ARMOR™

BETWEEN YOU AND THE THREAT

Cybersecurity — Whose responsibility is it?

IDENTIFYING ACCOUNTABILITY GAPS FOR TRUE COMPREHENSIVE CYBERSECURITY

Everyone sells security tools

A tool seems like the obvious solution to a security problem; tools can be easily bought and easily bolted on to existing security systems to defend against emerging threats. Yet the numbers of breaches that are splattered across the headlines every week provide evidence that tools are not the answer.

Enterprise executives recognize that their expenditures on tools are not necessarily in proportion to the security of their assets. Despite the fact that the market is saturated with security tools, the vendors that sell them are not willing to bear the risk of guaranteeing outcomes.

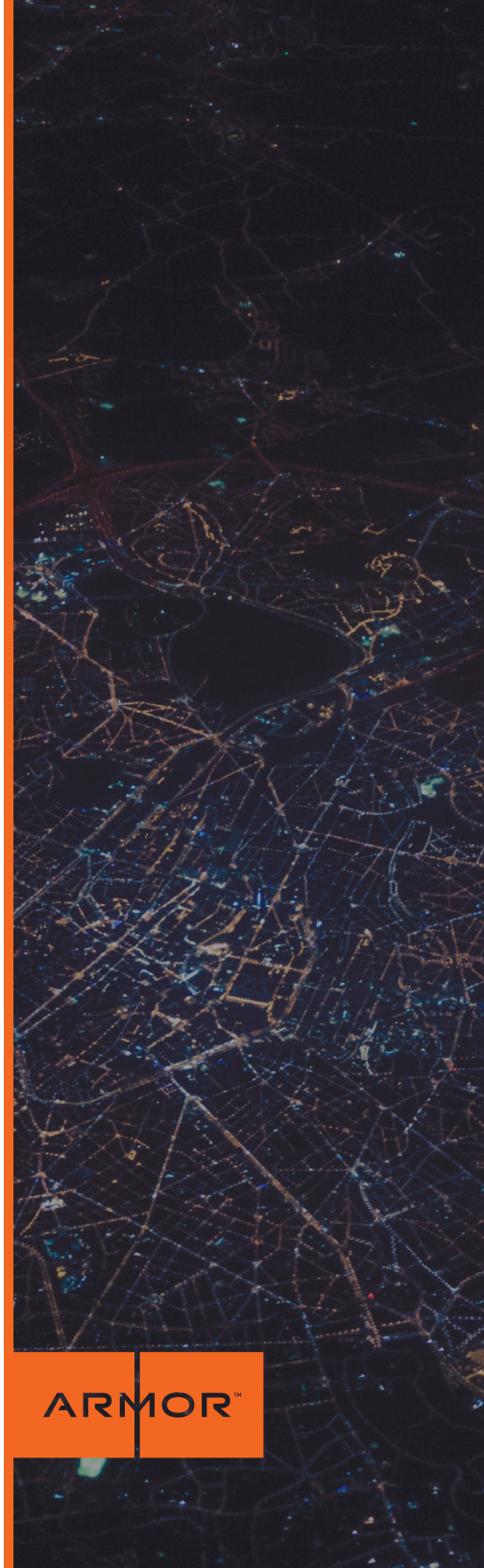
After an enterprise makes its purchase, the vendor's participation ends and the buyer is left on its own to implement and manage the tool. No other industry places such a heavy burden on its customers.

Is the problem faulty tools? It is not. The tools can only work as well as the security professionals who use them every day to monitor, identify and resolve network anomalies.

But a shortage of cybersecurity talent makes it hard to find qualified security experts to run daily security operations. And staffing is not the only people problem that impacts network security; the way that most corporations structure their leadership does not support the culture of security that is fundamental to a strong proactive posture.

No wonder executives are worried.

> "Tools can only work as well as the security professionals who use them every day to monitor, identify and resolve network anomalies."



Who is responsible for security?

Who is responsible for security in the enterprise? Every company takes a different approach, but in many cases, accountability and authority do not reside in the same role. When this happens, it's hard to tell who is responsible for securing digital assets.

Security ownership is a game of Hot Potato

Executive leaders are business experts. Their job is not to understand how security operations work, and so they may not know the best way to delegate authority for security activities.

The obvious role to own responsibility for security is that of a technology executive, and that's who is often in charge of securing the enterprise — at least nominally.

However, not all technology executives understand security operations, and those who do may not have the influence needed to sponsor strong initiatives or command necessary resources.

IT managers are often thrust into the role of security manager, but IT and security are different areas of expertise. An IT manager may not be able to get the training necessary to fully understand and manage security operations, and/or may not have the clout to make the organization-wide changes that are the heart of true security.

Some enterprises rely on vendors to protect their enterprises. However, security is not a technical problem. Security is a strategy that has to be built into every aspect of the business. Real security cannot simply be purchased; it has to be developed, even when partnering with a trusted vendor.

> "Security is not a technical problem. Security is a strategy that has to be built into every aspect of the business."

CEOs & CFOs

Chief executive officers and chief financial officers bear ultimate responsibility, but they must base highly technical decisions on advice from their security execs (if they have any), or from their CIO or IT executives.

CEOs and CFOs rightly and properly have a mindset focused on their core business. Security is often considered an operational cost rather than a strategic investment.

When this is the case, CEOs and CFOs often exclude security and IT professionals from the decision-making stage of business-critical software purchases; a recent survey showed that when choosing a cloud-based service,[1] only 34 percent of business leaders involved IT in the decision-making process, and only 29 percent involved IT while deploying the service. As a result, it is unlikely that proper security audits were conducted prior to purchase.

CIOs, CSOs & CISOs

CIOs

Chief information officers are responsible for all technology capabilities, but they may not be security experts. The people who fill this role tend to be risk-averse, a disposition that is at odds with the need to defend against a dynamic threat landscape; sometimes a choice must be made between a new approach and no approach at all.

A CIO's focus on technology can actually be a pitfall. Strong security has to be infused through an organization, from the security department to the business processes to the employee activities. Therefore, securing the enterprise requires more than a technical scope.[2]

CSOs

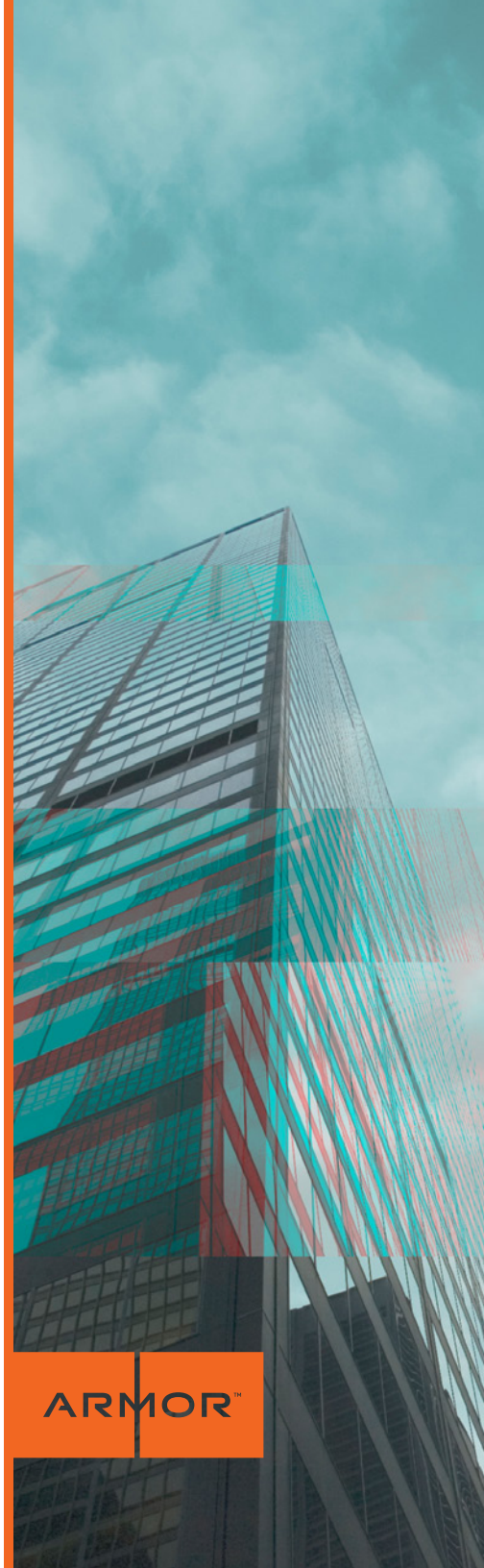
Chief security officers are responsible for all security in an organization, from customer data to door locks. They have the specialized knowledge needed to protect their organizations, but because CSOs do not usually report directly to the CEO, they may encounter difficulties in gaining the funding, purchasing authority and cross-enterprise support needed to implement an appropriate level of security

A common perception in the C-Suite is that the CSO should be responsible for failures in security, but the C-Suite does not always give the CSO the authority to take action against such failures. CSOs are sometimes pigeon-holed as "techies" and, however incorrectly, are not perceived as having a deep knowledge of the business as a whole.[3] This limits the ability of the CSO to be effective.

CISOs

Chief information security officers are responsible for aligning all information-related security initiatives with security programs and business objectives.

However, the role of CISO is a new one, and it is constantly evolving. CISOs often report to and work closely with the CIO, which can hamper the CISO's ability to remain independent during audits and IT decisions. CISOs are also at risk of having their decisions overridden by the supervising CIO.[4]



1 Quick, 2013
2 Burgess, 2014
3 McKendrick, 2013
4 Sarkar, 2013

IT director

To non-technical business leaders, security may be perceived as an IT responsibility. However, security encompasses more than information systems; it's an enterprise-wide mindset, beyond the scope of information systems alone.

IT managers are not security specialists and don't have the specialized skills needed to manage security across the enterprise; at the same time, IT managers may be uncomfortable sharing control of IT systems with the security department.

Also, IT managers naturally focus on building systems, and sometimes only add the security later; that can result in a leaky system.[5]

Because of their position on the org chart, IT managers are unlikely to have the authority to get the funding or wield the influence to work across lines of business to adequately secure the enterprise.

Line-of-business managers

According to a survey by Ponemon, 25 percent of organizations surveyed identified line-of-business (LOB) managers as responsible for security.[6] This is a clear disconnect; while the individuals in these roles contribute to the overall security (or lack of security) of their organizations, they are not equipped with the technical knowledge or the influence to drive security.

LOB managers are typically eager to implement business software to improve their processes. They need to be conditioned to bring security on board early in the software selection process, in the same way that they work with the IT department.

These individuals also play an important role in communicating the need for security and enforcing security policies within their own departments. LOB managers need to be kept aware of current enterprise security initiatives so they can align their departments' activities with them.

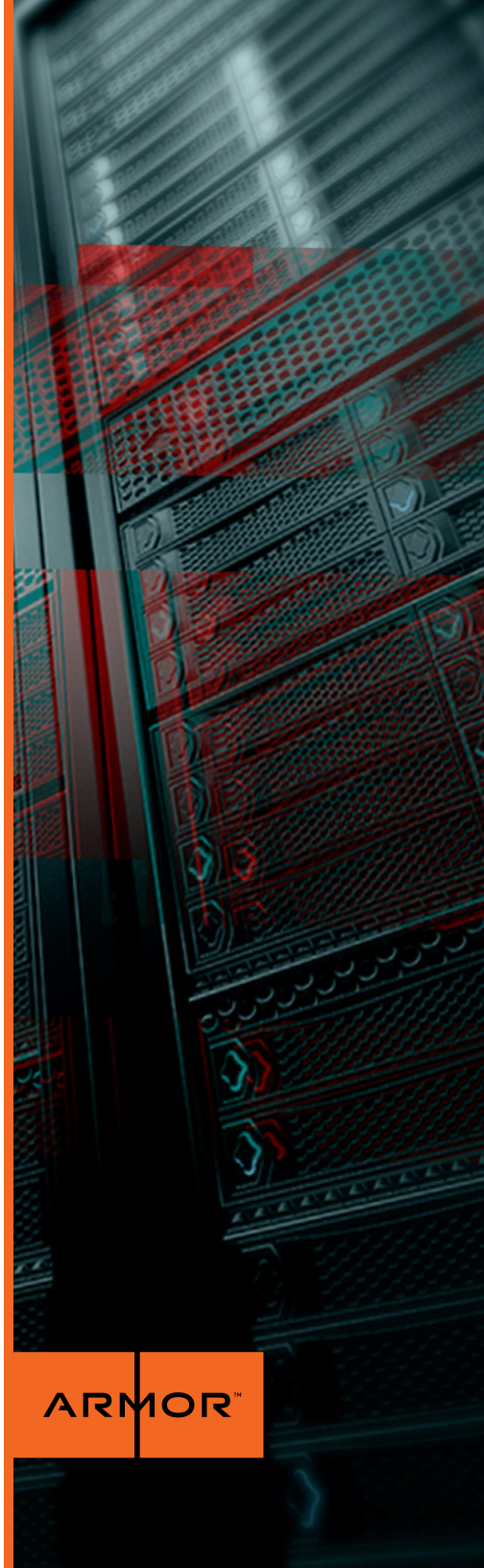
Security vendors

In a survey by Ponemon commissioned by Armor, one-third of IT and security professionals named their cloud provider as the entity most responsible for protecting sensitive data in the cloud.[7] Respondents clarified that they trusted their cloud providers to protect data assets more effectively than their own enterprises, with 57 percent agreeing on this point.

However, no vendor can ensure enterprise-wide security because no vendor has authority inside a customer's organization. That said, vendors can do more to ensure customer success.

Security vendors need to be clear about the assignment of security responsibilities. They can help develop processes and identify areas in which they can offer additional support, beyond simply implementing tools.

5 McKendrick, 2013
6 Ponemon Institute, 2015
7 McKendrick, 2013

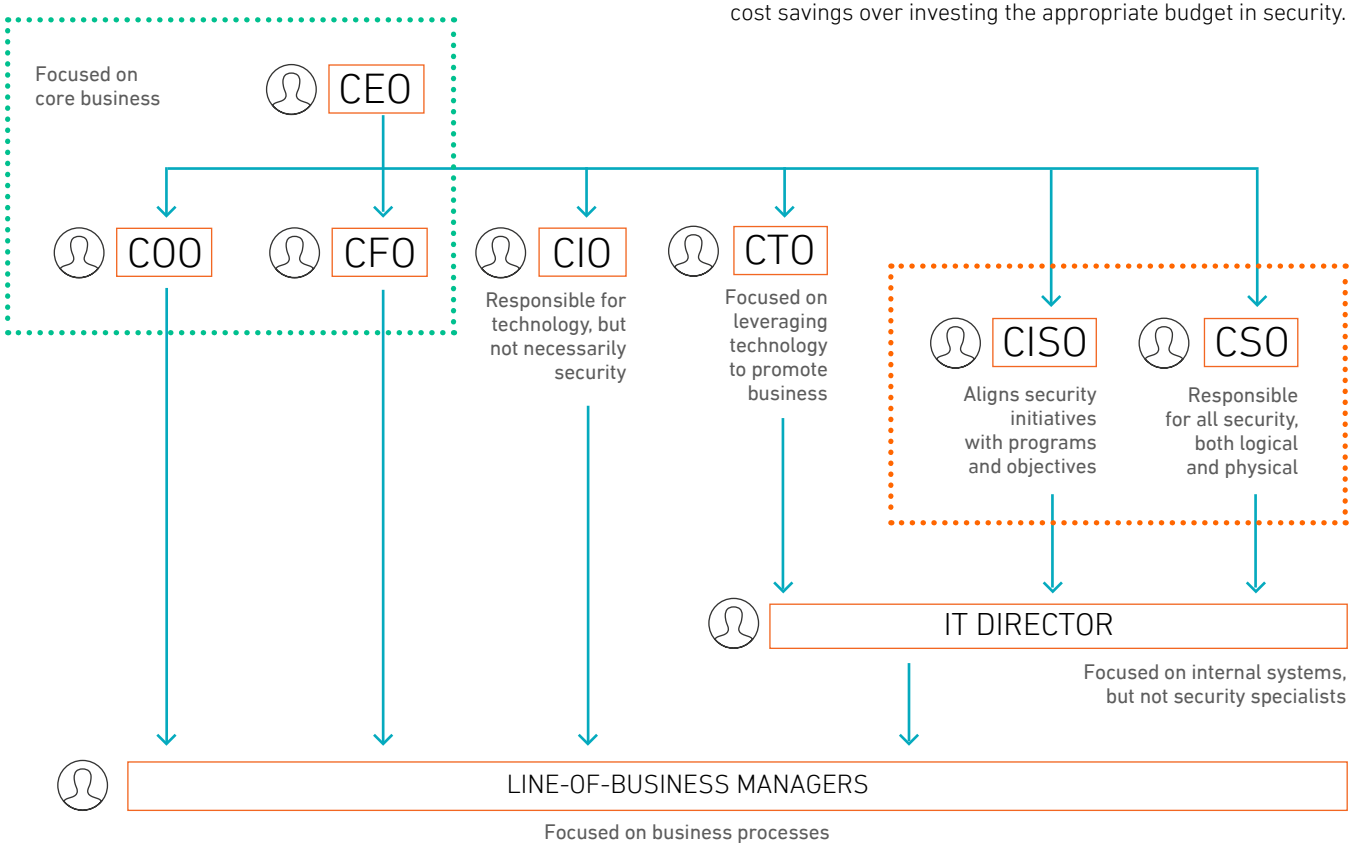


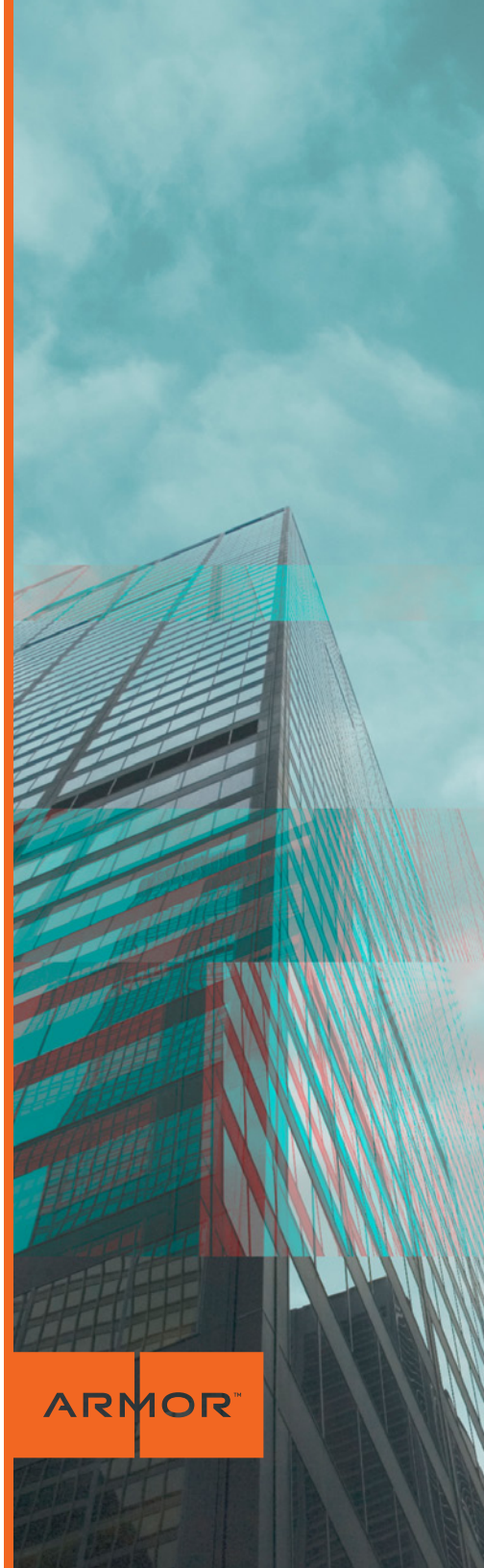
Security breakdowns

A look at an org chart can raise questions about where a breakdown in responsibility can occur. Currently, it is uncommon for enterprises to have a CSO who is at a level equal to that of a COO or CTO.

Is this because the leadership does not see security as a strategic concern, or does leadership lack the information needed to make that connection?

If security is not strategic, then it's a cost center. And if security is a cost center, security managers are under pressure to prioritize cost savings over investing the appropriate budget in security.





The empty chair problem

Over 200,000 security jobs are unfilled at any given moment.[8]

The common assumption is that this is a simple supply and demand problem; train more cybersecurity professionals and the problem will go away. Yet training is available, and there are plenty of computer-minded students who are eager to enter a career that will guarantee them their pick of jobs.

But no matter how many students graduate from academic programs in cybersecurity, the shortage is going to continue for the next few years. The exact mix of certifications and training needed in a specific security operations center (SOC) is not likely to be possessed by a recent graduate.

Classroom training does not prepare an individual to perform well on the job; rather, true security expertise is learned in the SOC, working on real threats on live systems under the tutelage of experienced analysts. For every 20 open security positions at a given company, there is only one qualified candidate[9] — with the key word being *qualified*.

And the problem goes deeper than a lack of warm bodies; rather, it is tightly coupled with the nature of security operations in an enterprise environment.

The typical security analyst is anything but typical. A broad range of roles and skills are needed in a SOC, and it can be hard to understand how a candidate will fit into the mosaic of the SOC team until he or she is on the job and working.

Also, as new threats emerge, new skills are needed to counter them — so this morning's new hire may not have the certifications and experience to proactively defend against this afternoon's malicious activities.

Training comes after experience

Cybersecurity training programs teach policy but do not focus strongly enough on technical expertise, so graduates have been taught concepts but cannot fix vulnerabilities.

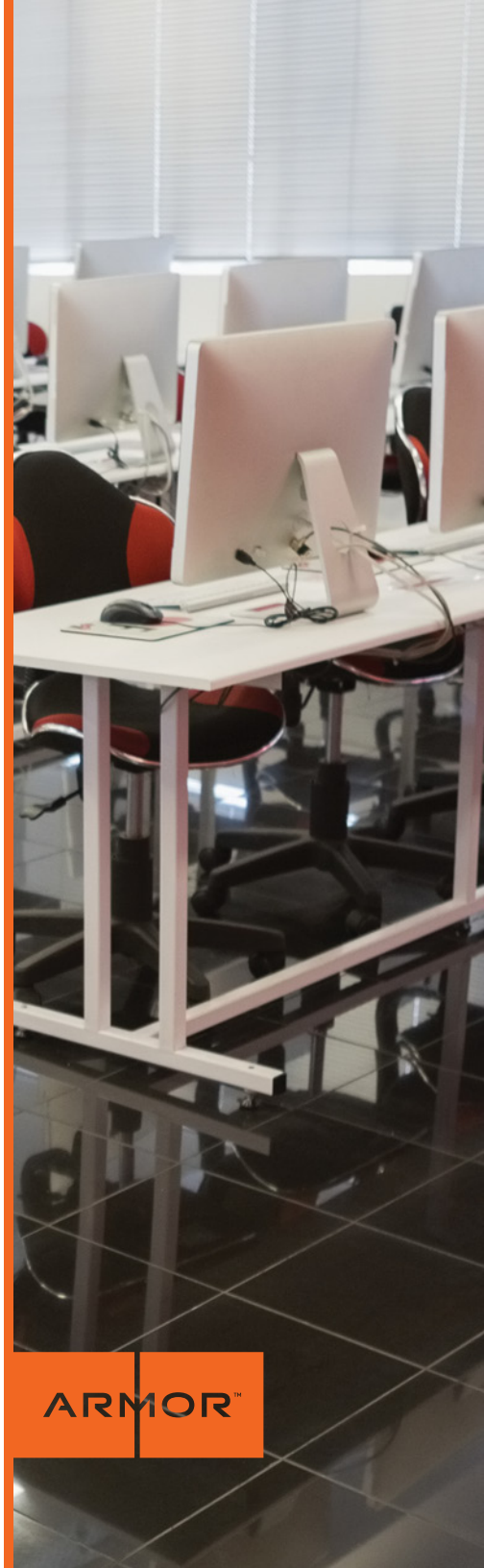
The most desirable experience a security professional can possess is a high level of real-world aptitude and understanding in a demanding environment.

A background that includes work with government agencies like the U.S. Department of Defense, National Security Agency, Central Intelligence Agency or military intelligence is particularly in demand. Professionals with this experience have learned how to protect the nation's most sensitive data from the world's most vicious threat actors.

They also bring another benefit to the enterprise; security professionals form what are called trust circles (or, more colorfully, *fight clubs*). Trust circles are professional networks focused on sharing the latest tactics, techniques and procedures, as well as alerting members to threats looming on the horizon.

High-level trust circles are by invitation only, and potential new members are vetted before being asked to join. Membership in an advanced trust circle is of tremendous value to an individual analyst and, in turn, of tremendous value to that analyst's employer.

An analyst with a strong network in the cybersecurity community is always aware of impending dangers and equipped to proactively deter them.



8 Carapezza, 2015
9 Lemos, n.d.

Because security professionals tend to learn their most useful skills on the job, entry-level employees may not be a good investment. Even entry-level certifications are based on the presumption of real-world experience; for instance, the CompTIA Security+ certification recommends candidates accrue two years of on-the-job (OTJ) experience and complete a network administration certification before taking the assessment.

Another desirable entry-level certification, GIAC Security Essentials, offers training that starts at the 300 level — the equivalent of a third-year college course. The student must independently pick up the skills needed to certify at that level before preparing for the assessment.

Most enterprises have immediate needs and do not want to invest two years in an uncertified employee before that employee can become qualified to do the job he's being paid to do.

But the alternative to an unprepared candidate might be no candidate, so companies that find individuals with these certifications should snap them up, even with the knowledge that the candidate will still need OTJ training, and also with the knowledge that a two-year investment does not guarantee the candidate will stay with the company long enough to 'pay back' the resources that were invested in his development.

Beyond the basic certifications, the areas of expertise become highly fragmented. Every time a company needs to add a new skill to its team, it's either going to have to remove a costly employee from daily work to prepare for a new certification, or it's going to have to hire the skill into the team.

Enterprises that are running specific platforms should look for vendor-specific certifications, such as the Cisco CCNA, EMC RSA or Symantec Certified Specialist.

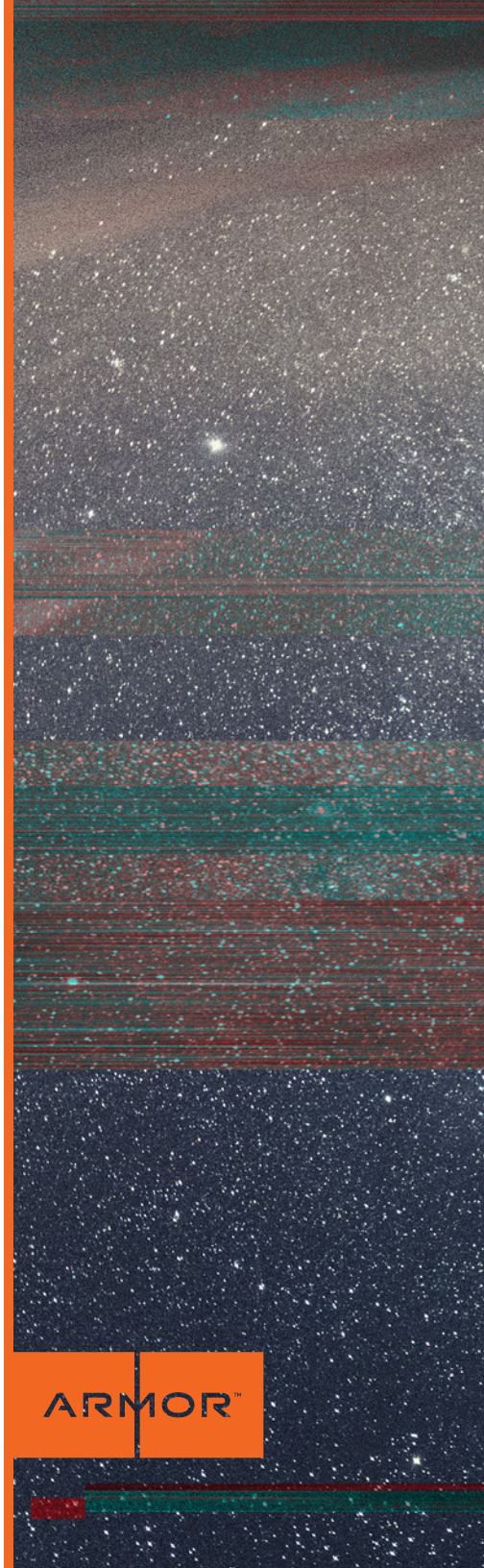
Companies that need to add more advanced skills to their team will look for candidates with specific certifications.

- Certified Ethical Hacker (CEH)
- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- Offensive Security Certified Professional (OSCP)

All of these certifications take time to complete. For instance, depending on the amount of experience a candidate has, preparing for the CompTIA+ certification can take anywhere from two to 12 weeks.

And all of these certifications must be refreshed periodically. Each certifying body has a different set of requirements, but the general parameters are that certifications must be retaken or proof of professional development demonstrated every 1-3 years.

Imagine a SOC with a dozen high-salaried security analysts; how many will be offline each year? How many man-hours are going to be devoted to maintaining certifications?



Churn is a security risk

Investing in these necessary certifications is a gamble. High demand drives high turnover, and the best security professionals have their pick of employers.

Enterprises that don't provide an attractive environment for their security professionals will have a hard time hanging onto them. Churn in the security department is a different beast than churn in any other department — it poses a threat to the enterprise.

The cost of continual recruitment and the burden of onboarding are the obvious drawbacks to managing a high-churn staff, but more important, and more dangerous, are the loss of historical knowledge, the fragmentation of the team as new members are constantly introduced, and the drain on morale that creates a vicious circle of churn driving more churn.

Go to the experts

Enterprises lacking the resources to hire and retain their own security teams do have other options — cloud and managed services. Managed secure cloud providers and elite cybersecurity vendors are able to attract and retain the most highly-skilled professionals available, including those with deep experience in sensitive environments such as government defense agencies.

Talented and well-connected professionals can work anywhere they choose, and they tend to choose environments in which their skills are the core business; these are the places that can offer them the best career paths and compensation packages. By utilizing a managed secure cloud provider, an enterprise gains access to the top talent in the industry without the burden of attracting and retaining costly personnel.

Processes and techniques are the basis for proactive stances

Threat actors are not focused on penetrating a particular network device. The device is merely the path to their true target, which are the processes a business uses to handle:

- Personally identifiable information (PII)
- Product development
- Customer data
- Financial transactions
- And other sensitive data

Think of technology as a hammer. A hammer doesn't build a house; a skilled worker uses a hammer to build a house. Likewise, security technology alone doesn't protect the enterprise; it is just a tool used by experts, and a strategy can't be based on a tool. It needs to be paired with the right talent and proven processes in order to be effective.

A good strategy is holistic, infused throughout the enterprise. The problem with buying tools is that vendors who sell tools do not sell success. They are moving units, while a secure enterprise needs its vendors to partner with it, helping to safeguard processes, define roles and responsibilities, and communicate security messages to the workforce as a whole.

The security team needs visibility into business processes in order to strategize and implement appropriate security policies. If R&D is developing on a test server, that server needs to be known to security. If marketing is subscribing to a new SaaS product, security needs to conduct an application security audit.

Policies should be developed in meetings between security and LOB managers to review how work is accomplished. This involves a series of steps, such as:

- Inventory systems
- Document workflow
- Develop test cases
- Identify vulnerabilities

With this type of information, a solid security policy can be developed. The policy should preserve security without smothering productivity; overly strict policies tend to be ignored, so they're a vulnerability in themselves.

When an instance of unauthorized access has been identified, a process must be in place that defines next steps.

Threat intelligence must be collected. The process should state how to capture data, which data is preserved, and how the data will be placed in context in order to be transformed into useful intelligence.

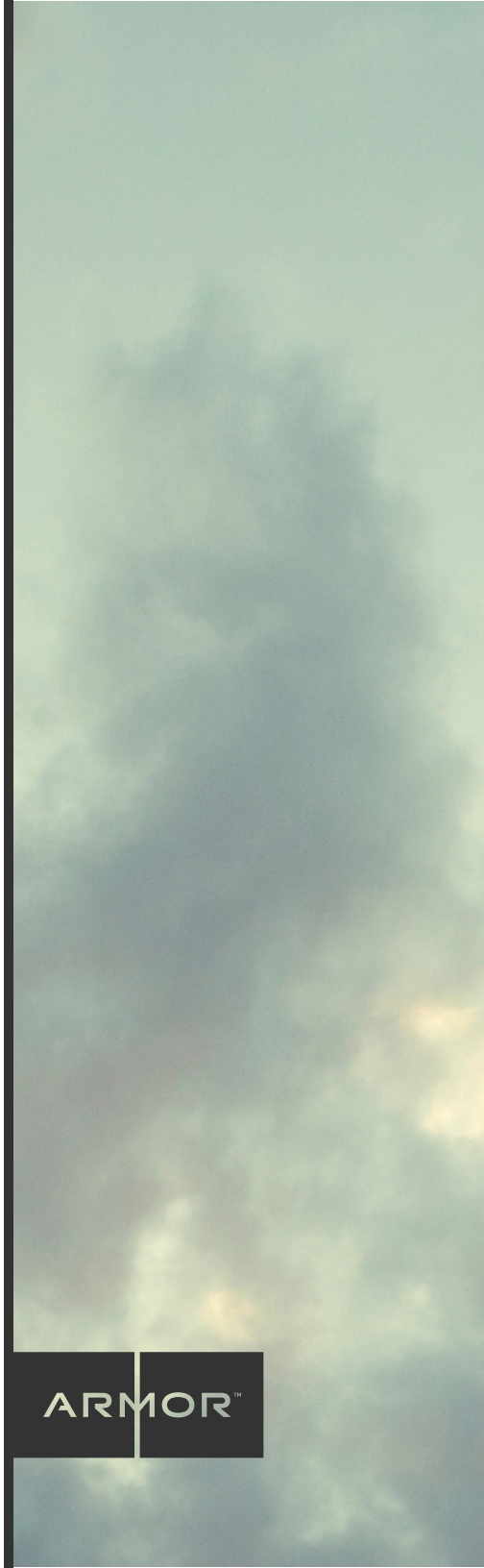
The contextual intelligence will drive the next step: the threat remediation process. When techniques, tactics and procedures are identified, remediation can begin and future attacks can be prevented.

Processes should include what-if scenarios.

- What if data is ransomed?
- What if a DDOS attack is launched?
- What if a disgruntled insider sabotages critical systems?

Clearly, no tool alone — and no bank of tools — can protect against all threats. People commit bad acts, and people are the final defense against those bad actors.

Security is a team effort. Get the support necessary to lock down entry points and respond if an intrusion occurs. A capable vendor will be able to provide guidance on how to dovetail business processes, accountability structures and technical solutions to create an effective security posture.[10] To foster a culture of security, think beyond tools and look for a vendor that is willing to carry some of the burden.



10 Jordan, 2014

The healthy org

In an organization with healthy security, the enterprise considers security to be a strategic part of the business.

The enterprise has a clear line of accountability for security issues,[11] ending with the CSO. The characteristics of an organization using its CSO fully are that the CSO:

- Reports directly to the CEO
- Is an influential executive
- Has the authority to ensure security operations are adequately funded
- Has ownership of the security framework, but the entire enterprise has accountability for managing security across lines of business and within business processes

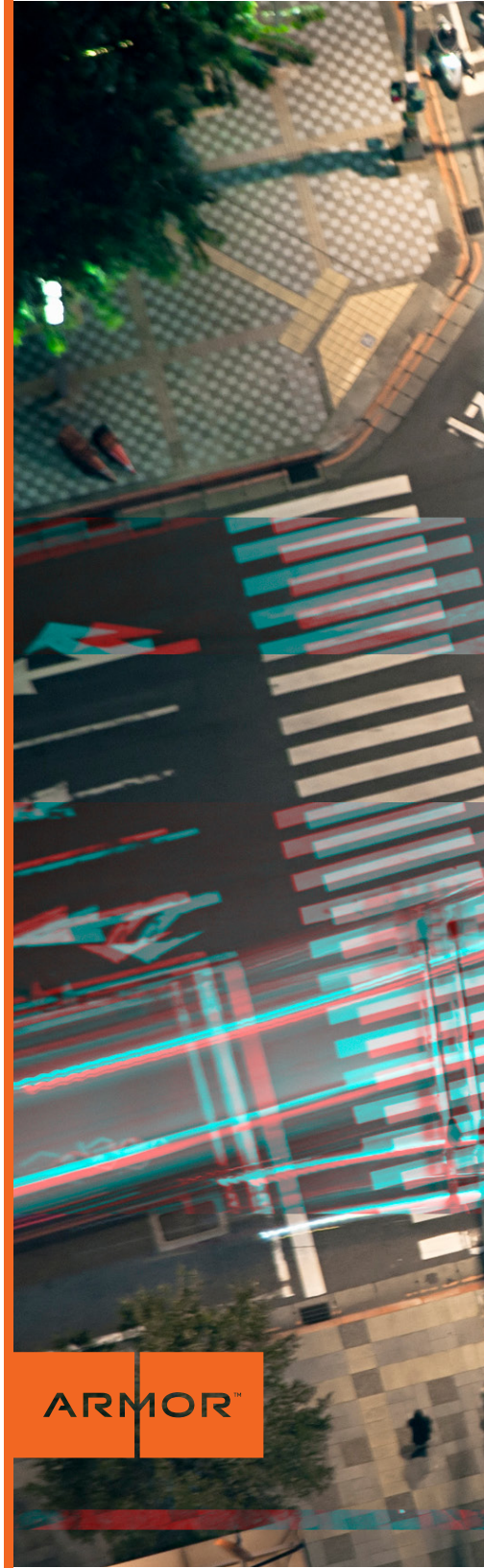
In companies that do not yet have a CSO, the CEO should take the lead in fostering security throughout the enterprise. The CEO is a more appropriate point person than the CIO because security is not a technology risk — it's a business risk.

All executive officers should support security initiatives throughout the enterprise. LOB managers should be willing to share their work processes and application inventory with the security department.

The entire enterprise should be security-conscious. Protecting sensitive data is everyone's responsibility, from the CEO to the temp at the front desk: a 'culture of security' must be overtly fostered in all corporate activities and communications.

In support of a culture of security, cybersecurity training should be part of the onboarding process for all employees, and continuing cybersecurity awareness part of the corporate culture.

"The entire enterprise should be security-conscious. Protecting sensitive data is everyone's responsibility, from the CEO to the temp at the front desk."



11 Ibid.

The enterprise should have a centrally managed 24/7 security department. Not all companies can make a strong business case for an investment of this size; security operations are both costly and complicated to staff and run.

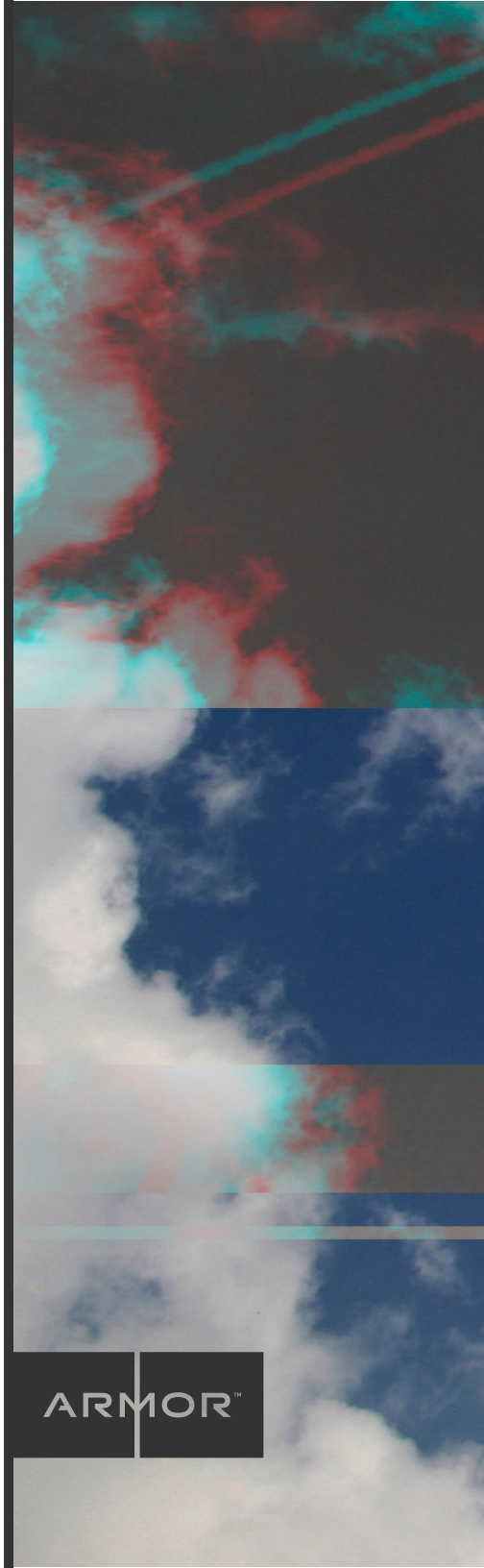
For businesses unwilling or unable to dive this deeply into security, the best strategy is to outsource security operations to a security provider who is an expert in delivering more than tools to the enterprise; the provider should be a partner who continually works both for and within the enterprise to strengthen its security posture.

In a healthy organization, specific security roles and responsibilities are defined. The individuals in these roles have the authority necessary to ensure the security of the enterprise. If on-premises, the security department must be staffed with the appropriate number of skilled and certified specialists.

A formal plan should exist to ensure the security staff receives ongoing training and certification without affecting daily operations. Ideally, there should also be a plan to scale the number and skills-focus of the security staff to respond to a critical threat.

Vendors should be selected based more on how they can support security processes than on the tools they offer. Vendors should be willing and able to engage in an ongoing relationship with the enterprise, taking on the role of security partner.

"For businesses unwilling or unable to dive this deeply into security, the best strategy is to outsource security operations to a security provider who is an expert in delivering more than tools to the enterprise."



Blend talent and technique

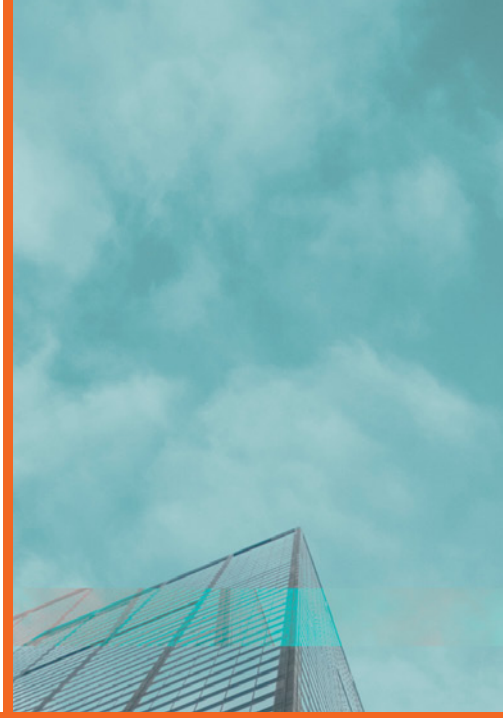
Although investment in full-time cybersecurity professionals has doubled, it's still too little and too small a percentage of overall IT. However, no amount of money can fix a broken process or place responsibility where it can do the most good — those decisions belong to the enterprise leaders.

True cybersecurity requires a top-down commitment. The structure of the security department needs to include outreach into all parts of the organization to establish practical and effective security policies.

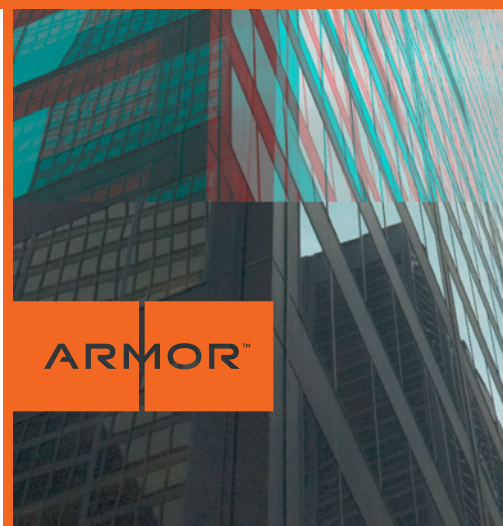
But enterprises should not feel compelled to figure everything out on their own. Most companies are not security experts, but they are experts on their own businesses; leverage that knowledge when working with a vendor, and partner together to align business processes with security operations.

The right vendor will provide more than tools; it will provide expert help on processes and techniques, and will share risk and deliver outcomes.

A culture of security does not appear out of thin air, and there is no template that applies to every business. Each enterprise has to make an organization-wide effort to identify the roles and responsibilities — and the policies and processes — that make the most sense for its business model and strategy, as well as its likely threats.



The right vendor will provide more than tools; it will provide expert help on processes and techniques, and will share risk and deliver outcomes.



Works Cited

- **Burgess, C., 2014. What Is the Role of Today's CISOs? 7 Questions Business Leaders Are Asking. [Online]**
  Available at: https://securityintelligence.com/what-is-the-role-of-todays-cisos-7-questions-business-leaders-are-asking/#.VcsF_flViko
  [Accessed 10 August 2015].

- **Carapezza, K., 2015. With more than 200,000 unfilled jobs, colleges push cybersecurity. [Online]**
  Available at: a. http://www.pbs.org/newshour/updates/college-struggle-keep-pace-need-cyber-soliders/
  [Accessed 11 August 2015].

- **Jordan, S., 2014. A Roadmap for CIOs & CSOs After the Year of the Mega Breach. [Online]**
  Available at: http://www.darkreading.com/attacks-breaches/a-roadmap-for-cios-and-csos-after-the-year-of-the-mega-breach/a/d-id/1269679
  [Accessed 10 August 2015].

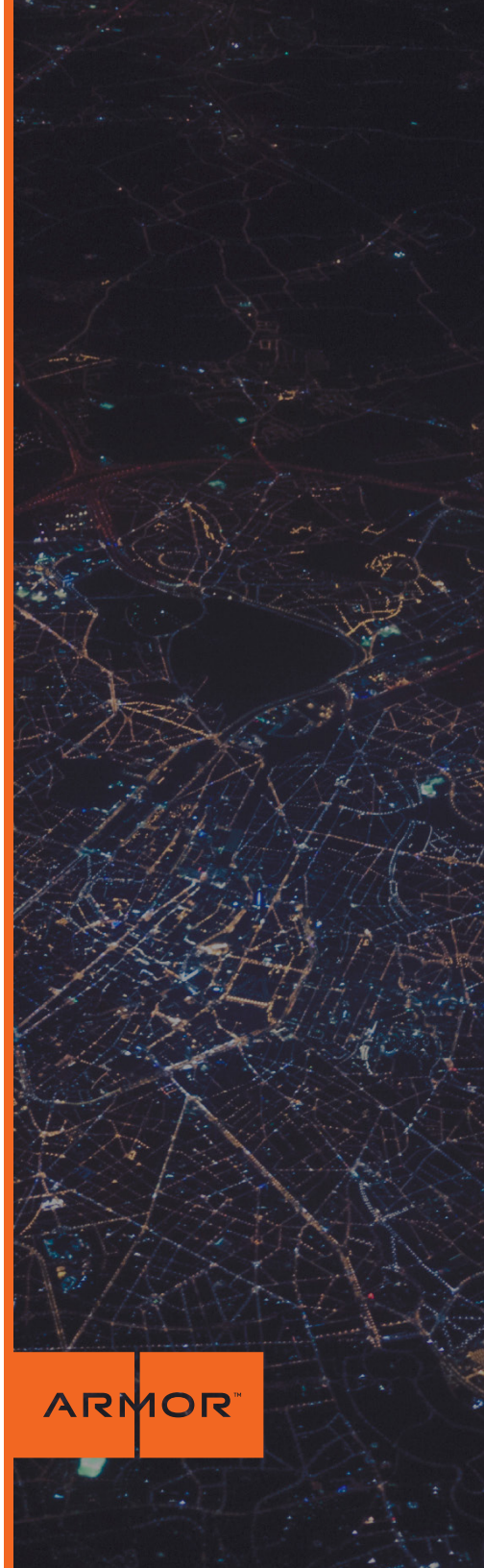
- **Lemos, R., n.d. Bridging the IT security skills gap. [Online]**
  Available at: http://searchsecurity.techtarget.com/feature/Bridging-the-IT-security-skills-gap
  [Accessed 10 August 2015].

- **McKendrick, J., 2013. Enterprises' Security Practices Not Keeping Pace With Cloud Growth, Studies Find. [Online]**
  Available at: http://www.forbes.com/sites/joemckendrick/2013/06/29/enterprises-security-practices-not-keeping-pace-with-cloud-growth-studies-find/
  [Accessed 10 August 2015].

- **Ponemon Institute, 2015. Cloud Security: Getting It Right, s.l.: Ponemon Institute.**

- **Quick, R., 2013. Enterprise Cloud security: What are the risks and what you can do about them?. [Online]**
  Available at: http://thenextweb.com/insider/2013/09/20/enterprise-cloud-security-what-are-the-risks-and-what-you-can-do-about-them/
  [Accessed 10 August 2015].

- **Sarkar, D., 2013. 5 Common Challenges Faced By Indian CISOs. [Online]**
  Available at: http://www.cioandleader.com/articles/17995/5-common-challenges-faced-by-indian-cisos
  [Accessed 10 August 2015].



US 2360 Campbell Creek Boulevard, Suite 525, Richardson, Texas 75082 | Phone: +1 877 262 3473
UK 5 New Street Square, London, EC4A 3BF | Phone: +44 800 500 3167