Cheapskate! Free and Excellent Infosec Career Resources

Nathan Chan, CISSP C|EH

Who Am I

- Three careers
  - Flight Simulation – both trainers and engineering
  - Software Tester
  - Security
- Worked in defense, commerical software, consulting, security
- Got CISSP in 2011 and C|EH in 2012

Agenda

- How I see Cyber Security / Information Security
- Free info to get started and where to find it
- Local meetings to attend
- Security Certifications

How I See Cybersecurity

- When I look around at the careers and positions in cybersecurity, and to keep things organized in my mind, I see three broad categories:
  - Management
  - Infrastructure
  - Engineering
- There is overlap in these three categories, and where something may fit depends on how you see the position.

Management

- Management is the mostly non-technical support structure for organization security.
  - Policy
  - Procedures
  - Human Resources
  - Legal
  - Compliance
  - Training

Infrastructure

- Infrastructure is anything needed to get the organization's work done. The infrastructure needs to be kept secure.
  - Network
  - Third-Party Applications
  - Cloud
  - Wireless

Engineering

- Engineering is anything the organization creates, sells or provides to customers. All these things need to be made in a secure manner so they will be difficult to hack.
  - Applications
  - Web Site
  - Services

These Classifications are not Precise

- There can be overlap or things fit in multiple classifications
- For example – how about Forensics?
  - Forensics is often a legal (managerial) requirement.
  - When actually executed, it is usually network or endpoint drives (infrastructure) that are imaged.

These Classifications are not Precise - Overlap

- Another example – how about Pen Testing?
  - Pen Testing is often a compliance (managerial) requirement.
  - When actually executed, it depends on the subject of the pen test.
    - A physical pen test (getting into the building, getting information) is managerial.
    - If the pen test is against the network, it is infrastructure.
    - If an application, web service or web site is being pen tested, it is engineering.

Free Stuff - NIST Notes

- A great free source for a lot of information is the National Institute for Standards and Technology (NIST) Computer Security Resource Center.
- https://csrc.nist.gov/publications/
- NIST documents can be considered authoritative.
- However, NIST documents are extremely dry reading.

Free Stuff - Introduction

- Introduction to Information Security
  - NIST SP 800-12 Rev 1: “An Introduction to Information Security”, 2017, https://csrc.nist.gov/publications/detail/sp/800-12/rev-1/final
  - NIST SP 800-100: “Information Security Handbook: A Guide for Managers”, 2007, https://csrc.nist.gov/publications/detail/sp/800-100/final

Free Stuff - Introduction

- Introduction to Information Security (cont'd)
  - Cybersecurity is Everyone's Job, NIST, 2018, https://www.nist.gov/news-events/news/2018/10/cybersecurity-everyones-job
  - The Infosec Handbook, Apress Open, 2014, https://link.springer.com/book/10.1007%2F978-1-4302-6383-8
  - Navigating the Digital Age 1st ed, Caxton Business and Legal, 2015, https://www.securityroundtable.org/wp-content/uploads/2015/09/Cybersecurity-9780996498203-no_marks.pdf

Free Stuff - Introduction

- Introduction to Information Security (cont'd)
  - Navigating the Digital Age 2st ed, Palo Alto Networks, 2018, (requires signup)
    https://www.securityroundtable.org/navigating-the-digital-age-2nd-edition/
  - A CISO's Guide to Bolstering Cybersecurity Posture, Center for Internet Security, 2018, (requires signup)
    https://www.cisecurity.org/white-papers/ebook-a-cisos-guide-to-bolstering-cyber security-posture/
  - Defender's Dilemma, RAND, 2015, https://www.rand.org/pubs/research_reports/RR1024.html

Free Stuff - Management

- Compliance
  - Two lists of compliance requirements can be found at Telos and TDCI sites

    https://www.telos.com/cyber-risk-management/xacta/compliance-standards/
    https://www.tcdi.com/information-security-compliance-which-regulations/
  - PCI DSS (Payment Card Industry Data Security Standard)

    https://www.pcisecuritystandards.org/document_library
  - GDPR – (General Data Protection Regulation EU)

    https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

Free Stuff - Management

- Privacy
  - CCPA (California Consumer Privacy Act) https://www.oag.ca.gov/privacy/ccpa
  - CCPA Amendments (still in flux) https://www.infolawgroup.com/blog/2019/9/20/ccpa-act-ii-amendments-pass-california-legislature-head-to-governors-desk
  - IAPP (International Association of Privacy professionals) – some material is free, paid membership required for full access. https://iapp.org/resources/research/

Free Stuff - Management

- Risk
  - DHS Cyber Risk Management Primer for CEOs

    https://www.dhs.gov/sites/default/files/publications/C3%20Voluntary%20Program%20-%20Cyber%20Risk%20Management%20Primer%20for%20CEOs%20_5.pdf
  - NIST Cybersecurity Framework

    https://www.nist.gov/cyberframework
  - CMU SEI Blog on Risk Management, 2018

    https://insights.sei.cmu.edu/insider-threat/2018/02/7-considerations-for-cyber-risk-management.html

Free Stuff - Management

- Training and Awareness
  - Cybersecurity and Information Systems Information Analysis Center (CSIAC)
    https://www.csiac.org/series/cyber-awareness-videos/
  - Australian Defense Cybersense
    https://www.youtube.com/playlist?list=PLAA359AC9EEA14569
  - EDUCAUSE Security Awareness
    https://library.educause.edu/topics/cybersecurity/security-awareness
  - DHS Stop. Think. Connect. Toolkit
    https://www.dhs.gov/stopthinkconnect-toolkit

Free Stuff - Management

- Checklists
  - NIST Manufacturing Extension Partnership (MEP) Cybersecurity Self-Assessment Handbook, 2017
    https://nvlpubs.nist.gov/nistpubs/hb/2017/nist.hb.162.pdf
  - US Cyber Consequences Unit Cybersecurity Matrix Checklist, 2016
    http://usccu.us/documents/US-CCU%20Cyber-Security%20Matrix%20(Draft%20Version%202).pdf

Free Stuff - Infrastructure

- Center for Internet Security (CIS) 20 Controls V7.1 (requires signup for download)
  https://www.cisecurity.org/controls/cis-controls-list/
- SANS Posters of CIS Controls
  https://www.sans.org/critical-security-controls/
- Mozilla Server Side TLS
  https://wiki.mozilla.org/Security/Server_Side_TLS
- OWASP TLS Cheat Sheet
  https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html

Free Stuff - Infrastructure

- Better Crypto, https://bettercrypto.org/
- IIS Crypto Free Tool by Nartac Software
  https://www.nartac.com/Products/IISCrypto
- Mozilla OpenSSH Recommendations
  https://infosec.mozilla.org/guidelines/openssh
- Cloud Security Alliance (CSA) Security Guidance V4
  https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/security-guidance-v4-FINAL.pdf

Free Stuff - Infrastructure

- CSA Cloud Control Matrix V3.0.1, 2016
  https://downloads.cloudsecurityalliance.org/assets/research/cloud-controls-matrix/CSA_CCM_v.3.0.1-10-06-2016.xlsx
- Cyber Kill Chain
  - Lockheed Martin
    https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
  - Mitre ATT&CK https://attack.mitre.org/
- Pen Testing Execution Standard
  http://www.pentest-standard.org/index.php/Main_Page

Free Stuff - Infrastructure

- Incident Response
  - CMU SEI Resources for Creating a Computer Security Incident Response Team (CSIRT)
    https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=485643
  - CMU SEI Handbook for CSIRTs, 2003
    https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6305

Free Stuff - Infrastructure

- Incident Response
  - Centre for Research and Evidence on Security Threats (CREST, UK) Cyber Security Response Guide V1, 2014
    https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf
  - US Dept of Justice Best Practices for Victim Response and Reporting of Cyber Incidents, 2015
    https://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents2.pdf

Free Stuff - Engineering

- Software / Secure Development Lifecycle (SDLC)
  - OWASP Software Assurance Maturity Model (OpenSAMM) V1.5
    https://www.owasp.org/index.php/OWASP_SAMM_Project
  - Building Security In Maturity Model (BSIMM) V10 – (download requires signup)
    https://www.bsimm.com/framework.html
  - BSIMM V9 download
    https://www.bsimm.com/content/dam/bsimm/reports/bsimm9.pdf

Free Stuff - Engineering

- Software / Secure Development Lifecycle (SDLC)
  - Microsoft SDL
    https://www.microsoft.com/en-us/securityengineering/sdl/
  - Free Microsft SDL Book (2006)
    https://blogs.msdn.microsoft.com/microsoft_press/2016/04/19/free-ebook-the-security-development-lifecycle/
  - CMU SEI Capability Maturity Model (CMM) for Development V1.3, 2010,
    https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=9661
  - Rugged Software (2012) https://ruggedsoftware.org/

Free Stuff - Engineering

- Training
  - OWASP AppSec Tutorial Series
    https://www.youtube.com/user/AppsecTutorialSeries
  - SAFECode Training https://safecode.org/training/
  - Andrew Buttner and Larry Shields Slides, 2015
    - Introduction to Secure Coding
      http://opensecuritytraining.info/IntroSecureCoding.html
    - Secure Code Review
      http://opensecuritytraining.info/SecureCodeReview.html

Free Stuff - Engineering

- OWASP has a lot of great material in this area
  https://www.owasp.org/index.php/Category:OWASP_Project#tab=Project_Inventory
- Don’t forget the OWASP Cheat Sheets
  https://cheatsheetseries.owasp.org/
- Mitre Corporation
  - Common Weakness Enumeration
    https://cwe.mitre.org/data/index.html
  - Common Vulnerabilities and Exposures
    https://cve.mitre.org/data/downloads/index.html

Free Stuff - Engineering

- Other sources
  - IEEE Avoiding the Top 10 Security Flaws
    https://ieeecs-media.computer.org/media/technical-activities/CYBSI/docs/Top-10-Flaws.pdf
  - SANS Securing Web Application Technologies (SWAT) Checklist
    https://software-security.sans.org/resources/swat
  - CMU SEI CERT Top 10 Secure Coding Practices
    https://wiki.sei.cmu.edu/confluence/display/seccode/Top+10+Secure+Coding+Practices

Free Stuff - Engineering

- Other sources
  - CWE/SANS Top 25 Most Dangerous Software Errors https://www.sans.org/top25-software-errors/
  - CMU SEI CERT Secure Coding Standards https://wiki.sei.cmu.edu/confluence/display/seccode/SEI+CERT+Coding+Standards
  - Mozilla Web AppSec Secure Coding Guidelines https://wiki.mozilla.org/WebAppSec/Secure_Coding_Guidelines
  - Microsoft .NET Secure Coding Guidelines https://docs.microsoft.com/en-us/dotnet/standard/security/secure-coding-guidelines?redirectedfrom=MSDN

Free Stuff - Engineering

- Other sources
  - Institute for Security and Open Methodologies (ISECOM) Open Source Security Testing Methodology Manual V3 (OSSTMM 3)
    https://www.isecom.org/OSSTMM.3.pdf

Free Stuff - General Subjects

- Dr. Ross Anderson, “Security Engineering 2nd ed”, 2008, – A 900 page overview of security issues, many non software related.
  https://www.cl.cam.ac.uk/~rja14/book.html
- Dr. Peter Gutmann, “Engineering Security”, 2014, – very technical at over 800 pages
  https://www.cs.auckland.ac.nz/~pgut001/pubs/book.pdf
- Software Engineering Body of Knowledge (SWEBOK) V3, also Standard ISO/IEC TR 19759:2015
  https://ieeecs-media.computer.org/media/education/swebok/swebok-v3.pdf

Free Stuff - General Subjects

- Charles M. Kozierok, “The TCP/IP Guide”, 2005, http://www.tcpipguide.com/free/index.htm
- Menezes, Oorschot and Vanstone, “Handbook of Applied Cryptography”, CRC Press, 1996, http://cacr.uwaterloo.ca/hac/
- H X Mel and Doris Baker, “Cryptography Decrypted”, Addison-Wesley, 2001, https://hxmel.com/book.html

Free Stuff - General Subjects

- Tsipenyuk, Chess and McGraw, “Seven Pernicious Kingdoms: A Taxonomy of Software Security Errors”, Fortify / Cigital, https://samate.nist.gov/SSATTM_Content/papers/Seven%20Pernicious%20Kingdoms%20-%20Taxonomy%20of%20Sw%20Security%20Errors%20-%20Tsipenyuk%20-%20Chess%20-%20McGraw.pdf
- CMU SEI “A Taxonomy of Operational Cyber Security Risks Version 2”, 2014, https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=91013
- EU Agency for Cybersecurity (ENISA) “Reference Incident Classification Taxonomy”, 2018, https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy

Free Stuff - General Subjects

- NIST Interagency Report (NISTIR) 7298 R3, “Glossary of Key Information Security Terms”, 2019, https://csrc.nist.gov/glossary online only
- NIST Interagency Report (NISTIR) 7298 R2, “Glossary of Key Information Security Terms”, 2013 (withdrawn 2019), https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

Free Stuff - Local Meetings

- CSA So Cal Chapter - usually 1st week of the month, Cloud security focus. https://www.csa-la.org/
- ISACA LA Chapter - 2nd Tuesday evenings, usually at Luminarias, Monterey Park (intersection of the 10 and the 710) - more business and audit oriented, the Big Four accounting firms are most likely to appear at this meeting. https://isacala.org/

Free Stuff - Local Meetings

- ISSA LA Chapter - 3rd Wednesday either lunch at Taix in Echo Park or evenings usually on the West Side - this is the most general of the meetings, can cover a wide range of topics.
  https://www.issala.org/
- OWASP LA Chapter - 4th Wednesday evening, usually on the West Side - this is the most "techy" of the meetings, often covering coding.
  https://www.owasp.org/index.php/Los_Angeles

Free Stuff - Local Meetings

- HTCIA SoCal Chapter - These meetings are usually criminal / forensics oriented. http://www.socalhtcia.org/

Free Stuff - Local Meetings

- Also in the area:
  - ISACA OC https://engage.isaca.org/orangecountychapter/home
  - ISSA Ventura County https://issa-vc.org/
  - ISSA Inland Empire http://ie.issa.org/
  - ISSA Orange County https://issa-oc.org/
  - OWASP San Fernando https://www.meetup.com/OWASP-San-Fernando-Valley-Chapter/
  - OWASP Inland Empire https://www.meetup.com/OWASP-Inland-Empire-Open-Web-Application-Security-Project/
  - OWASP Orange County https://www.owasp.org/index.php/Orange_County

Free Stuff - Certifications

- Certifications are useful in proving a certain minimum knowledge base.
- If you are just starting out with no background, CompTIA Certifications are a good start. https://certification.comptia.org/
- Professor Messer provides free videos for several CompTIA certifications – A+, Network+ and Security+ https://www.professormesser.com/

Free Stuff - Certifications

- CompTIA has a nice IT Certification Roadmap showing many certification organizations at https://certification.comptia.org/docs/default-source/downloadablefiles/it-certification-roadmap.pdf
- One organization that is highly recommended for Pen Tests are the Offensive Security certs https://www.offensive-security.com/information-security-certifications/
  - The base OSCP cert requires an online course and labs before taking the exam, which is NOT multiple choice but more realistic actual hacking. The cert is a great value, becoming highly recognized and much cheaper than SANS. But it is very difficult.

Free Stuff - Certifications

- CompTIA does not have the Offensive Security certs on their roadmap.
- CompTIA also does not have certs from the International Association of Privacy Professionals (IAPP)
  - IAPP offers certs depending on your background – law, managerial or technical https://iapp.org/certify/programs/

Free Stuff - Certifications

- Different random lists of top paying certifications
  - https://blog.trainace.com/top-5-highest-paying-cyber-security-certifications
  - https://www.globalknowledge.com/us-en/resources/resource-library/articles/top-paying-certifications/
  - https://www.roberthalf.com/blog/salaries-and-skills/10-highest-paying-it-certifications-for-tech-pros
  - https://www.infosec-careers.com/the-best-cyber-security-certifications-in-2019/

Free Stuff - Education

- Education
  - Cybrary - https://www.cybrary.it/
  - Open Security Training - http://opensecuritytraining.info/Training.html
  - SANS CyberAces - https://www.cyberaces.org/
  - US DHS ICS-CERT VLP (Virtual Learning Portal) – focus on industrial control systems - https://ics-cert-training.inl.gov/learn

Free Stuff - Education

- Education
  - Massive Open Online Courses (MOOCs)
    https://www.cyberdegrees.org/resources/free-online-courses/
    https://www.mooc-list.com/tags/cybersecurity?page=1
- Security Test Questions Site
  - Cccure – some free information but pay required to access questions
    https://www.cccure.education/

Free Stuff - Education

- CISSP Podcasts and Practice Questions
  - Eric Conrad
    https://booksite.elsevier.com/companion/conrad/

Free Stuff - Hacking

- Linux Distribution
  - Kali Linux https://www.kali.org/
- Virtual Machine
  - Oracle VirtualBox (free for non-commercial use) https://www.virtualbox.org/
- Vulnerable Targets
  - VulnHub https://www.vulnhub.com/

Free Stuff

- QUESTIONS?

Free Stuff

- THANK YOU!
- chan8w111@gmail.com
- If you want to connect on LinkedIn (Nathan Chan CISSP CEH), please state where / when we met – I generally ignore connect invites