (NE)
- Bellevue University (NE)
- Iowa State University (IA)
- Georgetown University (DC)
- The George Washington University (DC)
- A full list of Centers of Academic Excellence for Cybersecurity can be found at
  - https://www.iad.gov/nietp/reports/current_cae_designated_institutions.cfm

College Outcomes for Computer Degrees

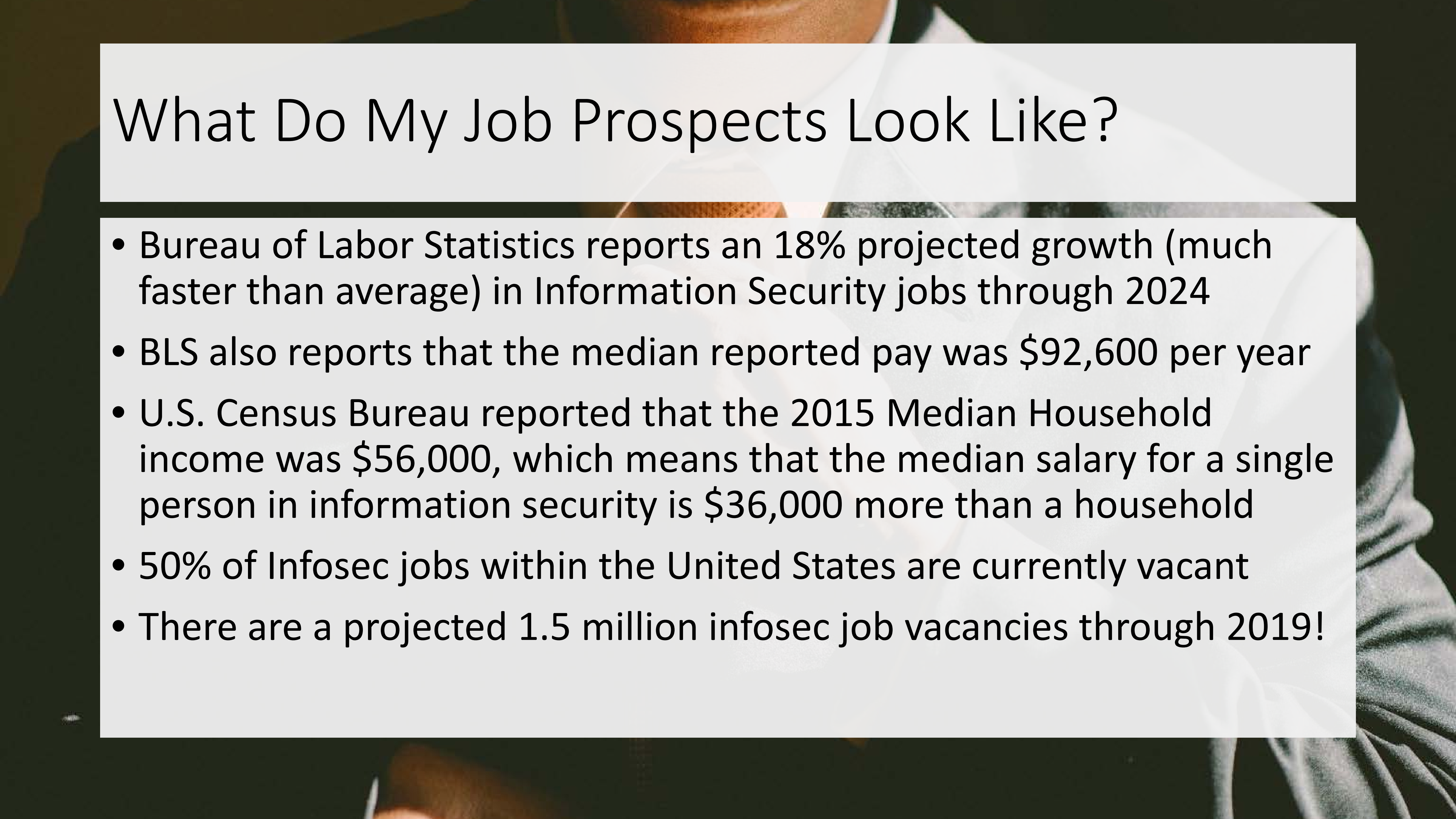


National data for Computers, statistics, and mathematics majors

Sort Majors ▲	
Applied mathematics	30
Computer and information systems	118
Computer engineering	72
Computer science	88
Information sciences	107
Mathematics	28
Miscellaneous computer	129
Statistics and decision science	26

Massive OnlineOpen Courseware (MOOC)

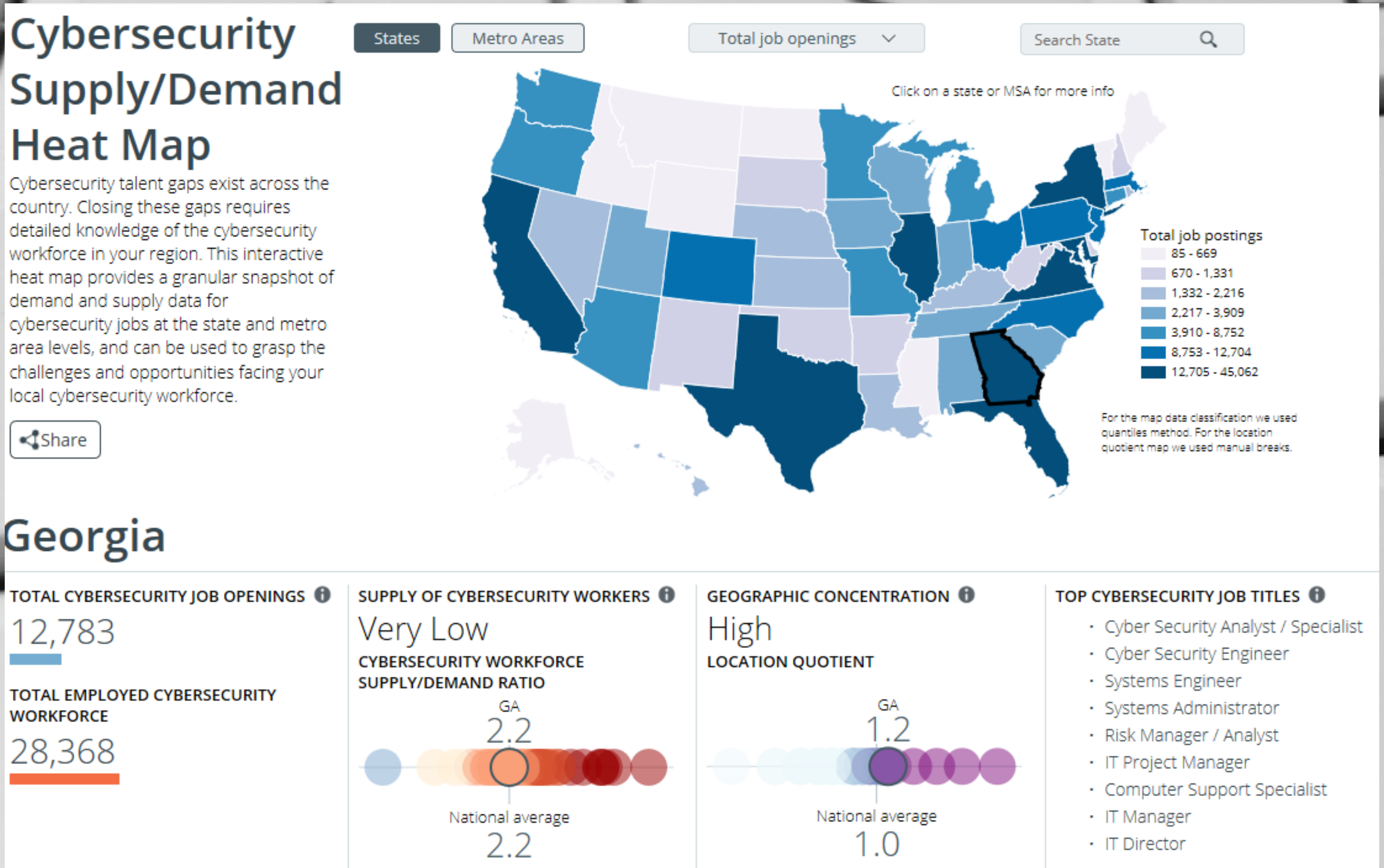
- Udemy
- LEAP - http://www.leapcourses.com/aboutus.php
- Coursera
- edX
- FutureLearn
- Udacity
- Carnegie Melon University Open Learning Initiative
- Cyber Security Base with F-Secure (Freely provided)



What Do My Job Prospects Look Like?

- Bureau of Labor Statistics reports an 18% projected growth (much faster than average) in Information Security jobs through 2024
- BLS also reports that the median reported pay was $92,600 per year
- U.S. Census Bureau reported that the 2015 Median Household income was $56,000, which means that the median salary for a single person in information security is $36,000 more than a household
- 50% of Infosec jobs within the United States are currently vacant
- There are a projected 1.5 million infosec job vacancies through 2019!

What Do My Job Prospects Look Like?



Cybersecurity Supply/Demand Heat Map

Cybersecurity talent gaps exist across the country. Closing these gaps requires detailed knowledge of the cybersecurity workforce in your region. This interactive heat map provides a granular snapshot of demand and supply data for cybersecurity jobs at the state and metro area levels, and can be used to grasp the challenges and opportunities facing your local cybersecurity workforce.

Total job postings

▢	85 - 669
▢	670 - 1,331
▢	1,332 - 2,216
▢	2,217 - 3,909
▢	3,910 - 8,752
▢	8,753 - 12,704
▢	12,705 - 45,062

For the map data classification we used quantiles method. For the location quotient map we used manual breaks.

Georgia

TOTAL CYBERSECURITY JOB OPENINGS

12,783

TOTAL EMPLOYED CYBERSECURITY WORKFORCE

28,368

SUPPLY OF CYBERSECURITY WORKERS

Very Low

CYBERSECURITY WORKFORCE SUPPLY/DEMAND RATIO

GEOGRAPHIC CONCENTRATION

High

LOCATION QUOTIENT

TOP CYBERSECURITY JOB TITLES

- Cyber Security Analyst / Specialist
- Cyber Security Engineer
- Systems Engineer
- Systems Administrator
- Risk Manager / Analyst
- IT Project Manager
- Computer Support Specialist
- IT Manager
- IT Director

- The National Institute for Cybersecurity Education commissioned a website to show where jobs are located and the types of jobs required.
- This website hosts an interactive Heat Map that shows the supply and demand of Cyber Security workforce
- This website can be accessed at http://cyberseek.org

- If you like the images selected for this presentation, please support Pixabay and their selection of Creative Commons licensed clip art, photographs and artwork.
  - WWW.PIXABAY.COM

Other Resources

- National Initiative for Cybersecurity Education
  - https://www.nist.gov/itl/applied-cybersecurity/nice
- National Initiative for Cybersecurity Careers and Studies
  - https://niccs.us-cert.gov/
  - If you are a Veteran or a federal government employee you are authorized free Cybersecurity training from the FedVTE
  - **https://fedvte.usalearning.gov/**
  - Veteran's can sigh up through the ID.me program on Hire our Heroes website.
- AWS Educate provides free cloud training to veterans and their spouses
  - https://aws.amazon.com/education/awseducate/veterans/