#RSAC

RSAConference2018

San Francisco | April 16 – 20 | Moscone Center

SESSION ID: STR-F02

KNOWLEDGE ASSETS, THEIR DEFENSE AND REGULATION – MAKING THEM WORK FOR YOU

Jon Neiditz
Partner & Cybersecurity/Privacy Lead
Kilpatrick Townsend & Stockton LLP
Study Co-Author

Will Bracker
Senior Director, Privacy
Cox Communications
Study Co-Author

Dr. Chris Pierson
Chairman & Founder
Binary Sun Cyber Risk Advisors
Moderator

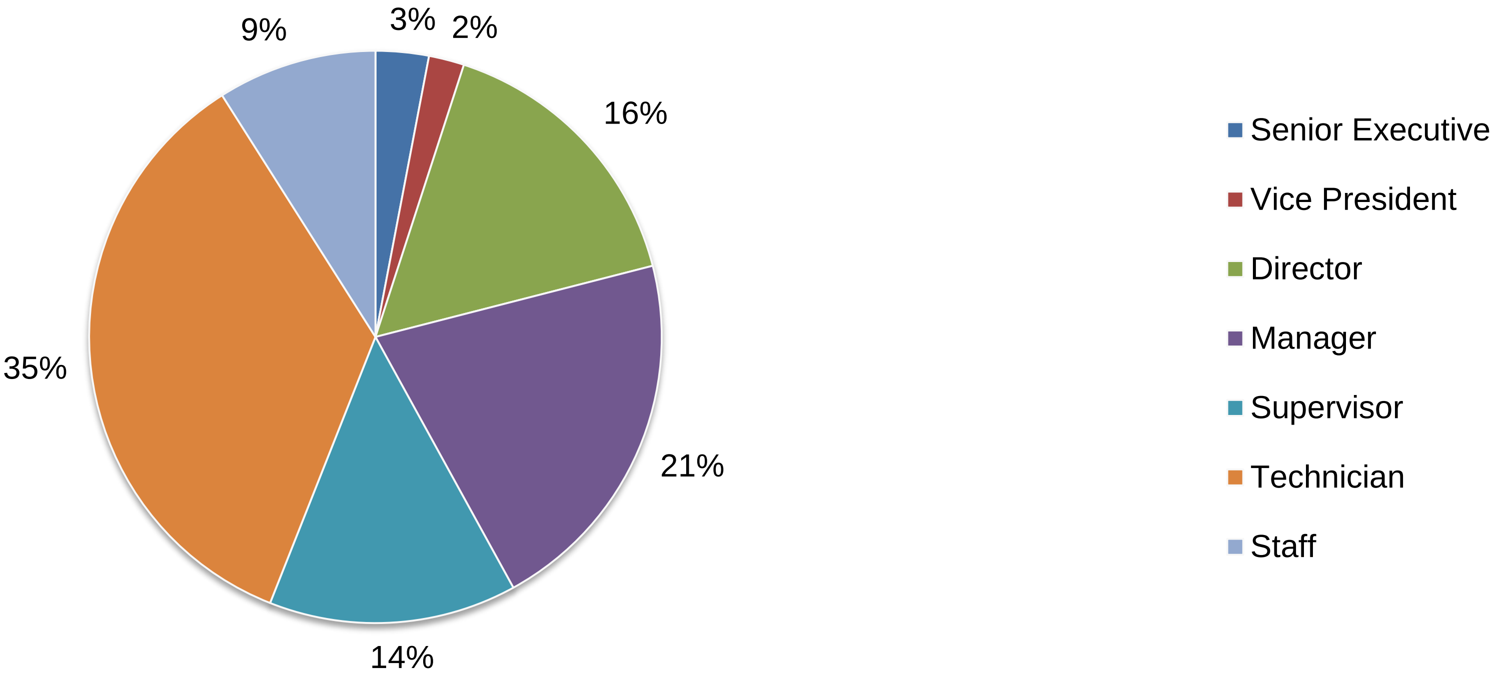
About this study

- The *Second Annual Study on the Cybersecurity Risk to Knowledge Assets*, produced by the Ponemon Institute and Kilpatrick Townsend, was done to see whether and in what ways organizations are beginning to focus on safeguarding "knowledge assets" (also often known as "crown jewels") in a period of targeted attacks on those assets.
- "Knowledge assets" are defined as confidential information critical to the development, performance and marketing of a company's core business, other than personal information that would trigger notice requirements under law. For example, they include:
  - trade secrets and corporate confidential information such as product design, development or pricing;
  - sensitive non-public information about the organization, its plans or relationships; and
  - competitively valuable or other important information of or about customers, including profiles.
- This presentation is about how the study provides practical guidance for successful advocacy and action toward securing knowledge assets.

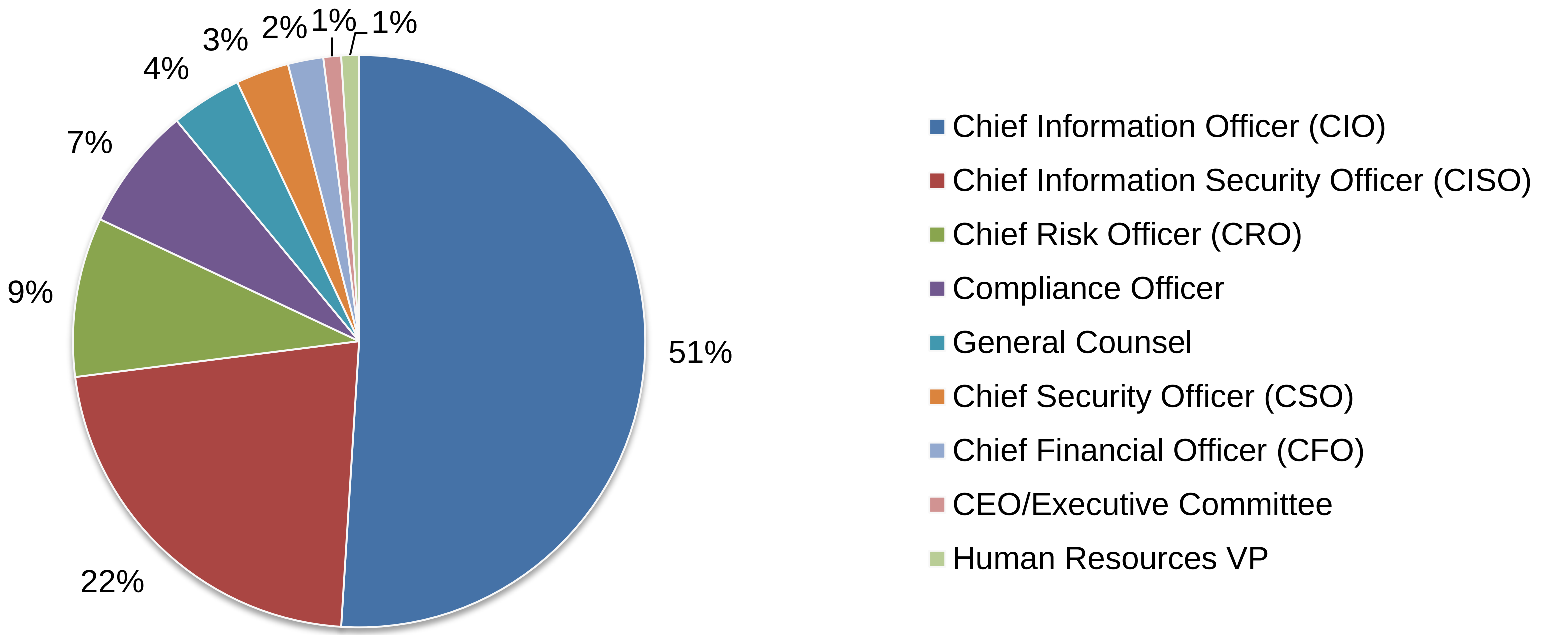
About our sample response

Sample response	FY2017	FY2016
Sampling frame	17,991	17,540
Total returns	709	691
Rejected or screened surveys	75	88
Final sample	634	603
Response rate	3.5%	3.4%

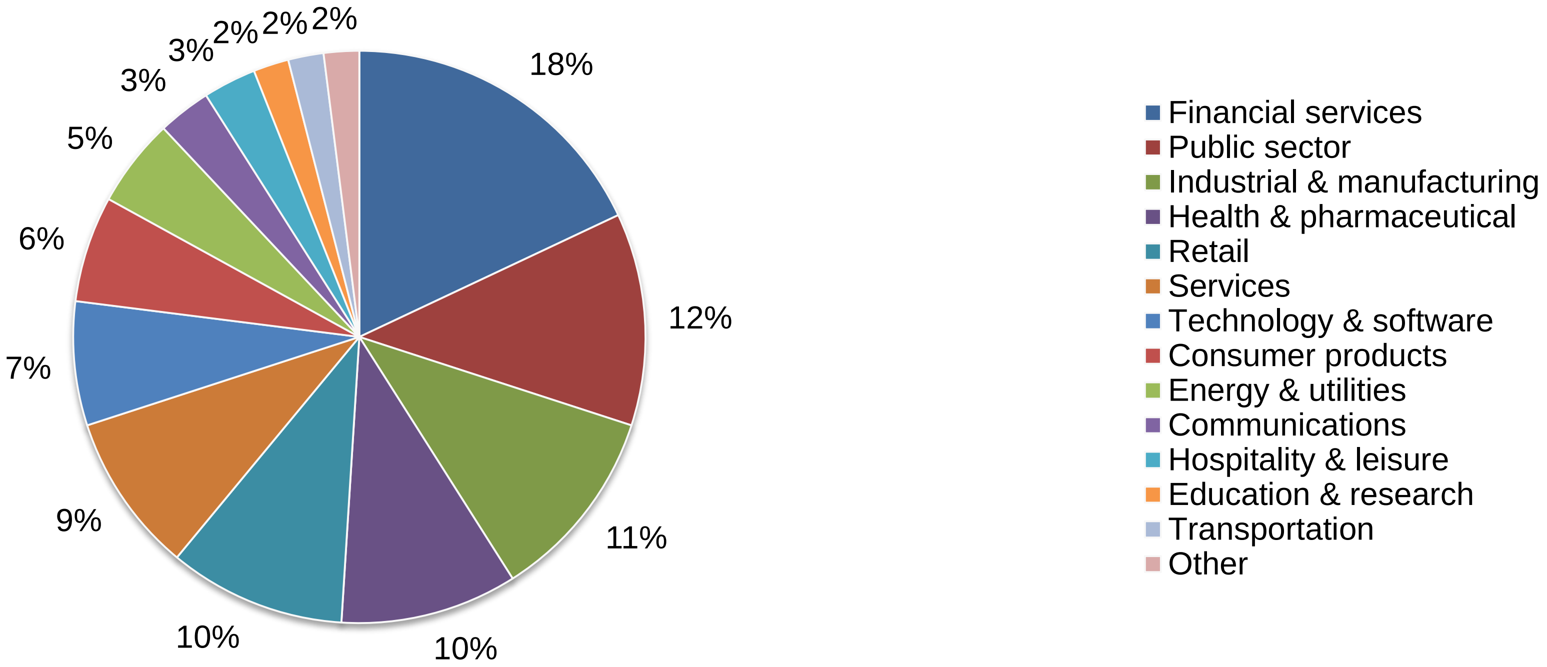
Current position within the organization



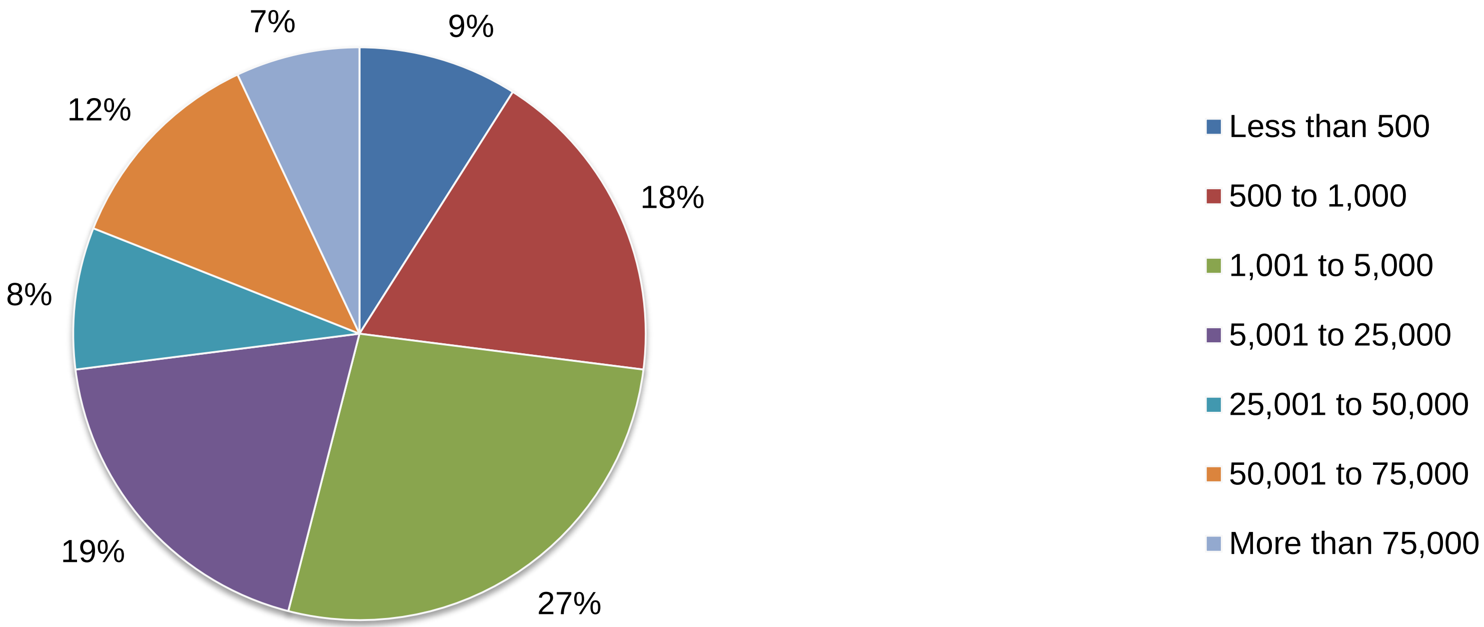
The primary person reported to within the organization



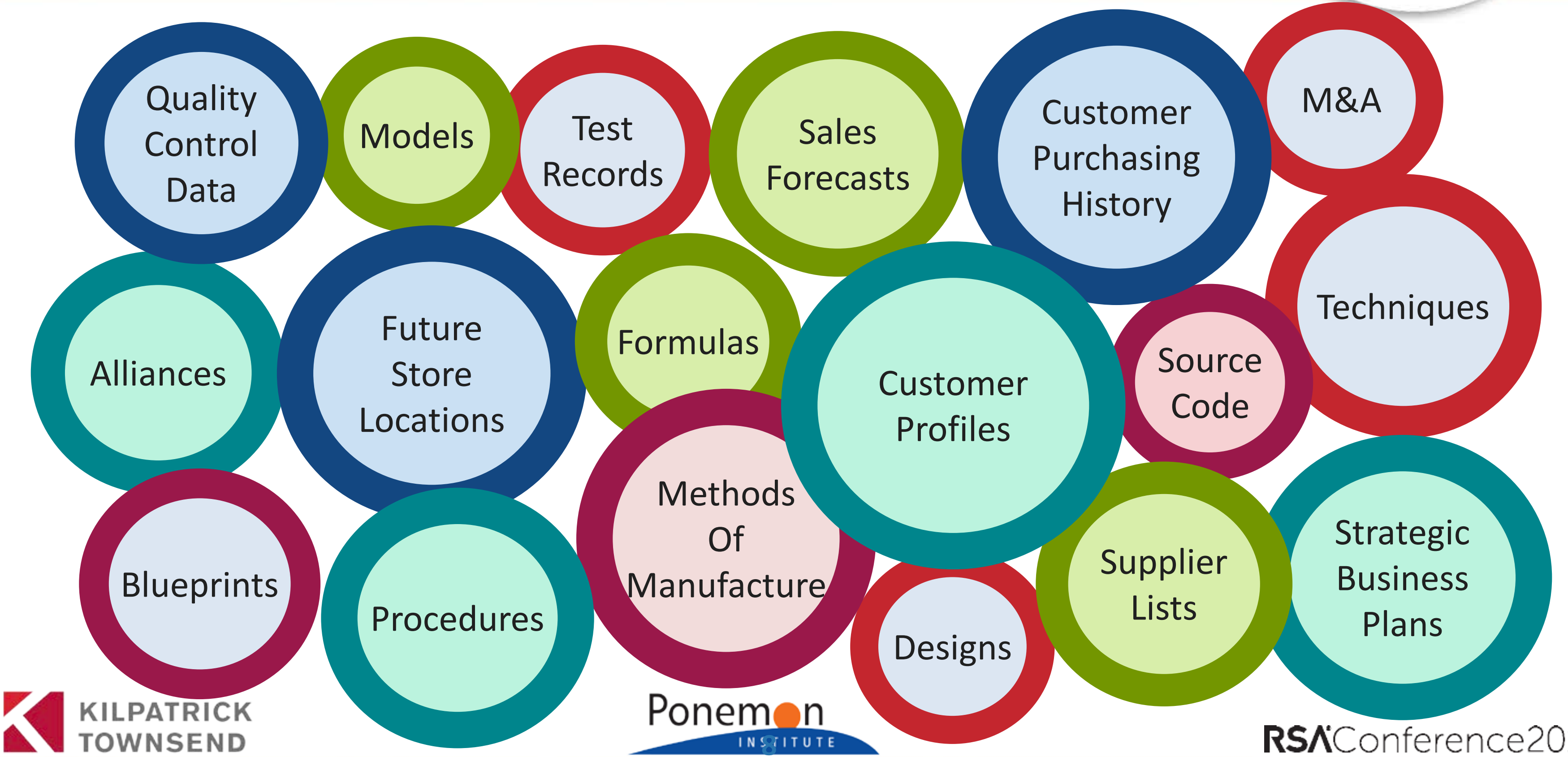
Primary industry classification



Worldwide headcount of the organization



What are your crown jewels?



Quality Control Data

Models

Test Records

Sales Forecasts

Customer Purchasing History

M&A

Alliances

Future Store Locations

Formulas

Customer Profiles

Source Code

Techniques

Blueprints

Procedures

Methods Of Manufacture

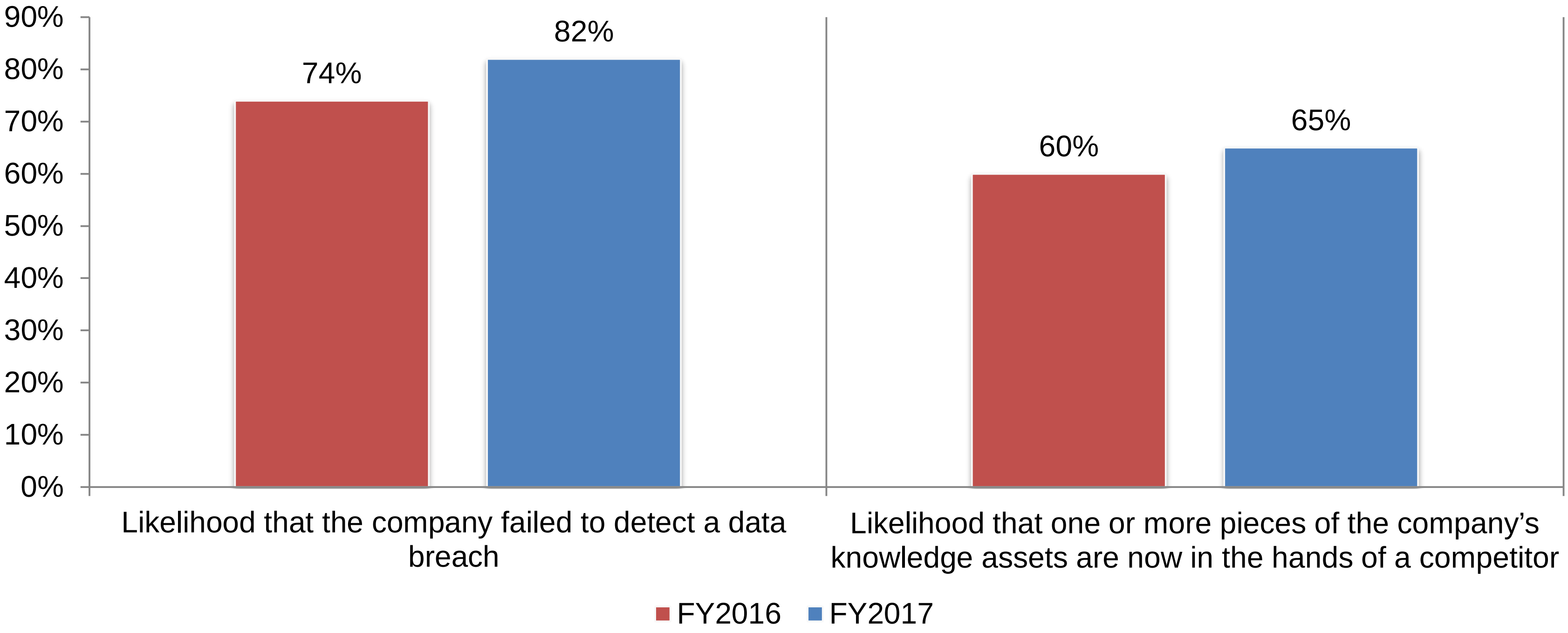
Designs

Supplier Lists

Strategic Business Plans

New study: Increased threats and awareness

Very likely and Likely responses combined



Evidence of the growing awareness of threats to knowledge assets

Boards of directors requiring assurances

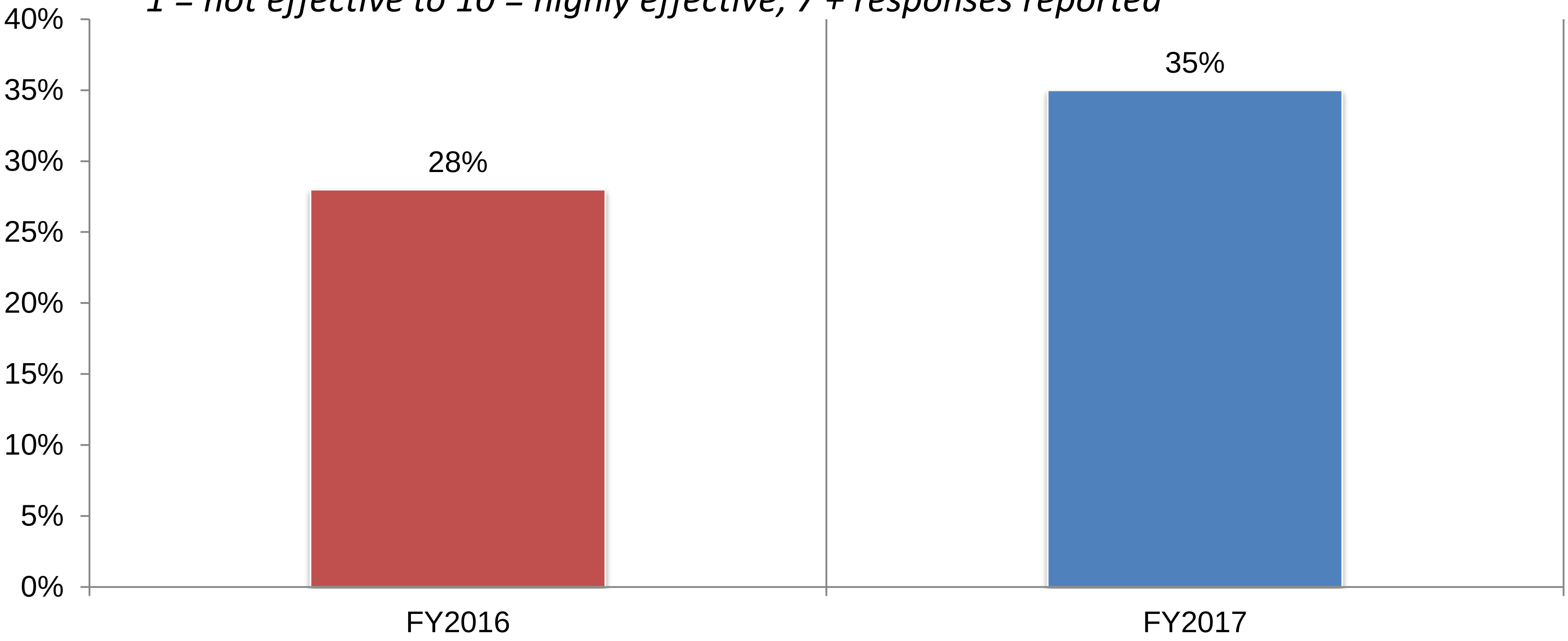
Integration into IT security strategy

Focus on **employee carelessness** and **third party access**

Clear trends in **technologies** to protect knowledge assets

Some more – but still few – consider their organizations good at this

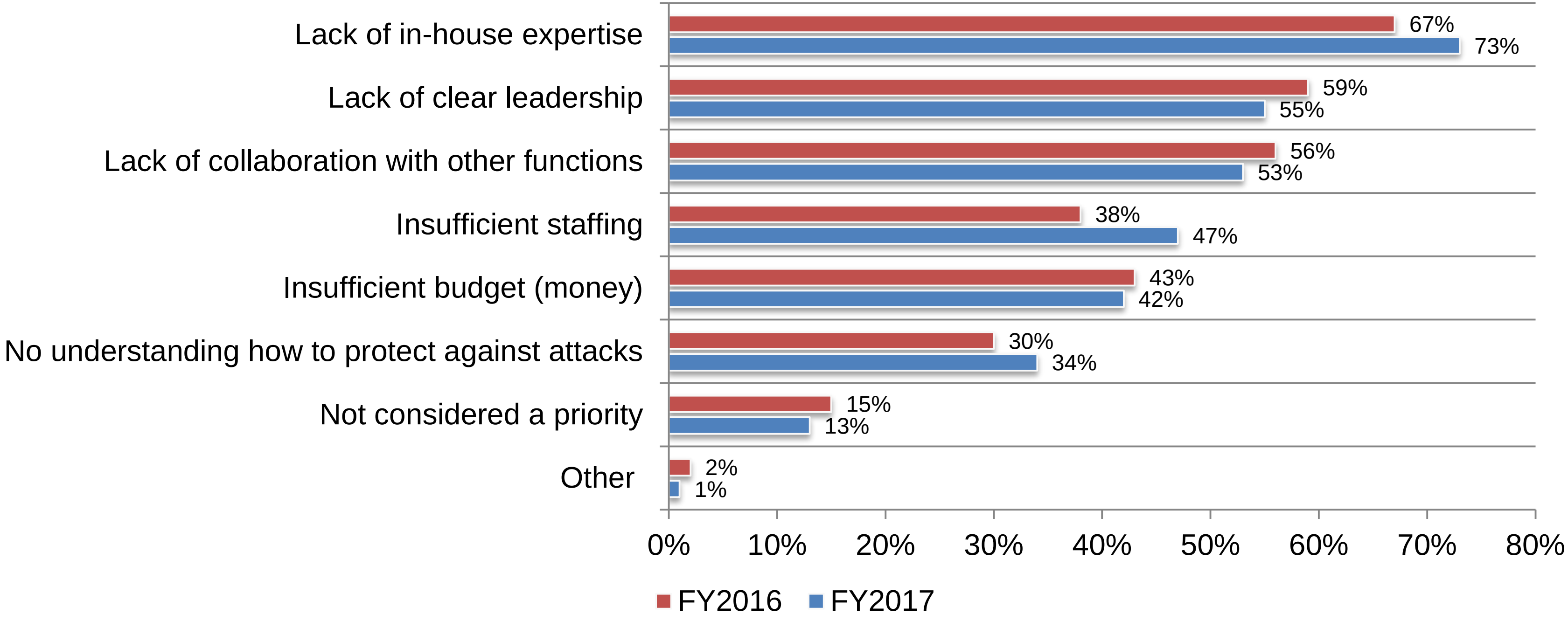
1 = not effective to 10 = highly effective, 7 + responses reported



For the 65% who don't think they've got this: What is holding your company back?

#RSAC

More than one response allowed



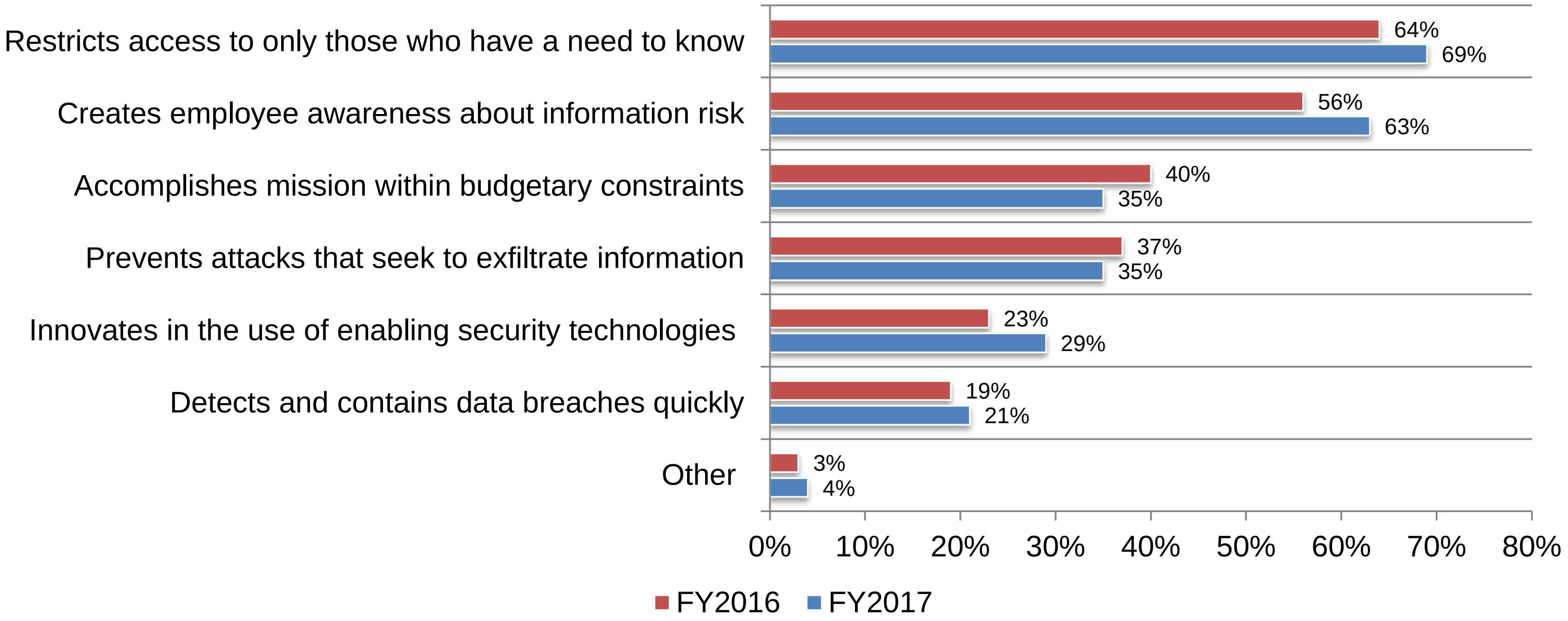
KILPATRICK TOWNSEND

Ponemon INSTITUTE

For the 35% who think their company is effective: Why?

#RSAC

More than one response allowed



KILPATRICK TOWNSEND

Ponemon INSTITUTE

The “high performers,” the 14% who rate their firms 9 or 10, are instructive:

Much greater attention by **senior management** and **the board**

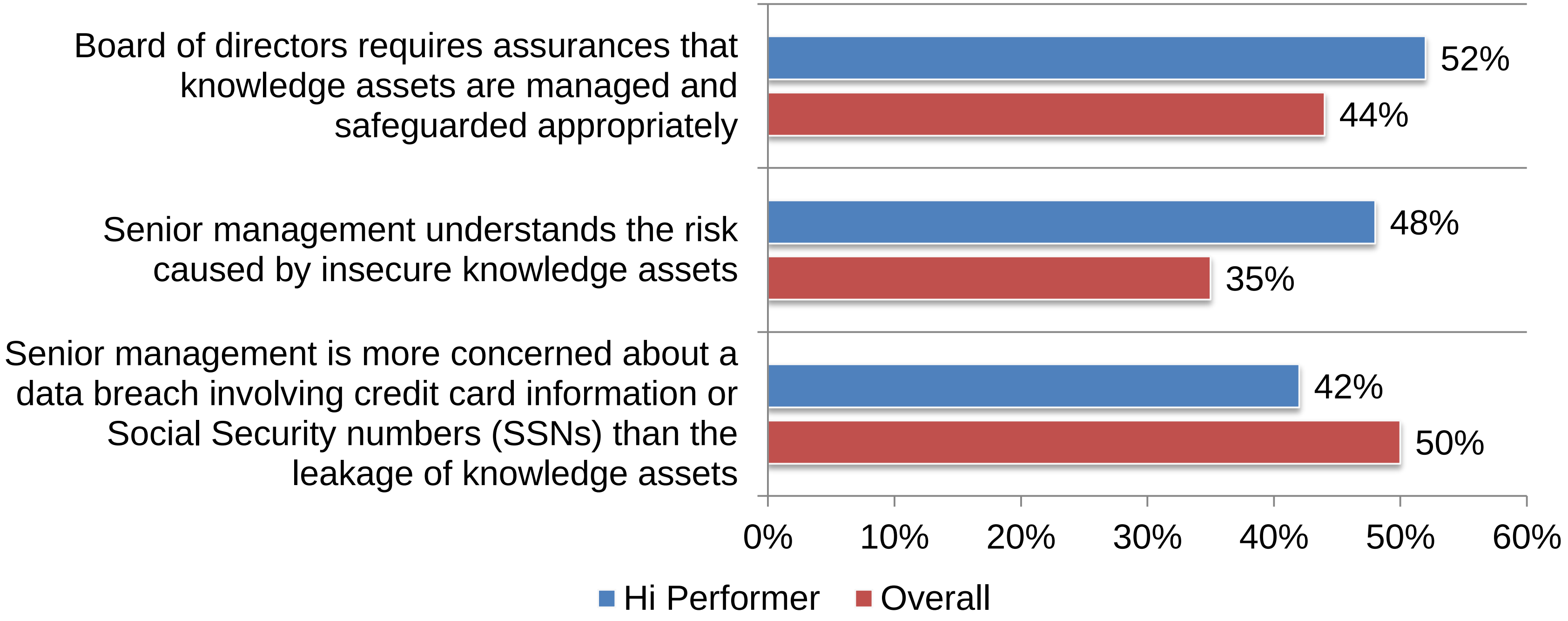
External, third-party **audits** and regular, customized, actionable **training**

Much greater reliance on these 3 techs/processes: **access governance, privileged user management** and **DLP**

More convinced that their knowledge assets are very valuable to a **nation state attacker**

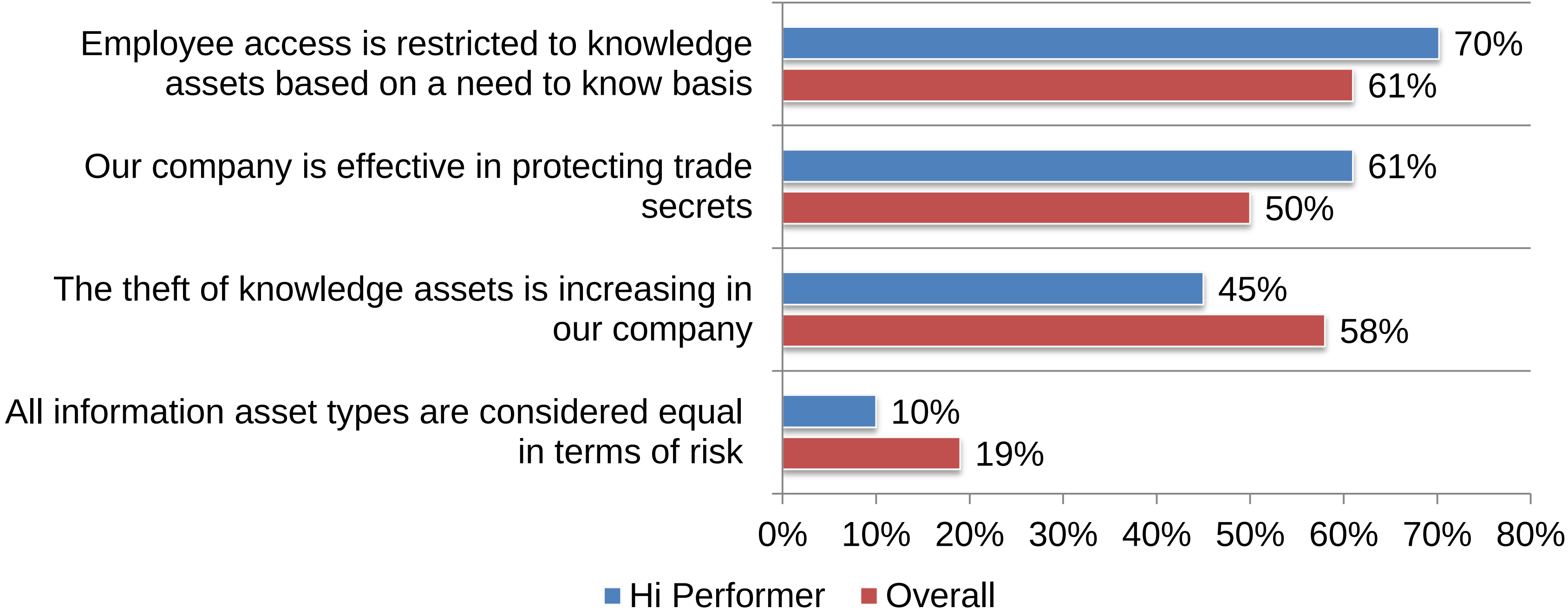
Perceptions about senior management and boards of directors

Strongly agree and Agree responses combined

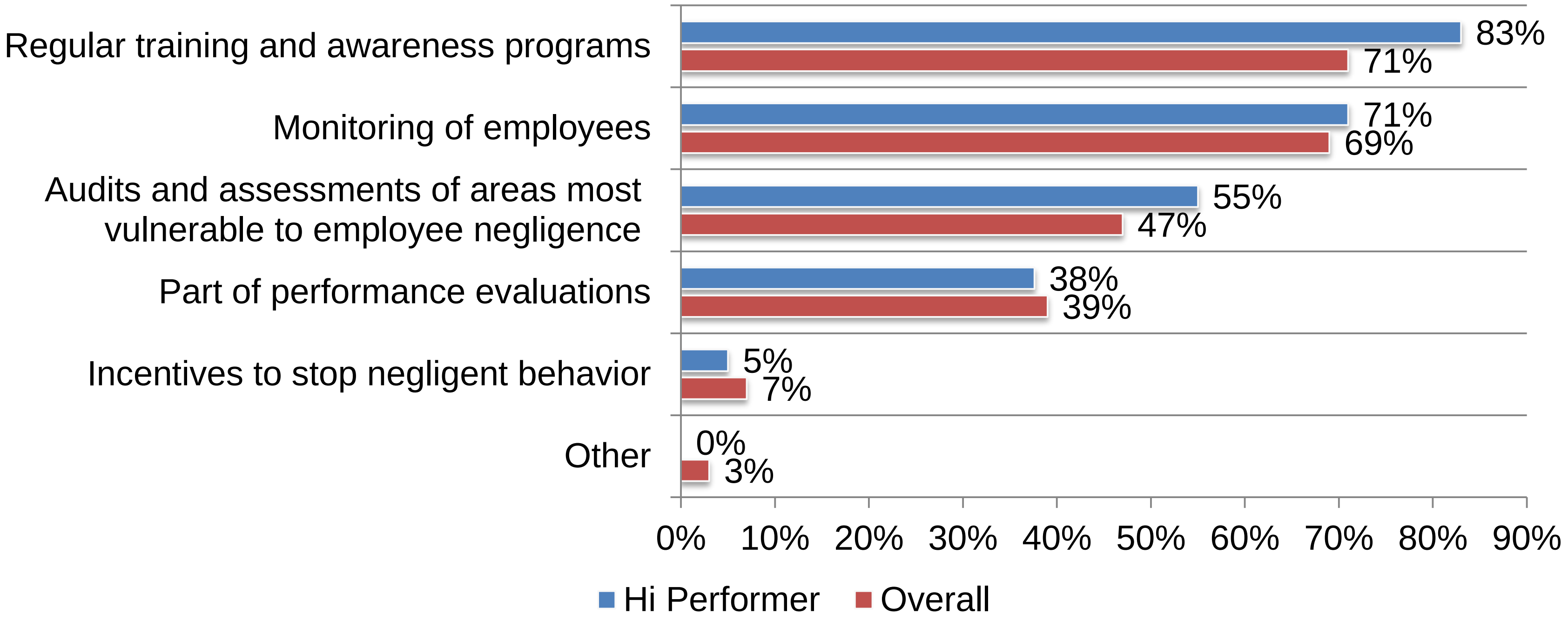


Differences in security practices

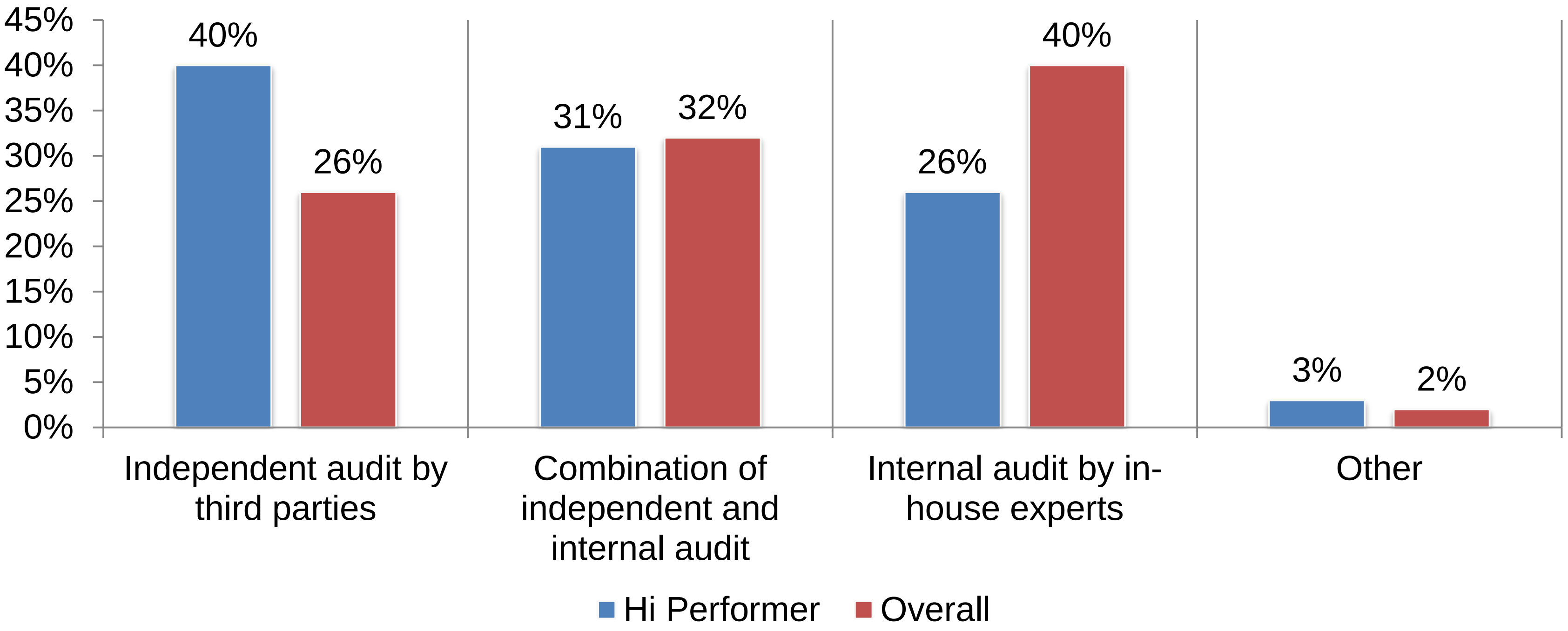
Strongly agree and Agree responses combined



More training/awareness, audits for the handling of insiders (vs. monitoring, evals, incentives)



High performers strongly favor independent 3rd-party audits



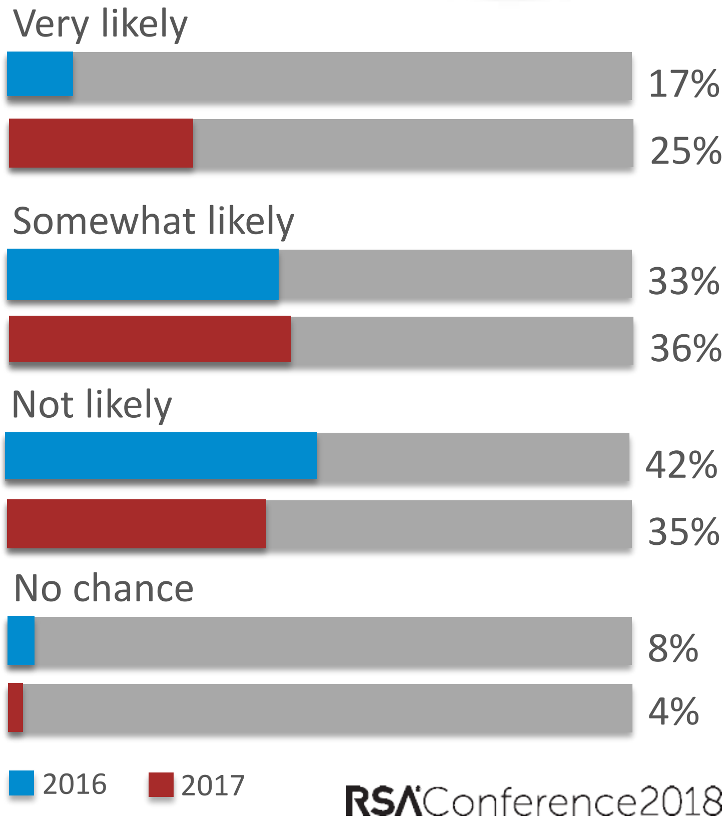
KILPATRICK TOWNSEND

Ponemon INSTITUTE

Root Causes: Rise of Nation State Attackers

52% of High Performers think their Knowledge Assets are “very valuable” to nation states, vs. 45% of all participants

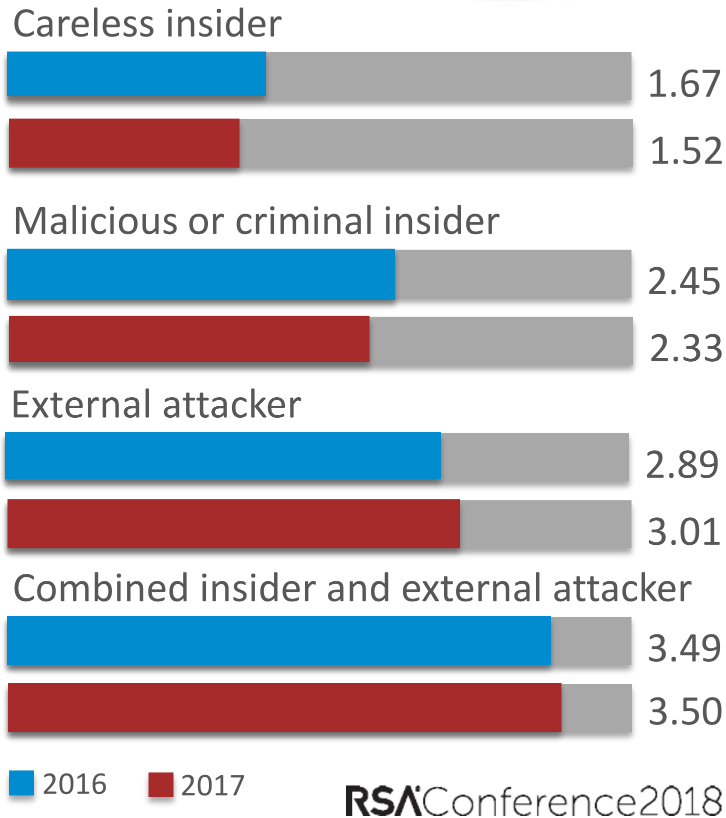
All participants are increasingly seeing nation-state attacks as “very likely”



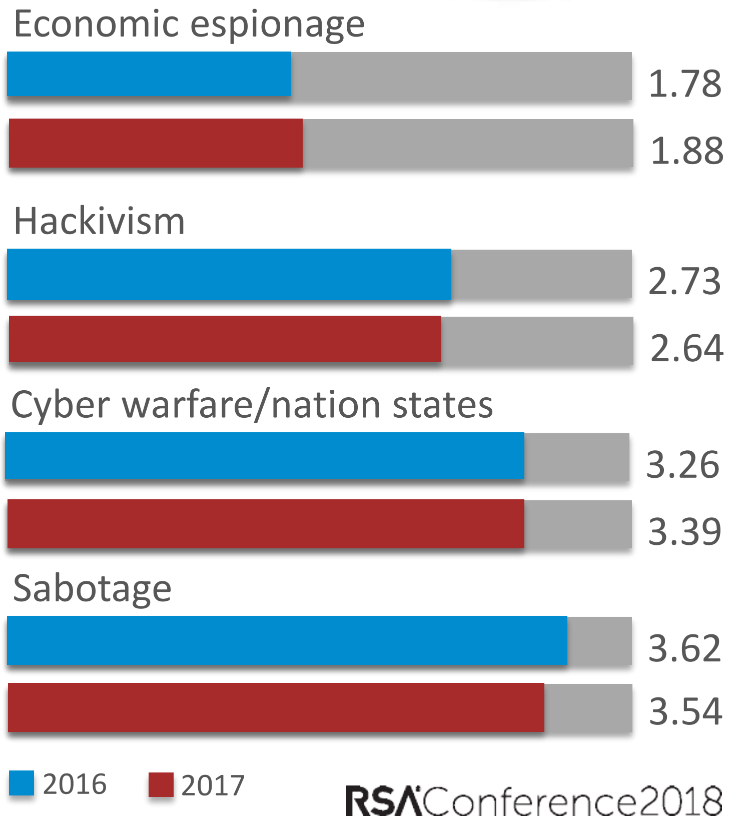
Root Causes: Who is responsible?

Careless insider most likely

75% of both High Performers & all respondents rate "employee negligence" "most significant" in 2017



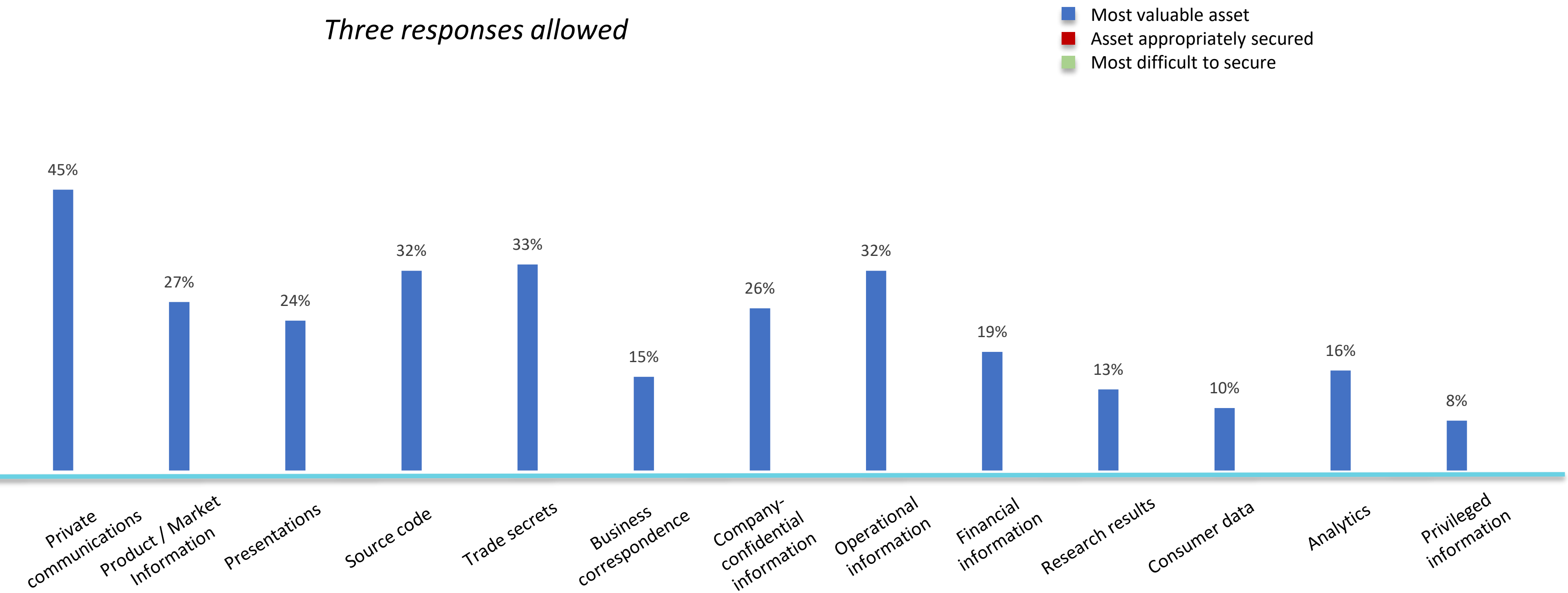
Root Causes: Attacker motives



Economic espionage most likely, particularly when one considers such espionage by nation states

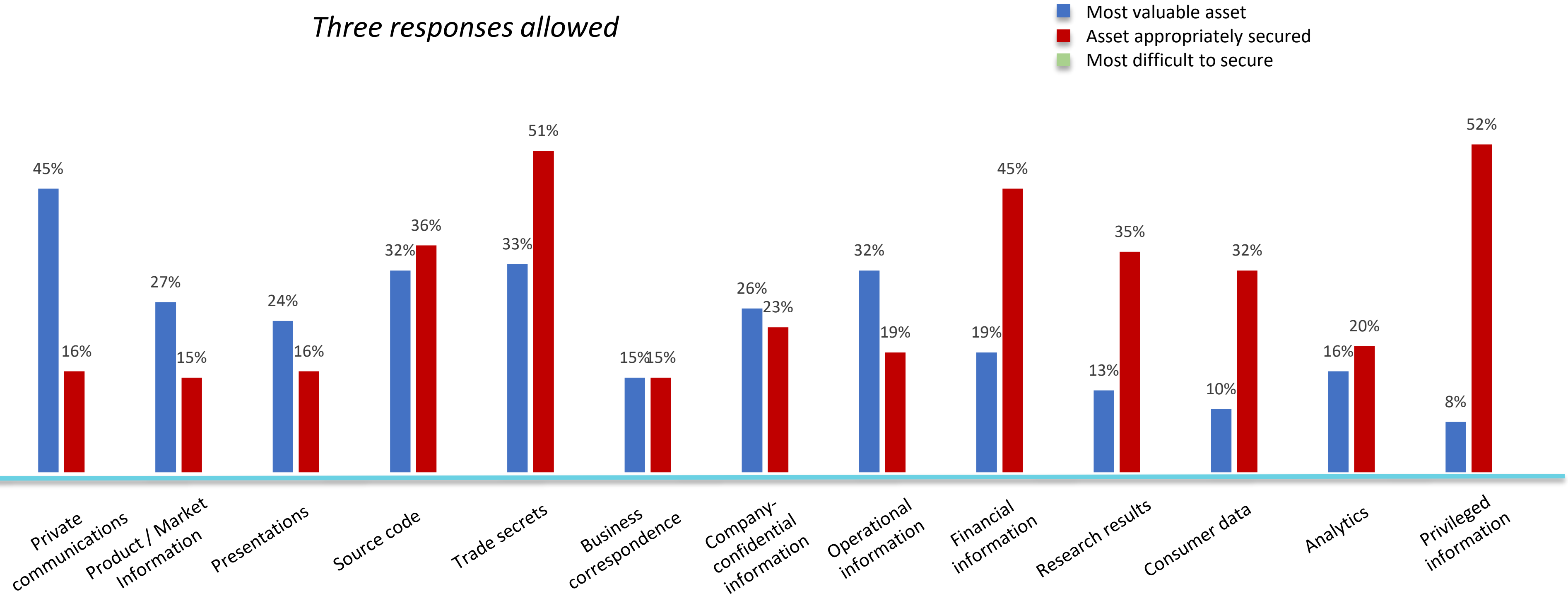
The knowledge-asset-type security gap

Three responses allowed



The knowledge-asset-type security gap

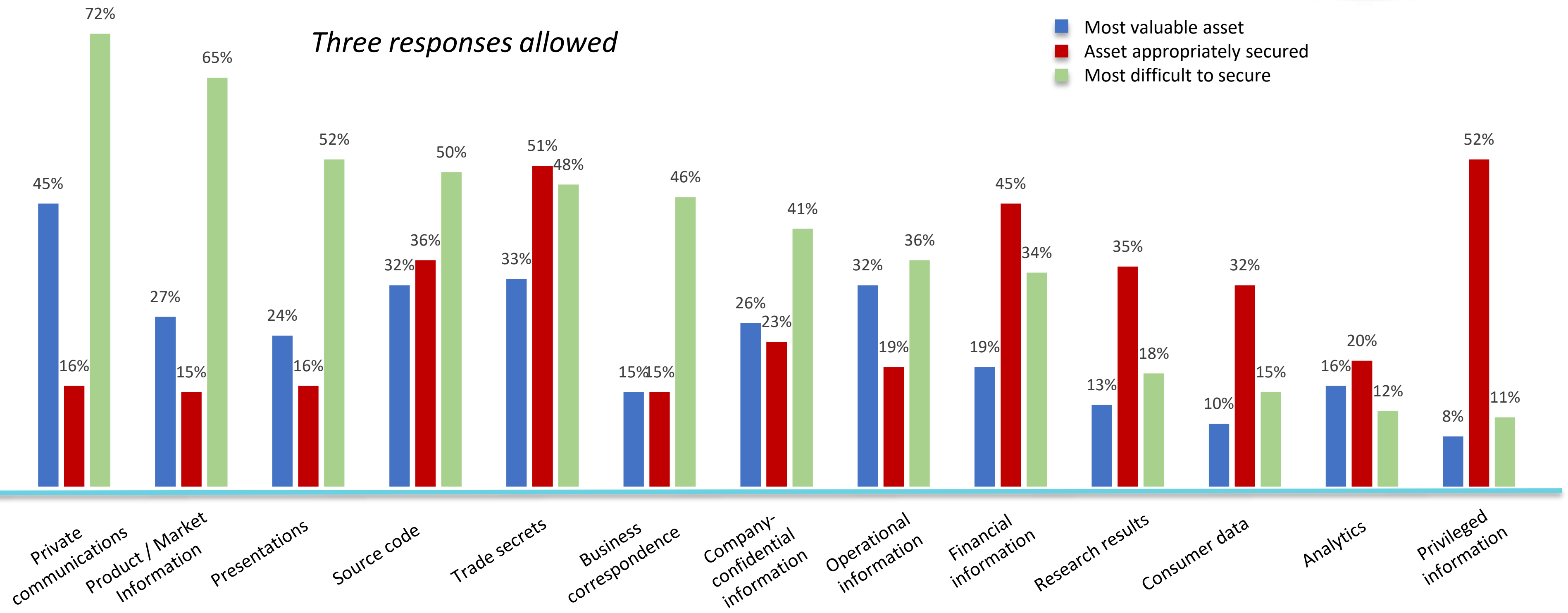
Three responses allowed



KILPATRICK TOWNSEND

Ponemon INSTITUTE

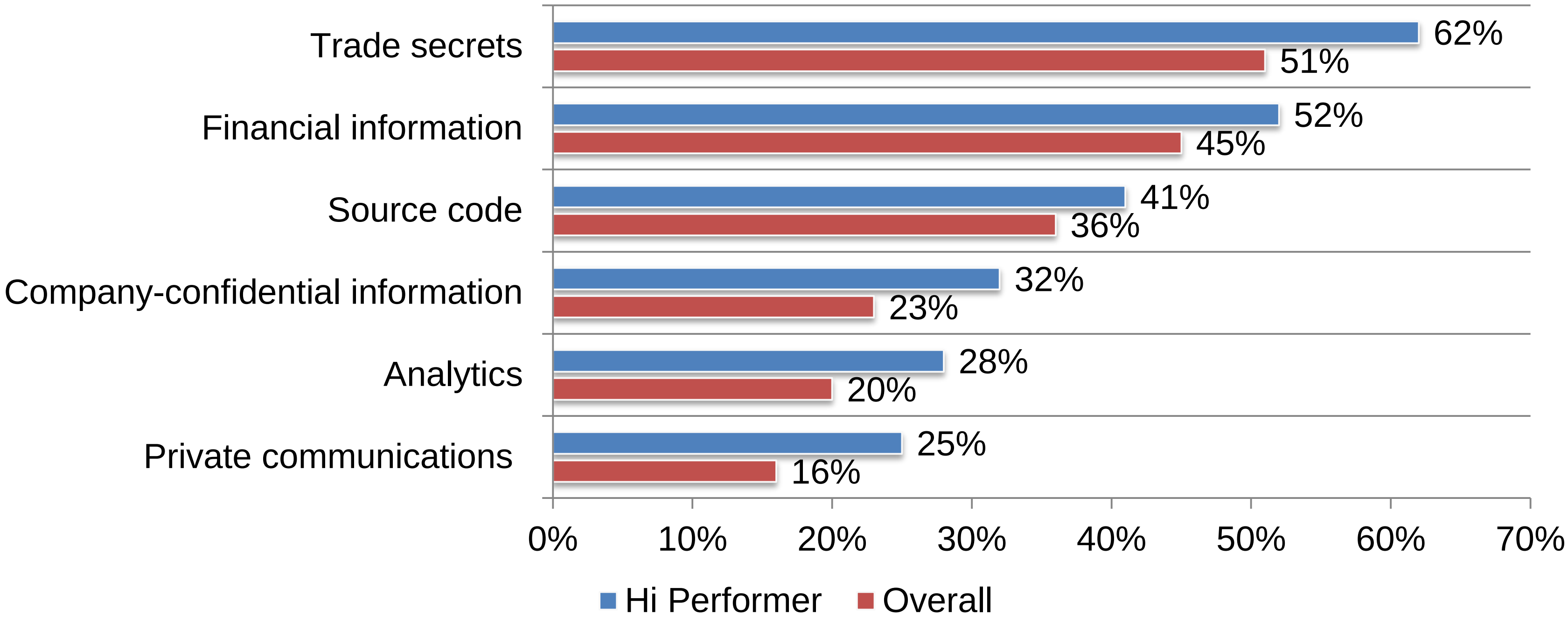
The knowledge-asset-type security gap



KILPATRICK TOWNSEND

Ponemon INSTITUTE

Note that the high performers are making strides here as well, even for private communications

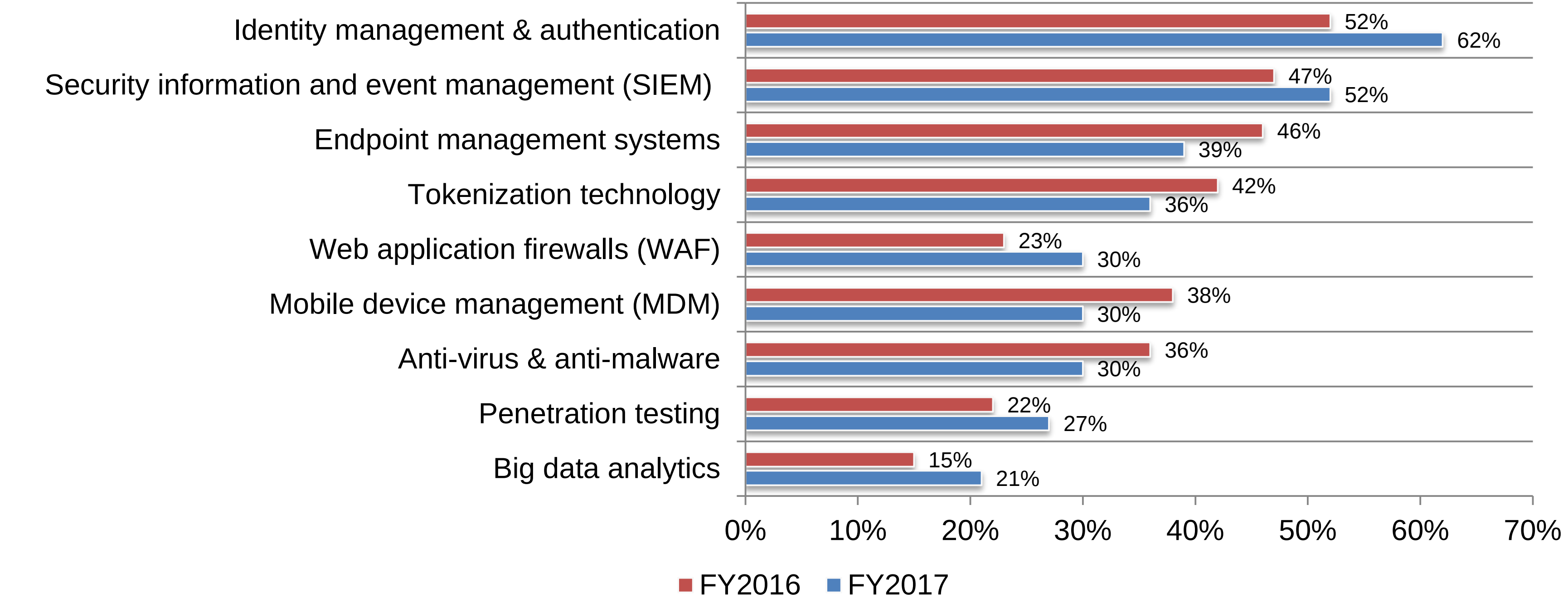


KILPATRICK TOWNSEND

Ponemon INSTITUTE

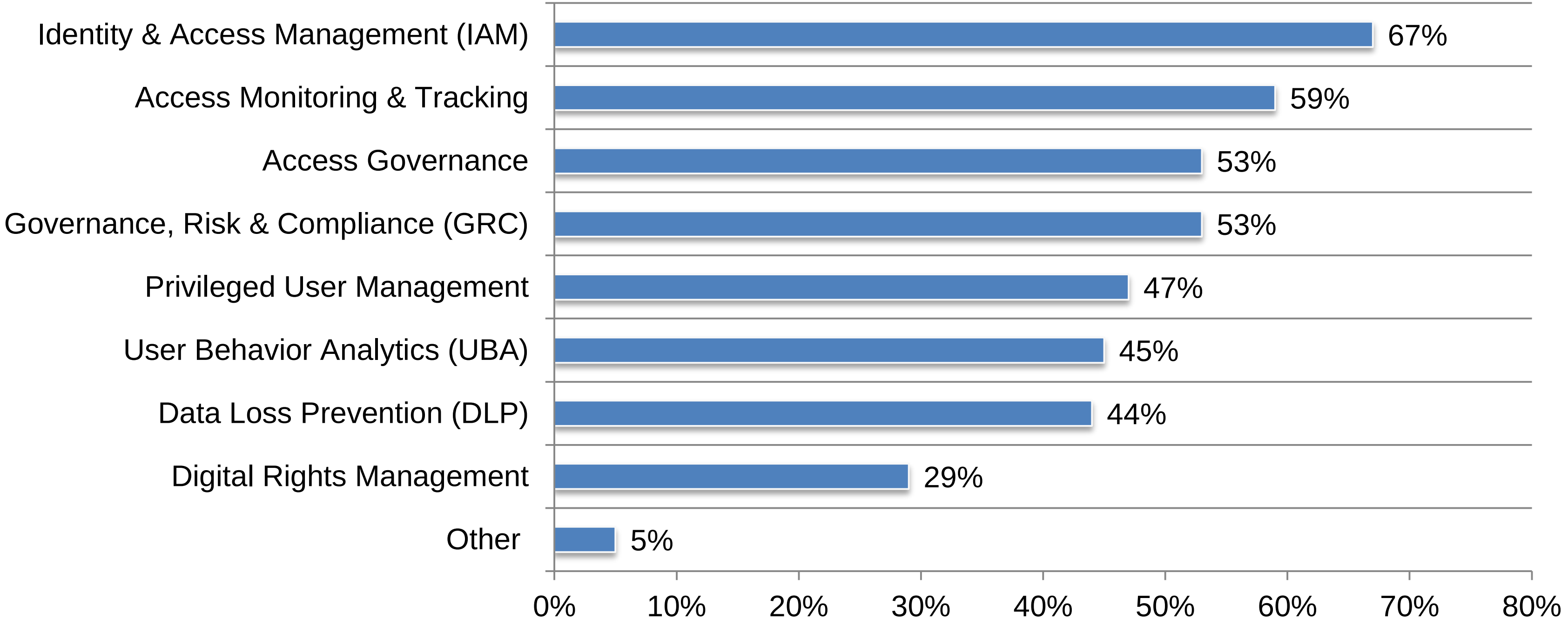
Trends in overall security technologies for protecting knowledge assets

Eight responses allowed

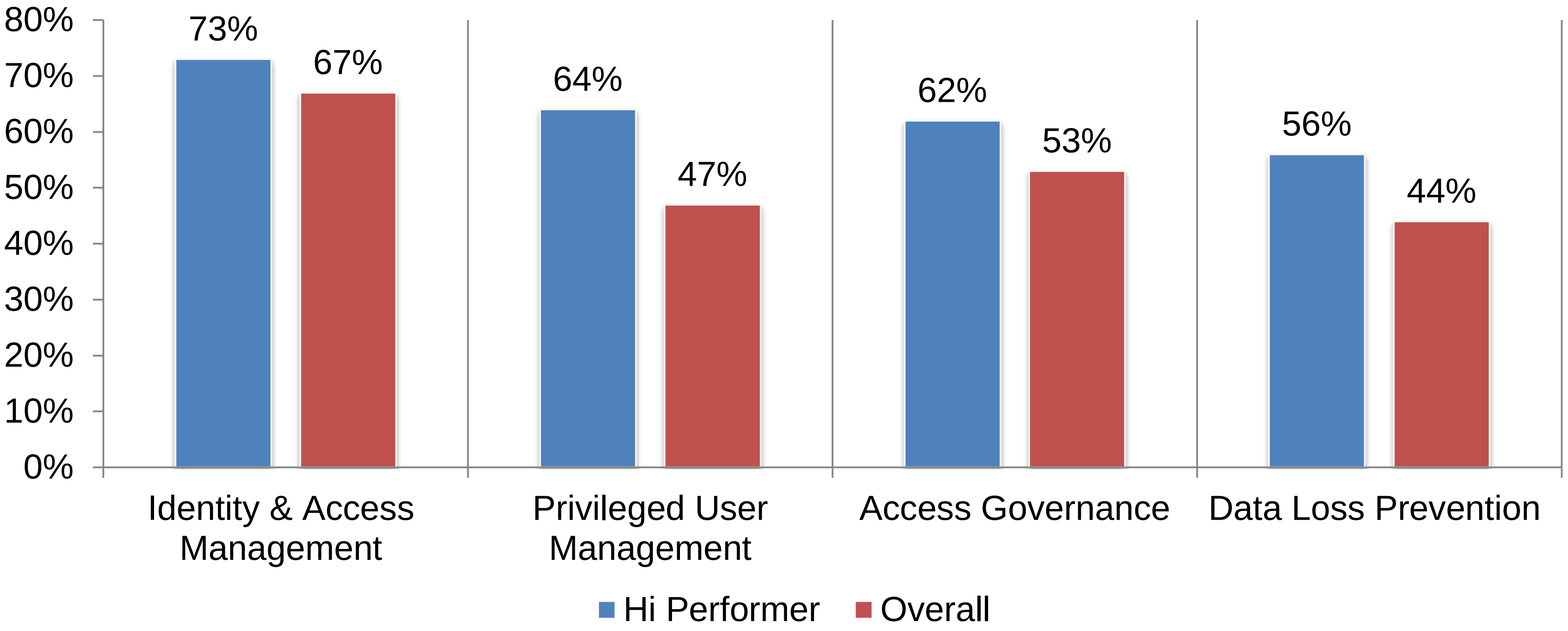


What technologies are used to secure *access* to knowledge assets?

Three responses allowed



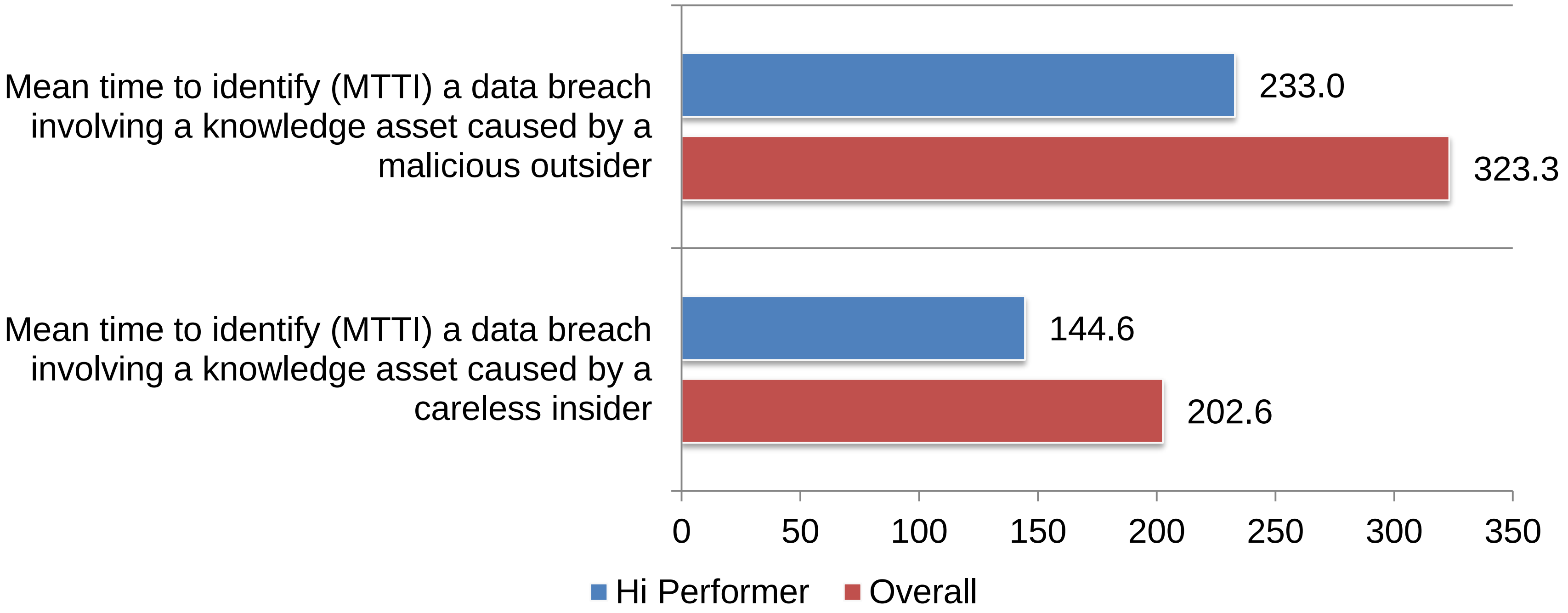
High performers rely more on 4 technologies



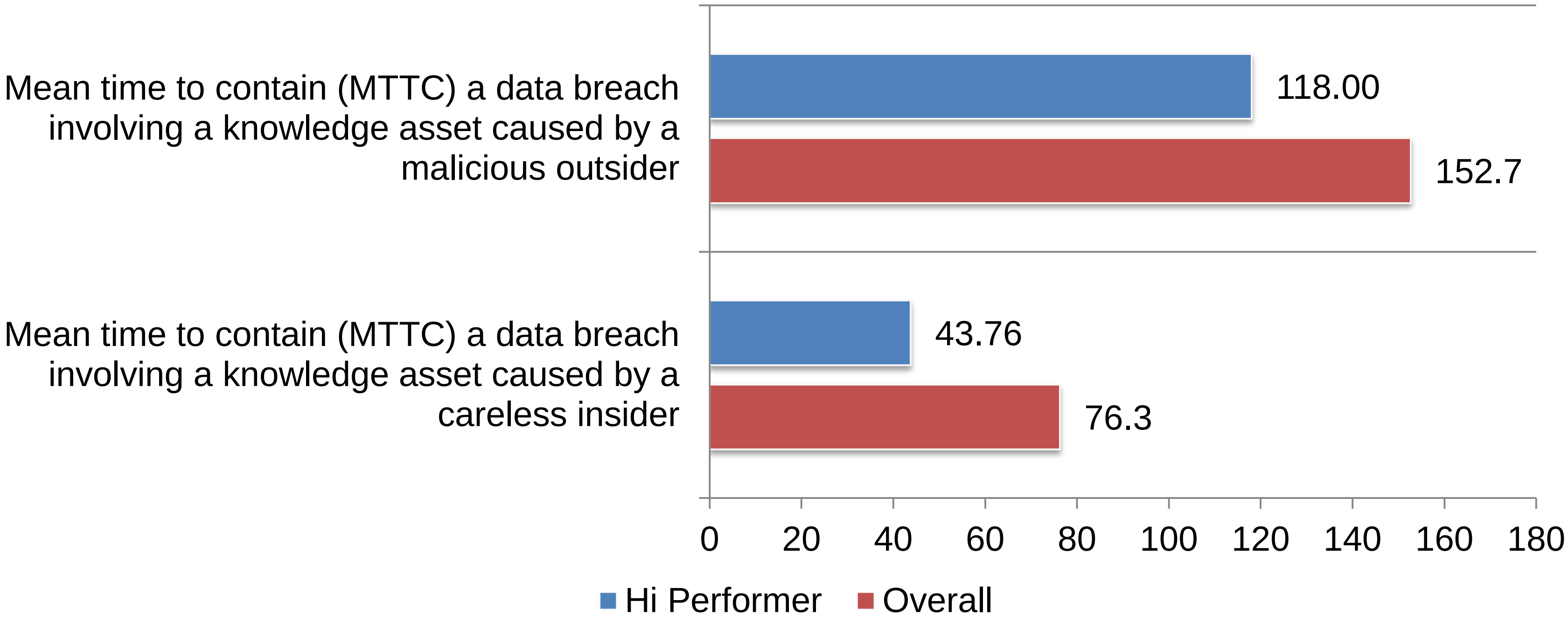
KILPATRICK TOWNSEND

Ponemon INSTITUTE

The mean time to identify (MTTI) a data breach involving knowledge assets caused by a careless insider or malicious outsider (in DAYS)

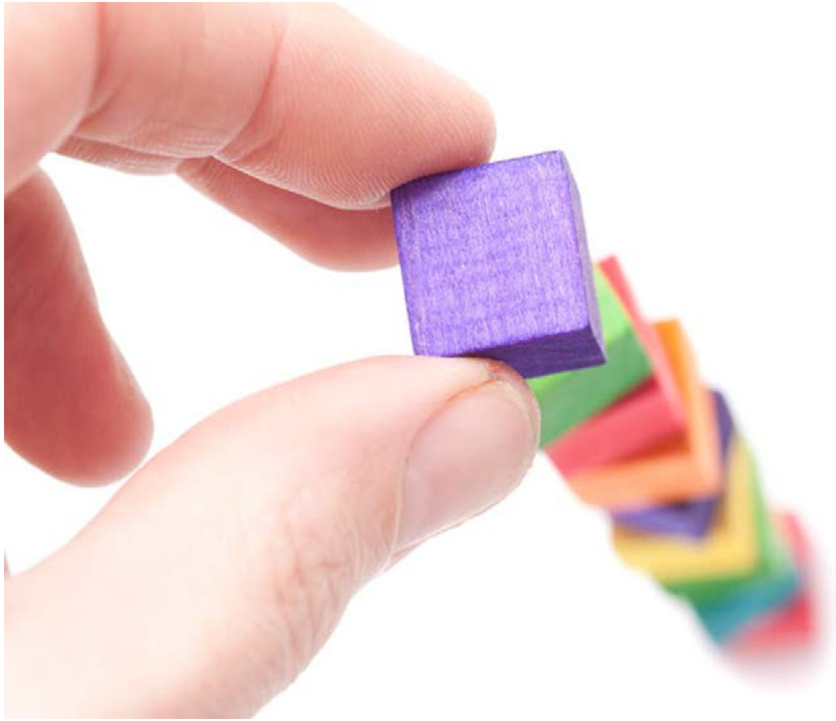


The mean time to contain (MTTC) a data breach involving knowledge assets caused by a careless insider or malicious outsider (in DAYS)



Building for success

- Read the study
- Benchmark against the High Performers
- Understand where you have unbalanced security vs. value
- Benchmark technology use
- Benchmark MTTI & MTTC
- Raise awareness of gaps



Questions?

Ponemon Institute
Toll Free: 800.887.3118
Michigan HQ: 2308 US 31 N.
Traverse City, MI 49686 USA
research@ponemon.org

Jon Neiditz
jneiditz@kilpatricktownsend.com
https://www.linkedin.com/in/informationmanagementlaw
@jonneiditz
404.815.6004

Caveats

- This study utilizes a confidential and proprietary benchmark method that has been successfully deployed in earlier Ponemon Institute research. However, there are inherent limitations to benchmark research that need to be carefully considered before drawing conclusions from findings.
- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.
- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are familiar with their companies' approach to managing knowledge assets and involved in the process and are located in the United States. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a Web-based collection method, it is possible that non-Web responses by mailed survey or telephone call would result in a different pattern of findings.
- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.