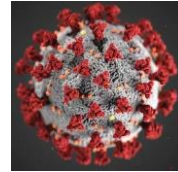


Covid-19 Messages



Here are 4 ways you can help prevent **COVID-19** (coronavirus).



Wash your hands with soap and water.



Avoid touching eyes, nose or mouth with unwashed hands.



Avoid close contact with people who are sick.



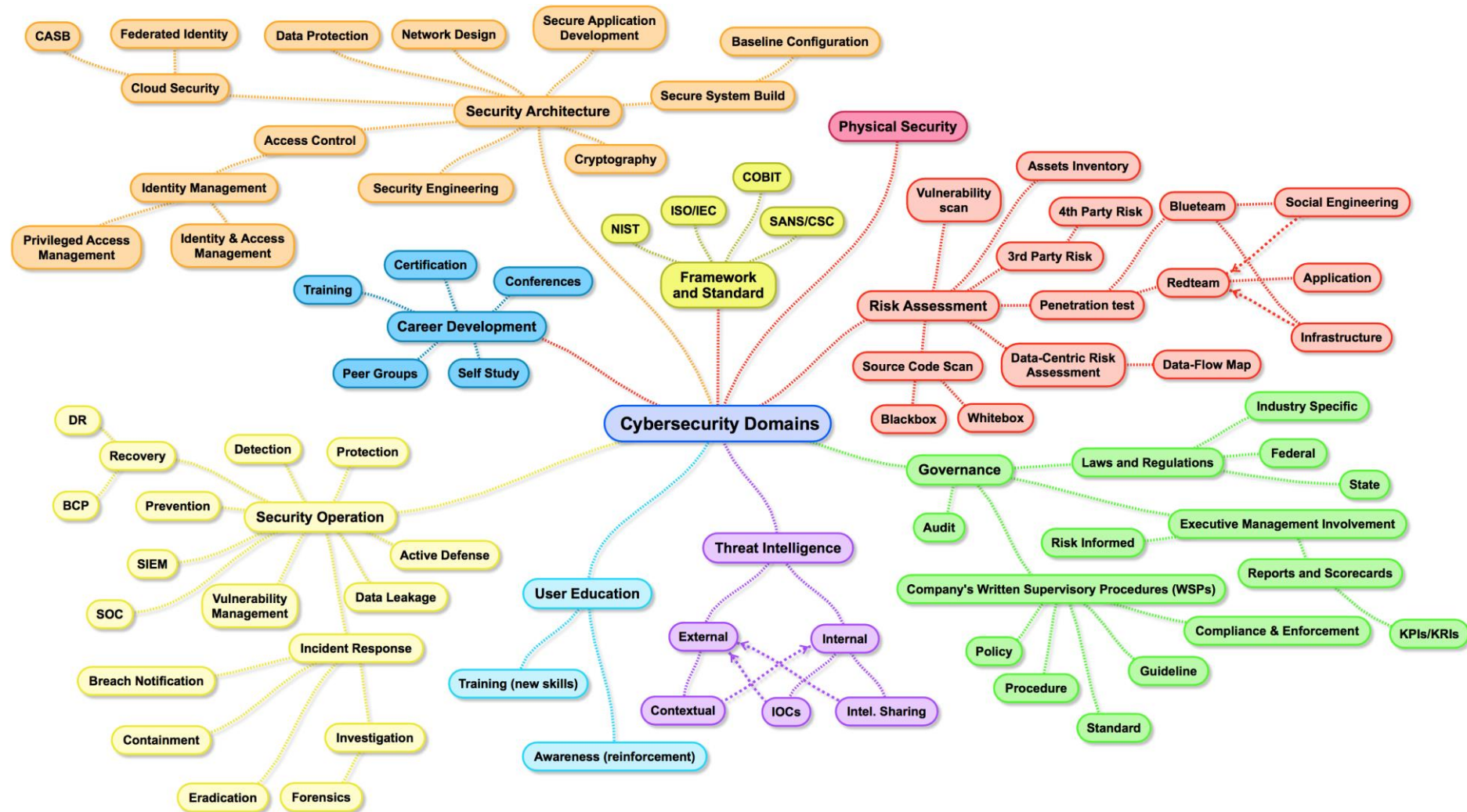
Stay home if you are sick.

Stay Home, Save Lives

Stay Safe, Save Lives



Cybersecurity World - Very Complex



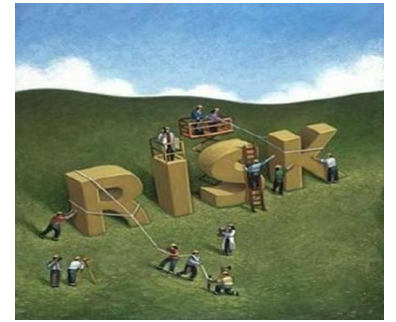
Henry Jiang

“Multiple” Issues



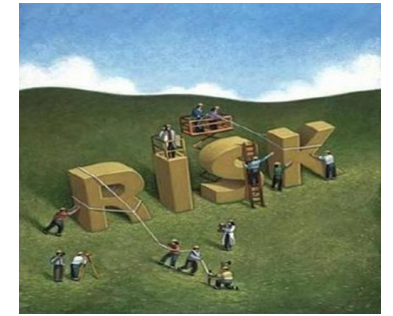
- Accelerated Digital Transformation
- Human factor (Common sense; Alertness; Motivation; Intelligence; Resistance to change, Willingness to learn; Ability to learn; Ethics; Habits (Desire Paths), etc)
- Budgets
- Corporate sizes (Large to small)
- Corporate cultures (Head office; Satellite office; Road warriors; etc)
- Industries (Finance; Industry; Welfare; Hospitality; Public; Private; etc)
- Asset values (CIA; Sensitivity; Criticality; additional Parkerian Hexad elements (Possession or Control, Authenticity, and Utility); etc)
- Physical / Logical / Virtual
- Threat agents / Threat vectors
- Experience of staff and management (Lots to none)

Homeworking/Remote Workers Access



- Minimal Risk Assessment (possibly none)
- Lack of understanding of technical issues:
 - Patch management, Use of Public WiFi, Adequacy/suitability of home office IT, VPN, Proxy, Networking, Bandwidth scalability, etc
 - Software and Hardware Do's and Don'ts
 - Poor/inappropriate access control management
 - Asset management / BYOD
- Minimum Digital Hygiene (more later)
- Lack of ownership/classification
- Data leakage potential
- Leg/Reg/Policy non-compliance (GDPR, Internet usage, etc)

Homeworking/Remote Worker Access



- Health and Safety (Comfort, Space, Lighting, Ergonomics, Office Equipment (Chairs, desks, mouse), Display Screen Assessments (DSE), etc)
- Insurance/Legal liability
- Contingency/Continuity/Recoverability
- Communication (Landline, Mobile, VOIP, IM, SMS, etc)
- Video Conferencing (Zoom, Slack, MS Teams, Skype, Google Meet, GoToMeeting, Bluejeans, Facebook Live, YouTube Live, etc)
- Lack of training: Staff; Help desks; customers; partners; suppliers
- Licensing; Contracts; NDA's; SLA's; OLA's, Asset registry; etc

Digital Hygiene



- Digital Footprint (Work, Social media, Personal Hobbies, Shopping, etc) plus multiple gadget addiction
- People naturally take uninformed risks (Dunning/Kruger)
- Permanently connected/Everything on
- Lacking inhibitions
- Gen Z/Gen Y habits
- Questionable Apps/Downloads/Websites
- Information Security Naivety



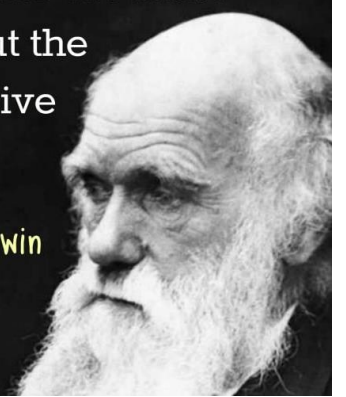
Good Digital Hygiene - A guide to staying secure in cyberspace By Ed Gelbstein (Bookboon)

Challenges – Interest, Success, and Follow-ups

- Budgets with a Sponsor
- Having the right Staff with Awareness Development skills
- Developing a Plan
 - Clear goals
 - Short/Long Term SMART objectives
 - Align with other company initiatives
 - Awareness “raising” items
 - Awareness “targeted” items
- Working with Partners/best practice innovators
- Having tools and delivery mechanisms

It is not the strongest species that survive, nor the most intelligent, but the most responsive to change.

-Charles Darwin



Challenges – Interest, Success, and Follow-ups

- Obtain visible Senior staff support and promotion
- Getting staff interested and getting buy-in
 - Making messages personal
 - Changing “normal” behaviour
- Knowing what good looks like
- Monitor and Evaluate
 - Gather meaningful metrics
 - Proving success – including evidential enthusiasm
 - Kill failures fast



“The most successful awareness programs make people aware without them realising it’s a campaign”

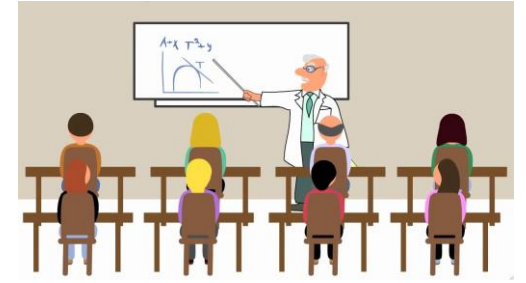
Effective Awareness Programs



- Change Behaviour
- Heighten awareness of critical topics
- Are delivered in a way that is acceptable to all the various cultures and influence a belief in the messages
- Recognise and address resistance to change
- Provide individual motivation
- Get people to accept personal responsibility



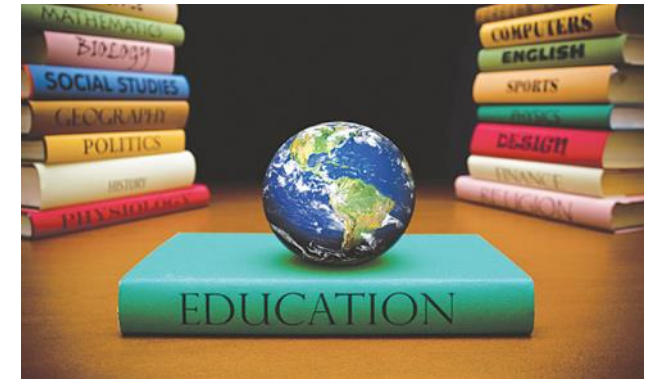
Critical Success elements



- Understanding important Policy/Rules
- Aware of current and emerging risks for home workers
- Good logical and physical access controls
- VPN/Firewalls/etc
- Malfeasant software protection
- BYOD issues
- Helpline access for advice and guidance

Success Measurement – Data Analytics

- Customer, Partner and Staff reach
- Applause Rate
- Amplification Rate/Content resonance
- Testing
- Help Desk utilisation
- Awareness landing zone monitoring
- Downloads of additional material and advice



Many Vendors offered free training for month of April and May

- 1. Microsoft - Azure certification <https://lnkd.in/g4E6FfJ>
- 2. AWS - All AWS technology <https://lnkd.in/fkcMAKg>
- 3. IBM - All IBM technology <https://lnkd.in/gR4zq2W>
- 4. Oracle University - Cloud Infrastructure and Autonomous Database <https://lnkd.in/fVBv9KT>
- 5. Fortinet - NSE1 and NSE2 <https://lnkd.in/gH7SCE9>
- 6. Palo Alto - Networks <https://lnkd.in/gfj9f6h>
- 7. Cisco - Cyber Security <https://lnkd.in/gwZBBPJ>
- 8. Qualysguard - Vulnerability management <https://lnkd.in/fMHuKc4>
- 9. Nessus - Vulnerability management <https://lnkd.in/gEvcJeh>
- 10. SAN's - cyber security <https://lnkd.in/gexceQz>
- 11. Homeland security - ICS Security <https://lnkd.in/g7G4Ebh>
- 12. Coursera - Cloud courses <https://lnkd.in/fTCXqFm>
- 13. Pluralsight - All Training <https://lnkd.in/djPvKDe>
- 14. Sololearn - All Training <https://lnkd.in/fYHT27z>

Summary



and



- Awareness Training
 - Depends on your starting point
 - Do a risk analysis and summarise the issues
 - Simple Uncomplicated Focused messages
 - Address your riskiest areas and weakest links (eat the Elephant)
- Education
 - Matters more than ever
 - Motivates
 - Maintains currency
 - Promotes understanding and ownership of issues

Questions?



Awareness Links

- <https://www.thesecuritycompany.com/>
- <https://csrc.nist.gov/Topics/Security-and-Privacy/security-programs-and-operations/awareness-training-education>
- <https://csrc.nist.gov/Projects/fissea/contests-and-awards/fissea-sate-winners>
- <https://www.wholewhale.com/tips/measure-awareness-campaigns/>
- <https://resources.infosecinstitute.com/category/enterprise/securityawareness/security-awareness-roles/security-awareness-issues-for-remote-workers/>

Extra Education Links

- <https://misti.com/infosec-events>
- <https://www.isc2.org/Resource-Center?filter=featured>
- <https://www.readynez.com/en/learning-services/>
- <https://community.checkpoint.com/t5/Training-and-Certification/Check-Point-Jump-Start-Free-video-training/td-p/73414>
- <https://www.linkedin.com/learning/cissp-cert-prep-4-communication-and-network-security-2/welcome>
- <https://tutorials.cyberaces.org/tutorials.html>

Mixed Interesting Links

- <https://www.linkedin.com/pulse/map-cybersecurity-domains-version-20-henry-jiang-ciso-cissp/>
- <https://www.isc2.org/News-and-Events/Webinars/EMEA-Webinars?commid=395138>
- <https://www.linkedin.com/learning/paths/remote-working-setting-yourself-and-your-teams-up-for-success?src=li-ghom&trk=li-gal-lls-b2c-learning-cQ420v-wfh-home&mcid=6650462232138395648>
- <https://www.qualys.com/apps/asset-inventory/>
- <https://www.comparitech.com/blog/information-security/security-remote-working/>
- <https://www.nist.gov/cyberframework>
- <https://csrc.nist.gov/publications/detail/sp/800-100/final>
- <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf>
- <https://www.infosecurity-magazine.com/news/remote-employees-content-devices/>

Collaborative Website links

- <https://www.thesasig.com/join/>
- <https://monday.com/>
- https://slack.com/intl/en-gb/?eu_nc=1

Lots of Advice and help

Changing to online teaching in a hurry? We can help

In light of COVID-19, education providers are facing a huge challenge. They need to move staff with varying levels of experience and technical confidence to online teaching quickly, while ensuring quality is maintained.

We can help you adapt to change and support your students. For guidance on online support and wellbeing, teaching and learning, assessment and learning design, take a look at our free [online teaching, learning and student support guide](#).



INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

October 2006



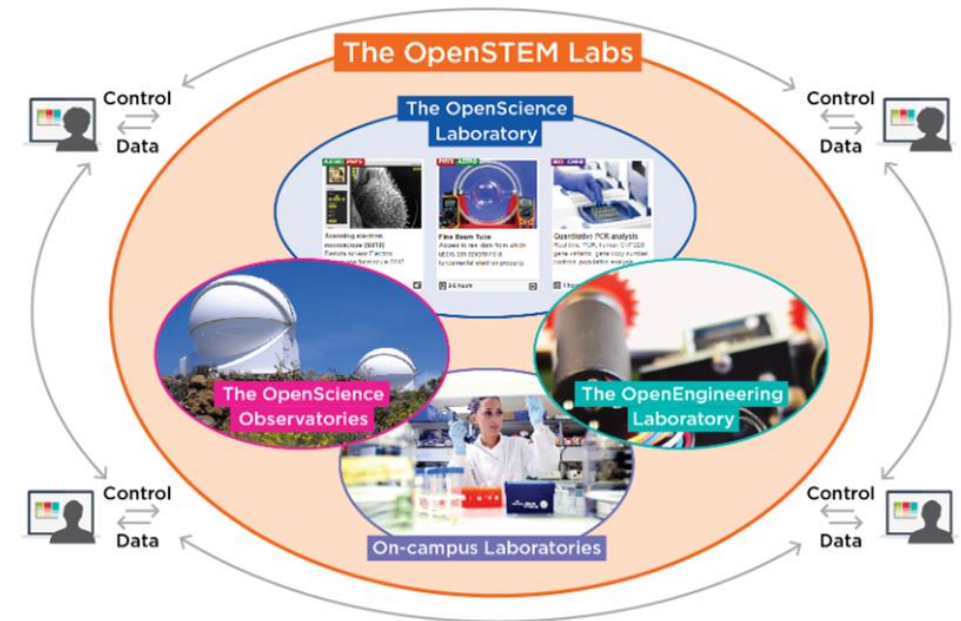
U.S. Department of Commerce
Cyber-Security Services
Technology Administration
Robert Cranston, Under Secretary of Commerce for Technology



COMPUTER SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

October 2003



Security Awareness Issues For Remote Workers

EXPLORE WITHIN SECURITY AWARENESS

Compliance Mandates	Creating Strong Passwords	Email Security Awareness
Employee Security Threats	File Sharing Security	Managing Desktop Security
Managing Physical Security	Managing Wireless Network Security	Mobile, Smartphone, and BYOD
Removable Media	Security Awareness Fundamentals	Security Awareness Roles
Security Awareness Training	Security Threats by Industry	

FISSEA - Federal Information Security Educators

- *An organization run by and for Federal government information security professionals to assist Federal agencies in strengthening their employee cybersecurity awareness and training programs*
- **Have an Annual Conference and Competitions** - FISSEA is accepting nominations for the FISSEA 2020 Cybersecurity Awareness and Training Innovator Award from March 2 – August 7, 2020
- **Free online help and assistance (and examples).**
- ***2020 Vision: Bringing the Future of Cybersecurity Awareness and Training into Focus***



<https://csrc.nist.gov/projects/federal-information-systems-security-educators-as/>

Staying **CYBERSAFE** at **HOME**

Defend yourself and your family.

Good cybersecurity hygiene is important at work and at home. Follow these tips to ensure your personal devices, information, and networks remain “cybersafe.”



When You're On the Go

- Beware of **public charging stations**—use a wall outlet
- Avoid using **public Wi-Fi networks**



Be Smart on Social Media

- **Never share personal details**, like your home address, birth date, etc.
- **Use privacy settings** to control what people see
- **Be selective** when connecting with new people

House illustration with cutaway scenes describing safe everyday usage of end-user technology.



Use Secure Networks

- **Rename your network** after purchasing a router
- **Secure your Wi-Fi** with a password
- **Turn off your wireless network** when leaving for long time periods



Keep Your Mobile Devices Safe

- **Password protect** your phone
- **Never click links** in texts from unknown senders
- **Update your device** with the latest software



Protect Your Finances

- **Set up spending and activity alerts** with your bank or credit card provider
- **Use trusted websites** when making online purchases
- **Never respond** to unsolicited requests for personal or bank information



Set Strong and Unique Passwords

- **Never re-use passwords** that were previously hacked
- **Use passphrases**—avoid dictionary words alone
- **Avoid keyboard sequences** or repeating characters (e.g., 1234, aaaa)



Look Out for Suspicious Emails

- **Report spam** using tools from your email provider
- **Avoid opening attachments** from unknown senders
- **Hover over hyperlinks** to reveal the destination before clicking

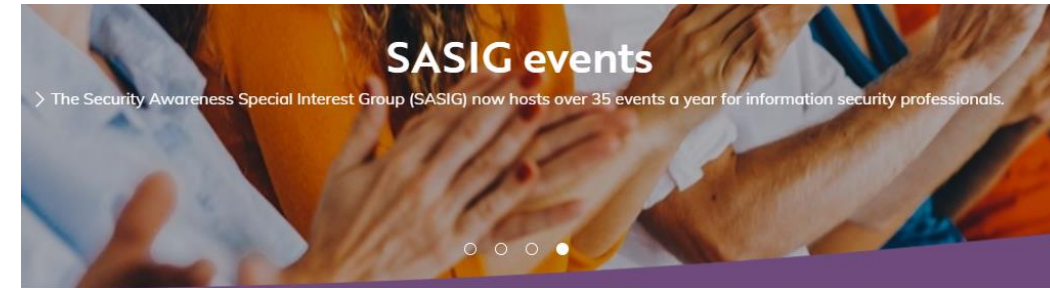
For more information, visit <https://uspscybersafe.com>. Employees can go to <https://blue.usps.gov/cyber> or <https://liteblue.usps.gov/cyber>. For questions, email cybersafecomms@usps.gov.



<https://csrc.nist.gov/CSRC/media/Events/FISSEA-32nd-Annual-Conference/documents/FISSEA%20Poster%20Winner.pdf>

The Security Company and SASIG (Security Awareness Special Interest Group)

- 30-minute interactive training session
- Webinar
- For up to 500 employees. The session will cover:
 - Current threat landscape – why attacks have increased and how they are evolving
 - Best information security practices while working from home
 - Technical tips to strengthen security while working from home
 - Practical guidance on how to stay sane in a mad world
 - Live interactive Q&A session



Help your employees work from home securely

COVID-19 has driven a sudden increase in working from home. A change likely to endure beyond the current lockdown — work has come home.

Whether you have been operating a working from home policy for years or have been thrust into it over recent weeks, it pays to review your colleagues' knowledge and ability to work securely away from the office.

Check out TSC's working from home resources which help your employees continue working in the most secure way possible. [> Learn More](#)

Online Education Examples



MISTI'S VIRTUAL CLASSROOM TRAINING

Train Without Travel

Need CPEs but can't travel? MISTI's Virtual Classroom training allows you to watch, hear and participate in our courses as if you were sitting in the classroom. All our virtual classroom seminars are delivered by expert instructors and allow you to save on time away from work and home, and your organization's budget.

[CLICK HERE TO LEARN MORE](#)



UPCOMING TRAINING

DATE	TRAINING	TYPE
MAY 13 2020	How to find Fraud and Corruption - Masterclass 1: Demystifying Fraud and Corruption and how to perform a Fraud Risk Analysis of your organisation	Webinar
MAY 18 2020	Intermediate IT Audit School	Virtual Training Only
MAY 21 2020		
JUN 1 2020	Chief Audit Executive Masterclass	Virtual Training Only
JUN 5 2020		
JUN 8 2020	Data Analytics, Continuous Auditing and Audit Automation	Virtual Training Only
JUN 12 2020		
JUN 22 2020	Information Management and CDMF Professional Certification	Virtual Training Only
JUN 26 2020		
JUN 29 2020	CyberSecurity Audit for Non-Cyber Professionals	Virtual Training Only
JUL 3 2020		

BSc (Honours) Cyber Security

Our cyber security degree combines three sought after streams of computing: networking, cyber security and digital forensics. It gives you a thorough understanding of socio-technical systems and skills to prevent or respond to cyber security incidents. And develops your ability to critically analyse and apply digital solutions to security examination and digital forensic investigations. This includes an appreciation of tools, techniques and legal requirements. The degree programme, with its well-balanced theory and practice, has a strong technical focus. You'll develop your understanding of how networked cyber systems function and how they might be abused. The course centres around the relationship between technology, people, processes, the physical environment and cyber security. You'll be able to pursue a wide array of career pathways within the public, private and charity sectors.

Key features of the course

- Curriculum aligned with The Cyber Security Body of Knowledge (CyBOK) and with the Institute of Information Security Professionals (IISP) framework.
- The cyber security skills gap and shortage of cyber security professionals globally will increase your employability.
- Develop your understanding of how cyber security fits into business and commerce through applied learning.
- Demonstrate your knowledge and skills through a substantial cyber security-related independent project.



Build for Your Future with a Concentrated Skill Set

Save More than 50% for a Limited Time

Advance Your Career with a CISSP Concentration

We're always here to support your next professional challenge. To prove it, here's an excellent opportunity to build for the future with a concentrated skill set in information security architecture, engineering or management.

For a limited time, take advantage of a [virtual training and exam voucher bundle](#) that brings unparalleled confidence and value to your CISSP-ISSAP, CISSP-ISSEP or CISSP-ISSMP journey. Pursue any concentration for \$1,398 – a savings of more than 50% off Official (ISC)² Online Self-Paced Training!

Expert Learning Anytime, Anywhere

Official (ISC)² Online Self-Paced Training gives you the freedom to move ahead on your schedule. Throughout your learning experience, you have on-

Lots of online training available

MIS Training

UPCOMING TRAINING

MAY 13 2020	How to find Fraud and Corruption - Masterclass 1: Demystifying Fraud and Corruption and how to perform a Fraud Risk Analysis of your organisation Webinar	MAY 18 2020	MAY 21 2020	Intermediate IT Audit School Virtual Training Only	
JUN 1 2020	JUN 5 2020	Chief Audit Executive Masterclass Virtual Training Only	JUN 8 2020	JUN 12 2020	Data Analytics, Continuous Auditing and Audit Automation Virtual Training Only
JUN 22 2020	JUN 26 2020	Information Management and CDMF Professional Certification Virtual Training Only	JUN 29 2020	JUL 3 2020	CyberSecurity Audit for Non-Cyber Professionals Virtual Training Only

Readynez

PUBLIC SCHEDULE

TAILORMADE TRAINING

BLENDED LEARNING

CAREER MOVER

TALENT PROGRAMMES

SKILLS RECRUITMENT

READYNEZ TRACKS

READYNEZ INSIGHTS

ISC2



Guides

CISSP Ultimate Guide



Guides

CCSP Ultimate Guide



Guides

Enterprise Solutions Catalog



#Books

The (ISC)² Cybersecurity Lexicon



Research

Hiring Top Cybersecurity Talent



Research

The Multicultural Cybersecurity Workforce



Videos

2018 (ISC)² Security Congress Recap



Videos

What is the Associate of (ISC)² Designation?

NIST



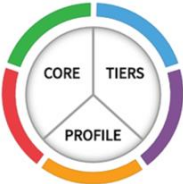
RECOVER
IDENTIFY
PROTECT
DETECT
RESPOND

FRAMEWORK

Framework Version 1.1

The Cybersecurity Framework is ready to download.

[Learn More](#)



CORE
TIERS
PROFILE

New to Framework

This voluntary Framework consists of standards, guidelines and best practices to manage cybersecurity risk.

[Learn More](#)



Online Learning

Intro material for new Framework users to implementation guidance for more advanced Framework users.

[Learn More](#)

SANS



Streaming Tutorials

1. Introduction to Operating Systems

- Linux
 - [VMware Installation and Configuration](#)
 - [OS Background & Building the Linux VM](#)
 - [Core Commands](#)
 - [Users and Groups](#)
 - [Applications and Services](#)
 - [Files and Permissions](#)
 - [Installing Software](#)
- Windows
 - [Windows Virtual Machine Installation](#)
 - [Updating Windows](#)
 - [Command Line Basics](#)
 - [File System](#)
 - [Users and Groups](#)
 - [Policies and Credential Storage](#)
 - [Registry](#)
 - [Networking and Sharing](#)
 - [Services and Processes](#)

2. Networking

- [Introduction and Layer 1](#)
- [Layer 2 - Data Link](#)
- [Layer 3 - Network, Part 1: Addressing & Masking](#)
- [Layer 3 - Network, Part 2: Routing](#)

Linked-In and SANS Cyber Aces Online Tutorials

- A months FREE online training at Linked-In

SANS

Streaming Tutorials

1. Introduction to Operating Systems

- Linux
 - [VMware Installation and Configuration](#)
 - [OS Background & Building the Linux VM](#)
 - [Core Commands](#)
 - [Users and Groups](#)
 - [Applications and Services](#)
 - [Files and Permissions](#)
 - [Installing Software](#)

- Windows
 - [Windows Virtual Machine Installation](#)
 - [Updating Windows](#)
 - [Command Line Basics](#)
 - [File System](#)
 - [Users and Groups](#)
 - [Policies and Credential Storage](#)
 - [Registry](#)
 - [Networking and Sharing](#)
 - [Services and Processes](#)

2. Networking

- [Introduction and Layer 1](#)
- [Layer 2 - Data Link](#)
- [Layer 3 - Network Part 1: Addressing & Masking](#)
- [Layer 3 - Network Part 2: Routing](#)

Top picks for Charles V

- COURSE**
How to Create a Perfect Elevator Pitch
By: CareerCake
12m
- COURSE**
Creating a Security Awareness Program
By: Lauren Zink
1h 1m
- COURSE**
CCSP Cert Prep: 2 Cloud Data Security
By: Mike Chapple
2h 4m
- COURSE**
Penetration Testing: Advanced Enumeration
By: Malcolm Shore
1h 33m
- COURSE**
Photoshop: Advanced Studio Portrait
By: Chris Orwig
1h 33m

Most liked on LinkedIn Learning

- COURSE**
Additive Manufacturing for Business
2h 10m
- COURSE**
Leadership Stories: 5-Minute Lessons in Leading People
3h 6m
- COURSE**
Chair Work: Yoga Fitness and Stretching at Your Desk
33m
- COURSE**
C++ Game Programming 1
By: John Horton
6h 5m
- COURSE**
Learning Java
By: Kathryn Hoot
1h 33m

<https://www.linkedin.com/learning/me>

<https://tutorials.cyberaces.org/tutorials.html>

