

# The State of Cybersecurity and Digital Trust 2016

Identifying Cybersecurity Gaps  
to Rethink State of the Art

High performance. Delivered.



# Table of Contents

Executive Summary	3
The State of Cyber Threats	7
The State of Cyber Response	11
The Talent Gap	12
The Technology Gap	13
The Organizational Parity Gap	14
The Budget and Funding Gap	16
The Management and Operations Gap	17
Final Thoughts and Recommendations	19
Appendix A: Focus and Methodology	21
Appendix B: About the Authors	23



# Executive Summary

**While the advent of digital technology has fueled new business models and opportunity, it has also brought an element of risk as valued assets become less tangible, more distributed, and more vulnerable to cyber threats.**

Today, many different types of cyber attackers threaten organizations, from individuals working alone ("lone wolves") to highly organized, well-sponsored teams-for-hire capable of breaching the most sophisticated cybersecurity systems target personal, corporate or state secrets.

Cybersecurity today must include a rethinking of the nature of security, and a shift from an approach that stresses protecting vulnerable assets to one based upon strengthening assets, making them more resilient and part of a holistic cybersecurity process that delivers greater value to the enterprise.

**Cybersecurity needs to be part of a larger value framework that includes both risk management and the development of digital trust.**

Digital trust is not a technology, nor a process—it's an outcome exemplified by secure, transparent relationships and engagement between the enterprise and its employees, partners, and customers. Attainment of digital trust is driven by how information and data assets are both secured and used, and it helps keep a digital brand memorable and successful.

But how can a company achieve digital trust in an environment where state-of-the-art technology and tactics are often at a disadvantage against adversaries engaged in asymmetrical cyber tactics? Organizations should focus not on technology state-of-the-art, but instead on state-of-the-art cybersecurity as an organizational mindset—one that continually evolves and adapts to counter changing threats. Attainment of digital trust requires a leadership-driven cybersecurity culture throughout the enterprise. And it requires a holistic security approach that results in shared "digital trust" and greater value for all stakeholders.

Research shows a number of gaps that both cybersecurity professionals and business executives must close to build a successful digital enterprise in the trust-based economy. These gaps consist of deficiencies in five key areas: talent, technology (detection and response), organizational parity, budgets and funding, and management.

But cybersecurity is still a young profession—the current role of the chief information security officer (CISO) is barely a decade old—and the idea of "digital trust" as a foundation of business success is still an emerging concept in the digital economy.



Digital trust is more important than ever and cybersecurity is not only expected by consumers, it's demanded in today's trust-based digital economy.



State-of-the-art in cybersecurity is an approach, a mindset—not an implementation or technological end-state. It evolves and adapts as the value of assets shift and the type or level of threat changes.

The results of this survey are sobering: cybersecurity leaders do not believe the threats are going away—in fact they expect them to increase and continue to impact, or act as an inhibitor to, achieving enterprise-wide digital trust. While organizations are making investments in basic technology defenses such as firewalls, and new technology such as behavioral analytics tools, they simply do not have enough skilled professionals to leverage security technology properly. There are clearly gaps between where most enterprises are and where they feel they need to be. And yet, 36 percent of respondents believe that executive management views cybersecurity expenditures as an unnecessary cost.

Many cybersecurity teams are attempting to close the gaps, experimenting with advanced cognitive and other artificial intelligence (AI) technologies, while still struggling to find the security talent to execute on the basics effectively. Establishing digital trust, which is seen as crucial to competitive success, clearly requires a new mode of working, not simply incremental improvement.

## Key findings of the study include the following:

### On threats...

- Data theft of corporate information by outsiders and the theft or corruption of personal information by corporate insiders dominate the discussion, with 35 percent of respondents indicating they were strongly or critically concerned about these two threats over the past 12 months. But moving forward, overall data loss or destruction becomes a top rated concern, with 41 percent of respondents indicating strong or critical concern over the coming 12 to 18 months.
- The threat sources of most concern to enterprise security professionals are private, well-organized teams, organized criminals, and state-sponsored professionals, with agendas of corporate espionage and the targeting of critical infrastructure as their main concerns.
- Brand reputation and customer support are rated the most vulnerable business goals, with 43 percent and 37 percent (respectively) of respondents listing data security as critically important to supporting those efforts.
- Cloud computing, a culture of cybersecurity awareness, and cloud storage are rated as the most important enterprise initiatives, while mobile tops the list of initiatives at risk, with 47 percent of respondents listing a data breach or loss of service involving mobile as having the highest risk to the enterprise brand.
- Sixty-nine percent of respondents have experienced an attempted or realized data theft or corruption by corporate insiders, with media and technology firms and enterprises in the Asia-Pacific region reporting the highest rates (77 percent and 80 percent respectively).



In March 2016, HfS Research and Accenture surveyed 208 enterprise security professionals across a range of geographies and vertical industry sectors. Our key objective was to learn how cybersecurity threats are perceived and countered within the enterprise, with a goal of understanding the state of cybersecurity and the steps the enterprise should take to foster digital trust throughout the extended enterprise.

## On talent...

- Cybersecurity teams are struggling, with 42 percent of respondents believing that while they have enough budget for security technology, they need additional budget for hiring security talent and training. Thirty-one percent of respondents list lack of training or staffing budget as the single biggest inhibitor to cybersecurity readiness.
- Only 20 percent of respondents believe their managed security services provider (MSSP) is a true partner who leads through innovation, while 31 percent believe their MSSP could offer more innovation.
- Seventy-six percent of respondents believe they need some level of improvement in their ability to conduct threat and vulnerability assessments, while an additional 24 percent consider themselves to be state-of-the-art.

## On technology...

- Enterprises are relying on the same established technology, such as firewalls and encryption, to combat cyber threats, but the hottest growth areas are cognitive/AI, data anonymization, behavioral tracking, and automation—areas that involve new spending and new skills.

## On parity...

- Differences in security maturity among different enterprise units and functions continue to exist, with IT teams being rated the most secure and sales teams rated the least secure (with 25 percent of respondents stating their sales force is either not very or only somewhat secure).
- Between 35 percent and 57 percent of enterprises say they vet ecosystem partners for cyber-integrity and preparedness, with BPO partners being the least vetted and credit partners being the most vetted.
- Differences in cyber preparedness among business units, geographies, and vertical industries continue to demonstrate that not all ecosystem partners are at the same level of cybersecurity preparedness.

## On budget...

- Seventy percent of respondents cite a lack of, or inadequate, funding for either cybersecurity technology or security talent (including training).
- An additional 12 percent of respondents state they have inadequate funding/staffing levels and/or are being asked to cut back.



"In today's digital business environment, trust is built on two components: ethics and security. Trust is the cornerstone of the digital economy."

Source: Accenture Technology Vision 2016 Survey, People First: The Primacy of People in the Digital Age  
[www.accenture.com/technologyvision](http://www.accenture.com/technologyvision),  
#techvision2016

## On management...

- While 54 percent of respondents agree or strongly agree that cybersecurity is an enabler of digital trust for consumers, 36 percent believe their executive management considers cybersecurity an unnecessary cost.
- Large enterprises (greater than 50,000 employees) have the largest percentage of cybersecurity professionals who believe management views cybersecurity as an unnecessary cost (48 percent), a number matched within public sector/government/non-governmental organizations.
- Only a third (36 percent) of cybersecurity professionals have a direct reporting relationship to the CEO, with cybersecurity professionals anticipating a shift in reporting structure away from the CEO and CIO in favor of the COO and chief risk officer (CRO).
- Only 5 percent of respondents' organizations have a chief risk (or trust) officer who reports directly to the CEO or board of directors.

## Recommendations from our analysis of the study results include the following:



Executive management should assume a visible, vocal, and engaged position on cybersecurity, fostering a culture that values and leverages enterprise-wide digital trust.



Existing cybersecurity talent should be increased and trained, using holistic security practices and emerging technologies to address the number and sophistication of cyberattacks.



Cybersecurity operations and executive management should collaborate to identify and close gaps between security requirements and execution ability in areas such as talent and training; technology and process; and budgets and finance, with an eye toward ensuring a high level of enterprise-wide security preparedness.



Enterprise cybersecurity teams should establish innovation and testing capabilities to rapidly and efficiently identify and test new technologies (such as behavioral analytics, automation, cognitive computing and physical/digital integration) to keep pace with the evolution of cyber threats.



Enterprises should change how cybersecurity funding is viewed. Instead of treating costs as overhead, companies should adopt a holistic approach—one that includes the cost of securing data and allowing it to be used—as part of overall business initiative financial requirements.

# The State of Cyber Threats

## All threats are not created (or treated) equal

The cyber threat landscape continues to be complex, with increasing risk. External parties calculating enterprise "value" are considering the ability of an enterprise to protect and leverage its assets. Insurance firms writing new policies are weighing the type of data in an enterprise and corporate behavior. Credit agencies are penalizing organizations unable to protect themselves from cyber risk. And ecosystem partners, such as suppliers, distributors, and financial institutions—along with consumers who are continually evaluating brand trust—are increasingly asking for insight into data and security practices before they ink an agreement or deal.

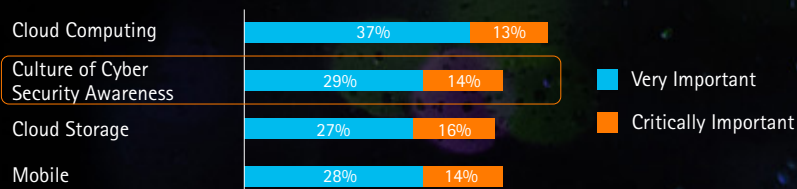
## Digital transformation and the shift to the cloud show no sign of slowing

Most enterprises today are deep into the process of digital transformation, including a massive shift from legacy, owned infrastructure to hybrid or outright public/private cloud environments. The power of digital is bringing both value and risk to the enterprise. It's no surprise that 50 percent of respondents listed cloud computing as either very important or critically important to their overall business strategy. Cloud computing, along with cloud storage, continues to be one of the top drivers of the move to digital.

Cloud is particularly important to banking and financial services; media and technology; and health care/pharma sectors, with each sector rating cloud computing as very or critically important at 64 percent, 54 percent, and 55 percent, respectively.

The counter balance here is in promoting a culture of cybersecurity awareness, also rated by 43 percent of respondents as being very or critically important. While this is a positive sign, we expect that rating to increase over the coming 12 to 18 months.

### How important are the following initiatives to your overall business? (Very or Critically Important responses only)



Other categories not shown include SaaS (31%/10%); ITO (26%/14%); BPO (27%/13%); IoT (26%/13%); BYOD (23%/9%).

Source: "The State of Cybersecurity and Digital Trust 2016"  
Accenture and HfS Research - Sample: 208 Enterprise Security Professionals



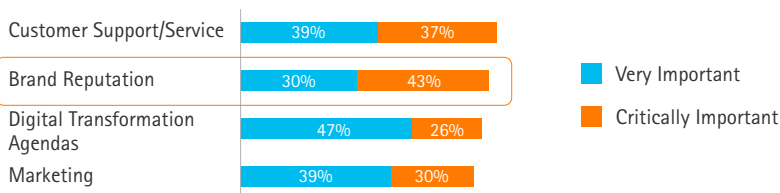
Cloud computing and IoT were ranked the least important overall initiatives to the Resources sector.



## Customer-facing initiatives require strong security for digital trust

Building on the shift to the cloud, the requirement to properly secure data is extremely strong because the cloud is often an element of a larger digital transformation agenda and the underlying mechanism for most customer-facing engagements. Our research shows that customer support/service, brand reputation, and marketing dominate the list of areas that respondents say must be properly secured.

**How important to the following business goals is your ability to properly secure your data? (Very or Critically Important responses only)**



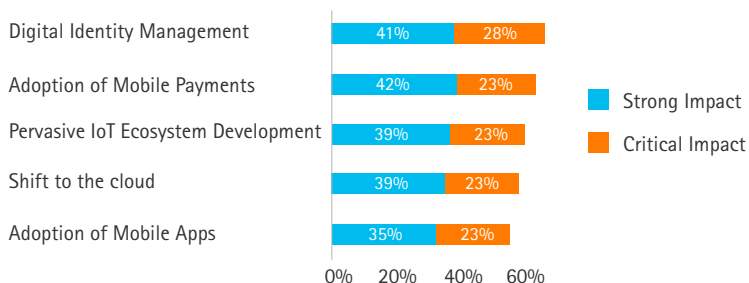
Other categories not shown include Business Expansion (39%/28%); Building Partner Ecosystem (37%/28%); Geographical Expansion (35%/22%).

Source: "The State of Cybersecurity and Digital Trust 2016"  
Accenture and HFS Research - Sample: 208 Enterprise Security Professionals

## Digital transformation is having a major impact on data security

As enterprises work through the process of digitally transforming both internal and customer-facing operations, there is a greater level of risk as the volume and kinds of data that are exposed (including aggregated data) increase, and stored (but accessible) data grows exponentially. Additionally, the number of mobile or remote digital devices and apps that need to engage within the enterprise continues to increase. Digital identity management, the adoption of mobile payments, and the implementation of a pervasive Internet of Things (IoT) deployment are all having a significant impact on enterprise security. Consistent across all enterprises, digital initiatives are considered by more than 50 percent of all respondents as having a strong or critical impact on data security.

**What impact are the following trends and/or initiatives having on business resilience and your ability to properly secure your data? (Strong or Critical Impact responses only)**



Source: "The State of Cybersecurity and Digital Trust 2016"  
Accenture and HFS Research - Sample: 208 Enterprise Security Professionals



## The threat to data comes from within

Previous research by HfS Research identified the emergence of the “corporate insider” as a key player in the theft of both corporate and personal data. Our current research confirms this finding, with 69 percent of respondents having experienced attempted or successful data theft or corruption by corporate insiders during the prior 12 months.

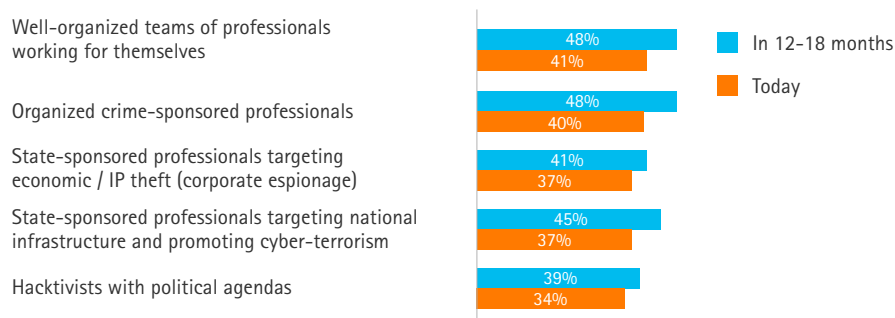
Media and technology firms, along with enterprises in the Asia-Pacific region, reported the highest rates (77 percent and 80 percent respectively). Unfortunately, this insider risk will continue to be an issue, with security professionals' concern over insider theft of corporate information alone rising by nearly two-thirds over the coming 12 to 18 months.

One positive data point from our research is the convergence of digital and physical security, with more than 30 percent of respondents rating unauthorized physical access in data and office facilities either a strong or critical concern. This level of attention can be viewed as positive in that it highlights an increased awareness of the importance of bringing physical and digital security together under a larger risk umbrella.

## The threat to data is also external

While our survey data shows a very high level of concern for the theft or corruption of data by insiders, the threat actors of greatest concern are typically external to the enterprise. The threat sources of most concern to enterprise security professionals are private, well-organized teams, organized criminals, and state-sponsored professionals, with agendas of corporate espionage and targeting critical infrastructure. Over the coming 12 to 18 months, while organized teams of professionals and organized crime are considered as strong or critical concerns by 48 percent of respondents, current or former employees (when grouped together) are rated at a similar level of concern by only 28 percent of the respondents, with contractors, ecosystem partners, or services providers (also considered potential “insiders”) drawing the attention of only 31 percent of respondents.

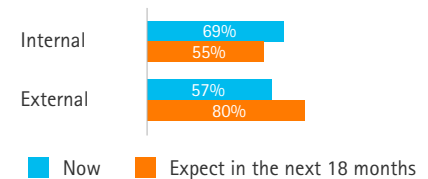
### What level of concern do you have for the following threat groups? (Strong & Critical Concern only)



Other categories not shown include Professionals (Individuals) working for themselves (32%/38%); Contractors, Ecosystem Partners or Service Providers (28%/31%); Amateurs (26%/34%); Current or Former Employees (21%/28%).

Source: “The State of Cybersecurity and Digital Trust 2016”  
Accenture and HfS Research – Sample: 208 Enterprise Security Professionals

### Have you experienced the theft or corruption of internal corporate or user/consumer information by Internal or External threat actors?



Source: “The State of Cybersecurity and Digital Trust 2016” Accenture and HfS Research –  
Sample: 208 Enterprise Security Professionals



We caution against using these metrics as a measure of trust. Instead, we believe it is consistent with a greater level of overall threat coming from organized threat actors, the anticipated ability of cybersecurity teams to more effectively monitor individuals within the enterprise, and reduced risk from former employees who no longer have access.

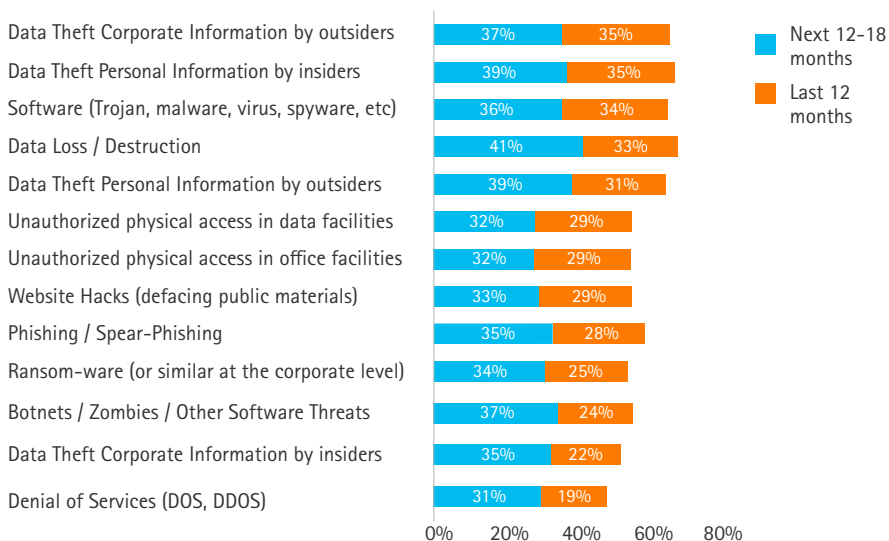
## Overall threats are shifting

A telling aspect of the shifts occurring in cyber threats can be seen when various threats are compared directly. Topping the list of current threats (rated as major or critical threats) are data theft of corporate information by outsiders and data theft of personal information by insiders—both slightly ahead of software (such as Trojan, malware and virus).

Looking forward over the coming 12 to 18 months, however, we see a stronger trend. While concern for every threat category is slated to increase, the most significant increases involve concern for data theft or corruption of corporate information by insiders (a 62 percent increase), denial of Service (DOS, DDOS) attacks (a 59 percent increase), and botnets, zombies, and other software threats (a 57 percent increase). The rate of increase in concern for these thefts significantly outpaces the remaining threats, and brings them up to par with others in terms of threat level.

The increased concern (or risk) involving insiders is troubling and hints at an expectation that the highest-rated threat groups will begin to rely on insider support as part of their cyber attack strategy. Also notable is the increase in concern for phishing, a technique that often involves turning unsuspecting staff into unwitting insider threat actors. This potential risk highlights the value of behavioral analytics tools as part of a cybersecurity strategy.

**How concerned were you during the prior 12 months of the following threats and how concerned are you moving into the coming 12 to 18 months?**  
(responses citing Major or Critical Threats only)



Source: "The State of Cybersecurity and Digital Trust 2016"  
Accenture and HfS Research – Sample: 208 Enterprise Security Professionals

# The State of Cyber Response

## How an enterprise views its capability to respond is just as critical as its actual ability to respond

Perception is reality—what we see and pay attention to is the reality we inhabit. Success in any activity requires a consistent, predictable, and reliable effort by all stakeholders.

Nowhere is this truer than the realm of cybersecurity and the efforts to protect and leverage enterprise data, relationships, and consumer trust. Staying one step ahead of cyber threats and creating a trusted enterprise requires a solid array of assets, including talent, trusted partners, technology, budget, and—most importantly—operational and executive management support.

So where does the enterprise stand today? Perhaps surprisingly, 40 percent of respondents report they have real-time detection of cyber monitoring/spyware and Web/content manipulation. These types of threats are relatively easy to spot and do not reflect the delayed detection and response times typical of well-orchestrated, mass-risk cyber attacks.

Additionally, there are gaps that are cause for concern: gaps between talent supply and demand, gaps between security teams and management expectations, and significant gaps between budget needs and budget realities.

What are these gaps? And how should they be addressed?

## The Five Cyber Gaps

Digital trust across the extended enterprise is critical to enabling the digital economy, and cybersecurity is a core enabler of digital trust. Our research identified five significant gaps, that have the ability to hinder cybersecurity efforts and the ability of enterprises to effectively counter increasingly well-organized and targeted cyber threats:

### Talent Gap

The growing gap between the technical and operational skill set required and the pool of talent, despite the increased value to be gained through automation

### Budget Gap

The growing gap, fueled by financial realities and management focus, between the budget required to secure the enterprise and available funds

### Technology Gap

The gap between the growth of cyber threats and the ability to quickly deploy and leverage new technologies to secure business initiatives

### Management Gap

The perception gap between executive management and security operations management—perhaps the one gap that, if addressed, can lead the way to closing the other gaps

### Parity Gap

The gaps in cyber preparedness (and threats) among regions and verticals, and within the extended enterprise, which increase risk for multi-national organizations



State-of-the-art cybersecurity technology is a means to an end, not an end in itself.



Failure to proactively address these gaps could significantly weaken enterprise security, slow cybersecurity maturity and lead to increased enterprise risk.



## The Talent Gap

**OVERVIEW:** Enterprise cybersecurity teams are struggling to overcome a gap between the security talent needed and the security talent available within the enterprise.

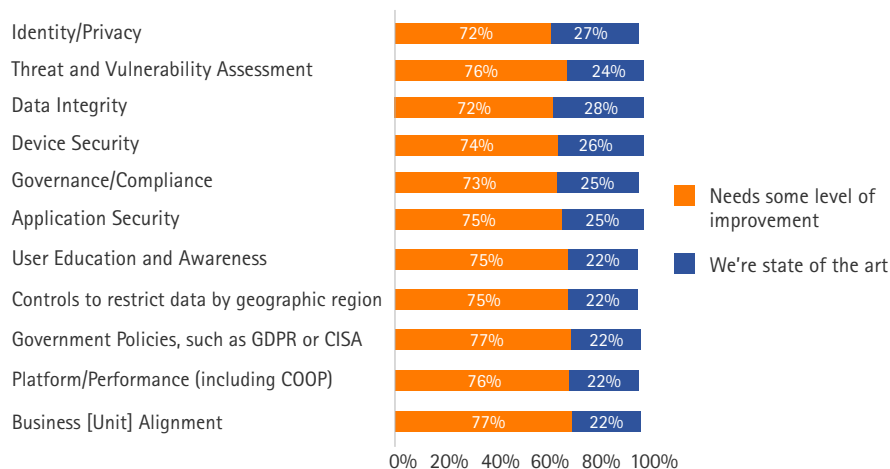
Why the need for security talent? Enterprise security is evolving rapidly.

New threats, enhanced disciplines and security tools, greater business integration, and new and disruptive enterprise initiatives and technologies are placing increased stress on existing staff.

While they have enough budget for security technology, 42 percent of respondents believe they need additional budget for hiring security talent and/or training, while 31 percent of respondents list either lack of training or staffing budget as their single biggest inhibitor to cybersecurity readiness.

Overall data (not shown) indicates 74 percent of respondents believe they need some level of improvement in their ability to conduct threat and vulnerability assessments (ranging from not very prepared to well prepared), while 24 percent actually consider themselves to be state-of-the-art.

### How prepared are you [your staff] to handle each of the following?



Source: "The State of Cybersecurity and Digital Trust 2016"  
Accenture and HFS Research – Sample: 208 Enterprise Security Professionals

Significant demand exists for greater levels of talent or understanding both within the enterprise cybersecurity team and throughout the greater enterprise ecosystem. 54 percent of respondents (70 percent within EMEA) indicate their employees are underprepared to prevent security breaches (not well prepared, somewhat prepared, or merely adequately prepared). The numbers are only slightly better when it comes to detecting and responding to breaches/incidents, at 47 percent and 45 percent respectively.

A gap—at least of perceptions—exists when it comes to the adequacy of talent to handle cyber emergencies. But when enterprise security teams look externally for help, only 20 percent of respondents believe their managed security services provider is a true partner who leads through innovation (a critical element when shifting responsibilities from internal to external organizations).

To counter this talent gap, many organizations and service providers are looking to inject a high level of automation and cognitive/AI into the cybersecurity mix, and this does show promise—particularly in the area of eliminating (or automating) much of the Level I work that is done today. But there is a potential side effect in that entry-level security talent will be expected to perform at (or close to) Level II from the beginning—again placing a strain on new and existing talent.



Collaboration will be critical to achieving maximum value from the extended cybersecurity team, from core professionals to the most remote user.



Acquiring top talent is a start, but continually "upgrading" existing talent through rigorous training and testing programs is essential to cybersecurity in the 21<sup>st</sup> century

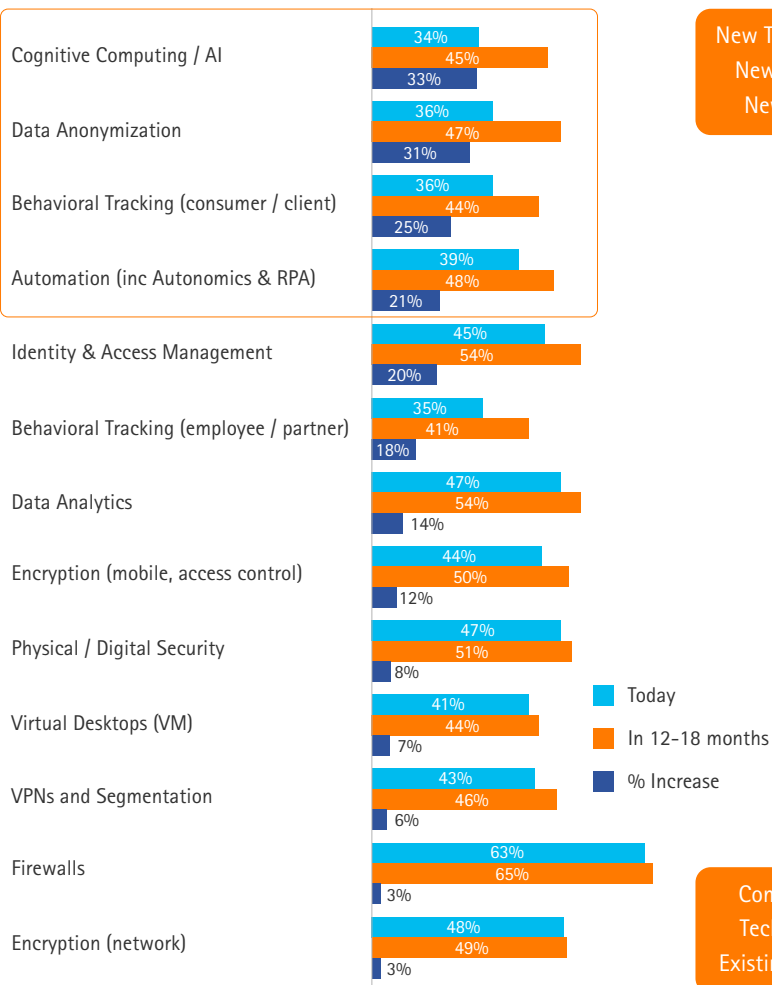
**OPPORTUNITIES:** The talent gap is very real and continues to be an issue for both service providers and enterprise cybersecurity teams. While security teams must find a budgetary solution to recruiting and training talent, there is an opportunity to address this gap through provider partnerships as well as rethinking how digital trust and security can be holistically woven into the enterprise fabric, including applications, automation, cognitive/AI, and business partnerships and processes.

## The Technology Gap

**OVERVIEW:** The Technology Gap—directly influencing the ability to both detect and respond to threats—is apparent across all sectors, and is highlighted by the upcoming shift from legacy to newer technologies that will strain both budgets and talent.

The move to digital dominates the enterprise planning cycle, and is key to most major business initiatives. Firewalls and encryption top the list of the most important technologies deployed today to combat cyber threats, but the largest increase in deployments anticipated over the coming 12 to 18 months are in the areas of cognitive computing/AI, data anonymization, behavioral tracking and automation—areas that involve significant new spend and talent growth.

Please indicate how important you feel each of the following technologies are today and how important they will be within 12 to 18 months (Very or Critically Important only)



55 percent of cybersecurity professionals in the healthcare/pharma sector believe cognitive computing/AI will be either very or critically important to their ability to become a secure, digital enterprise.



Rapid evolution of technology and parity between the enterprise and the threat actor has eliminated the concept of "technical" state-of-the-art.

Source: "The State of Cybersecurity and Digital Trust 2016"  
Accenture and HFS Research - Sample: 208 Enterprise Security Professionals

The idea that firewalls and encryption top the list of most important technologies is in line with the notion that these technologies have become commodity-driven table stakes—as the foundation of security, they have been embedded in cybersecurity for over a decade. Identity and access management, and data analytics, which round the top four, are similarly core, although the technologies themselves are rapidly transforming.

The challenge comes when viewing technologies that will see the largest increase in importance, and potentially have the greatest impact on cybersecurity preparedness, as all involve a new wave of implementation and skills: cognitive computing/AI, data anonymization, behavioral tracking (consumers and clients) and automation (including autonomies and RPA). These tools are fundamentally different than those before them, and bring with them significant implementation challenges.

Where will these emerging technologies have the greatest impact? Large enterprises (in excess of 50,000 employees) lead the way, with solid implementations expected in:

- Health care/pharma (through cognitive computing/AI and data anonymization), with an emphasis on both creating intelligent insights, and collaborating effectively and securely with the most sensitive data sets
- Products (through behavioral tracking of customers and partners, and automation), with an emphasis on preventing fraud.

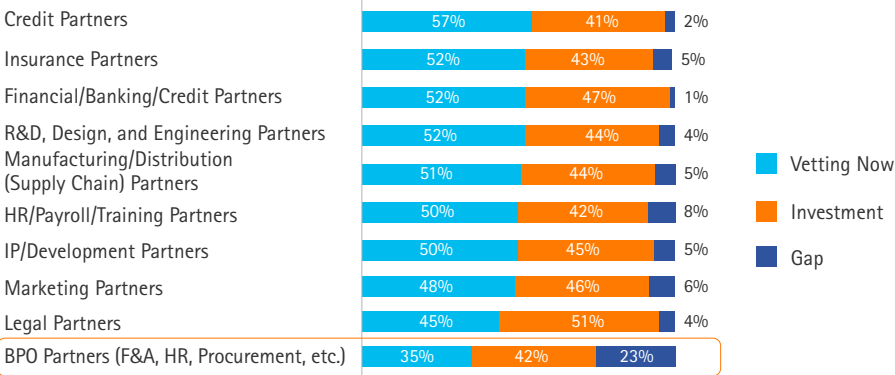
In tandem with the deployment challenge, we anticipate the platform required to implement and properly manage these types of systems will be fundamentally different than legacy security platforms, requiring a new level of data awareness as well as fundamental changes in both talent skillsets and cybersecurity processes.

## The Organizational Parity Gap

**OVERVIEW:** Even while talent and technology gaps exist within the enterprise, there is a solid move underway to bridge a parity gap between partners in the extended enterprise ecosystem.

An enterprise is only as secure as its least secure partner, a key point in several major security breaches over the past few years. For an enterprise that has addressed internal talent and technology gaps, those same gaps within partner networks—which can vary considerably among divisions, regions, or verticals—can create risk for information that has been shared with a partner or afford the opportunity for a threat actor to move laterally up the supply chain. This type of risk does not necessarily need to involve data; it may be enough for a threat actor to shut down an enterprise partner network to inflict damage onto the enterprise (particularly if that partner provides consumer-facing services).

**Do you have a mechanism or set of policies (SOP) to vet ecosystem partners for their own cyber-integrity and preparedness, and where do you expect to invest over the coming 12 to 18 months?**



Source: "The State of Cybersecurity and Digital Trust 2016"  
Accenture and HfS Research - Sample: 208 Enterprise Security Professionals

**OPPORTUNITIES:** To smooth the transition from legacy to emerging technologies and processes, enterprises should move quickly to adopt a long-range strategy coupled with a "conceptualize-test-implement-refine" methodology. Budgetary constraints, including both technology and talent, should be addressed up front, with a possible reallocation of resources anticipated over the coming two to three years.



The solution to addressing this gap is to properly vet the security and infrastructure architectures of partners, both before and after joining the enterprise ecosystem.

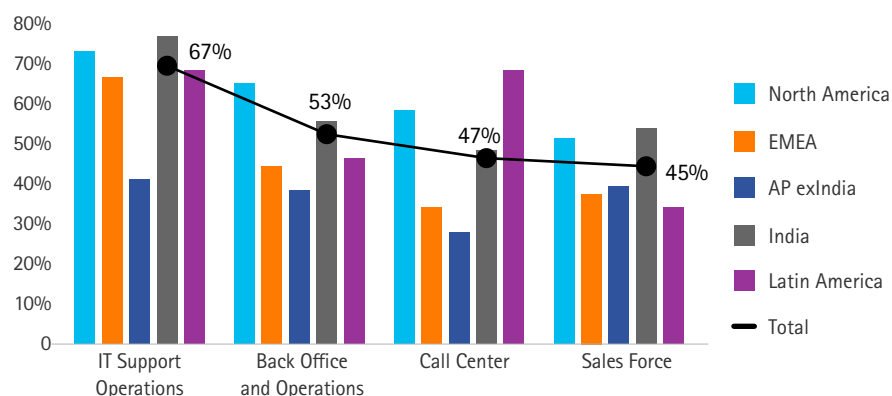
The levels of cyber-vetting are higher than expected, and there are some notable variations on regional and vertical responses. Vetting by firms based in India is consistently 10 to 15 points higher than the average, while Latin America had marginally higher levels of existing SOP for credit and marketing partners. As expected, larger enterprises were rated higher than smaller enterprises (below 1,000 employees), in line with their greater ability to require information from various partners. The highest-rated level of vetting for cybersecurity was within media and technology for credit partners (71 percent – expected due to the high level of subscription buys), and the lowest within resources for BPO partners (only 27 percent).

The challenge is both the gap between where the industry is today (35-57 percent) and where it needs to be tomorrow (100 percent), as well as what constitutes an acceptable cyber vetting process, and how much transparency partners are willing (or perhaps legally able) to provide to others within the extended ecosystem. It is not unreasonable to see these issues ultimately becoming part of a larger regulatory or corporate business requirement for certain industries.

- A 35-57 percent vetting rate is still considered low enough as to put most enterprises at significant risk.
- A 41-51 percent improvement in vetting enterprise partners (legal is the high-point) over the coming 12 to 18 months is a good sign, but still leaves gaps, and it is not clear if the indicated investment is in new vetting procedures or updates to existing procedures.
- Based on 1:1 interviews with enterprise cybersecurity and service provider professionals, there is reason to believe this number may be accurate, but that the depth of vetting at this point may not be significant. This is a critical point as customer data, for example, is increasingly shared across multiple business units—while this data may be secure in one unit, it may be at risk due to vulnerabilities in another, less secure, unit.

Even within a single enterprise, parity of cyber integrity may not exist between business units or geographically distributed organizations and may be significant.

**How cyber secure is <the following> within your organization?  
(respondents indicating Well or Very Well Secured only)**



Source: "The State of Cybersecurity and Digital Trust 2016"  
Accenture and HFS Research – Sample: 208 Enterprise Security Professionals

**OPPORTUNITIES:** Despite a majority of enterprises either currently vetting or planning to vet ecosystem partners for cybersecurity capabilities, enough gaps exist across business functions, market sectors, and geography to conclude this issue continues to be of major concern. Awareness of this gap will attract significant attention over the coming 12 to 24 months as credit ratings and cost of insurance increasingly depend in part on the ability of an enterprise to secure the complete ecosystem.

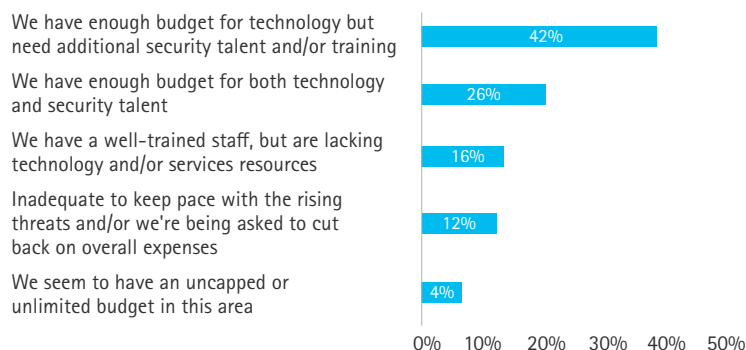
Further, this must be addressed from a top-down management perspective as the overhead associated with complete vetting of partners (as well as the ability to terminate relationships with partners that are not on par with enterprise expectations) could have a significant impact on business operations. Enterprise security professionals must convince executive management that the integrity and trust of the digital enterprise require a greater level of security partnership with all providers, including ensuring cybersecurity technology and process parity and the sharing of best practices and threat intelligence throughout the ecosystem.

## The Budget and Funding Gap

**OVERVIEW:** Budgets are not unlimited, nor are financial models infinitely flexible. The reality of cybersecurity in 2016 is that budgets are under great stress, and cybersecurity professionals are often either short on technology and talent budgets or being asked to do more with less. This has become a key point as technology cycles in the cybersecurity sector are increasingly measured in months, not years.

Cybersecurity has the attention of most executives, with 64 percent of survey respondents reporting they agree or strongly agree that executive management asks for regular updates on overall security and risk management. This is particularly the case in North America and India, with 74 percent and 81 percent respectively (Asia-Pacific was the notably low region at 47 percent). But this has not necessarily translated into budget dollars, as 70 percent of respondents cite a lack of, or inadequate, funding for either cybersecurity technology or security talent (including training).

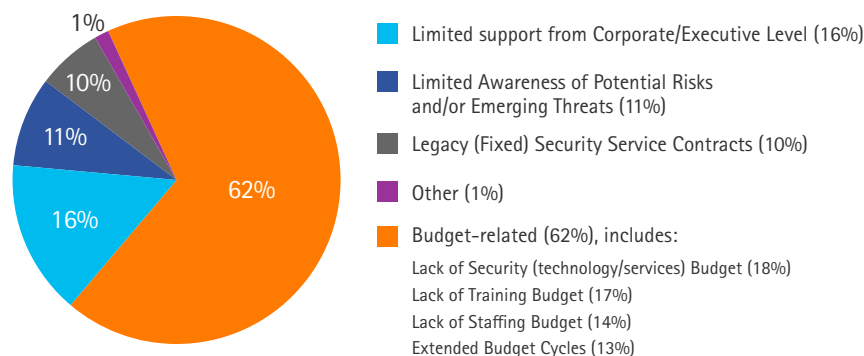
### Which of the following most accurately describes your current funding/staffing levels for Cybersecurity?



Source: "The State of Cybersecurity and Digital Trust 2016"  
Accenture and HFS Research - Sample: 208 Enterprise Security Professionals

This issue is highlighted when we look at the importance of cybersecurity to core business initiatives, with 62 percent of respondents indicating that the biggest inhibitor to their organization's security readiness is budget-related.

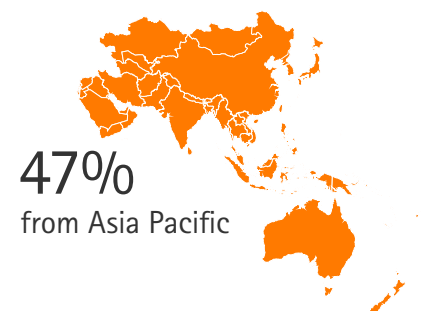
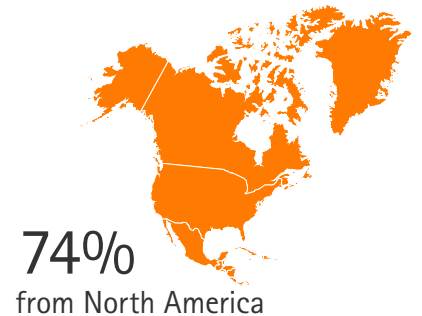
### Which of the following are the biggest inhibitors to your organization's security provision? (single biggest inhibitor)



Source: "The State of Cybersecurity and Digital Trust 2016"  
Accenture and HFS Research - Sample: 208 Enterprise Security Professionals

# 64%

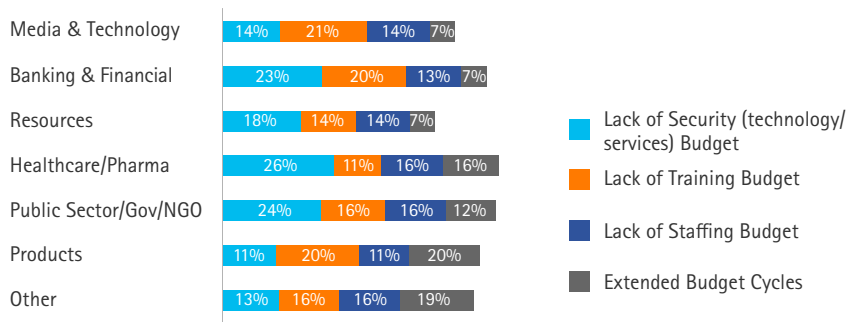
of survey respondents reporting they Agree or Strongly Agree that executive management asks for regular updates on overall security and risk management



What are the vertical sectors most at budgetary risk? Healthcare/pharma, public sector/government/NGO, and banking and financial services are the top three, budget-constrained sectors.

The limited support from corporate/executive level can potentially be seen as a budgetary issue—executives that are limiting overall support are likely to also limit support for budget increases (highlighting not only a budget issue but a potential gap between cybersecurity professionals and the executive team from a management perspective).

**Which of the following are the biggest inhibitors to your organization's security provision? (single biggest budgetary inhibitor, by industry)**



Source: "The State of Cybersecurity and Digital Trust 2016"  
Accenture and HFS Research – Sample: 208 Enterprise Security Professionals

**OPPORTUNITIES:** Budgets for cybersecurity are a relatively new phenomenon—an incremental expense tied directly to the shift to the digital economy. Moving forward, the ability to secure proper funding for emerging technology, staffing, and services may be found in the ability to link or embed cybersecurity directly within risk management (the securing of data assets) and digital trust (the leveraging of secured assets).

## The Management and Operations Gap

**OVERVIEW:** The security-related gaps that exist today within the enterprise can be overcome with a shifting of focus from state-of-the-art technology to state-of-the-art mindset, where the process is continually tested and allowed to evolve and mature. The first step is recognition by both operational and executive management that cybersecurity, and its role in delivering a trusted, digital experience, is one of critical importance to the entire enterprise—security in the digital age is everyone's responsibility.

Our data reveals that cybersecurity professionals understand the importance of holistic cybersecurity, with 43 percent rating a culture of cybersecurity awareness as very or critically important to the overall business of the enterprise (second behind cloud computing).

The challenge lies in the gaps that are revealed between security operations and executive management.

- 35 percent of respondents believe management doesn't concern themselves with security.
- 36 percent of respondents believe management considers security an unnecessary cost.

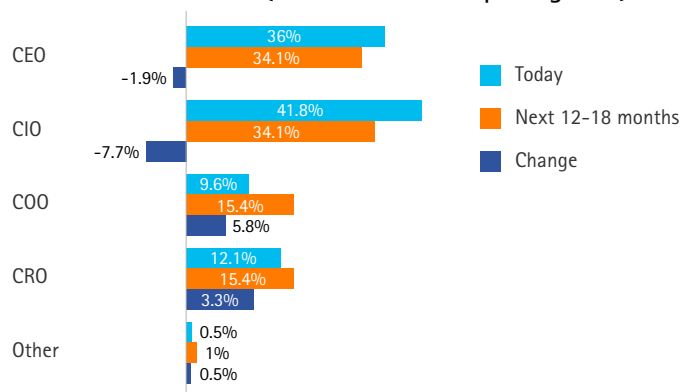
When we look at the individual categories, however, the picture of dissatisfaction becomes clearer. While the net change in reporting structures between the current and the coming 12 to 18 months is marginal, there is a slight decline in the number of security executives reporting directly to the CEO and CIO, in favor of a shift towards the COO and CRO (Chief Risk Officer).



Leadership will be critical in creating an enterprise mindset that is focused on both corporate and personal data responsibility and security—without leadership, digital trust for the enterprise brand cannot be achieved.



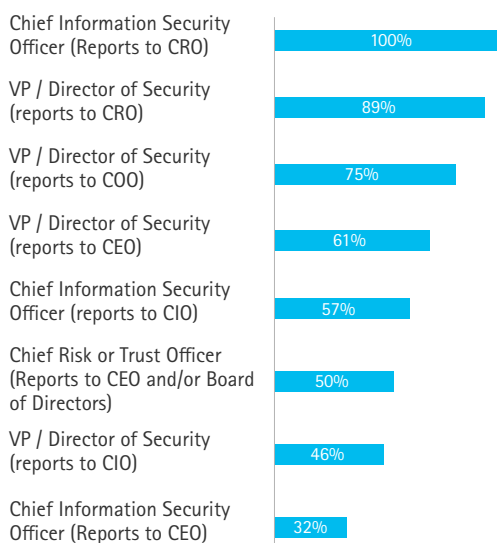
**Which of the following best describes your Security Management Reporting Structure today, and how do you believe it should change within 12–18 months? (data shows % of reporting lines)**



Source: "The State of Cybersecurity and Digital Trust 2016"  
Accenture and HfS Research – Sample: 208 Enterprise Security Professionals

This is within expectations, as we believe the role of the Chief Risk (and Trust) Officer reporting into the CEO or Board of Directors is a sign of growing security maturity from an organization perspective. However, there is tremendous dissatisfaction with all existing reporting lines.

**Which % Respondents want to change reporting lines? (grouped by current reporting structure)**



Source: "The State of Cybersecurity and Digital Trust 2016"  
Accenture and HfS Research – Sample: 208 Enterprise Security Professionals

The numbers are clear: Reporting to a Chief Risk Officer is not a welcome role in today's enterprise—possibly a result of the legacy, risk management approach of most CROs who have yet to integrate digital trust (as an outcome) into what has traditionally been a compliance-based role. This gap must change, even for traditional reporting structures (to the CIO, COO, or CEO) where significant satisfaction gaps also exist.

**OPPORTUNITIES:** The role of the lead cybersecurity professional is still evolving, and there appear to be no clear-cut models that work across the board. What is clear, however, is that the level of dissatisfaction with existing reporting structures is high, budget gaps are increasingly stressing the cybersecurity talent pool, and the threats show every sign of increasing in intensity and risk. This type of gap can only be solved by leadership stepping up, and there exists an opportunity for executive management to become proactively involved in cybersecurity—to incorporate and solicit the input of other executives by reframing the discussion from pure security to enabling digital trust, which impacts all aspects of the enterprise.

# Final Thoughts and Recommendations

## How does the enterprise drive Digital Trust and move into 2017?

Our research results were clear: cybersecurity professionals are asking for help from management, in the form of staffing, training, and the ability to drive a culture of cybersecurity awareness throughout the ecosystem.

The future of the digital enterprise relies upon the ability of cybersecurity professionals, working in tandem with business units, executives, partners, providers and end users — all members of the extended enterprise ecosystem—to create an environment of digital trust where business can flourish. But the challenges, and the perceived diversity of threats and resources, are both significant and varied.

If an organization is unable to properly secure, and trust, its data, if it is unable to procure advanced technology, or lacks the staff to deploy, or if its overall cybersecurity posture isn't enabling a higher level of trust and customer benefit, CEOs and executive team members must drive a cultural shift that embraces cybersecurity. This requires the concept of cybersecurity to be woven into the business model—enabling digital trust and delivering on the brand promise must come from executive leadership.

For the executive, the near-term agenda must be on closing existing cybersecurity gaps in talent, technology, organizational parity, budgets, and management.

## What CEOs and Executive/Operational Management Should Do Today

Achieving a culture of cybersecurity awareness was rated the second most important business initiative to overall business success, surpassed only by cloud computing. Failure to achieve it is considered a strong or very strong risk to enterprise or corporate brand value by 41 percent of respondents. Taking this concept further, it's about developing a culture that enables and leverages digital trust. This must weave throughout the ecosystem of partners, both business and cybersecurity, including threat information sharing, proper mutual vetting of cyber preparedness, and a mechanism for rapidly piloting and implementing new cybersecurity technologies and processes.

What can an enterprise do to foster a culture of cybersecurity and begin to move closer to a state of digital trust? Recognize that state-of-the-art no longer applies to technology but to an adaptive, evolutionary approach to addressing all aspects of holistic security on an ongoing basis.



"The first leadership competency is the management of attention... in the sense of outcome, goal, or direction."

Warren Bennis, from  
"The Essential Bennis: Essays on  
Leadership by Warren Bennis," 2009

### Here are five questions every enterprise should be asking today:

- Are we properly allocating budget dollars towards training and the smart use of automation to improve detection and response capabilities? It's more cost effective to "train up" than it is to hire and onboard new talent, and smart technology can ease the burden.
- Are we measuring the success, or value, of cybersecurity efforts correctly? Tying cybersecurity to specific levels of digital trust and business initiatives can help to properly recognize the value of security technology, training and services.
- Do we have a working process for the vetting and implementation of new technologies, including behavioral analytics, automation and cognitive, for inclusion in our cybersecurity architecture? Planning ahead for emerging technologies—and adopting a fast-fail/minimum-viable-product lab environment—can ease the cost and fail rate for new production security implementations.
- Are we properly ensuring parity among our business units and between our ecosystem partners? Imbalances in security technology, training or process can expose the most secure and trusted network to high levels of risk from less-secure/less-trusted organizations. Vetting, with a goal of achieving parity and limiting unnecessary or risky information exchanges, is critical to eliminating weak access points and lateral threat movement within the enterprise network.
- Are we properly managing our migration towards a state-of-the-art cybersecurity approach that includes embedded and holistic security throughout the enterprise and a focus on enabling digital trust between business units, partners and consumers?

"To gain the trust of individuals, ecosystems and regulators in the digital economy, businesses must possess strong security and ethics at each stage of the customer journey. And new products and services must be ethical and secure by design. Businesses that get this right will enjoy such high levels of trust that their customers will look to them as guides for the digital future."

Source: Accenture Technology Vision 2016 Survey, People First: The Primacy of People in the Digital Age, [www.accenture.com/technologyvision](http://www.accenture.com/technologyvision), #techvision2016

# Appendix A: Focus and Methodology

This research was focused primarily on IT-oriented security—how enterprises protect the data within their core enterprise systems—and was not intended to address the issues that exist in areas such as operational technology and industrial control systems (OT/ICS), embedded device security, application integrity, or physical security. These additional areas, while outside the research scope, are equally important in establishing digital trust and potentially customer safety, and must be ultimately secured against cyber threats (something that may well further stress management, governance, funding and talent resources).

HfS Research and Accenture surveyed 208 organizations as part of its "State of Cybersecurity 2016" project. The fieldwork was conducted in the months of March, April, and May 2016. Enterprise security professionals and members of enterprise executive teams with security oversight were asked about the current and future state of cybersecurity within the enterprise. The survey consisted of 25 questions, developed jointly between HfS Research and Accenture, and spanned three general areas:

- General Background Information: 5 Questions
- Cyber Threats and Trends: 7 Questions
- Organizational Readiness: 13 Questions

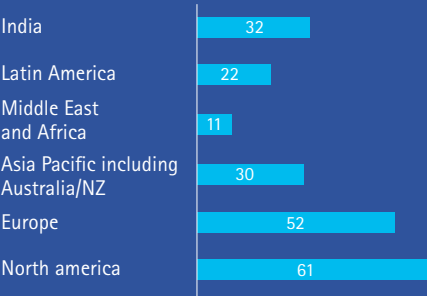
## Respondents

Our respondents were global in nature, with the largest represented geography being North America (29 percent) and the smallest the Middle East and Africa (5 percent). Where appropriate, multiple regions have been grouped to present aggregate results, notably Middle East and Africa being occasionally grouped with Europe as EMEA (representing 30 percent of the respondents).

## Size of Enterprise

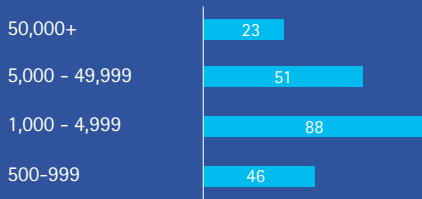
To understand the differences between enterprises of varying size, we collected demographic data on the number of employees within each enterprise (note that multiple survey responses within the same enterprise security team were not allowed). Our largest response group was within enterprises with between 1,000 and 4,999 employees (42 percent) while our smallest response group was within enterprises with greater than 50,000 employees (11 percent, or 23 responses).

# Respondents by Region



Source: "The State of Cybersecurity and Digital Trust 2016" Accenture and HfS Research - Sample: 208 Enterprise Security Professionals

# Respondents by Enterprise Size



Source: "The State of Cybersecurity and Digital Trust 2016" Accenture and HfS Research - Sample: 208 Enterprise Security Professionals



Survey responses were balanced where possible to ensure parity based on industry vertical, geography, and scale. All respondents actively participate in the operations, management, or oversight of cybersecurity within their organization.



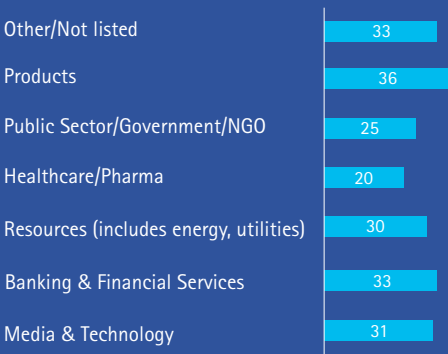
## Vertical Industry

The ability to reasonably compare responses across multiple industry verticals was achieved by sampling representative numbers within each of seven key verticals.

## Role/Position

Respondents were asked to self-identity with the most appropriate role (or position/ title) provided in the survey, with the stipulation that they be involved directly in the operations and/or management oversight of cybersecurity.

# Respondents by Vertical Industry



Source: "The State of Cybersecurity and Digital Trust 2016" Accenture and HfS Research – Sample: 208 Enterprise Security Professionals

# Respondents by Title



Source: "The State of Cybersecurity and Digital Trust 2016" Accenture and HfS Research – Sample: 208 Enterprise Security Professionals

# Appendix B: About the Authors



## Fred McClimans

Research Vice President  
Cybersecurity & Digital Trust, HfS Research

As Research Vice President, Fred McClimans leads our research coverage in the area of digital trust, including technologies and services that enable the trusted ecosystem, such as cybersecurity, secure cloud, customer experience, and trust-enabling technologies (such as automation, analytics, anonymization, and blockchain).

Fred is a seasoned technology and analyst veteran, having founded two analyst firms, including Current Analysis, a global competitive intelligence and market advisory firm that pioneered the use of real-time market analysis coupled with social SaaS tools to help business and brands monetize changes in global markets. Current Analysis, which grew to over 100 global employees, was acquired by Progressive Digital Media (UK) in 2014.

Previously, Fred co-founded Decisys, an analytical consultancy, which was acquired by the Burton Group, and later by Gartner (in 2009). In addition to his years as an analyst at Gartner, Fred's experience includes helping Newbridge Networks (now Alcatel) stand up their Advanced Technology Group, serving as the Chief Information Officer at DTECH LABS (a secure mobile communications provider, now part of Cubic Corporation), and Ernst & Young, where he was a Manager in the Technology Consulting Practice.

Fred lives outside of Washington, DC with his wife and family. An avid competitor, Fred has logged his time as an amateur hockey player/coach, a martial arts instructor, and an assistant to his son's basketball team.

Fred can be reached at [fred.mcclimans@hfsresearch.com](mailto:fred.mcclimans@hfsresearch.com) and followed on Twitter at [@fredmcclimans](https://twitter.com/fredmcclimans).



## Phil Fersht

### Founder & Industry Analyst, HfS Research

Phil Fersht is Founder, CEO and Industry Analyst for leading global analyst authority for the services industry, HfS Research. He is an acclaimed author, analyst and visionary in Global IT services and business operations and has been focusing heavily on automation, cognitive computing and evolving "Digital talent" strategies. Fersht coined the term "The As-a-Service Economy," which is HfS Research's vision for the future of the global services and outsourcing industry and has become widely adopted by the global services industry.

Fersht founded HfS Research in 2010 and has masterminded the development of the HfS organization as a leading analyst for the firm, in addition to steering the business operations. He is also author and creator of the most widely-read and acclaimed blog in the global services industry, entitled "Horses for Sources" and now entering its ninth year, attracting over a million visits per year across the globe. At HfS, he directs the firm's research, advisory and global knowledge community, which today totals over 100,000 professionals and is served by a growing and widely respected global analyst team. HfS has been named Analyst Firm of the Year for 2016, alongside Gartner and Forrester, by leading analyst observer InfluencerRelations.com.

Over the past 20 years, Fersht has lived and worked in Europe, North America and Asia, where he has advised on hundreds of operations strategy, outsourcing, and global business services engagements. During his career, Phil Fersht has worked at Gartner Inc. (AMR Research), directing the firm's BPO and IT Services practices and served as market leader for Deloitte Consulting's BPO Advisory Services, where he led numerous outsourcing and offshoring advisory engagements with Fortune 500 enterprises. He began his career with IT analyst IDC.

Fersht contributes regularly to media such as Wall St Journal, Business Week, Economist, The Times of India and CIO Magazine and is a regular keynote speaker at major industry events, such as NASSCOM, Sourcing Interests Group and the HfS Blueprint Sessions.

He received a Bachelor of Science, with Honors, in European Business & Technology from Coventry University, United Kingdom and a Diplôme Universitaire de Technologie in Business & Technology from the University of Grenoble, France. He also has a diploma from the Market Research Society in the United Kingdom.

Phil can be reached at [Phil.Fersht@HfSresearch.com](mailto:Phil.Fersht@HfSresearch.com) and followed on Twitter at [@pfersht](https://twitter.com/pfersht).



## Jamie Snowdon

### EVP, Research Operations, HfS Research

Jamie Snowdon has primary responsibility for overseeing the development of HfS' Quarterly Market Index, in addition to managing and developing the firm's data-centric products and services. He works across the HfS analyst teams to define evolving services markets and create market size estimates and forecasts. He also manages HfS' quantitative survey and benchmark data.

Jamie has over seventeen years experience in the IT and Business Services industry. In that time he has worked in a variety of roles including sales, marketing, consulting and as an industry analyst. Jamie's analyst career has largely been spent conducting data analysis including market size/forecast models, quantitative/qualitative survey analysis and competitive analysis.

Prior to HfS, Jamie worked for UK-based analyst firm Nelson-Hall as a Research Director, conducting vendor and market analysis within the IT and Business Services community. Prior to Nelson-Hall, Jamie spent seven years at IDC, where he was the European consulting director for IDC's services group, managing all of their bespoke research. Jamie specialized in delivering custom market forecast models and forecasting tools tailored to his client's individual needs. In addition, Jamie ran IDC's European outsourcing research, covering both IT and business process outsourcing. Jamie has wide industry knowledge covering IT consulting, enterprise applications, IT & business process outsourcing, desktop & network services, equipment maintenance, and business continuity.

Earlier in his analyst career, Jamie spent four and a half years at the IT services research specialist INPUT in a mixture of marketing and analysis roles. He left as the UK operations manager having spent two years as a customer services industry analyst. Jamie completed his graduate training at one of the UK's leading electronic and IT distribution companies.

Jamie's passion is learning; he holds university degrees in general science (computing), law and has a post graduate diploma in legal practice. He lives in Twickenham, London with his partner (and soon to be wife), step daughter and Lucky the cat. His other loves include cycling, reading trashy sci-fi, cool technology and the perfect pint.

You can find him on Twitter at [@TheWizeOne](https://twitter.com/TheWizeOne) and via email at [Jamie.Snowdon@HfSresearch.com](mailto:Jamie.Snowdon@HfSresearch.com)





## Bill Phelps

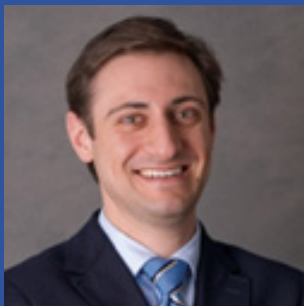
### Managing Director Accenture Security

Bill has led the Accenture Security Services business since 2014. Under his leadership the practice is growing over 20 percent annually, and is a priority growth area for Accenture. Accenture delivers security solutions in three core areas, Digital Identity, Cyber Defense and Managed Security Services. The security services business operates globally, with presence in all major Accenture geographies, and in the Global Delivery Network. Prior to his global role, Bill led the North America Security Services business for four years.

Bill's team delivers innovative security transformation services, as well as comprehensive managed security services for clients who seek to outsource all or part of their security function. Bill is a trusted advisor to senior client security executives and a regular speaker and panelist at major security conferences.

Bill rejoined Accenture in early 2004 after spending four years founding and growing SevenSpace, a company he founded to provide remote infrastructure management services. At SevenSpace, Bill helped pioneer remote infrastructure management capabilities, gaining hands on experience building and operating the infrastructure to support complex, high availability environments. SevenSpace supported one of the largest broadband email and portal platforms, overseeing the design of a resilient infrastructure processing tens of millions of messages daily. SevenSpace was sold to Sun Microsystems and now forms the core of Sun Management Services (now Oracle). Before rejoining Accenture, Bill also served as a member of the Board of Directors for True North Solutions, a security consulting firm providing services and solutions to large government and private sector organizations. Bill has also served as an advisor to a variety of other successful information technology related start-ups.

Bill began his professional career with Accenture in 1986, and spent the majority of his early career in the communications industry, including a year in London. Bill earned his MBA from the University of Texas at Austin where he won the 1986 Moot Corp Venture Design Competition. He also holds a Bachelor of Arts degree from the University of Connecticut. Bill lives in Virginia, just outside of Washington, DC with his wife Cathleen and three children.



## Ryan LaSalle

### Managing Director Growth & Strategy, Accenture Security

Ryan LaSalle is the managing director of Accenture's global growth and strategy for security services. Ryan oversees Accenture's strategic roadmap for the security practice—including offering development, industrialization, strategic alliances, innovation and Cyber Labs—helping clients dramatically improve their ability to adapt and thrive in an evolving threat landscape.

As a senior member of the global security leadership team, Ryan directs the go-to-market plans for enabling client value with responsibilities for embedding next generation innovation into Accenture's suite of security offerings. These differentiated offerings drive transformational value and productivity for clients across strategic industry groups—and are delivered through Accenture's Global Delivery Network, which consists of more than 50 delivery centers across five continents. Prior to assuming his current role, he was managing director of Cyber Labs—part of Accenture's cross-industry research and development Technology Labs—where he led the incubation and launch of mission-focused and active defense strategies.

During his 17 years with Accenture, Ryan has led client engagements across commercial, non-profit and the public sector by integrating emerging technologies into advanced solutions to drive agility and meet business needs. He consults with customers on focused solutions that bring together analytics, knowledge discovery, and cyber-security to improve threat assessment and response methodologies.

A widely recognized thought leader, Ryan is a Ponemon Institute Fellow, active with the Greater Washington Board of Trade and sits on security innovation advisory councils for clients across multiple industries. He holds patents in human resource management, knowledge discovery and establishing trust between entities online. Ryan is a frequent speaker at international security conferences and has authored numerous articles on cybersecurity. Ryan holds a bachelor of science degree in electrical engineering from Princeton University and resides in Alexandria, Virginia with his wife Melissa and two children.

## About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 373,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at [www.accenture.com](http://www.accenture.com).

## About HfS Research

HfS Research is The Services Research Company™—the leading analyst authority and global community for business operations and IT services. The firm helps enterprises validate their global operating models with world-class research and peer networking. HfS Research coined the term The As-a-Service Economy to illustrate the challenges and opportunities facing enterprises needing to re-architect their operations to thrive in an age of digital disruption, while grappling with an increasingly complex global business environment. HfS created the Eight Ideals of Being As-a-Service as a guiding framework to help service buyers and providers address these challenges and seize the initiative. HfS facilitates a thriving and dynamic global community of more than 100,000 active subscribers, which adds richness to its research. Visit us at [www.hfsresearch.com](http://www.hfsresearch.com).

Copyright © 2016 Accenture  
All rights reserved.

Accenture, its logo, and  
High Performance Delivered  
are trademarks of Accenture.

This document makes descriptive reference to trademarks that may be owned by others.

The use of such trademarks herein is not an assertion of ownership of such trademarks by Accenture and is not intended to represent or imply the existence of an association between Accenture and the lawful owners of such trademarks.