Healthcare Needs Your Help!
How To Become the next Security Leader or Information Security Officer

Roy Wattanasin
September 14, 2017
ISSA CISO Mentoring Series
Agenda

• whoami
• Healthcare Challenges
• Leadership Skills
• Security Professional Skills
• Recommendations
• Resources & “continuing” the Discussion
whoami

• healthcare, IoT, medsec, appsec & building communities

• How did I start?
• What degrees do I have?
• Where do you currently teach?
• What conferences have I been involved with?
Healthcare Challenges

- Interconnected Systems
- Devices
- Hardware
- Software
- Applications – EMR / EHR
- Patient Privacy / Laws
Healthcare Challenges

- People
- Technologies
- Data Security – CIA
- Ransomware, DDOS
- Patching
- Third parties

Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (formerly St. Jude Medical's) Implantable Cardiac Pacemakers: FDA Safety Communication

- [https://www.healthcareinfosecurity.com/](https://www.healthcareinfosecurity.com/)
- [https://twitter.com/PrivacyProf](https://twitter.com/PrivacyProf)
Healthcare Challenges

• The supply of skilled cybersecurity professionals has not kept pace with the demand

• Cybersecurity in healthcare is getting harder

• Staffing for cybersecurity and healthcare is a serious challenge
Healthcare Challenges

The skills gap will hurt healthcare

- Assume that 4 out of 5 of organizations are finding it hard to hire
- And the demands of the job in healthcare are above average
- And some healthcare job locations are not universally appealing
- The experience of “direct and measurable damage” due to cybersecurity under-hiring in healthcare could exceed 71%

Cobb, S. (2016) “Getting to know CISOs: Challenging assumptions about closing the cybersecurity skills gap” University of Leicester MSC dissertation

Efforts to fix skills gap

• NICE – National Initiative on Cybersecurity Education

• NIST SP: 800-181

• Multiple organizations involved
  • See talk at: Most Top Computer Science Programs Skip Cybersecurity
    http://theinstitute.ieee.org/career-and-education/education/most-top-computer-science-programs-skip-cybersecurity
Efforts to fix skills gap


- Proposed College Curriculum Changes for Producing Secure Developers, Christine Fossaceca (MIT Lincoln Laboratory), Leah Goggin (Massachusetts Institute of Technology), and Elitza Neytcheva (University of Massachusetts-Amherst), IEEE SecureDev Conference 2017
Cyberseek.org

The New Way to Decipher the Cybersecurity Jobs Market

Cybersecurity jobs are in high and growing demand. But, there's a critical shortage of qualified workers across the nation. While discussing the many challenges and questions associated with the cybersecurity job landscape, we had a lightbulb moment. There must be a new way to assess and ultimately improve the cybersecurity talent pipeline. And thus, CyberSeek™ was born.

• http://www.cyberseek.org
Women are twice as likely as men to be dedicated full-time to security awareness.

Women were twice as likely as men to have that background in soft skills. On the flip side, men were three times as likely to have a technical background.
Leadership Skills

1. Communication and presentation skills;
2. Policy development and administration;
3. Political skills;
4. Knowledge about the industry;
5. Collaboration and conflict management skills;
6. Planning and strategic management skills;
7. Supervisory skills;
8. Incident management;
9. Knowledge of regulation and standards compliance;
10. Risk assessment and management.

• https://www.govinfosecurity.com/blogs/top-10-skills-state-cisos-need-to-succeed-p-602

• Negotiation
• Organization
• Interpersonal skills

• CISO Mindmap
C-Level Dashboards

• Number of reported incidents (security/privacy)
• PHI/PII sensitive data leakage
• Number of visits to unapproved sites
• Email filter(s) acceptable use violations
• Phishing susceptibility, attack rate, reported rate
• Average time to audit network passwords
C-Level Dashboards

- Detected insider attacks vs. Reported insider incidents
- Incidents through VPN / Infections when Remote
- Number of lost devices / Avg. time to report loss
- Social Media Audits
- User-reported infections
- Physical security audits
Security Professional Skills

Healthcare CISOs may need more of everything

12 factors for success as an information security professional rated and ranked: the healthcare sector versus all sectors

Source: Secondary analysis of (ISC)² Global Information Security Workforce Survey data tables by the author

- Broad understanding of the security field
- Communication skills
- Awareness and understanding of the latest...
- Technical knowledge
- Knowledge of relevant regulatory policy
- Security policy formulation and application
- Leadership skills
- Possession of an information security certification
- Project management skills
- Business management skills
- Legal knowledge
- Possession of an information security degree

Security Professional Skills

I would also add:

- Passion
- Confidence
- Critical thinking – “think outside the box”
- See ”Information Security Careers” talk at: https://www.youtube.com/watch?v=GTt3qvdTexM
Certifications

• Certifications help but experience is better

• It depends what you want to do and pursue

• Some recommended certifications from: ISC2, ISACA, GIAC, Offensive Security, Comptia etc.
  
  • [https://www.globalknowledge.com/us-en/content/articles/top-paying-certifications/](https://www.globalknowledge.com/us-en/content/articles/top-paying-certifications/)
Recommendations

• Network, network and network #HallwayCON
  – Attend conferences and contribute
  – Pre-professionals - Check #infosec, #infosec101, #introsec

• Passionate and stay up to date on trends – Twitter, Linkedin, Peerlyst, Slack etc.

• Participate in CTF and other events
Recommendations

• Participate & contribute to something that you are interested in to learn more

• Read, blogs, watch and do your research
  – Palo Alto’s Cybersecurity Cannon, Blogs, 50 Blogs,
  – Peerlyst’s Free Infosec Book List, Top 50 WIS, 2017 Global Knowledge IT Skills and Salary Report

• Seek mentor(s) & become a mentor
Recommendations

- ISSA Pre-Professional Virtual Meetup
- ISSA Special Interest Groups
- ISSA CISO Mentoring Webinar Series
- ISSA International Conference
- Join your local ISSA Chapter
  – Help create/join your local ISSA student meetup
Recommendations

- I Am The Cavalry, OWASP, Security BSides, ISACA, ISC2, SecureWorld, Defcon, Defcon Biohacking Village, IEEE, ACM, HIMSS, NH-ISAC (depending on industry/sector), MedSec Linkedin, CSA, CISO Wiki, SANS ISC, WISP, InfosecWorld, SourceConference, Derbycon, local TOOOL, EdX, KhanAcademy, KodeWithKlossy, CTFTime, Find a CTF, local Meetup.com meetings, local makerspaces/hackerspaces etc.
Recommendations

• Continually improve your skills, do you recon

• Have fun, help **eliminate stress**, manage your time and stay healthy

• “Hack the planet!” & Join healthcare!!!
Resources

• Security Awareness Maturity Model, SANS https://securingthehuman.sans.org/blog/2016/02/25/security-awareness-maturity-model-your-path-to-success
Thank you!

• Would I do things “differently” today?

• @wr0

• Questions / Comments?