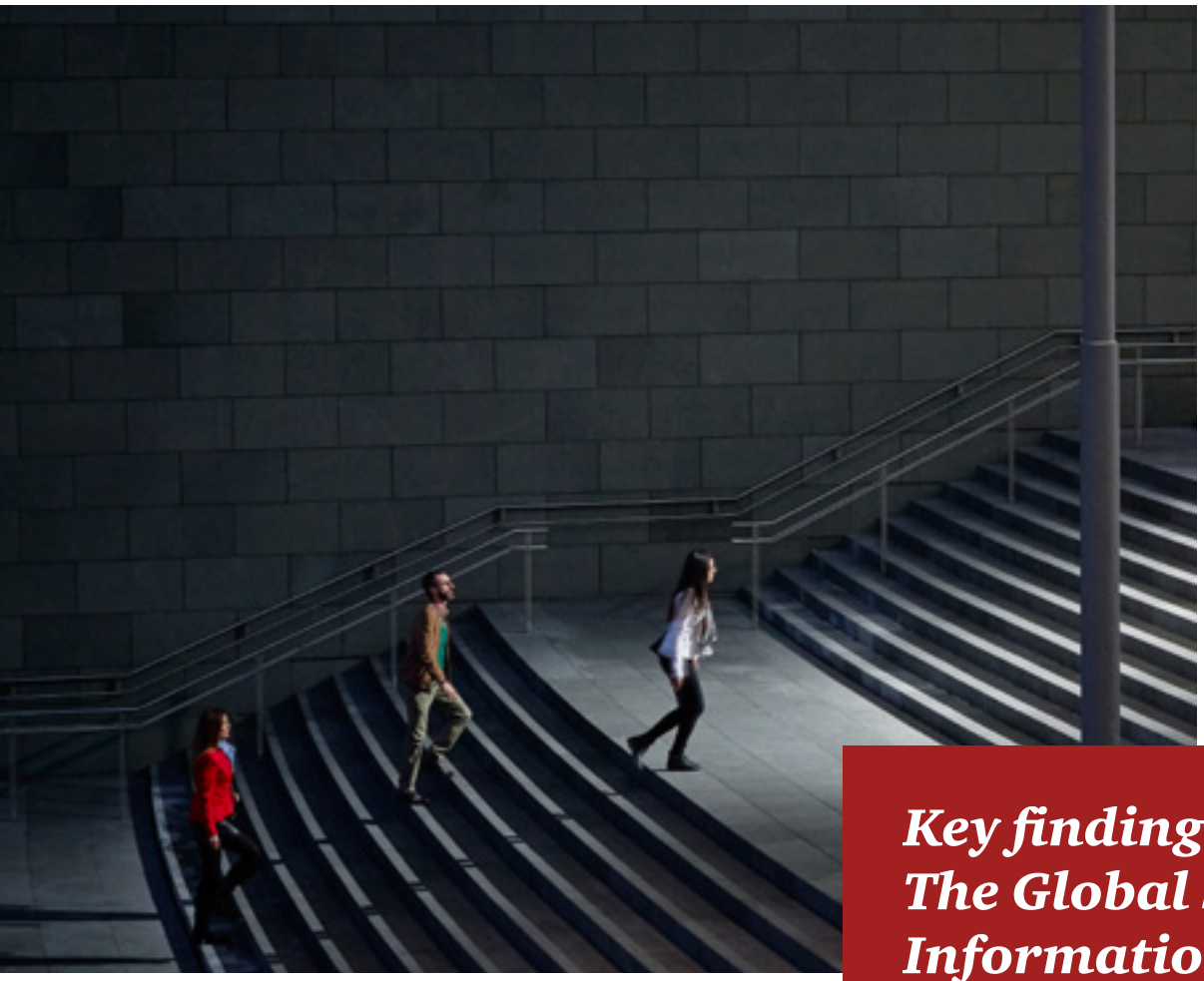
www.pwc.com/gsiss

Moving forward with cybersecurity and privacy

How organizations are adopting innovative safeguards to manage threats and achieve competitive advantages in a digital era



Key findings from The Global State of Information Security® Survey 2017

pwc

Table of contents

Today, business executives want to hear about innovative new approaches to cybersecurity and privacy—not the same rehash of fear, uncertainty and doubt (FUD). They want to move beyond FUD and think more broadly about cybersecurity and privacy as both protectors and enablers of the business, third-party partners and customers.

This represents a distinct shift: Many organizations no longer view cybersecurity as a barrier to change or as an IT cost. They understand that cybersecurity solutions can also facilitate business growth, create market advantages and build brand trust.

In large part, this shift in thinking is an outgrowth of the digitization of business. Today, organizations not only create products but they also deliver complementary (and sometimes complimentary) software-based services for products that extend opportunities for customer engagement and growth.

59%

say digitization of the business ecosystem has impacted security spending

PwC, CIO and CSO, *The Global State of Information Security® Survey 2017*, October 5, 2016

As more products and services of all sorts become connected to the Internet, the need to proactively address cybersecurity and privacy risks increases. It's not the only driver, however: Data privacy and trust have also become critical business requirements as exponentially more consumer and business information is generated and shared.

As a result, forward-thinking organizations are pivoting toward a new model of cybersecurity, one that is agile, capable of acting on analytic inputs and adaptive to evolving risks and threats. At the core of this new approach are solutions like data analytics and real-time monitoring, managed security services, advanced authentication and open-source software.

While not all of these technologies are new, the way they are distributed and managed often are—many are cloud-based or offered as managed security services. Some, such as adoption of open-source software, represent a radical shift in how organizations develop and run on-premises systems.

If there is one unifying thread, it's the cloud. The power and interoperability of cloud-based platforms enables organizations to synthesize a range of synergistic technologies. What's more, businesses can leverage the inherent simplification of cloud architectures to confidently build secure new products and services on the cloud. These architectural advantages represent a breakout opportunity for the integration and improvement of cybersecurity and privacy tools.

"We're seeing more and more that cybersecurity can actually become a remarkable way to help a company innovate and move faster," said David Burg, US and Global Leader, Cybersecurity and Privacy. *"In certain kinds of digital innovation, the security considerations, controls and capabilities, alongside a frictionless means of authentication, are essential to the design and development of these new products and services."*

Cloud-integrated solutions also can enhance data privacy capabilities and boost customer trust and brand reputation. These are must-have safeguards as consumers become more concerned about how their sensitive data is gathered and shared, and governments step up scrutiny of how their citizens' information is used across borders.

Use of technologies to address threats and create value

Source: PwC, CIO and CSO, *The Global State of Information Security® Survey 2017,* October 5, 2016

As technology reshapes cybersecurity and privacy models, one mainstay remains constant: Security fundamentals are the *sine qua non* of an effective program.

Businesses may invest more (or less) in cybersecurity, and sophisticated technologies certainly can help prevent the spread of attacks or reduce impacts. But threat actors will likely remain ahead of the game by leveraging new tactics and techniques as their motives and technologies evolve.

Organizations that hew to the basics of cybersecurity—fundamentals such as employee training, up-to-date policies and controls, and a commitment to readiness and resilience—will likely be better prepared to manage simple attacks and preserve resources for more complex incidents.

When analyzing results from The Global State of Information Security® Survey 2017, four key trends came to the fore: Digital businesses are adopting new technologies and approaches to cybersecurity, threat intelligence and information sharing have become business-critical, organizations are addressing risks associated with the Internet of Things, and geopolitical threats are rising.

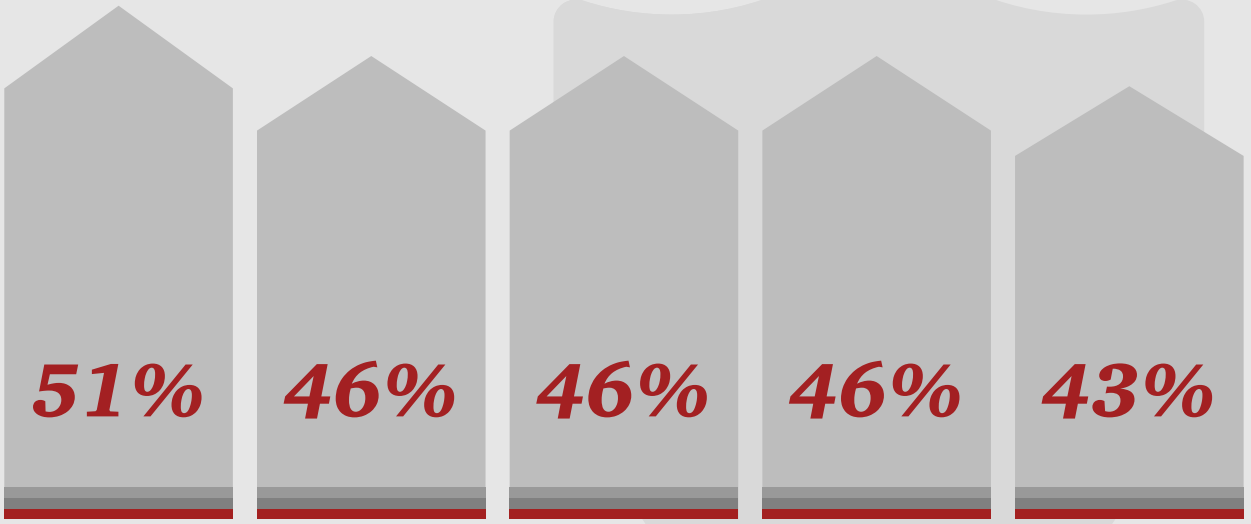
Over the next few months, we will release survey results in four installments. This initial paper explores how digital organizations are leveraging new technology safeguards to build a cybersecurity and privacy program that jumpstarts success—and creates a truly differentiating business capability.

Thinking broadly about cybersecurity and privacy

Most businesses today are fundamentally digital, and software is becoming the backbone of operations, products and services. Increasingly, organizations are exploring new opportunities to create value and competitive advantages by integrating cybersecurity and privacy with digital business strategies.

Consider the automotive industry. In the past, buying an automobile focused on performance, design, capabilities and price of the vehicle. Today, these factors are being eclipsed by connectivity, in-car digital content and services, and autonomous driving features. A growing range of automobile manufacturers, telecommunications operators, software vendors and consumer electronics firms provide a robust aftermarket in digital services.

Cybersecurity spending priorities for the next 12 months



Source: PwC, CIO and CSO, *The Global State of Information Security® Survey 2017,* October 5, 2016

This means sale of a product or service is no longer a one-time event; companies are providing add-on digital services throughout the product life cycle. This example holds across most industries and represents a paradigm shift in business models.

It also places more emphasis on the quality and safety of overall digital services. Customers expect that these products be wrapped in an intuitive, engaging digital package that also protects their sensitive data. As a result, a highly secure digital experience has become a must-have capability.

"You have to deliver those services in a secure manner so that the customer continues to trust its interaction with you as a company and with the product," said Christopher O'Hara, PwC US Co-leader, Cybersecurity and Privacy. *"Cybersecurity becomes a part of the fabric of what these companies offer both in products and services, as well as customer trust."*

Doing so will require a budgetary commitment to the integration of cybersecurity with digitization from the outset. It's an imperative that many organizations have begun to address: 59% of Global State of Information Security® Survey 2017 respondents said digitization of their business ecosystems has impacted their cybersecurity spending. Technologies that organizations are integrating with their digital business models include encryption, next-generation firewalls, network segmentation and identity and access management. Organizations also should consider moving security controls closer to the data.

The payoff? *"Businesses that integrate cybersecurity with digital strategies will be better poised to build trust into everything they do and transform faster,"* said Tom Puthiyamadam, PwC's Global Digital Services Leader. *"Leading companies are integrating cybersecurity, privacy and digital ethics from the outset. And that enables them to better engage with existing customers and attract new ones. Many also see efficiencies in operations, business processes and IT investments."*

Powerful synergies in the cloud

By now, it's clear that off-premises cloud-based storage of applications and data can be more secure than on-premise corporate systems. No wonder, then, that more businesses are entrusting more sensitive data and workloads to cloud providers.

Many, in fact, are running data and workloads such as finance, operations and customer service in the cloud. Even highly regulated businesses, including large financial services firms with very mature cybersecurity programs, are entrusting sensitive data to cloud providers.

63%

run IT operations in the cloud

PwC, CIO and CSO, *The Global State of Information Security® Survey 2017*, October 5, 2016

"We're seeing almost an explosion in companies considering the use of cloud to store critical business processes and functions like accounting, finance, operations and human resources," said Burg of PwC. *"And I think that trend will likely continue as the benefits become increasingly clear."*

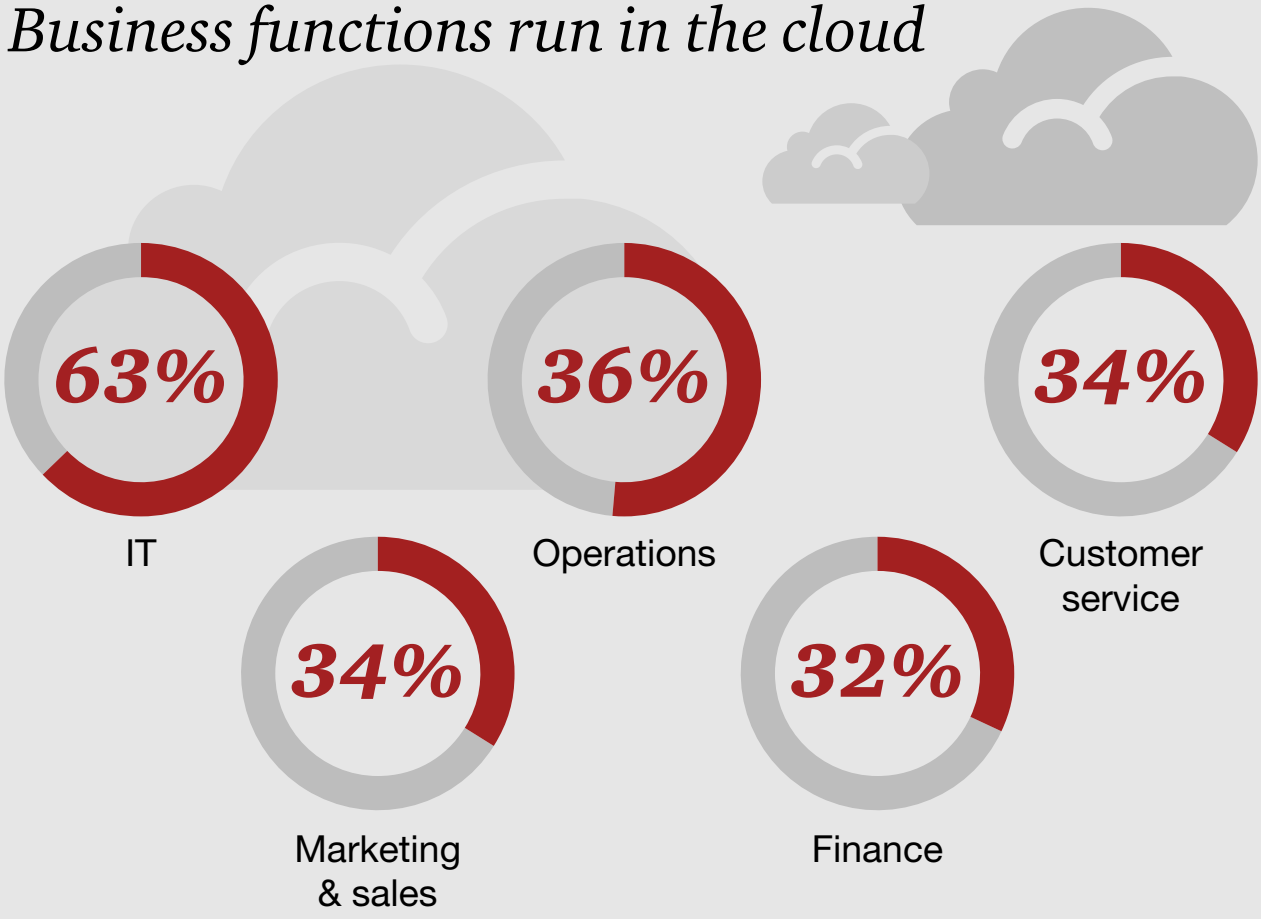
Cloud-centric cybersecurity represents a dynamic approach to risk that can help an organization better understand its overall business ecosystem and internal and external threats. Cloud-based cybersecurity can be augmented with machine learning and artificial intelligence to analyze network activity and amalgamate threat and log information, then parse this data in real time to create actionable intelligence.

The most sophisticated cloud platforms also offer heuristic capabilities. Their computational and analytic powers enable the platform to adapt in real time and grow stronger with every attack on the network and data. In other words, a cloud platform is not only resilient, but it also can bounce back stronger and better.

Cloud-based cybersecurity not only helps deter intruders but it also monitors those who do get in—including legitimate employees, third-party partners and customers—to learn from their behavior. When cloud-based cybersecurity is integrated with functions like marketing, customer service and logistics, the system can track activities of everyone who interacts with their business ecosystem. This enables businesses to assess customer behavior and ultimately improve the experience.

The fusion of advanced technologies with cloud architectures will empower organizations to more quickly identify and respond to threats, better understand customers and the business ecosystem, and ultimately reduce costs. Cybersecurity, in essence, becomes a source of strength—one that can yield truly differentiating business capabilities.

Business functions run in the cloud



Source: PwC, CIO and CSO, *The Global State of Information Security® Survey 2017,* October 5, 2016

Managing security from the outside in

Designing and implementing a cybersecurity and privacy program is challenging enough, but the work doesn't stop there. Once a program is in place, disparate components must be thoroughly integrated, professionally managed and continuously improved.

That's a tall order for resource-constrained organizations, and many are addressing this challenge by adopting managed security services. In fact, almost two-thirds (62%) of Global State of Information Security® Survey 2017 respondents say they use security service providers to operate and enhance their cybersecurity programs.

A primary driver is the global dearth of skilled cybersecurity specialists. A recent report by Cybersecurity Ventures predicted that the existing cybersecurity workforce gap will widen to 1.5 million job openings by 2019.[1] The ongoing talent squeeze is likely to drive more organizations to turn to third parties to help run some or all of their security programs.

1 CSO, *Market expansion adds to cybersecurity talent shortage, July 13, 2016*

62%

use managed security services for cybersecurity and privacy

PwC, CIO and CSO, *The Global State of Information Security® Survey 2017*, October 5, 2016

"With the fast pace of technology disruption, keeping up to date with skill sets around new technologies such as the Internet of Things and cloud computing is more and more difficult for organizations," said Grant Waterfall, PwC's Global Cybersecurity and Privacy Co- Leader. *"Managed security services enables them to procure those skill sets from a service provider and get the niche-specific skills they need to augment their own capabilities."*

Cost is another factor. Businesses may not have the resources to hire an end-to-end team of full-time cybersecurity and privacy professionals. Or they may need to scale an existing solution but do not want to tie up highly skilled in-house staff to execute a relatively simple initiative.

Use of managed security services

Source: PwC, CIO and CSO, *The Global State of Information Security® Survey 2017,* October 5, 2016

Whatever the driver, businesses are outsourcing a range of technology safeguards to managed security providers, including authentication, data loss prevention, identity and access management, and real-time monitoring.

Managed services can be grouped in two broad categories. The first is protect and prevent technologies like identity and access management, data loss prevention and privileged access management. The second category comprises detect and respond, which includes advanced analytics and threat intelligence.

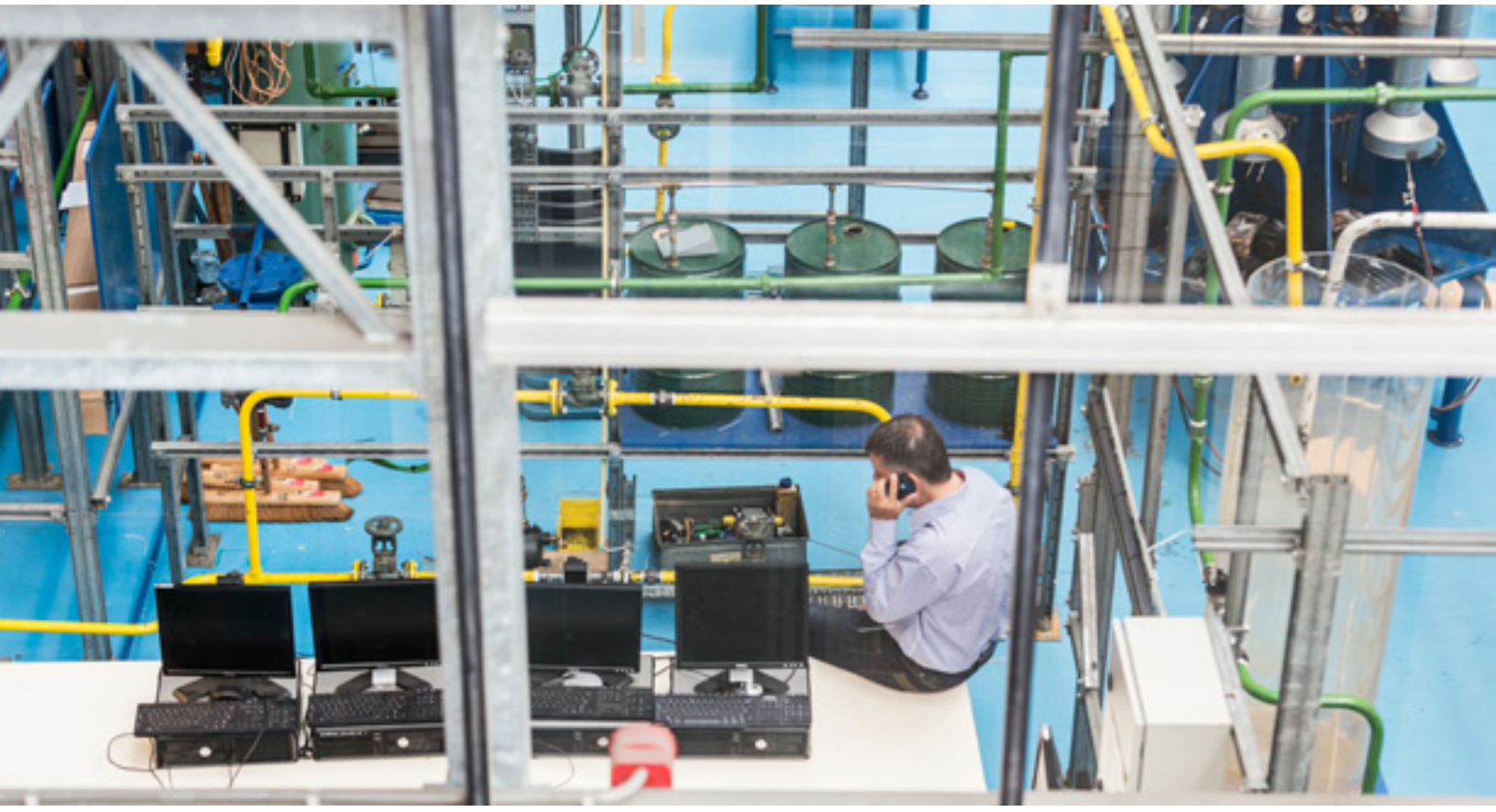
Leading providers are bringing these two categories of services together to deliver seamless capabilities. They typically employ sophisticated technologies and highly trained personnel to deliver 24x7 security operations to quickly detect and respond to emerging threats. They also assist organizations in managing technology and people resources to improve investments and continuously enhance cybersecurity processes. And that means security teams can be freed up to focus on responding to threats and other strategic activities.

Anticipating risks with analytics and threat intelligence

Businesses that do not understand the motivations and tactics of adversaries—both internal and external—will be in the dark when it comes to anticipating and detecting threats.

What's needed is advanced analytics and real-time threat intelligence to gain contextual awareness of risks and understand the tactics, techniques and procedures of adversaries. When analytics and threat intelligence are synthesized in the cloud, it becomes possible to create a single source of enterprise-wide data that is seamlessly correlated and can be managed in real time.

The computational power and storage capabilities of the cloud allows organizations to monitor huge volumes of data, as well as highly complex and interconnected applications, to identify suspicious activity. Cloud-centric analytics can compare all activities across the network, continually assessing activity against norms and across a global repository of threat indicators. When a

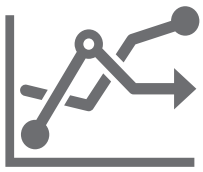


new threat is identified, cloud-based analytics can prioritize responses based on the business impact to data assets.

This year, more than half (51%) of Global State of Information Security® Survey respondents say they use Big Data analytics to model for cybersecurity threats and identify incidents. Big Data represents a considerable challenge for many businesses, however. It requires massive storage and processing power, as well as experienced data scientists to code sophisticated algorithms and analysis applications. As noted above, the scarcity of cybersecurity professionals and budgetary constraints may curtail the ability to implement sophisticated Big Data solutions.

51%

use Big Data analytics to model for and identify threats



PwC, CIO and CSO, *The Global State of Information Security® Survey 2017*, October 5, 2016

That's another reason why we're seeing more organizations adopt cloud-based solutions. Among respondents who use managed security services, 55% say they use service providers for real-time monitoring and analytics. In addition to computational and storage advantages and technical know-how, large managed service providers often have access to global Security Operations Centers (SOCs) and threat intelligence fusion centers. SOCs and threat intelligence fusion are absolutely critical to aggregate data, filter out false positives and get actionable information.

Monitoring and analysis tools are considerably more powerful when threat intelligence is shared with business peers, industry groups and government agencies. Again, the cloud provides a single, secure platform for storing and sharing information with others. We'll explore information sharing in depth in a subsequent report.

Moving beyond passwords toward advanced authentication

When it comes to authentication, passwords are about as useful as, well, 123456. This you-guessed-it string of numbers is still the most commonly used password today.

User disregard for strong password practices is one reason why many businesses are turning to advanced authentication technologies to add an extra layer of security and improve trust among customers and business partners.

Authentication technologies not only make authentication easier for users, but also help bolster overall data security. In fact, 46% of organizations that employ advanced authentication say it has made online transactions more secure, according to this year's survey results. Respondents also report that authentication technologies boost consumer confidence in their security and privacy capabilities, as well as enhance the customer experience and protect brand reputation.

57%

use biometrics for authentication

PwC, CIO and CSO, *The Global State of Information Security® Survey 2017*, October 5, 2016

In the past, advanced authentication was primarily the technological domain of government systems and large financial institutions; more recently, social media and consumer email providers introduced multifactor authentication. Now, more sectors are adopting multifactor authentication across a range of transactions.

The concept of multifactor authentication is simple: After entering a name and password, the user receives a text message on their mobile device that provides a code (the second factor) to complete authentication. Beyond multifaction, some businesses are developing and implementing more advanced on-premises technologies. This type authentication employs methods such as a pattern that a user must enter, an access card or fob or biometric information such as fingerprint or iris scans.

As organizations implement new authentication technologies, they may need to rethink their approach to identity management in order to design solutions that build identity trust relationships and ensure ease of use for customers. It's also important to map authentication to the level of risk the access brings to the business.

Opening possibilities with open-source software

Adoption of open-source software represents a major shift in how organizations develop and run on-premises solutions and deliver IT services.

And it's proliferating across industries. Some of the world's largest companies are embracing the open-source movement, including software titan Microsoft: The company has made components of SQL Server, .NET and PowerShell available in Linux.[2] Even the US government has launched a pilot program requiring agencies to release at least 20% of new code for federally funded websites, apps and other software projects as open source.[3]

49%

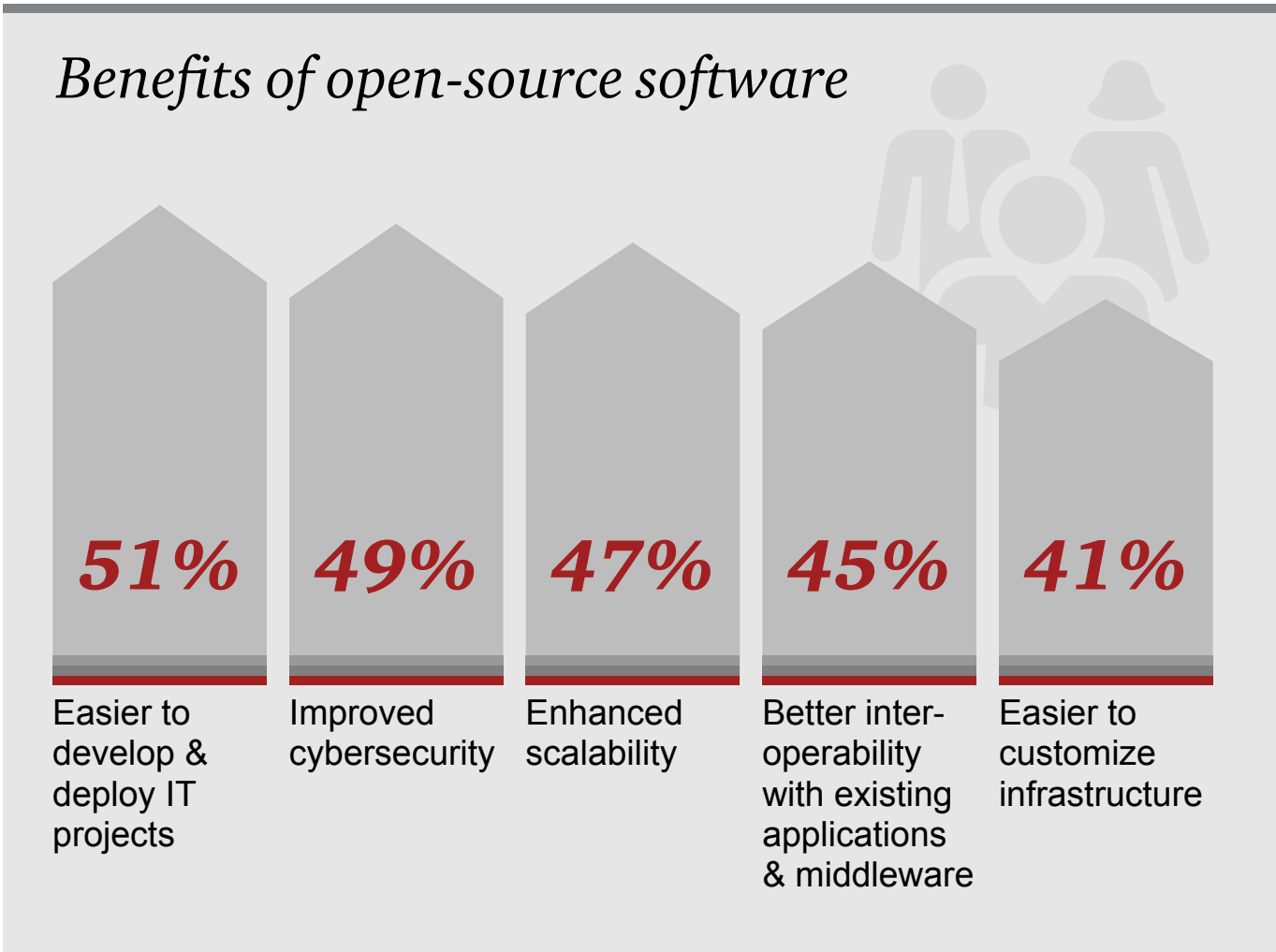
of respondents who use open-source software say it has improved their cybersecurity program

PwC, CIO and CSO, *The Global State of Information Security® Survey 2017*, October 5, 2016

So it's not entirely surprising to learn that more than half (53%) of survey respondents use some form of open-source software. It was a bit eye-opening, however, to find that 49% of those who use open-source technology say it has improved their cybersecurity posture.

Businesses are adopting open-source software for several key reasons. Open-source applications can scale quickly and effectively, and in many cases they have been collaboratively developed and tested by security talent across industries. The software is typically available at little or no cost, providing an inexpensive method to create new solutions. And when combined with the cloud, open-source technologies can help enhance interoperability among an expanding constellation of devices, sensors, technologies and identities.

2 Microsoft Azure Blog, *PowerShell is open sourced and is available on Linux*, August 18, 2016
3 Federal Source Code Policy, *5. Open Source Software*, accessed September 20, 2016



Source: PwC, CIO and CSO, *The Global State of Information Security® Survey 2017,* October 5, 2016

These advantages combine to make open-source a potentially game-changing technology. *"We believe that more and more industries will likely embrace open-source,"* said PwC's Burg. *"Open-source takes advantage of groupthink to make an application or a service as good as it can be in as efficient a manner as possible."*

Increasing global risk for data privacy

While interconnected digital ecosystems and the threats they generate are driving changes in cybersecurity, technology advances are also creating regulatory change around the world. The legislative churn, in turn, is paving the way for record levels of enforcement actions, class-action lawsuits and regulator scrutiny over new technologies such as geolocation tracking and Big Data analytics.

Indeed, this year, a slew of new requirements are either in effect or have been announced.

One of the most impactful is the EU's General Data Protection Regulation (GDPR), which goes into effect April 2018. The GDPR will bring cascading privacy demands that will require a renewed focus on data privacy for companies that offer goods and services to EU citizens. Businesses that do not comply with GDPR face fines as high as 4% of the company's global annual revenue.[4] Court precedents in Europe are also introducing a new risk for companies there: privacy class actions.

4 European Union, *General Data Protection Regulation*, accessed September 20, 2016

"GDPR requires a level of internal control over privacy practices we've never seen before," said Jay Cline, Principal, Cybersecurity and Privacy at PwC. *"A half-billion EU citizens will be poised to hold multinationals accountable to this higher bar through new rights they will begin exercising one spring morning a year and a half from now."*

Five key GDPR requirements are likely to have in-depth impact on organizations that do business in Europe:

- Mandatory data inventorying and record keeping of all processing of European personal data.
- Mandatory data-breach notification to regulators and individuals whose information is compromised.
- The right to be forgotten, which allows individuals to request that their personal data be erased.
- Routine privacy impact assessments.
- Mandatory data protection officers (DPOs).

Compliance with GDPR will be a challenge for many. Businesses may be required to conduct comprehensive risk assessments and implement new end-to-end security enhancements. Many will need to rethink data-governance strategies, and implement processes and technologies for maintaining comprehensive data inventories.

Only the proactive will be prepared. Organizations can help get ahead of the regulation by conducting a GDPR readiness assessment, remediating GDPR gaps to a level of operational adequacy and instituting an ongoing compliance-monitoring process.

In addition to GDPR, many US businesses also will need to address Privacy Shield, the successor to the Safe Harbor framework that governs trans-Atlantic transfer of personal data of EU citizens. Privacy Shield membership will undoubtedly increase scrutiny of the storage and transfer of any kind of data, from social media posts to payroll processing.

Compliance is likely to be potentially onerous. US businesses, for instance, will be required to identify third parties with which they share personal data of EU citizens. They also must conduct privacy due diligence of third parties that process EU personal data and produce evidence of compliance on demand—signed by an officer of the company.[5]

To get there, many businesses will need to update data inventories and dataflow maps to verify the scope of how they handle of EU personal data. They also should conduct a cost-benefit analysis of Privacy Shield compliance and complete operational adequacy controls that test model contract commitments.

Burdensome new regulations and legislation extends beyond the EU and the US, of course. Other significant new regulations have been introduced in Asia, including China, South Korea, Hong Kong and Singapore.

In China, increasingly strident government regulations— such as increased obligations and censorship duties to prevent the spread of prohibited and illicit information under a proposed cybersecurity law—are potential challenges to outside businesses.[6] A slate of recent cybersecurity laws requires technology companies and financial institutions to store their data in China, submit to security checks and help the government with decryption if requested. As a result, many organizations are strengthening joint ventures or are conducting more business through Chinese partners.

5 US Department of Commerce, *Privacy Shield Framework Requirements of Participation*, accessed September 20, 2016
6 Broader Perspectives, *Chinese Cybersecurity Rules Alter Business Paths*, June 14, 2016

Recently, however, China has signalled a more cooperative attitude by allowing foreign businesses to participate in meetings of the government administration that defines cybersecurity standards.[7] It is encouraging that China is acknowledging the global nature of the technology supply chain and recognizing the need to align its policy with international trends.

Other examples of stringent cybersecurity and privacy legislation include an amendment to South Korea's Personal Information Protection Act (PIPA). The amendment establishes new penalties that include fines of up to KRW 100 million (US $87,994) and/or as much as 10 years in prison.[8]

In Hong Kong, the Personal Data (Privacy) Ordinance sets forth enhanced regulations for collection and handling of personal data, including a rule for transferring data to third parties and cross-border transfers.[9] It is enforced by fines of up to HK $1 million

7 SC Magazine, *China allows foreign tech firms to participate in creating cybersecurity standards*, August 31, 2016
8 South Korea Ministry of Security and Public Administration, *Personal Information Protection Act, Article 70*, accessed October 3, 2016
9 PwC, *Are you taking action on data privacy?*, January 2013

(US $128,900) and prison sentences of up to five years. In May, the Hong Kong Monetary Authority issued a draft consultation framework on cyber-resilience management, titled Cyber Fortification Initiative, that it expects all banks to follow. The new framework likely will be issued in late 2016 or early 2017.

And in Singapore, the Personal Data Protection Act, which took effect in July 2014, provides new regulations on the collection, use and disclosure of personal data, as well as cross-border transfers. It is enforced by penalties of up to SGD $1 million (US $735,862) and imprisonment of up to three years.[10]

An overall trend toward more data-localization requirements, mandatory data-breach notification and restrictions on Big Data analytics will require that organizations proactively engage their business and technology leaders in developing a global privacy strategy. Successful strategies should aim beyond compliance to include procedures for global transfer and monetization of data.

10 Personal Data Protection Commission Singapore, *Legislation and Guidelines*, accessed September 30, 2016

How organizations are addressing regulatory challenges

These evolving data privacy regulations and Internet-use rules create new obstacles for organizations, and many executives are clearly worried. In PwC's 19th Annual Global CEO Survey, executives cited over-regulation as this year's top threat to business growth.[11]

Among GSISS respondents, the most-cited privacy priority over the next 12 months is privacy training and awareness, with updating of privacy policies and procedures a close second.

"To improve training and awareness programs, organizations should set the tone from the top, making it really about enabling the company's digital future," said PwC's Waterfall. "They then should tie this to the purpose of the company and design programs around that."

Beyond these measures, organizations should develop and update methodologies to manage privacy and compliance, as well as implement or update a data-use governance framework, perform impact assessments and ensure that a current data privacy life cycle program is in place. Many may benefit by securely consolidating infrastructures and technologies to address IT redundancies and, when appropriate, transferring these systems to the cloud.

Like never before, it's essential to carefully consider the types of information that is gathered about customers and ensure collection and storage of data is kept to a minimum. The business benefits should outweigh the risk.

11 PwC, PwC 19th Annual Global CEO Survey, January 2016

Privacy priorities for the next 12 months

38% Privacy training & awareness

36% Privacy policies & procedures

32% Privacy assessments

31% Privacy incident response

Source: PwC, CIO and CSO, *The Global State of Information Security® Survey 2017,* October 5, 2016

Then, now and opportunities for the future

Technology and cybersecurity progress over the past decade has been astonishingly swift and sweeping.

Consider, for instance, that it was only 10 years ago that Amazon launched its Amazon Web Services (AWS) to deliver IT to businesses.[12] Today, the majority of organizations around the world (63% of survey respondents) say they run IT services in the cloud.

The digital business model was an enigma to many companies a decade ago. In 2007, most organizations simply did not understand advantages of a digital model, much less how to implement one. Some mistrusted the idea altogether: Just a few years earlier, after all, the $350 billion AOL-Time Warner merger had resulted in what is widely regarded as a business mistake.[13]

Fast-forward 10 years, and 59% of survey respondents say they are boosting their spending on security as a result of digitization. To get there, businesses are optimizing business models for the digital era. Many are implementing foundational elements—cloud computing, sophisticated data monitoring and analytics, and open-source technologies, to name a few—and integrating digitalization with cybersecurity and privacy.

And then there's the ability to understand cybersecurity and privacy threats to the organization. In 2008, 42% of our survey respondents did not know the source of detected security incidents.[14] This year, only 13% of respondents couldn't identify what type of actors—such as employees, business partners, hackers, hacktivists and nation-states—were responsible for intrusions.

Finally, more organizations understand that cybersecurity and privacy are no longer simply an IT task. Today, many recognize that cybersecurity can create business advantages, trust and shareholder value. They also understand that combining digital business models with cybersecurity can enable them to confidently create entirely new digital platforms, products and services.

The future is ultimately unknowable. But we believe we'll see advances in technologies such as artificial intelligence, machine learning, sophisticated advanced authentication and adaptive controls. When combined on the cloud, they will very likely engender new architectural models and powerful cybersecurity and privacy capabilities that will help organizations get ahead of sophisticated—and mundane—threats.

12 CIO, *10 Cloud Computing Companies to Watch*, May 18, 2009
13 The New York Times, *How the AOL-Time Warner Merger Went So Wrong*, January 10, 2010
14 PwC, CIO and CSO, *The Global State of Information Security® Survey*, October 2008

Methodology

The Global State of Information Security® Survey 2017 is a worldwide study by PwC, CIO and CSO. It was conducted online from April 4, 2016 to June 3, 2016. Readers of CIO and CSO and clients of PwC from around the globe were invited via email to participate in the survey.

The results discussed in this report are based on responses of more than 10,000 CEOs, CFOs, CIOs, CISOs, CSOs, VPs and directors of IT and security practices from more than 133 countries.

Thirty-four percent (34%) of survey respondents are from North America, 31% from Europe, 20% from Asia Pacific, 13% from South America and 3% from the Middle East and Africa.

The margin of error is less than 1%; numbers may not add to 100% due to rounding. All figures and graphics in this report were sourced from survey results.

PwC cybersecurity and privacy contacts by country

Australia

Richard Bergman
Partner
richard.bergman@au.pwc.com

Andrew Gordon
Partner
andrew.n.gordon@au.pwc.com

Steve Ingram
Partner
steve.ingram@au.pwc.com

Austria

Christian Kurz
Senior Manager
christian.kurz@at.pwc.com

Belgium

Filip De Wolf
Partner
filip.de.wolf@be.pwc.com

Brazil

Edgar D'Andrea
Partner
edgar.dandrea@br.pwc.com

Canada

David Craig
Partner
david.craig@ca.pwc.com

Sajith (Saj) Nair
Partner
s.nair@ca.pwc.com

Richard Wilson
Partner
richard.m.wilson@ca.pwc.com

China

Megan Haas
Partner
megan.l.haas@hk.pwc.com

Ramesh Moosa
Partner
ramesh.moosa@cn.pwc.com

Kenneth Wong
Partner
kenneth.ks.wong@hk.pwc.com

Denmark

Christian Kjær
Director
christian.x.kjaer@dk.pwc.com

Mads Nørgaard Madsen
Partner
mads.norgaard.madsen@dk.pwc.com

France

Philippe Trouchaud
Partner
philippe.trouchaud@fr.pwc.com

Germany

Derk Fischer
Partner
derk.fischer@de.pwc.com

India

Sivarama Krishnan
Partner
sivarama.krishnan@in.pwc.com

Israel

Rafael Maman
Partner
rafael.maman@il.pwc.com

Italy

Fabio Merello
Partner
fabio.merello@it.pwc.com

Japan

Yuji Hoshizawa
Partner
yuji.hoshizawa@pwc.com

Sean King
Partner
sean.c.king@pwc.com

Naoki Yamamoto
Partner
naoki.n.yamamoto@pwc.com

Korea

Soyoung Park
Partner
s.park@kr.pwc.com

Luxembourg

Vincent Villers
Partner
vincent.villers@lu.pwc.com

Mexico

Fernando Román Sandoval
Partner
fernando.roman@mx.pwc.com

Yonathan Parada
Partner
yonathan.parada@mx.pwc.com

Juan Carlos Carrillo
Director
Carlos Carrillo@mx.pwc.com

Middle East

Mike Maddison
Partner
mike.maddison@ae.pwc.com

Netherlands

Gerwin Naber
Partner
gerwin.naber@nl.pwc.com

Otto Vermeulen
Partner
otto.vermeulen@nl.pwc.com

Bram van Tiel
Director
bram.van.tiel@nl.pwc.com

New Zealand

Adrian van Hest
Partner
adrian.p.van.hest@nz.pwc.com

Norway

Lars Erik Fjørtoft
Partner
lars.fjortoft@pwc.com

Poland

Rafal Jaczynski
Director
rafal.jaczynski@pl.pwc.com

Jacek Sygutowski
Director
jacek.sygutowski@pl.pwc.com

Piotr Urban
Partner
piotr.urban@pl.pwc.com

Russia

Tim Clough
Partner
tim.clough@ru.pwc.com

Singapore

Vincent Loy
Partner
vincent.j.loy@sg.pwc.com

Jimmy Sng
Partner
jimmy.sng@sg.pwc.com

South Africa

Sidriaan de Villiers
Partner
sidriaan.de.villiers@za.pwc.com

Elmo Hildebrand
Director/Partner
elmo.hildebrand@za.pwc.com

Busisiwe Mathe
Partner/Director
busisiwe.mathe@za.pwc.com

South East Asia

Jimmy Sng
Partner
jimmy.sng@sg.pwc.com

Spain

Javier Urtiaga Baonza
Partner
javier.urtiaga@es.pwc.com

Elena Maestre
Partner
elena.maestre@es.pwc.com

Sweden

Martin Allen
Director
martin.allen@se.pwc.com

Rolf Rosenvinge
Director
rolf.rosenvinge@se.pwc.com

Switzerland

Reto Haeni
Partner
reto.haeni@ch.pwc.com

Turkey

Burak Sadic
Director
burak.sadic@tr.pwc.com

United Kingdom

Neil Hampson
Partner
neil.r.hampson@uk.pwc.com

Richard Horne
Partner
richard.horne@uk.pwc.com

Alex Petsopoulos
Partner
alex.petsopoulos@uk.pwc.com

United States

David Burg
Principal
david.b.burg@pwc.com

Scott Dillman
Principal
scott.dillman@us.pwc.com

Chris O'Hara
Principal
christopher.ohara@us.pwc.com

Grant Waterfall
Partner
grant.waterfall@us.pwc.com

www.pwc.com/gsiss
www.pwc.com/cybersecurity

229699-2017