

# Toward new possibilities in threat management

How businesses are embracing a modern approach to threat management and information sharing.



*Key findings from  
the Global State of  
Information Security<sup>®</sup>  
Survey 2017*

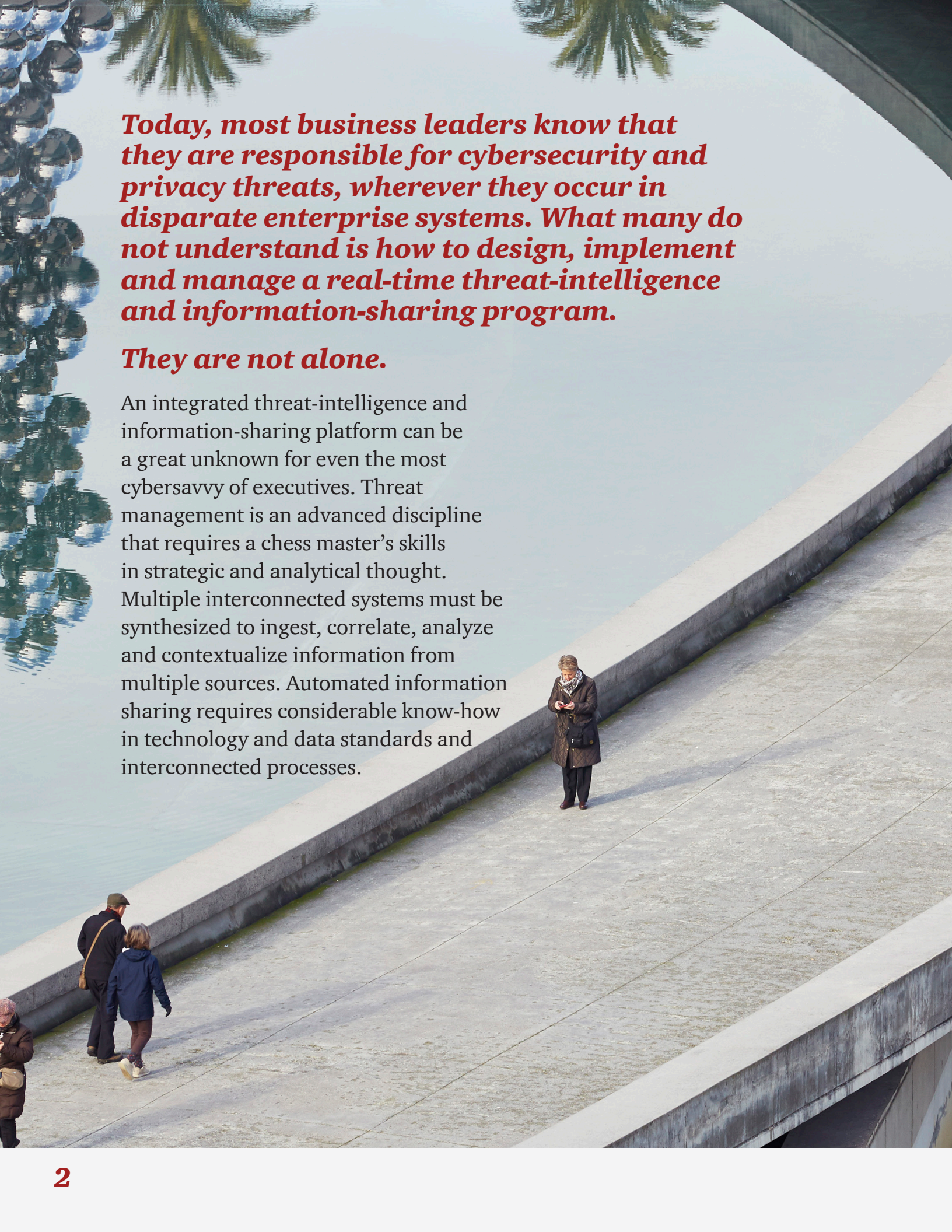




## ***Table of contents***

Introduction .....	<b>2</b>
Bold new combinations in the cloud.....	<b>5</b>
Integrating key threat-management tools in the cloud .....	<b>7</b>
Advanced authentication to catch phishers.....	<b>9</b>
What cloud-based threat intelligence looks like .....	<b>13</b>
The power of a centralized platform.....	<b>14</b>
Tapping into a network of information-sharing resources .....	<b>16</b>
<i>How ISAOs improve prospects for information sharing.....</i>	<b>20</b>
A state of pioneering cybersecurity .....	<b>22</b>
Toward the future of threat intelligence.....	<b>23</b>
Methodology .....	<b>24</b>
Contacts .....	<b>25</b>





***Today, most business leaders know that they are responsible for cybersecurity and privacy threats, wherever they occur in disparate enterprise systems. What many do not understand is how to design, implement and manage a real-time threat-intelligence and information-sharing program.***

***They are not alone.***

An integrated threat-intelligence and information-sharing platform can be a great unknown for even the most cybersavvy of executives. Threat management is an advanced discipline that requires a chess master's skills in strategic and analytical thought. Multiple interconnected systems must be synthesized to ingest, correlate, analyze and contextualize information from multiple sources. Automated information sharing requires considerable know-how in technology and data standards and interconnected processes.

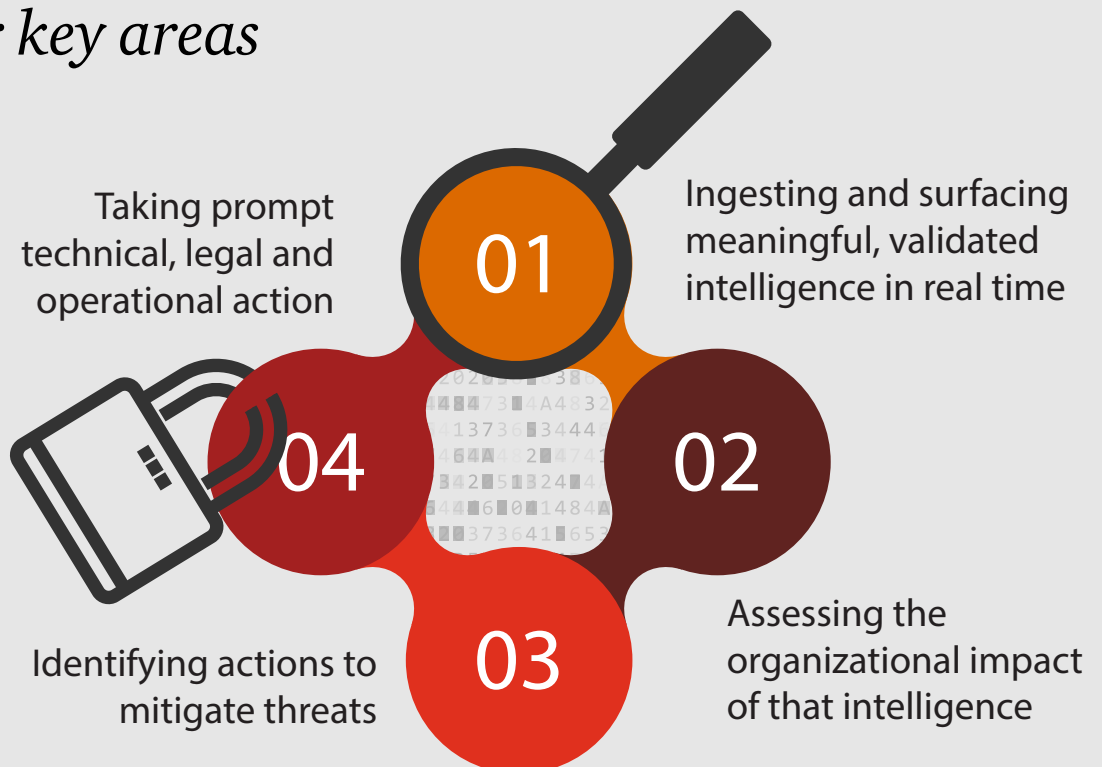


Both demand a foundation of cloud-based monitoring and analysis technologies, an interoperable information-sharing strategy and platform, and carefully tailored processes. To get there, businesses will need in-house or external expertise in four key areas:

- Ingesting and surfacing meaningful, validated intelligence in real time.
- Assessing the organizational impact of that intelligence.
- Identifying actions to mitigate threats.
- Taking prompt technical, legal and operational action.

These four distinct skill sets require no small sum of technical expertise and resources. As such, organizations will need deep cybersecurity expertise as well as a multidisciplinary team that includes stakeholders from IT, legal counsel, risk, privacy and business units. This team will be responsible for creating custom processes to integrate activities across systems and the enterprise.

## *Threat management requires expertise in four key areas*



We believe that cloud computing services are foundational to the integration and management of the many moving parts of a threat-management program. A cloud-based model can deliver computational power to monitor and analyze all digital interactions and create a unified repository of information to generate actionable intelligence in real time.

A cloud-centric solution may not be the choice of all businesses—some may opt to implement and run an on-premise threat-management solution. And there are concrete advantages to this approach. For one, organizations own on-premise solutions, and that allows them to fully customize and integrate systems to accommodate individual business needs. It can also give organizations complete control in compliance with government and industry regulations. And because data and applications are stored on servers in house, cybersecurity teams always know where data is stowed.

Despite the advantages, on-premise threat management entails complex challenges and internal resource requirements. Chief among them: Businesses must hire and retain key talent with niche skills to manage large amounts of unstructured threat information and process it so that it can be leveraged effectively. An on-premise solution also requires the resources to hire and retain highly skilled cyberthreat-intelligence analysts to review data and take immediate action on that information. Finally, organizations must have an agile technology ecosystem that can scale to a large set of both internal and external threat information as needed.

Whether on-premise or on the cloud, implementation of a threat-management system will be a challenge for even the most highly resourced organizations. But those that tackle this initiative will be better prepared to proactively monitor for threats, identify compromises, quickly respond to incidents and share threat intelligence. Ultimately, these capabilities will help build competitive advantages by protecting customer data, business assets and brand reputation.



Take a look at our interactive timeline.  
***Connecting the dots: A timeline of technologies, threats and regulations that redefined cybersecurity and privacy***

## ***Bold new combinations in the cloud***

When it comes to threat intelligence and information sharing, the cloud platform provides a centralized foundation for constructing, integrating and accessing a modern threat program.

The power and interoperability of a centralized cloud platform enables organizations to synthesize a range of synergistic threat-management technologies. What's more, businesses can leverage the inherent simplification of cloud architectures to build new robust and scalable threat-detection capabilities. The cloud also can enable safer information sharing by combining analytics from multiple sources without compromising data security.

The fusion of advanced technologies with cloud architectures can help organizations more quickly identify and respond to threats, better understand customers and the business ecosystem, and ultimately reduce costs. This model can, for instance, leverage machine learning and artificial intelligence techniques to aggregate and analyze enormous volumes of data, correlate this data with a global database of threat intelligence, identify threats in real time and prioritize responses based on impact to affected assets.

**48%**  
*of IT services  
are delivered  
via the cloud*



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

Cloud-based threat-management capabilities are evolving rapidly—and are changing the model of on-premise cybersecurity and privacy solutions. *“We’re seeing rapid uptake of the cloud model because of its cost advantages, the compute and scalability that it provides—and the ability to rapidly and flexibly adjust computing capabilities,”* said Christopher O’Hara, PwC US Co-Leader, Cybersecurity and Privacy. *“We believe cloud-based cybersecurity will evolve to the point where you can realistically take any type of threat data and process it, normalize it and understand its impact to your business in real time. Today’s on-premise solutions simply can’t do that.”*

That’s because traditional on-premise systems are often constrained by inadequate storage capacity, processing power and scalability. These limitations can impede cybersecurity teams’ ability to view and analyze data across their enterprise, restrict search efforts and increase the volume of false positives.

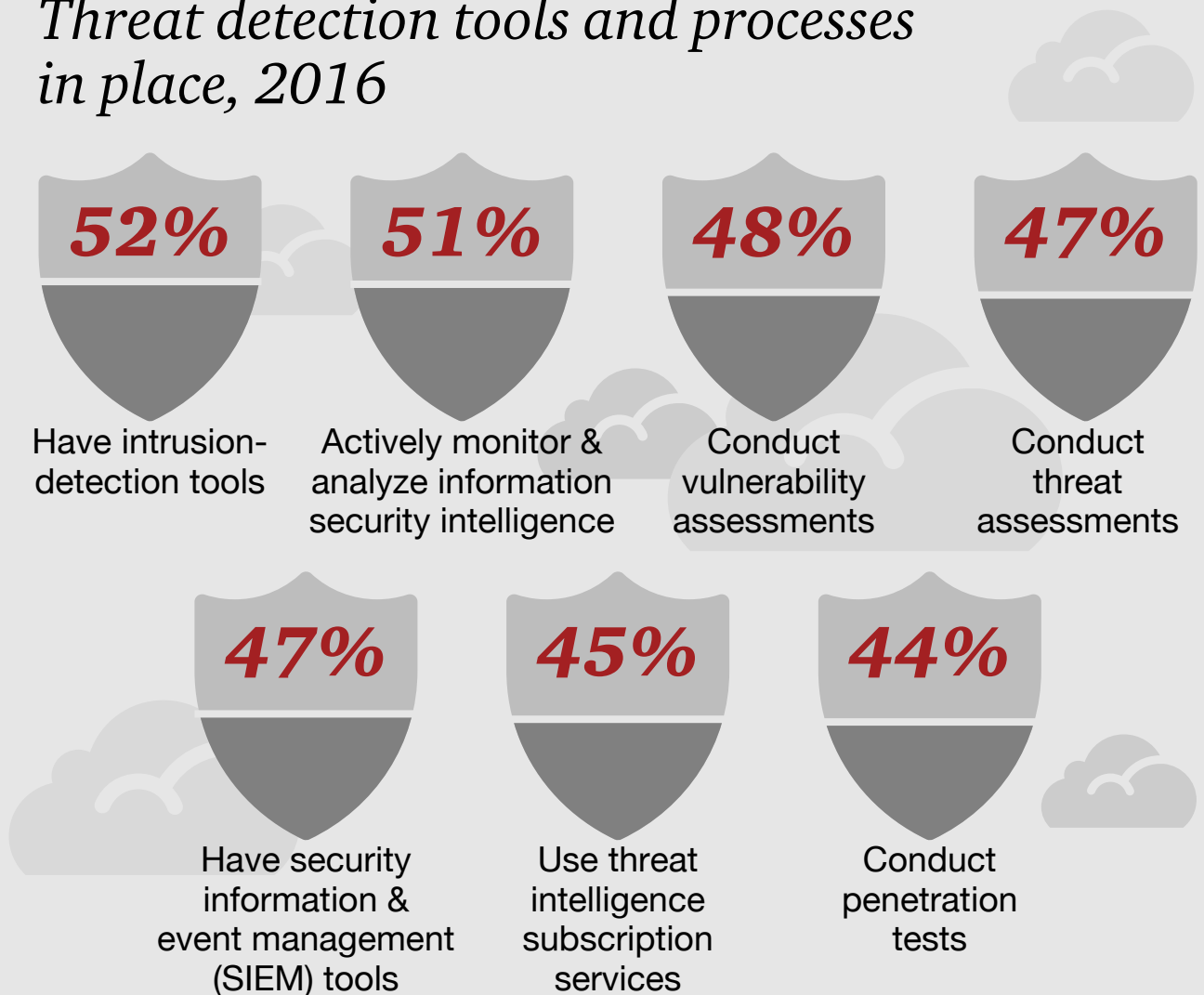


## ***Integrating key threat-management tools in the cloud***

Many organizations are proactively adopting or updating key technologies that are essential to gathering and analyzing threat intelligence. Increasingly, they are opting for cloud-based managed security services rather than traditional on-premise systems.

In fact, 62% of respondents use managed security services for initiatives like authentication, identity and access management, real-time monitoring and analytics, and threat intelligence.

### *Threat detection tools and processes in place, 2016*



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



Few capabilities are more fundamental to proactive threat intelligence than real-time monitoring and analytics. This year, more than half (51%) of respondents say they actively monitor and analyze threat intelligence to help detect risks and incidents.

Businesses have traditionally focused on internal information such as log files and access activity. But recently the cybersecurity and privacy capabilities of external business partners became a priority after several high-profile breaches were attributed to the compromise of vendors' systems.

As the scope of monitoring and analytics expands, solutions should include capabilities to ingest real-time monitoring and analytics programs should include capabilities to ingest and interpret raw data to provide contextual awareness of threats and an understanding of 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, can be quickly searched and can be managed in real time.

## ***Advanced authentication to catch phishers***

Over the past year, phishing has emerged as a significant risk to businesses of all sizes and across industries. The technique represents a re-emergence of traditional social engineering tactics, although phishing is more highly focused and effective. Cybercriminals have become adept at using phishing schemes to obtain user credentials and then gain access to information systems and data.

This year, in fact, 38% of survey respondents reported phishing scams, making it the top vector of cybersecurity incidents. The surge in phishing incidents suggests that cybercriminals are relying less on sophisticated malware to conduct attacks and instead are “living off the land” by exploiting existing administrator tools and functions.

To combat theft of user credentials, many businesses are adopting advanced authentication to replace all-but-useless passwords. This type of prevention has become a critical business requirement as exponentially more consumer and corporate information is generated and shared, and consumers expect that their personal data will be secured.

Today, the most widely used advanced-authentication technologies are hardware and software tokens, followed by biometrics such as fingerprint and iris scanners. In the coming year however, survey respondents say their No. 1 spending priority for authentication is smartphone tokens. This year, 28% of survey respondents reported security compromises of mobile devices, and securing smartphones and tablets is clearly top of mind.



*“We’re seeing quite a bit of interesting innovation to make it easier for consumers to authenticate,”* said David Burg, PwC’s US and Global Co-Leader, Cybersecurity and Privacy. *“The way that a consumer authenticates to an application may be on a mobile device, and today that is far easier and more secure than it ever has been.”*

The use of password-less authentication and apps will require that organizations rethink their approach to identity management and calibrate the level of authentication to the risk of access. Above all, authentication must be frictionless and intuitive for end users. You need only consider the IAM and authentication techniques employed by “sharing economy” services to understand the potential impact of frictionless access on business growth.

*“Who would have thought hailing a cab would be so easy, or staying in a stranger’s house so affordable? These are all new experiences, and their success is based on transactions being invisible to the customer,”* said David Clarke, PwC’s Digital Services and Experience Center Leader. *“New experiences are co-dependent on new ways of thinking about cybersecurity. Teaming these diverse talents at the inception of an idea is critical to the speed at which we can execute.”*

Authentication technologies not only help quicken the pace of product roll out, but they also help bolster overall data security. In fact, 46% of organizations that employ advanced authentication say the technology 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.

**60%**   
**of respondents who use managed security services tap their service providers to handle identity and access management**

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

As security perimeters dissolve and identity expands from people to connected devices, identity and access management (IAM) tools are more essential than ever to protect access and prevent incursions.

*“Identity has been at the heart of most every breach in the past two years,”* said Richard Kneeley, PwC US Managing Director, Cybersecurity and Privacy. *“Many of these breaches have involved someone gaining access by using compromised identity, then changing their identity once inside the network to ratchet up access to data and systems by taking over a privileged account and in the process gaining unlimited access to the network, to systems and to data.”*

While the number of organizations that have deployed IAM solutions has remained stable at about 50% in recent years, we’re seeing a trend toward adoption of cloud-based identity services. Among organizations that use managed security services, 60% say they have tapped service providers to handle their IAM programs. One of the key reasons is that clients typically find it difficult to hire and retain the skills needed to run an IAM system. IAM in the cloud often comes with trained operators and engineers who run the service.

Another trend lies in adaptive authentication. As IT systems capture increasingly more information, businesses are starting to leverage additional data points to identify suspicious behaviors and patterns. Adaptive authentication uses data such as the user’s login time and location, patterns of access and type of device to create a risk-based access decision. If the application detects aberrant activity during a login attempt, it can require further authentication steps or halt the process altogether.

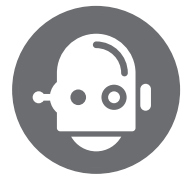


There is no off-the-shelf solution for adaptive authentication. Instead, it combines existing tools such as security information and event management (SIEM) to create a risk profile. *“You can’t implement adaptive authentication if you don’t have good security tools in place because it lives off security systems and the data they produce,”* said Kneelely. *“So adaptive authentication takes identity to a new level while also enabling businesses to gain additional value from existing technologies. That’s a great opportunity for CISOs because it allows them to say, ‘You gave me a million dollars to solve one problem, and I used it to also improve and get greater value from our previous investments’.”*

Truly forward-thinking businesses are beginning to combine adaptive authentication techniques with artificial intelligence (AI) and machine learning to build predictive authentication mechanisms. The use of predictive variables can make authentication a continuous event tied to the risk associated with the specific access attempts. Doing so can significantly improve the end-user experience while increasing the level of security and trust.

It’s no wonder, then, that 23% of survey respondents say they plan to invest in artificial intelligence and machine learning over the next 12 months. That’s an impressive buy-in considering that these technologies were considered the stuff of science fiction not too long ago.

**23%**  
*plan to invest in  
artificial intelligence  
and machine  
learning this year*



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

## ***What cloud-based threat intelligence looks like***

To date, few businesses have successfully implemented an integrated cloud-based threat-intelligence and information-sharing platform. In part, that's because some of the component technologies are just now becoming accessible to businesses. But enterprise-wide threat management is also an enormously complicated puzzle to piece together on premises, one that can easily stretch technology and resource capabilities.

That's starting to change, however as cloud-based technologies mature and deliver new levels of service. *“This year, we have figured out how to use technology to ingest massive amounts of unrelated information and find the relationships that make information understandable,”* said Burg.

PwC has, in fact, harnessed technology advances to design and develop a new cloud-based cybersecurity solution called Secure Terrain.™ Powered by the Google Cloud Platform, Secure Terrain™ empowers businesses to scrutinize activity across the enterprise to help strategically manage cybersecurity risks and protect critical assets.





To do so, the centralized solution leverages scalable machine learning techniques and enterprise-class cloud technology to rapidly aggregate and analyze enormous volumes of structured and unstructured data. It correlates this data with a massive global database of threat intelligence to identify threats in real time and prioritize responses based on impact to the business. The Secure Terrain™ solution is supported by PwC's global Terrain Operations Centers (TOCs), which provide security monitoring and support that go beyond the alerts, including hunt team analysis, threat research and remediation.

PwC has also addressed the other aspect of the challenge: an integrated threat-sharing platform, Terrain Intelligence that aggregates threat intelligence sources into a single, searchable location. The use of Google's data centers and high-speed global fiber backbone allows for almost instantaneous analysis and correlation of indicators of compromise—which can provide an invaluable time advantage when businesses are in the thick of managing cybersecurity incidents.

### ***The power of a centralized platform***

The architectural and operating advantages of the cloud model enable service providers to deliver powerful, centralized threat management and information sharing.

An integrated cloud solution has the compute and storage capability to ingest and analyze open and closed data, as well as commercial sources of threat indicators. It also has the horsepower to monitor enterprise-wide network and user data for unusual activity to detect potentially dangerous, but previously unknown, anomalies.

To yield maximum value, threat intelligence must be actionable. That means the information must be appropriately prioritized, highly accurate and meaningful to the business—and delivered in real time. When actionable intelligence is shared, it can enhance the defenses of an individual business and ultimately improve the defense of an entire ecosystem, be it an industry, peer group or a geographically oriented organization.

Once a threat is detected, the threat-management system should prioritize responses by factoring in business context to help expedite support to the parts of the business that will be most affected. Doing so will require a database of relevant information—such as asset inventories, sensitive data types and infrastructure—to intelligently filter, prioritize and contextualize threats.

The complexity and scope of real-time threat management may require the expertise of an ASOC, which can employ sophisticated, cloud-powered analytic techniques to deliver rapid insights into cyber-risks. ASOC teams do so by providing real-time, 24/7 monitoring as well as targeted searches and analytics on an organization's historical security data.

After a threat intelligence solution has been designed and deployed, businesses often find it a challenge to operate and continually improve the system. Increasingly, they are turning to managed security services to help monitor the digital ecosystem, respond to incidents and share threat.

Managed security services can also help businesses address two other ongoing challenges: The global shortage of skilled cybersecurity workers and perennial budget constraints. The cybersecurity talent squeeze, in particular, is likely to drive more organizations to turn to third parties for help running some or all of their security programs.

It is also likely to change the business case for managed security services. *“We think there’s a market that is focused on the difference between the talent that exists in an organization and low-cost routine managed services,”* said O’Hara. *“We see a new model for managed services that provides value-add to a business and access to talent that companies cannot employ full-time on their payroll.”*

In other words, managed security services is an outsourcing model that may redefine how businesses operate their cybersecurity and privacy programs.

## ***Tapping into a network of information-sharing resources***

By now, one thing seems certain: Cybercriminals do a very good job of networking with one another to share technical knowledge, tools and methodologies.

As cyberthreats become increasingly sophisticated, many organizations are taking a cue from their adversaries: They are sharing critical threat intelligence with business peers, industry groups and government agencies to collectively advance cybersecurity capabilities.

*“Information-sharing programs really began to ramp up in 2016,” said Burg. “Various business groups, state and local organizations as well as very sophisticated industry groups rallied in extraordinary ways to share threat information with one another and solve this problem together.”*

The advantages of a unified front against cybercriminals are many. Collaboration and information sharing can enable organizations to gain actionable visibility into their most relevant risks, understand the motives and tactics of adversaries and shed light on the most effective response methods.

To achieve these benefits, an information-sharing platform will need to analyze activity, classify and validate threats, and push alerts in real time.

As noted above, it’s critical that the information is actionable: An information-sharing platform should deliver accurate, contextual intelligence about how threats impact an organization’s specific environment.

**55%**  
***collaborate with external partners to improve security and reduce risks***



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



As with any new platform that aims to be interoperable with multiple disparate systems, data types and organizations, there are considerable challenges. Chief among them is a lack of a unified framework, platform, and data standards for information sharing. While some organizations with advanced cybersecurity operations have implemented information-sharing platforms, most are not interoperable with those of governments and business peers.

And then there is the potentially massive volume of data, which can be overwhelming and downright unmanageable. *“Most organizations just end up with too much data coming in and they really can’t work out what to do with it,”* said Grant Waterfall, PwC’s US and Global Co-Leader, Cybersecurity and Privacy. *“This is where threat fusion centers and Advanced Security Operating Centers are absolutely critical to aggregate data and filter out false positives.”*

This year, 55% of survey respondents say they collaborate and share information with others to improve cybersecurity. Those that do report they gained actionable information from business peers and established Information Sharing and Analysis Centers (ISACs).

A new type of group, Information Sharing and Analysis Organizations (ISAOs), which aim to help businesses share threat information with one another and the public sector, is already



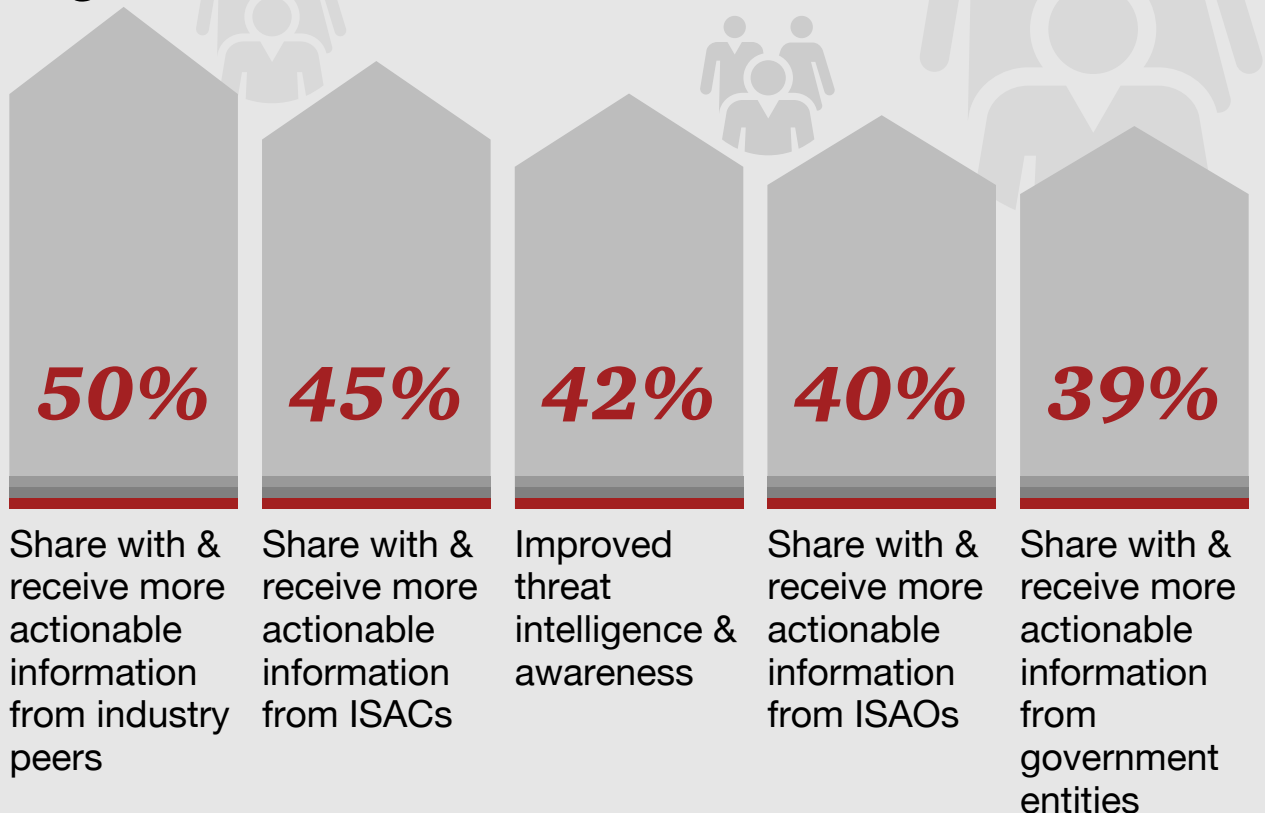
showing great promise. ISAOs had their start in February 2015, when US President Barack Obama issued Executive Order 13691 ([\*Promoting Private Sector Cybersecurity Information Sharing\*](#)) to encourage the creation of these organizations.<sup>1</sup>

Since then, numerous entities in the public and private sectors have formed ISAOs or have announced plans to do so. Examples include the Commonwealth of Virginia ISAO (see sidebar), The Legal Services ISAO, Retail Industry ISAO, The National Credit Union ISAO, and the Maritime & Port Security Information Sharing and Analysis Organization, among others.<sup>2</sup>

1 Whitehouse.gov, [\*Executive Order — Promoting Private Sector Cybersecurity Information Sharing\*](#), February 13, 2015

2 The ISAO Standards Organization, [\*Information Sharing Groups\*](#), accessed October 18, 2016.

## Impact of collaboration with external organizations



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



Similarly, the European Union recently approved a Network and Information Security Directive that lays out parallel objectives. The Directive, which was adopted in July, requires that member nations form a Computer Security Incident Response Team (CSIRT) and that businesses in critical infrastructures notify national authorities when cybersecurity incidents occur. It also mandates that businesses set up a cooperation group to facilitate sharing of information about risks.<sup>3</sup>

In the U.K., four large banks have formed the Cyber Defense Alliance to work with the UK National Cyber Crime Unit. This industry-government group aims to enable banks to swap timely information on cyberthreat intelligence and response techniques. One of the banks has also dispatched an analyst to Interpol's cybersecurity investigations unit in Singapore.<sup>4</sup>

---

3 European Commission, *The Directive on security of network and information systems (NIS Directive)*, accessed October 17, 2016.

4 Bloomberg, *Nothing Brings Banks Together Like a Good Hack*, October 18, 2016





## *How ISAOs improve prospects for information sharing*

ISAOs present a new opportunity for businesses to band together and better understand the threat landscape, make more informed investments to address the most significant cyber-risks and rapidly adjust security controls to address emerging threats. The resulting improvements in cybersecurity could increase the cost of doing business for hackers in a way that benefits an entire economy. ISAOs provide a uniquely powerful model for cybersecurity information sharing, with the following potential benefits:

- Creating a trusted and connected network that, significantly strengthens an individual organization's capabilities for identifying and mitigating cyber-risks.
- Quickly delivering, actionable cyberthreat intelligence to support measurable cybersecurity improvements.
- Lowering cost and barriers of entry for cybersecurity information sharing.
- Enhancing and simplifying cybersecurity information management, analysis and intelligence.
- Qualifying members for legal protections from certain liability, anti-trust and regulatory enforcement actions.
- Helping meet or exceed regulators' rising expectations for cyber-risk mitigation at a time in which company executives are increasingly held accountable for breaches.
- Transforming business models for information sharing to increase economies of scale.

The private sector recently developed voluntary guidelines for ISAOs that could help transform the way industry and government manage cyber-risks. The [new guidelines](#)—drafted by industry stakeholders, including PwC—provide Boards and executives with tangible recommendations for establishing successful ISAOs. The guidelines appear in four substantial documents:

- [ISAO 100-1: Introduction to ISAOs](#)
- [ISAO 100-2: Guidelines for Establishing an ISAO](#)
- [ISAO 300-1: Introduction to Information Sharing](#)
- [ISAO 600-2: US Government Relations, Programs and Services](#)







## ***A state of pioneering cybersecurity***

The Commonwealth of Virginia announced the formation of a state-level ISAO in April 2015, making it one of the first US states to do so.<sup>5</sup> It was also the earliest state to implement the US NIST Cybersecurity Framework, which specifically encourages the sharing of cyberthreat information to enhance security.<sup>6</sup>

More recently, Virginia established a public-private working group with the Virginia State Police to address the potential for cyberattacks on connected automobiles.<sup>7</sup> The working group comprises stakeholders from federal and state government agencies, academia and private-sector cybersecurity companies. It aims to help officials understand how to detect and prevent cybersecurity attacks on vehicles and other consumer devices.

Virginia has also taken the lead in implementing a threat-intelligence solution from a cybersecurity solutions provider. The commonwealth holds a vast trove of personally identifiable information (PII) of residents, including birth and death records, tax returns and health information. Last year state officials noted an increase in incidents attributed to phishing attacks and employees. To mitigate these risks, Virginia implemented a threat-intelligence solution that enables it to monitor inbound and outbound traffic for suspicious activity and malware. The solution also helps security analysts safely execute and inspect advanced malware, zero-day threats and advanced persistent threat (APT) attacks.

This united front against malicious adversaries makes the commonwealth's motto—*Sic Semper Tyrannis* (Thus always to tyrants)—more fitting than ever.

5 Virginia.gov, [Governor McAuliffe Announces State Action to Protect Against Cybersecurity Threats](#), April 20, 2015

6 Virginia.gov, [Commonwealth of Virginia Cyber Security Commission: Threats and Opportunities](#), August 2015.

7 Virginia.gov, [Governor McAuliffe Announces Initiative to Protect Against Cybersecurity Threats](#), May 15, 2015



## ***Toward the future of threat intelligence***

Ten years ago, threat intelligence was limited to reactive prevention and analysis of only known threats. And there were plenty of unknowns: Among GSISS respondents that detected a security incident in 2008, 42% did not know the source of the incident. In recent years, that number has dipped below 10%.

Today, more organizations are implementing dynamic threat intelligence and information sharing to shift cybersecurity and privacy capabilities from reactive to proactive. They understand that they can build business advantages and customer trust by better visibility into specific threats—and sharing that information with private- and public-sector entities.

In the near future, technologies that enable organizations to ingest and compare threat feeds in real time will continue to rapidly evolve, according to O'Hara. *“This includes technologies such as machine learning, artificial intelligence and Big Data analytics,”* he said. *“We believe that the application of data science to threat intelligence and security-incident management will be the future of how companies address threat intelligence.”*

That means threat intelligence will become increasingly predictive and will be able to better help thwart incidents before they occur. This discipline also will become more conducive to protection of consumer information as the Internet of Things takes off.

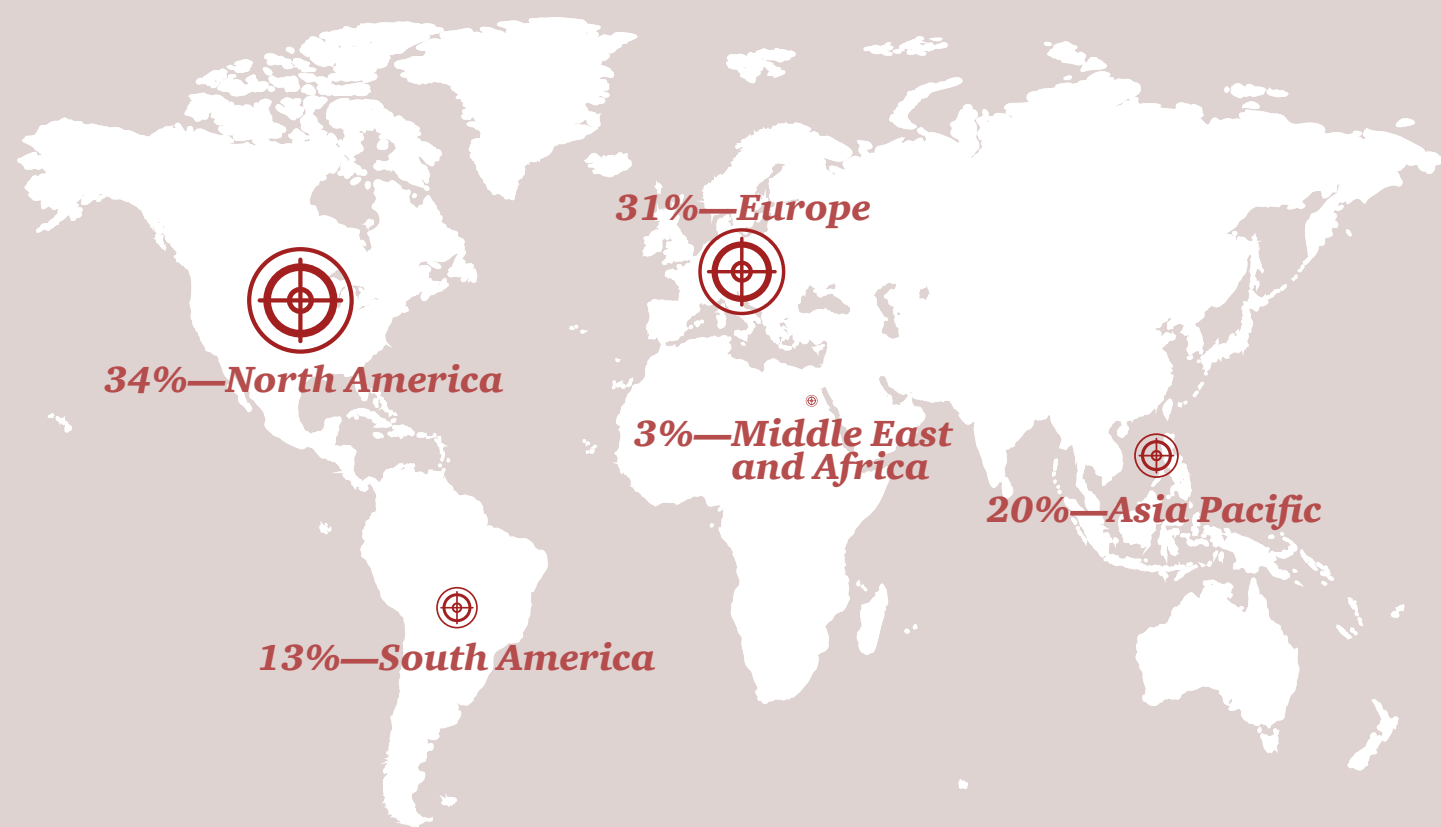
As for information sharing, new types of collaborative organizations will likely enable a more inclusive approach to distributing cyberthreat intelligence and deliver intelligence tailored to individual members. Access to actionable information can ultimately help enable continuous security improvements that benefit businesses, governments and individual users alike.

# 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

## ***Switzerland***

### **Reto Häni**

Partner and Leader

Cybersecurity

+41 58 792 75 12

reto.haeni@ch.pwc.com

### **Yan Borboën**

Partner Cybersecurity

+41 58 792 84 59

yan.borboen@ch.pwc.com

### **Mark Barwinski**

Director Active Cyber Defence

+41 58 792 20 89

mark.barwinski@ch.pwc.com





***www.pwc.ch/gsiss2017***

***www.pwc.ch/cybersecurity***

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 208,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at [www.pwc.com](http://www.pwc.com).

PwC has exercised reasonable professional care and diligence in the collection, processing, and reporting of this information. However, the data used is from third party sources and PwC has not independently verified, validated, or audited the data. PwC makes no representations or warranties with respect to the accuracy of the information, nor whether it is suitable for the purposes to which it is put by users.

PwC shall not be liable to any user of this report or to any other person or entity for any inaccuracy of this information or any errors or omissions in its content, regardless of the cause of such inaccuracy, error or omission. Furthermore, in no event shall PwC be liable for consequential, incidental or punitive damages to any person or entity for any matter relating to this information.

PwC will not disclose the name of any respondent without their prior approval and under no circumstances will PwC disclose individual entity data.

© 2016 PwC. All rights reserved. PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see [www.pwc.com/structure](http://www.pwc.com/structure) for further details.

229699-2017.2