



CYBERSECURITY TALENT

The **BIG GAP** in
Cyber Protection

Eight Recommendations for How
Organizations Can Bridge the
Cybersecurity Talent Gap



By Capgemini Digital
Transformation Institute





There are many dimensions to effective cyber-risk management and protection—from strategy and operations, to governance and culture—but one of the biggest problems is simply the lack of talent. Those companies that are able to attract and retain cybersecurity talent will be much more successful in managing digital risk and profiting from the digital opportunity.

In our 2017 research with LinkedIn, *“The Digital Talent Gap—Are Companies Doing Enough?”* we looked at how the digital talent gap has widened and what needs to happen for organizations to tackle this critical issue. This latest research builds on what we learned but focuses on cybersecurity talent, a skill set that is in low supply and in particularly high demand. We have:

- Surveyed over 1,200 senior executives and front-line employees
- Interviewed key experts, drawn from academia, cybersecurity associations, and the recruitment sector
- Analyzed social media sentiment of around 8,400 current and former employees at 53 cybersecurity firms.

The research methodology at the end of the report provides more detail on our approach. In this report, we offer eight key recommendations for organizations to address two key priorities.

- Priority One: Stepping up the acquisition of cybersecurity talent
- Priority Two: Improving the retention of cybersecurity talent.

Organizations that can successfully attract and retain the best cybersecurity talent will be more effective in containing cyber risks and building a competitive advantage.¹



Who are today's cybersecurity talent?

In our research, we defined cybersecurity talent as those people:

- Who are proficient in cybersecurity
- Who are employed in cybersecurity-related roles
- Are proficient in at least four of the eight soft digital skills that constitute a “digital-first mindset” and are necessary for a successful digital transformation (see Appendix).

Employees with these characteristics constitute nearly a third (31%) of those surveyed. This allows us to compare the responses of cybersecurity professionals with the sentiments of all employees to identify issues that are specific to the cybersecurity segment.

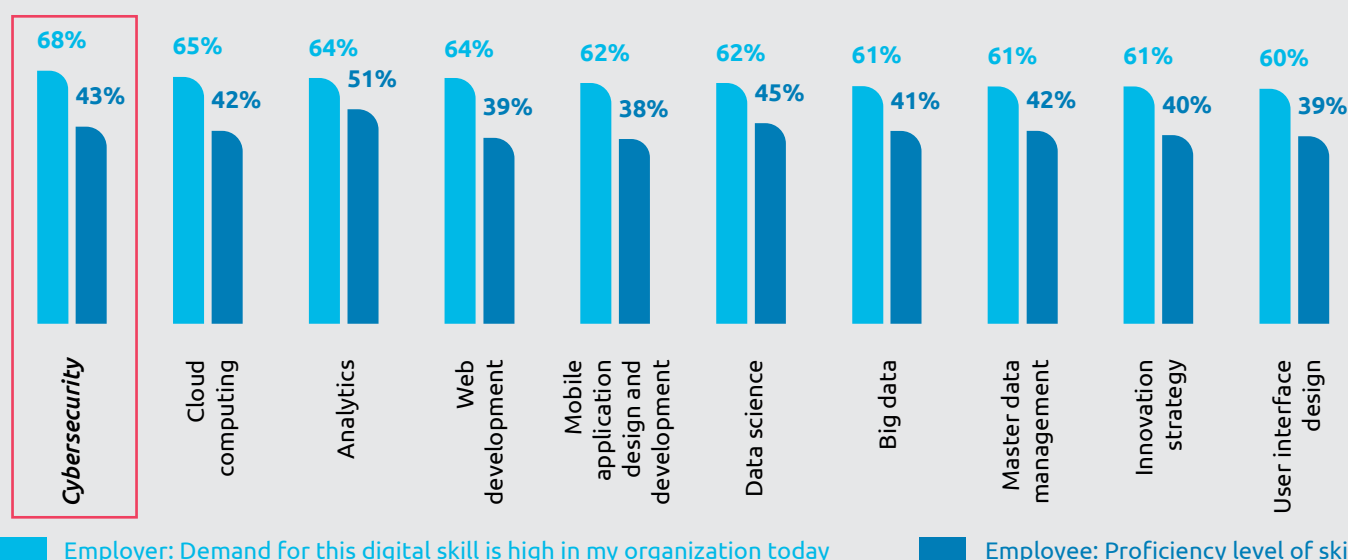
The *“profile of cybersecurity talent”* provides more detail on their defining characteristics.

A rare breed: cybersecurity talent

Over half (55%) of companies say that the digital talent gap is widening and cybersecurity skills rank first in both demand and in talent gap, i.e. the difference between demand and supply (see Figure 1).

Figure 1. Cybersecurity has the largest demand as well as the largest gap between demand and supply

Percentage of organizations that acknowledge that demand for a hard digital skill is high in their organization today and percentage of employees who are proficient in that hard digital skill



Source: Capgemini Digital Transformation Institute survey, June–July 2017, N=501 employers; N=753 employees; ranked by employer demand.

*Demand defined as a rating of at least 5 for the statement “Demand for this digital skill is high in my organization today” on a scale of 1 to 7, where 1 = strongly disagree and 7 = strongly agree; Proficiency defined as level of skill of at least 5 on a scale of 1 to 7, where 1 = least skilled and 7 = highly skilled.

Demand for cybersecurity skills is going to be at the same level for the next five years (see Figure 2).

Figure 2. The demand for cybersecurity is not likely to diminish in the next few years

Percentage of organizations that acknowledge demand for cybersecurity is high in their organization



Source: Capgemini Digital Transformation Institute survey, Digital Talent Gap; June–July 2017, N=501 employers.



Cybersecurity is in such high demand and low supply that candidates sometimes have two, three, or even four job offers at the same time."

Kate Shannon

Managing Partner, Heidrick & Struggles

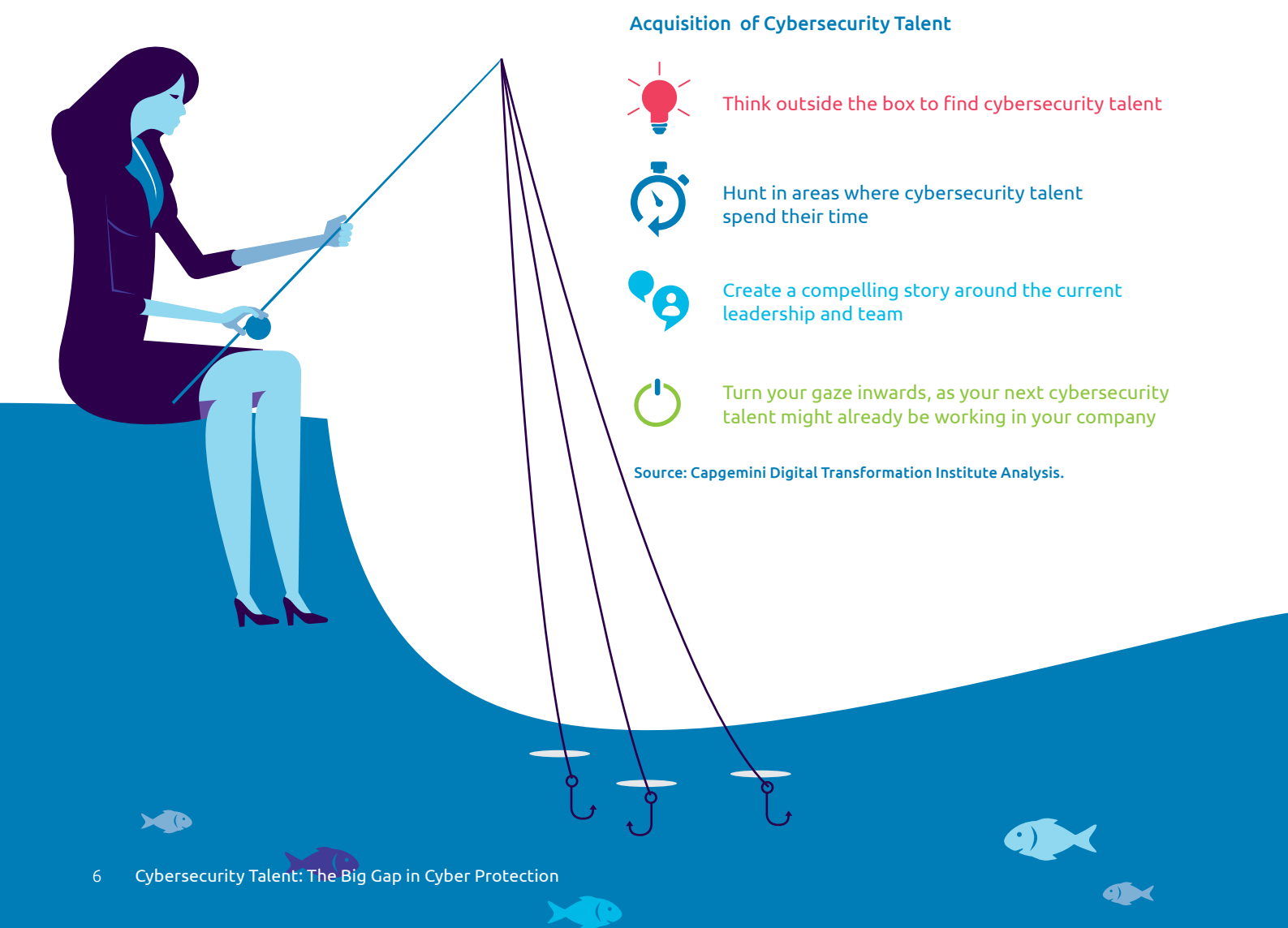


Priority One: Step up the acquisition of cybersecurity talent

Based on the research, we believe there are four areas organizations should focus on to attract cybersecurity talent:

1. Think outside the box to find cybersecurity talent.
2. Hunt in areas where cybersecurity talent spend their time.
3. Create a compelling story around the current leadership and team.
4. Turn your gaze inwards, as your next cybersecurity talent might already be working in your company.

Figure 3. How to step up the acquisition of cybersecurity talent



Think outside the box to find cybersecurity talent

Organizations should look beyond their traditional recruiting models to hire cybersecurity professionals. A few organizations are looking at networking platforms and conferences such as RSA and Black Hat to source talented professionals and are hiring from outside their sector.² Recorded Future, a cybersecurity startup, has successfully recruited from the ranks of military and government alumni.³ There is also a growing body of research on the benefits of recruiting neurodiverse candidates into cybersecurity, such as individuals on the autism spectrum. Autistic people are often analytical, detail-oriented, honest, and respectful of rules, skills that are ideal for cybersecurity. Auticon, a UK-based information and communication technology firm only employs autistic professionals with many working in cybersecurity roles and firms like Microsoft, SAP, and Freddie Mac have pilot programs in place for hiring people with autism to fill IT roles.^{4,5}



Cybersecurity skills are very specialized. You cannot just expect these skills to be developed in a large company without some new talent coming on board. Companies need to recruit new talent and also train the rest of their teams.”

Tuck Rickards

Managing Director,
Russell Reynolds

Organizations could also use a bug bounty program to develop a talent pipeline. Bug bounties are a way of rewarding individuals for reporting security bugs and organizations could turn this into a recruitment tool. Tech firms such as Apple, Facebook, Google, Microsoft, and Intel, and companies outside the industry also use bug bounty programs. Google has paid more than USD 100,000 to a single researcher as a part of its Android Security Rewards program.⁶ Statistics from Bugcrowd, a platform for bug bounty programs, estimates that the average payout for a critical vulnerability is USD 1,776 and total payouts have been more than USD 6 million.⁷ More than 500 bug bounty programs are available currently, with companies offering rewards, gifts or acknowledgement.⁸ These programs can offer a pool of “ethical hackers” for organizations to find and hire cybersecurity talent who already understand the security landscape of the firms.

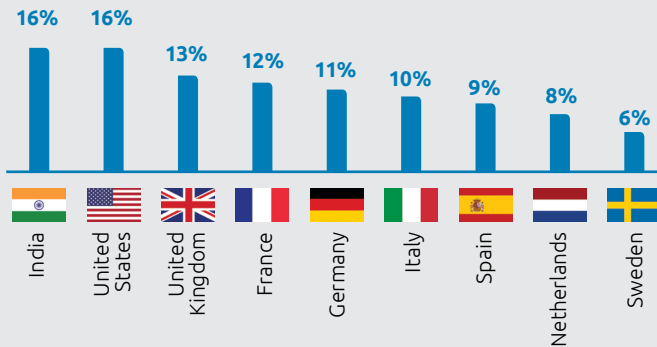
Organizations should also think ahead to help build their talent pipeline. As Michel Cukier, the director for the Advanced Cybersecurity Experience for Students—an undergraduate program at the University of Maryland—says: *“What is really important for companies is to provide internships even at the freshman levels. It’s not just about the junior and senior level, when a company can make an offer. They need to identify early if they want to build a strong relationship with cybersecurity students, especially given how in-demand these students are.”* Jessa Gramenz, Director of Communications at National Cybersecurity Student Association advocates that organizations need to be flexible with whom they recruit. She says: *“The cybersecurity field is constantly changing. New programs are being developed at universities all the time. So, it is important for organizations to look for talent who are adaptable and can fit more than a single job description.”*



Profile of cybersecurity talent

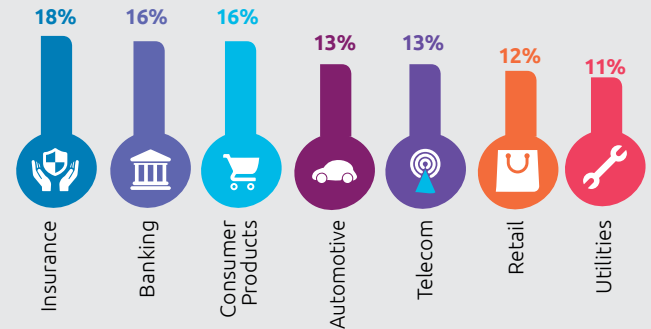
India and the US have the largest cybersecurity talent pool

Cybersecurity talent by geography



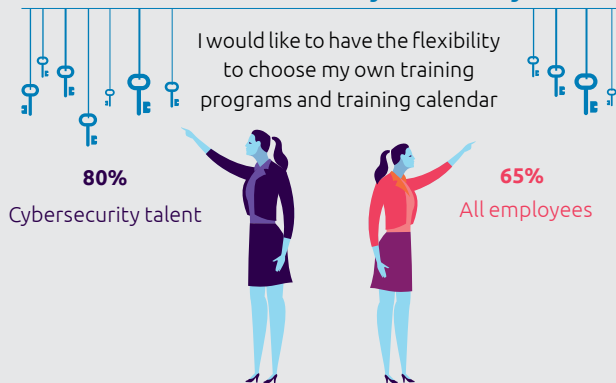
Insurance has the highest proportion of cybersecurity talent followed by Banking and Consumer Products

Cybersecurity talent by industry



Source: Capgemini Digital Transformation Institute survey, Digital Talent Gap; June–July 2017, N=230 cybersecurity talent employees.

Cybersecurity talent want to choose their training



Source: Capgemini Digital Transformation Institute survey, Digital Talent Gap; June–July 2017, N=230 cybersecurity talent employees; N=753 employees.

Top five preferences of cybersecurity talent while switching jobs

- A flexible work-life balance (83%)
- Open and collaborative physical work space (82%)
- Flat hierarchy and accessible management (82%)
- Opportunities to engage with the local community (82%)
- A clear career development path (81%)

Source: Capgemini Digital Transformation Institute survey, Digital Talent Gap; June–July 2017, N=230 cybersecurity talent employees; N=753 employees.

Top five **POSITIVE** factors cited by cybersecurity professionals about why they join or stay with an organization on social media

1. Compensation/benefits
2. Culture
3. Technology
4. Career development
5. Collaborative work environment and learning and development



Top five **NEGATIVE** factors cited by cybersecurity professionals about why they are not satisfied with or leave their organization on social media

1. Career progression
2. Infrastructure
3. Job security
4. Work-life balance
5. Communication

Source: Capgemini Social Media Analysis; January 2018, N=53 cybersecurity organizations, 8,400 employees.

Hunt in areas where cybersecurity talent spend their time

Gen Y and Gen Z talent are looking to join organizations that apply an innovative lens to recruiting. In our survey, 82% of Gen Y and Gen Z cybersecurity professionals (and 78% of all cybersecurity employees) agree with the statement: “I am more willing to engage with firms that use innovative approaches for recruiting or hiring digital talent.” This drops to 57% for all employees (see Figure 4).

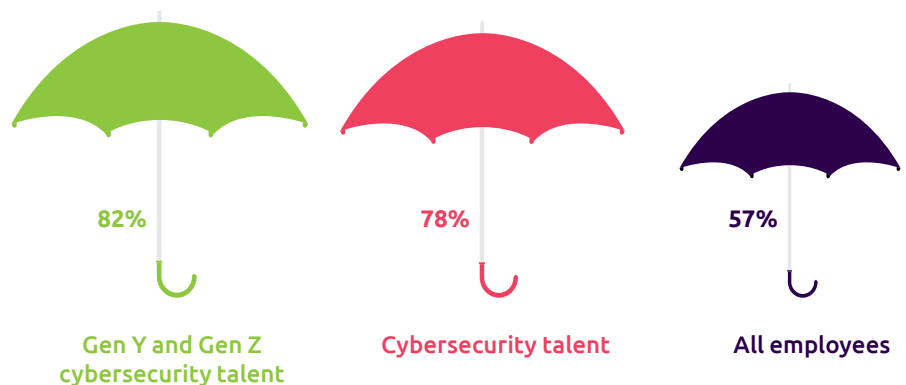
82%

Percentage of Gen Y and Gen Z cybersecurity professionals willing to engage with firms that use innovative approaches for hiring

Figure 4. Every four in five cybersecurity employees want to join a firm that uses innovative hiring practices

Percentage of employees preferring a firm which uses innovative approaches for hiring

I am more willing to engage with firms that use innovative approaches for recruiting or hiring digital talent



Source: Capgemini Digital Transformation Institute survey, Digital Talent Gap; June–July 2017, N=230 cybersecurity talent employees; N=753 employees.

Organizations are beginning to realize the importance of reaching out to a millennial, mobile audience through their platform of choice. For example, Debut, a career app for students and graduates in the UK, brings students and large organizations together in one place. Tesla, Deutsche Bank, and L’Oreal are among the organizations that are using the platform for targeted communications to potential candidates.⁹

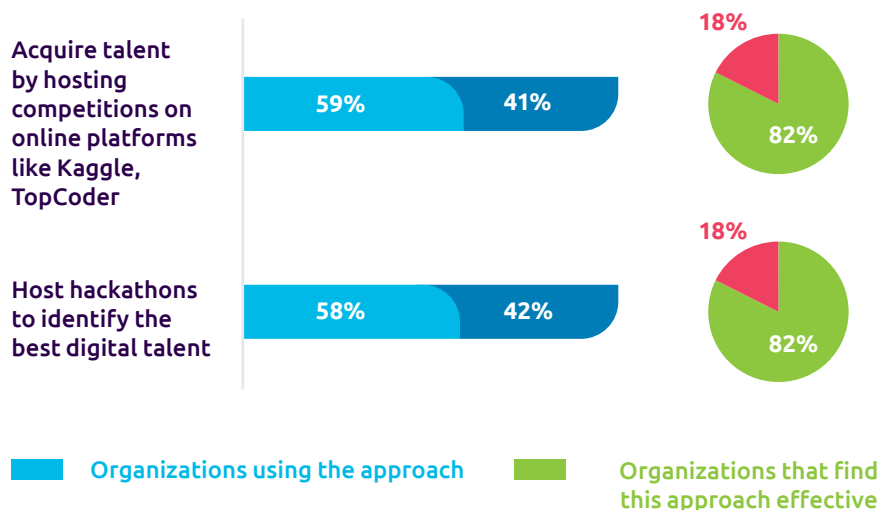
Gamification also provides unique, engaging methods to attract the younger workforce and many leading organizations have incorporated it into their hiring strategy:

- Cyber Security Challenge UK, a non-profit organization conducts yearly gaming competitions to recruit cybersecurity talent. The rewards for winners range from prizes to job opportunities.¹⁰
- Marriott International has deployed a recruiting game that is specifically targeted at millennial employees.¹¹
- L’Oreal uses a game called Brandstorm to attract bright undergraduates.¹²
- Unilever has added game-based assessments to its hiring process to attract millennial candidates and project itself as an innovative employer.¹³

Gamification holds particular relevance for cybersecurity talent. It allows potential candidates to undertake a series of simulation activities and assess their ability to mitigate cybersecurity issues in real time. Our survey findings corroborated this view. Fifty-nine percent of employers we surveyed say that they acquire external talent by hosting competitions on online platforms like Kaggle and TopCoder. Eighty-two percent of those organizations employing this method said it was effective. And the majority (58%) of employers we surveyed say that they acquire external talent by hosting hackathons to identify the best digital talent (see Figure 5).

Figure 5. Three out of every five organizations host competitions and hackathons to acquire talent and the majority of organizations find these approaches effective

Percentage of organizations using the following approaches



Source: Capgemini Digital Transformation Institute survey, June–July 2017, N=501 employers.

ISACA, an association focused on IT governance, developed a new toolset that provides a live platform to assess potential cybersecurity professionals. Through this gamified approach, HR and IT departments can assess a candidate's suitability for cybersecurity roles.¹⁴ GCHQ, the British intelligence and security agency famous for cracking the code for Enigma during World War II, launched a brain-teaser to fill its open positions in security. The successful candidates were then asked to participate in an online treasure hunt.¹⁵ Companies are incorporating Capture the Flag (CTF) competitions—educational exercises that tackle computer security problems in a series of real-world scenarios—into their recruiting process. Trend Micro Inc., an IT security company has run a CTF competition for the past three years to identify a pool of cybersecurity talent and invites the top competitors to finals at their global headquarters in Japan.¹⁶

Getting this right can be very positive, as one current cybersecurity employee expressed: *“I had a fantastic candidate experience before and after joining my firm. The recruiting process was awesome, with quick responses and updates from the talent acquisition team.”*

Create a compelling story around the current leadership and team

Organizations need to create a compelling story to attract cybersecurity talent, particularly around the environment that they are potentially joining:

78%

Percentage of Cybersecurity talent who prefer their peer group to be digitally talented

- Hiring senior executives such as CISOs (Chief Information Security Officers) who can bring new talent along with them. Over half (58%) of employers we surveyed say they use anchor hiring—recruiting experts in an area to attract more talent from that area—to attract digital talent. Employees want to join firms with charismatic leaders. As Governor of the Bank of England, Mark Carney changed the perception toward Canadians in the UK, influencing more people to join the bank and transformed the bank's culture.¹⁷
- Our survey showed that four out of every five employees prefer a digitally talented peer group (see Figure 6). Our social media analysis also corroborates this finding. Cybersecurity employees rank “a talented peer group” in the top 10 positive factors about why they join and stay with an organization. Providing information in a job posting on the peer group that an employee can expect to join can be a powerful influence.
- Organizations can build stories around their star employees, highlighting their credentials and achievements thereby providing role models for interested candidates looking to join the ranks.

Figure 6. Every four in five cybersecurity employees want to join a firm with a peer group that is digitally talented

Percentage of employees who would like a digitally talented peer group

I prefer joining firms where my peer group would be digitally talented



Source: Capgemini Digital Transformation Institute survey, Digital Talent Gap; June–July 2017, N=230 cybersecurity talent employees; N=753 employees.

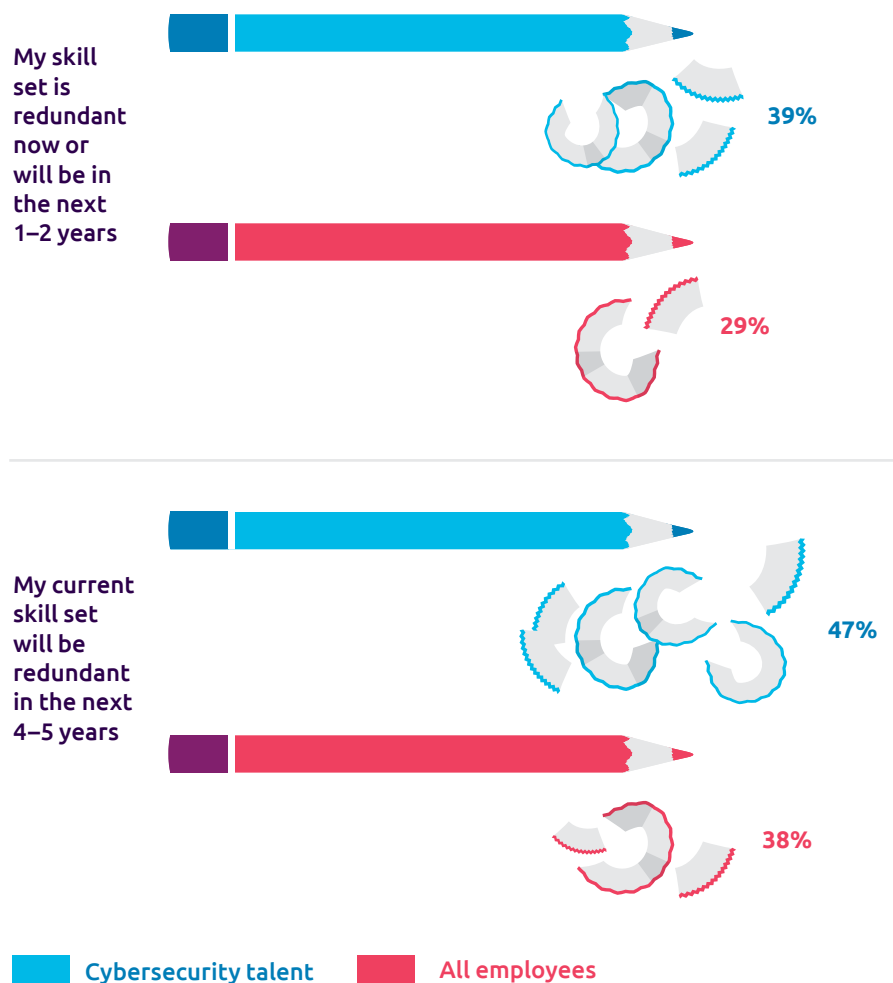
Furthermore, an engaging story about why a cybersecurity professional should join your company would appeal to millennials. According to Michel Cukier, of the University of Maryland: *“The millennial class makes decisions with their hearts. Students want to know the companies they are signing on with. Making yourself known to a student, what your company is about, what the work-life will look like and making the process open, transparent, on a first-name basis... like a family. The stronger the relationship with the company and the student, the more likely they are to hire and keep those students.”*

Turn your gaze inwards, as your next cybersecurity talent might already be working in your company

In the digital age, employees are anxious about their skills becoming quickly redundant. Over a third of all employees—and close to half of cybersecurity talent—believe their skill set will be redundant in the next four to five years (see Figure 7).

Figure 7. Employees believe their skill set is or will be redundant

Percentage of employees believing their skill set is redundant now or will be redundant



Source: Capgemini Digital Transformation Institute survey, Digital Talent Gap; June–July 2017, N=230 cybersecurity talent employees; N=753 employees.

In this environment, people are investing time in learning new skills. We found that one in every two employees said they were investing their own resources to develop digital skills. Organizations need to tap into those people who have invested time in building their cybersecurity expertise and/or train other IT or engineering professionals on security (e.g. training database administrators to become security control engineers or improving the security skills of application developers) to offset the lack of cybersecurity skills. To do so, organizations can:

- Create an inventory of the skills represented in their teams, including skills they utilize in their personal lives that may be applicable to their work (e.g., coding) and motivating employees to add new skills.
- Create a community of cross-functional professionals working in, or interested in, cybersecurity within the organization. This builds and shares knowledge and creates a pool of potential cybersecurity talent.
- “Re-purpose” employees from other IT or engineering specializations. Aflac’s Global Chief Security Officer Tim Callahan suggests that employees like network engineers understand the IT environment and could have an aptitude for security.¹⁸

Keyaan Williams, President of the ISSA (Information Systems Security Association) International Board of Directors says: *“From my perspective, because compliance is such an important business driver, organizations’ focus is on hiring security professionals that are skilled in compliance and they often overlook the skills necessary for a holistic security and risk management program. For example, a security professional that understands risk management, business processes, and knows how to communicate.”* Companies can also consider non-security profiles to complement technical professionals. Keyaan continues: *“If I were running a security program, I’d hire non-security professionals and integrate them into the security team. For example, by hiring a technical writer or a marketing professional into the security team, you get people that can communicate like business folks and have a deeper background in soft skills that complements a team well versed with the legal aspects. It’s hard to teach a highly skilled risk management and security professional to be a good marketer, a good communicator, or a good writer. Technical skills can be taught.”*

Priority Two: Improve the retention of cybersecurity talent

As well as finding the right people, you also need to keep them. Based on our research, we see four actions that are critical to retention:

1. Incentivize employees to upgrade their cybersecurity quotient.
2. Promote gender inclusion by changing the perception of the cybersecurity field.
3. Ensure Gen Y and Gen Z cybersecurity talent can visualize their career path.
4. Automate the mundane tasks to free up cybersecurity talent's time to focus on value-adding activities.

Figure 8. How to improve the retention of cybersecurity talent

Retention of cybersecurity talent



Incentivize employees to upgrade their cybersecurity quotient



Promote gender inclusion by changing the perception of the cybersecurity field



Ensure Gen Y and Gen Z cybersecurity talent can visualize their career path



Automate the mundane tasks to free up cybersecurity talent's time to focus on value-adding activities

Source: Capgemini Digital Transformation Institute Analysis.



Incentivize employees to upgrade their cybersecurity quotient

More than eight out of 10 Gen X employees do not mind spending additional time beyond office hours to learn new skills (see Figure 9). Our social media analysis also reveals that cybersecurity employees value organizations that encourage training. Education and learning rank at five in their list of reasons about why they stay with an organization.



I think that everyone coming out with a university degree should be exposed to some computer science and basic cybersecurity in the same way they are exposed to Math or English. It should be a part of general education. Basic cybersecurity hygiene—such as why strong passwords are important—is very important for the public to learn, especially since we see so many attacks on unskilled users.”

Professor Jonathan Katz
University of Maryland

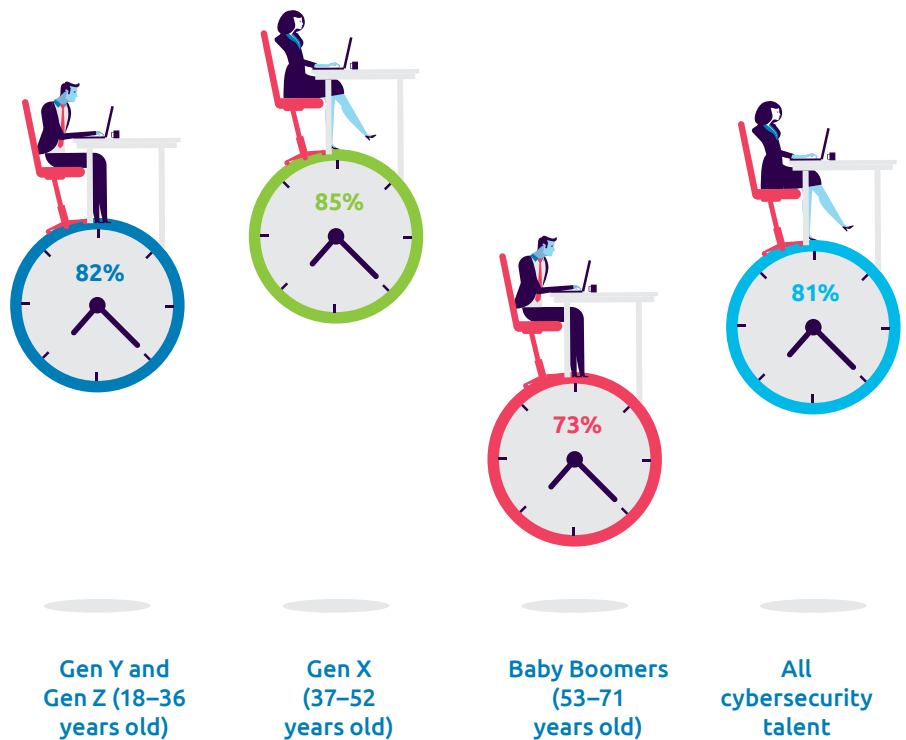


Dear kids: If you want a job in five years, study computer science. If you want a job forever, study computer security.”¹⁹

Aaron Levie
CEO of Box

Figure 9. Cybersecurity employees are keen on learning beyond their office hours

Percentage of employees willing to spend time beyond office hours for learning



Source: Capgemini Digital Transformation Institute survey, Digital Talent Gap; June–July 2017, N=230 cybersecurity talent employees.

In early 2017, AT&T took on a massive retraining initiative for 100,000 of its employees. The aim is that by 2020 they will be prepared for the technological advances that are disrupting the telecommunications industry. The program puts a considerable onus on employees themselves, with the firm providing reimbursement for relevant courses that they attend.²⁰

Promote gender inclusion by changing the perception of the cybersecurity field



A difficult work-life balance”

One of the top five negative factors cybersecurity professionals say as the reason they leave their organization on social media

Studies show that women are underrepresented in cybersecurity.²¹ A root cause for this underrepresentation might be attributed in part to education. As Keyaan Williams of ISSA says, more needs to be done to increase female representation in the cybersecurity field, such as promoting STEM education (science, technology, engineering, and mathematics) among female students. *“The lack of women in cybersecurity goes well before you get to the profession. STEM program enrollment for women is much lower than men. The beginning to the answer to the problem is how to get more women interested in STEM early in elementary and middle school and maintaining that interest in high school and college.”*

It is important for organizations to encourage and support female employees to join the cybersecurity field and remain in the field to bridge the talent gap. Some ways to go about this include:

- Promoting cybersecurity as a career to young female students in elementary and middle school
- Offering more internship programs targeted to female college students
- Providing mentors to female cybersecurity talent
- Highlighting the stories of female role models in cybersecurity on social media.

Another important factor is to ensure all cybersecurity employees, irrespective of gender, have a flexible work-life balance. Flexible work arrangements have become an important factor for employee satisfaction, helping reduce absenteeism, increase productivity, and enhance employee engagement.²² Four out of every five female and male cybersecurity employee we surveyed preferred organizations that allow a flexible work-life balance (see Figure 10). “A difficult work-life balance” falls in the top five negative factors cybersecurity professionals discuss on social media about why they leave or are not satisfied with their organization.

Figure 10. Four out of every five female and male cybersecurity employees prefer a flexible work-life balance

Percentage of employees preferring a flexible work-life balance

I prefer joining organizations that allow a flexible work-life balance



Source: Capgemini Digital Transformation Institute survey, Digital Talent Gap; June–July 2017, N=230 cybersecurity talent employees; N=753 employees.

Organizations can provide flexible work options in many ways, from flexible work schedules to remote working.

Ensure Gen Y and Gen Z cybersecurity talent can visualize their career path

Cybersecurity talent value their career path more than other employees. The clear majority (81%) of cybersecurity talent agree with the statement: “I prefer joining organizations where I have a clear career development path” compared to 62% of all respondents. The number is even higher (84%) for Gen Y and Gen Z cybersecurity talent (see Figure 11). Lack of career progression is the top most negative factor cited by cybersecurity professionals on social media about why they are not satisfied with their current organization.



Figure 11. Most Gen Y and Gen Z prefer a clear career development path

Percentage of employees preferring a clear career development path

I prefer joining organizations where I have a clear career development path



Source: Capgemini Digital Transformation Institute survey, Digital Talent Gap; June–July 2017, N=230 cybersecurity talent employees; N=753 employees.

A current cybersecurity employee sums up the importance of a career path, saying: *"I feel that [my cybersecurity employer] truly values its employees from the top to the bottom. I am in a junior role, but I always feel like my opinion matters and that my voice is heard ... I have a clear and defined career path and am given everything I need to succeed."*

Organizations need to establish processes that provide clarity to its employees. Key actions can include:

- Publishing the job requirements for all roles at all levels, thereby allowing employees to self-evaluate themselves on whether they are eligible for a promotion
- Providing regular feedback on the developmental areas that need to be addressed to progress to the next level
- Creating a career map that details the experience needed for a top performer, average performer, and a below-average performer to move to the highest level in their function/department
- Introducing mobility programs to allow employees to move to other areas of the organization that interest them.

Automate the mundane tasks to free up cybersecurity talent's time to focus on value-adding activities

Automating security intelligence not only removes the boring aspects of the job, but also frees up employees' time.²³ Mastercard, a global payments company, acquired a software company that provides security and fraud protection services through AI. This allows the firm to direct its cybersecurity staff to more critical roles.²⁴ Daqri, a company that makes augmented-reality glasses for architecture and manufacturing, has only one cybersecurity employee in its 300-strong organization. The firm has deployed machine-learning algorithms that monitor feeds from over 1,200 of the company's devices to help manage security issues.²⁵

Conclusion

The implications of a cyber breach for organizations are potentially devastating, from direct costs to reputational damage. But organizations are struggling with a shortage of cybersecurity talent and the problem is certainly not going away. By adopting acquisition, training, and retention strategies that will appeal to cybersecurity talent, organizations can take an important step in upgrading their cyber protection for the current and emerging risks of our connected world.

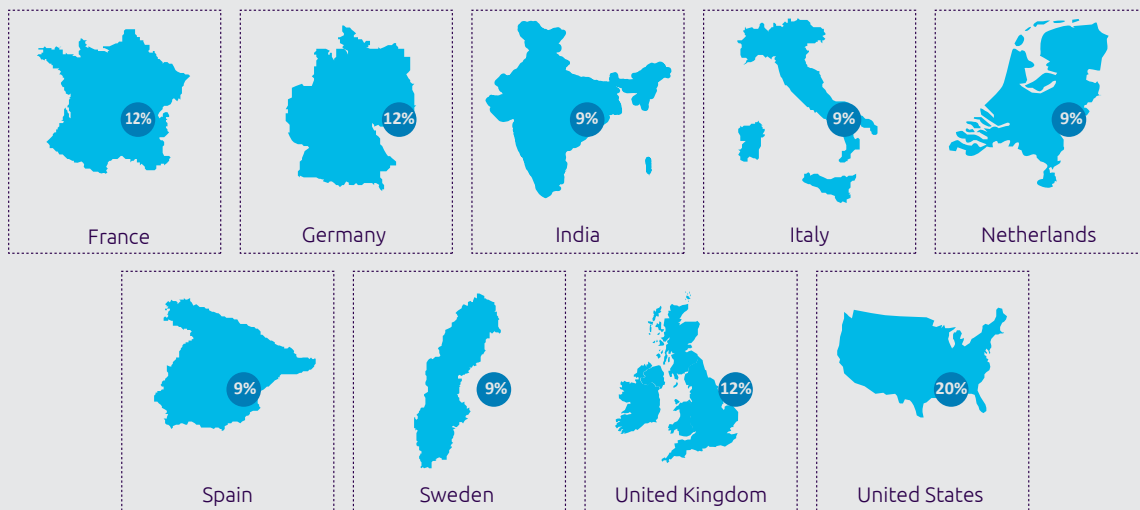




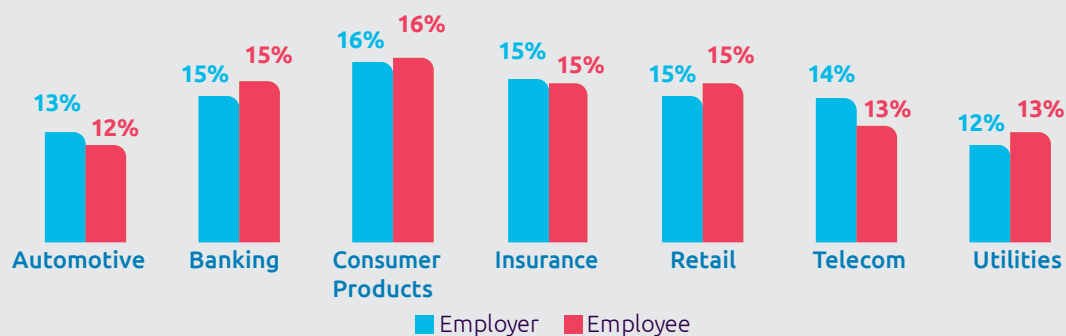
Research Methodology

We surveyed 753 employees and 501 executives at the director level or above at large companies with reported revenue of more than USD 500 million for FY 2016 and more than 1,000 employees. The survey took place from June to July 2017, and covered nine countries—France, Germany, India, Italy, the Netherlands, Spain, Sweden, the United Kingdom, and the United States and seven industries—Automotive, Banking, Consumer Products, Insurance, Retail, Telecom, and Utilities. More detail is below.

Geography distribution—Employers and Employees



Industry distribution



Focus interviews

We conducted several interviews with recruiters from global firms, cybersecurity associations and academics. This helped us to understand and to identify best practices to mitigate the cybersecurity talent gap.

Social media analysis

We analyzed the sentiments of around 8,400 current and former employees at 53 cybersecurity firms on social media. We selected firms that operate primarily in the cybersecurity space covering (but not limited to) data security, cloud security, mobile security, enterprise security, email security, and application security. All these organizations have a workforce of at least 100 employees.

References

1. Forbes, "Securing Your Digital Future: Cyber Trust As Competitive Advantage," May 2017
2. Fast Company, "Chief Security Officer May Be The Job Of The Future That No One Wants," June 2016
3. Ibid.
4. Info Security, "Neurodiversity and Cybersecurity Careers: Recruiting and Retaining Autistic Cybersecurity Professionals," March 2017.
5. Wired, "Autistic People Can Solve Our Cybersecurity Crisis," November 2016.
6. Digit, "Google awards \$112,500 to Android bug hunter for exposing vulnerability affecting Google Pixel smartphones," January 2018
7. Bugcrowd, "2017 State of the Bug Bounty Report," 2017
8. Vulnerability Lab, "Bug Bounties, Rewards and Acknowledgements," January 2018
9. Business Insider, "Debut App Allows Companies to Headhunt Students," May 2017
10. The Next Web, "4 ways gamification is advancing cybersecurity," June 2016
11. Society for Human Resources Management, "The Gamification of Recruitment," November 2015
12. Ibid.
13. Talent Tech Labs, "How These Top Brands Are Using Gamification To Recruit," May 2017
14. SecurityIntelligence, "Closing the Skills Gap: New Tech Test Roots Out Talented Security Recruits," April 2017
15. The Telegraph, "Can you crack the code? GCHQ unveils fiendish puzzle for new recruits," September 2013
16. CSO, "Look Beyond Job Boards to Fill Cybersecurity Roles," July 2017
17. Owen, Nikki. *Charismatic to the Core: A Fresh Approach to Authentic Leadership*. [UK]: SRA Books, 2015.
18. RSA Conference, "An Aflac Case Study: Moving a Security Program from Defense to Offense," February 2017
19. Levie, Aaron(@levie). "Dear kids: If you want a job in 5 years, study computer science. If you want a job forever, study computer security. <https://twitter.com/levie/status/547234465198526464>" December 22, 2014, 7:37 PM. Tweet.
20. Fortune, "Can AT&T Retrain 100,000 People?," March 2017
21. (ISC),² "The Global Information Security Workforce Study," 2015
22. The Guardian, "Why Now's the Time to Embrace Flexible Working," January 2017
23. Betanews, "The 'Age of Automation' Can Benefit the Security Landscape," November 2016
24. The Wall Street Journal, "For Cybersecurity, AI Helps Alleviate Shortage of Human Experts," October 2017
25. MIT Technology Review, "A Lack of Cybersecurity Talent Is Driving Companies to Use AI Against Online Attacks," October 2017

Appendix

1. We included eight soft digital skills in our research as shown below.

Soft Digital Skills	Definition
Change management	Helping an organization transform itself by focusing on organizational effectiveness, improvement, and development
Collaboration	Processes that help multiple people or groups interact and share information to achieve common goals
Comfort with ambiguity	Feeling comfortable and confident to act within an environment of uncertainty or constant change and having higher risk tolerance
Customer-centricity	Committing to a top tier level of service to the customer and considering the customer experience above all
Entrepreneurial mindset	State of mind that orientates human conduct towards entrepreneurial activities and outcomes; drawn to opportunities, innovation, and new value creation and able to take calculated risks and accept the realities of change and uncertainty
Data-driven decision making	Using data and insights to develop a theory, testing the theory in practice to determine its validity, and making business decisions
Organizational dexterity	Flexibility to perform varied roles, actions, or activities with skill and grace and the ability to transition between roles, actions, and activities quickly and effectively
Passion for learning	A deeply ingrained enthusiasm for seeking out and acquiring new information and knowledge, often across a variety of fields and topics

2. We interviewed experts from global recruitment agencies specializing in cybersecurity, cybersecurity associations and academics. Below is the list of experts quoted in the report.

Name	Title	Organization	Category
Jessa Gramenz	Director of Communications	National Cybersecurity Student Association	Cybersecurity association
Jonathan Katz	Professor	University of Maryland	Academic
Kate Shannon	Managing Partner	Heidrick & Struggles	Recruiter
Keyaan Williams	President	Information Systems Security Association (ISSA)	Cybersecurity association
Michel Cukier	Director, Advanced Cybersecurity Experience for Students (ACES)	University of Maryland	Academic
Tuck Rickards	Managing Director	Russell Reynolds	Recruiter

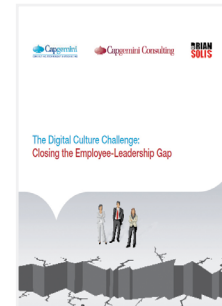
Discover more about our recent research on digital transformation



[The Digital Talent Gap: Are Companies Doing Enough?](#)



[The Digital Talent Gap: Developing Skills for Today's Digital Organizations](#)



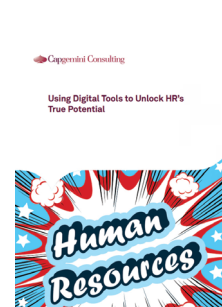
[The Digital Culture Challenge: Closing the Employee-Leadership Gap](#)



[Digital Transformation Review 10: The Digital Culture Journey: All on Board!](#)



[The Currency of Trust: Why Banks and Insurers Must Make Customer Data Safer and More Secure](#)



[Using Digital Tools to Unlock HR's True Potential](#)



[Bring Your Own Device: It's all about Employee Satisfaction and Productivity, not Costs!](#)



[Organising for Digital: Why Digital Dexterity Matters](#)



[Being Digital: Engaging the Organisation to Accelerate Digital Transformation](#)

About the Authors



Jerome Buvat

Global Head of Research and Head,
Capgemini Digital Transformation Institute
jerome.buvat@capgemini.com

Jerome is head of Capgemini's Digital Transformation Institute. He works closely with industry leaders and academics to help organizations understand the nature and impact of digital disruptions.



Mike Turner

Chief Operating Officer,
Capgemini Cybersecurity
mike.a.turner@capgemini.com

Mike is the Chief Operating Officer (COO) of Capgemini's Global Cybersecurity Practice as well as Head of Cybersecurity Services in the UK Region. Prior to this Mike held roles as the Head of Apps UK Cybersecurity and Chief Security Officer for a key account.



Marisa Slatter

Manager, Capgemini Digital Transformation Institute
marisa.slatter@capgemini.com

Marisa is a manager at Capgemini's Digital Transformation Institute. Also a manager within Capgemini Consulting North America, she advises clients on customer experience, brand strategy, digital transformation, and digital talent strategy.



Ramya Krishna Puttur

Senior Consultant,
Capgemini Digital Transformation Institute
ramya.puttur@capgemini.com

Ramya is a senior consultant at Capgemini's Digital Transformation Institute. She is eager to understand the growing role of analytics in posing the right questions that shape and transform the digital boundaries of traditional business consortiums.

The authors would like to thank Surya Prakash Prayaga and Satish Allumallu from Capgemini Consulting and Subrahmanyam KVJ and Amrita Sengupta from Capgemini Digital Transformation Institute for their contributions to this report.

The authors would also like to thank Marjorie Daniel from Capgemini Group Marketing, Anne Gauton from Capgemini Consulting UK, and Jérôme Desbonnet from Capgemini Sogeti Group for their contribution to this research.

The Digital Transformation Institute



The Digital Transformation Institute is Capgemini's in-house think-tank on all things digital. The Institute publishes research on the impact of digital technologies on large traditional businesses. The team draws on the worldwide network of Capgemini experts and works closely with academic and technology partners. The Institute has dedicated research centers in the United Kingdom and India.

dti.in@capgemini.com

For more information, please contact:

Global

Mike Turner

mike.a.turner@capgemini.com

France

Pierre-Luc Refalo

pierre-luc.refalo@sogeti.com

Germany

Claudia Crummenerl

claudia.crummenerl@capgemini.com

Paul Lokuciejewski

paul.lokuciejewski@capgemini.com

Netherlands

Erik Hoorweg

erik.hoorweg@capgemini.com

India

Samir Khare

samir.khare@capgemini.com

Italy

Alessandra Miata

alessandra.miata@capgemini.com

United Kingdom

Andy Powell

andy.powell@capgemini.com

United States

Drew Morefield

drew.morefield@capgemini.com

Spain

Jose Luis Diaz Rivera

jose-luis.diaz-rivera@capgemini.com

Sweden

Klas Rutberg

klas.rutberg@capgemini.com

Capgemini Cybersecurity Services

With 3,000+ cybersecurity experts, Capgemini and Sogeti offer a full range of services that safeguard the digital and cloud platforms, IT infrastructures, and OT systems of companies and administrations worldwide. Our security specialists use the very best technology products tested and proven by our own R&D team specializing in malware analysis and forensics. We have ethical hackers, an international network of multi-client security operation centers (SOCs) and are global leaders in testing. We Advise. We Protect. We Monitor.

Learn more about our services at

www.capgemini.com/cybersecurity-and-risk



About Capgemini

A global leader in consulting, technology services and digital transformation, Capgemini is at the forefront of innovation to address the entire breadth of clients' opportunities in the evolving world of cloud, digital and platforms. Building on its strong 50-year heritage and deep industry-specific expertise, Capgemini enables organizations to realize their business ambitions through an array of services from strategy to operations. Capgemini is driven by the conviction that the business value of technology comes from and through people. It is a multicultural company of 200,000 team members in over 40 countries. The Group reported 2017 global revenues of EUR 12.8 billion.

Visit us at

www.capgemini.com

People matter, results count.

The information contained in this document is proprietary. ©2018 Capgemini.
All rights reserved.