STUDENT360
secure your future

Playing Security Poker – I match your degree and raise you by a certification

or

2 Grumpy Old Security Men – What's up Cert?

Presented by:

Curtis Coats, CISSP, CAP

Kelley P. Archer, CISSR

MN ISSA

Agenda

STUDENT360
secure your future

- **Types of Certifications**
  - ASIS ISSA/ISC2, SANS, ISACA, BCP/DR, etc.
- **Why are certain ones better than others**
  - Technical vs. Non-technical
- **5 Great 'Starter‘ Cybersecurity Certifications**
- **Which ones have the stronger earning power**
  - CISSP - Certified Information Systems Security Professional
- **Do I need more than one?**

Types of Certifications

STUDENT360
secure your future

- ASIS Certifications
  - CPP – Certified Protection Professional
  - PCI - Professional Certified Investigator
  - PSP – Physical Security Professional

- ISC2 Certifications
  - CISSP – Certified Information Systems Security Professional
    - ISSAP – Architecture; ISSEP – Engineering; ISSMP - Management
  - SSCP – Systems Security Certified Practitioner
  - CCSP – Certified Cloud Security Professional
  - CAP – Certified Authorization Professional
  - CSSLP – Certified Secure Software Lifecycle Professional
  - HCISPP – HealthCare Information Security and Privacy Practitioner
  - Associate of (ISC)2

Types of Certifications – cont.

STUDENT360
secure your future

- SANS Institue Certifications
  - GCFE - GIAC Certified Forensics Examiner
  - GISP - GIAC Information Security Professional
  - GSEC - GIAC Security Essentials Certification
  - GCIH – GIAC Certified Incident Handler
  - GCIA – GIAC Certified Intrusion Analyst
  - GWAPT – GIAC Certified Web Application Penetration Tester
  - GCED - GIAC Certified Enterprise Defender
  - GIAC Information Security Fundamentals (GISF)
  - GIAC Global Industrial Cyber Security Professional (GICSP)
  - GIAC Certified Forensics Examiner (GCFE)
  - GIAC Information Security Professional (GISP)
  - GIAC Security Essentials Certification (GSEC)

Types of Certifications – cont.

STUDENT360
secure your future

- SANS Certifications
  - GIAC Systems and Network Auditor (GSNA)
  - GIAC Certified Forensic Analyst (GCFA)
  - GIAC Network Forensic Analyst (GNFA)
  - GIAC Advanced Smartphone Forensics (GASF)
  - GIAC Law of Data Security & Investigations (GLEG)
  - GIAC Security Leadership Certification (GSLC)
  - GIAC Certified Project Manager Certification (GCPM)
  - GIAC Certified Perimeter Protection Analyst (GPPA)
  - GIAC Certified Intrusion Analyst (GCIA)
  - GIAC Certified Incident Handler (GCIH)
  - GIAC Certified UNIX Security Administrator (GCUX)

Types of Certifications – cont.

STUDENT360
secure your future

- SANS Certifications
  - GIAC Certified Windows Security Administrator (GCWN)
  - GIAC Certified Enterprise Defender (GCED)
  - GIAC Certified Penetration Tester (GPEN)
  - GIAC Web Application Penetration Tester (GWAPT)
  - GIAC Mobile Device Security Analyst (GMOB)
  - GIAC Critical Controls Certification (GCCC)
  - GIAC Continuous Monitoring Certification (GMON)
  - GIAC Python Coder (GPYC)
  - GIAC Response and Industrial Defense (GRID)
  - GIAC Secure Software Programmer - .NET (GSSP-NET)
  - GIAC Secure Software Programmer - Java (GSSP-JAVA)

Types of Certifications – cont.

STUDENT360
secure your future

- SANS Certifications
  - GIAC Certified Web Application Defender (GWEB)
  - GIAC Reverse Engineering Malware (GREM)
  - GIAC Security Expert (GSE)
  - GIAC Assessing Wireless Networks (GAWN)
  - GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)

- ISACA Certifications
  - CISA – Certified Information Auditor
  - CRISC – Certified in Risk and Information Control
  - CISM – Certified Information Security Manager
  - CGEIT – Certified in the Governance of Enterprise IT
  - CSX – Cybersecurity Nexus – CSX Certificate and CSX-P Certification

Types of Certifications – cont.

STUDENT360 secure your future

- BCP Certifications – BCI - https://www.thebci.org/
  - CBR – Certified Business Resilience Audit
  - CBRITP – Certified Business Resilience IT Professional
  - CBRM – Certified Business Resilience Manager
  - MABR – Master's Achievement in Business Resilience
  - CBCI – Certificate of the Business Continuity Institute
  - MBCI – A level of CBCI – may not apply as a certification per se

- DR Certifications – DRII - https://drii.org/
  - EDRP – EC-Council Disaster Recovery Professional
  - ABCP – Associated Business Continuity Professional
  - CFCP – Certified Functional Continuity Professional
  - CBCP – Certified Business Continuity Professional
  - MBCP – Master Business Continuity Professional
  - CBCA – Certified Business Continuity Auditor
  - CBCLA – Certified Business Continuity Lead Auditor
  - ARMP – Associate Risk Management Professional
  - CRMP – Certified Risk Management Professional

Technical vs Non-technical

STUDENT 360
secure your future

- Is a technical certification worth more than a non-technical one?
  - Not a matter of tech vs non-tech, depends on man things;
  - Area of specialty
  - Company/market
  - Geo location
  - Your experience
- CISSP is considered a baseline INFOSEC Certification for everyone
  - GIAC is primarily technical
  - Others will vary depending on the certification itself
    - ISACA
    - ASIS
    - Others

5 Great 'Starter' Cybersecurity Certifications*

STUDENT360
secure your future

1. Microsoft Technology Associate (MTA) Security Fundamentals
2. ISACA CSX Cybersecurity Fundamentals Certificate
3. CompTIA Security+
4. GIAC Information Security Fundamentals (GISF)
5. (ISC)^2 Systems Security Certified Practitioner (SSCP)

* By Kim Lindros, Business News Daily Contributing Writer December 28, 2016 12:19 pm EST

MS Technology Associate (MTA) Security Fundamentals

STUDENT 360 secure your future

- The MTA Security Fundamentals is the most "entry-level" one of the five.
- Aimed at high school and early college students, as well as those in the workforce who are looking to change careers.
- It recognizes knowledge of core security principles as well as the basics of operating system, network and software security
- To achieve certification, you must pass a single exam, which costs $127.

ISACA CSX Cybersecurity Fundamentals Certificate

STUDENT360
secure your future

- The CSX Cybersecurity Fundamentals Certificate is geared toward recent post-secondary graduates and those seeking career changes.
- This certificate covers five cybersecurity-related domains:
  - concepts;
  - architecture principles;
  - network, system, application and data security;
  - incident response;
  - and security of evolving technology.
- The single exam costs $150, and the certificate doesn't expire or require periodic recertification.

CompTIA Security+

STUDENT360
secure your future

- the Security+, which covers a wide array of security and information assurance topics, including network security, threats and vulnerabilities, access controls, cryptography, risk management principles, and application, host and data security. The certification meets U.S. Department of Defense Directive 8570.01-M requirements — an important item for anyone looking to work in IT security for the federal government — and complies with the Federal Information Security Management Act (FISMA).
- CompTIA recommends that candidates have two years of relevant experience and achieve the Network+ credential before taking the Security+ exam. At $311, is at the median price of the others.

GIAC Information Security Fundamentals (GISF)

STUDENT360
secure your future

- The SANS GISF is considered to be more challenging that the CompTIA Security+ exam.
- GIAC exams in general require test takers to apply knowledge and problem-solving skills, so hands-on experience that has been gained through training or on-the-job experience is recommended.
- If taken as part of SANS training sitting for the GISF exam, the exam cost alone is $689. Taking the exam without completing training, referred to as a "certification attempt" by GIAC, bumps the exam cost to a whopping $1,249. GIAC includes two practice exams in the certification-attempt package.

(ISC)² Systems Security Certified Practitioner (SSCP)

STUDENT360
secure your future

- The SSCP fills the entry-level slot or (ISC)².
- To achieve the SSCP, you must pass a single exam that includes questions that span seven common body of knowledge (CBK) domains: (1) Access Controls, (2) Security Operations and Administration, (3) Risk Identification, Monitoring, and Analysis, (4) Incident Response and Recovery, (5) Cryptography, (6) Network and Communications Security, and (7) Systems and Application Security.
- The exam costs $250, and (ISC)2 offers a variety of study resources for purchase on its website.

Associate of (ISC)²

STUDENT 360
secure your future

- You can take an (ISC)² certification exam without the minimum work experience.
- If you pass, you need to meet your continuing professional education (CPE) requirements, while you work to get the experience needed to certify as a

  - **CISSP** – 5 years cumulative, paid, full-time work experience in 2 or more of the 8 domains of its CBK.
  - **SSCP** – 1 year of cumulative work experience in 1 or more 7 domains of its CCSP CBK
  - **CCSP** - 5 years cumulative, paid, full-time work in **I.T**; 3 yrs in **I.S**. and 1 yr in its CBK
  - **CAP** - 2 yrs cumulative, paid, full-time work experience in 1 or more of the 7 domains of its CBK.
  - **CSSLP** - 4 years cumulative, paid, full-time SDLC professional experience in 1 or more of the 8 domains of its CBK
  - **HCISPP**- 2 ys of cumulative, paid, full-time work experience in 1 or more knowledge areas of its CBK that includes security, compliance and privacy. One year must be in Healthcare.

Stronger Earning Power

STUDENT360
secure your future

- Today's market a combination is best, i.e. CISSP and a GIAC
  - CISSP is most recognized by companies today
  - Others are becoming popular
  - Least popular is CEH, Certified Ethical Hacker
    - Companies normally can't afford to have someone on staff
    - Usually this service is outsourced – few companies provide
    - CEH people are under utilized in corporate world. Most work is focused other than Hacking related

Certified Information Systems Security Professional

STUDENT360
secure your future

- The most-esteemed cybersecurity certification in the world. The CISSP recognizes information security leaders who understand cybersecurity strategy, as well as hands-on implementation.
- Candidates must have a minimum of five years cumulative, paid, full-time work experience in two or more of the eight domains of the CISSP Common Body of Knowledge (CBK).
- Only a one-year experience exemption is granted for education.
- The exam costs $699

Do I need more than one?

STUDENT360
secure your future

- A combination is best, i.e. CISSP and a GIAC or similar
  - C++ can add value

- Base and sub-concentration, i.e. CISSP and
  - **CISSP-ISSAP -** Information Systems Security Architecture Professional
  - **CISSP-ISSEP -** Information Systems Security Engineering Professional
  - **CISSP-ISSMP -** Information Systems Security Management Professional

Questions

STUDENT360
secure your future

Curtis Coats, CISSP, CAP

Kelley P. Archer, CISSR
issaman@mchsi.com