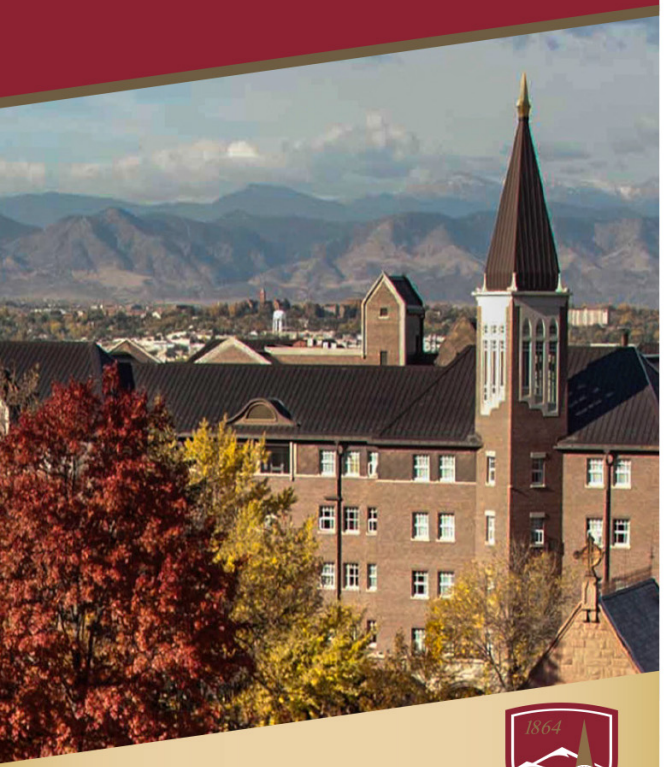
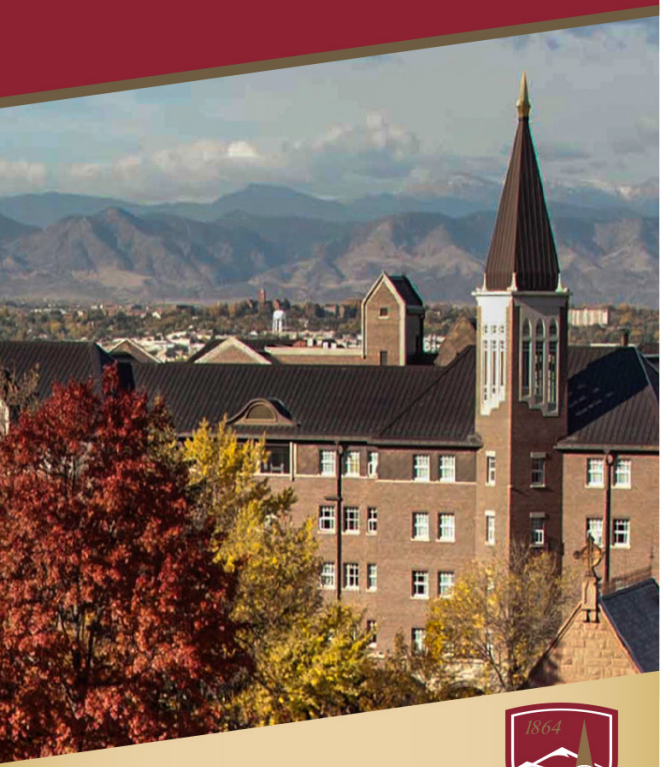
Cyber Security



A Career in Cybersecurity

Cyber Security



Your Presenter Today

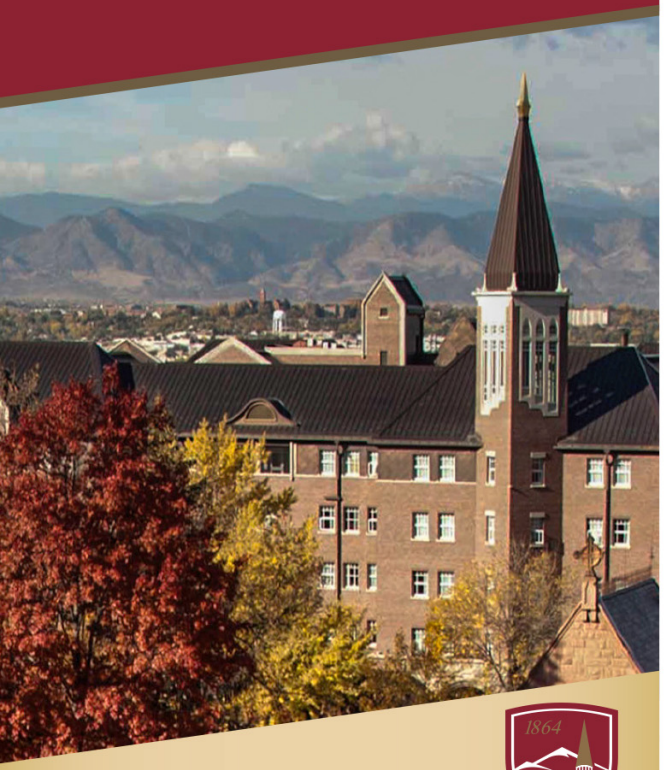
Richard Staynings

Chief Security Strategist, Cylera, Manhattan, New York

Chief Security Officer, Cyber Associates LLP

Adjunct Professor, University of Denver, University College

Cyber Security



Learning Objectives

This 60 minute interactive educational session is targeted at individuals in the 18 to 35 age group who may be considering a career in information technology, governance, compliance , or cybersecurity. It is anticipated that attendees will possess some information technology knowledge, as well as basic concepts of information security governance and compliance.

Educational Objectives

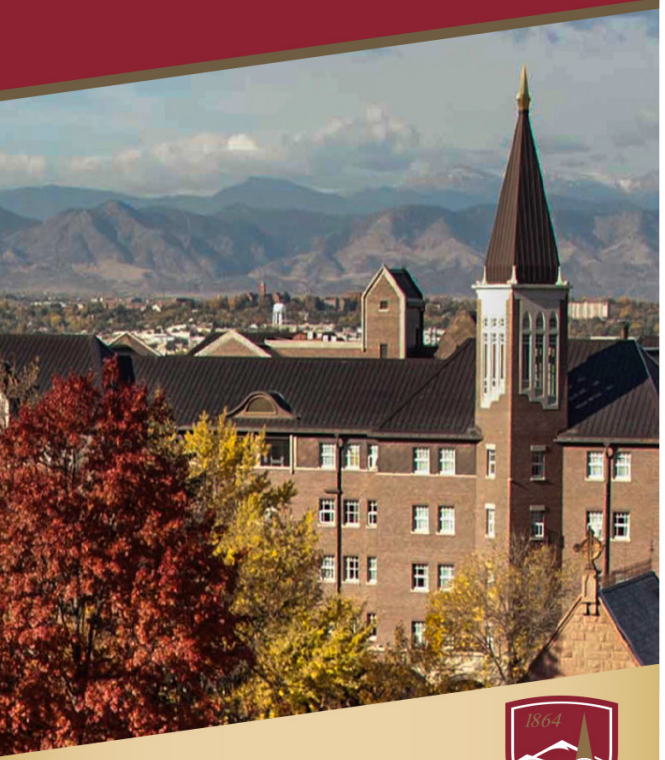
The following educational objectives have been established for the activity and will be used as a benchmark for judging the success of the endeavor.

Upon completion of the activity, participants should be better able to:

- **Explain the three main pillars of cybersecurity and how each is important in its own regard.**
- **Understand who are the main perpetrators of cyber crime and what their motivations are.**
- **Explain why cybersecurity is so important in our hyper-connected world today.**
- **Describe, evaluate, and potentially apply, one of the security frameworks to protecting all of us from cyber attack.**
- **Understand the various roles in cybersecurity and what career opportunities exist for those willing to take the challenge.**

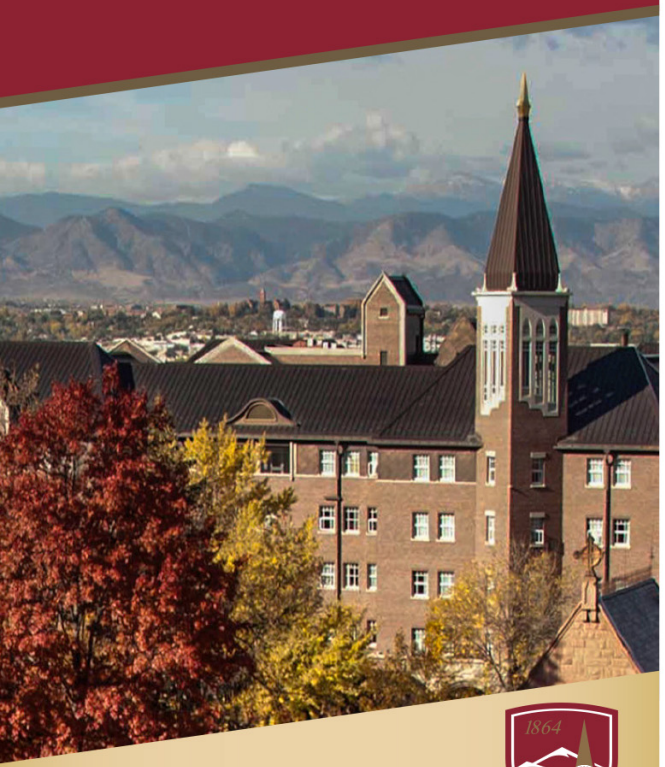

admin
*****
Cybersecurity

Cyber Security



What is Cybersecurity?

Cyber Security



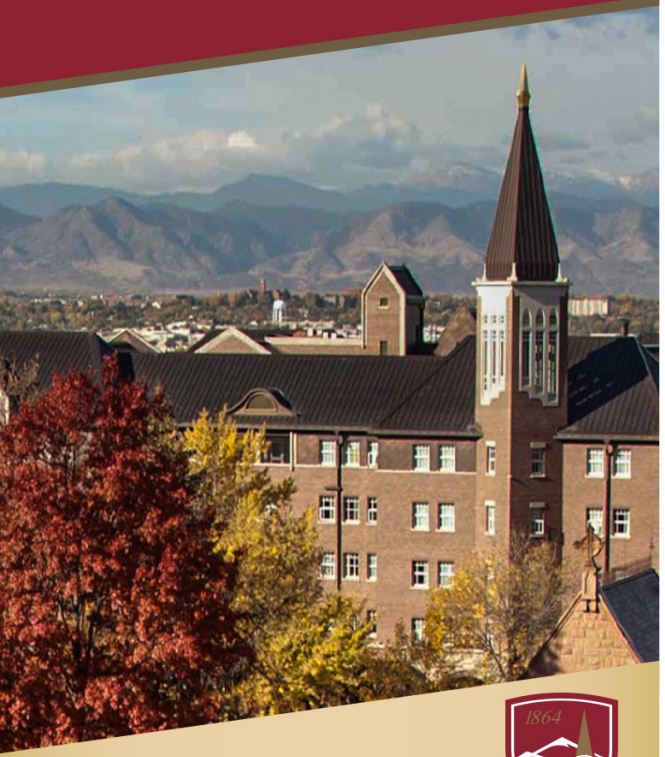
According to NIST

(National Institute of Standards and Technology)

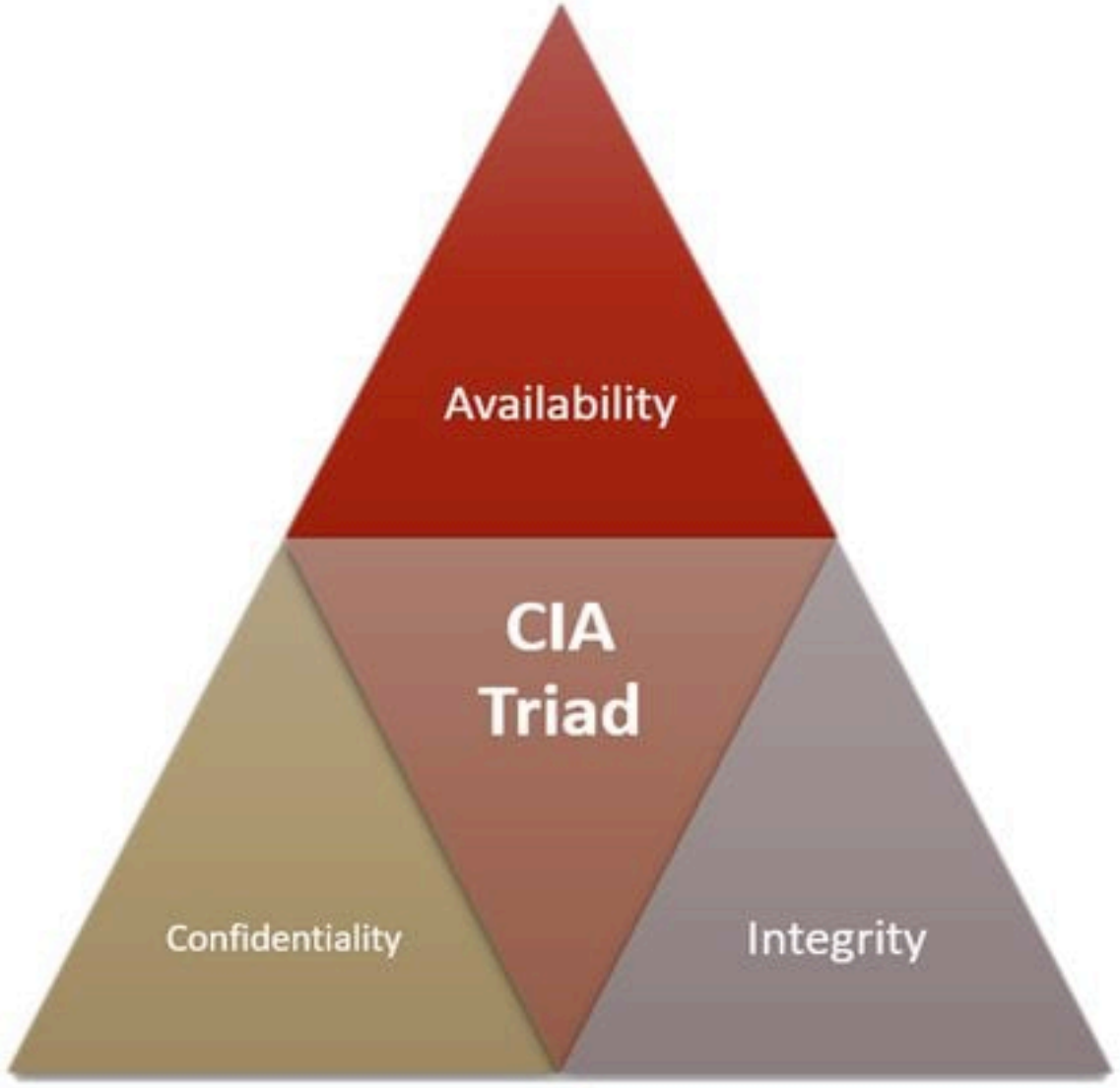
Cybersecurity is the ‘Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.’

NIST SP 800-37 Rev. 2

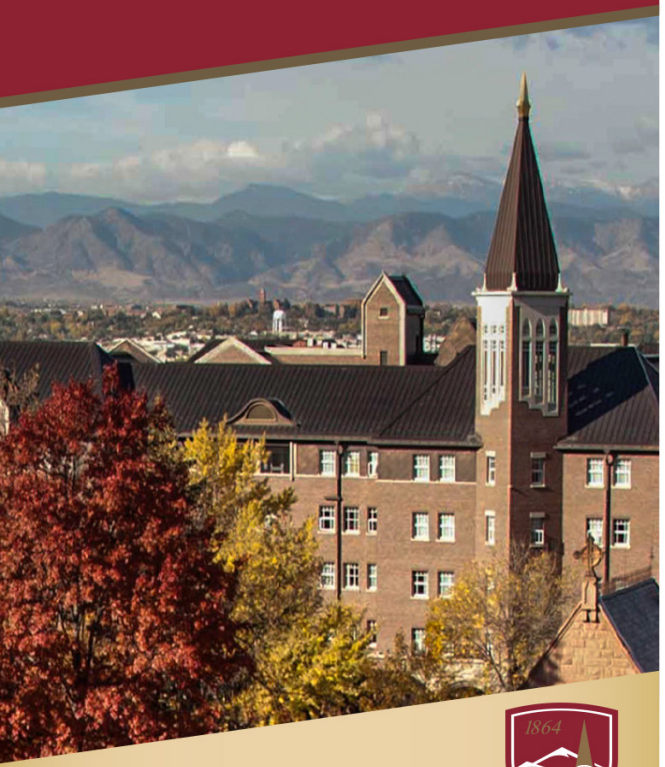
Cyber Security



What does it encompass?



Cyber Security



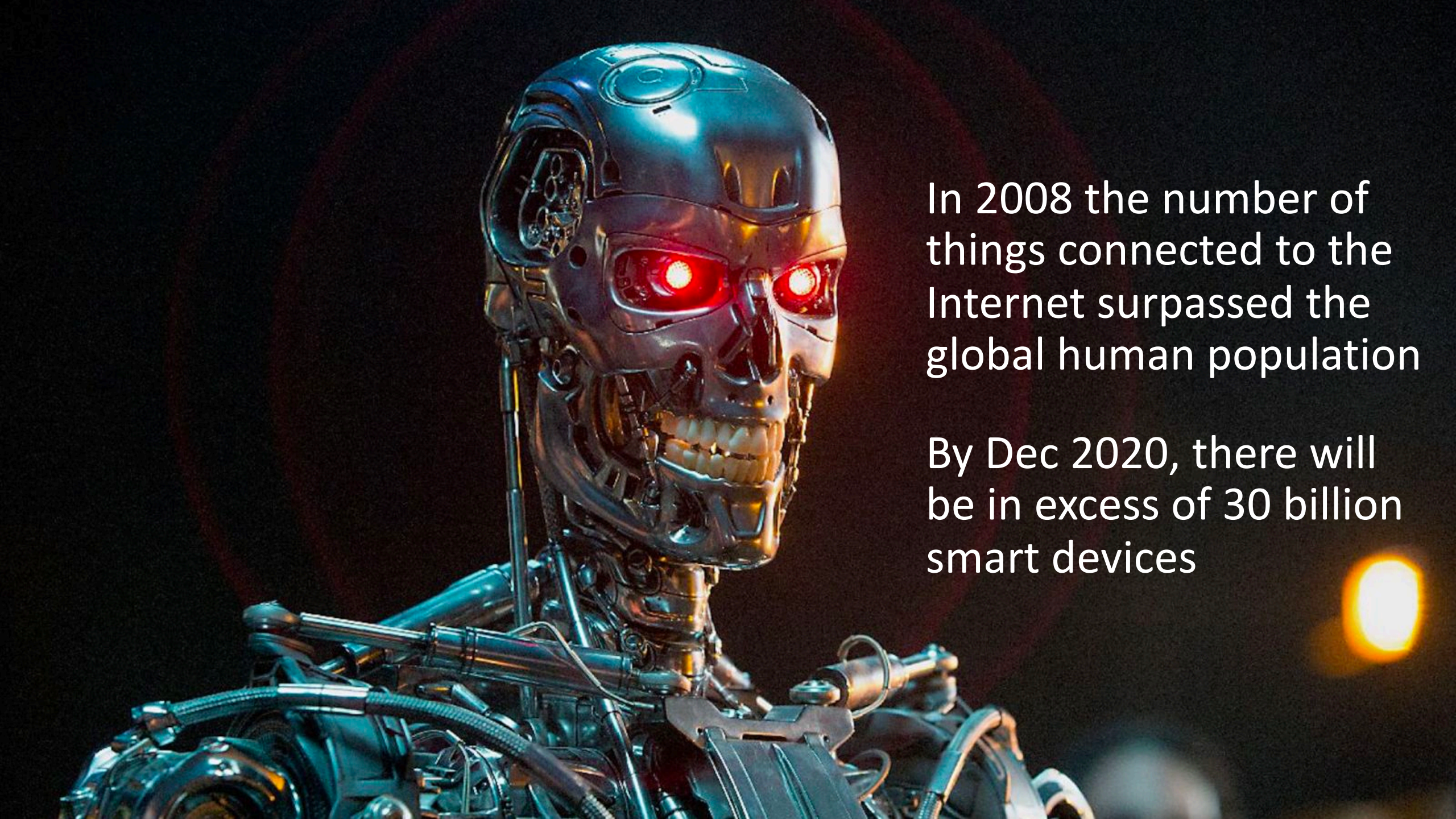
Why is it SO important?

The field is becoming more important due to increased reliance on computer systems, the Internet and wireless network standards such as Bluetooth and Wi-Fi, and due to the growth of smart devices, including smartphones, televisions, and the various devices that constitute the "Internet of things". Owing to its complexity, both in terms of politics and technology, cybersecurity is also one of the major challenges in the contemporary world.

Wikipedia

Cyber Security

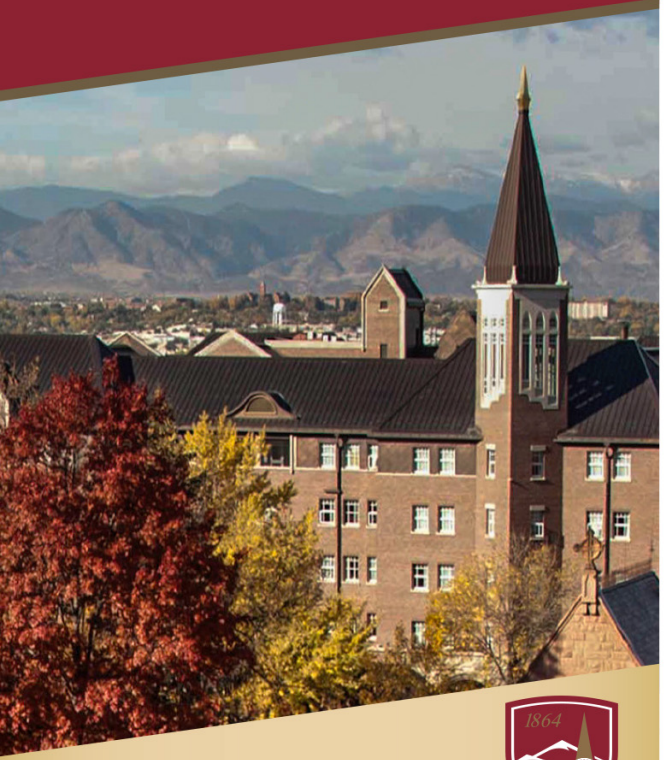
Today, We Are All Hyper-Connected



In 2008 the number of things connected to the Internet surpassed the global human population

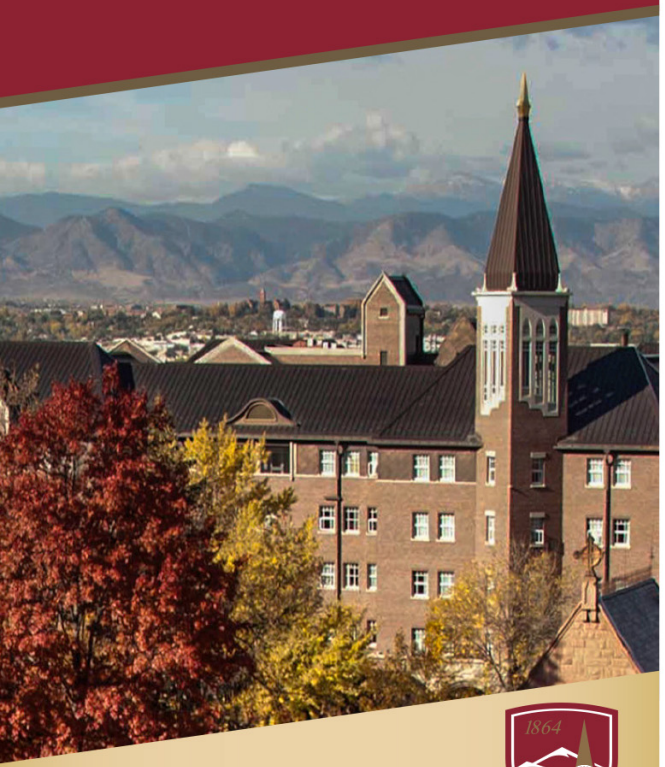
By Dec 2020, there will be in excess of 30 billion smart devices

Cyber Security



Who is Attacking us?

Cyber Security

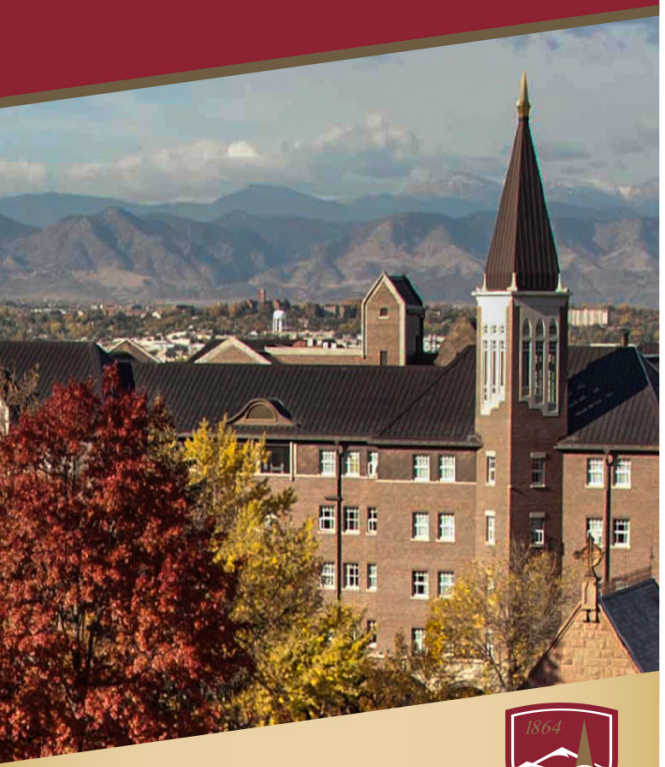


Who Are Perpetrators of Cybercrime?

- Nation States – opponents of the United States. This is hybrid cyber war!
- Organized Crime Gangs – The Russian Mob for example
- Hacktivists – want to change the world – PETA, Anonymous, etc.
- Script Kiddies – teenagers who want to show off / prove themselves

We are Outnumbered Five to One currently

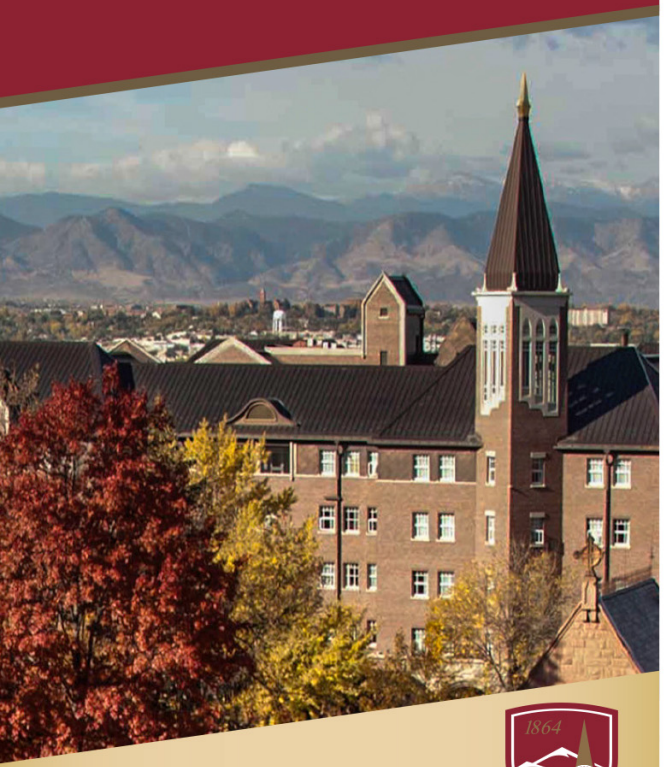
Cyber Security



Organized Crime - Motivations

- Its all about Money – the more the better.
- Often act as proxies for Governments that shelter and protect them.
- Motivated and ruthless criminals willing to use any means possible to increase their return on investment.
- Gangs have formed into specialists companies for each stage of the Attack Chain:
- Construction of Footholds, Creation of exploits, Parsing and Sale of Stolen Goods, etc.
- Some are even listed on Stock Exchanges.
- Increasingly using emulation tools and techniques to fool victims – CEO Fraud.

Cyber Security



A New Type of Attack in CEO Fraud

Reputation Destruction, and many other uses

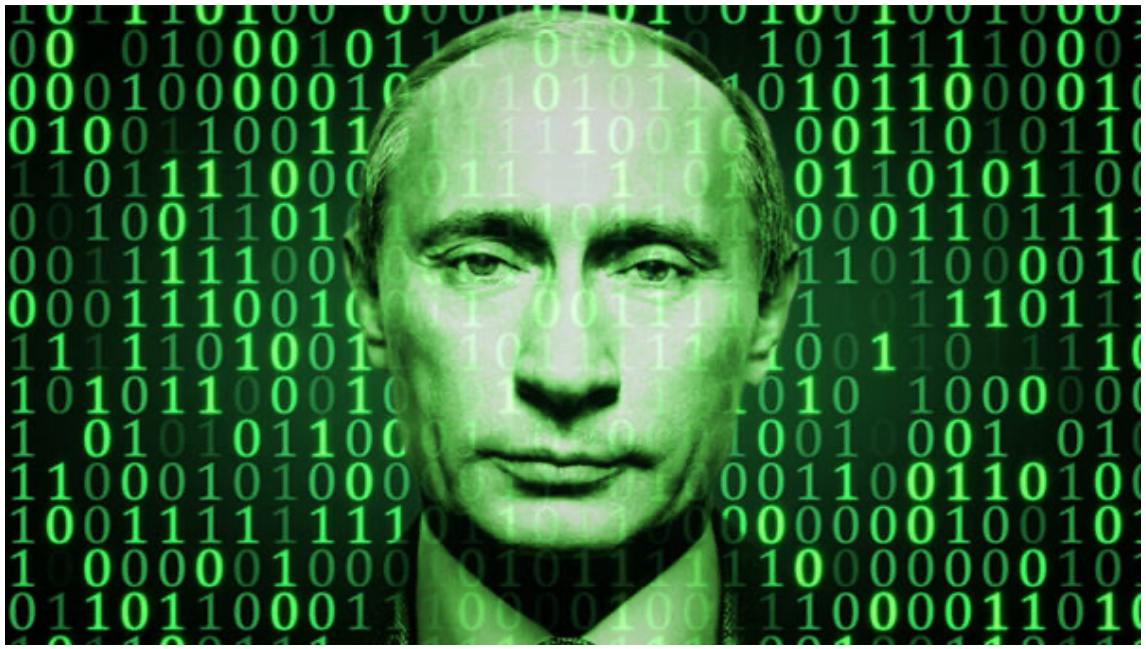
Cyber Security

Artificial Intelligence

- Was that really the CEO on the phone telling me to transfer money to a numbered Cayman Island bank account?
- Or a deepfake audio bot?
- Did the election candidate really just say that on live TV?

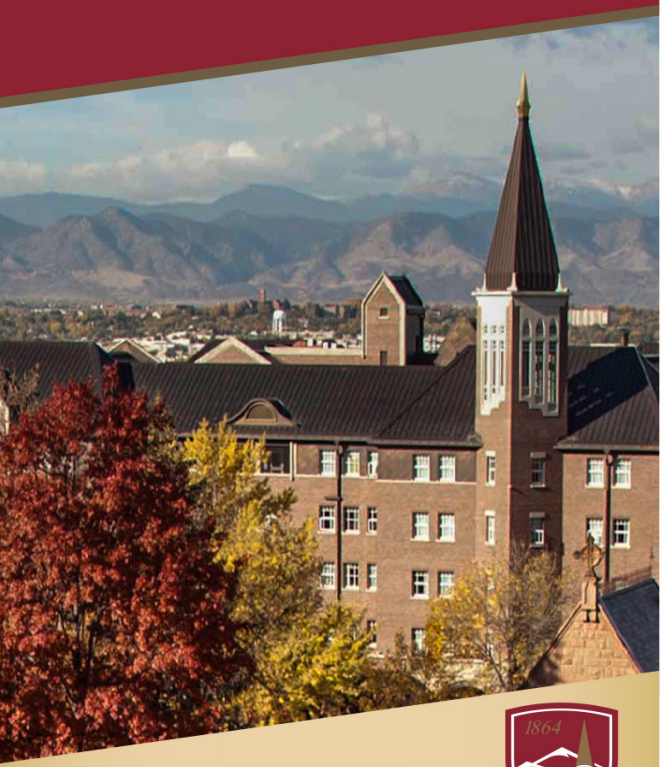
Cyber Security

Nation States - Motivation



- To exert political / economic / military pressure to execute their agenda
- To steal intellectual property / money for national gain
- To undermine the pillars of society – like confidence in electoral systems
- To manipulate, or even eliminate data and throw a trust-based system into chaos

Cyber Security



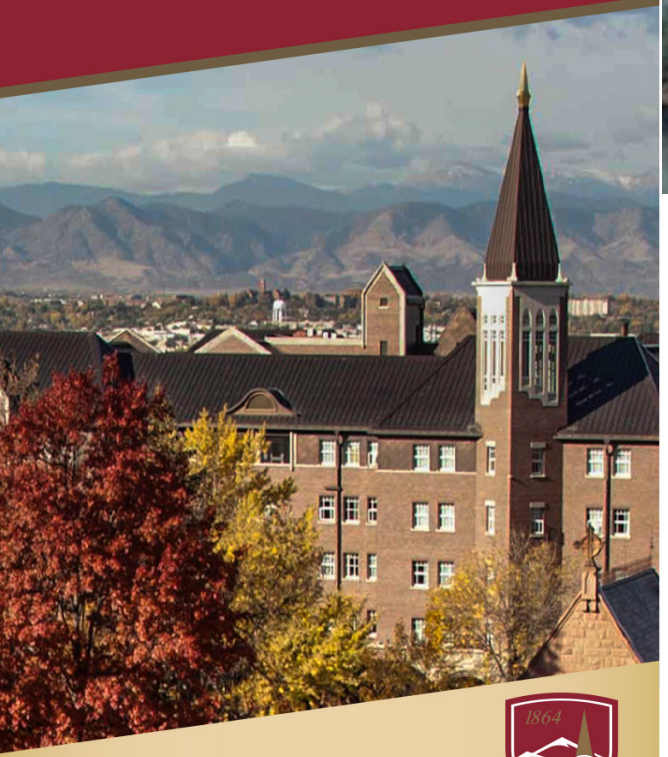
Disinformation

Who REALLY won the 2016 US Presidential Election,

or BREXIT or French and German elections?

- Its just a 21st century version of spycraft
- Release of compromising data – email today, spy mistresses in the 1950s
- Subliminal manipulation of the masses - via social media today, unions in 1950
- These are activities of nation state counter espionage
- It's been evolving since the height of the Cold War

Cyber Security



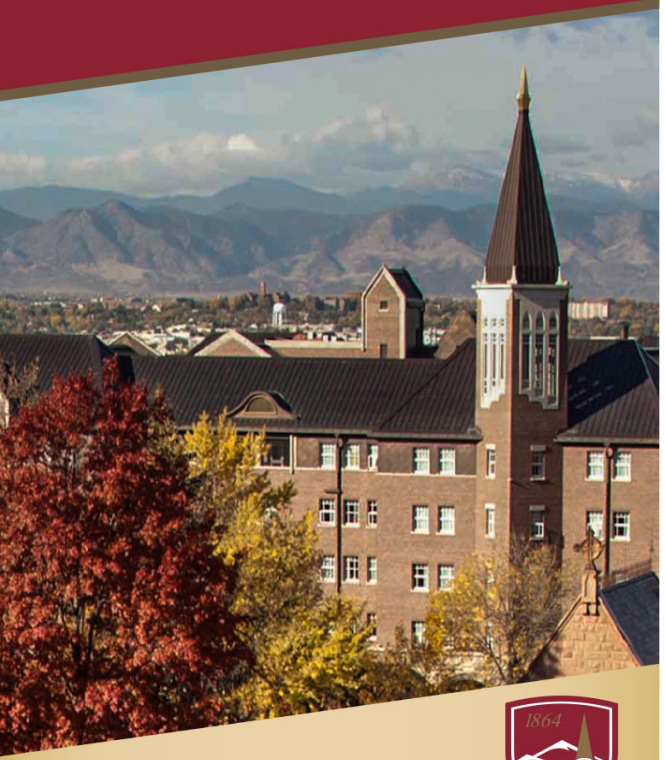
Cyber Attacks against Critical Infrastructure

Russian GRU blew up

Baku-Tbilsi-Ceyan pipeline

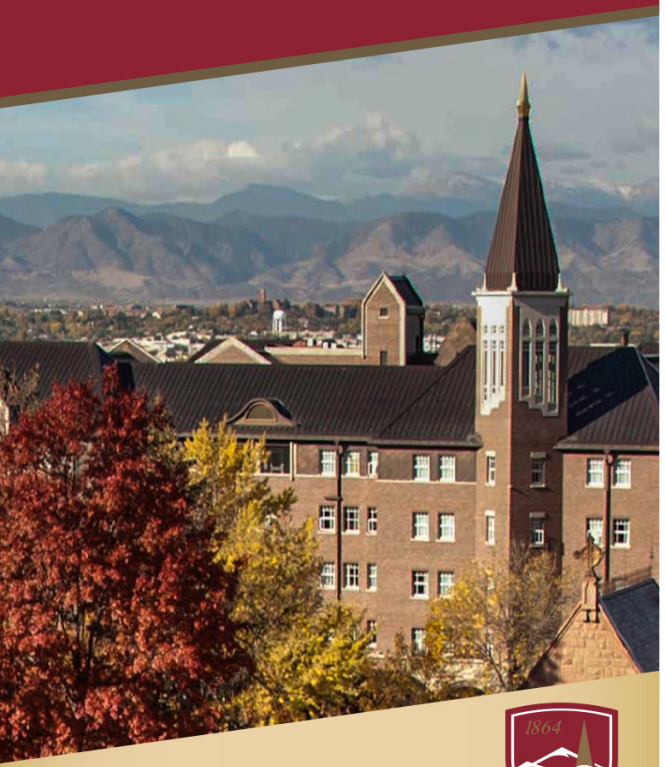
by cyber attack in 2008

Cyber Security



Russia Has Blown Up / Shut Down the Power Grid in Ukraine Multiple Times by Cyberattack

Cyber Security



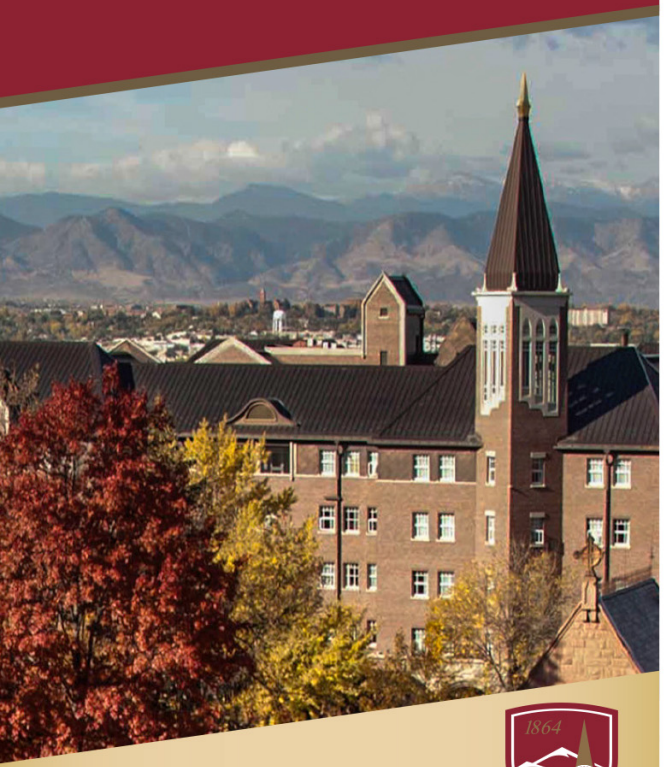
Its not just the Russians!

The New York Times

A Dam, Small and Unsung, Is Caught Up in an Iranian Hacking Case

Iranians caught in attempted to cyber attack against Bowman Avenue Dam in Rye Brook, Westchester County, 2016

Cyber Security



Who Are Perpetrators of Cybercrime?

Which Country has stolen most of the world's research, commercial trade secrets and intellectual property?

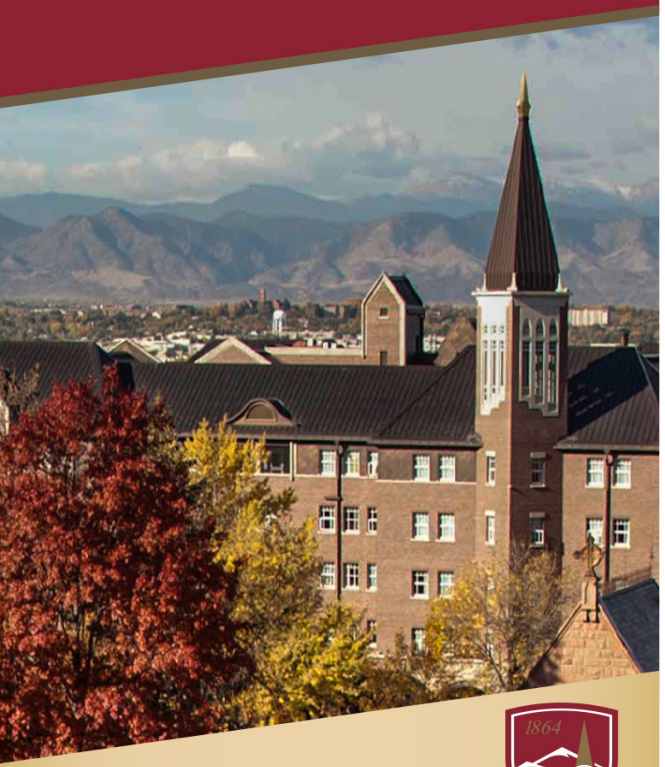

Communist China
employs an army of tens
of thousands of hackers
in its PLA

Who is Stealing our IP and COVID Cure Research?

Both Russia and China behind attacks against recent New Jersey pharmaceutical research companies according to FBI.

Both want to be first to market with COVID vaccine.

Cyber Security



Why is Cybersecurity So Important?


CAR HACKING JUST GOT REAL

Woman killed in Car Crash

Hospitals are full of “connected” equipment

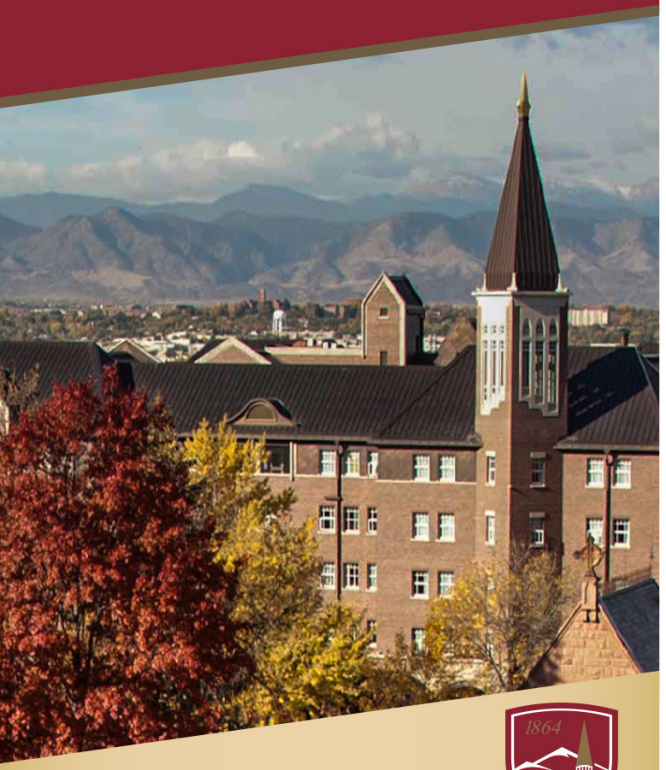
Cyber Assassin

You don’t need to be James Bond armed with a Walther PPK and a “Licence to Kill” to carry out assassinations when you own the medical device a target is attached to!


Russian Oligarch,
Mafia Boss or innocent
patient?

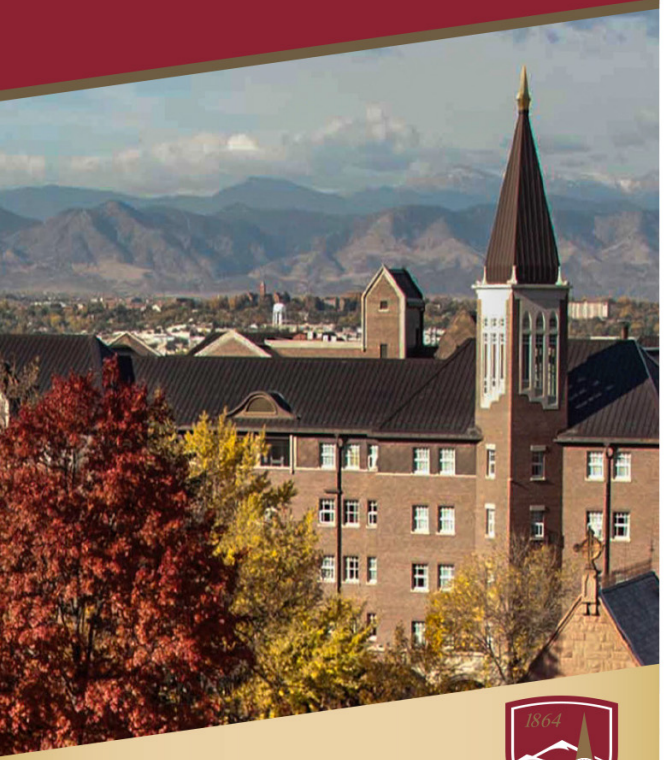
What happens when you or a loved one needs to go to hospital but the hospital has been hacked?

Cyber Security



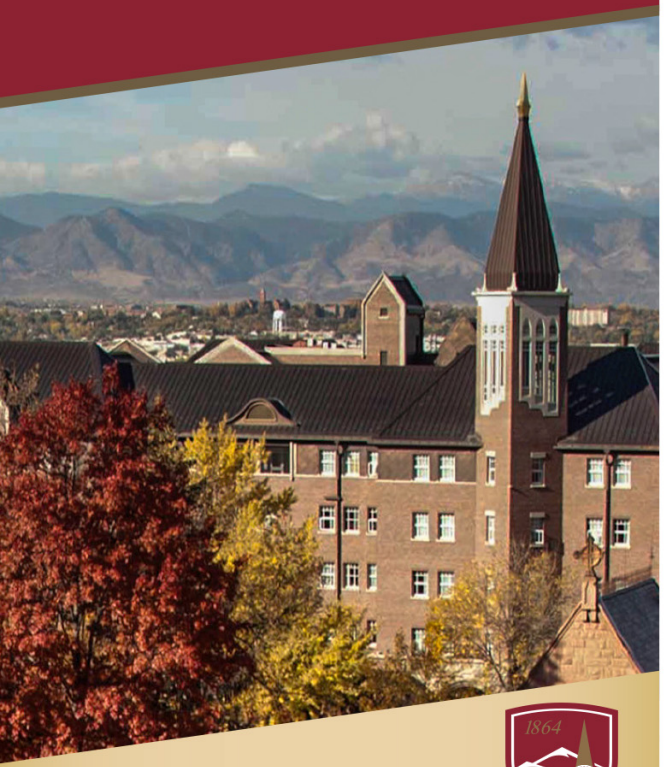
When IT Systems are not available Patient Care Declines

Cyber Security



Security Domains

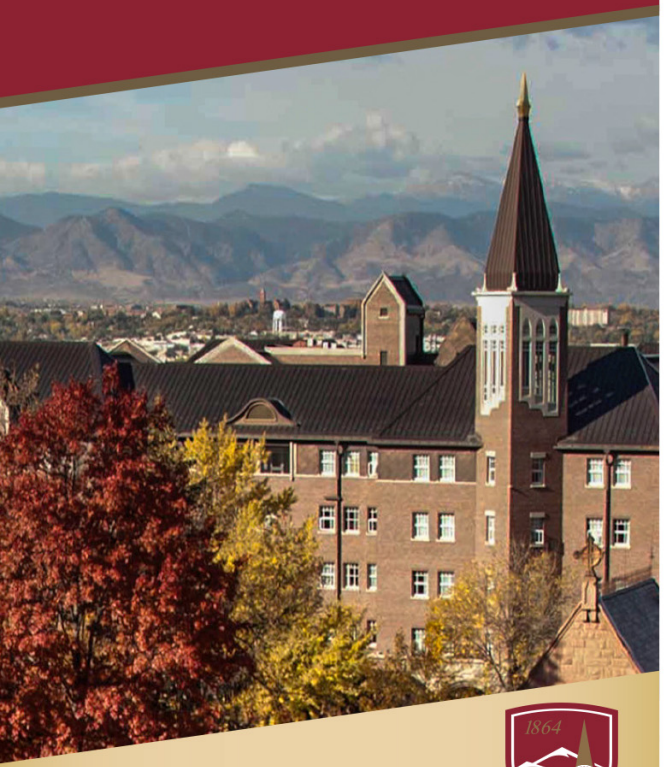
Cyber Security



ISO Security Domains

- A.5 Information Security Policies
- A.6 Organization of Information Security
- A.7 Human Resource Security
- A.8 Asset Management
- A.9 Access Control
- A.10 Cryptography
- A.11 Physical and Environmental Security
- A.12 Operations
- A.18 Compliance
- A.13 Communications
- A.14 System Acquisition, Development and Maintenance
- A.15 Supplier Relationships
- A.16 Information Security Incident Management
- A.17 Business Continuity Management

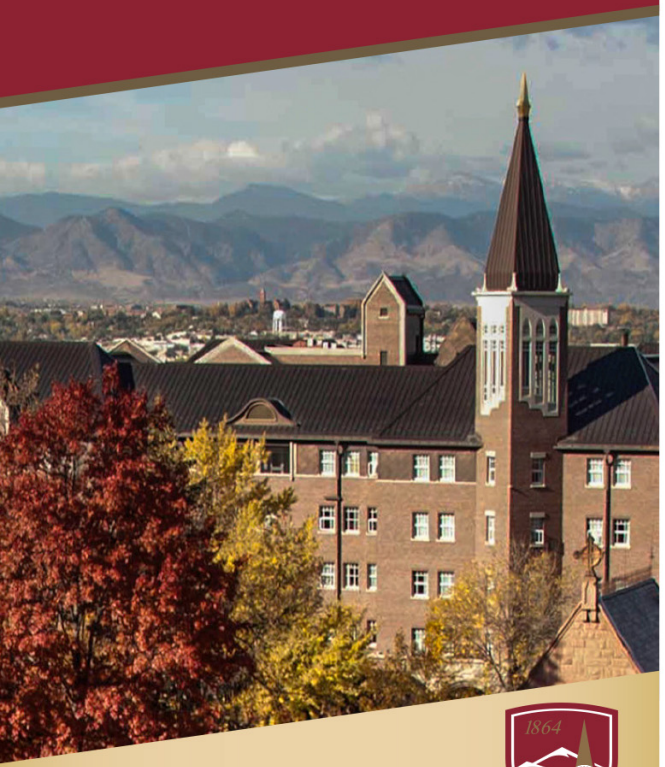
Cyber Security

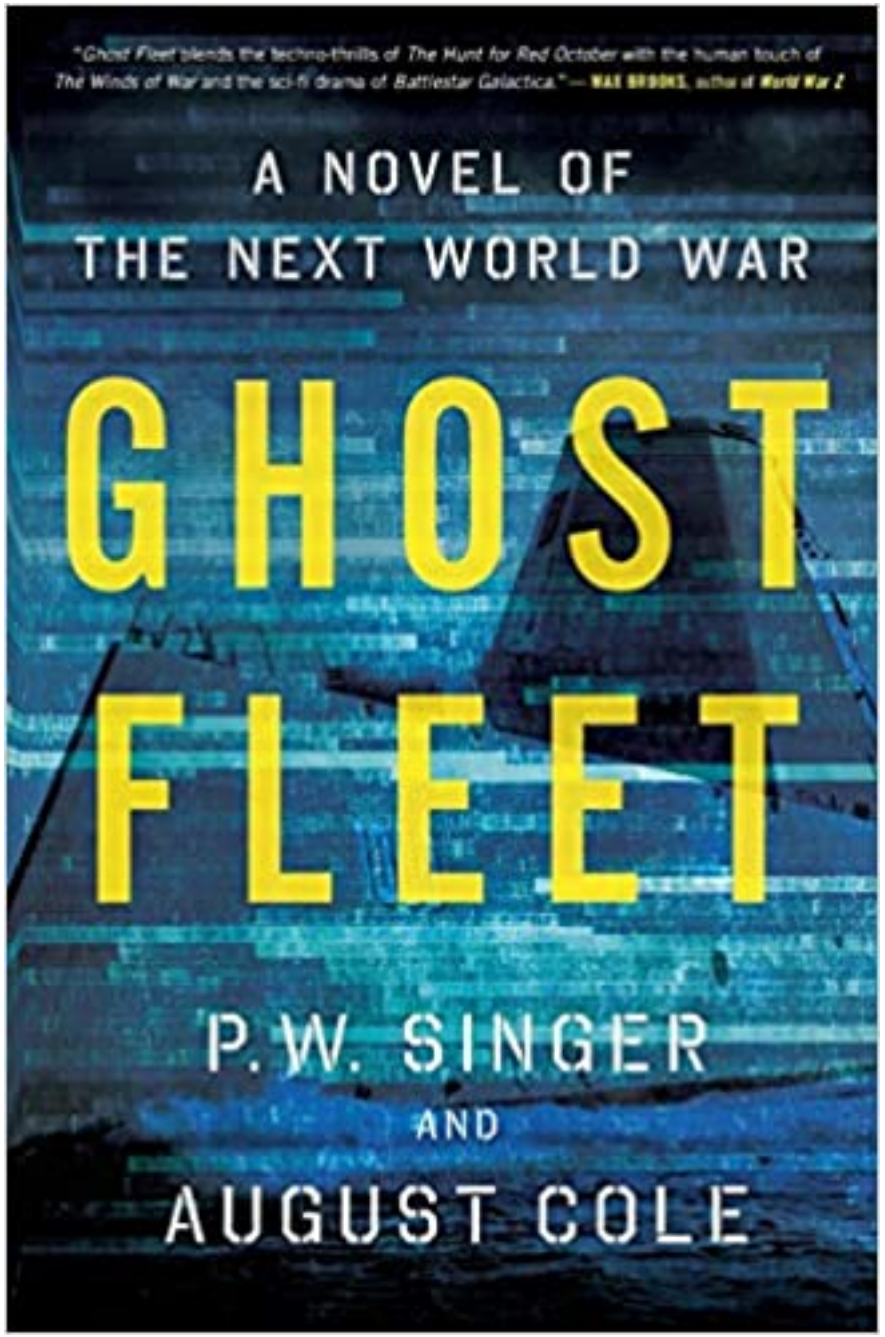


NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

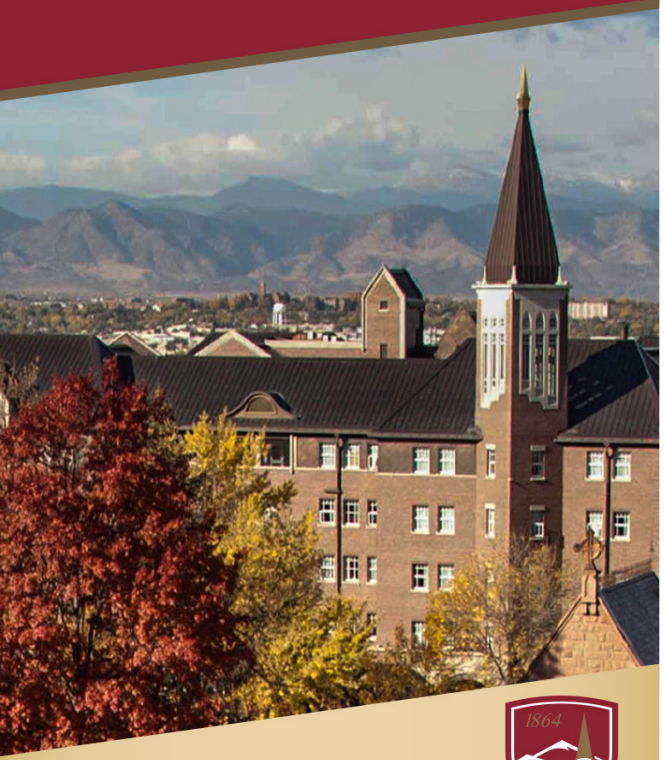
Cyber Security





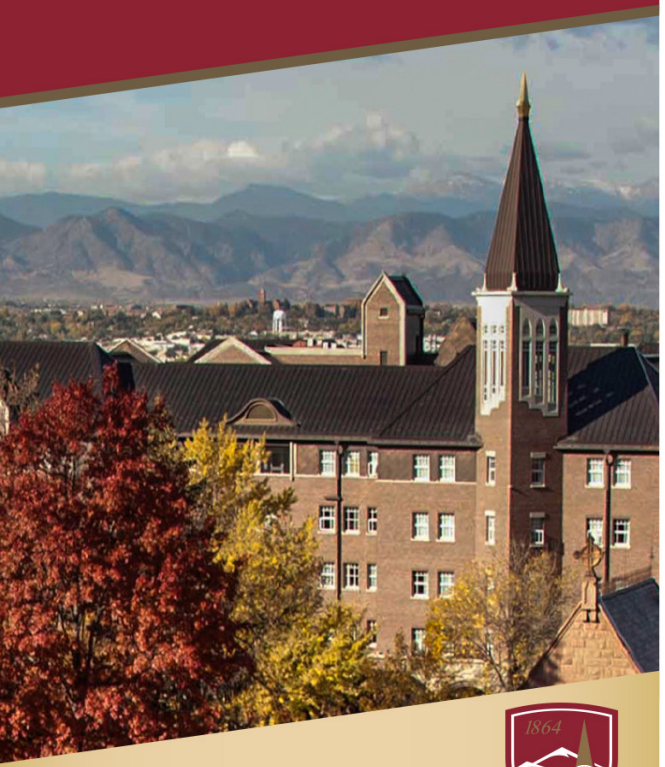
Set in the near future, the book portrays a scenario in which a post-Communist China, assisted by Russia, is able to launch a technologically sophisticated attack against the United States in the Pacific, leading to the occupation of the Hawaiian Islands.

Cyber Security



Job Prospects

Cyber Security



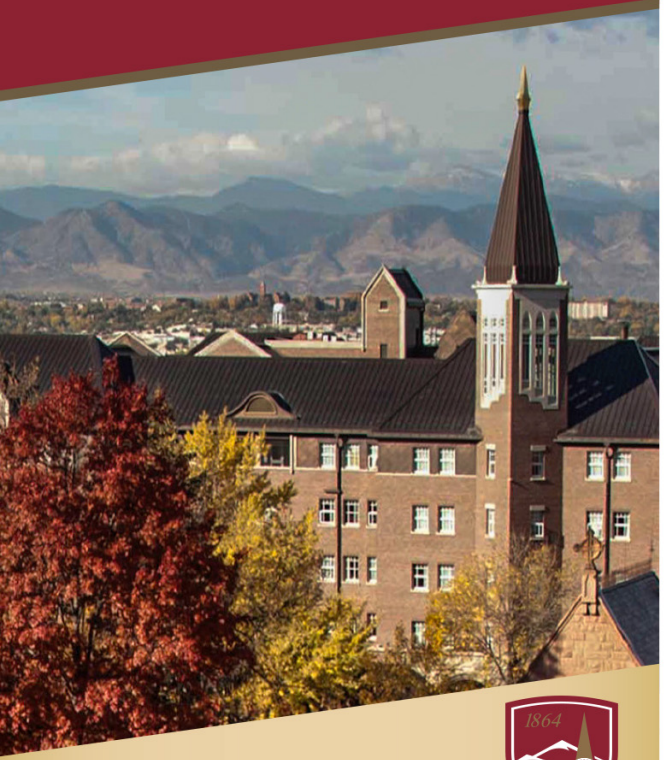
Why You Should Consider A Career in Cybersecurity

- It’s a growing profession and an ideal time to move in
- Its well paid – 15~25% better paid than IT
- There are lots of career opportunities for progression
- Vertical into management / leadership or to become an SME
- Horizonal across domains
- Its noble profession – you are:
  - Defending your grandmother from having her life savings stolen
  - Defending your kids against online sex predators
  - Defending your friends, neighbors, buddies from online scams or extortion
  - Defending your company – to help keep the lights on

A Career in Cybersecurity

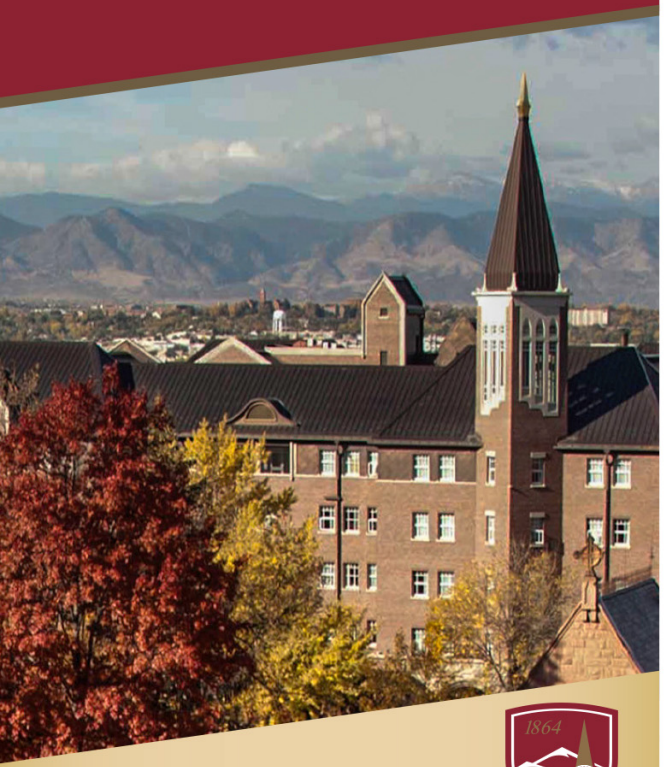
Security Operations Center

Cyber Security



Career Opportunities

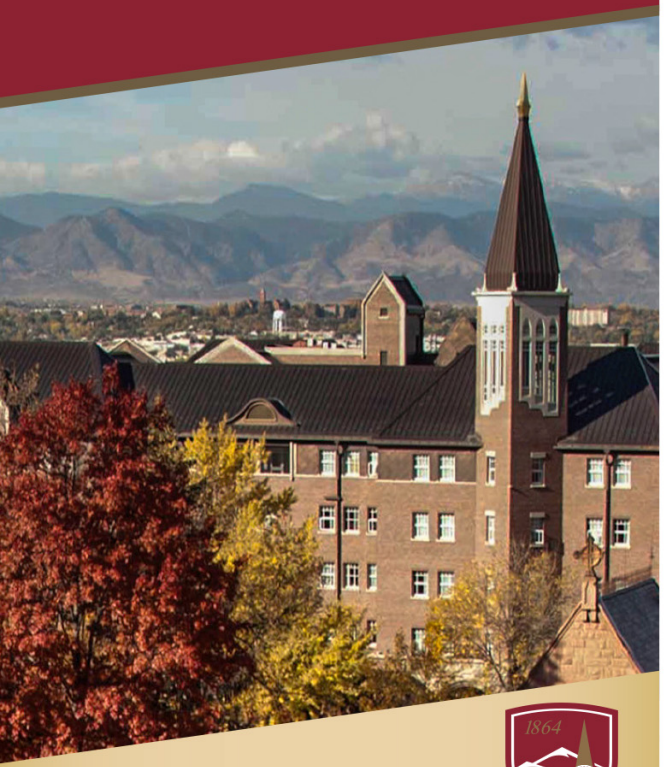
Cyber Security



Entry Level

- Companies are crying out for cybersecurity professionals
- There is a MASSIVE shortage of certified, qualified or experienced professionals
- CISCO claims there is a 12x demand over supply for good security people
- I think its more from what I see!
- **YOU WILL HAVE A WELL–PAYING JOB FOR LIFE!**
- In the industry of your choice – finance, healthcare, retail, hospitality, chemical, oil & gas, electrical generation & distribution, manufacturing, etc.

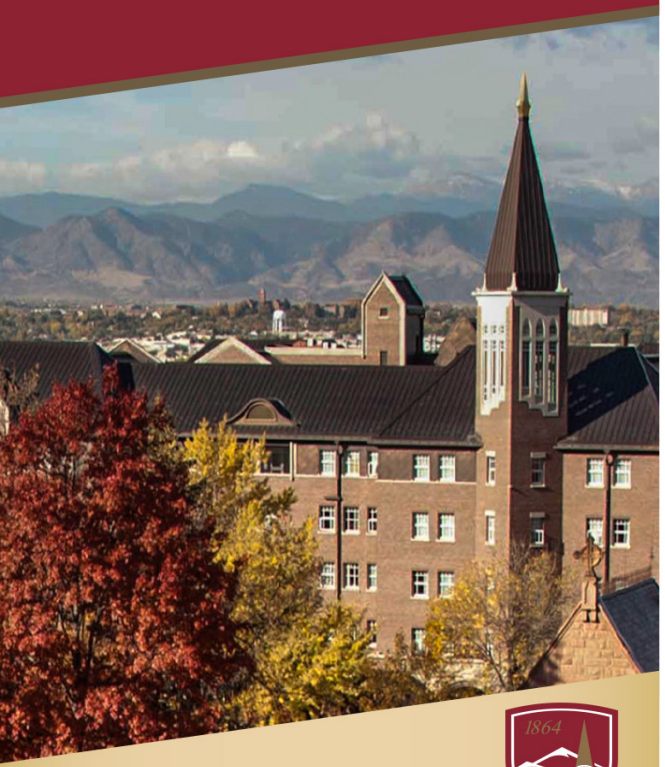
Cyber Security



Getting a Foot in the Door

- Getting any job requires you to do some work
- But it's a Catch 22 – you need experience and you can't get experience without a job
- You need a job-strategy!
- **Internships are a key way of opening the door**
- Being enrolled in an educational program will allow you to get an internship
- Complete the internship and you have a reference and experience to add to your resume. Now you have experience

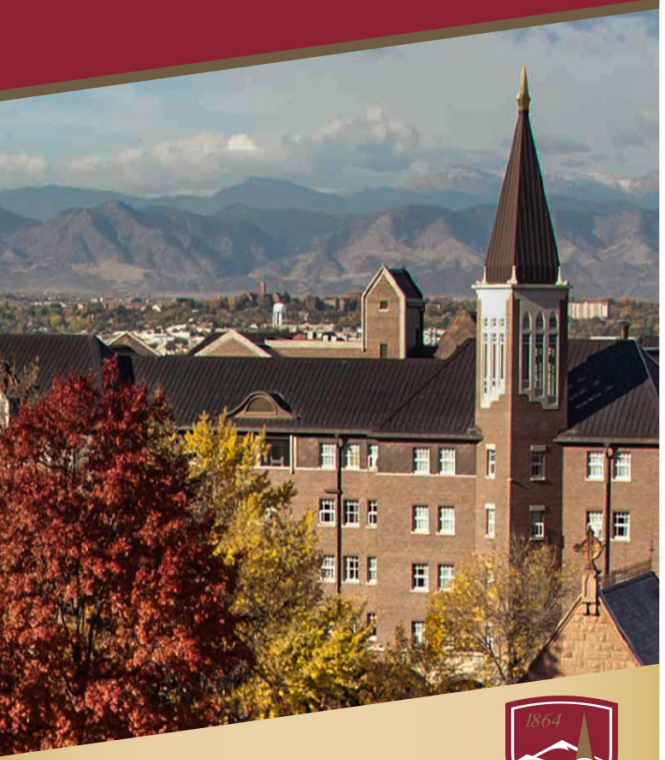
Cyber Security



Some Job Hunting Advice

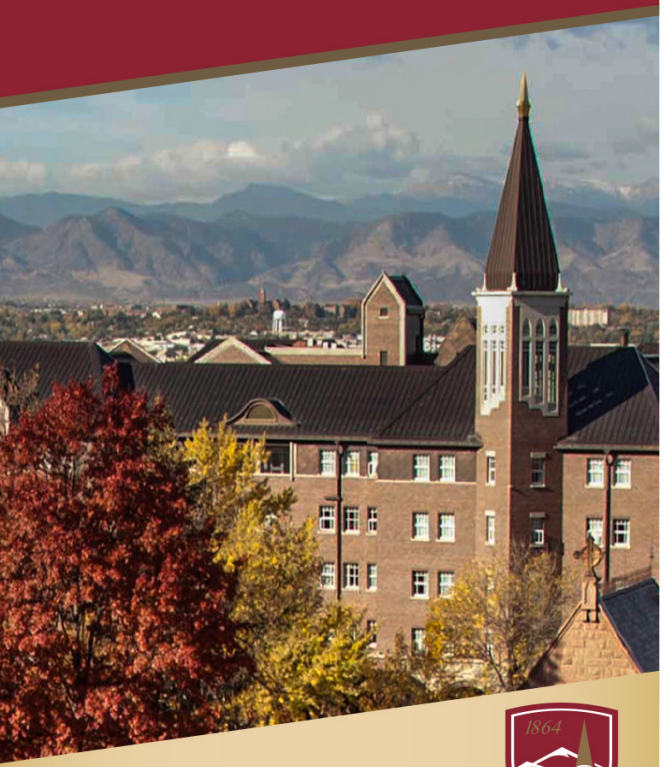
- Forget mailing out 100 copies of your printed resume – it doesn't work
- **Build a PROFESSIONAL Social Media Presence on LinkedIn to sell yourself**
- Do not use Linkedin for your Facebook or Twitter rants – exercise decorum. Linkedin is a Professional Network.
- Prospective Employers will conduct a thorough search of your online persona so be careful what you post online – it never goes away!
- **ITS ALL ABOUT NETWORKING**
- Attend Security Conferences, meet and chat with people
- Join ISSA, ISACA, OWASP, etc., and attend monthly meetings
- If you are focused on an industry join an industry group like HIMSS and go to their meetings – people you meet may be able to help you find your dream job.

Cyber Security



Certifications

Cyber Security



Advanced IT Training Programs at EJC

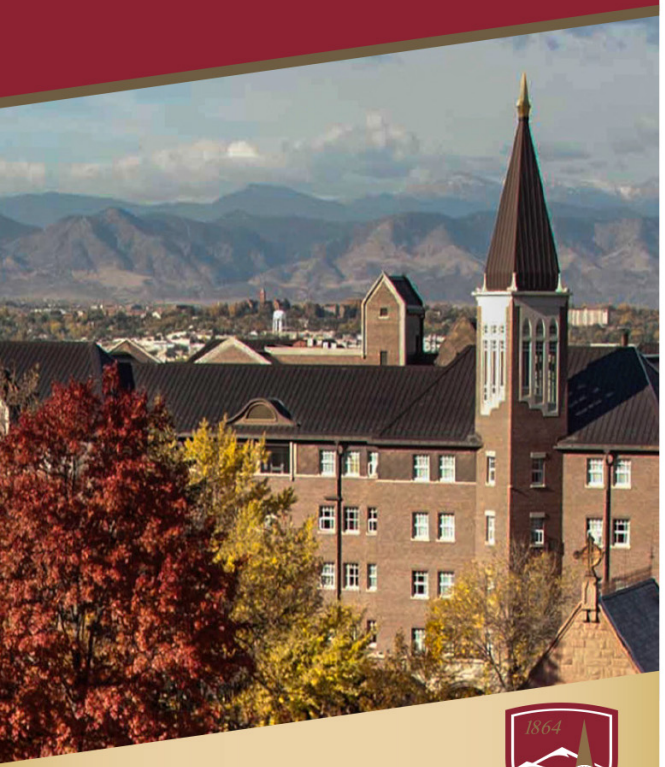
CompTIA A+ Certification (Core)

This program exposes students to A+ (1001 and 1002) components, focusing on developing skills for becoming a Computer Service Technician. The course lasts six to eight months during which students will need to demonstrate understanding and competency by successfully passing two exams (1001 and 1002) required to become CompTIA A+ Certified PC Technician.

Important Note: Acceptance is based on students completing a basic trade; specifically one tied to Information and Office Technologies (ex: IT trades on security, networking, network data cabling, web design, Linux, telecommunications, Strata IT, and Microsoft Office products to name a few).

Contact Miguel Hervas for details

Cyber Security



Advanced IT Training Programs at EJC

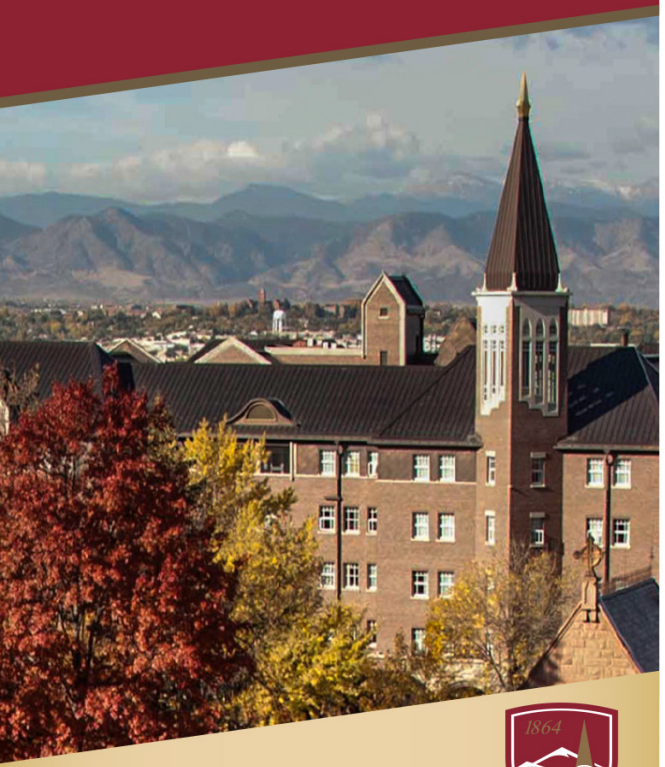
CompTIA Security+ Certification (non-core)

This program exposes students to IT security technologies; focusing on skills for becoming an IT Security Technician. This course last four to six months during which students will need to demonstrate understanding and competency by successfully passing relevant exams required to achieve goal in becoming a CompTIA Security+ Certified Technician.

Important Note: Acceptance into Security+ training program requires approval from Instructor and CTT Manager based on prior performance in the EJC Advanced A+ training program, early TAR completion, behavioral conduct in and outside of training, professionalism, and attendance record. Only students who are enrolled in the A+ program at EJC will have the opportunity to be enrolled in the Security+ programs. Students who already obtained A+ certification at another center are not eligible.

Contact Miguel Hervas for details

Cyber Security



Technical Security Certifications

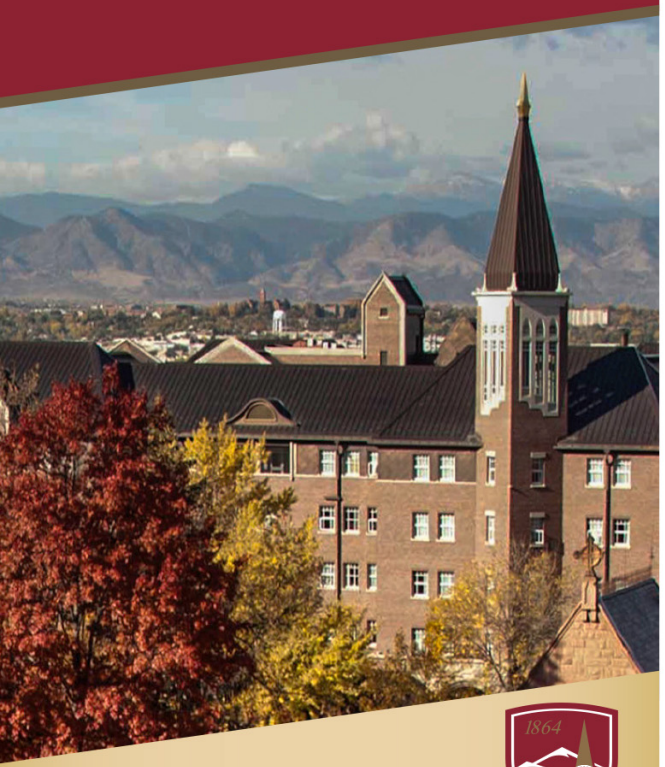
Certified Ethical Hacker (CEH)

This program is a qualification obtained by demonstrating knowledge of assessing the security of computer systems by looking for weaknesses and vulnerabilities in target systems, using the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of a target system. This knowledge is assessed by answering multiple choice questions regarding various ethical hacking techniques and tools. The certification is administered by EC Council.

Requirements
2 years of experience
Pass 4 hour multiple choice exam
Valid 3 years – revaluate by CPEs

Costs
Exam Prep (typical) $100
Exam Fee ($1199)
Annual Renewal Fee $80

Cyber Security

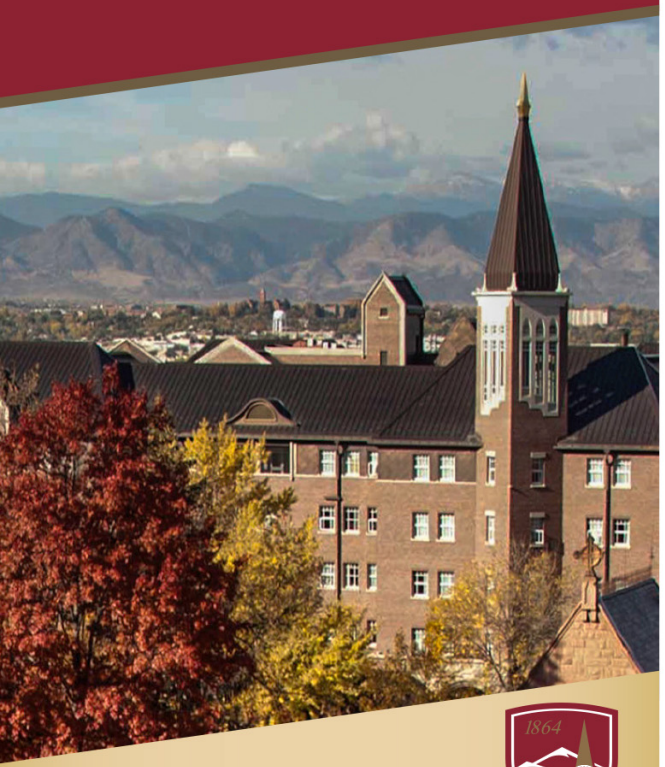


SANS Security Certifications

GIAC Information Security Fundamentals (GISF)

Security Professionals that want to demonstrate they are qualified for IT systems hands-on roles with respect to security tasks. Candidates are required to demonstrate an understanding of information security beyond simple terminology and concepts.

Cyber Security

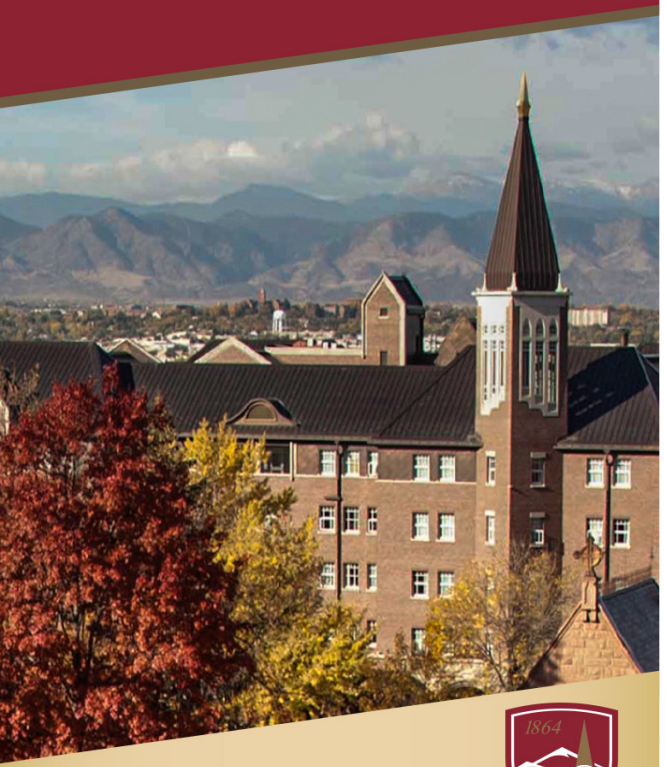


SANS Security Certifications

GIAC Security Essentials (GSEC)

Security Professionals that want to demonstrate they are qualified for IT systems hands-on roles with respect to security tasks. Candidates are required to demonstrate an understanding of information security beyond simple terminology and concepts.

Cyber Security

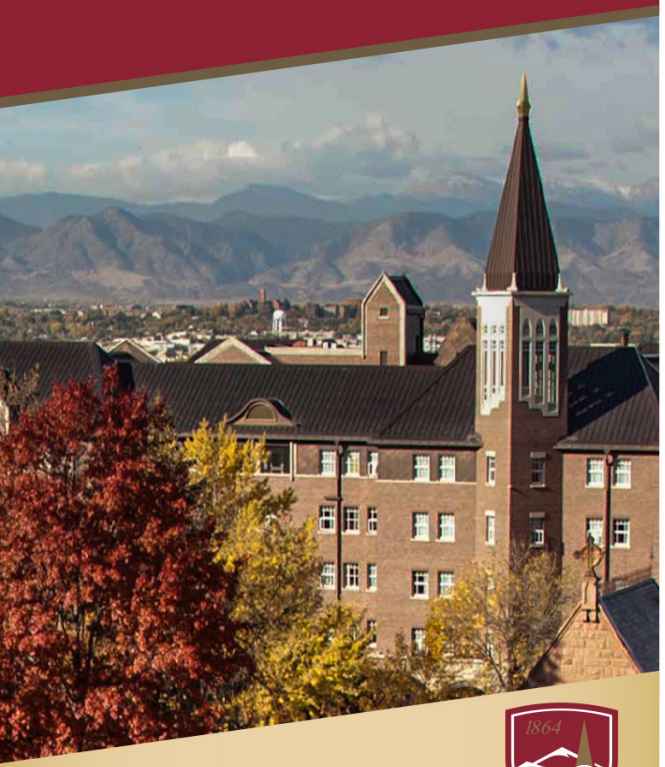


SANS Security Certifications

GIAC Open Source Intelligence (GOSI)

Security Professionals that want to demonstrate they are qualified for IT systems hands-on roles with respect to security tasks. Candidates are required to demonstrate an understanding of information security beyond simple terminology and concepts.

Cyber Security



SANS Security Certifications

GIAC Certified Intrusion Analyst (GCIA)

Security Professionals that want to demonstrate they are qualified for IT systems hands-on roles with respect to security tasks. Candidates are required to demonstrate an understanding of information security beyond simple terminology and concepts

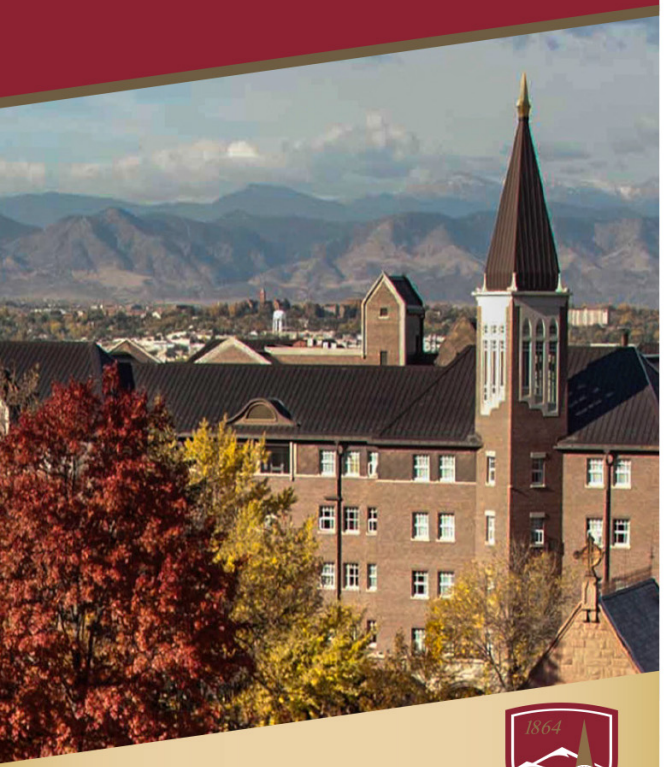
Cyber Security

SANS Security Certifications

GIAC Continuous Monitoring Certification (GMON)

Security Professionals that want to demonstrate they are qualified for IT systems hands-on roles with respect to security tasks. Candidates are required to demonstrate an understanding of information security beyond simple terminology and concepts

Cyber Security

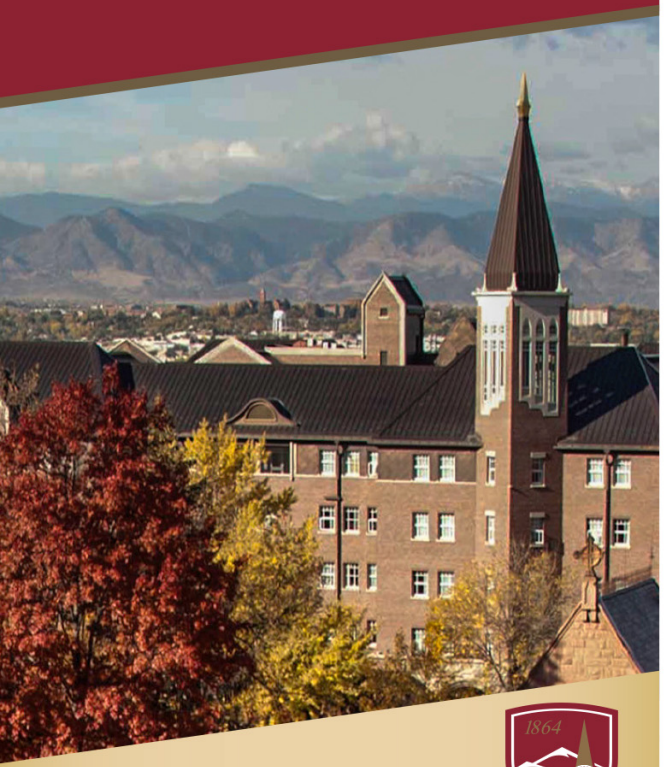


SANS Security Certifications

GIAC Defending Advanced Threats (GDAT)

Security Professionals that want to demonstrate they are qualified for IT systems hands-on roles with respect to security tasks. Candidates are required to demonstrate an understanding of information security beyond simple terminology and concepts

Cyber Security



SANS Security Certifications

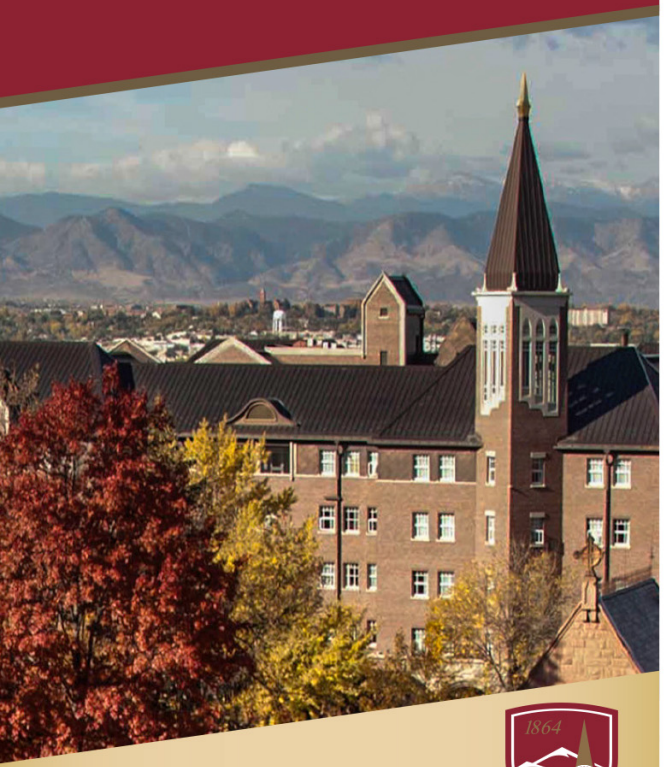
GIAC Information Security Professional (GISP)

Security Professionals that want to demonstrate they are qualified for IT systems hands-on roles with respect to security tasks. Candidates are required to demonstrate an understanding of information security beyond simple terminology and concepts.

SANS MGT414: SANS Training Program for CISSP® Certification is an accelerated review course that is specifically designed to prepare students to successfully pass the CISSP® exam.

MGT414 focuses solely on the 8 domains of knowledge as determined by (ISC)2 that form a critical part of CISSP® exam. Each domain of knowledge is dissected into its critical components, and those components are then discussed in terms of their relationship with one another and with other areas of information security.

Cyber Security



Professional Security Certifications

Certified Information Systems Security Professional (CISSP)

This program was one of the first security certifications and now has over 140,000 members worldwide. It is recognized by companies and governments alike as being a standardized, vendor-neutral certification program that provides structure and demonstrated competence. It is based upon the Common Body of Knowledge (CBK) of 8 security domains. The certification is administered by EC Council and is a recognized equivalent to a Masters Degree in some countries.

Requirements

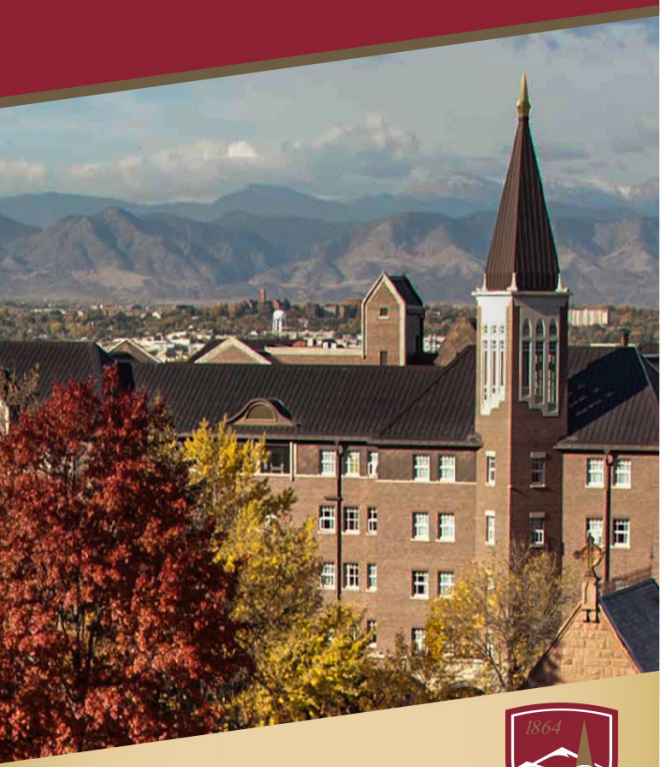
5 years of F/T security experience (4 with a Bachelors or Masters Degree in subject)
Pass Adaptive multiple choice exam (3 – 6 hours)
Valid 3 years – revalidate by CPEs

Costs

Exam Prep (typical) $1,000
Exam Fee ($699)
Annual Renewal Fee $125

INSPIRING A SAFE AND SECURE CYBER WORLD.

Cyber Security



Professional Security Certifications

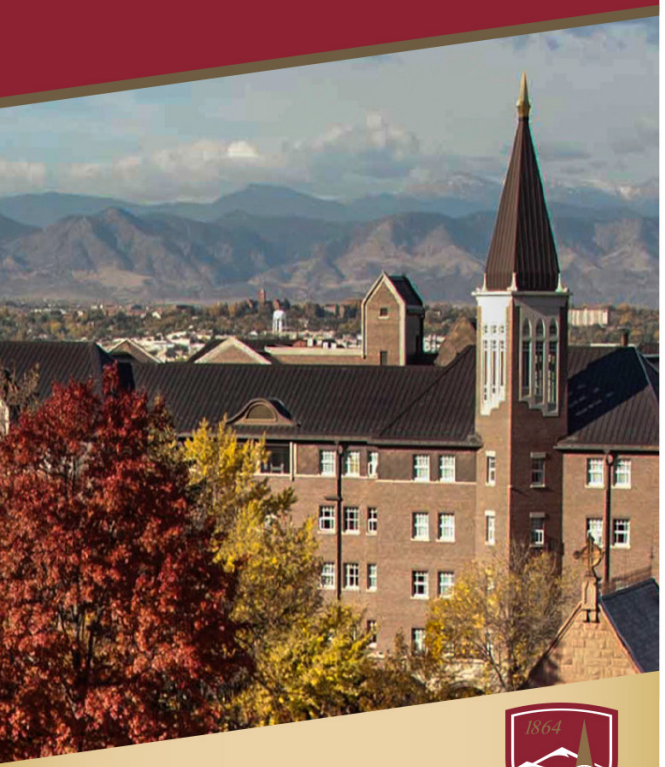
Certified Information Systems Auditor (CISA)

This is a certification issued by ISACA to people in charge of ensuring that an organization's IT and business systems are monitored, managed and protected; the certification is presented after completion of a comprehensive testing and application process. The CISA certification is a globally recognized standard for appraising an IT auditor's knowledge, expertise and skill in assessing vulnerabilities and instituting IT controls in an enterprise environment. It is designed for IT auditors, audit managers, consultants and security professionals.

Requirements
Pass multiple choice exam (3 hours)
Apply for CISA membership
Maintain annual CPEs & ethical code of conduct

Costs
Exam Fee ($670 + $50 exam fee)
Annual Renewal Fee $45 members / $85 non-members
ISACA membership is $135 annually

Cyber Security



Professional Security Certifications

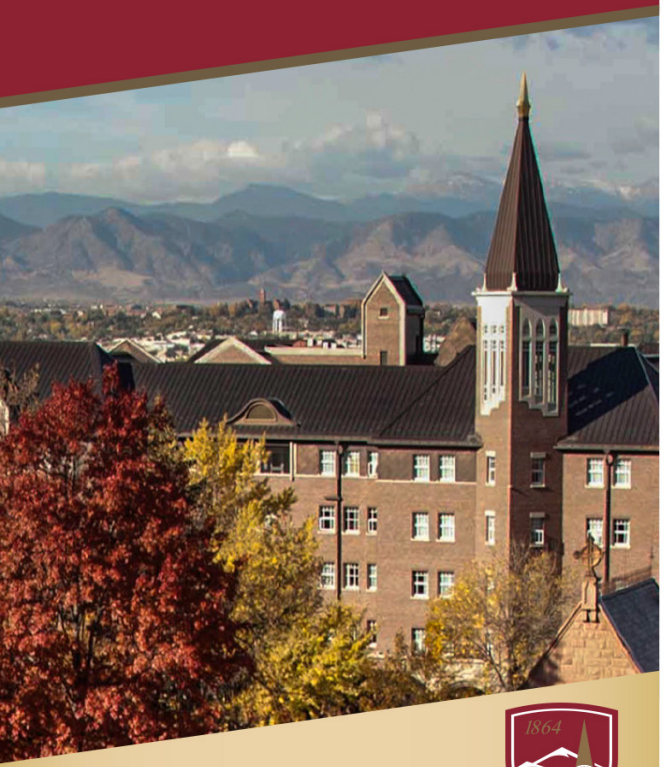
Certified in the Governance of Enterprise IT (CGEIT)

This is a vendor-neutral certification designed for IT professionals responsible for managing IT enterprise governance to validate their skills in the field. ... It's designed for IT professionals in large organizations who are responsible for directing, managing and supporting the governance of IT.

Requirements
Pass multiple choice exam (3 hours)
Apply for CGEIT membership
Maintain annual CPEs & ethical code of conduct

Costs
Exam Fee ($670 + $50 exam fee)
Annual Renewal Fee $45 members / $85 non-members
ISACA membership is $135 annually

Cyber Security



Professional Security Certifications

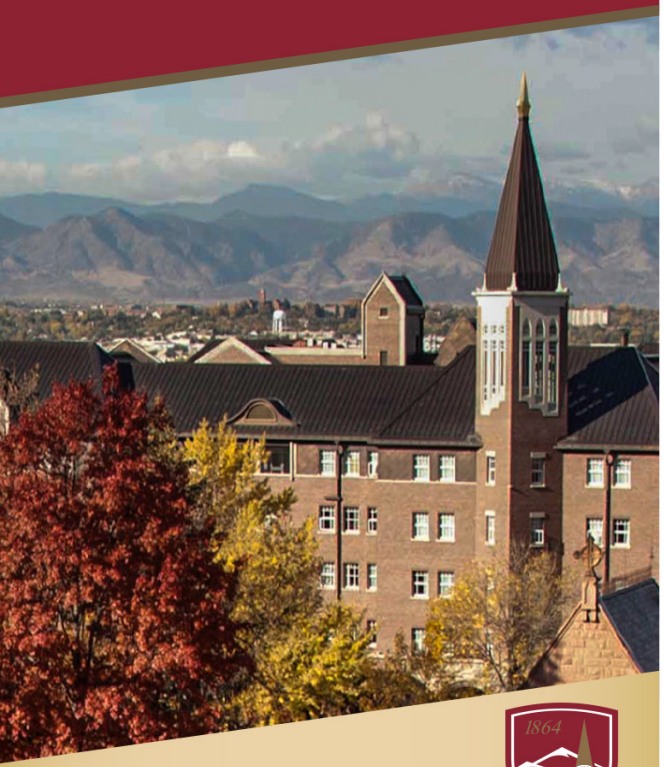
Certified in Risk and Information Systems Control (CRISC)

This is a vendor-neutral certification designed to test the most current and rigorous assessment available to evaluate the risk management proficiency of IT professionals and other employees within an enterprise or financial institute

Requirements
Pass multiple choice exam (3 hours)
Apply for CRISC membership
Maintain annual CPEs & ethical code of conduct

Costs
Exam Fee ($670 + $50 exam fee)
Annual Renewal Fee $45 members / $85 non-members
ISACA membership is $135 annually

Cyber Security



Professional Security Certifications

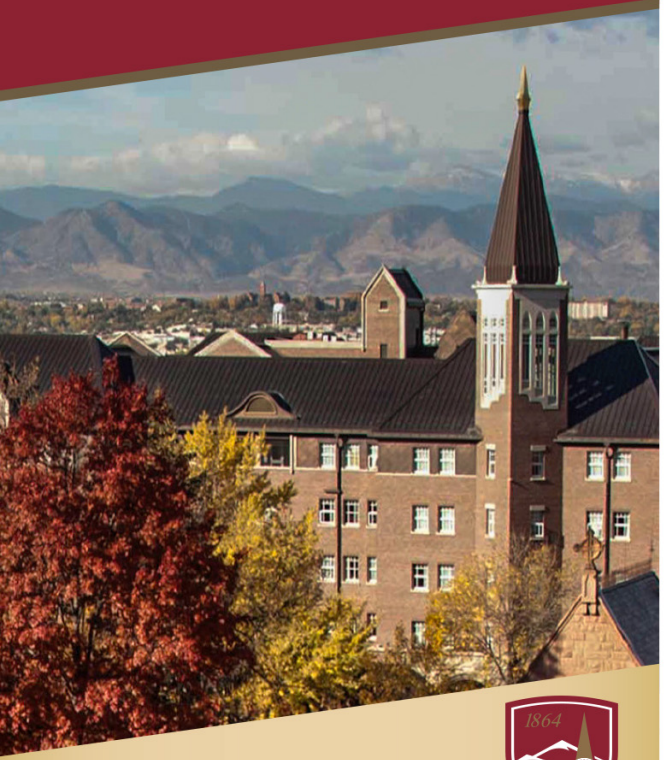
Certified Information Security Manager (CISM)

This certification indicates expertise in information security governance, program development and management, incident management and risk management. It is one of the two top professional certifications and is widely accepted globally with over 46,000 members.

Requirements
Pass multiple choice exam (150 questions, 4 hours) across 4 domains
Apply for CISM membership
Maintain annual CPEs & ethical code of conduct

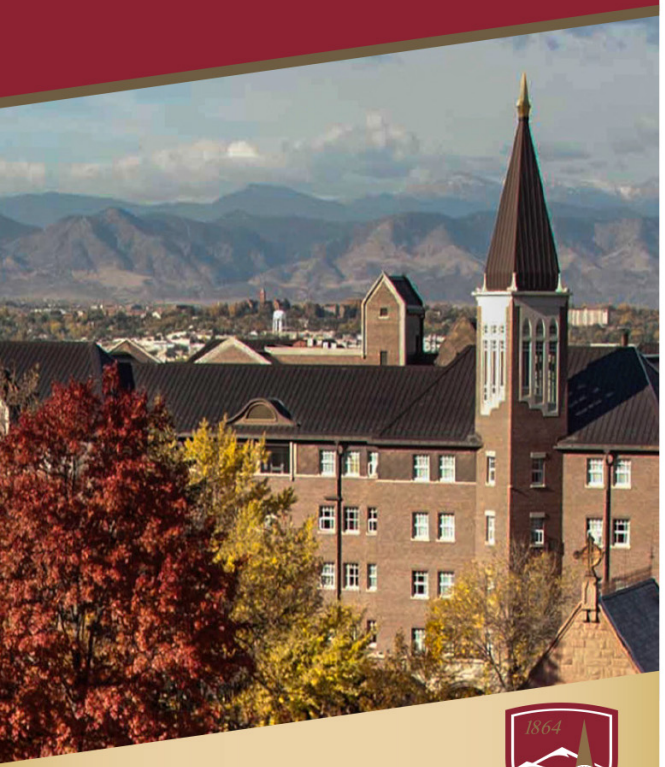
Costs
Exam Fee ($525 / $710 + $50 exam fee)
Annual Renewal Fee $45 members / $85 non-members
ISACA membership is $135 annually

Cyber Security



Qualifications

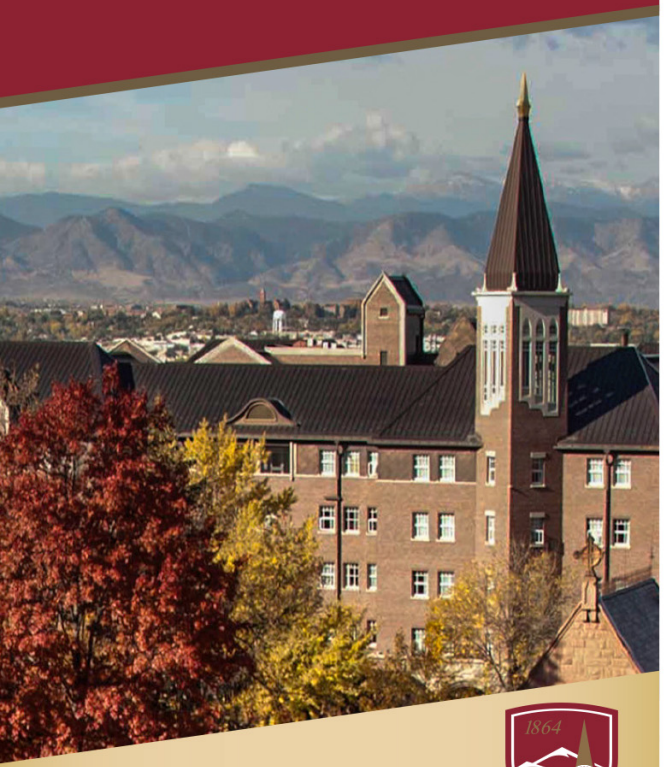
Cyber Security



Academic Certificate or Degree Programs

- Many universities and collages now offer AS, BS and MS degrees in Cybersecurity
- Many locally in the Tri-State area
- Many offer (cheaper) online programs
- Many will allow you to enroll in a certificate program (usually half of the degree credits) with lower admission requirements. After completing the certificate you can continue to the degree.
- Join the military or a good company and they will usually help pay your fees.
- Questions to ask:
  - What is the graduation percentage? 40%, means 6 out of 10 dropped out - why?
  - What is the cost and are any govt / Uni grants / sponsorships available?
  - Can you work independently or do you need to attend class in person?
  - What area of cybersecurity interests you most? Focus on what you like & enjoy

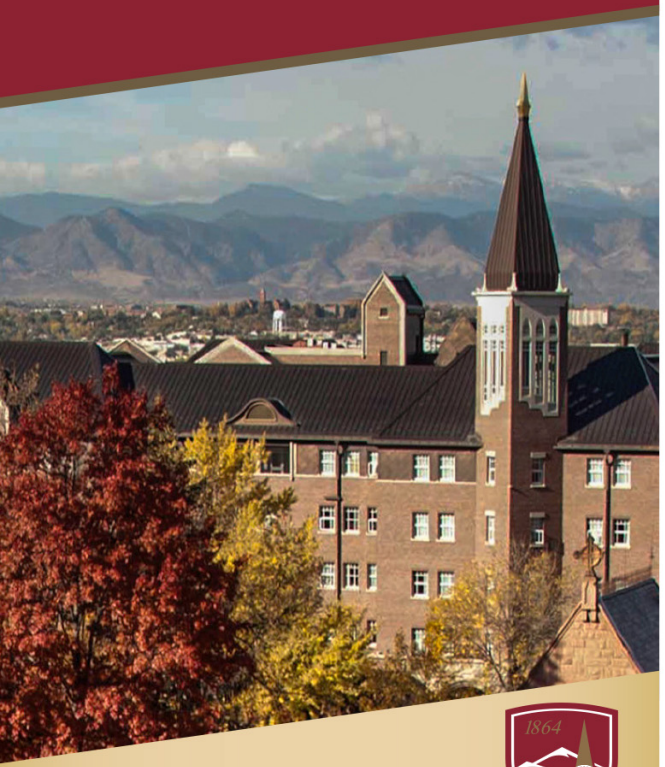
Cyber Security



You Don’t Need a Degree

- There are many different ways to enter the cybersecurity industry
- You don’t need a degree or even a certification but it helps and you will earn more and be promoted faster
- Start Small and Look Big
- Once you have a foot in the door you can wedge that door open

Cyber Security

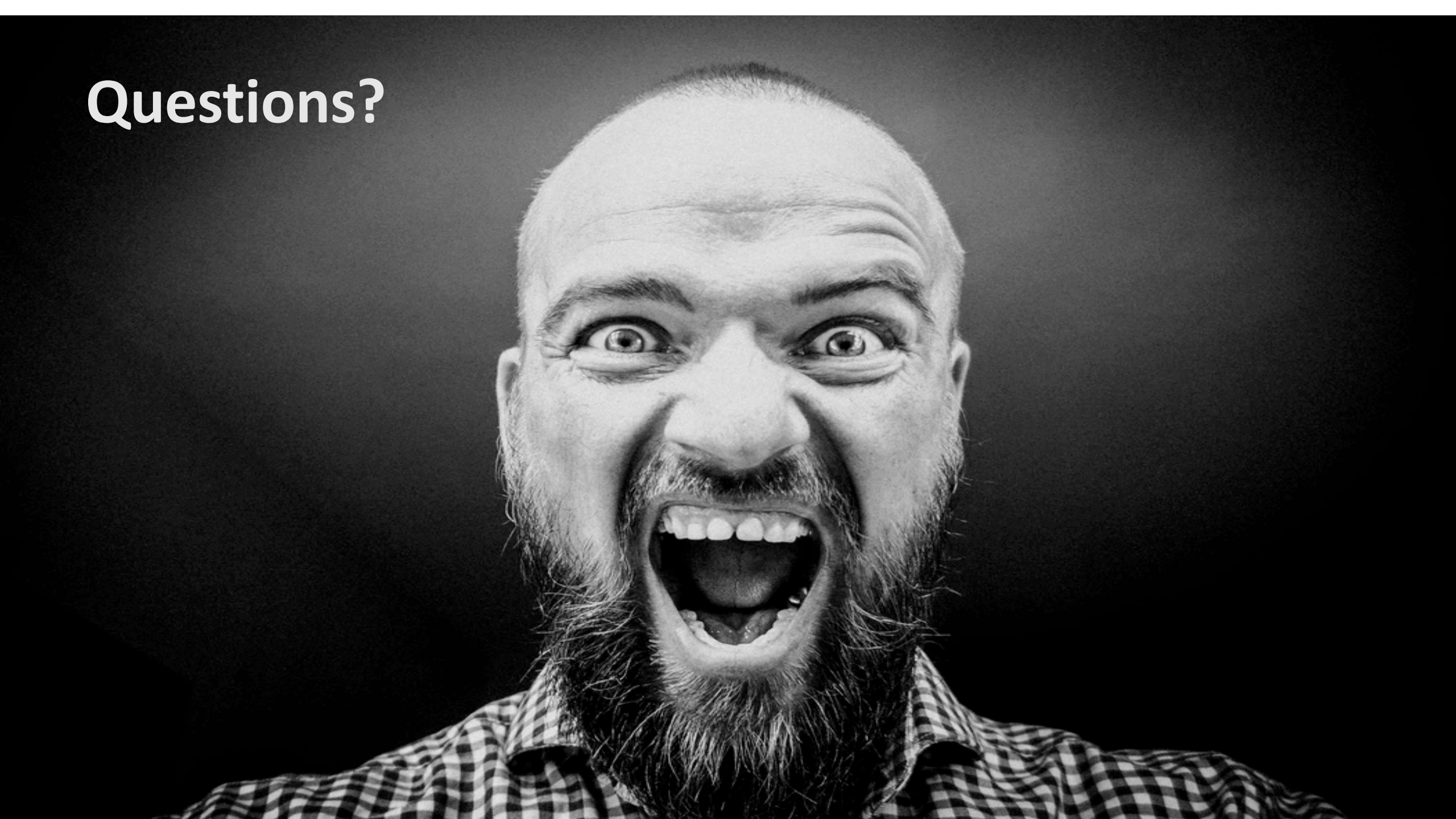


Important Traits

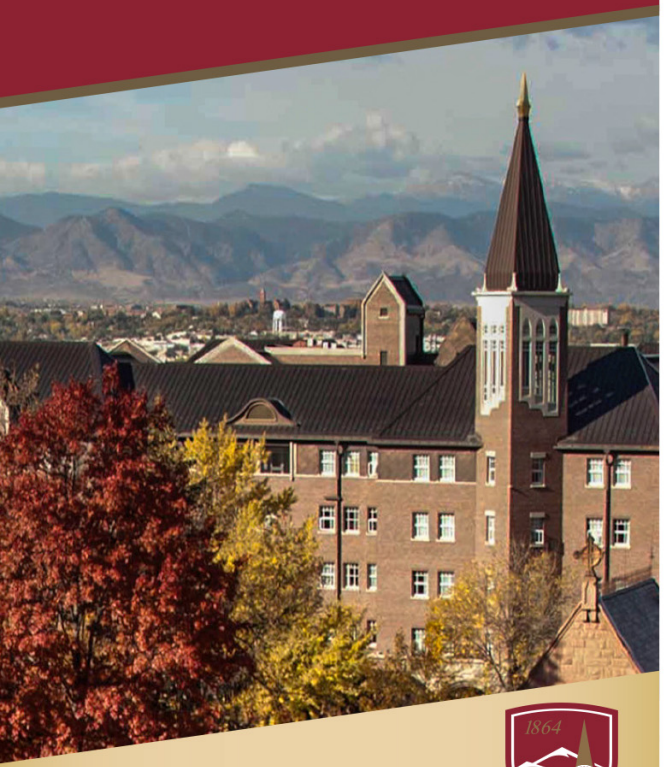
- **TENACITY** is probably the best trait to have in this profession whether you are are:
- **A White Hat** cyber attacker – performing penetration testing of systems or conducting security assessments and audits
- **A Cyber Defender** – perhaps working in a SOC watching and waiting for an attack or conducting pro-active threat hunting across the network
- **A Security Administrator** – managing users and permissions for example
- **A Security Engineer / Architect** – designing and implementing security technologies
- **A Security Manager**, managing a team of experts that keeps an organization safe from attack

- **PASSION** is also important and a desire to win – to beat the bad guys!

Questions?



Cyber Security



Additional Questions

Personal Blog: https://www.cyberthoughts.org/

Linkedin: https://www.linkedin.com/in/richardstaynings/

Twitter: @rstaynings