Experis™
ManpowerGroup

PROTECTING YOUR ORGANIZATION IN A TALENT-SCARCE MARKET

Information Security

INTRODUCTION

Recent high profile security breaches have moved information security from a hidden corner of the IT function to front page international news. **It has become a topic of strategic importance to both business and society.** As organizations grapple to find solutions, they now face a widening security talent shortage that further complicates an already complex situation.

Based on recent global IT skills research[1] conducted by Experis across 10 major markets, this paper explores the impact of the security talent shortage, providing insights into the issues, along with guidance on how to minimize the associated risks.

The Experis global research was based on information gathered from those whose responsibilities included hiring decisions. One of the key findings of the research is that 32% of IT leaders mentioned information security as an in-demand and hard-to-find skill, both today and over the next 12 to 18 months. This compares to 18% with respect to software development, which was the next most popular skill. Access to adequate information security resources was identified as a primary concern of IT respondents, highlighting the increasing criticality of acquiring and retaining information security talent.

1/3 of IT leaders see information security as an in-demand and hard skill to find.

IT IS NO LONGER A QUESTION OF WHETHER INFORMATION SECURITY BREACHES WILL HAPPEN, IT IS A QUESTION OF **"WHEN"** *AND* **"HOW MUCH"**

1 — Experis IT Skills Research 2015

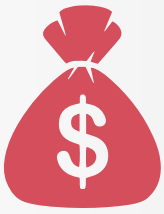
CURRENT SITUATION

Security under the spotlight

More than ever before, information security and the impacts of breaches have become mainstream topics of conversation. The seemingly endless parade of high profile cases in leading retail companies, financial institutions and government organizations is also serving to educate the public on the real impacts security failures have at the personal, professional and company level. Even mainstream media is embracing the theme, with prime time programs such as *CSI: Cyber* and *Mr. Robot*, which incorporate different fictional cyber threat scenarios derived from real stories. Whether the original goals of recent cyber-attacks were financial, political or personal, the net effect is an increasing number of C-suites and Boards of Directors who find themselves **forced to redirect more and more resources** every year toward dealing with **information security threats.** This has resulted in **increased demand for information security talent,** especially for the high-level expertise needed to plan and execute security strategies. Such strategies are required to combat the increasingly sophisticated threat environment that most organizations are facing.

$3.8 MILLION
average consolidated total cost of a data breach.

23% since 2013



$154
cost incurred for each lost/stolen record with sensitive information.

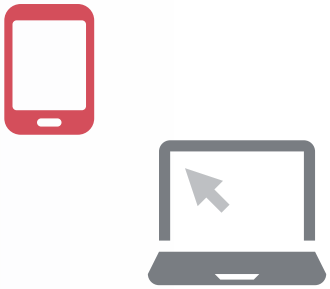
6% since 2013

38%
increase of security breaches in 2015 vs. 2014.

Keeping up with technological advances

Technology advances, coupled with increased interconnectedness, have provided society with tangible benefits. Clearly, the emerging "Internet of Things" that promotes interconnecting every device has produced **an explosion in the creation and exchange of information.** Virtualization, cloud computing and the expansion of processing power and data bandwidth in handheld devices **have enabled the creation, collection and sharing of various forms of personal, private and corporate information,** often through entirely new business models. Unfortunately, many users and providers have failed to understand (and deal with) **the consequences of improperly protecting this information, and have, unwittingly in many cases, created vast collections of personal and private data that are ideal targets for cyber attacks.**

In addition, the growing BYOD (Bring-Your-Own-Device) culture has created an environment where most asset management capabilities are inadequate to control the devices used in the workplace. **This has resulted in operational inconsistencies that quickly have become security vulnerabilities.** Clearly, the strong perimeter security architecture, beloved by many CIOs, can no longer adequately protect the business processes and information. However, providing more advanced governance that goes beyond simply locking down users through firewalls and network controls requires security talent that many organizations just don't possess.



"Many users and providers have failed to understand (and deal with) the consequences of improperly protecting this information..."

Experis

Stuck in neutral

Key themes from the recent RSA Conference 2015[2] reinforce the message that security concerns continue to escalate. They indicate that even though organizations are spending more money on information security, from a readiness perspective, they are 'stuck in neutral'.

Breaches are accelerating in terms of number, sophistication and impact. Both nations and organized criminals increasingly see the IT infrastructure of their targets as the best access channel, providing both a high rate of return and a low probability of arrest. They count on organizations having software issues such as poor process design and inter-process communications, which leave infrastructure and applications vulnerable. In addition, **common control areas impacted by inadequate resources,** such as poor access management, improper configuration management, limited maintenance, human error and inadequate oversight, all create exploitable chinks in an organization's armor that can be exploited by motivated attackers.

A key factor that must be considered in assessing security is the perspective of the attackers which is much different than their targets' in terms of what level of investment is considered cost-effective. Attackers have shown they are adept at using readily available equipment to exploit their targets' weaknesses, often adopting a long-term attack plan that can wear down defenses. **Hackers are getting more sophisticated,** building malware into the tools and libraries used by others to develop application software. And, while attackers tend to gain access most often through persistence, they are also extremely opportunistic, exploiting vulnerabilities in a matter of seconds when the conditions are right.

Large organizations such as global banks spend hundreds of millions of dollars on protecting their data. While this level of spend is of course not feasible for many organizations, it also **draws the talent away from those organizations with smaller budgets,** thus leaving smaller organizations increasingly vulnerable. There are increasing incidences of attackers using third party vendors to compromise organizations and to infiltrate their network. Though third party vendor management is improving, often these third party vendors are not examined as thoroughly or as often as necessary. Thus, one cannot be certain that an adequate level of acceptable risk is being maintained, given these third parties face equal, if not greater, challenges in accessing adequate security resources.

High profile exploits have woken up organizations to the reality that they do not have sufficient security detection skills or appropriate security response plans within their organization to proactively address and combat increasingly sophisticated and frequent attacks. Some large breaches and newly targeted industries have triggered responses for increased controls within peer organizations. Many still display, however, **a reluctance to rapidly respond to attacks** and adopt defensive measures as a community. This is due, at least in part, to the shortage of available security resources to develop and implement the required solutions. The seemingly endless regulatory, legislative and contractual mandates that inevitably follow major breaches also drive **increased demand for information security talent.**

While some see the new security tools that are emerging as a useful alternative to hiring talent, these **often require specialized training or a learning curve** before they can be put to effective use, thus exacerbating rather than alleviating the talent shortage.

2 — RSA Conference 2015 Slides - https://www.rsaconference.com/writable/presentations/file_upload/prof-m01_status-of-the-industry-2015-global-information-security-workforce-study.pdf

Global security talent shortage

Unfortunately, the sheer number of positions being posted has so dramatically exceeded the available (worldwide) talent pool that **organizations are finding themselves increasingly in either a race or a bidding war with their peers to acquire and retain scarce, critical security skills.** This includes security roles beyond the cyber space domain. Recognizing that not all skills are in short supply, there is a huge demand for information security personnel, ranging from policy writers to ethical hackers and technical security solutions engineers.

The Experis research highlighted that many organizations are dealing with the talent shortage by turning to contractors to augment their internal staff. The respondents indicated that 40% currently use contractors in information security. Of these, 27% are planning to increase their use of contractors, while 40% will maintain the same level, citing cost effectiveness, flexibility and access to expertise as the reasons why they choose contracting as an option.

27%
of organizations will increase use of contractors

40%
will maintain the same level of contractors

A critical issue is that **the demand for key security talent outpaces the worldwide growth in the talent pool.** A recent study by Frost and Sullivan, referenced in the 2015 (ISC)2 Global Information Security Workforce Study[3], highlights a projected global growth in demand for information security professionals to be 2.5 million by 2019 while the supply is only projected to grow by about 1 million. The data in this report projects a compound annual growth rate (CAGR) of around 10% in security talent demand, but only a 5.6% CAGR in the supply from 2014 to 2019. These projections indicate the security talent situation is unhealthy, and **unless actions are taken to reduce the talent gap, the shortage is likely to worsen over time.**

global demand of
2.5 Million
by 2019

This projected 1.5 million resource disparity between positions and candidates will place significant upward pressure on information security labor costs, increasing pressure on hiring organizations to lower the quality bar with respect to what is considered an 'acceptable' level of competence to fill long-term vacancies. Unfortunately, trying to shortchange security will only exacerbate the problem and result in higher risks to the organization.

1.5 Million
disparity between positions and candidates

3 — Information Security Workforce Study - https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf

COMPLICATIONS

As if the current situation wasn't challenging enough, organizations of all types need to prepare for a more complicated and complex information environment.

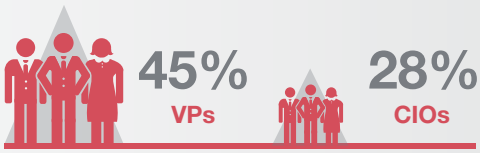
Leadership is lacking

There is a general lack of agreement over who should own information security, and where in the organization the CISO should report. Should the ultimate owner be the CEO, CIO, CFO, CRO, or CISO, and should the CISO report directly to the CEO or Board of Directors? In light of the current threat environment, **many organizations find that nobody really wants to own this responsibility** among the leadership team, **even though ultimately it is a risk to the C-suite as a whole.**

Effective management requires interior lines of communication throughout the organization. The 2015 New York Stock Exchange (NYSE) special report "Managing Cyber Risk: Are Companies Safeguarding Their Assets?"[4] found that **42% of board members admitted to only occasionally discussing cyber/IT security.** As far as prioritization of the hiring of security resources, the Experis research shows disparities between functional leaders and organizations' CIOs: 45% of VPs put information security at the top of their list of concerns compared to 28% for CIOs.

42%

of board members only occasionally discuss cyber/IT security



put information security at the top of their list of concerns

4 — Managing Cyber Risk: Are Companies Safeguarding their Assets – https://www.nyse.com/publicdocs/nyse/listing/NYSE_Governance_Services_ Managing_Cyber_Risk.pdf

Workforce composition is unbalanced

Organizations often struggle to achieve adequate security protection because they do not have a suitable **security workforce composition** or a **security resourcing strategy,** particularly with respect to information security management. There are a number of workforce configurations and strategies that can be implemented by organizations today, including:

in-house staff

staff augmentation with temporary resources

complete outsourcing of major security capabilities to a full service managed security services organization

function specific contracting with third parties

project solutions

The Experis research found that the **majority of employers favor a single resourcing strategy, even though it can often add stress to their workforce effectiveness[1].** The results indicated that 52% of employers surveyed use only permanent employees. This model reduces the organization's ability to incorporate fast-evolving technologies or to react to emerging threats. Fifteen percent of employers surveyed use only contractors. Adopting a resourcing model that primarily utilizes third party service providers for security functions and the delivery of security initiatives can be an effective means for organizations to build a flexible workforce. Though, this approach is not without its challenges. Depending on the skills available, there might still be training required to ensure contractors can effectively support the specific technologies of the organization. Ultimately, these organizations may see a significant erosion of their in-house security staff's knowledge and situational awareness due to their lack of direct contact with the operational environment. This will impact their ability to achieve any long term visions of creating a fully capable internal workforce.

The Experis survey shows that only 33% of organizations favor a more balanced, optimal mix of approaches to security workforce resourcing. **Using a balanced resourcing approach not only helps address shortages more quickly, but can also expose resources that have an affinity to broaden their skills or leadership abilities,** which creates a more robust internal information security talent pipeline in the long run.

52%
only permanent employees

15%
only contractors/freelancers

33%
use a mix

1 — Experis IT Skills Research 2015

Experienced talent is scarce

"The fact is there simply isn't enough mature security expertise to go around, either today or for the foreseeable future," says Michael Gerdes, Director of the Information Security Center of Expertise at Experis. "At the core of the problem is the conundrum that mature skills and security experience cannot be taught by any academic program. It takes time in the right jobs to develop." What many organizations are discovering is it is somewhat easier to find security specialists for basic operational roles, or more advanced resources to cover the policy/vision end of the spectrum, because these areas tend to use skills that can be taught and applied immediately.

The availability of resources becomes much scarcer when looking for senior, experienced resources that can effectively create actionable plans and manage organizational security risks. The required degree of pragmatism and ability to effectively balance the practicalities of business culture, control effectiveness and implementation pitfalls only comes after security resources have some actual real-world experience ('school of hard knocks' alumni).

One complication that impedes the labor pool from getting the required experience is the quandary posed by organizations seeking a much larger candidate pool, only to hire experienced staff. This practice often leaves inexperienced candidates with no option but to take jobs outside security. When failing to create opportunities for novice security practitioners to learn their trade from senior colleagues and to become part of the in-house talent pool, **companies foster an employment environment that further erodes the long term pool of talent.**

"At the core of the problem is the conundrum that mature skills and security experience cannot be taught by any academic program..."

Michael Gerdes, Director of the Information Security Center of Expertise at Experis

A broken education pipeline

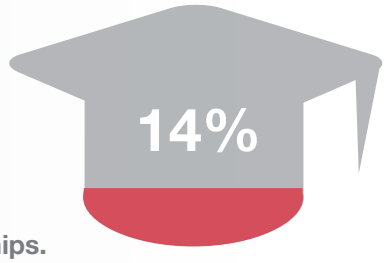
The current education and training systems do not supply an adequate talent pool to address either the current demand for security resources or the growth of expected future demand. Worse still, the educational models, primarily based on industrial-era training and career principles, may no longer be wholly appropriate in meeting the workforce needs and challenges of the digital age.

Traditional degree programs are continually challenged to deliver a curriculum that is consistent with an academic mission, yet still provide quality, timely and relevant content in a rapidly evolving security risk and threat environment. While employers drive the demand by looking for degreed staff for the majority of their positions, **they need to consider that candidates with newly minted degrees typically require years of experience to transform their raw knowledge into practical skills.** In addition, the need for degreed staff in many security roles (e.g., platform operations, configurations, and maintenance) tends to become less justified in roles that are highly technical and critically dependent on discrete skills that need to be learned and expanded each time the platforms evolve.

THE NEED FOR INNOVATION

Rethinking security talent development

Organizations need to rethink the educational requirements associated with their information security positions and **consider alternative ways the workforce can become educated beyond** traditional degrees. This talent development need might be better met through the use of security trade schools or technical colleges where rapid, **highly focused** training of technical skills **ramps up the talent pool in far less time** than the typical degree programs. If expanded appropriately, these security education centers could create additional capacity to train valuable security talent with specific technical skills in far less time - and perhaps help close the talent gap fast enough to meet employer demand.



Google is leading the way with teams where up to 14% are made up of people who have never attended college[5].

Institutions and businesses should partner to develop capable security candidates in less time with the development of **broad-based work-study programs,** or internships facilitated through **academic-industry partnerships.** Curriculums should propose bridges for candidates from other disciplines looking to enter a security career.

Education must start early. In the corporate world, tech companies are known for setting new boundaries in teenage recruiting. **Google is leading the way with teams where up to 14% are made up of people who have never attended to college[5].** Whilst information security is still out-of-bounds for many of these young people, there is an opportunity for both business and institutions to rethink a fast track for promising students.

Certifications pros and cons

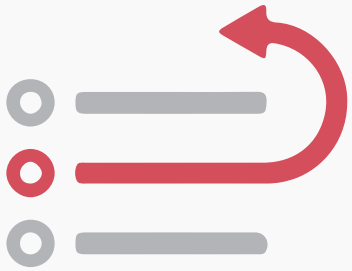
The Experis research also found that IT leaders in many markets expressed a need for certified talent. Certifications can be helpful in differentiating the degree of mastery, but they are not predictive of how well candidates will perform in a specific role. The capabilities and potential value information security specialists will bring to the table better correlates to their real world experiences and job history than their certifications. More than certification, organizations would be better served with programs that provide candidates with opportunities to acquire the practical experience needed to develop both their knowledge and abilities.

5 — Google Has Started Hiring More People Who Didn't Go To College. http://www.businessinsider.com/google-hiring-non-graduates-2013-6

RECOMMENDATIONS

It is clear that the current methods of talent acquisition, retention, workforce composition and education are not always effective and are thus putting some organizations at greater risk. So let us take a look at ways in which your organization can more effectively manage and expand your stable of information security talent, and deal with the widening security talent shortage:

Make information security talent management a priority



Ensure the boardroom is educated, and kept informed, in respect of information security matters, including the level of resources required to mitigate unacceptable risks. The C-suite needs to own security. The CISO needs to be an effective business leader adept at bridging any language barriers brought about by the cultural differences between users and technologists. Resource planning and talent management are a critical part of the ongoing communication. This needs to be established along the reporting lines of the business through the development of a flexible and agile plan that can adapt to emerging and foreseeable security risks, as well as the changing security requirements peculiar to your target markets.

Evaluate your staff

Institute an annual skills inventory review process to identify and track critical security skills currently employed or anticipated by your organization. Similarly, review the coverage level provided by your existing resources. This process will provide valuable information that can aid in career development, resource retention and staff acquisition planning.

Growth from within

Critical security skills are getting more expensive to acquire and often need a lot more care and feeding to retain. Developing your capability from within is often overlooked. Adding this to your growth plan often makes more sense. It eliminates the acquisition cost, and builds on a resource that is known to be a cultural fit. Identify staff with some exposure to security matters, no matter how indirect, and consider them for cross-training. Develop a program that provides **hands-on opportunities in real-world situations** to get the best results in the shortest period of time.

It is a seller's market, so ensure you provide a stimulating environment and total compensation that will counter the attraction of incentives offered by other organizations looking to boost their security talent.

Carefully evaluate new talent before hiring

The increased need for security talent has created an environment in which candidates searching for a job try to leverage common security buzzwords in their resumes to attract company recruiters. Often these 'pretenders' match their resumes to a company job description and are able to convince recruiters they meet the company requirements. This makes it important to incorporate screening by experienced security staff to provide the next level of **examination that goes beyond the buzzwords** and probes more deeply into the functional areas and skills desired.

Manage your talent supply chain

Think outside the box when evaluating the best way to acquire additional resources. Many security needs are one-time or periodic rather than ongoing and might be best served by one or more of the following:

- Contract expertise or thought leadership
- Project-based consulting
- Deliverables-based temporary staffing initiatives

Talent agents should demonstrate deep information security expertise and an innovative approach to recruitment. They should have access to information security talent pools and have established relationships with their candidates, thus knowing their skills and experience beyond buzzwords written on a resume. Given the evolving nature of the skills required, regular review of agents and their capabilities should be included in the supply chain plan.

Consider implementing technical screening as a mandatory element of external staffing groups in order to minimize your staff's valuable time in reviewing the initial candidates.

CONCLUSION

Organizations are not going to see an end to the shortage of experienced information security talent in the near term, **so they need to get imaginative and innovative in finding ways to leverage the talent they can acquire** (temporarily or permanently) to their best advantage. The greatest success in this endeavor will be achieved through management processes that incorporate monitoring and feedback to facilitate adjustments to the roles, responsibilities and sourcing of talent.

We need to recognize that information security is a rapidly evolving field, and **we must brace ourselves for more than one battle.** Any solutions (individual or combined) we choose to pursue to close the talent shortage **will take time to both develop and yield any significant results.**

Recognizing the true extent of the problem is the first step toward solving it. Executive awareness of the problem, innovative and flexible approaches to education and training, and increased collaboration across organizations are the keys to successful security workforce management. These improvements also lie at the heart of addressing information security challenges in the longer term.

ABOUT EXPERIS:

Experis® is the global leader in professional resourcing and project-based solutions. Experis accelerates organizations' growth by intensely attracting, assessing and placing specialized expertise in IT, Finance and Engineering to precisely deliver in-demand talent for mission-critical positions and projects, enhancing the competitiveness of the organizations and people we serve. Experis is part of the ManpowerGroup® family of companies, which also includes Manpower®, ManpowerGroup® Solutions and Right Management®.
To learn more, visit www.experis.com.