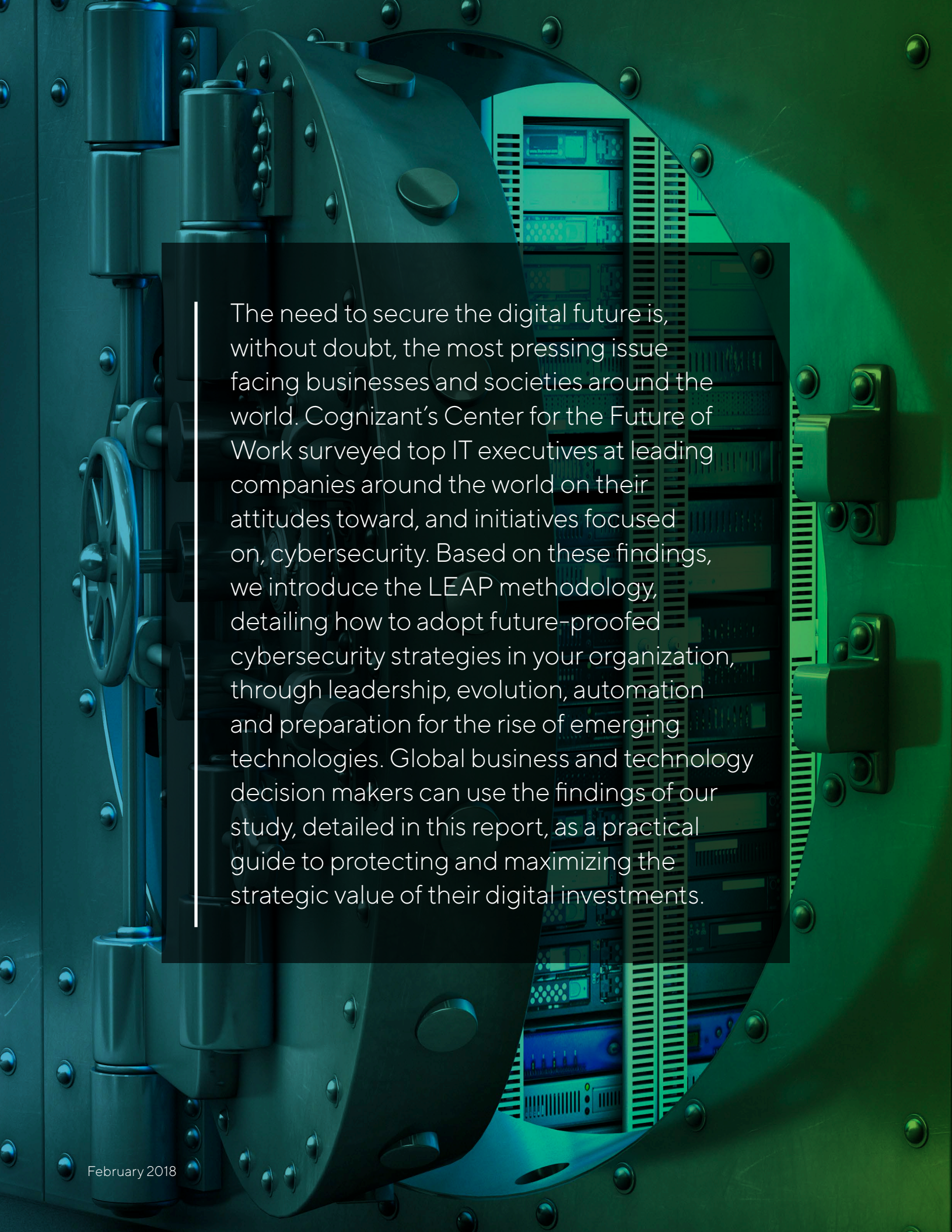


SECURING THE DIGITAL FUTURE

In their pursuit of a digital approach to business, organizations are opening themselves up to greater cybersecurity risks – and yet few have elevated security to a senior leadership concern, according to our recent research. Here's what businesses are thinking about cybersecurity, and how they can strengthen their strategies to minimize the revenue and reputational losses of a breach.

By Michael M. Cook





The need to secure the digital future is, without doubt, the most pressing issue facing businesses and societies around the world. Cognizant's Center for the Future of Work surveyed top IT executives at leading companies around the world on their attitudes toward, and initiatives focused on, cybersecurity. Based on these findings, we introduce the LEAP methodology, detailing how to adopt future-proofed cybersecurity strategies in your organization, through leadership, evolution, automation and preparation for the rise of emerging technologies. Global business and technology decision makers can use the findings of our study, detailed in this report, as a practical guide to protecting and maximizing the strategic value of their digital investments.

Executive Summary

As organizations reimagine their future through a digital lens, they are adopting new technologies at greater scale and with greater speed. Technologies such as intelligent automation, big data analytics and cloud computing are combining to create the “new machine,” with the potential to supercharge revenues and significantly reduce costs.

In the race against, and with, the machine,¹ however, there is one critical factor that is all too frequently overlooked: security. In fact, security has never been more important, due to the broadening of the “surface area” of potential risks, the lack of established security frameworks for new and emerging technologies, and the rapid corporate shift to new digital capabilities.

It’s clear that the information technology in use today is not nearly as secure as it needs to be, given the scale of organizations’ digital build-outs. Even the most blue-chip and deep-pocketed of corporations admit (off the record) that they have been and continue to be targeted – and subsequently compromised. A casual glance at recent events bears this out, from global threats like WannaCry,² to the latest WikiLeaks data dump.³

The bottom line is, if advanced persistent threat actors intend to hack you, they probably can. Our ability to function amid this unfortunate truth stems from our individual and collective hardwired inclination to ignore and deny it. On a personal level, most of us find solace in our perceived protection of “security through obscurity,” while at a collective level, we take comfort in “that’s John’s problem, not mine.”

However, businesses must deal with this issue, and deal with it now, as evident tensions are rising in organizations worldwide. On the one hand, the critical need to become more digital is an all-consuming and vital task, with global digital revenues expected to hit \$604 billion by 2018, as indicated by our recent Work Ahead study.⁴ But in pursuing this, organizations are increasingly opening themselves up to greater risk of security breaches. These threats are not diminishing in frequency either; on the contrary, according to our study, companies endured an average of 40 security incidents in 2016 alone, costing each around \$1.3 million.⁵ Sixty-eight percent of respondents suffered the loss of reputation and brand value as a result of a breach. Respondents see the situation worsening, with 60% saying there are more emerging threats than they can currently control.

But with the increased threat, the discipline of security is still struggling to find its place in organizations, as evidenced by the continued debate of where the role of chief security officer (CSO) fits vis-a-vis the role of the CIO. Then there’s the board, which is now being encouraged by organizations such as the Federal Financial Institutions Examination Council (FFIEC)⁶ and the National Association of Corporate Directors (NACD)⁷ to take a much more active role in security governance. The position of board involvement and accountability can no longer remain an unanswered question.


The need to secure the digital future is, without doubt, the most pressing issue facing businesses and societies around the world. Progress toward the “Fourth Industrial Revolution”⁸ rests on it. It’s one thing to see your Twitter account hacked and quite another entirely to witness the hacking of your smart car or home. The infamous Jeep experiment⁹ of 2015, in which researchers successfully took control of a vehicle using the car’s internal computer network, is a pointed example of how this could happen in the real world.

To equip organizations to deal with this existential number one priority, Cognizant's Center for the Future of Work surveyed top IT executives at leading companies around the world on their attitudes toward, and initiatives focused on, cybersecurity (see Methodology and Demographics, page 23). Our study revealed the following key insights:

- **Security needs to move out of the back office and into the C-suite.** Only 9% of respondents said their organization is making cybersecurity a board-level priority. Leadership needs to embrace cybersecurity as a board-level initiative and not just relegate it to IT.
- **Cybersecurity threats remain clouded.** Cloud migration is seen as the most vulnerable digital trend for organizations. Prioritizing security controls and resilient architectures around this migration is fundamental to achieving digital success.
- **Talent will remain key, but AI will close the gap.** Sourcing adequately trained cybersecurity talent is a major concern today, and artificial intelligence (AI) is set to mitigate this to a certain extent.
- **The battle for cybersecurity is an endless war.** Threats are never consistent in the cyber realm; thus, neither is cybersecurity. Organizations will need to update, evolve and reimagine strategies and execution in order to remain secure.
- **The next generation of security-related technology is emerging:** The massive leap in processing power and the potential security benefits that new technologies such as blockchain, quantum computing, advanced analytics, DevSecOp models and software-defined infrastructures are core considerations for organizations today. The need to quickly adapt and evolve security practices will be vital for organizations moving forward.

Based on these findings, we introduce the LEAP methodology, detailing how to adopt future-proofed cybersecurity strategies in your organization, through leadership, evolution, automation and preparation for the rise of emerging technologies.

Global business and technology decision makers can use the findings of our study, detailed in this report, as a practical guide to protecting and maximizing the strategic value of their digital investments.

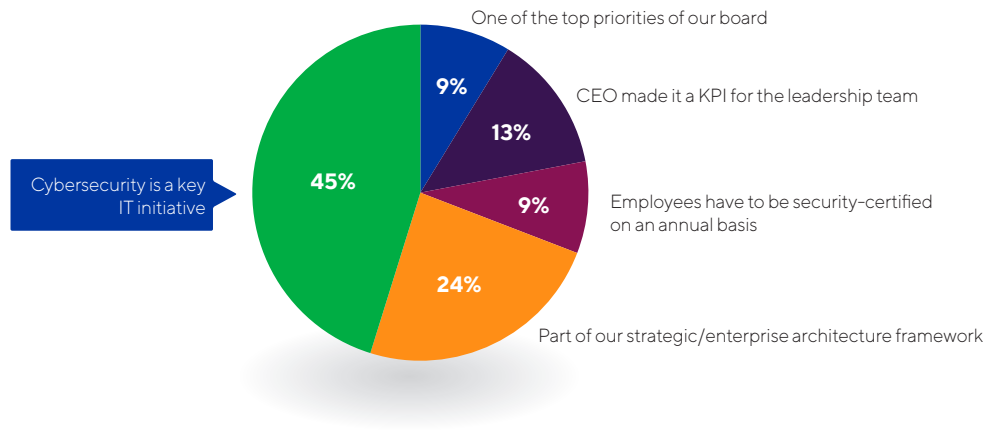


But with the increased threat, the discipline of security is still struggling to find its place in organizations, as evidenced by the continued debate of where the role of chief security officer fits vis-a-vis the role of the CIO. Then there's the board, which is now being encouraged by organizations such as the FFIEC and the NACD to take a much more active role in security governance. The position of board involvement and accountability can no longer remain an unanswered question.

MOVING SECURITY INTO THE C-SUITE

Cybersecurity's Execution Shortcomings

Which of the following statements best describes how critical cybersecurity is for your organization?



Response base: 1,018 senior IT executives
Source: Cognizant Center for the Future of Work
Figure 1

In 2012, then FBI Director Robert Mueller observed: “There are only two types of companies: those that have been hacked, and those that will be.”¹⁰ A glance at the headlines over the intervening six years bears out that statement. With the average cost of a security incident hovering around \$1.3 million,¹¹ hacking isn’t a matter to be taken lightly. But why, then, do business leaders appear to be keeping their heads in the proverbial sand and not tackling the issue of cybersecurity in the boardroom?

From our studies, we’re seeing a significant contradiction in business leaders’ views toward cybersecurity. When asked which technologies were having the greatest impact on their business today, 96% of respondents in our Work Ahead study named cybersecurity, and 99% cited cybersecurity when looking out to 2025. At the same time, only 9% of respondents in our current study said their organization made cybersecurity a board-level priority; moreover, the largest proportion (45%) is keeping it as a purely IT initiative (see Quick Take, page 8, explaining why this is a concern). This perceived contradiction presents a worrying indication of the attitude organizations have toward cybersecurity (see Figure 1).

A recent study by Harvard Business School¹² provides insight into why this is the case. Typically, most corporate boards lack the processes and expertise required to adequately deal with, evaluate and remediate cyber threats. They suffer from:

- **Inadequate process:** The majority of boards are well equipped to deal with financial planning, compliance and growth strategy. Cybersecurity, on the other hand, is lower down in the pecking order. According to the study, directors ranked the effectiveness of their cybersecurity-related processes dead last out of 23 processes surveyed.

Quick Take

The Downside of Entrusting IT with Cybersecurity

Given the ever-rising technological intensity of business, decision makers could easily conclude that cybersecurity should be the preserve of the IT department. It would, therefore, follow that boards should simply provide the budget and sponsorship needed. But how well-equipped is IT to cope with, and integrate, security measures in its core infrastructure? Not very well, as it turns out.

In our study, an alarming 58% of respondents stated that their IT infrastructure and IT security strategies were not integrated. Given that these two should go hand-in-hand, this is a noteworthy result. Boards, therefore, need to address these two areas and double down on cybersecurity processes by procuring adequate expertise. Board involvement in ensuring IT and cybersecurity integration needs to be step one for organizations in their efforts to build appropriate cyber defenses.

In addition to upskilling board members, organizations also need to prioritize an executive-sponsored security objective. In one large organization,¹⁴ the CEO highlighted the issue of cybersecurity by getting involved directly with senior security executives in making decisions, while other organizations have placed divisional chief information security officers (CISO) in business units, pairing them with senior executives in these roles. By making cybersecurity a core value proposition of the organization, it becomes a key component of all board-level decision making and, therefore, automatically filters into other board objectives. For companies that do this, cybersecurity will become a business opportunity¹⁵ by creating end-to-end customer experiences that are both convenient and secure.

- **Lack of expertise:** The reason boards do not make cybersecurity a priority and instill processes around the issue comes down to a lack of expertise, which is directly related to the increased complexity in the industry, subject matter, attack vectors and types of adversaries. A large proportion of boards at companies in the Financial Times Stock Exchange (FTSE) 100, for example, consist of financially trained members¹³ who are not skilled in dealing with and installing cybersecurity processes.

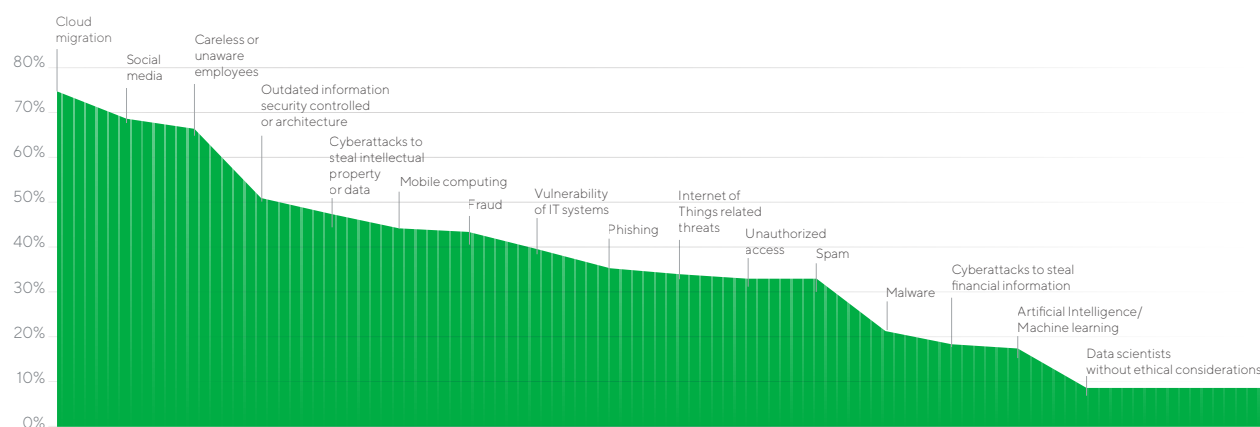
Boards of directors must step forward to take a full leadership position on cybersecurity; this will require them to more fully immerse themselves in the business and technology issues at stake.

Boards of directors, therefore, must step forward to take a full leadership position on cybersecurity; this will require board members to more fully immerse themselves in the business and technology issues at stake to ask tougher questions of senior executive leadership teams. Equifax's \$4 billion loss¹⁶ of market capitalization in the aftermath of its recent breach should be all the evidence needed for board members to realize that their fiduciary responsibility very much includes ensuring that every possible step – and then some – is taken to maintain a best-in-class security posture.

CYBERSECURITY THREATS REMAIN CLOUDED

Key Cyber Soft Spots

Which threats and vulnerabilities will increase your risk exposure over the next 12 months?



Response base: 1,018 senior IT executives
Source: Cognizant Center for the Future of Work
Figure 2

Cybersecurity vulnerabilities stem from a range of sources, including not only technology itself, but also the design and execution of business processes and, most importantly, from employees within the organization. Figure 2 portrays respondents' views on three critical areas and processes that need to be addressed now to bolster security: cloud migration, social media and careless/unaware employees.

Cloud Migration

In our study, leaders perceived the most significant cybersecurity threat to be the process of migrating information to the cloud. This reality stems from the fact that cloud migration is now a core component of many organizations' digital strategies. Organizations are now moving en masse away from legacy on-premise systems to infrastructure-, platform- and software-as-a-service-based models; in doing so, however, they are struggling with cloud-related expertise and the inherent risks of this migration process.

While experts have viewed security for many years as a weakness of a "cloud-first" IT strategy, there is a common agreement now that the cloud is ready for prime-time, with the major cloud providers offering state-of-the-art native and third-party ecosystem security controls. However, many organizations mistakenly assume that their providers will entirely take care of security-related issues in the migration process despite the fact that the cloud providers position security as a shared responsibility between the client and the provider. As our study shows, assuming this provider accountability is not a tenable position. The onus is still on the organization to embed the proper security controls into the migration process.

In our study, 68% of respondents agreed they could be doing more when it comes to cloud security. Moreover, we have found that this lack of attention, as well as the perceived increased security threats because of cloud migration, is slowing down the pace of adoption.

Cloud application fragmentation is another major security concern, especially when dealing with cross-enterprise ecosystems. Business and IT leaders should realize that while their cloud application and infrastructure partners are indeed highly focused on ensuring their offerings are secure, cloud providers take a different approach. Unless contractually obliged (an obligation for which very few cloud server providers will sign up), they are not focused on ensuring the integrity of an entire solution or busi-

ness process, of which the cloud provider's technology is but one part. This false assumption, according to IDC,¹⁷ is typically where cloud-related security breaches originate, and is a matter for which buyers (ultimately the final "system integrator") must continue to be responsible.

Business and IT leaders must take a holistic end-to-end view to understand each step in the digital transaction, the threats and the in-place security controls, as well as the responsibility for security at each level of the IT stack. The migration of data to the cloud solves many problems, but introduces others.

For example, the pace of technology change within cloud environments is accelerating as these technologies enable frictionless access to data, increase interoperability and provide mobile access. Rapid innovation is a business advantage, but it can also result in neglected or inadequate security controls if security innovation does not keep pace with cloud innovation.

Closing Cloud Security Gaps

A cornerstone of any sturdy cybersecurity defense program is to first identify weak areas and then plug the holes; for cloud migration in particular, it's vital that those spearheading this migration first understand the risks and threats to data that arise through the transition. From this point, organizations can then act accordingly from a security perspective. Encrypting information can protect from unauthorized disclosure, but as a web-based service, cloud systems must also be on guard against denial of service attacks. Eliminate choke points and heed the lesson of Chinese military strategist and philosopher Sun Tzu to "know your enemy."¹⁸

More often than not, securing cloud-based data entails not simply building a wall around the data but also securing the data itself through access controls, digital rights management and encryption.

More often than not, securing cloud-based data entails not simply building a wall around the data but also securing the data itself through access controls, digital rights management and encryption. Looking to the future, access control architectures are evolving to include risk-based models. No longer will organizations rely just on authentication to grant access, but user and asset posture will also be considered. Access to data and systems can also be granular, such as providing read-only access or access to only a certain class of systems or documents, depending on the perceived risk. Rather than relying just on user passwords, organizations are also turning to biometric authentication, device proximity and N-factor authentication methods to reduce unauthorized access. Encryption needs to be utilized wherever the data is stored and also as it is transmitted. In addition, providing contextualized device security through situational-based public key infrastructure (PKI) will further bolster internal security measures.

Social Media

With social platforms becoming more crucial to business strategies, the number of cyber risk “entry points” into the enterprise has increased well beyond traditional attack vectors such as e-mail. The threats posed by phishing attacks and other illegitimate access through Twitter, LinkedIn, Facebook, Instagram, Snapchat and other social media platforms are a continually pervasive problem, particularly with the fast-evolving sophistication of attacks.

Previously, hackers would enter an enterprise through the inadvertent exposure of a user’s credentials. Today, however, hackers are using workarounds and phishing techniques to gain access. Famously, it took only one attempt by a Russian hacker to gain access to a Pentagon official’s laptop,¹⁹ in something as innocuous as a link to a package holiday on Twitter. While staff training on e-mail and website security are commonplace, few organizations have extended security training to social media platforms.

While learning to tweet doesn’t require a training manual, learning to tweet responsibly and effectively without falling prey to its downsides, does. If your organization does not provide this type of training to everyone from the newest entry-level recruit to the CEO (who is probably increasingly active on social media after trying to hold out for years), it should take action on this today.

While learning to tweet doesn’t require a training manual, learning to tweet responsibly and effectively without falling prey to its downsides, does. If your organization does not provide this type of training to everyone from the newest entry-level recruit to the CEO (who is probably increasingly active on social media after trying to hold out for years), it should take action on this today.

Protecting Against Employee Threats

For the majority of cyber attacks, hackers need organizations to “open the door” before they can wreak havoc. According to a 2016 *Harvard Business Review* study,²⁰ 60% of cyber attacks involved insiders, including malicious and inadvertent participants. Therefore, a fundamental component of any cybersecurity policy is staff training and staff monitoring. Before instituting these policies, it’s important to understand the types of insider risks:

- Employees can and will make mistakes as part of their day-to-day role and function. Many data exposures are not due to malicious intent but rather well-intentioned employees making unwise decisions.
- Administrators and privileged users are frequently targeted due to their elevated access and permissions. Yes, people do leak passwords.
- E-mail and social engineering are the most common attack vectors on employees.

TALENT WILL
REMAIN KEY,
BUT AI WILL
CLOSE THE GAP

Although a wave of cybersecurity-related technology innovation is emerging (see Quick Take, page 18), human workers are still the ultimate masterminds behind any cybersecurity defense.²¹ Unfortunately, there is a significant global shortfall of cybersecurity talent.²² As Aaron Levie, CEO of the cloud storage company Box, recently said, “if you want a job for the next five years, get a job in IT; if you want a job for life, study computer security.”²³ According to research conducted by the ISACA,²⁴ a nonprofit information security advocacy group, cybersecurity jobs growth is expanding at three times the rate of overall IT jobs, and by 2019, there will still be a global shortage of two million cybersecurity positions. In March 2017, ISACA says, 53% of organizations were experiencing up to six-month delays in filling open cybersecurity positions.

In our study, respondents saw cyber threats increasing in volume and severity over the next 12 months, and over 60% of respondents believe they have inadequate resources (namely talent) to address these concerns. Budgets are another issue; a recent study by HfS Research²⁵ found that in medium- to large-sized enterprises, a leading internal inhibitor to cybersecurity was a lack of staffing budget.

While not a silver bullet, the introduction of AI tools into cybersecurity platforms will spur organizations to rethink how they approach cybersecurity.

Combined with fast-changing threat vectors, this talent and budget shortage has many looking to AI-driven automation to improve the cybersecurity outlook. In a recent CFoW podcast,²⁶ NelsonHall industry analyst Mike Smart provided pragmatic guidance on how industry participants can use AI in cyber defense during the coming years:

“Using artificial intelligence-based cybersecurity platforms can be used to automate some very time-intensive processes that cybersecurity professionals currently perform. Using platforms with embedded AI, the time to do the grunt work to identify threats reduces analysis from 60 minutes to three minutes, a 20-times reduction! That is obviously going to work wonders to help address the volume side of the skills gap.”

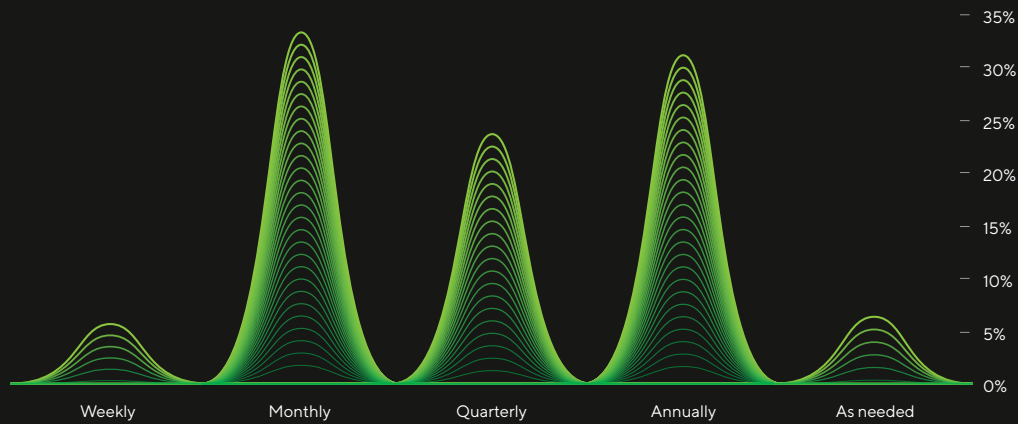
While not a silver bullet, the introduction of AI tools into cybersecurity platforms will spur organizations to rethink how they approach cybersecurity. AI tools can help businesses more quickly analyze growing volumes of data, increase the signal-to-noise ratio for security analysts, provide contextual enrichment for quicker decision making, and reduce the mundane technical work that can lead to security analyst burnout.

AI won't completely mitigate the shortage of talent, but it will lessen the burden. Also, the enhancement of level-one contact (a.k.a., tier one) analysts will enable further analysis in other areas, thereby increasing the effectiveness of security operations.

AN ENDLESS WAR

Catching Up with Cybersecurity Threats

How often are you finding it necessary to refresh your organization's information security strategy?



Response base: 1,018 senior IT executives
Source: Cognizant Center for the Future of Work
Figure 3

Because security is an ever-changing dynamic of resources, threats and solutions, it's not enough for organizations to refresh their cybersecurity strategy annually; most organizations, in fact, are now reviewing and updating these strategies on a quarterly or even monthly basis (see Figure 3).

The reason for this is threefold:

- **New technologies:** Technologies such as Internet of Things (IoT), mobile applications, cloud computing and machine learning are reshaping the way we work and the work we do, as well as how organizations recognize value in the years to come. At the same time, these technologies also pose new entry points for hackers, such as new logical vulnerabilities.
- **New data:** As organizations develop new technologies and add intelligent sensors to more of the goods they produce, vast new streams of data are being generated, and this will only increase moving forward. However, with this data onslaught comes new and changing risks. Vast unstructured data sets are ready and waiting to be infiltrated. Data exfiltration is an area that should be given continuous attention by organizations; data stewardship, the requirement to responsibly handle data, will become a significant construct in data security. The imminent arrival of the General Data Protection Regulation (GDPR) in the EU, as well as New York's Personal Privacy Protection Law, the Chinese Cybersecurity Law and Russia's Privacy, Data Protection and Cybersecurity Law, are all the start of state-led regulation in regard to stewardship, and could provide the tipping point for other countries to follow suit.
- **Sophisticated adversaries:** Like technology itself, cybersecurity threats are fast evolving. And with the money at stake,²⁷ new and increasingly sophisticated hackers are coming onto the scene. A frightening example of this was the recent penetration of U.S. energy company systems that could be manipulated to sabotage the U.S. power grid.²⁸

Ultimately, cybersecurity needs to be an ongoing endeavor in every organization. Failure to adapt processes and systems on a regular basis will leave an organization open to further attacks. Hackathons, war rooms and threat modeling must become part of every business's corporate dialect.

Quick Take

The Next Generation of Security-Related Technology

In our Work AHEAD framework,²⁹ we advocated for using digital technologies and approaches to discover and invent new markets, products and processes to succeed in the Fourth Industrial Revolution. Likewise, R&D, innovation and blue-sky thinking are crucial to remaining one step ahead of potential cybersecurity threats. In this vein, blockchain and quantum computing, in years to come, are just two of the new technologies that will upend the cybersecurity protocols of many organizations.

The exponential jump in processing power³⁰ that quantum computing will usher in will make current encryption methods, such as PKI, obsolete. This type of cryptography is arguably secure against computing power available today, but with quantum computing, which can use quantum bits³¹ to calculate at an exponentially faster rate than binary-processing computers today, this type of encryption suddenly accounts for very little.³² Therefore, any hacker armed with this technology would be able to wreak havoc on both national and organizational security with impunity.

However, with quantum computing, the opportunity to develop new encryption methods becomes a reality, and with the early-stage prohibitive cost of these machines (estimated at \$15 million³³), it's more than likely that organizations will have them before hackers.

Although the likelihood of seeing a quantum computer in your server room is a long way off (with the standard consensus being around 2040), businesses such as Microsoft,³⁴ D-Wave,³⁵ IBM³⁶ and Google³⁷ are investing heavily in this technology today, with the goal of overcoming substantial challenges to making it work practically.

Closer on the horizon, blockchain technology is set to reinforce organizations' defenses significantly, particularly with the technology's capabilities in the areas

of transparency and immutability. For example, traditional methods of software integrity verification using checksums can be replaced with blockchain to establish an entire genealogy of every change to a software download, patch, firmware, installer, etc. Because of this capability, integrity attacks such as certificate stealing will be ineffective.

Utilizing a decentralized ledger, peer-to-peer transactions on a blockchain network no longer require dependency on a trusted third-party. Existing systems can be made faster and more resilient by moving from one or two centralized methods of attestation to N-number of factors distributed across many nodes.

For example, blockchain has the potential to remove one of the most fragile of hacker targets: passwords. Today, companies such as Guardtime³⁸ and REMME³⁹ are using blockchain to create a keyless signature infrastructure – entirely removing passwords and, therefore, PKI – by harnessing decentralized systems on the blockchain. In theory, the use of blockchain will mitigate the threat posed by quantum systems in years to come and, in the medium term, will significantly bolster organizational and personal security.

We see take-up of blockchain-enabled cybersecurity today. For example, Ukroporoprom, Ukraine’s umbrella association for its defense industry, has established a strategic partnership with REMME to enable secure, password-free access to its employees.⁴⁰

Blockchain is set to rewrite the rules of current security protocols by supplementing weaknesses in human behavior that frequently result in security incidents. By leveraging distributed ledgers, and eliminating the risk of single points of failure, as is currently the case with password access, blockchain has the potential to provide holistic security and encryption while maintaining convenience for users.

(To learn more, read our e-book, “[Demystifying Blockchain](#).”⁴¹)

EXPLORING THE LEAP METHODOLOGY

Cybersecurity is a multidimensional, complex problem facing organizations today. From our study, four critical elements have emerged that organizations can follow to bolster their cybersecurity strategies, allowing them to future-proof digital operations. We call this our LEAP methodology.

L**ead:** Cybersecurity needs to be a fundamental concern of every employee, but ultimately this directive needs to come from the top. This top-down approach doesn't just entail sponsoring cybersecurity initiatives; instead leaders need to understand the technology and the processes behind cybersecurity for it to become a vital component of every strategic decision made.

As referenced earlier, practical ways of doing this include placing divisional CISOs in business units and pairing them with senior executives in these roles. Also, making cybersecurity a core value proposition of marketing outreach has proved to be an effective way of integrating cybersecurity into the DNA of the organization.

Finally, leadership needs to double down on cybersecurity processes by themselves becoming "armchair experts" on the subject. Once boards understand the finer detail, this knowledge can then be used to influence processes throughout the organizational value chain, making it a fundamental component.

E**volve:** Some organizations require a kickstart to begin their cybersecurity journey. As a practical example, a CEO- or COO-issued directive, followed by a business unit-led initiative to focus on "security for and by everyone" style campaign, would appropriately demonstrate the need for a shift. Once this initial phase has occurred, complacency cannot take hold. Organizations will need to continually evolve their cybersecurity strategies as they will never entirely win the race against cyber threats. Furthermore, R&D needs to be an integral part of the organization's security divisions. R&D doesn't need to be confined to an in-house endeavor; making use of new business practices like hackathons and war-rooming are practical ways to bring in external talent and co-create security initiatives.

To effectively implement these measures, organizations need to enable agile execution of their core strategies. It's no good identifying areas for improvement or detecting new threats promptly if your organization is unequipped to make the changes happen in a short enough timeframe. Consider how security change management teams or consultants could expedite this process.

A**utomate:** With crippling global cybersecurity talent shortages and an increased scale and variety of cyber threats, AI-based approaches are progressively becoming readily available and should become a part of any organization's larger cybersecurity execution strategy. Businessness should work quickly to make AI-based tools, such as Darktrace⁴² and Deep Instinct,⁴³ work in their security departments. Rote, repetitive work is being automated in the front, middle and back offices of organizations, and cybersecurity should be no different.

While automation won't solve your security talent requirements completely, it will mitigate select shortages in the junior- to mid-level analysis roles, as we discuss below. More importantly, the benefits of intelligent automation extend beyond simple labor shortages. With intelligent automation's ability to calculate and contextually analyze massive volumes of data, it's becoming a "no-brainer" to use this approach given the type of analysis cybersecurity work entails. AI has the potential to drastically enhance the effectiveness and reach of cyber analysis in this regard. Of course, it's essential to keep in mind that for cybersecurity initiatives to be successful, people, processes and technology need to work as one.

P**repare:** Prepare for the new technologies that will entirely shift the current dynamic of the cybersecurity strategy, including blockchain and – further out on the horizon – quantum computing. Although the ability to quickly adapt to current security needs is vitally important, it's fundamental to keep an eye on the future. Just as the Internet changed our lives, so will blockchain and quantum computing change cybersecurity.

A FINAL WORD

Organizations around the world are reaching a tipping point: New digital technologies and approaches promise a new era of productivity, growth and economic expansion; however, these outcomes rely on countering the rising tide of cyber threats, the scales of which are already significant and are poised to grow exponentially.

To avoid the resulting loss of customers, reputation and revenue, any company that hopes to do business in the digital economy must strengthen its cyber defenses to remain viable.

On the one hand, companies face the genuine threat of irrelevance if they fail to embrace digital technologies, but it's these very technologies that are opening the doors to would-be cyber criminals. To avoid the resulting loss of customers, reputation and revenue, any company that hopes to do business in the digital economy must strengthen its cyber defenses to remain viable. Such a shift is possible for businesses that center their efforts around strong leadership, continuous evolution, AI-driven automation and a plan for embracing the capabilities emerging in the near- and long-term future.

Methodology and Demographics

We conducted a worldwide telephone-based survey in May and June 2017, with 1,018 senior IT executives across industries. The survey was run in 18 countries in English, Arabic, French, German, Japanese and Chinese. Survey respondents were distributed across the financial services, healthcare, insurance, life sciences, manufacturing and retail industries. We interviewed companies with a minimum of 2,000 employees for this research.

Endnotes

- ¹ A phrase made famous by Erik Brynjolfsson and Andrew McAfee in their seminal book, *Race Against the Machine*, Digital Frontier Press, 2011, <https://www.amazon.co.uk/Race-Against-Machine-Accelerating-Productivity-ebook/dp/B005WTR4Z1>.
- ² Josh Fruhlinger, "What Is WannaCry Ransomware, How Does it Infect, and Who Was Responsible?" CSO, Sept. 27, 2017, <https://www.csoonline.com/article/3227906/ransomware/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html>.
- ³ WikiLeaks is a multinational media organization headed by Julian Assange that specializes in analysis and publication of large datasets of censored or otherwise restricted data. WikiLeaks website: <https://wikileaks.org/>.
- ⁴ "The Work Ahead: Mastering the Digital Economy," Cognizant Technology Solutions, 2016, <https://www.cognizant.com/white-papers/the-work-ahead-mastering-the-digital-economy-codex2115.pdf>.
- ⁵ "Cyber Attacks Cost U.S. Enterprises \$1.3 Million on Average in 2017," CSO, Sept. 20, 2017, <https://www.csoonline.com/article/3227065/security/cyber-attacks-cost-us-enterprises-13-million-on-average-in-2017.html>.
- ⁶ Greg Reber, "Corporate Board Responsibility – The Cybersecurity Buck Stops Here," *Infosecurity Magazine*, Feb. 2, 2017, <https://www.infosecurity-magazine.com/opinions/corporate-board-responsibility/>.
- ⁷ "Resource Center: Cyber Risk Oversight," National Association of Corporate Directors, <https://www.nacdonline.org/Resources/BoardResource.cfm?ItemNumber=20789>.
- ⁸ Klaus Schwab, "The Fourth Industrial Revolution: What It Means, How to Respond," World Economic Forum, Jan. 14, 2016, <https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/>.
- ⁹ Andy Greenberg, "Hackers Remotely Kill a Jeep on the Highway – With Me In It," *Wired*, July 21, 2015, <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>.
- ¹⁰ "28 Cybersecurity Quotes for a Safe and Secure Cyberspace," EnkiQuotes, <https://www.enkiquotes.com/cyber-security-quotes.html>.
- ¹¹ "Cyber Attacks Cost U.S. Enterprises \$1.3 Million on Average in 2017," CSO, Sept. 20, 2017, <https://www.csoonline.com/article/3227065/security/cyber-attacks-cost-us-enterprises-13-million-on-average-in-2017.html>.
- ¹² J. Yo-Jud Cheng and Boris Groyberg, "Why Boards Aren't Dealing with Cyber Threats," *Harvard Business Review*, Feb. 22, 2017, <https://hbr.org/2017/02/why-boards-arent-dealing-with-cyberthreats>.
- ¹³ Rebecca Smith, "What Do You Need to Be CEO of a FTSE 100 Company?" *Real Business*, May 19, 2015, <http://realbusiness.co.uk/hr-and-management/2015/05/19/what-do-you-need-to-be-ceo-of-a-ftse-100-company/>.
- ¹⁴ James Kaplan, Shantnu Sharma and Allen Weinberg, "Meeting the Cybersecurity Challenge," McKinsey & Co., June 2011, <http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/meeting-the-Cybersecurity-challenge>.
- ¹⁵ Ibid.
- ¹⁶ Paul J. Lim, "Equifax's Massive Data Breach Has Cost the Company \$4 Billion So Far," *Money*, Sept. 12, 2017, <http://time.com/money/4936732/equifax-massive-data-breach-has-cost-the-company-4-billion-so-far/>.
- ¹⁷ Christian Kirsch, "IDC Says 70% of Successful Breaches Originate on the Endpoint," Rapid7 blog, March 31, 2016, <https://blog.rapid7.com/2016/03/31/idc-says-70-of-successful-breaches-originate-on-the-endpoint/>.
- ¹⁸ "If you know the enemy and know yourself, you need not fear the result of 100 battles." Sun Tzu, *The Art of War*.
- ¹⁹ Sheera Frenkel, "Hackers Hide Cyberattacks in Social Media Posts," *The New York Times*, May 28, 2017, <https://www.nytimes.com/2017/05/28/technology/hackers-hide-cyberattacks-in-social-media-posts.html>.
- ²⁰ Marc van Zadelhoff, "The Biggest Cybersecurity Threats Are Inside Your Company," *Harvard Business Review*, Sept. 19, 2016, <https://hbr.org/2016/09/the-biggest-Cybersecurity-threats-are-inside-your-company>.
- ²¹ "Is HR the Missing Link in Your Cyber Security Strategy?" Hfs Research, Oct. 28, 2016, <https://www.hfsresearch.com/point-sofview/is-hr-the-missing-link-in-your-cyber-security-strategy>.

- ²² Kasey Panetta, "Confront the Cybersecurity Talent Shortage," Gartner, June 23, 2017, <https://www.gartner.com/smarterwith-gartner/solve-the-cybersecurity-talent-shortage/>.
- ²³ From an Aaron Levie tweet: <https://twitter.com/levie/status/547234465198526464?lang=en>.
- ²⁴ "2016 Cybersecurity Skills Gap," ISACA, <https://image-store.slidesharecdn.com/be4eaf1a-eea6-4b97-b36e-b62dfc8dc-bae-original.jpeg>.
- ²⁵ "Is HR the Missing Link in Your Cybersecurity Strategy?" HfS Research, Oct. 28, 2016, <https://www.hfsresearch.com/point-of-view/is-hr-the-missing-link-in-your-cyber-security-strategy>.
- ²⁶ "Digital Trust Reimagined in the Porous Digital World," Cognizant Center for the Future of Work podcast, Aug. 24, 2017, <http://www.futureofwork.com/article/details/cfow-podcast-episode-3-digital-trust-reimagined-in-the-porous-digital-world>.
- ²⁷ Cale Guthrie Weissman, "Some Hackers Make More than \$80,000 a Month, and Here's How," Business Insider, July 14, 2015, <http://uk.businessinsider.com/we-found-out-how-much-money-hackers-actually-make-2015-7>.
- ²⁸ Steven Melendez, "More Details Are Emerging About the Sophisticated Hackers Who Penetrated U.S. Power Grid Systems," *Fast Company*, <https://www.fastcompany.com/40464477/more-details-emerging-about-the-sophisticated-hackers-who-penetrated-u-s-power-grid-systems>.
- ²⁹ "The Work Ahead: Mastering the Digital Economy," Cognizant Technology Solutions, 2016, <https://www.cognizant.com/white-papers/the-work-ahead-mastering-the-digital-economy-codex2115.pdf>.
- ³⁰ Nicole Kobie, "The Quantum Clock Is Ticking on Encryption – and Your Data Is Under Threat," *Wired*, Oct. 4, 2016, <http://www.wired.co.uk/article/quantum-computers-quantum-security-encryption>.
- ³¹ Quantum bits definition from Futurism: <https://futurism.com/glossary/quantum-bits/>.
- ³² Paul Edlund, "What Is the Future of Cybersecurity?" YouTube, March 30, 2016, <https://www.youtube.com/watch?v=Y3fYUL-VIZRO>.
- ³³ Chaim Gartenberg, "D-Wave Is Now Shipping its New \$15 Million, 10-Foot Tall Quantum Computer," *The Verge*, Jan. 25, 2017, <https://www.theverge.com/circuitbreaker/2017/1/25/14390182/d-wave-q2000-quantum-computer-price-release-date>.
- ³⁴ "The Microsoft Journey into Quantum Computing," Microsoft Corp., <https://stationq.microsoft.com/>.
- ³⁵ Temporal Defense System website: <http://temporaldefense.com/>.
- ³⁶ IBM Q website, <https://www.research.ibm.com/ibm-q/>.
- ³⁷ Karla Lant, "Google Just Revealed How They'll Build Quantum Computers," *Futurism*, Oct. 6, 2017, <https://futurism.com/google-just-revealed-how-theyll-build-quantum-computers/>.
- ³⁸ Guardtime is a software security company headquartered in Amsterdam. Website: <https://guardtime.com/>.
- ³⁹ REMME is based in San Marcos, Texas, and provides password-free approaches to protecting against cyber attacks. Website: <https://remme.io/>.
- ⁴⁰ Omri Barzilay, "Three Ways Blockchain Is Revolutionizing Cybersecurity," *Forbes*, Aug. 21, 2017, <https://www.forbes.com/sites/omribarzilay/2017/08/21/3-ways-blockchain-is-revolutionizing-cybersecurity/#4e21f6792334>.
- ⁴¹ "Demystifying Blockchain," Cognizant Technology Solutions, 2017, <https://www.cognizant.com/whitepapers/demystifying-blockchain-codex2199.pdf>.
- ⁴² Darktrace is a global machine learning company for cyberdefense, headquartered in Cambridge, UK, and San Francisco. Website: <https://www.darktrace.com/>.
- ⁴³ Deep Instinct is a cybersecurity start-up in San Francisco. Website: <https://www.deepinstinct.com/>.

About the Author



Michael Cook
Senior Manager, Cognizant's
Center for the Future of Work,
EMEA

Michael Cook is a Senior Manager in Cognizant's Center for the Future of Work in EMEA. In this role, Mike identifies the changing dynamics that will shape the business ecosystem of the future, and delivers original research and analysis of work trends in Europe. Mike also collaborates with a wide range of technology thinkers and academics about what the future of work will look like as digital changes many aspects of our working lives. Mike is an established speaker with broad experience across the services market, including customer experience management, buy-side advisory, talent and workforce solutions, and cybersecurity.

Prior to joining Cognizant, Mike served as Global Research Director with HfS Research, where he worked across multiple research topics and led HfS's buy-side focused research program.

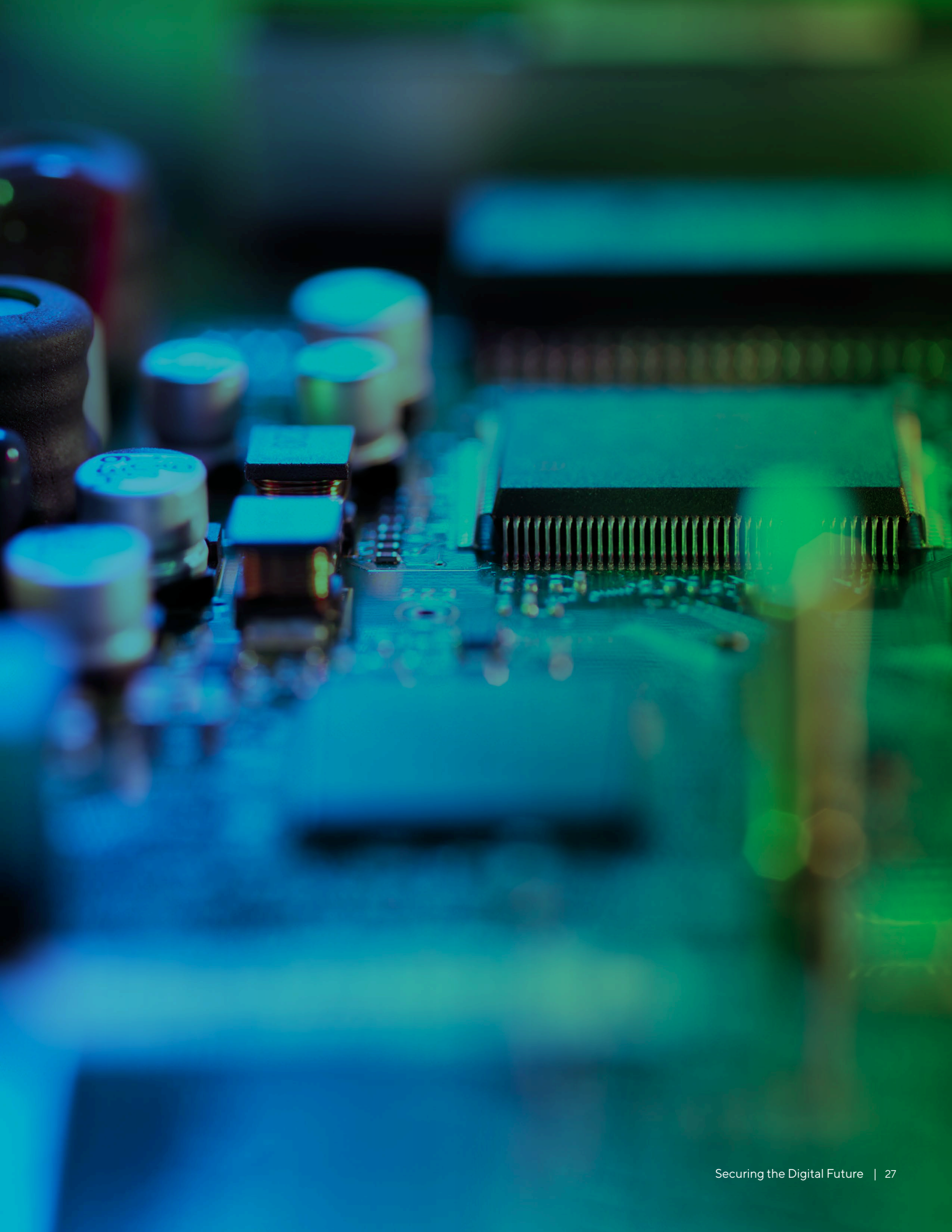
Michael can be reached at Michael.Cook@cognizant.com

Twitter: <https://twitter.com/MikeMarkC>

LinkedIn: <https://www.linkedin.com/in/mike-cook-85550755/>

Acknowledgments

The author would like to thank Daniel Smith, Jacob Rubin, Robert Missak, Matthew Tuttle, Jeffrey Lewis and Tom Le from Cognizant's Security Practice for their thorough review and significant contributions to this white paper.





ABOUT THE CENTER FOR THE FUTURE OF WORK

Cognizant's Center for the Future of Work™ is chartered to examine how work is changing, and will change, in response to the emergence of new technologies, new business practices and new workers. The Center provides original research and analysis of work trends and dynamics, and collaborates with a wide range of business, technology and academic thinkers about what the future of work will look like as technology changes so many aspects of our working lives. For more information, visit Cognizant.com/futureofwork, or contact Ben Pring, Cognizant VP and Managing Director of the Center for the Future of Work, at Benjamin.Pring@cognizant.com.

Cognizant

Cognizant (Nasdaq-100: CTSI) is one of the world's leading professional services companies, transforming clients' business, operating and technology models for the digital era. Our unique industry-based, consultative approach helps clients envision, build and run more innovative and efficient businesses. Headquartered in the U.S., Cognizant is ranked 195 on the Fortune 500 and is consistently listed among the most admired companies in the world. Learn how Cognizant helps clients lead with digital at www.cognizant.com or follow us @Cognizant.

World HEADQUARTERS

500 Frank W. Burr Blvd.
Teaneck, NJ 07666 USA
Phone: +1 201 801 0233
Fax: +1 201 801 0243
Toll Free: +1 888 937 3277
Email: inquiry@cognizant.com

European HEADQUARTERS

1 Kingdom Street
Paddington Central
London W2 6BD
Phone: +44 (0) 20 7297 7600
Fax: +44 (0) 20 7121 0102
Email: infouk@cognizant.com

India Operations HEADQUARTERS

#5/535, Old Mahabalipuram Road
Okkiyam Pettai, Thoraipakkam
Chennai, 600 096 India
Phone: +91 (0) 44 4209 6000
Fax: +91 (0) 44 4209 6060
Email: inquiryindia@cognizant.com

© Copyright 2018, Cognizant. All rights reserved. No part of this document may be reproduced, stored in a retrieval system, transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the express written permission from Cognizant. The information contained herein is subject to change without notice. All other trademarks mentioned herein are the property of their respective owners.