www.pwc.com/cybersecurity

Key findings from The Global State of Information Security® Survey 2016

October 9, 2015

pwc

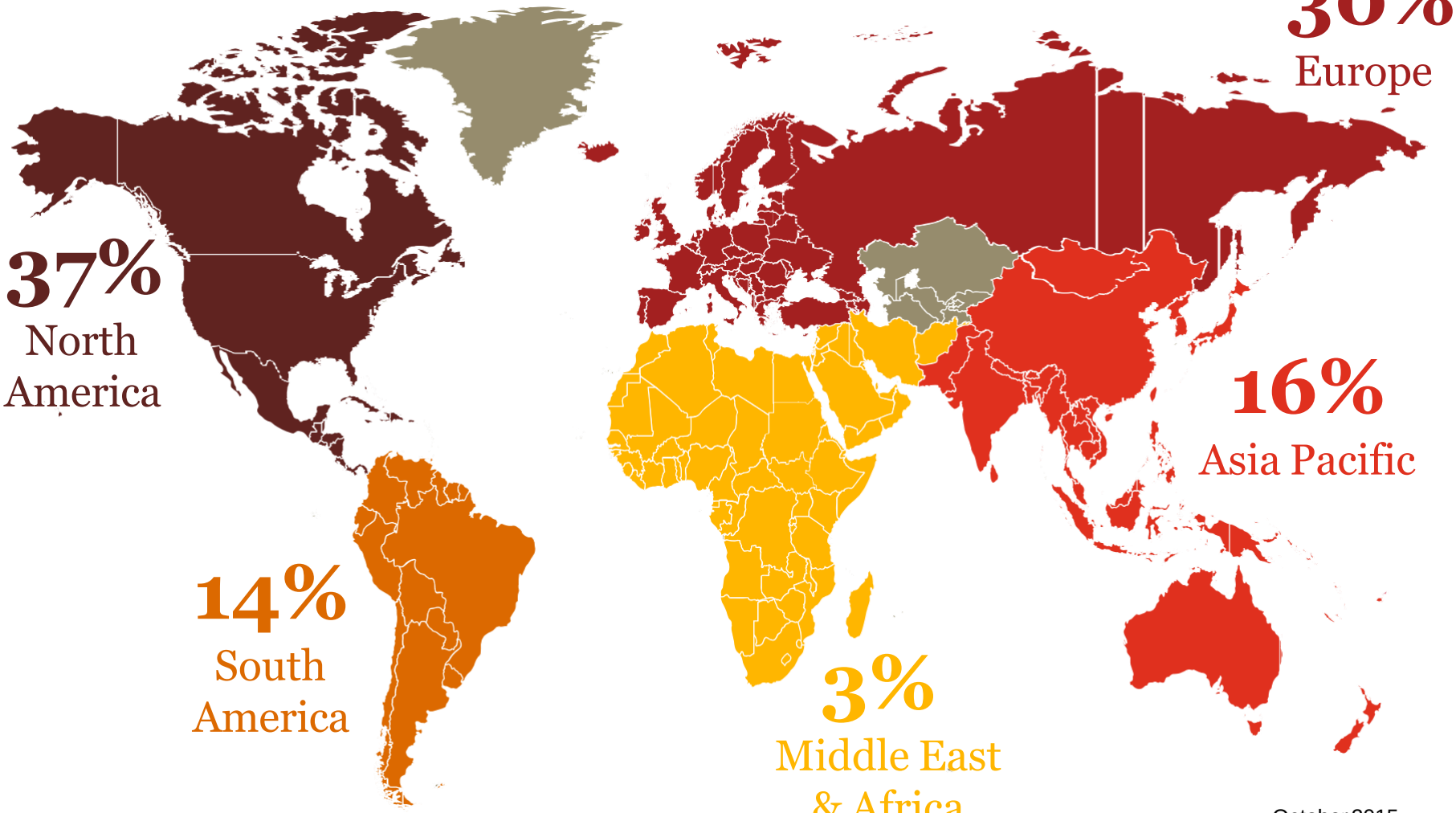
Methodology

- The Global State of Information Security® Survey 2016, a worldwide study by PwC, CIO and CSO, was conducted online from May 7, 2015 to June 12, 2015.
- PwC's 18th year conducting the online survey
- Responses from more than 10,000 CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security practices
- Forty-nine percent (49%) of respondents from companies with revenue of $500 million+
- More than 40 questions on topics related to privacy and information security safeguards and their alignment with the business
- The margin of error is less than 1%; numbers may not add to 100% due to rounding

The survey includes 10,000 respondents from 127 countries.

89 participants in Switzerland

Respondents by region of employment

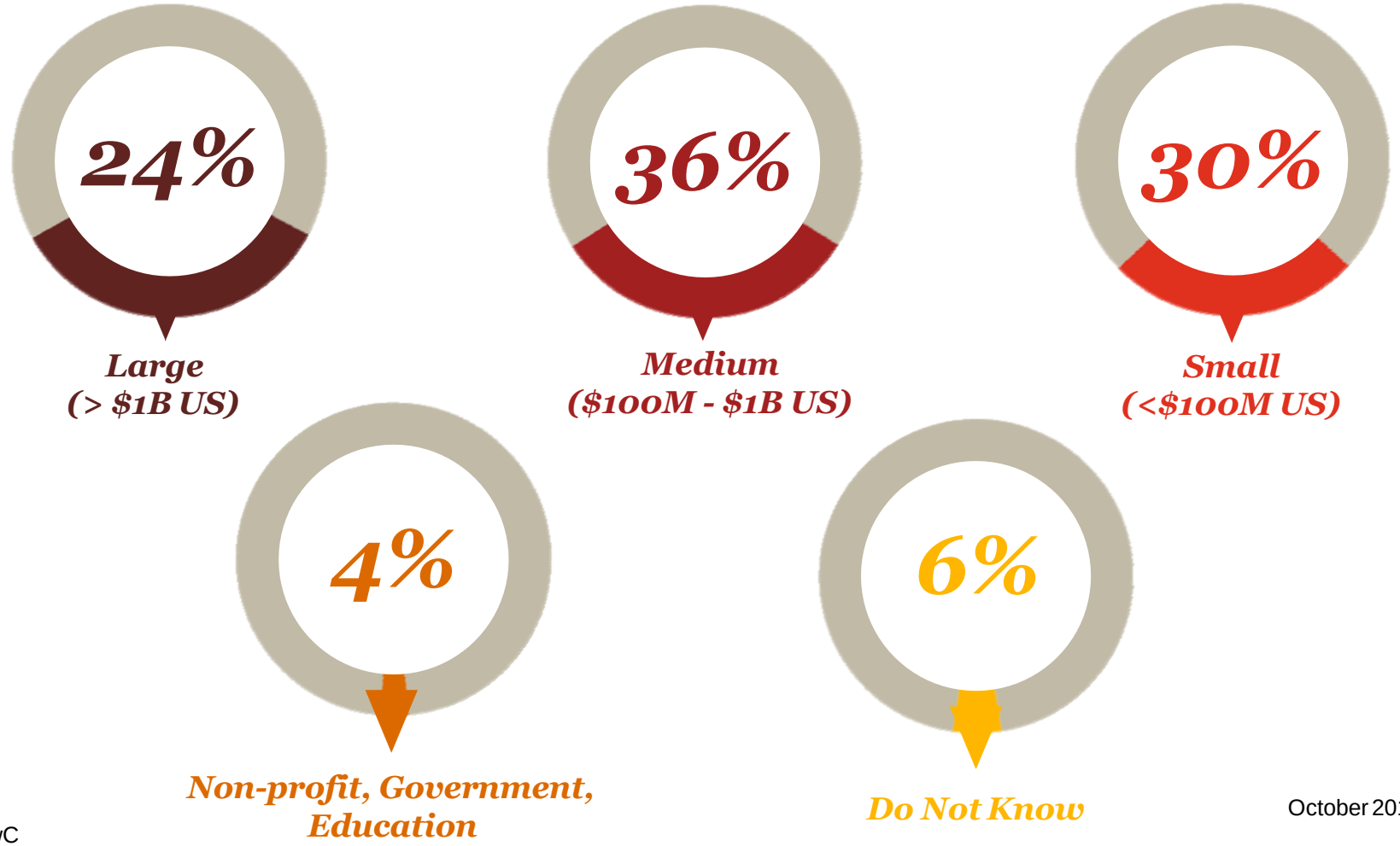


A mix of business and IT security executives are represented.

Swiss respondents by title

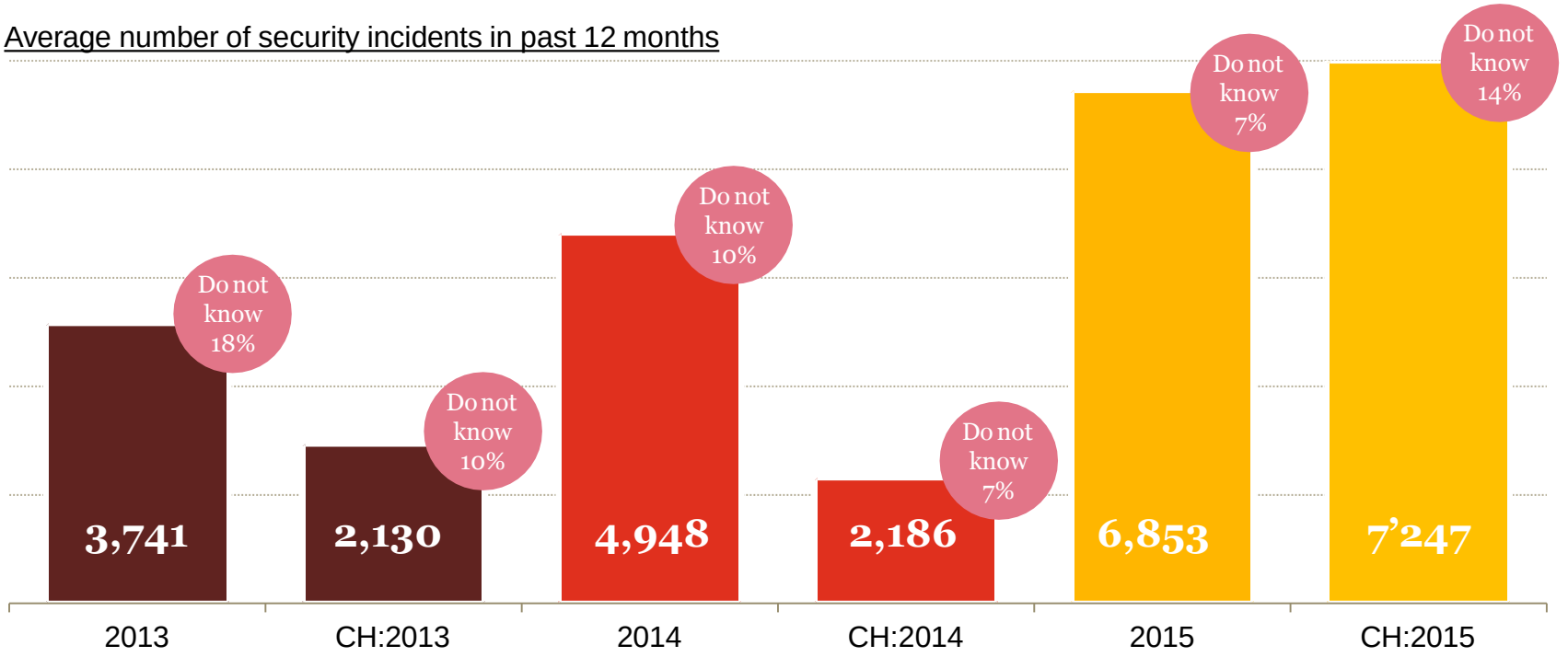
A balanced range of organization sizes by revenue.

Swiss respondents by company revenue size



*In 2015, Swiss respondents detected 330% more information security incidents.**

Swiss organizations reported a dramatic increase in incidents. Incident detection capacities improved between global and Swiss companies. It is troubling that respondents who do not know the number of incidents has doubled over two years. This may be due to continued investments in security products based on outdated models or on awareness of respondent.



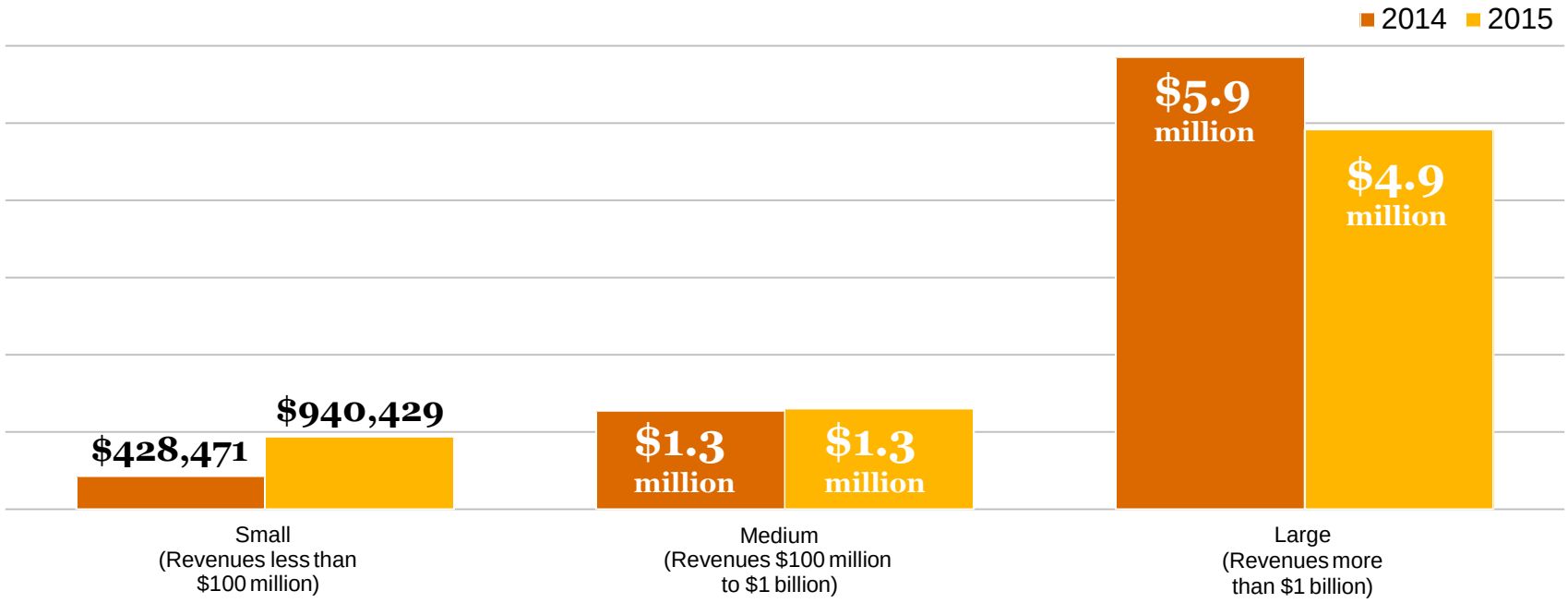
* A security incident is defined as any adverse incident that threatens some aspect of computer security.

Question 18: "What is the number of security incidents detected in the past 12 months?"

The financial costs of incidents more than doubled for small organizations.

Small companies reported a two-fold increase in financial losses attributed to security incidents, while large companies said losses dropped by 16% in 2015.

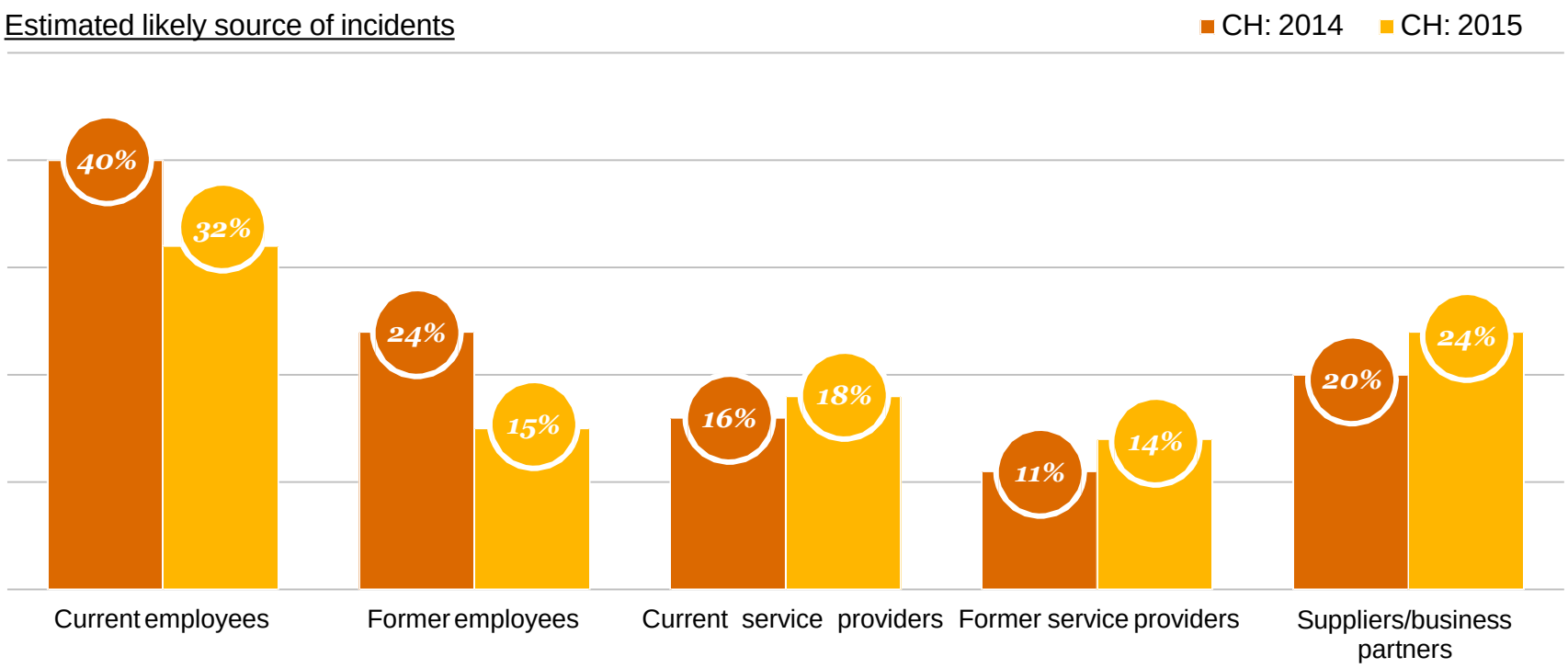
Average financial losses due to security incidents



Question 22a: "Estimated total financial losses as a result of all security incidents: (Please answer in US dollars)"
Question 4: "Please select the US dollar amount that best represents the annual gross revenues or operating budget for your corporation or organization, including all plants, divisions, branches, parents, and subsidiaries worldwide."

Employees remain the most cited source of compromise, but incidents attributed to business partners are up substantially.

Security events ascribed to current and former third-party partners jumped 20% over the year before, while those attributed to current and former employees decreased by 26%.

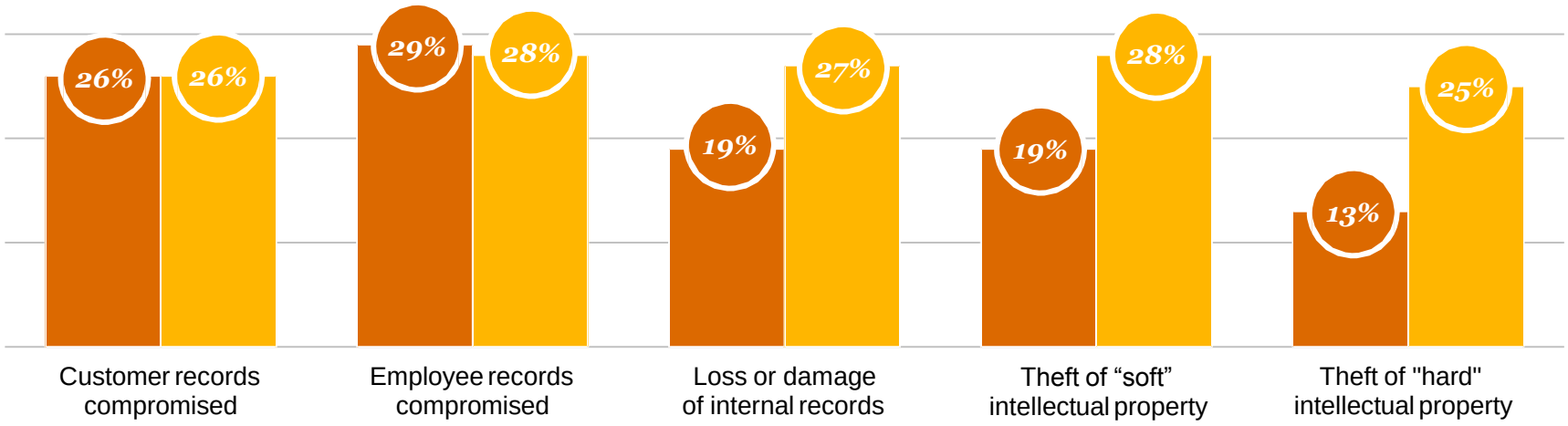


Question 21: "Estimated likely source of incidents" (Not all factors shown.)

Increasingly, organizations report that employee, customer, and internal data are primary targets of cyberattacks.

While compromise of customer records stayed stable, theft of “hard” intellectual property like strategic business plans and financial documents increased more than any other data loss (+92%).

Impact of security incidents

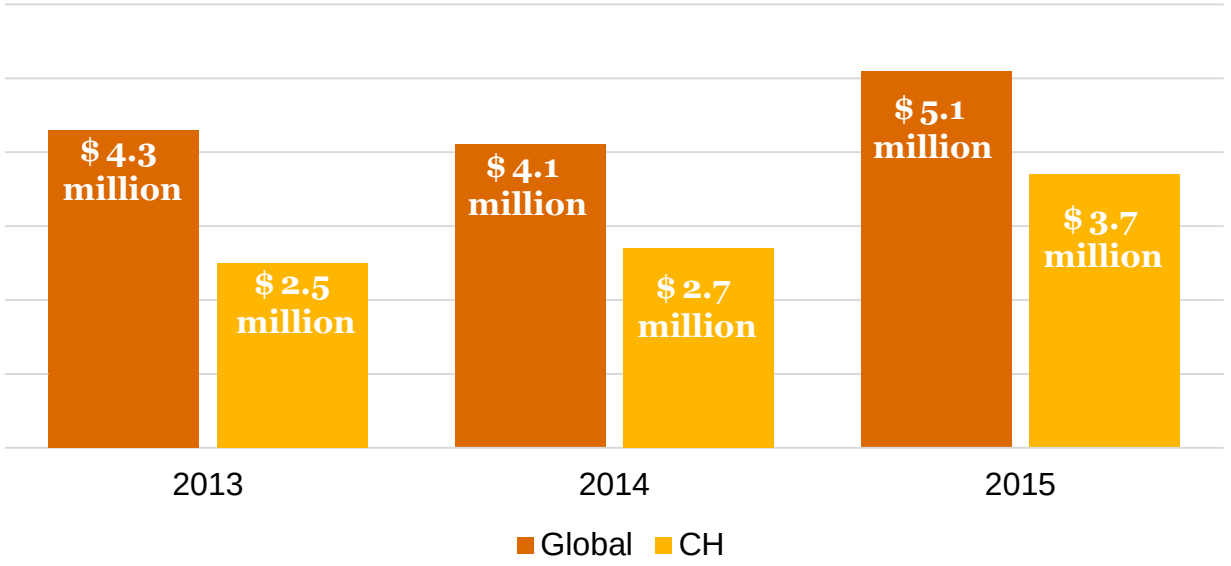


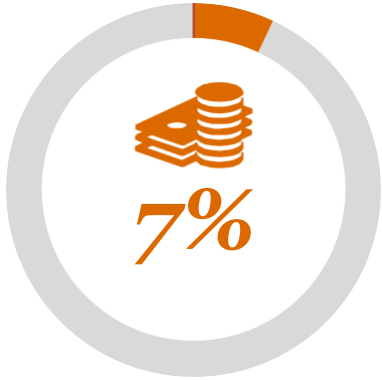
Question 22: “How was your organization impacted by the security incidents?” (Not all factors shown.)

*As risks rise, organizations significantly boost investments in information security.**

Security budgets average $3.7 million this year, a gain of 37% over 2014. Organizations understand that today's elevated threat landscape demands a substantial boost in security investment.

Information security budgets for 2013, 2014 and 2015





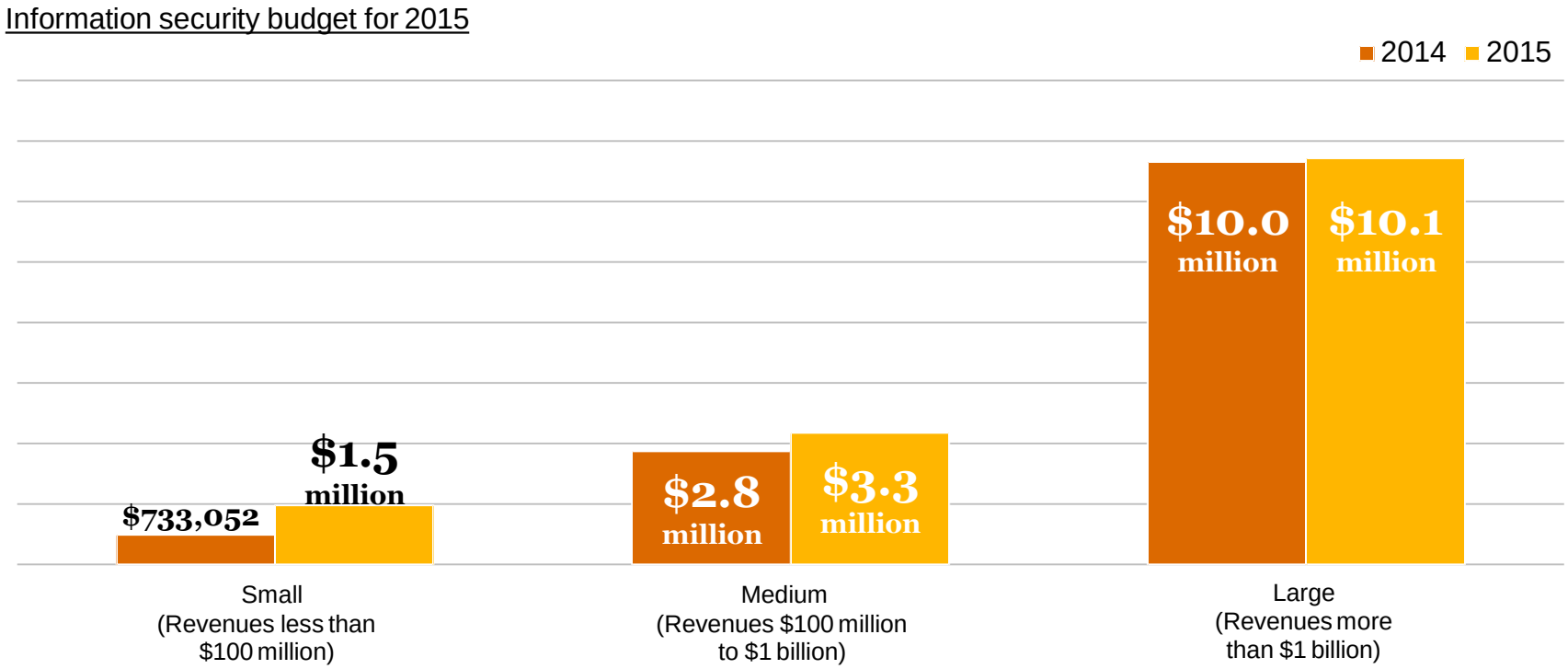
of IT budget spent on information security

* Information security budget refers to funds specifically and explicitly dedicated to information security, including money for hardware, software, services, education, and information security staff.

Question 7: "What is your organization's total information technology budget for 2015?"
Question 8: "What is your organization's total information security budget for 2015?"

Small companies take a decisive lead in expanding spending for security programs.

Small organizations doubled information security budgets in 2015, while large companies' spending has remained stable.

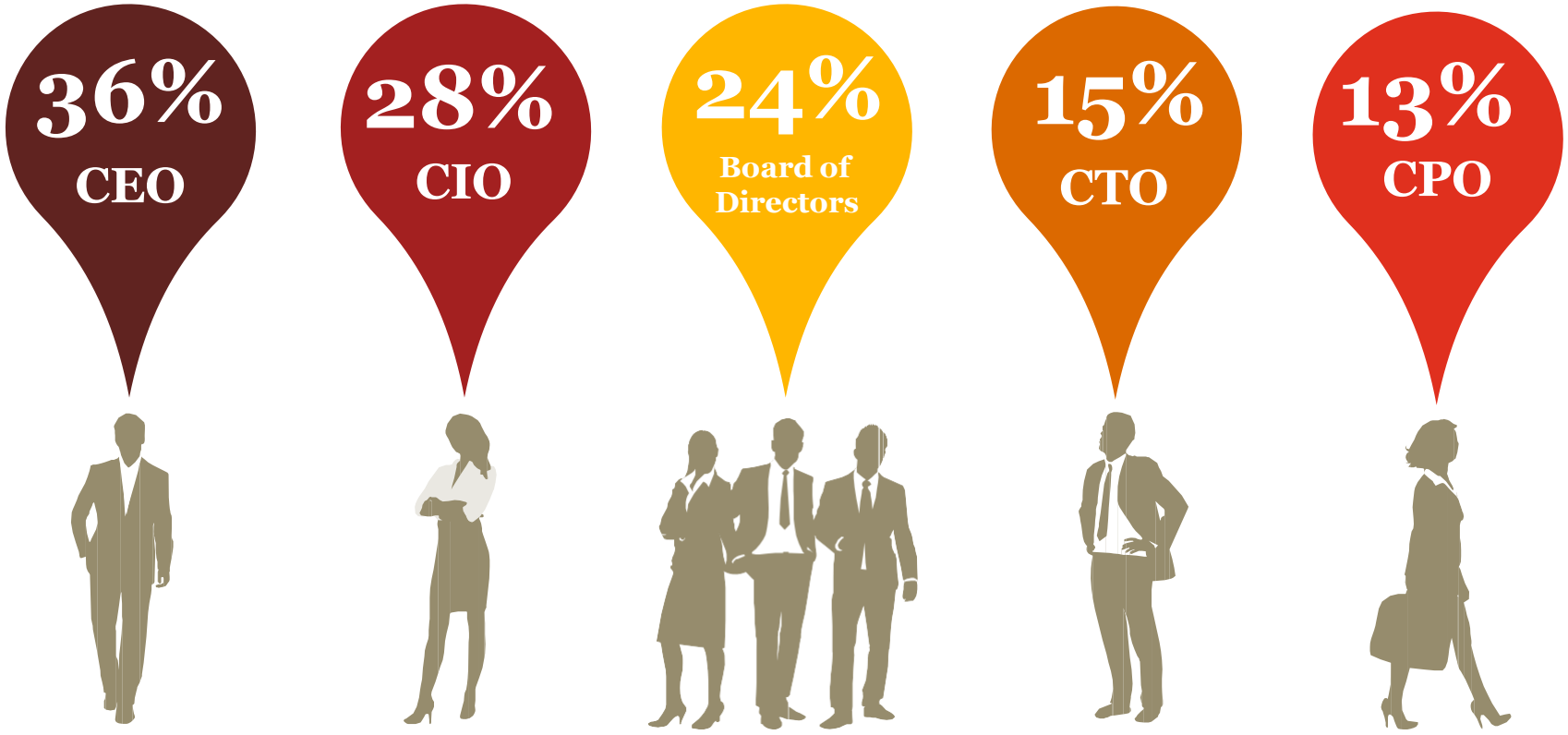


Question 8: "What is your organization's total information security budget for 2015?"

Among organizations that have a CISO or CSO, the security executive is most likely to report directly to the CEO.

More than half (51%) of respondents said they employ a CISO or CSO to oversee security.

Where the CISO/CSO reports (CH respondents)

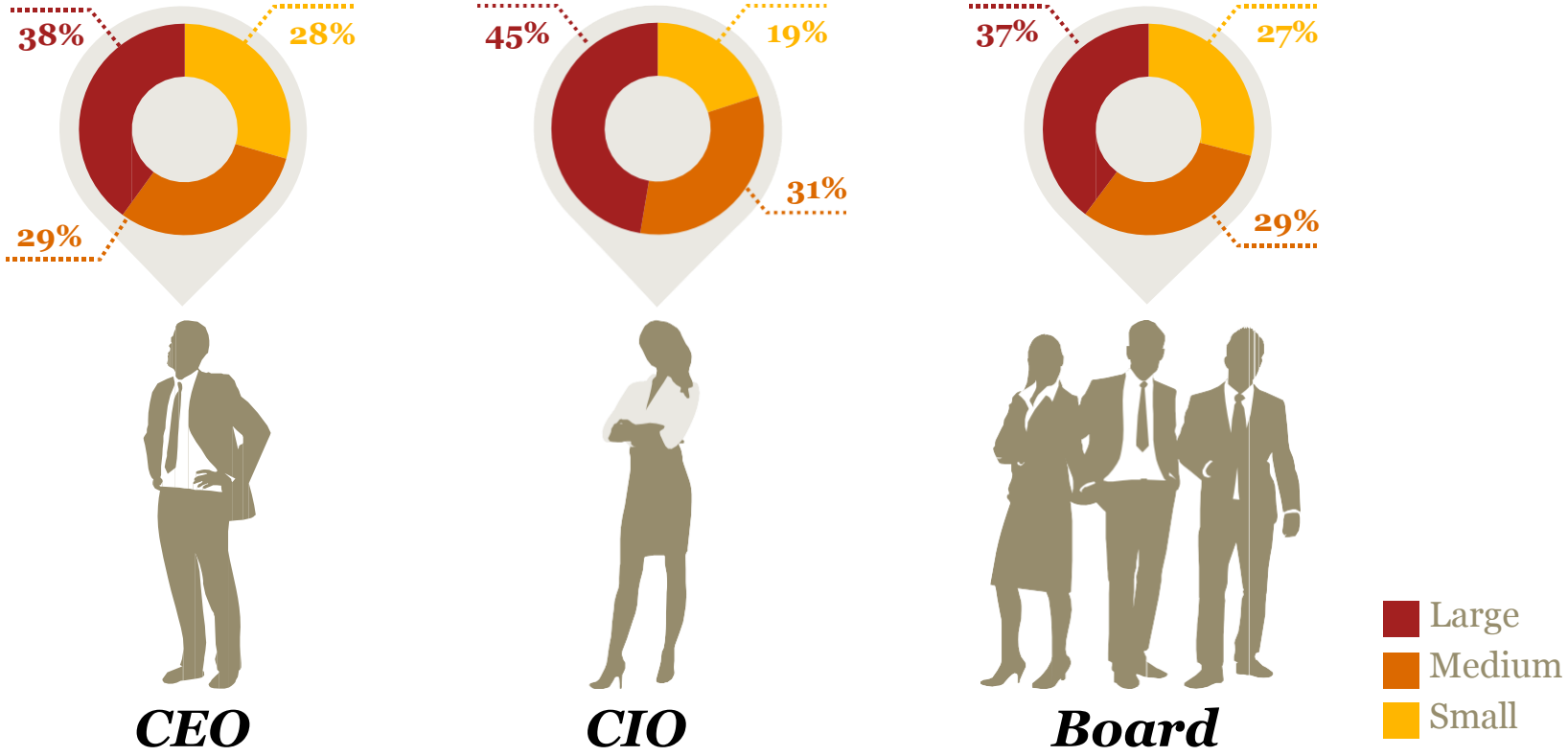


Q13a2015: "Where/to whom does the CISO, CSO, or equivalent senior information security executive report directly?"

In large businesses, the security function is often organized under the CIO.

Regardless of company size, however, CISOs and CSOs do still report directly to the CEO.

Where the CISO/CSO reports (by company size)

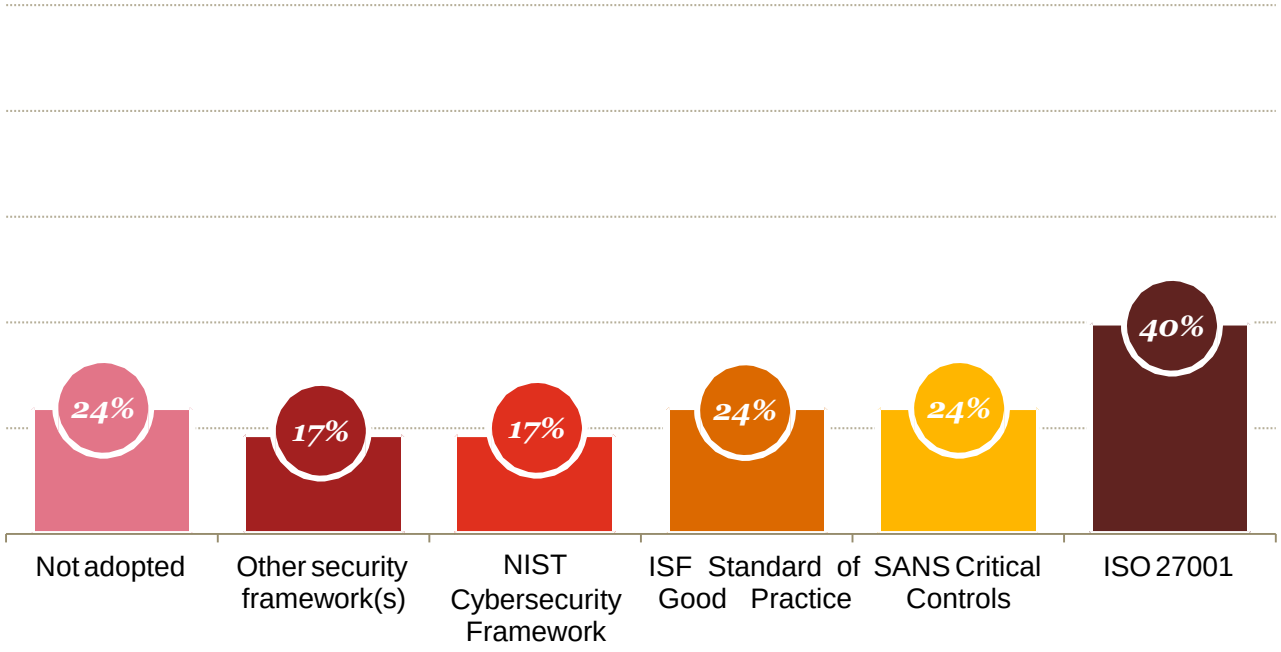


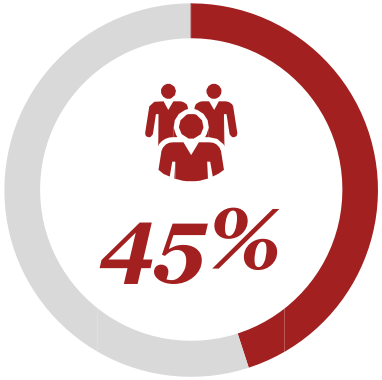
Q13a2015: "Where/to whom does the CISO, CSO, or equivalent senior information security executive report directly?"

Most Swiss respondents have implemented one or more risk-based information security frameworks.

A majority of organizations also say they collaborate with external industry partners to improve security and reduce risks.

Adoption of risk-based security frameworks

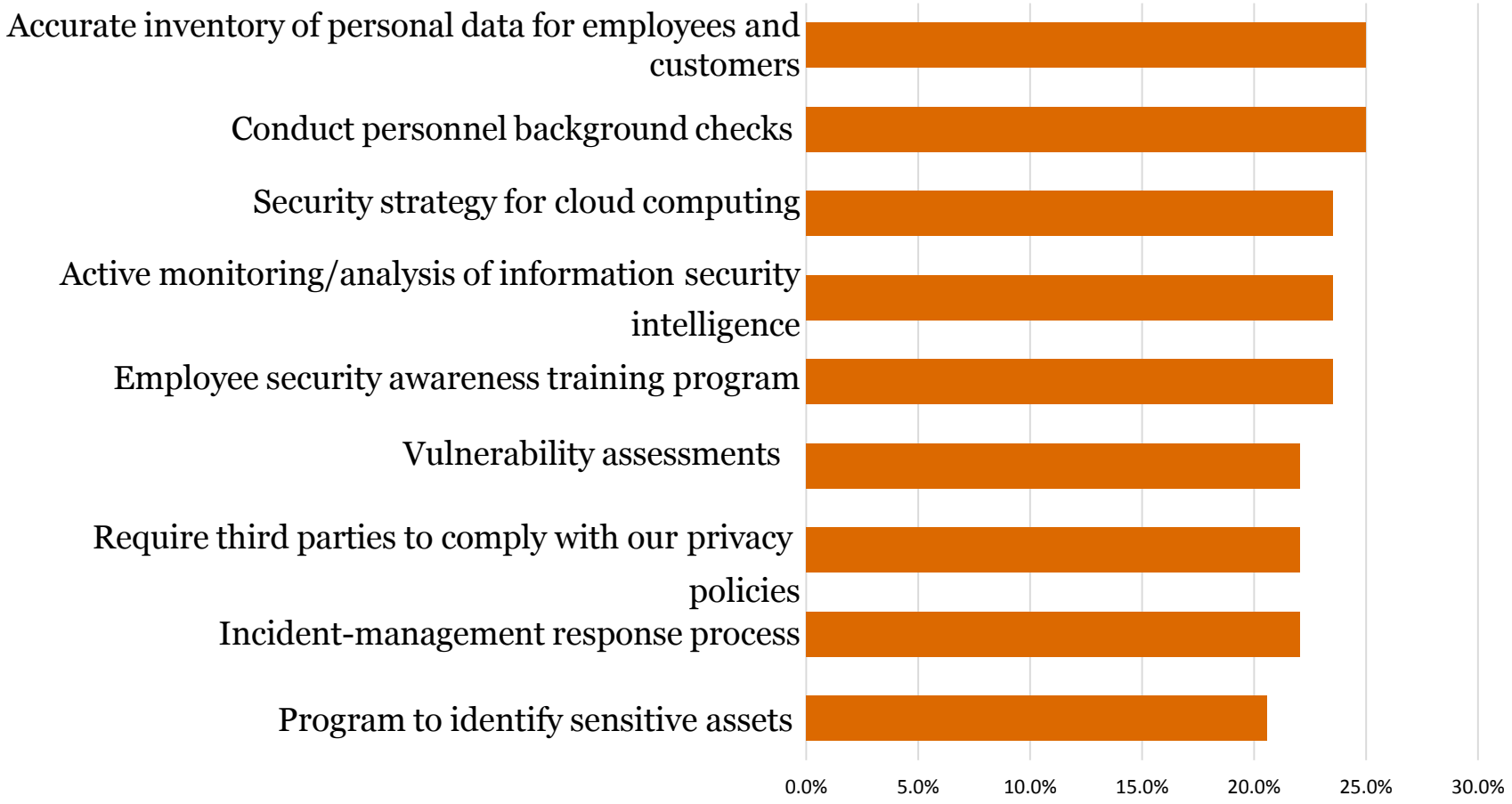




of respondents say they are better able to identify and prioritize security risks and investments

Question 22_2016: "Has your organization adopted a risk-based information security framework such as the NIST Cybersecurity Framework, ISO 27001, Information Security Forum (ISF) Standard of Good Practice, or SANS Critical Controls?"
Question 41: "Does your organization formally collaborate with others in your industry, including competitors, to improve security and reduce the potential for future risks?"

Swiss respondents will invest more in process and people over the next 12 months than in technology.



Q10c_2016 Which safeguards does your organization not have in place, but is a top priority over the next 12 months?

There is no "magic bullet" for effective cybersecurity, it is a path that starts with the right mix of technologies, processes, and people skills.

Based on our analysis of survey responses and PwC's experience in global security practices, the following are ten key strategies.

Essential safeguards for effective security	
1	Define an overall information security based on recognized security framework
2	Have a CISO /CSO in charge of Security
3	Perform internal and external risk assessments on privacy, security, confidentiality, and integrity
4	Identify your "crown jewels" and allocate and prioritize resources to protect them
5	Realize accurate inventory of where personal data of employees and customers is collected, transmitted, and stored, including third parties that handle that data
6	Implement strong technology safeguards for prevention, detection, and remediation
7	Conduct personnel background checks and employee security awareness training program
8	Have security baselines / standards for third parties
9	Conduct Threat assessments
10	Define incident-management response process

For more information on certain topics of our survey, please contact:

Yan Borboën
Partner Cyber security
Office: +41 58 792 8459
Mobile: +41 79 580 7353
Main: +41 58 792 8100
Email: yan.borboen@ch.pwc.com

Please reserve your time for our PwC Digital Trust Event on March, 15 2016

visit www.pwc.com/gsiss to explore the data further.