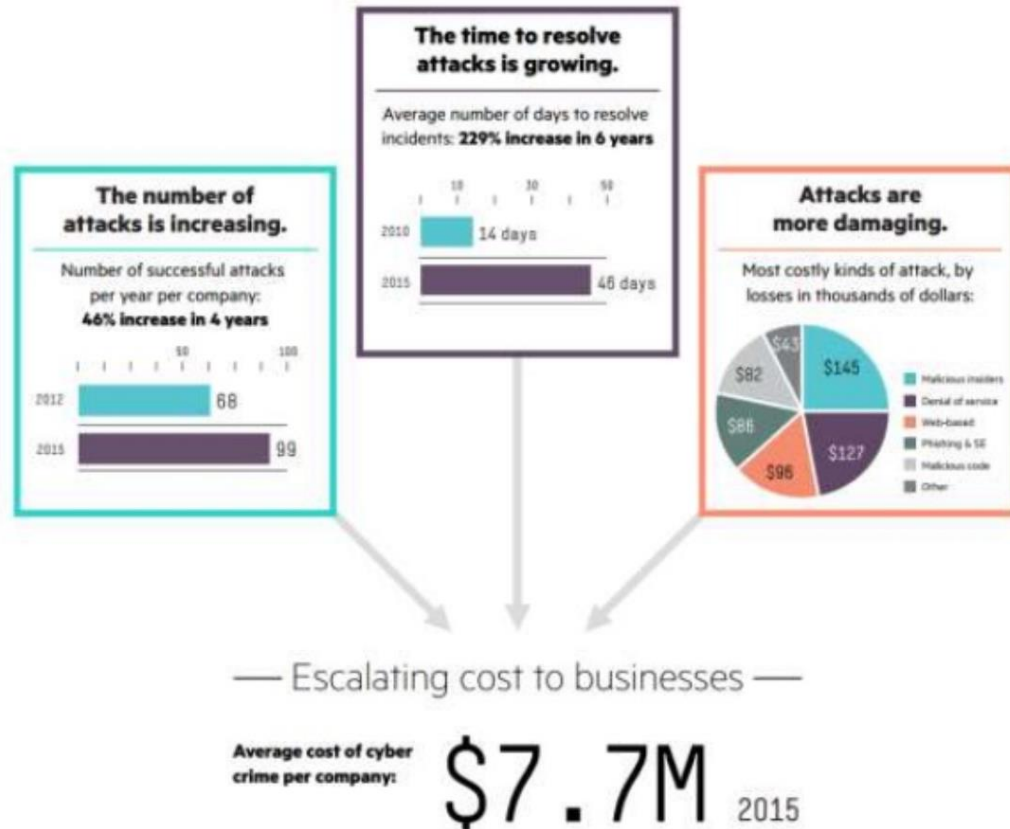# Attracting and Retaining Cybersecurity Talent

Cybersecurity job prospects

- ❑ One of the hottest fields
  - ❑ Expected to grow from $75b in 2015 to $170b by 2020
- ❑ Bureau of Labor Statistics information suggests more than 209,000 cybersecurity jobs in the U.S. are unfilled
  - ❑ Postings up 74% over the past five years
- ❑ Cisco reporting suggests 1m global job openings in cybersecurity
  - ❑ Demand expected to rise to 6m globally by 2019
  - ❑ Projected shortfall of 1.5m (according to Symantec)

Cybercrime is growing

The time to resolve attacks is growing.

Average number of days to resolve incidents: **229% increase in 6 years**

2010	14 days
2015	46 days

The number of attacks is increasing.

Number of successful attacks per year per company: **46% increase in 4 years**

2012	68
2015	99

Attacks are more damaging.

Most costly kinds of attack, by losses in thousands of dollars:

- $145 Malicious insiders
- $127 Denial of service
- $96 Web-based
- $88 Phishing & SE
- $82 Malicious code
- $43 Other

— Escalating cost to businesses —

Average cost of cyber crime per company: $7.7M 2015

Source: 2015 Verizon DBIR Report; ITRC ; HP 2015 Cost of Cyber Crime Study; The Global State of Information Security Survey 2015; McAfee Net Losses – Estimating the Cost of Cybercrime

What everyone (should be) looking for

- ❑ Broad Technical Knowledge
  - ❑ This is the basic requirement
  - ❑ Specific requirement of a particular system can be outdated quickly and/or limit consideration of alternative responses
- ❑ Focus on Detail
  - ❑ Ability to stay with problem at a small detail level until solved
  - ❑ Answers often obscured by misdirection
- ❑ Security Instinct
  - ❑ Understanding how incidents are developed and having a sense of what is happening
  - ❑ Only developed through hands-on experience

Where to begin

- ❑ Recognize you will need to train cybersecurity your future professionals
- ❑ Determine which jobs you can bring entry level candidates into immediately
  - ❑ Vulnerability Assessment
  - ❑ Level 1 SOC Analyst
- ❑ Hopefully, all areas can identify an entry level position
  - ❑ Some areas may need more advanced entry level
    - ❑ For example, Penetration testers may come from SOC analysts
  - ❑ Do not underestimate the need for technical knowledge in all areas – including compliance

Where to begin

❑ Step 1: Train your trainers

    ❑ Make sure the people you have can train the people you need to bring in

    ❑ Train in basic management and communication as well as technical skills

❑ Step 2: Document processes

    ❑ Entry positions identified should lend themselves to detailed repeatable processes

    ❑ Document these processes in detail

Where to begin

- ❑ Step 3: Hire your farm team
  - ❑ Hopefully with good, broad basic technology skills
  - ❑ Good attitude, ready to work and learn
- ❑ Consider hiring through a contractor
  - ❑ Contract to hire

Where to begin

❑ Step 4: Create paths for upward mobility within team

    ❑ i.e. level 1 SOC analyst to level 2 SOC analyst

    ❑ Current team members could become team leads of small groups and eventually managers of larger groups

❑ Opportunities for growth will help with retention

    ❑ Top reason cybersecurity professionals leave their current position is they don't see an opportunity for growth

    ❑ Continued training and develop also key to retention

Where to go next

❑ Always be on the lookout for great "free agents"

- ❑ Especially where they fit into your system
- ❑ Can also help expand your system and structure as you grow

Three Basics of Cybersecurity Team retention

❑ Substantive, regular technical training

Three Basics of Cybersecurity Team retention

❑ Regular Feeding

Three Basics of Cybersecurity Team retention

❑ Big Monitors