The Value of IT Certifications:

Fair and reliable means to assess and professionalize our evolving industry

cybersecuritycc.org

October 2018

Cybersecurity Credentials Collaborative (C3)
Overview

- Formed in 2011 to provide awareness of and advocacy for vendor-neutral credentials in information security, privacy, and related IT disciplines. The C3 provides the cybersecurity industry with a collaborative forum to address matters of shared concern.
- The C3 has furthered the professionalization of our industry via the Unified Framework of Professional Ethics for Security Professionals.
- This presentation provides some basic data and evidence gathered from C3 member organizations to substantiate the continued importance of our shared industry's certifications.

CERTNEXUS CompTIA GIAC CERTIFICATIONS iapp international association of privacy professionals ISACA (ISC)²

Certification Benefits:
Industry Professionalization

- There is a documented and increasing need for cybersecurity professionals with demonstrable skills. Certifications provide a common baseline for hiring managers, job seekers and technical practitioners across the globe.
- All established, reputable industries have common codes of ethics which are agreed upon by professional industry associations. To help further professionalize the cybersecurity industry, the C3 established a Unified Framework of Professional Ethics for Security Professionals adopted by each C3 member organization and endorsed by the ISSA.
- Each C3 member organization has resulting individual codes of ethics which apply to individual certification holders, whereas the Unified Framework binds all of these individual codes and is applicable to the industry at large.

Cybersecurity Credentials Collaborative (C3)
Unified Framework of Professional Ethics for Security Professionals

Integrity

- Perform duties honorably, justly and responsibly, in accordance with existing laws, exercising the highest moral principles
- Act in the best interests of stakeholders
- Refrain from activities that would constitute a conflict of interest
- Report ethical violations to the appropriate governing body in a timely manner

Objectivity

- Perform all duties in a fair manner and without prejudice
- Exercise professional judgment in order to provide unbiased analysis and advice
- When an opinion is provided, note it as opinion rather than fact

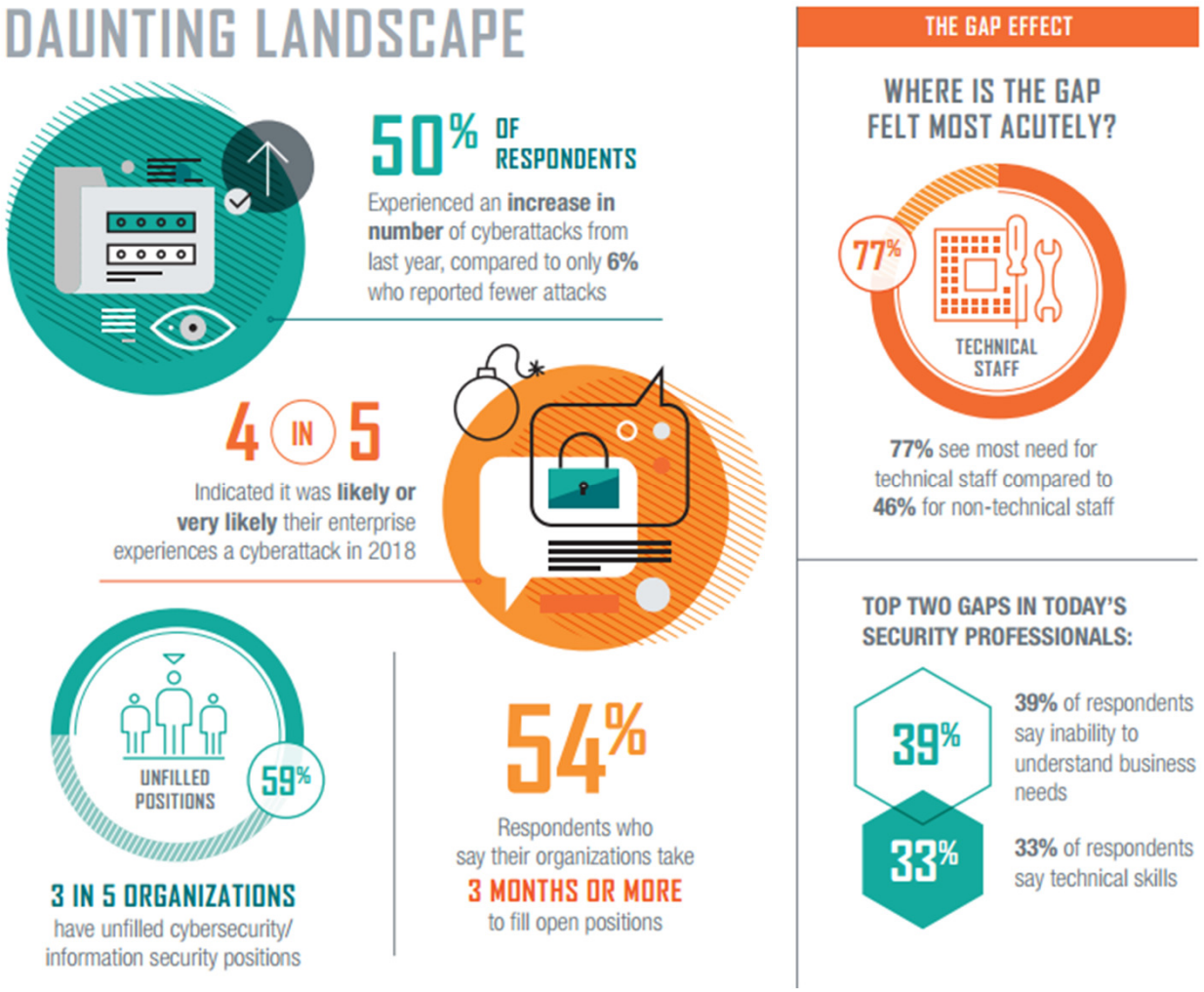
Confidentiality

- Respect and safeguard confidential information and exercise due care to prevent improper disclosure
- Maintain appropriate confidentiality of proprietary and otherwise confidential information encountered in the course of professional activities, unless such action would conceal or result in the commission of a criminal act

Professional Competence

- Perform services diligently and with professionalism
- Render only those services for which you are fully competent and qualified
- Recognize and acknowledge the contributions of others
- Refrain from professional misconduct which would damage the reputation of the profession
- Participate in professional development activities to maintain the skills necessary to function effectively

Market Overview:
Cybersecurity is an Increasing Focal Point for Enterprises



Source: ISACA State of Cybersecurity 2018

Market Overview:
Cybersecurity Jobs Posts are Growing and Harder to Fill

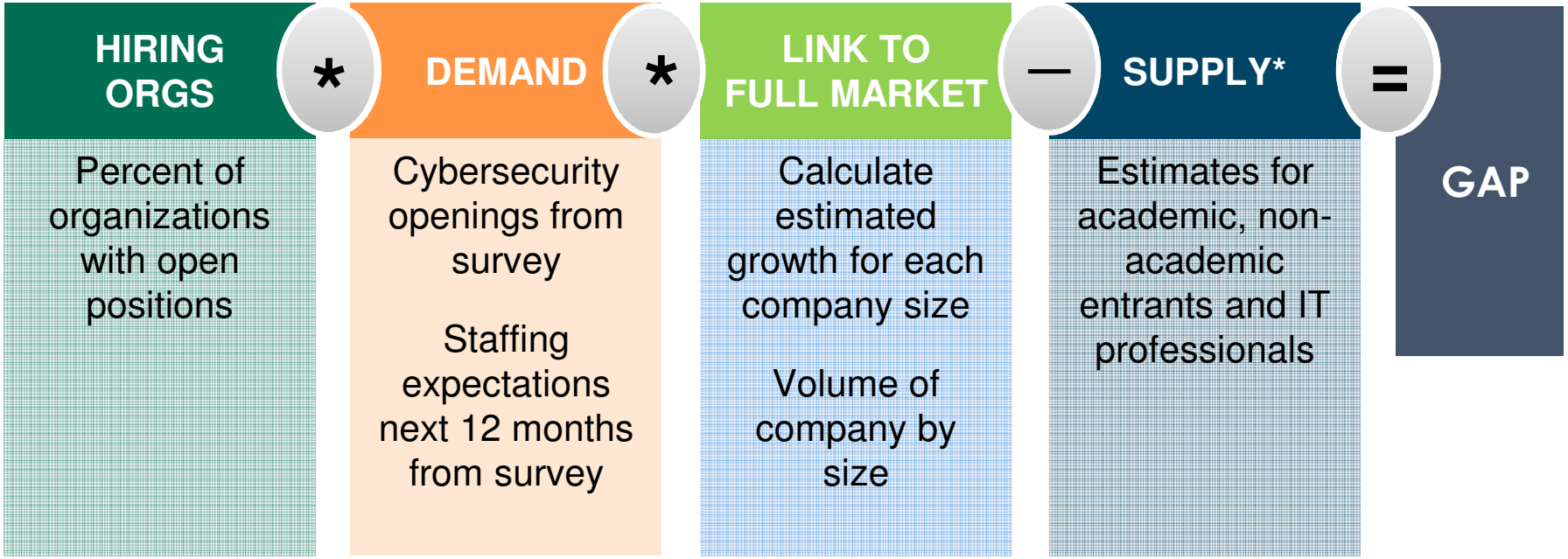
- In 2018 there are more than 300,000 cybersecurity job openings
- Total employed U.S. cybersecurity workforce in same period was 768,096
- 2.5 currently employed cybersecurity workers for every job opening
- By contrast, there are 6.5 current workers for every job opening overall, in what is already a tight labor market.
- Of the “core” cybersecurity roles, the largest demand was for Cybersecurity Engineers with 37,580 openings

Certifications help validate critical skill sets aligned to job openings

Source: Burning Glass Technologies 2018 ©

Market Overview:
Calculating the Gap in Cybersecurity Professionals

To calculate this, the survey captures total estimated cybersecurity professionals and expected future growth in headcount.



*Supply: represents partial supply impacts and reflect net new cybersecurity professionals from academia (19K) and organic market growth (364K).

Wharton estimates 1% of college prospects are aware of cybersecurity as a career. This factor is the multiplier to total 2017 graduates (1.9M), sourced from The Wall Street Journal. Organic growth factors include annualized projections from the Cybersecurity Workforce Alliance and estimated head count extrapolated from CompTIA 2018 Cyberstates annual report.

Source: (ISC)2 2018 Global Cybersecurity Workforce Trends Survey

Market Overview:
2018 Gap in Cybersecurity Professionals

The tables below provide an the estimated gap calculation within the US and the rest of world.

Geo: US	Median Cybersecurity Hires (Current market + future need, balanced)	Total Hiring Entities (link to full market)	Total Hiring Demand (link to full market)	Supply
Small (1-99)	10.29	16,989	174,750	New Academic Entrants: 19,000
Mid-market (100-499)	16.28	18,954	308,484	New Non-Academic Entrants: 164,763
Enterprise (500+)	40.44	6,008	242,986	Training IT Pros: 87,656
			726,219	**271,419**

US GAP: 454,800

Geo: Rest of World	Median Cybersecurity Hires (Current market + future need, balanced)	Total Hiring Entities (link to full market)	Total Hiring Demand (link to full market)	Supply
Small (1-99)	4	214,886	844,963	
Mid-market (100-499)	8	383,995	2,692,984	
Enterprise (500+)	12	19,561	273,573	Training IT Pros: 1,341,498
			3,811,520	**1,341,498**

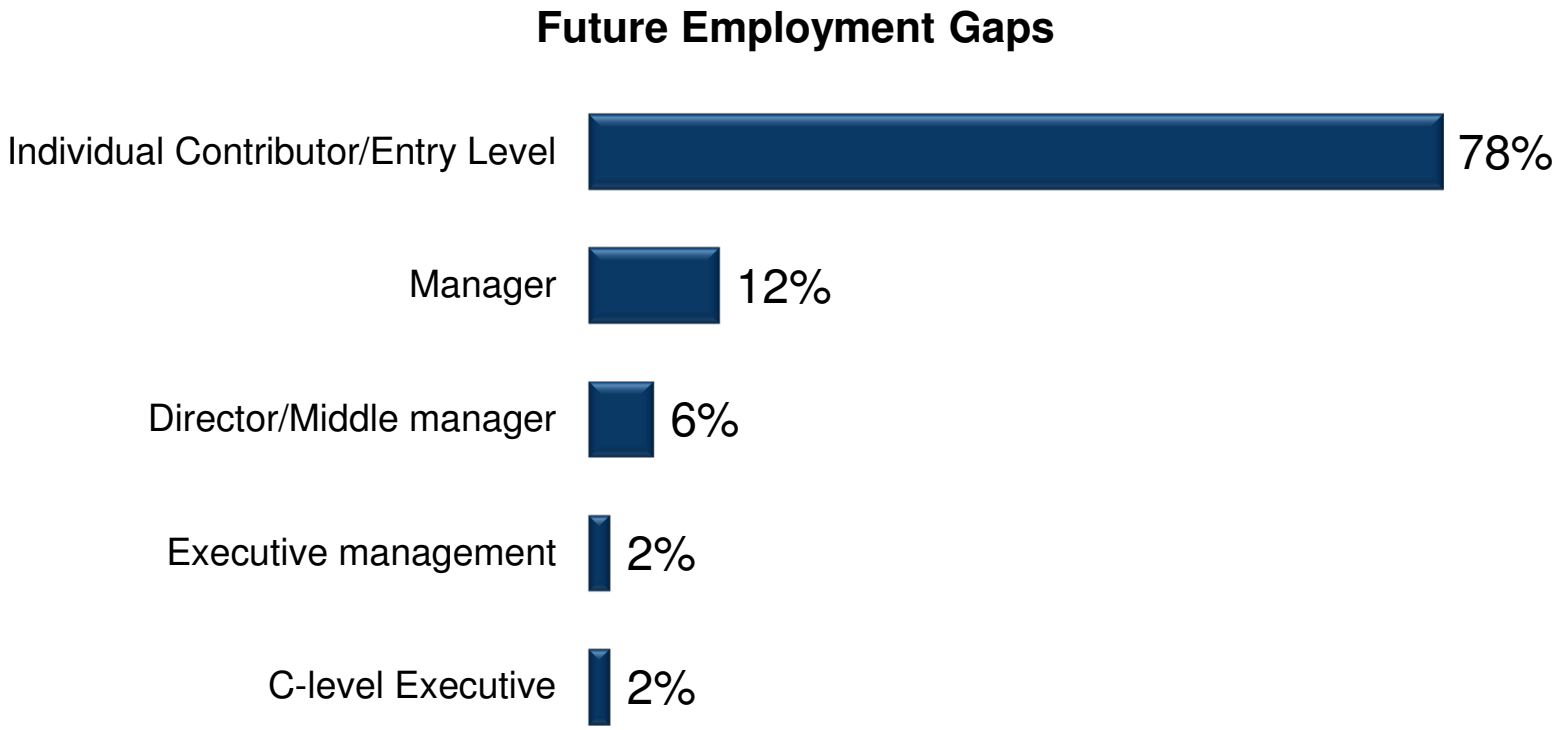
Rest of World GAP: 2,470,022

2018 Global Gap in Cybersecurity Professionals: 2,924,822

Certification programs help address this gap

Source: (ISC)2 2018 Global Cybersecurity Workforce Trends Survey

Market Overview:
What Experience Level has the Most Demand for New Hires?



The vast majority of security professionals anticipate the greatest need for future resources to be in individual contributor / entry level positions.

Certification programs reduce entry level skills gaps

Source: (ISC)2 Global Information Security Workforce Survey

Cybersecurity Credentials Collaborative (C3)

Certification Matters:
Certification is a Priority of Hiring Managers and IT Executives

- IT certification is a priority to 86% of hiring managers
- 81% of hiring managers expect IT certification to grow in importance
- 62% of IT and business executives agree IT certified staff have proven expertise
- 54% of IT and business executives agree their organization is more secure from malware & hackers due to staff with IT certifications
- 73% of IT and business executives agree it's important to test after training to confirm knowledge gains

Source: CompTIA International Technology Adoption & Workforce Trends

Certification Benefit:
Retention and Competence

Certification preparation leads to confidence

Well-trained IT professionals are more confident that the skills they possess are appropriate and useful for their responsibilities.

Validation reliably attests to the level of knowledge

Certified employees can be relied on to perform at a higher level and have more domain knowledge than untrained employees.

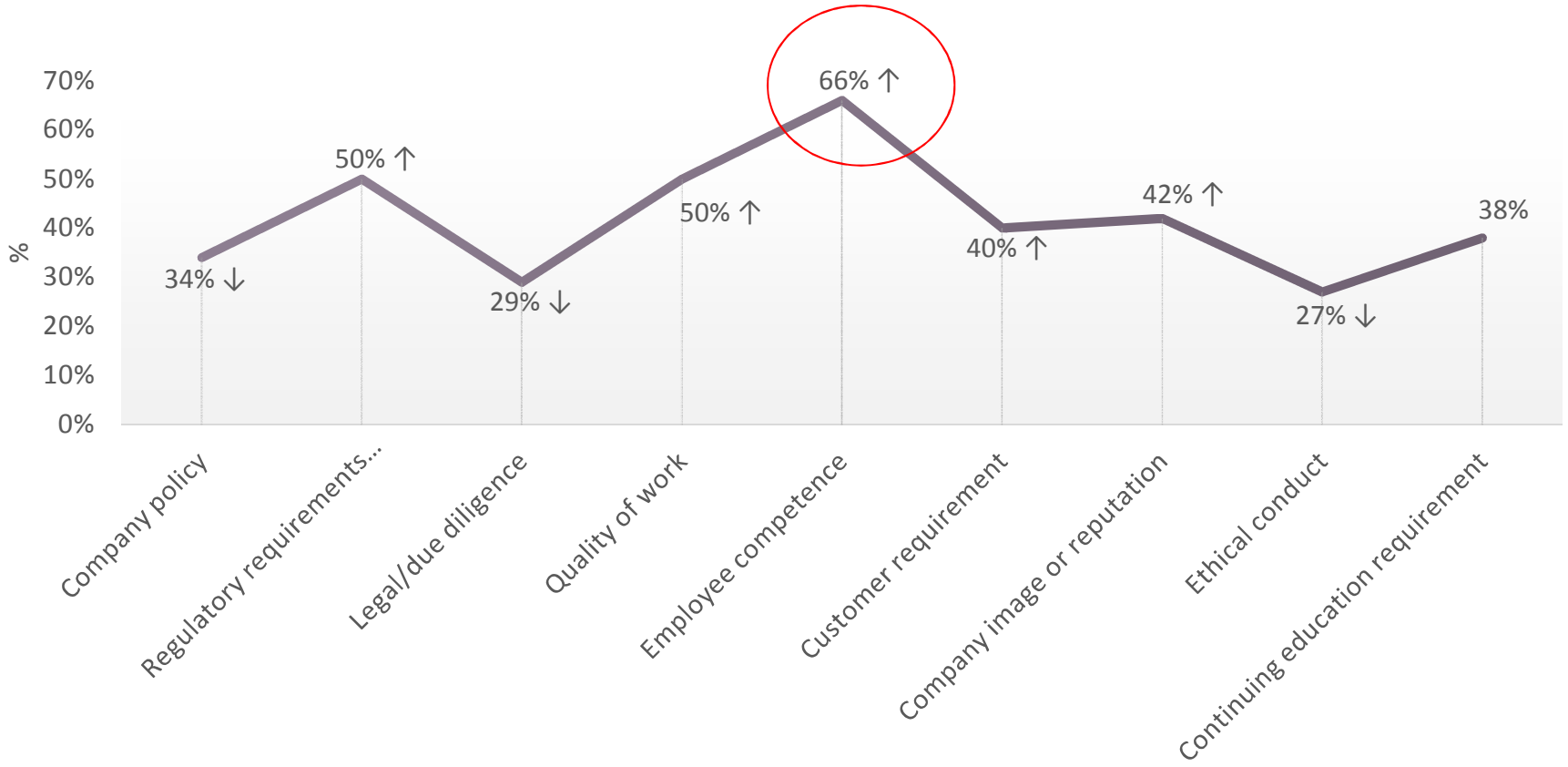
Business activities are executed more consistently

Certified employees can be expected to perform assigned tasks more consistently, increasing reliability and overall organizational execution.

Certifications increase confidence, knowledge and consistency

Source: CompTIA 2nd Annual IT Career Insights

Market Overview: Certification Justification



Certifications validate employee competence

Source: (ISC)² 2017 Global Information Security Workforce Survey

Cybersecurity Credentials Collaborative (C3)

Employer Benefit:
Productivity

Certified team members:

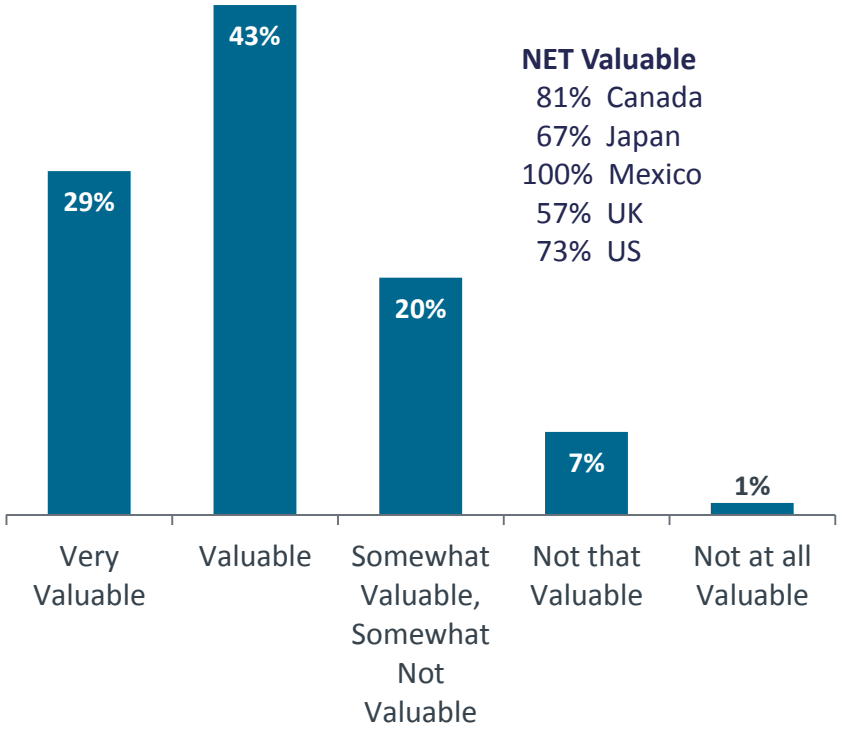
- Perform work faster (44%)
- Possess sought after expertise within organization (39%)
- Implement systems more efficiently (33%)
- Deploy products and services more efficiently (23%)

Greater impact on workflow and productivity

Source: 2017 Global Knowledge IT Skills and Salary Report

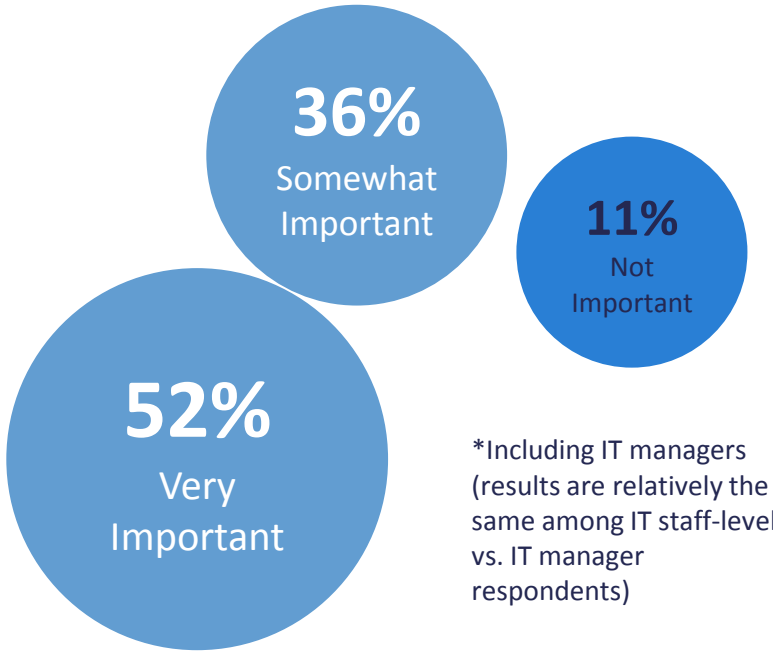
Employer Benefit:
Valuable to IT Managers

Managers' Rating of Value of IT Certifications



Valued by 72% of IT managers

IT Pros' Opinions of Testing After Training to Confirm Knowledge Gains*



*Including IT managers (results are relatively the same among IT staff-level vs. IT manager respondents)

89% support post-training assessment

Source: CompTIA *Evaluating IT Workforce Needs* | Overall results, n=213 IT managers | n=1,802 IT pros

Employer Benefit: Retention

Overall

68% Stayed with employer after certification
15% Didn't leave after certification, but wanted to or hope to soon
11% Left employer to work somewhere else some time (> 6 months) after certification
6% Left employer to work somewhere else shortly after getting certified

NET Stayed by Country

83% Overall
78% Canada
93% Japan
89% Mexico
77% UK
80% US

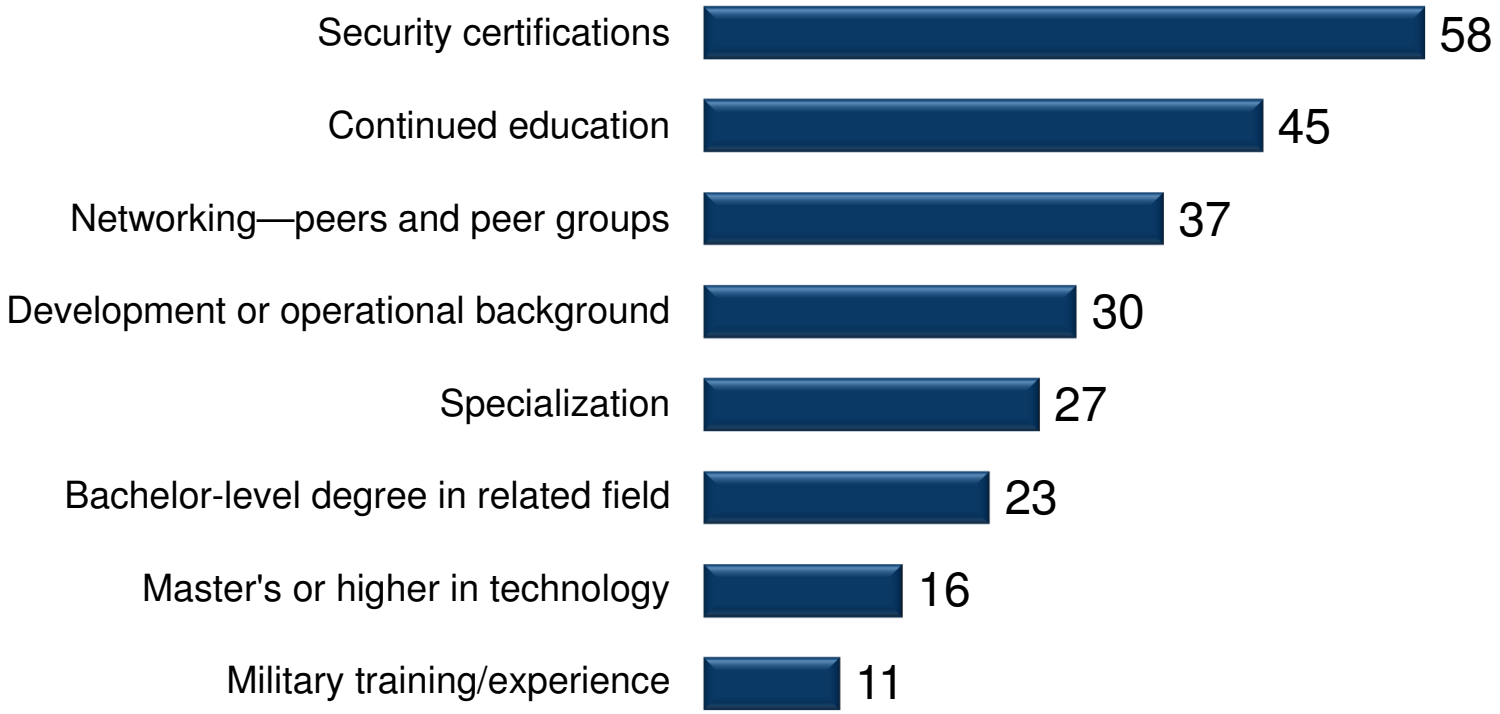
Note: Consider that many factors may influence retention such as job satisfaction, age, etc. For instance, retention rates tend to rise as age increases.

Majority (83%) stay with employer after getting certified

Source: CompTIA *Evaluating IT Workforce Needs* | Overall results n=1,398 IT pros employed at time of certification

Employee Benefits: Career Success

What are the biggest contributing factors to your career success so far? Select all that apply.



Certification programs contribute to career success

Source: SANS Salary Survey and Cyber Security Professionals Trends