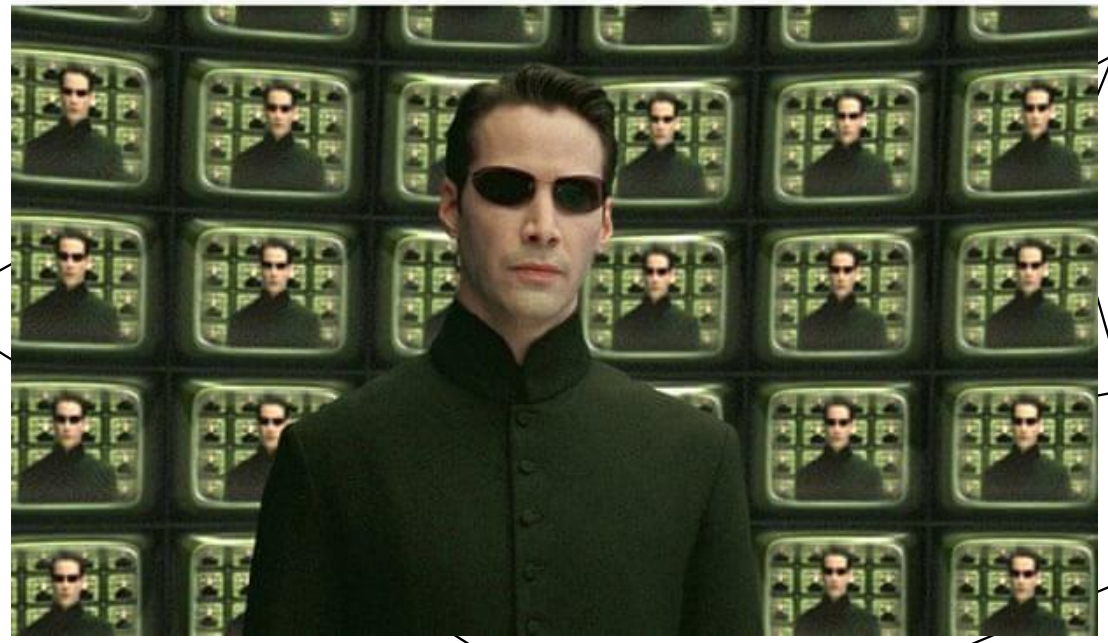


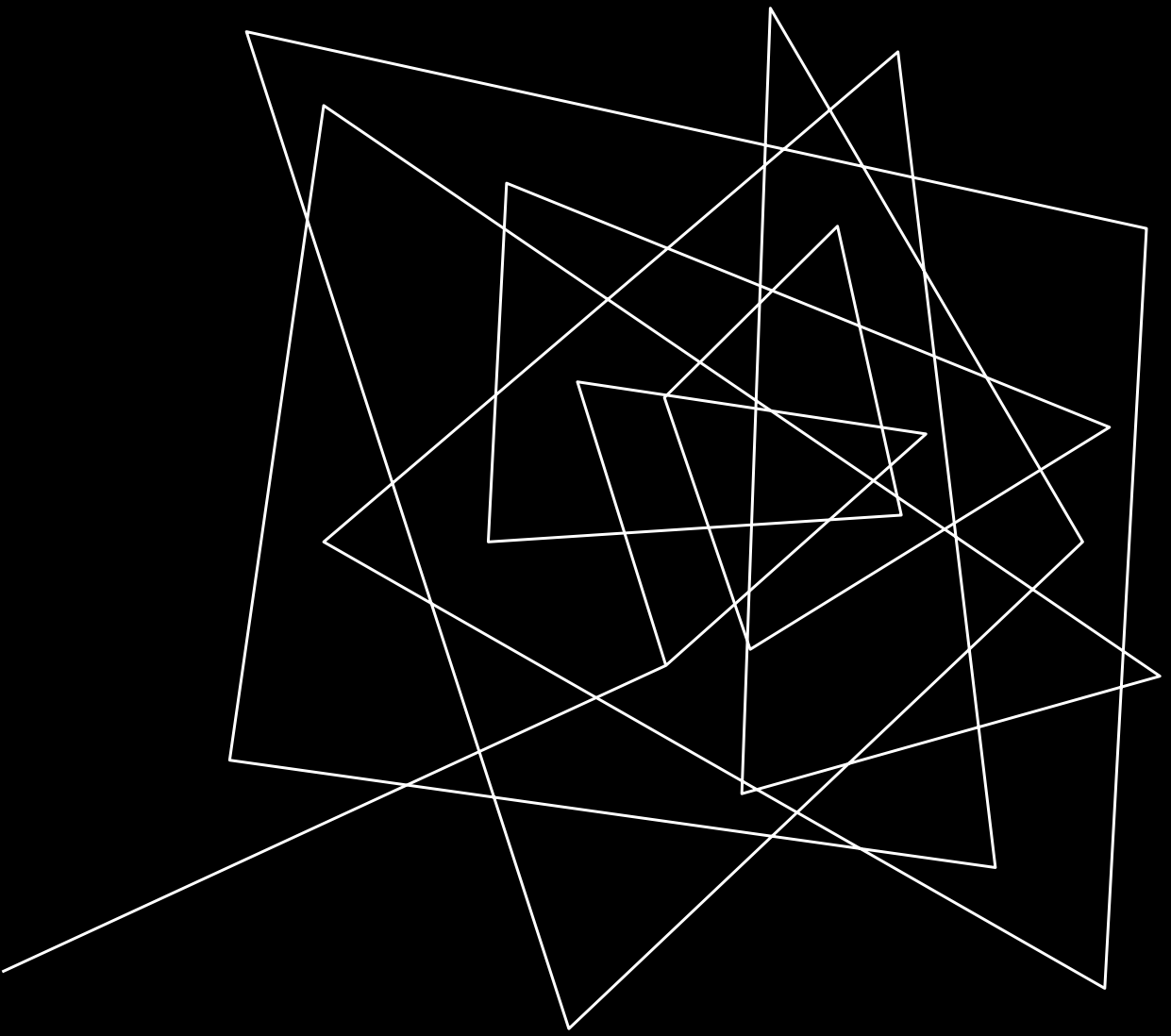
PRINCIPLES OF INFORMATION SECURITY |#1

Keinaz N. Domingo

INTRODUCTION

• Information security: a “well-informed sense of assurance that the information risks and controls are in balance.” — Jim Anderson, Inovant (2002)

• Students must review the origins of this field to understand its impact on our understanding of information security today



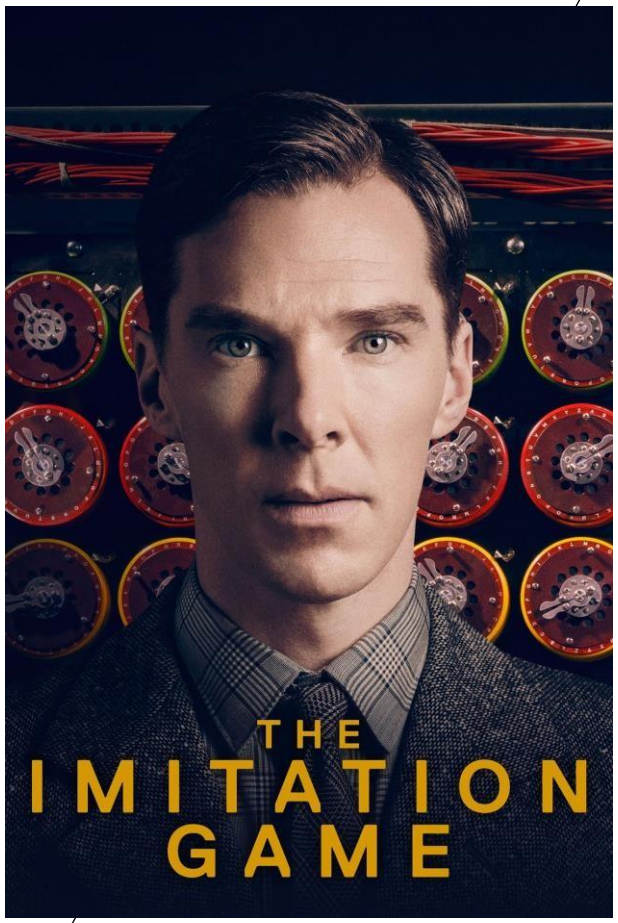
BACK TO BASICS

THE HISTORY OF INFOSEC

- Began immediately following development first mainframes
- Developed for code-breaking computations [Encryption]
- During World War II
- Multiple levels of security were implemented
- Physical controls

<u>Rudimentary</u>

- Defending against physical theft, espionage, and sabotage



INFOSEC IN 1960’S

Original communication by mailing tapes

- Advanced Research Project Agency (ARPA)
- Examined feasibility of redundant networked communications
- Larry Roberts developed ARPANET from its inception Plan
- Link computers
- Resource sharing
- ARPANET is predecessor to the Internet

INFOSEC IN 1970'S AND 80'S

- ARPANET grew in popularity
- Potential for misuse grew
- Fundamental problems with ARPANET security
- Individual remote sites were not secure from unauthorized users
- Vulnerability of password structure and formats
- No safety procedures for dial-up connections to ARPANET
- Non-existent user identification and authorization to system

INFOSEC IN 1970'S AND 80'S

Rand Report R-609

- Paper that started the study of computer security
- Information Security as we know it began
- Scope of computer security grew from physical security to include:
- Safety of data
- Limiting unauthorized access to data
- Involvement of personnel from multiple levels of an organization

INFOSEC IN 1990’S

- Networks of computers became more common
- Need to interconnect networks grew
- Internet became first manifestation of a global network of networks
- Initially based on de facto standards
- In early Internet deployments, security was treated as a low priority

2000’S TO PRESENT

- Millions of computer networks communicate
- Many of the communication unsecured
- Ability to secure a computer’s data influenced by the security of every computer to which it is connected
- Growing threat of cyber attacks has increased the need for improved security

WHAT IS SECURITY?

"The quality or state of being secure—to be free from danger"

A successful organization should have multiple layers of security in place:

- Physical security
- Personal security
- Operations security
- Communications security
- Network security
- Information security

WHAT IS SECURITY?

•The protection of information and its critical elements, including systems and hardware that use, store, and transmit that information

• Necessary tools: policy, awareness, training, education, technology

• C.I.A. triangle

• Was standard based on confidentiality, integrity, and availability
• Now expanded into list of critical characteristics of information

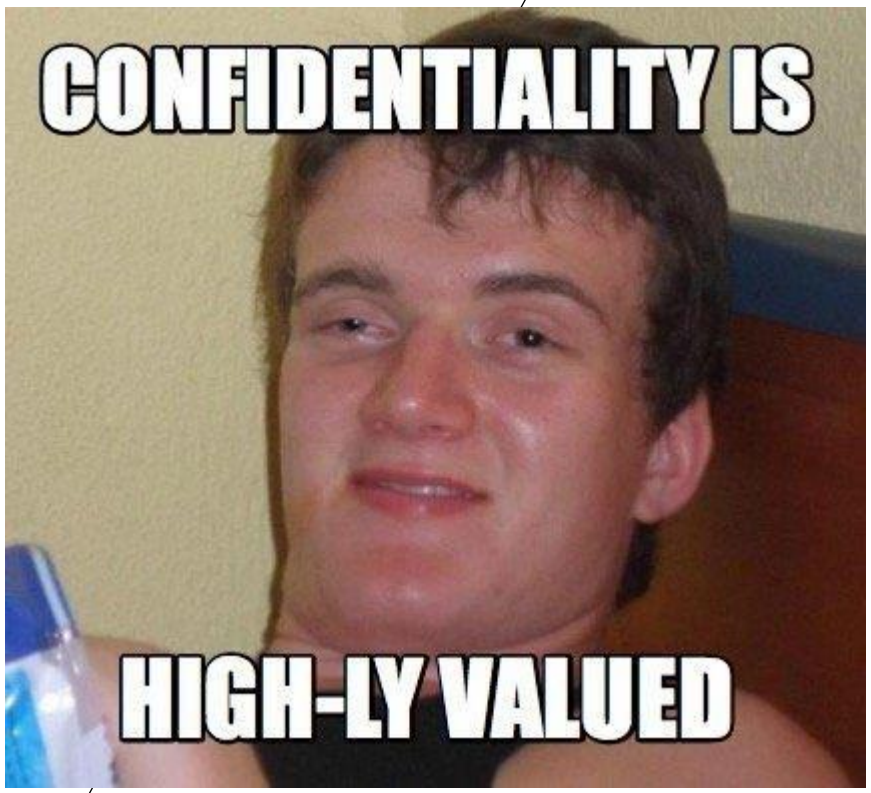
CIA TRIANGLE

In the information security (InfoSec) community, **“CIA”** has nothing to do with a certain well-recognized US intelligence agency. These three letters stand for confidentiality, integrity, and availability, otherwise known as the CIA triad.

The CIA triad is so foundational to information security that anytime data is leaked, a system is attacked, a user takes a phishing bait, an account is hijacked, a website is maliciously taken down, or any number of other security incidents occur, you can be certain that one or more of these principles has been violated.

CIA TRIANGLE (CONFIDENTIALITY)

Confidentiality refers to an organization's efforts to keep their data private or secret. In practice, it's about controlling access to data to prevent unauthorized disclosure. Typically, this involves ensuring that only those who are authorized have access to specific assets and that those who are unauthorized are actively prevented from obtaining access



<u>Examples:</u>

- Password
- Address
- Name
- Credit Cards
- Salary

CIA TRIANGLE (INTEGRITY)

In everyday usage, integrity refers to the quality of something being whole or complete. In InfoSec, integrity is about ensuring that data has not been tampered with and, therefore, can be trusted. It is correct, authentic, and reliable.

Examples:

- Encryption
- Digital Signatures

CIA TRIANGLE (AVAILABILITY)

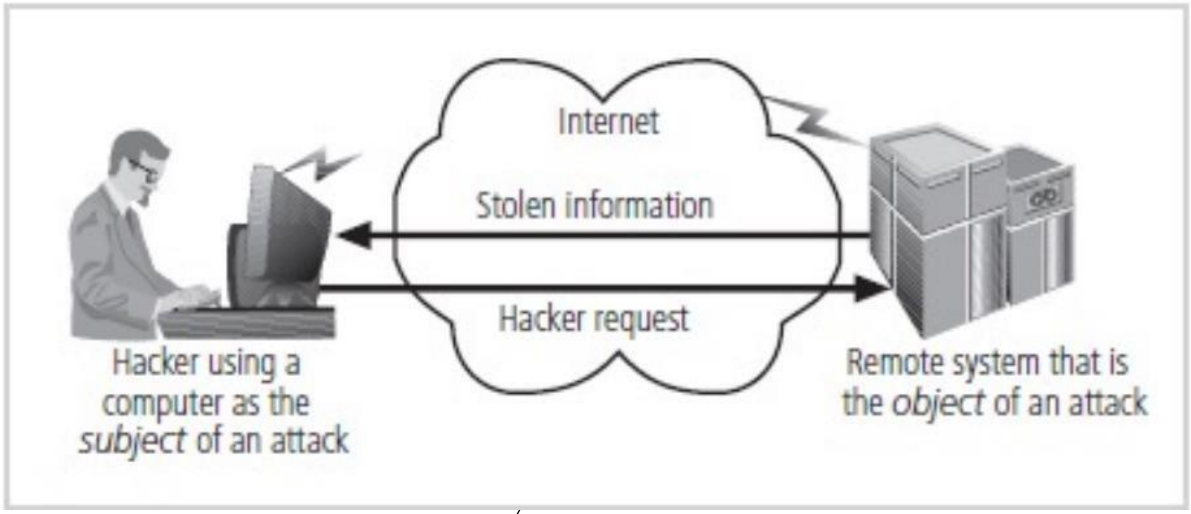
Systems, applications, and data are of little value to an organization and its customers if they are not accessible when authorized users need them. Quite simply, availability means that networks, systems, and applications are up and running. It ensures that authorized users have timely, reliable access to resources when they are needed.

Examples:

- Applications

KEY INFORMATION SECURITY CONCEPTS

- Computer can be subject of an attack
- Computer can be the object of an attack
- When the subject of an attack
- Computer is used as an active tool to conduct attack
- When the object of an attack
- Computer is the entity being attacked



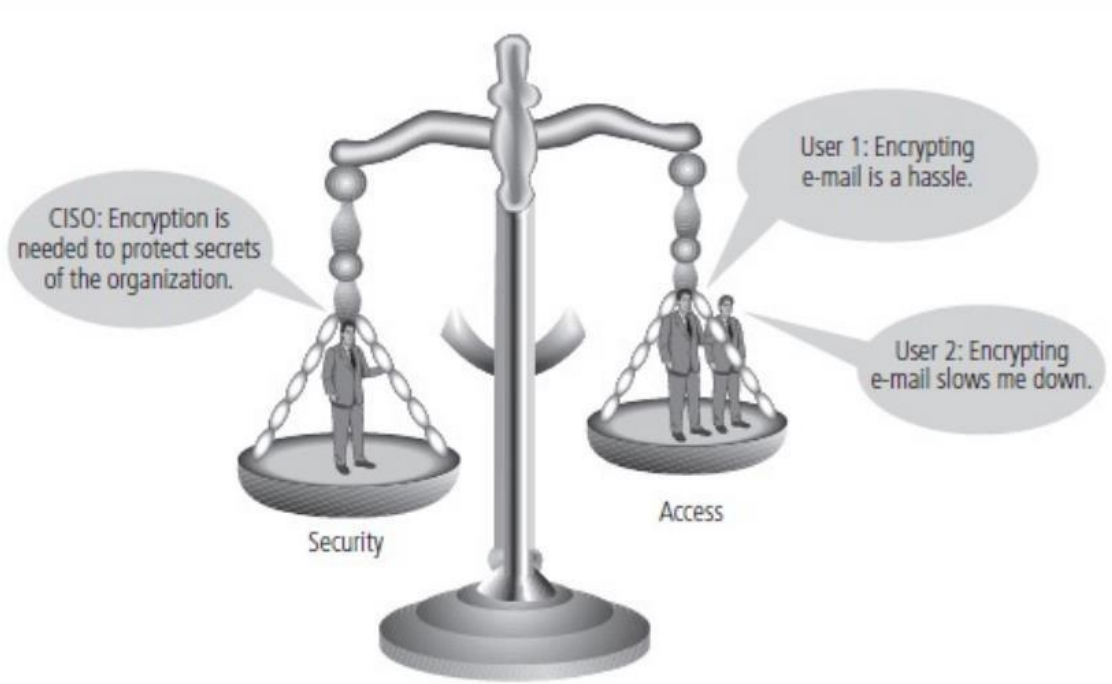
BALANCING INFORMATION SECURITY AND ACCESS

- Impossible to obtain perfect security
- Process, not an absolute
- Security should be considered balance between

protection and availability

- Must allow reasonable access, yet protect

against threats



REAL LIFE CYBER SECURITY NEWS

Porn – Tagging Scam

MALICIOUS TAGGING ❗

Sa lahat po ng mata-tag at mame-mention po ng gantong mga porn links pls po wag niyo pong bubuksan, isa 'to sa mga patibong para ma hack account mo. Kapag na click mo 'to may makikita kang update kung gusto mo talagang panoorin at siguro dahil sa gusto nga panoorin na click yung update then dun na maha-hack account mo.

Kung makikita niyo pa sa video na galing sa acc. ko yung iba sa kanila hindi ko kilala o friend sa facebook may isang babae na friend ko sa facebook nag mention din sakin at nag-chat ako since marami na ngang victim, sabi niya hindi daw siya nag mention niyan dahil hindi daw niya magagawa at siya daw yung name-mention sa ganyan. I ask kung na click ba niya yung link and she said "yes."

Kung ma-mention man kayo dito i report niyo or block para safe account niyo, pwede niyo din i click sa settings kung sino lang pwedeng makapag mention sa inyo. So yun lang keep safe, aware lang ako and paki-kalat itong informatiom na 'to dahil napaka delikado nito lalo na't andito sa acc. natin yung mga privacy natin.

FREEMAN CEBU BUSINESS

Cybersecurity skills gap still a challenge for Philippines

Ehda M. Dagooc - The Freeman ⓘ

August 22, 2024 | 12:00am

CEBU, Philippines — More companies in the Philippines continue to face difficulties in hiring cybersecurity professionals, as 77 percent of organizations indicated that the cybersecurity skills shortage creates additional risks.

According to the report released by global cybersecurity firm Fortinet, an estimated 4 million professionals are needed to fill the growing cybersecurity workforce gap.

Organizations are attributing more breaches to a lack of cyber skills.

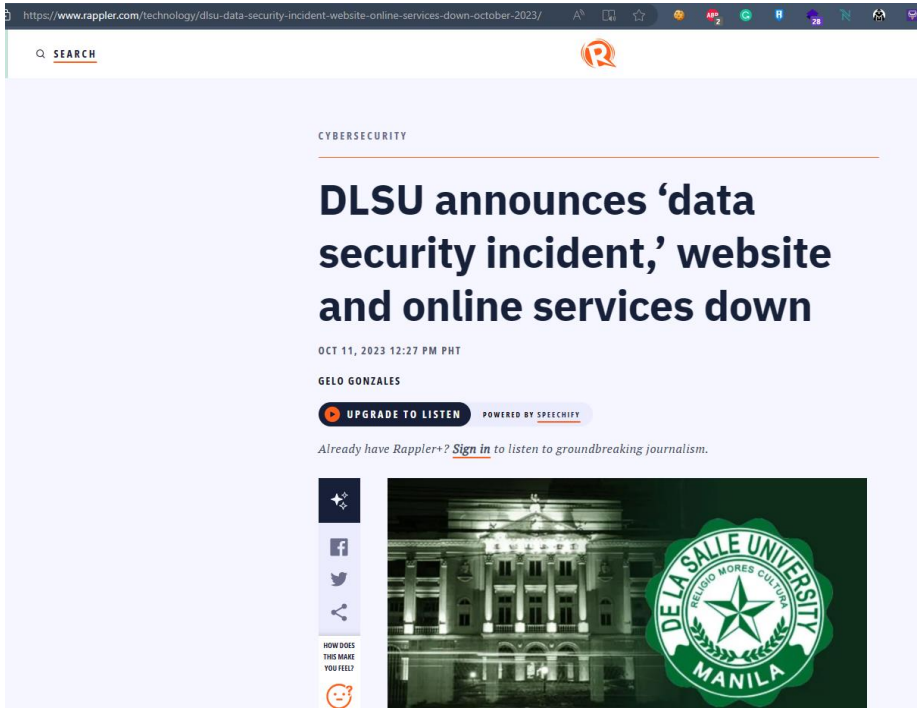
In the past year, for instance, 94 percent of organizational leaders in the Philippines said they experienced a breach that they can partially attribute to a lack of cyber skills, up from 92percent in the 2023 report.

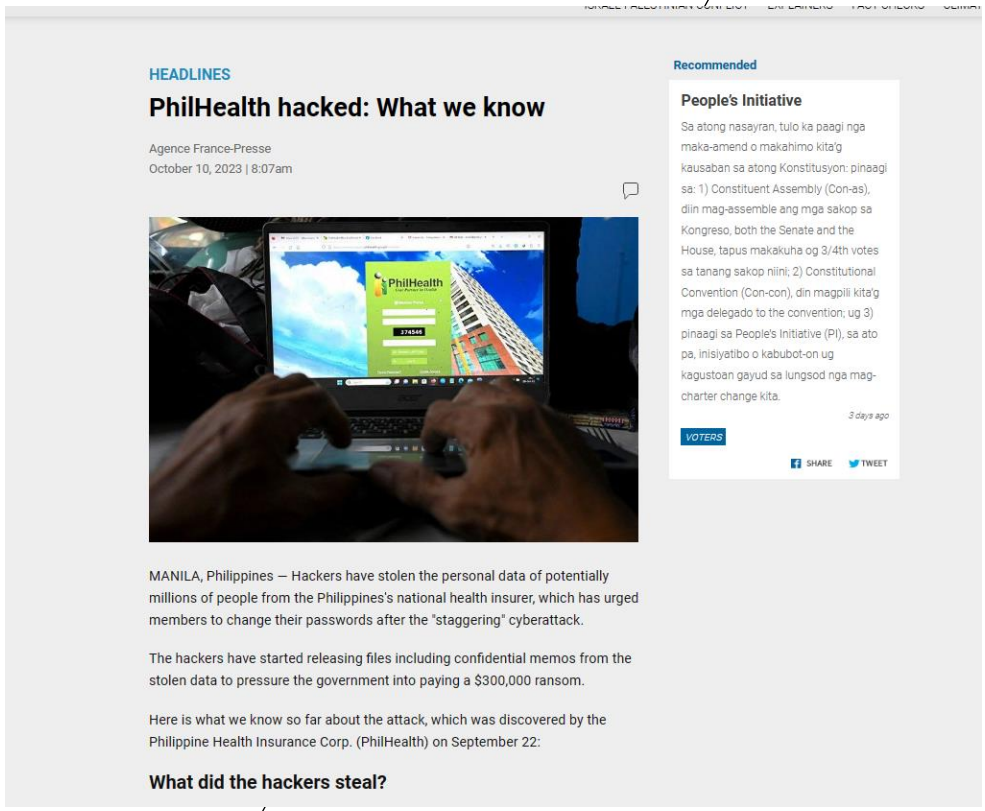
Breaches have a variety of repercussions, ranging from financial to reputational challenges.

This year's survey revealed that corporate leaders are increasingly being held accountable for cyber incidents, with 62 percent of respondents noting that directors or executives have faced fines, jail time, loss of position, or loss of employment following a cyberattack.

https://web.facebook.com/RealTalkDarbs/videos/837611528092574/

REAL LIFE CYBER SECURITY NEWS

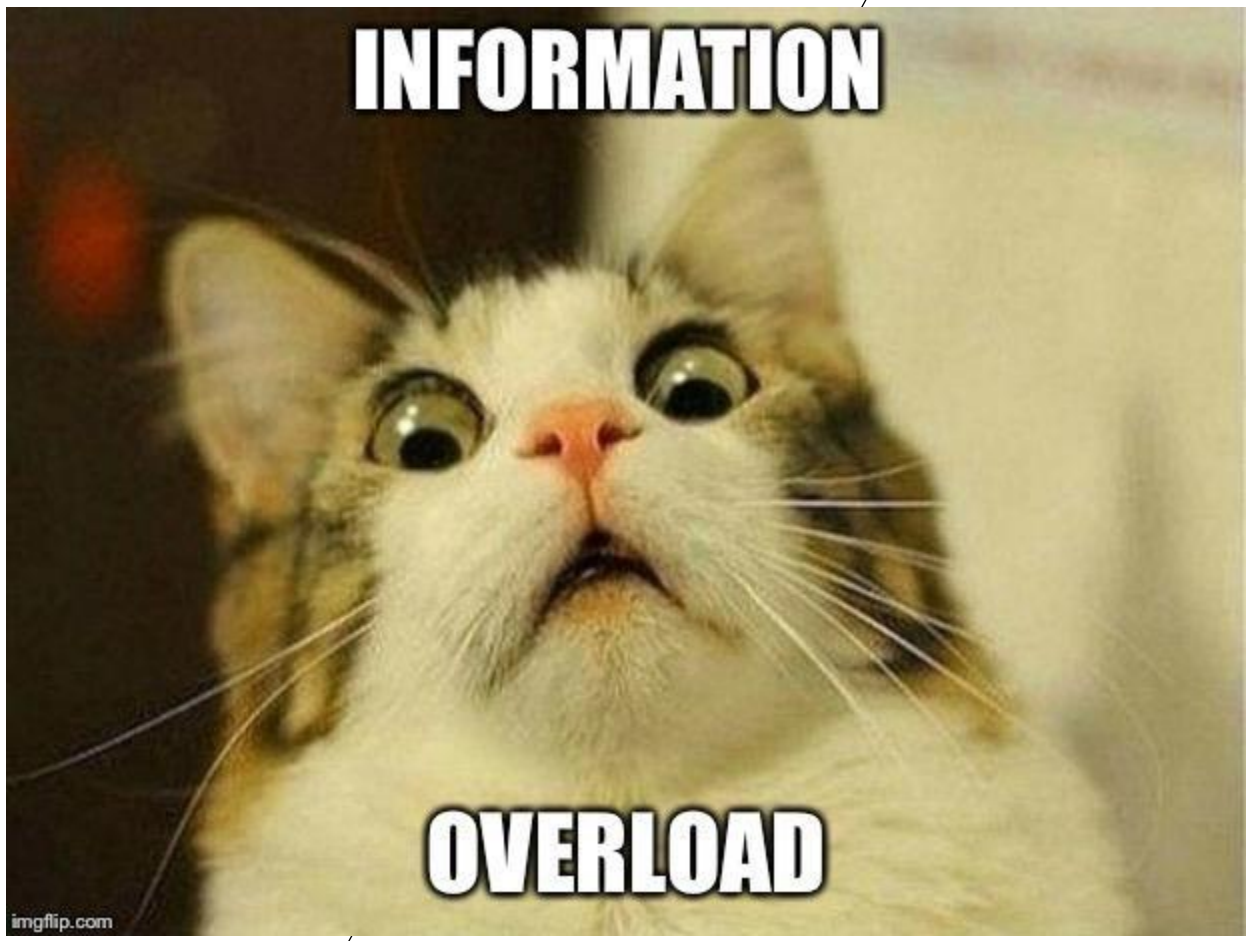




HOW TO MANAGE INFORMATION SECURITY?

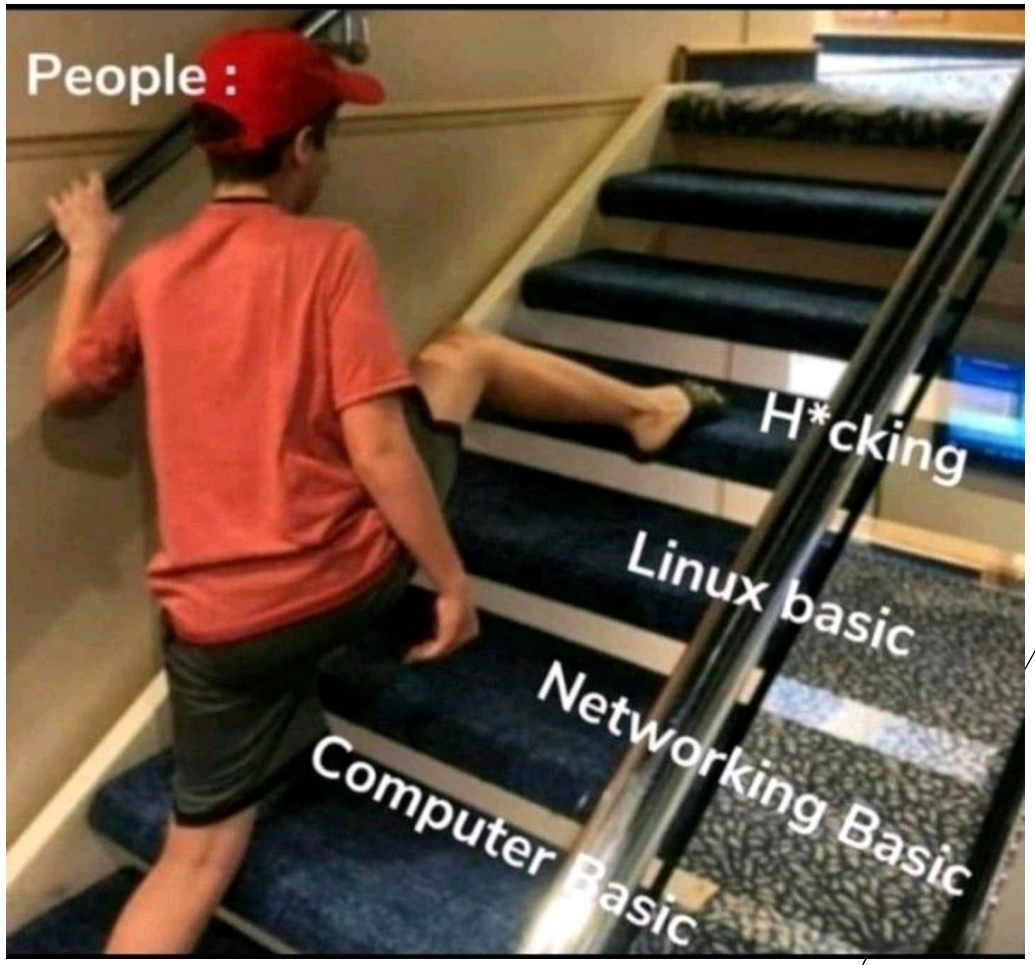
Examples of changes in input which require adaptation of the process are:

- Changes in business demands
- Organizational changes, mergers, acquisitions
- Changes in tasks or the importance of tasks
- Physical alterations, e.g. after relocating business premises
- Environmental alterations
- Changes in the assessment of the IT used
- Changes in legislation
- Changers in hardware and/or software
- Changes in threats
- The introduction of new technology
- Ageing or obsolete technology



SO, WHAT WILL BE MY FUNCTION HERE IN INFORMATION SECURITY INCASE I WANT TO PURSUE THIS SPECIALIZATION?

WELL, YOU THOUGHT CYBERSECURITY/INFOSEC IS ALL ABOUT..

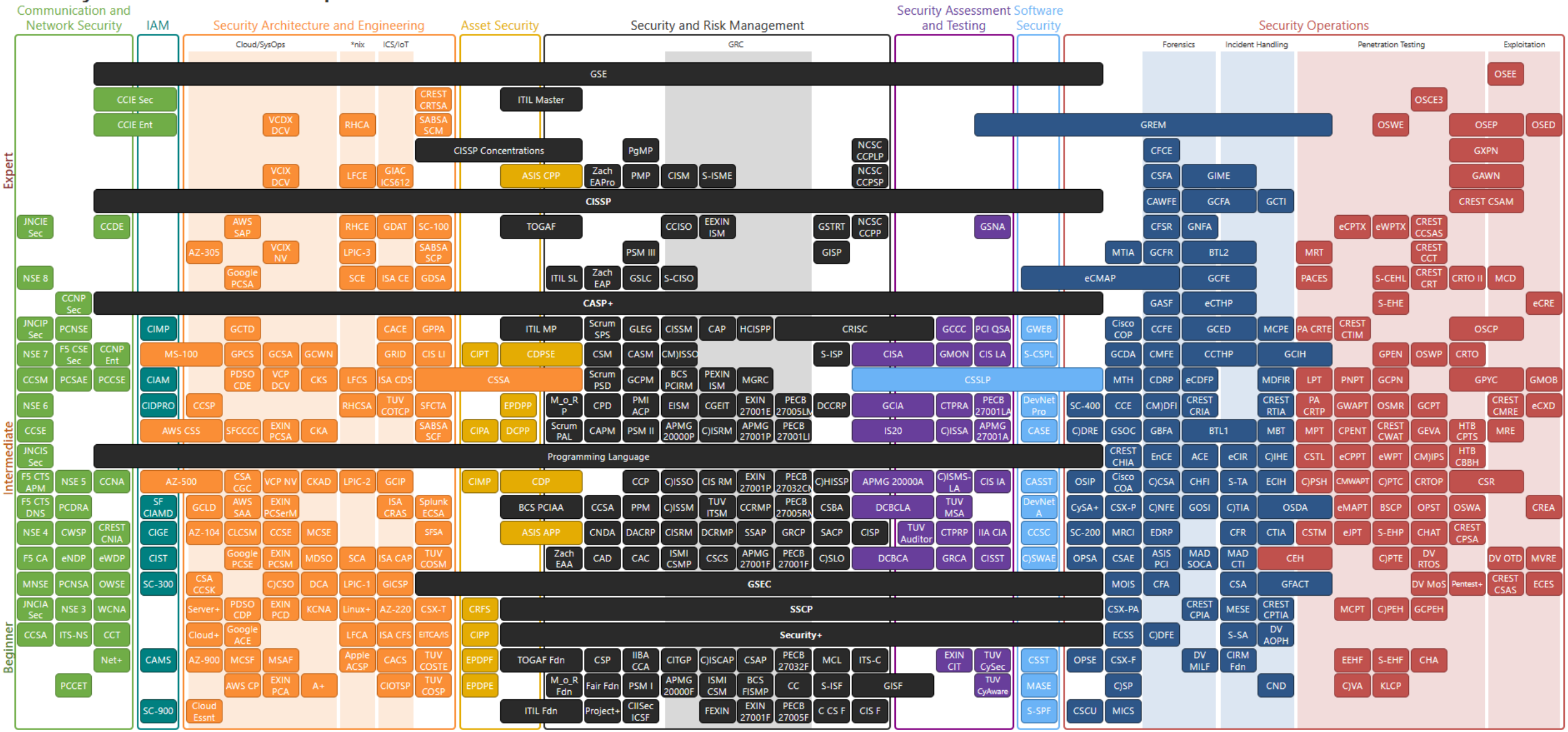


SIR…. HOW DO I START?

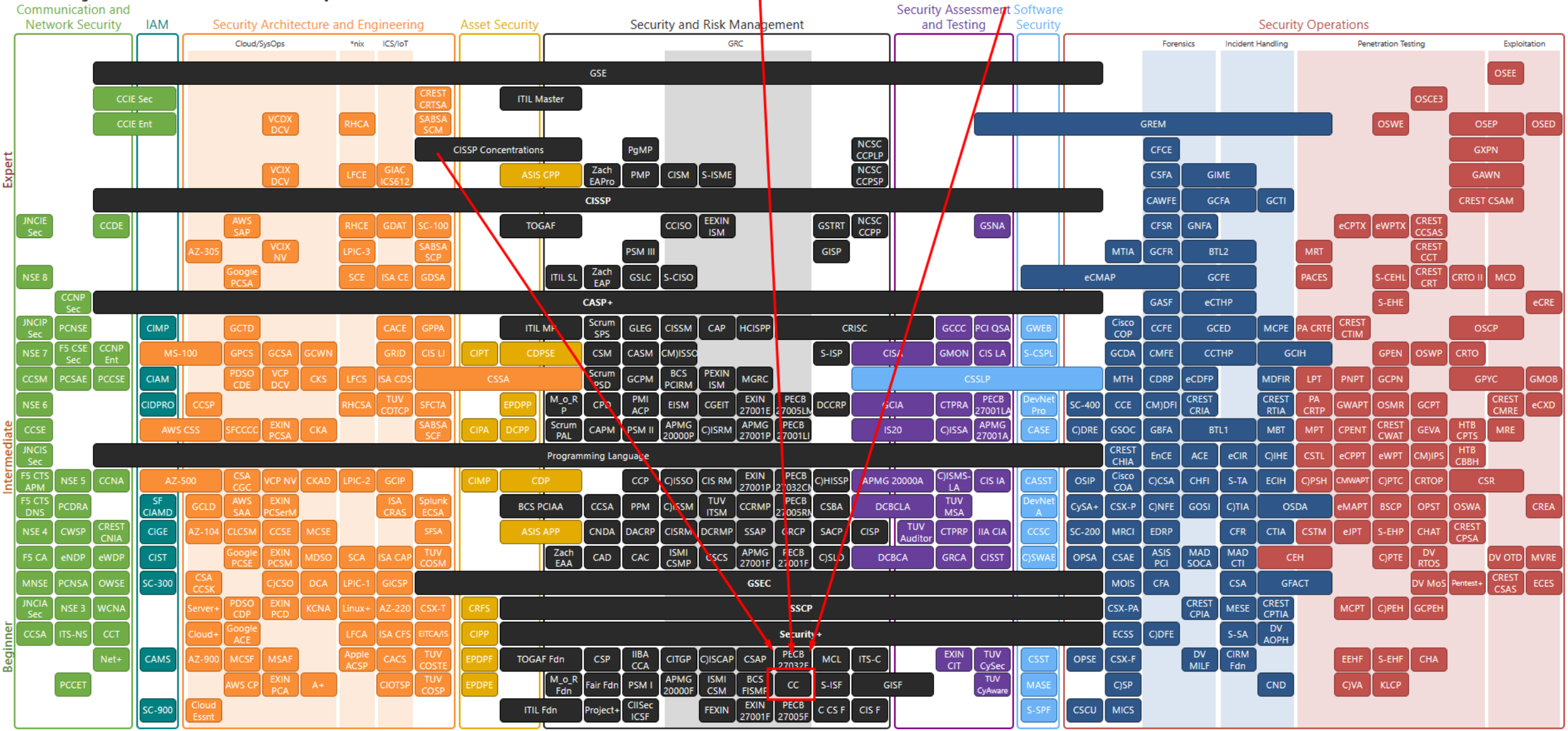
ANSWER: Take this course SERIOUSLY!

“SIR…. HOW ABOUT CERTIFICATIONS?”

Security Certification Roadmap



Security Certification Roadmap



473 certifications listed | January 2023

“WHY ISC2 Certified in Cybersecurity **CC**?”

https://www.isc2.org/landing/1mcc

About Certified in Cybersecurity Certification

Certified in Cybersecurity (CC) will prove to employers you have the foundational knowledge, skills and abilities necessary for an entry- or junior-level cybersecurity role. It will signal your understanding of fundamental security best practices, policies and procedures, as well as your willingness and ability to learn more and grow on the job.

There are five domains covered on the exam.

- Security Principles
- Business Continuity (BC), Disaster Recovery (DR) & Incident Response Concepts
- Access Controls Concepts
- Network Security
- Security Operations

Experience Requirements

There are no specific prerequisites to take the exam. It is recommended that candidates have basic information technology (IT) knowledge. No work experience in cybersecurity or any formal educational diploma/degree is required. The next step in the candidate’s career would drive to earning ISC2 expert-level certifications, which require experience in the field.

“WHY ISC2 Certified in Cybersecurity **CC**?”

CC Examination Information

Length of exam	2 hours
Number of items	100
Item format	Multiple choice
Passing grade	700 out of 1000 points
Exam availability	English, Chinese, Japanese, Korean, German, Spanish
Testing center	Pearson VUE Testing Center

CC Examination Weights

Domains	Average Weight
1. Security Principles	26%
2. Business Continuity (BC), Disaster Recovery (DR) & Incident Response Concepts	10%
3. Access Controls Concepts	22%
4. Network Security	24%
5. Security Operations	18%
Total	**100%**

- MisNET Exam Center (Makati)
- PearsonVue (Gil puyat)

“WHY ISC2 Certified in Cybersecurity **CC**?”

This badge was issued to KEINAZ DOMINGO on December 02, 2022
Expires on December 31, 2025

Verify Celebrate

ISC2

CC SM

Certified in Cybersecurity (CC)

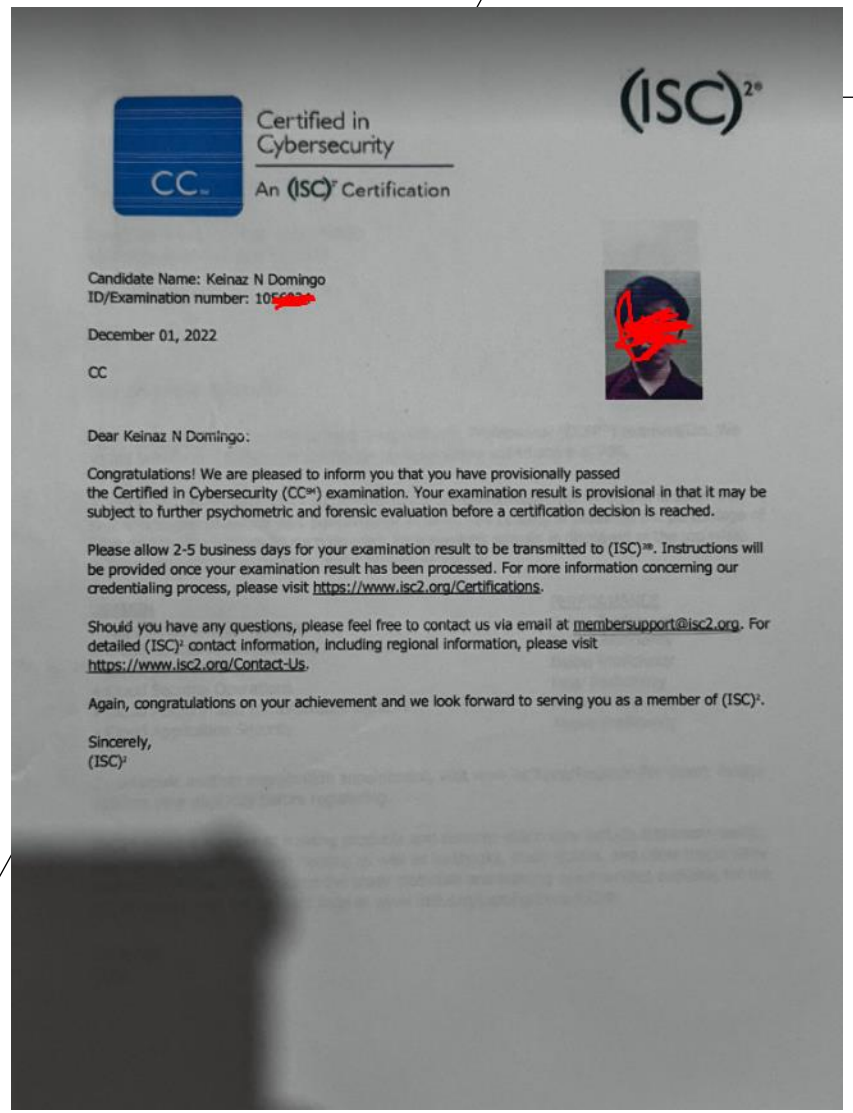
Issued by ISC2

The vendor-neutral CC credential starts newcomers on their path to advanced cybersecurity certifications and future leadership roles. It proves to organizations that newly certified team members understand fundamental security principles and operations, network security and access controls and that they have the skills to meet and exceed performance standards in their beginning roles. All this allows organizations to build a stronger line of defense.

Learn more

VOUCHER CODE:

CC1M12312024



CC

Certified in Cybersecurity

An (ISC)² Certification

(ISC)²

Candidate Name: Keinaz N Domingo
ID/Examination number: 10[redacted]

December 01, 2022

CC

Dear Keinaz N Domingo:

Congratulations! We are pleased to inform you that you have provisionally passed the Certified in Cybersecurity (CC℠) examination. Your examination result is provisional in that it may be subject to further psychometric and forensic evaluation before a certification decision is reached.

Please allow 2-5 business days for your examination result to be transmitted to (ISC)². Instructions will be provided once your examination result has been processed. For more information concerning our credentialing process, please visit https://www.isc2.org/Certifications.

Should you have any questions, please feel free to contact us via email at membersupport@isc2.org. For detailed (ISC)² contact information, including regional information, please visit https://www.isc2.org/Contact-Us.

Again, congratulations on your achievement and we look forward to serving you as a member of (ISC)².

Sincerely,
(ISC)²

“How to Enroll?”

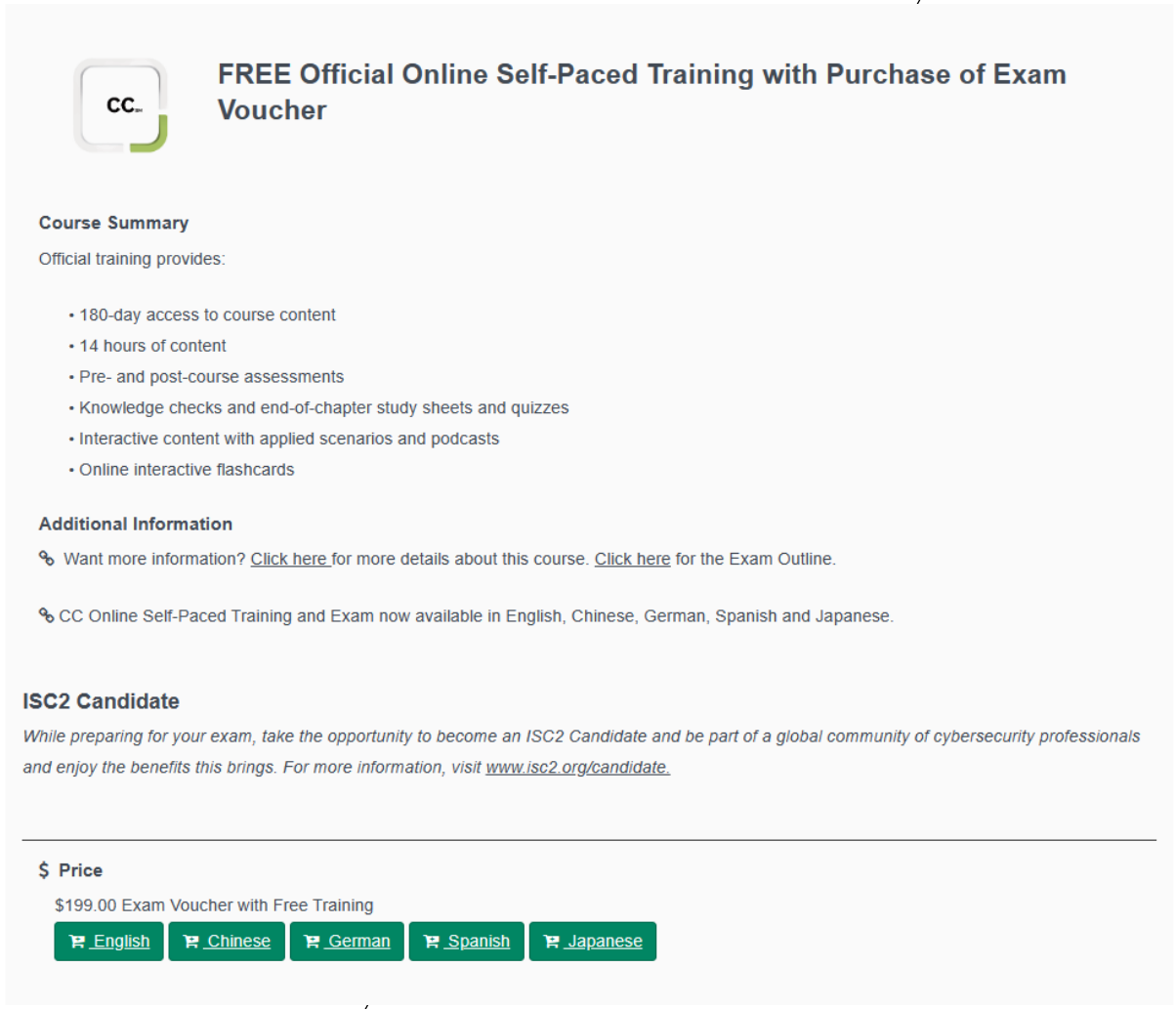
- Create an account with Pearson Vue, Select the certification: CC: Certified in Cybersecurity
- Select your testing location and schedule your exam.
- Enter the Voucher and click apply. Your total will automatically update to $0.

Free Self Phased Training:

https://enroll.isc2.org/product?catalog=CC-SPT-EXM-VOUCHER

Video for Step-by-step tutorial:

https://www.youtube.com/watch?si=2R7UZKyHtdPfC4i7&v=Tf6zLqr3Giw&feature=youtu.be



Text / Materials / References:

- **Text / Materials / References:**

  - Genung, J., & Bennett, S. (2023). CC Certified in Cybersecurity All-in-One Exam Guide. Edition. Publisher. ISBN 978-1265203818
  - International Organization for Standardization. (2022). ISO/IEC 27001:2022, Third Edition: Information security, cybersecurity and privacy protection - Information security management systems - Requirements. Paperback edition.
  - Republic of the Philippines. (2012). Data Privacy Act of 2012 (Republic Act No. 10173). (https://www.officialgazette.gov.ph/2012/08/15/republic-act-no-10173/)
  - Shelley, J., & Gibson, D. (2023). CompTIA Security+ Get Certified Get Ahead: SY0-701 Study Guide. ISBN 979-8988984801.
  - White, R. (2023). Cisco Certified Support Technician CCST Networking 100-150 Official Cert Guide. 1st Edition. ISBN 978-0138213428.
  - NIST Special Publications (http://csrc.nist.gov/publications/PubsSPs.html)
  - SP 800-137: Information Security Continuous Monitoring for Federal Information Systems and Organizations, September 2011
  - SP 800-128: Guide for Security-Focused Configuration Management of Information Systems, August 2011
  - SP 800-61 Rev 2.: Computer Security Incident Handling Guide, August 2012
  - SP 800-30: Risk Management Guide for Information Technology Systems, January 2002
  - SP 800-27: Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
  - SP 800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems

Course Summary:

BONUS CHALLENGE BY SIR NAZ ☺

IF YOU PASSED **CERTIFIED IN CYBERSECURITY** BEFORE END OF THE TERM.

YOU WILL RECEIVE

+3 up!

Ex: current final grade **2.5**, automatic will receive **4.0**

REQUIREMENTS:

- PASS CC
- TAKE SELFIE WITH THE TRAINING CENTER
- SEND ME THE ID NUMBER OF EXAM (FOR AUTHENTICATION)

GOING BACK……

“SIR, WHAT’S NEXT IF I PASSED CC?”

10 COOLEST JOBS IN CYBERSECURITY

WHY THEY MAKE A DIFFERENCE AND HOW TO QUALIFY FOR THEM

Initial Jobs With Lots of Advancement Opportunities

1 DIGITAL FORENSIC ANALYST; INVESTIGATOR

"The thrill of the hunt! It's CSI for cyber geeks! You never encounter the same crime twice."

You are the detective in the world of cybersecurity – searching computers and networks for evidence in the wake of an incident.

2 PENETRATION TESTER FOR SYSTEMS AND NETWORKS

"Be a hacker, but do it legally and get paid a lot of money!"

You look for security vulnerabilities in target systems and networks to help enterprises improve their security.

3 APPLICATION PEN TESTER

"We desperately need more of this, application security has been such a black hole for so long."

You're a programming/security wizard - testing applications before deployment so they don't present opportunities for intruders.

4 SECURITY OPERATIONS CENTER (SOC) ANALYST

"The fire ranger. Better catch the initial blaze, or there goes the forest."

With an eye for detail and anomalies, you see things most others miss. You implement active prevention, active detection, active monitoring, active response.

5 CYBER DEFENDER; SECURITY ENGINEER (ENTERPRISE AND ICS)

"A leg up on your IT and engineering buddies; talk shop with them but you are saving the world from the bad guys, too."

You implement and tune firewalls, IPS/IDS, patching, admin rights, monitoring, application white listing, more.

More Advanced Jobs - Open After A Few Years of Great Performance and Specialized Training

6 HUNTER; INCIDENT RESPONDER

"The secret agent of geekdom. You walk in and say 'OK I'll take it from here.'"

While everyone else is running around shouting, "The system's dead!," you have the sense and skills to rationally figure out why.

7 SECURITY ARCHITECT

"You get to design the solution, and not just for the perimeter."

You are creative and on top of the game both technically and in business; You design and build defensible systems and are part of an adept team.

8 SECURE SOFTWARE DEVELOPMENT MANAGER

"Coolest software developers"

You protect the development team from making errors that will allow hackers to penetrate your organization and steal data. You are a programmer, but a programmer with special powers.

9 MALWARE ANALYST / REVERSE ENGINEER

"The technical elite! Only go here if you have been called. You know who you are."

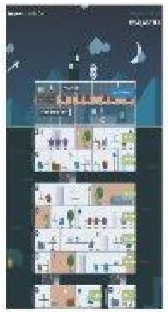
You look deep inside malicious software to understand the nature of the threat – how it got in, what flaw it exploited, and what it is trying to do or has done.

10 TECHNICAL DIRECTOR /CISO

"Making decisions; making things happen. That's coolness."

You are at the top of the tech ladder. A strategic thinker, you're hands on the design and deployment of solutions. You hold the keys to tech infrastructure.

1 CYBER FAST TRACK



"I loved CyberStart challenges - the coolest game I ever played."

"Taught me a lot; proved cybersecurity wasn't too hard to learn."

"The most fun I have had learning."

DISCOVER IF YOU HAVE THE APTITUDE

CYBERSTART: THE GAME

- No need for cyber or IT experience
- More than **250 fun challenges** protecting "real-world" bases
- **Available completely online** Everything you need is in the online Field Manual and hints.
- 19 U.S. Governors launched statewide programs for their students.

LEARN MORE AT CYBERSTART.US

2

CATAGORY/TOPIC	MODULES
Computer Hardware /Data	6
Linux and Windows	7
Networking	6
Programming	6
Common Attacks & Security	10
Others (Kali, Google, etc)	11

"We now hire cybersecurity grads only if they have hands on mastery of these foundations" (CISO, multi $billion Silicon Valley tech leader)

MASTER THE FOUNDATIONS

CYBERSTART: ESSENTIALS

- Core technologies: How they work and are attacked
- Online, hands-on immersion training, in **46 modules**
- Progress at your own pace. Quizzes and tests on each module
- **National exam** to reach silver or gold levels

3 EMPLOYER INTERVIEWS BEFORE ACCEPTANCE

GET SKILLS EMPLOYERS NEED AND A COOL JOB!

- Veterans' Academies, Women's Academies, and Open Academies
- Three SANS immersion courses and three high value GIAC certifications
- **%90 job placement** in 6 months
- Also available as Certificate in Applied Cyber Security (ACS) at SANS.edu and other accredited colleges and universities

LEARN MORE AT USCYBERACADEMY.SANS.ORG

"Completing the SANS VetSuccess Academy not only influenced my career plans, it defined them - opening doors that were inaccessible to me otherwise. In fact, being selected into the VetSuccess program was a "hitting the jackpot" moment for me."

Ed Russell, USAF (ret) NTT Security

UNITED STATES CYBER ACADEMY

More information: CyberStart.US

CONCLUSION

THANK YOU

KEINAZ N. DOMINGO