Finding, Developing, & Retaining Cyber Talent

Brian Isle
Mike Johnson

TECHNOLOGICAL LEADERSHIP INSTITUTE

The Cyber Skills Issue

Cybersecurity Skills Shortage Puts Organizations At Risk, Study Shows

The oft-discussed and lamented cybersecurity skills gap isn't just a hiring issue, it's putting your organization at risk, Intel Security-CSIS study finds.

InformationWeek DARKReading

Forbes One Million Cybersecurity Job Openings In 2016

Zero-percent cybersecurity unemployment, 1 million jobs unfilled

CSO FROM IDG

Cybersecurity labor crisis expected to continue through 2021.

CSO | Sep 19, 2016 5:43 AM PT

Attracting & Developing Talent

- What's working for Employers & Employees
  - Security Challenges & Solutions
- Training & Education as a Key Strategy

Who We Talked To

- Major retailers
- Federal agency
- Financial Institutions
- Small/Medium Sized High Tech Businesses
- State Agency
- Health Care

Security Challenges – Sourcing Talent

Develop Talent From Within Your Organization

- Look to your IT roles like Network/Desktop/Help Desk/O&M staff
  - "We look for aptitude and interest in security"
- Consider Alternate Paths – Tapping other employee types
  - Business line employees – understand the organization
  - May have aptitude for technology but not direct training
  - Bring a unique perspective & problem solving approaches
  - "Examples of non traditional security being effective in security: non – IT hospital room process person now leading Med Device security."

Security Challenges – Sourcing Talent

The need is huge: we can't meet the need from cyber security programs alone

"We have cyber openings posted for a year before they fill."
"Lack of people with base line skills and desire to work in the area."

- Look to non-traditional external applicants
  - English, Psychology, Math, and engineering majors can bring new ideas
  - "I look for specific baseline skills, based on the role but I also train individuals in areas that are lacking"

Security Challenges – Sourcing Talent

Find talent through professional networking

- Be a member of the professional community
  - “Networking and “word of mouth” is the best. People on the team and the other security departments reach out to networks to find talent.”
  - “Professional groups have mailing lists that push job openings to folks in the group. “
- LinkedIn: A useful recruiting tool
  - “use LinkedIn to find & contact talent with skills that you need.”
  - “Recruiters troll LinkedIn looking for professionals looking for a job and companies looking for people.”

Security Challenges – Sourcing Talent

Traditional "tried and true" methods still work

- **Internships**
  - Work with HR to create a flexible internship program
  - Consider partnerships with higher education
  - "We have good luck with Interns. Try before you buy!"
  - "Spot high potential and direct their development"
  - "We created a HR funded internship program to build a pipeline for difficult to fill cyber roles."
  - "Some universities have an internship requirement. Partner with education institutions to get access to students for internships"

Security Challenges – Sourcing

Traditional "tried and true" methods still work

- **Internships**
  - "Security internship was successful partially due to establishing one large project … Shadowed every person on the team for at least one day. Student identified areas of interest for further investigation. Big project was mapping current policies to NIST Cybersecurity framework. Valuable for the student who hadn't previously been exposed to the real world governance issue"
  - "Offer jobs to good interns before they go back to school so when they graduate they come into the department"

Security Challenges – Sourcing

Partner with HR to leverage Corporate sourcing system

- Need to train HR on what's important in the cyber security world.
- "HR doesn't know that 5 years of Red Teaming qualifies as a Pen Tester"
- "HR and outside recruiters don't work. They don't know the industry and can't find anyone that isn't already known in such a small, close-knit security community."

Security Challenges - Retention

Retention of cyber talent is a problem!

“We have an issues: there is no career path for cyber security talent. We are a great talent proving ground for the other agencies”

- Provide challenging job with career path
  - “Provide clear roles and responsibilities for junior and senior talent”
  - “The senior folks mentor the Junior”
  - “Folks without experience need more specific direction which requires management to be much more crisp in what they are doing and that they can be effective.”

Security Challenges - Retention

Cyber professionals are learners

- Provide training internally and leverage external sources
  - “We pay for application specific training, tuition for college courses, and SANS and similar courses”
- Pay for and support professional certification
  - “All of our people have at least one cert.”
  - “We pay for the classes, testing and maintenance of certification.”

Security Challenges - Retention

People join and stay for many reasons

- “A rich benefits package is a draw.”
- “Young folks like extra PTO.”
- “Education and training is a strong retention.”
- “Flexibility in work schedules and location. Working remote is a big benefit.”
  - “Need to have purposeful team meetings to build relationships with remote employees.”

Security Challenges - Retention

"Some retention strategies are outside of your control (e.g. compensation and benefits). However, there are strategies that can be used to help keep some people around:"

1. Be genuine. Security practitioners are very smart and they can tell when leaders are being fake or disinterested.
2. Get into the details. Security practitioners like to talk tech and they like to get in the weeds. Make time to hear them.
3. Cultivate fun, special, innovative projects.
4. Cross train. Security practitioners like learning new things. Find ways to cross train in different areas.
5. Pay decently.

Security Challenges - Trends

- “More autonomous, work-from-home style staffing arrangements.
- “I suspect the next emerging trend will be the condensed work week or reduced schedule model. I think this will be driven by a desire to have more family/free time from the younger workforce and also to help save costs by employers.”
- “Replace outgoing seniors with higher costs, with entry level lower costs but also new thinking and approaches, requires stronger development processes”
- “Take advantage of “free money” like federal or state funding for targeted training. Initiative for creating standardized skills need and job descriptions for IT. Can’t wait for training to come to you, you need to go find it.”
- “Big issue is the drive for required compliance. “Compliance is not security.” “Excess compliance requirements is soul-sucking!”

Security Challenges - Training

Training is a recurring theme in attracting, growing, and retaining cyber talent

- "Remember to fund training, certification, and conferences. In my experience this is the most frequent reason people leave. Try and accommodate one conference and one training/certification per person per year. Always include training when implementing new tools."
- "We build training into the work flow every week. The training is driven by needed skills and current threat environment"

Security Challenges - Training

- Education & Training
  - Establish internal programs – especially important for non-traditional
  - Job Shadowing – good training for existing staff and interns
  - Certifications – target & support the most valuable to your organization
  - Conferences and events – support competitions and hands-on
  - Support degree programs – 2 yr, 4 yr, and advanced degree options
  - Learn the options for each degree path and connect with higher ed
  - Explore grants and other funding sources for business

The Power of Formal Security Education

"I began MSST as a part time security guard with a BA in English, and no IT background. 5 years later, I have been a corporate security specialist, an IT security consultant, and a threat/malware hunter. At this point, the sky is the limit. MSST taught me how to focus on the big picture, translate security issues into business risks, and smartly prioritize own skills development in an industry where there is simply too much for any one person to know."

"MSST enabled me to take my general aptitude for technology and prepare me for a specific career in cybersecurity. The program cultivated an interest that I was able to - through long hours and hard work - apply toward advancing my career."

"As a former marketing professional, I had very few hard skills in the security industry. MSST not only provided me with a robust knowledge of information and cyber security foundations, it also taught me to think like a security practitioner… tactical exercises in risk assessment helped me in my current role, as did the understanding of security policy and procedures… My security education gave me an solid introduction to the security 'language' that my colleagues and clients speak, and my classmates became a security network I can count on…"

Cyber Education

Mn(C)3 MINNESOTA CYBER CAREERS CONSORTIUM

THE FORMULA FOR SECURITY

MnC3.org

Mission: To advance the professional development of Minnesota talent to address cyber risks.

TECHNOLOGICAL LEADERSHIP INSTITUTE

Cyber Education

MnC3 Goal is to positively impact this national issue starting here in MN

- MnC3 is about
  - Understanding the current state of needs & build pathways to fill the gap
  - Establish partnerships between education institutions and employers
  - Support outreach – education – collaboration – awareness
- Multiple institutions in MN that have targeted cyber education
  - Metro State – Contact Dr. Faisal Kaleem & Dr. Firasat Khan
  - Minnesota State Mankato – Contact Dr. Chris Velstos
  - St. Cloud State – Contact Dr. Tirthankar Ghosh
  - Technological Leadership Institute – Contact Mike Johnson
  - Multiple other MN institutions also offer targeted security education

Cyber Education – MS Security Technology

- The Master of Science in Security Technologies program builds a foundation for security through broad based understanding of Critical Infrastructure Protection.
- From that security and risk base, the program adds context for what has become a core consideration of security for nearly every critical infrastructure – “all roads lead through cyber”.
- Students get training where cybersecurity intersects with other key security disciplines, and gain an understanding of cybersecurity program requirements.
- The MSST program allows for deeper dives into areas of specific interest for the student or their funding employer, including classes like securing cyberspace and cyber threat intelligence.

Q&A