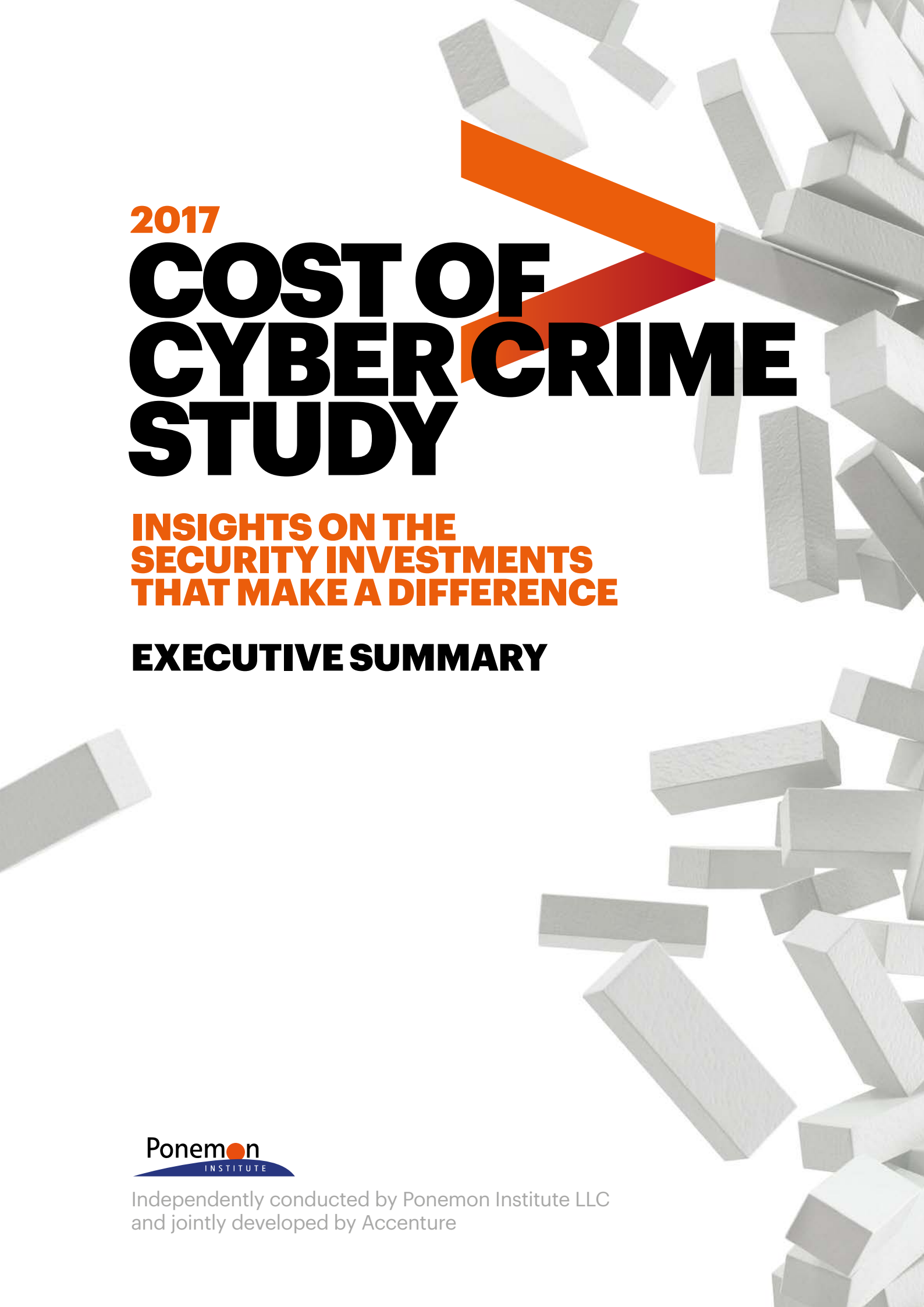
2017

COST OF CYBER CRIME STUDY

INSIGHTS ON THE SECURITY INVESTMENTS THAT MAKE A DIFFERENCE

EXECUTIVE SUMMARY



Ponemon INSTITUTE

Independently conducted by Ponemon Institute LLC
and jointly developed by Accenture

Average annualized cost of cybersecurity (USD)

$11.7M

Percentage increase in cost of cybersecurity in a year

22.7%

Average number of security breaches each year

130

Percentage increase in average annual number of security breaches

27.4%

PRIORITIZING BREAKTHROUGH INVESTMENTS

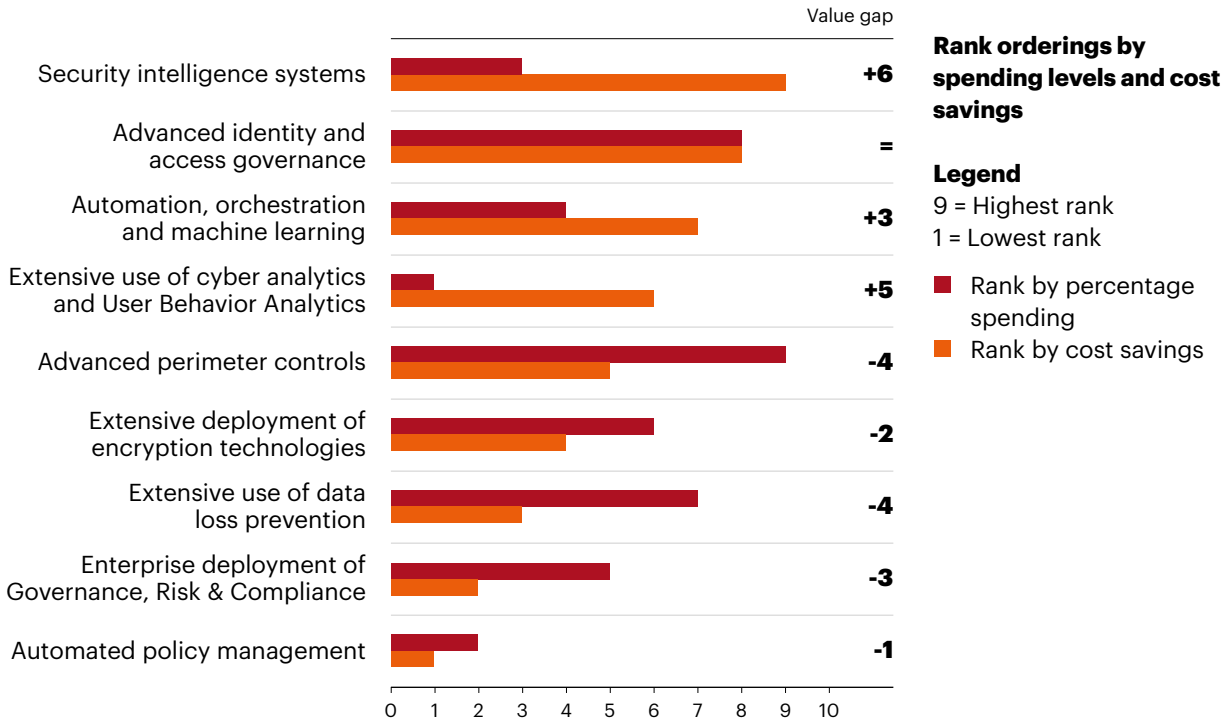
Over the last two years, the accelerating cost of cyber crime means that it is now 23 percent more than last year and is costing organizations, on average, US$11.7 million. Whether managing incidents themselves or spending to recover from the disruption to the business and customers, organizations are investing on an unprecedented scale—but current spending priorities show that much of this is misdirected toward security capabilities that fail to deliver the greatest efficiency and effectiveness.

A better understanding of the cost of cyber crime could help executives bridge the gap between their own defenses and the escalating creativity—and numbers—of threat actors. Alongside the increased cost of cyber crime—which runs into an average of more than US$17 million for organizations in industries like Financial Services and Utilities and Energy—attackers are getting smarter. Criminals are evolving new business models, such as ransomware-as-a-service, which mean that attackers are finding it easier to scale cyber crime globally.

With cyber attacks on the rise, successful breaches per company each year has risen more than 27 percent, from an average of 102 to 130. Ransomware attacks alone have doubled in frequency, from 13 percent to 27 percent, with incidents like WannaCry and Petya affecting thousands of targets and disrupting public services and large corporations across the world. One of the most significant data breaches in recent years has been the successful theft of 143 million customer records from Equifax—a consumer credit reporting agency—a cyber crime with devastating consequences due to the type of personally identifiable information stolen and knock-on effect on the credit markets. Information theft of this type remains the most expensive consequence of a cyber crime. Among the organizations we studied, information loss represents the largest cost component with a rise from 35 percent in 2015 to 43 percent in 2017. It is this threat landscape that demands organizations re-examine their investment priorities to keep pace with these more sophisticated and highly motivated attacks.

To better understand the effectiveness of investment decisions, we analyzed nine security technologies across two dimensions: the percentage spending level between them and their value in terms of cost-savings to the business. The findings illustrate that many organizations may be spending too much on the wrong technologies. Five of the nine security technologies had a negative value gap where the percentage spending level is higher than the relative value to the business. Of the remaining four technologies, three had a significant positive value gap and one was in balance. So, while maintaining the status quo on advanced identity and access governance, the opportunity exists to evaluate potential over-spend in areas which have a negative value gap and rebalance these funds by investing in the breakthrough innovations which deliver positive value.

THE POSITIVE OR NEGATIVE VALUE GAPS ASSOCIATED WITH SECURITY INVESTMENTS



Following on from the first *Cost of Cyber Crime*[1] report launched in the United States eight years ago, this study, undertaken by the Ponemon Institute and jointly developed by Accenture, evaluated the responses of 2,182 interviews from 254 companies in seven countries—Australia, France, Germany, Italy, Japan, United Kingdom and the United States. We aimed to quantify the economic impact of cyber attacks and observe cost trends over time to offer some practical guidance on how organizations can stay ahead of growing cyber threats.

1: The study examines the total costs organizations incur when responding to cyber crime incidents. These include the costs to detect, recover, investigate and manage the incident response. Also covered are the costs that result in after-the-fact activities and efforts to contain additional costs from business disruption and the loss of customers. These costs do not include the plethora of expenditures and investments made to sustain an organization's security posture or compliance with standards, policies and regulations.

HIGHLIGHTS FROM THE FINDINGS INCLUDE:

Organizations need to better balance investments in security technologies.

Security intelligence systems (67 percent) and advanced identity and access governance (63 percent) are the top two most widely deployed enabling security technologies across the enterprise. They also deliver the highest positive value gap with organizational cost savings of US$2.8 million and US$2.4 million respectively. As the threat landscape constantly evolves, these investments should be monitored closely so that spend is at an appropriate level and maintains effective outcomes. Aside from systems and governance, other investments show a lack of balance. Of the nine security technologies evaluated, the highest percentage spend was on advanced perimeter controls. Yet, the cost savings associated with technologies in this area were only fifth in the overall ranking with a negative value gap of minus 4. Clearly, an opportunity exists here to assess spending levels and potentially reallocate investments to higher-value security technologies.

Compliance technology is important but don't bet the business on it.

Spending on governance, risk and compliance (GRC) technologies is not a fast-track to increased security. Enterprise-wide deployment of GRC technology and automated policy management showed the lowest effectiveness in reducing cyber crime costs (9 percent and 7 percent respectively) out of nine enabling security technologies. So, while compliance technology is important, organizations must spend to a level that is appropriate to achieve the required

capability and effectiveness, enabling them to free up funds for breakthrough innovations.

Organizations need to grasp the innovation opportunity.

Innovations are generating the highest returns on investment, yet investment in them is low. For example, two enabling security technology areas identified as "Extensive use of cyber analytics and User Behavior Analytics (UBA)" and "Automation, orchestration and machine learning" were the lowest ranked technologies for enterprise-wide deployment (32 percent and 28 percent respectively) and yet they provide the third and fourth highest cost savings for security technologies. By balancing investments from less rewarding technologies into these breakthrough innovation areas, organizations could improve the effectiveness of their security programs.

RECOMMENDATIONS

$2.8M cost savings from security intelligence systems and most positive value gap

The foundation of a strong and effective security program is to identify and "harden" the higher-value assets. These are the "crown jewels" of a business—the assets most critical to operations, subject to the most stringent regulatory penalties, and the source of important trade secrets and market differentiation. Hardening these assets makes it as difficult and costly as possible for adversaries to achieve their goals, and limits the damage they can cause if they do obtain access.

CONCLUSION

By taking the following three steps, organizations can further improve the effectiveness of their cybersecurity efforts to fend off and reduce the impact of cyber crime:

1 > Build cyber-security on a strong foundation

Invest in the "brilliant basics" such as security intelligence and advanced access management and yet recognize the need to innovate to stay ahead of the hackers.

2 > Undertake extreme pressure testing

Organizations should not rely on compliance alone to enhance their security profile but undertake extreme pressure testing to identify vulnerabilities more rigorously than even the most highly motivated attacker.

3 > Invest in breakthrough innovation

Balance spend on new technologies, specifically analytics and artificial intelligence, to enhance program effectiveness and scale value.

Organizations need to recognize that spending alone does not always equate to value. Beyond prevention and remediation, if security fails, companies face unexpected costs from not being able to run their businesses efficiently to compete in the digital economy. Knowing which assets must be protected, and what the consequences will be for the business if protection fails, requires an intelligent security strategy that builds resilience from the inside out and an industry-specific strategy that protects the entire value chain. As this research shows, making wise security investments can help to make a difference.

$2.4 million average cost of malware attack spend and the top cost to companies

50 days average time to resolve a malicious insiders attack

23 days average time to resolve a ransomware attack

COST OF CYBER CRIME
Frequently Asked Questions

What types of cyber attacks are included in this research?
For purposes of this study, we define cyber attacks as criminal activity conducted through the organization's IT infrastructure via the internal or external networks or the Internet. Cyber attacks also include attacks against industrial controls. A successful cyber attack is one that results in the infiltration of a company's core networks or enterprise systems. It does not include the plethora of attacks stopped by a company's firewall defenses.

How does benchmark research differ from survey research?
The unit of analysis in the *2017 Cost of Cyber Crime Study* is the organization. In survey research, the unit of analysis is the individual. In our experience, a traditional survey approach does not capture the necessary details required to extrapolate cyber crime costs. We conduct field-based research that involves interviewing senior-level personnel about their organizations' actual cyber crime incidents.

How do you collect the data?
In our 2017 study, our researchers collected in-depth qualitative data through 2,182 separate interviews conducted over a 10-month period in 254 companies in seven countries: the United States, the United Kingdom, Germany, France, Italy, Australia and Japan. In each of the 254 participating organizations, we spoke with IT, compliance and information security practitioners who are knowledgeable about the cyber attacks experienced by the company and the costs associated with resolving the cyber crime incidents. For privacy purposes we did not collect organization-specific information.

How do you calculate the cost?

To determine the average cost of cyber crime, organizations were asked to report what they spent to deal with cyber crimes over four consecutive weeks. Once the costs over the four-week period were compiled and validated, these figures were then grossed-up to determine the annualized cost. These are costs to detect, recover, investigate and manage the incident response. Also covered are the costs that result in after-the-fact activities and efforts to reduce business disruption and the loss of customers. These costs do not include expenditures and investments made to sustain an organization's security posture or compliance with standards, policies and regulations.

Are you tracking the same organizations each year?

For consistency purposes, our benchmark sample consists of only larger-sized organizations (that is, a minimum of approximately 1,000 enterprise seats).[2] Each annual study involves a different sample of companies. In short, we do not track the same sample of companies over time. To be consistent, we recruit and match companies with similar characteristics such as the company's industry, headcount, geographic footprint and size of data breach.

2: Enterprise seats refer to the number of direct connections to the network and enterprise systems.

CONTACT US

Kevin Richards
k.richards@accenture.com

Ryan LaSalle
ryan.m.lasalle@accenture.com

Tom Parker
tom.parker@accenture.com

Floris van den Dool
floris.van.den.dool@accenture.com

Josh Kennedy-White
j.kennedy-white@accenture.com

Ponemon Institute LLC
Attn: Research Department
2308 US 31 North
Traverse City, Michigan 49629 USA
1.800.887.3118
research@ponemon.org

Visit us at http://www.accenture.com

Follow us @AccentureSecure

Connect with us

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 411,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at **www.accenture.com**

ABOUT ACCENTURE SECURITY

Accenture Security helps organizations build resilience from the inside out, so they can confidently focus on innovation and growth. Leveraging its global network of cybersecurity labs, deep industry understanding across client value chains and services that span the security lifecycle, Accenture protects organization's valuable assets, end-to-end. With services that include strategy and risk management, cyber defense, digital identity, application security and managed security, Accenture enables businesses around the world to defend against known sophisticated threats, and the unknown. Follow us @AccentureSecure on Twitter or visit the Accenture Security blog.

ABOUT PONEMON INSTITUTE

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.