Introduction to Cybersecurity Practitioner

19 November 2020
Agenda

6.30pm   Agenda and House Rules
6.35pm   Background to CSX
6.40pm   Speaker Introductions
6.50pm   Panel Questions
7.10pm   Questions from Attendees
7.20pm   Poll
7.25pm   Next Steps
7.30pm   Close
House Rules

• Questions welcome! Q&A available at the bottom of the Zoom screen
• Look out for the quiz and poll questions
• Small prize for the best quiz score
• Chat function available for discussion - please keep it civil
• 1 CPE awarded for ISACA members, to be awarded after the event
Background to CSX

https://www.youtube.com/watch?v=1SzO_KiGziA
Background to CSX - ISACA Cybersecurity Certifications

Cybersecurity Practitioner: A comprehensive certification showing globally validated cybersecurity skills and the ability to resolve network and host cybersecurity issues as a cyber 'first responder'.

CSX Cybersecurity Fundamentals: Understanding the principles of cybersecurity and the role of cybersecurity professionals in protecting enterprise data.

Cybersecurity Nexus: Real-world skills, covering advanced exploitation, forensics, analysis, system configuration, packet analysis, penetration testing, technical foundations and vulnerability/exploitation.

Cybersecurity Audit: Provides audit/assurance professionals with the knowledge for audits, and gives IT risk professionals an understanding of cyber-related risks and mitigating controls.

Certified Information Systems Manager: Show expertise in information security governance, program development and management, incident management and risk management.
Speaker Introductions

Alwin Pandey CISA, CRISC, CDPSE, CSX-P

Kevin Murphy CISM, CRISC, CSX-P
Quiz Question 1

According to the NIST cybersecurity framework, which of the following are considered key functions necessary for the protection of digital assets?

(choose three)

- Encrypt
- Protect
- Investigate
- Recover
- Identify
Panel Questions

1. When you chose CSX-P, how much time did you give yourself to prepare?
2. What sort of support and encouragement did you seek from your employer?
3. After you hit the “buy” button, what aids were you given to help with studying, training and preparation?
4. What other resources did you look into to build up your knowledge and awareness? Did you seek any help from colleagues or technical specialists?
5. Did you follow a particular pattern of studying, practising and rehearsing the exam? What worked best for you?
6. How did the labs vary from traditional exam revision and how challenging were they?
7. When you did the final exam, what was the balance of showing technical knowledge as opposed to showing your skills in practice?
8. After you passed, was there any immediate change in your professional role? How about over the following months?
9. Do you feel that you have been rewarded with greater responsibilities or rewards as a result of being CSX-P?
10. There are plenty of alternatives to CSX-P, such as CISSP, ISF, CompTIA Security+ and various Microsoft certificates. Why do you feel that CSX-P was better for you than any of those?
Quiz Question 2

You want to assign permissions to a Linux file with the notation of “-rwxrw-r--”. Which of the following numbers needs to be appointed while using the chmod command?

• 764
• 755
• 321
• 777
Quiz Question 3

Three common controls used to protect the availability of information are:

- Redundancy, backups and access controls
- Encryption, file permissions and access controls
- Access controls, logging and digital signatures
- Hashes, logging and backups
Panel Questions

Can you provide a specific example of a lab activity/question? Thanks.

Based on what you’ve seen from the CSX-P content, what’s the biggest cybersecurity issue facing industry today? How does that compare with your real-life experience?

How confident does the CSX-P make you feel that, if you were looking for a new job, you could move into something in Scotland with relative ease?
Quiz Question 4

If you believe that a private IP on your LAN is spoofing their IP address in order to conduct nefarious activity, which of the following is the best command to run in order to map IP and MAC addresses?

• select * FROM Address WHERE MAC=IP
• nmap –sn
• arp -n
• match -IP -MAC
Quiz Question 5

Which of the following cybersecurity roles is charged with the duty of managing incidents and remediation?

- Board of directors
- Executive committee
- Cybersecurity management
- Cybersecurity practitioners
Poll

Which of the ISACA Cybersecurity qualifications/certifications are you interested in pursuing?

- CSX-P Cybersecurity Practitioner
- CSX Cybersecurity Fundamentals Certificate
- Cybersecurity Audit Certificate
- One of the CSX advanced technical skill certificates
- Certified Information Systems Manager
- Not interested at this time
Next Steps

First stop: [https://www.isaca.org/resources/cybersecurity](https://www.isaca.org/resources/cybersecurity)


Ask the Chapter: [csx@isaca-scotland.org.uk](mailto:csx@isaca-scotland.org.uk)

Sponsorship for First Certification: [membership@isaca-scotland.org.uk](mailto:membership@isaca-scotland.org.uk)

ISACA have limited time discounts of 20% on exams and training materials for CSX-P and CSX Cybersecurity Fundamentals
WELCOME TO YOUR FINAL EXAM.
THE EXAM IS NOW OVER.
I'M AFRAID ALL OF YOU FAILED.
YOUR GRADES HAVE BEEN STORED ON OUR DEPARTMENT SERVER AND WILL BE SUBMITTED TOMORROW.
CLASS DISMISSED.

Source: https://xkcd.com/2385/
Quiz Answers

1. Protect; Recover; Identify
2. 764
3. Redundancy, backups and access control
4. arp -n
5. Cybersecurity management