Solving the IoT Security Talent Gap: Where You Look Matters

Published 8 March 2018 - ID G00347310 - 15 min read

By Analysts Barika Pace, Ruggero Contu

Initiatives:Infrastructure Security

The alignment of IT and OT is inflating security risks for IoT, creating high demand for veracity in security specialists. IoT means security and risk management leaders must transform their organizations to meet digital risk, while facing a competitive labor market.

Overview

Impacts

- The mean salaries for cybersecurity professionals are set to rise in 2018, and they have grown over the past three years. However, those professionals with necessary business competencies to meet Internet of Things (IoT) security demands are often out of reach for some organizations' budgets.
- The unemployment rate for security professional is close to zero, extending the lead time to fill vacancies.
- Many organizations struggle to find experienced digital security leaders with the right mix of business knowledge, IoT knowledge and artificial intelligence (AI) experience, delaying companies' abilities to execute on digitalization and IoT initiatives.

Recommendations

To mitigate security risk in the face of IoT security hiring challenges, security and risk management (SRM) leaders must:

- Look internally, and weigh the cost of hiring an external candidate against the cost of training an internal candidate to ease budget woes.
- Diversify recruiting sources by working with human resources to build a talent pipeline, partnering with local certification programs and focusing on underrepresented communities.
- Hire leaders outside of IT where possible, to build the security organizations' business acumen needed to address digital business risk created by IoT.

Strategic Planning Assumption

The number of unfilled cybersecurity roles is expected to grow from 1 million in 2018 to 1.5 million by the end of 2020.

Analysis

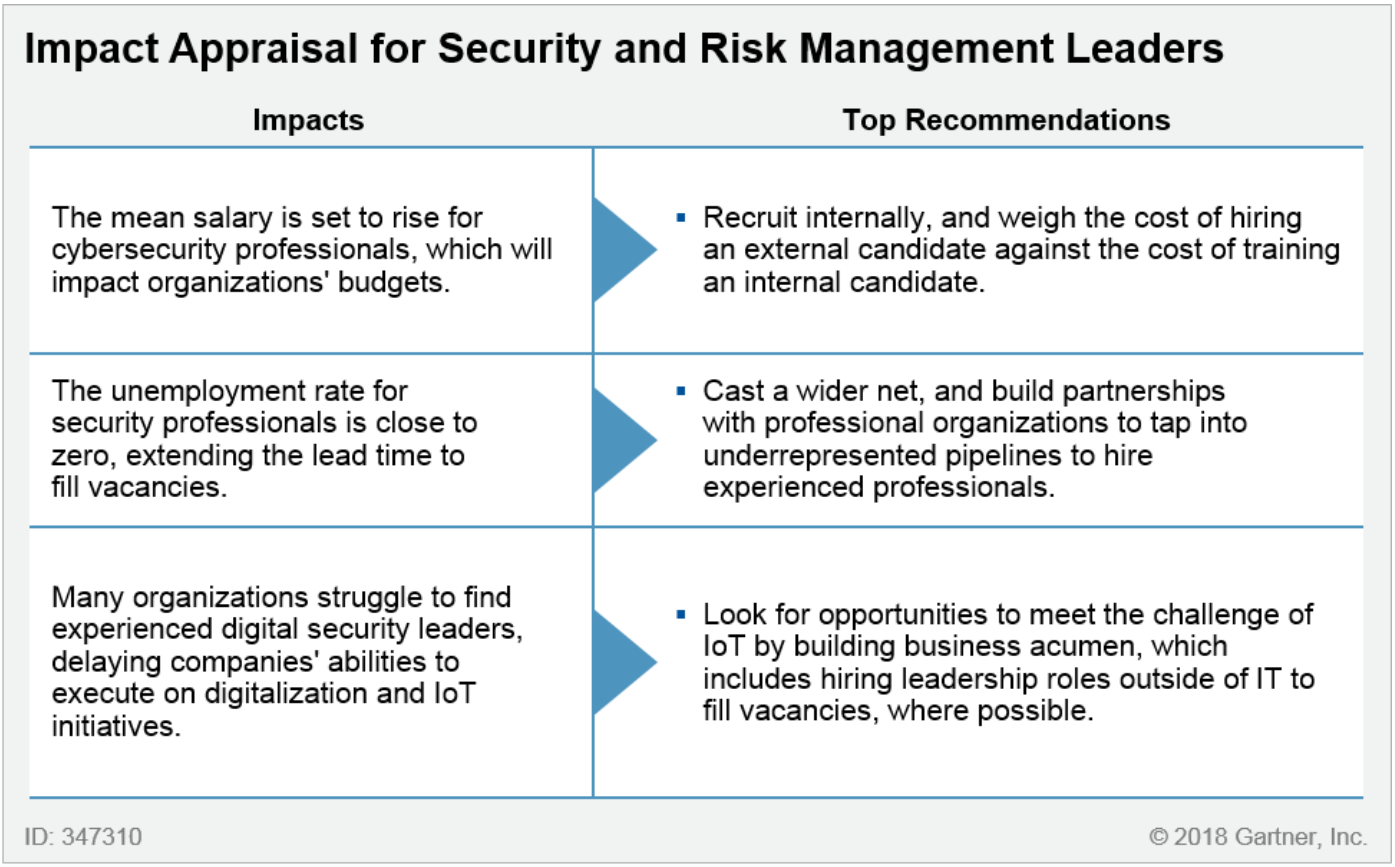
The convergence of IT and operational technology (OT) continues to expand the risk landscapes, creating high demand for security specialists with combined security expertise and operational knowledge. The future of security is no longer confined to the corridors of cubicles. According to the most recent Gartner security and risk survey, 86% of respondents say the digital world is creating new business risk. The next-generation digital security organization sits on the edge with an imaginative eye toward the next threat. The future of digital security is as much an IT institution as it is an operational arm ensuring reliability and safety through the IoT ecosystem. To accomplish this cybersecurity, organizations must amend their core skill sets, meaning organizations' competencies will become more versatile not only to account for challenges faced by IoT technology trends and IT/OT alignment, but also to address their present talent shortage.

Many organizations continue to look for a cybersecurity "jack of all trades" capable of addressing OT and IT security issues within IoT. However, the search often falls short of candidates having the operational knowledge, physical security expertise, IT and risk management capabilities. The skill set for cybersecurity professionals continues to evolve, and so must the places that SRM leaders look to fill vacancies. Modifying where you look to fill vacancies can impact the ability to meet the demands of IoT security.

Impacts and Recommendations

Figure 1 shows the impacts and top recommendations for security and risk management leaders.

Figure 1. Impacts and Top Recommendations for Security and Risk Management Leaders



Source: Gartner (March 2018)

The Mean Salary Set to Rise for Cybersecurity Professionals, Impacting Organizations' Budgets

Today's digital security organization struggles to meet increased demand to manage the scale of IoT security risk, and salary increases are impacting budgets. Gartner conducted its 2017 Security and Risk Survey with 712 respondents. The survey revealed that 22% of respondents believed salary expectations for security professionals were too high, and 33% of respondents said they did not have the budget to hire cybersecurity professionals.

Furthermore, PayScale (a U.S. firm tracking compensation for 6,500 customers globally), noted an increase in the U.S. mean salaries from 2014 through 2017 for cybersecurity roles. The increases averaged between 12% and 18.8% since mid-2014, with the highest increases coming at the management levels. The U.K. and Canada have experienced similar compensation pains. A regional look at a 2017 survey conducted by CWJobs.co.uk reveals a 16% increase in the U.K. for similar roles. SRM leaders are facing an uphill battle as a result of this compensation increase, coupled with the costs of recruiting external candidates

Hire Internal Candidates With Experience to Address IoT Operational Risks

The IoT security hiring landscape is challenging due to high operational competency requirements impacting SRM leaders' ability to scale for IoT. While traditional cybersecurity focuses on protection systems, IoT requires the projection and integrity of operational processes, as well.

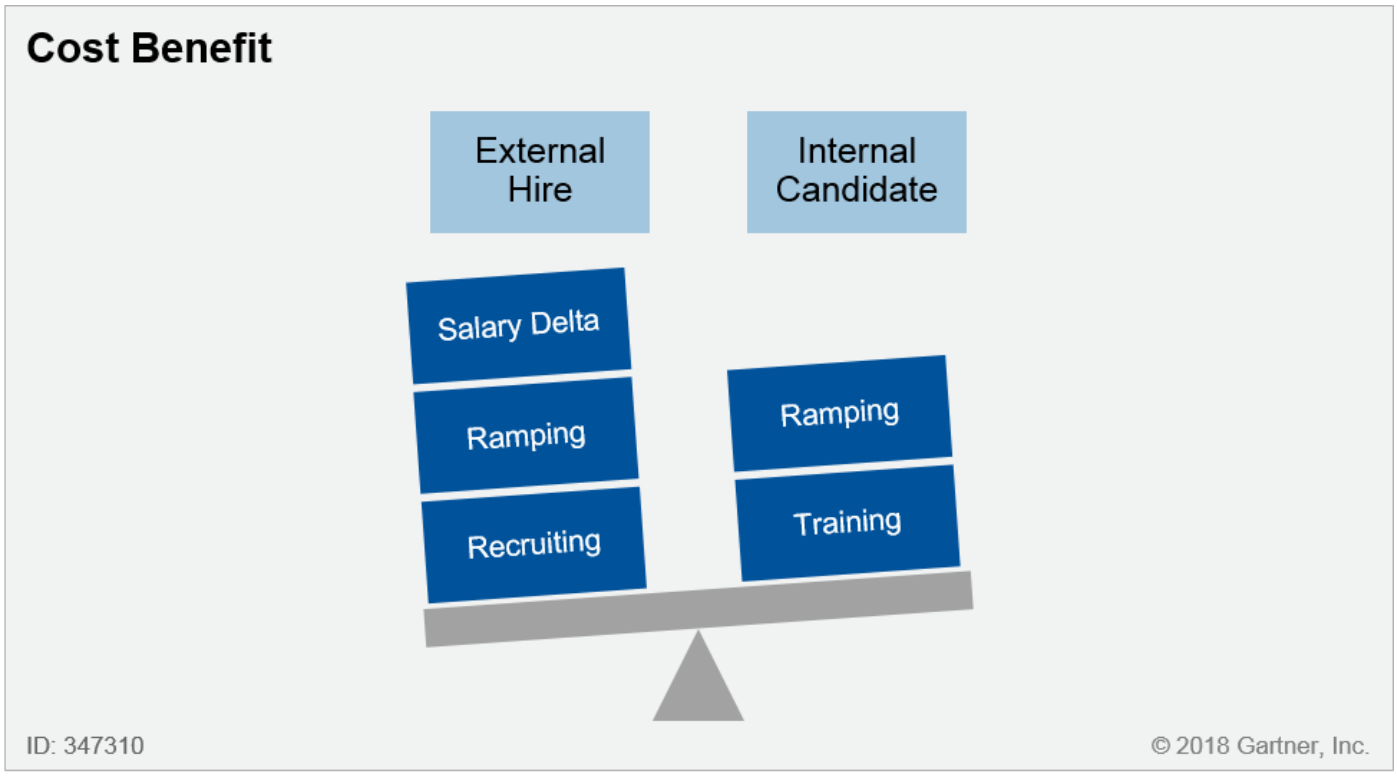
To meet this challenge, develop an organizational skills inventory to both match existing talent pool skills and identify gaps. Factor in the operational knowledge required to strengthen the IoT security posture. This strategy will mean adding more operational and business competencies to any existing skills inventory. Using your skills inventory, work with HR to identify internal candidates that sit outside the security functions and that can fill existing vacancies against the current gaps.

For example, one enterprise took advantage of a workforce reduction at its local area plant to backfill an open security awareness training role within connected factories. The candidate, a manufacturing engineer, had intimate knowledge of the factory floor that allowed the security organization to communicate security policy in manufacturing terms. The company also hired a veteran electrical engineer into its red team. This team focuses on multilayered attack simulations that are designed to measure how well a company's people and networks, applications and physical security controls can withstand an attack from a real-life adversary. This approach accelerated the team's ability to conduct penetration testing for aviation IoT offerings. The manufacturing engineer was able to serve as a subject matter expert, identifying process gaps, as well as improving countermeasures for the organization.

Calculate the Cost Benefits of External and Internal Hires

Calculating the external hiring cost against the cost to train the internal candidate (see Figure 2) can help organizations determine what resource investments to make to ease budget woes.

Figure 2. Cost Benefit: Internal Versus External Candidate Choices



Source: Gartner (March 2018)

IoT security provides a unique opportunity for SRM leaders to weigh both the cost of hiring externally and the cost of training an internal candidate in security competencies.

Leverage HR professionals, and actively review talent needs against internal resources available in other functions. HR staff may be in a position to identify candidates looking to make a career change. Depending on the role, there may be a need to train the internal candidates. One advantage is that some candidates may have an existing network internally within the organization, thus having a working knowledge of the business process. Considering IoT requires not only skills necessary to protect systems, but skills necessary to protect underlining business processes. The ramp-up time may be shorter training an internal candidate.

Shortening the Runway to Productivity

Taking a vested existing employee (or even someone with no experience), and incentivizing him or her to pursue certification or continue an education program in security can be more cost-effective than outsourcing or hiring an external candidate. Even national top-ranked colleges and universities offer affordable continuing education as an option to develop cybersecurity professionals. For example, Harvard University now offers a cybersecurity certificate through its extension school, providing students with four core courses. The school even offers a course focused solely on security challenges of the IoT and big data. The average cost of the program is $10,000. Compare this cost with hiring a certified information systems security professional (CISSP) candidate who takes 10% longer to find and may come with a premium pay tag of $17,000 a year or more. (For more information, see "Adapt Your Traditional Staffing Practices for Cybersecurity.") Creating a tuition reimbursement program that encourages the employees to stay, by tiered payback approach based on tenure, may also incentivize employees to remain onboard.

While these programs could take up to a year to complete, find areas in which the internal candidate can offer immediate value while taking courses in parallel. For example, one enterprise hired a manufacturing data analyst for its security analyst role. While the analyst was completing the security certification program, he used his data visualization skills and manufacturing knowledge to create a security key performance indicator (KPI) dashboard for the enterprise's connected factories, adding immediate value to the team. Weigh the options of waiting six to nine months to fill the role with the idea candidate, against the immediate impact of hiring an experienced candidate from the internal organization. By the end of the security certification program, the analyst had the needed skills for his role in threat detection, and he simplified processes that may have required additional head count.

Recommendations:

- Develop a skills inventory that accounts for operational experience needed to improve the organization's IoT security posture.
- Look internally for candidates who might fit into your security organization, and leverage their business experience to improve your IoT security profile.

- Make use of certification and training to boost competencies in cybersecurity, when needed.

Unemployment Rate for Security Professionals Is Close to Zero, Extending the Lead Time to Fill Vacancies

According to Gartner research and several job market reports (including from the U.S. Bureau of Labor Statistics), the unemployment rate for U.S. information security analysts is next to zero (see "Develop a Pragmatic Vision and Strategy for Digital Business Security"). By 2020, the estimated number of computers and mobile phones will reach 50 billion, but sensors and controllers for related IoT devices is estimated to reach 1 trillion. In addition, a Federal Trade Commission's (FTC's) report revealed 10,000 connected households can generate 150 million discrete data points a day. IoT is growing the need for security professionals who can face the challenges of new threat surfaces, provide data security across an even vaster landscape and address the issues of privacy brought on by IoT.

The U.S. Bureau of Labor Statistics estimated the growth rate in job demand for security professionals would grow an additional 28% for a 10-year period starting in 2016. Indeed, a global recruiting platform, reported in mid-2016 that only 66.5% of U.S. cybersecurity jobs posted received clicks (score of 100% represents the correct balance between employer demand and job seeker interest). The Indeed analysis went on to establish that job posting to job seeker mismatches existed across Europe, Brazil and Canada as well. This finding means that going a traditional route of posting a job, and waiting for candidates to apply, is an ineffective approach in the cybersecurity job market. For organizations struggling to meet the demands of managing security for IT and OT environments, this situation can impact the ability to cover both domains. Do not depend solely on traditional recruiting strategies.

Proactively Network to Tap Into Hidden Pipelines

Do not wait for the job post click to make connections with potential candidates. Cast a wider net, and partner with organizations representing underrepresented groups, such as women, minorities, veterans and retired people. There is a growing pipeline of experienced employees in underrepresented groups.

A 2017 study conducted by the Center for Cyber Safety and Education found that increasing numbers of women (in 170 countries) are completing degrees in information security. However, the study also found that women are globally underrepresented in the cybersecurity profession (at 11%), much lower than the representation of women in the overall global workforce.

For experienced hires, consider participating with the WiCyS. The WiCyS organization, with support from a National Science Foundation grant, launched an initiative in 2013 that focuses on partnering with corporations to highlight opportunities for women in the U.S. and the U.K. The group has ongoing recruiting resources for corporations that can elevate your openings beyond some traditional posting sites. Even for experienced hires, untraditional channels, such as Hire Our

Heroes (see Note 1) and the International Consortium of Minority Cybersecurity Professionals (ICMCP; see Note 2), can be effective hiring channels.

Start Building a Talent Pool Now

As discussed earlier, the scale of IoT will mean the talent crunch will continue. Consequently, this means proactively planning for future hiring needs. SRM leaders must build a future talent pipeline by early identification of qualified people through relationships with academic institutions. (See "CIOs Should Use Universities and Nontraditional Alternatives to Build Talent Pipelines.") A number of organizations are creating events like hackathons. Hackathons have become one of the ways that organizations — particularly organizations characterized as leaders — experiment with new talent, work and organization models (see "Survey Analysis: What Leading Enterprises Do Differently With Talent and Organization").

As the need to hire security professionals is impacted by the proliferation of IoT devices, the ability of organizations to hire a mix of experienced and entry-level talent remains a challenge. The No. 1 barrier to IoT adoption in Gartner's 2017 Security and Risk Survey remains cybersecurity resource and competency gaps to address IoT risk (see "2018 Planning Guide for the Internet of Things").

Recommendations:

- Cast a wider net, and build partnerships with professional organizations to tap into underrepresented pipelines to hire experienced professionals.
- Start building your talent pool early by raising brand visibility locally by offering co-op programs and training opportunities to local schools and organizations.

Many Organizations Struggle to Find Experienced Digital Security Leaders, Delaying Companies' Abilities to Execute on Digitalization and IoT Initiatives

The 2017 Security and Risk Survey also found that 39% of organizations are struggling to find experienced digital security leaders with IoT and AI experience, delaying companies' abilities to execute on digitalization and IoT initiatives. As digital technology advances, the ability to manage IoT security across vast entry points and surfaces means a one-size-fits-all security leader does not exist. Organizations that struggle to find the perfect candidate for leadership as they embrace IoT may find candidates by checking for complementary competencies in areas of functional business expertise.

Take, for example, a late 2016 "hacktivist" attack on a U.S. commercial airliner; that investigation was completed mid-2017. The re-engineering of this IoT attack that targeted the jet engine's preventive maintenance systems required knowledge from a cross-functional team that included cybersecurity leaders, sensor enablement engineers and aviation leaders. As enterprises connect more things, cars, jets and cows (for example, for digitalization of agricultural data), the need for leaders to leverage cross-functional expertise becomes greater.

Take a macrolevel approach to building a total organizational competency picture at the leadership level. This means taking a skills inventory of the leadership team, identifying the present employee core competency, identifying competency gaps early and reducing duplication within the organization. Filling gaps may include additional training for existing employees. Also, this approach does not necessarily mean hiring more individuals. As "soft" skills like innovation and influence become critical to meet the challenges of IoT security, the chief information security officer (CISO) organization must adapt its leadership skill set and build business acumen.

The material effect on the demands on the team requires a deeper understanding of business processes. Hence, the team's effectiveness hinges on having the right skill mix at the leadership level. This translates into an increased need for leaders who can innovate and influence business partners to address IoT enterprise risk. (For more information, see "Adopt a Lean Digital Security Organization to Mitigate the Skills Shortage.")

Most CIOs seek to build versatility — an IoT key driver of digital transformation — into their organizations as they embrace this transformation. IT organizations are shifting to multidisciplinary teams that are at the heart of the bimodal transformation. CIOs are also looking for staff that are more versatile and can take on a broader set of roles (see "Scaling Bimodal — Fusing IT With the Business: A Gartner Trend Insight Report").

SRM leaders must discover ways to attract top leadership talent internally, and build a pool of future talent. For example, if your organization has a leadership training rotation (a program focused on high potential early career individuals), finding opportunities to include these individuals in IoT security projects is an option. This strategy can elevate your organization's visibility and attract future leaders. Remember, IoT requires leadership to have greater knowledge of business processes and risks. Future leaders will require a greater mix of business and technical skills. This skill set can also provide the organization with an infusion of business acumen from leadership program rotation members.

Keep in mind the nature of IoT: Business leaders are forging ahead with their digital business initiatives, and those leaders are making technology-related risk choices every day, frequently without realizing the significance of what they are doing. Exposing future leaders to digital security has the benefit of providing short-term support to the security function. In addition, when a final rotation leads the candidate back to the business, an even longer-term benefit of raising the enterprise risk awareness posture can be realized. (See "Cybersecurity and Digital Risk Management: CIOs Must Engage and Prepare.")

Finally, make the rounds to raise your profile with prospective top leadership talent internally. Share the work security with other organizations at roundtables, town halls or internal social media platforms outside of IT. Working with manufacturing and supply chain partners to engage employees about opportunity and importance of digital security not only keeps security top of mind, but also provides employees with an opportunity to understand its importance as a potential career path.

Recommendations:

- Make security an opportunity for candidates outside of IT, especially if your organization has a leadership rotation or leadership development program.
- Raise your organization's profile internally by participating in town halls, roundtables and internal social media to engage prospective leaders.

Evidence

Gartner's Annual Global Risk and Security Survey, 2017

"What Is the Average Salary for Cyber Security Jobs?" CWJobs.co.uk.

"Global Information Security Workforce Study (GISWS)," Center for Cyber Safety and Education.

"Gifts Inspire Teens to Explore Technology," Eastern Michigan University's 2013 University and Foundation Annual Report.

"Internet of Things: Privacy & Security in a Connected World," FTC's Staff Report.

"Indeed Spotlight: The Global Cybersecurity Skills Gap," Indeed blog.

"Average Salary for Skill: Cyber Security," PayScale.

"Diversity in High Tech," U.S. Equal Employment Opportunity Commission.

"Information Security Analysts," U.S. Department of Labor, Bureau of Labor Statistics, Occupational Outlook Handbook.

Note 1
Hiring Veterans

Hire Our Heroes works with businesses to assist in the transition from military experience and skills to civilian work. Many of these candidates have gained valuable security experience in the military, but they are often overlooked.

Note 2
Hiring ICMCP

Organizations such as the ICMCP offers biannual events in which companies can make face-to-face connections with experienced candidates. The organization also offers a job posting service.

Recommended by the Authors

10 New Information Security Roles for the Digitization Era

Predicts 2017: IT and OT Convergence Will Create New Challenges and Opportunities

Demystify Seven Cybersecurity Myths of Operational Technology and the Industrial Internet of Things

How to Organize Security and Risk Management in a Converged IT/OT Environment

Maverick* Research: Disband Your Security Team Now

Adapt Your Traditional Staffing Practices for Cybersecurity

CIOs Should Use Universities and Nontraditional Alternatives to Build Talent Pipelines

Survey Analysis: Gender Diversity in Security and Risk Management Provides the Talent to Address the Skills Shortage

Recommended For You

Promoting Psychological Safety to Further Innovation

Strategic Planning: 3 Critical Pitfalls and How to Avoid Them

Digital Goldman Sachs: Five Lessons from Goldman Sachs and What They Could Herald for Business

Value Stories to Tell About Your Digital Initiatives

Infographic: Supporting a Midsize Digital Enterprise at Scale