



2017 Global Cybersecurity Assurance Report Card

Introduction

While malware attacks and data breaches continue to make headlines almost daily, the world's information security professionals are facing radical shifts in the enterprise attack surface as we move into 2017. They still struggle with a lack of visibility and risk assessment for cloud, mobile, BYOD and shadow IT, but now must address a new layer of complexity as organizations embrace the world of DevOps and containers.

The Global Cybersecurity Assurance Report Card was created by Tenable Network Security to measure the attitudes, beliefs and perceptions of security professionals and discover whether or not the world's cyber defenses are meeting expectations.

By averaging responses from 700 security practitioners across seven key industry verticals and nine countries, Tenable and research partner CyberEdge Group derived two summary indices that reflect the abilities of the world's enterprises to assess cybersecurity risks and mitigate threats. These scores were combined to produce a single report card score that represents overall confidence levels of security practitioners that the world's cyber defenses are meeting expectations.

61% down 12%
over 2016

2017 Risk Assessment Index

Represents the organization's ability to assess cybersecurity risks across 11 key components of enterprise IT infrastructure

79% no change
over 2016

2017 Security Assurance Index

Represents the organization's ability to mitigate threats by investing in security infrastructure fueled by executive and board-level commitment

70% down 6%
over 2016

2017 Global Cybersecurity Assurance Report Card

An average of the global risk assessment and security assurance indices

Executive Summary

The 2017 Tenable Network Security Global Cybersecurity Assurance Report Card picked up right where last year's study left off, with Risk Assessment for cloud and mobile ranking among the world's biggest enterprise security weaknesses. This year, however, accelerated adoption of cloud and mobile computing combined with the emergence of DevOps and containers to increase the complexity and decentralization of enterprise IT, are making it harder for security teams to see everything on their networks and accurately assess cyber risks.

With a modern enterprise network made up of mobile, cloud, web apps, virtual machines, internet of things, BYOD and containers the days of a well-defined network perimeter that can be secured and defended are long over. Today's network is ephemeral. The issue is not just one category of devices or apps and their individual risk, it is the totality of these assets and how they expand the corporate attack surface, creating new risk to an organization.

Complicated by the constantly evolving and multiplying threat landscape — cited for the second year in a row as the number one challenge for security pros — this heightened technological complexity is creating even more opportunity for attackers to exploit gaps in security coverage, leaving all organizations vulnerable to compromise and breach, regardless of the size of their security investments.

Indeed, the situation appears dire as the world enters 2017, with data reflecting an overall decline in global cyber readiness fueled by a pronounced inability to assess and mitigate cyber risks for the new and evolving IT landscape. It is more critical now than ever before that businesses and government organizations everywhere not only understand the threats aligned against them, but that they also possess a realistic assessment of their own cybersecurity strengths and weaknesses.

The following are some of the key takeaways from the 2017 report:

- 1 Risk Assessment Woe** In 2016, respondents were asked to rate their organizations' ability to assess security risks associated with 10 different IT components. In 2017, corresponding scores fell by an average of 12 percentage points.
- 2 Cloud Darkening** Cloud software as a service (SaaS) and infrastructure as a service (IaaS) were two of the lowest scoring Risk Assessment areas in the 2016 report. SaaS and IaaS were combined with platform as a service (PaaS) for the 2017 survey and the new "cloud environments" component scored 60% (D-), a seven point drop compared to last year's average for IaaS and SaaS.
- 3 A Mobile Morass** Identified alongside IaaS and SaaS in last year's report as one of the biggest enterprise security weaknesses, Risk Assessment for mobile devices once again dropped eight points from 65% (D) to 57% (F).
- 4 New Challenges Emerge** Two new IT components were introduced for 2017 — containerization platforms and DevOps environments.

DevOps is transforming the way software teams collaborate through increased consistency and automation, but it also introduces new security concerns. In fact, respondents reported just 57% (F) confidence in the ability to assess security during the DevOps process.

At the same time, adoption of containerization technologies like Docker is exploding as organizations look to accelerate innovation cycles and reduce time-to-market. Unfortunately, only 52% (F) of respondents this year felt that their organization had a handle on how best to assess risks within container environments.

- 5 Web App Security: Room for Improvement?** The single biggest drop in Risk Assessment this year is web applications, which fell 18 points from 80% (B-) in 2016 to 62% (D-) in 2017. The ability to access these services online and from mobile phones puts them right at users' fingertips, but also creates new security challenges. If application-centric security is the future, we have a long way to go.
- 6 Security Assurance Steady** Although respondents struggled to assess risks in an evolving threat landscape, they expressed confidence in their ability to mitigate security risks, once identified. Despite changes to three of the six Security Assurance survey questions in 2017, the three scores that carried over from last year only fluctuated by a few percentage points.
- 7 India Claims the Top Spot** New to the 2017 Global Cybersecurity Assurance Report Card, India debuted with the highest overall score at 84% (B), while last year's leader, the United States, fell two points to second place with 78% (C+).
- 8 Japan Lacking Confidence** Another new addition for this year, Japan's information security pros reported the lowest of the nine countries with an overall score of 48% (F). Even after taking margin of error into account, Japanese security practitioners graded themselves quite harshly, putting the country firmly in last place behind Germany, which fell 10 points this year to 62% (D-).
- 9 Education and Government Behind the Pack** Of the seven industries analyzed in the 2016 study, Education and Government earned the lowest overall scores. These two industries placed near the bottom again in the 2017 study, with Education remaining steady at 64% (D) and Government dropping three points to 63% (D).
- 10 Retail Takes the Lead Over Financial Services and Telecom** Last year, Financial Services and Telecom tied for first place among industries surveyed with an overall report card score of 81% (B-). This year, six of the seven overall industry scores fell, with Telecom experiencing the most significant drop, down 11 points to 70% (C-) followed closely by Financial Services, down nine points to 72% (C-). Retail remained relatively steady, losing only one point to take first place with a 2017 score of 76% (C).

The remainder of this report provides detailed Risk Assessment Index and Security Assurance Index results and insights globally, by country and by industry — followed by recommendations to help organizations improve their ability to minimize cybersecurity risks.

Risk Assessment Index

The Risk Assessment Index conveys an organization’s ability to assess cybersecurity risks across 11 key IT infrastructure components, as depicted in question 6 of the survey instrument (see Appendix 3) and in Figures 1, 2, and 3 below. In 2017, “cloud apps” and “cloud infrastructure” were collapsed into “cloud environments.” And two additional IT components were added, “containerization platforms” and “DevOps environments.”

Figure 1 depicts the Risk Assessment score changes between 2016 and 2017, with the 2016 cloud infrastructure score stemming from the combination of cloud apps and cloud infrastructure in that same year.

	2016	2017	Change
Risk Assessment Index (Global)			
Cloud environments	67%	60%	-7%
Containerization platforms	-	52%	
Datacenter / physical servers	77%	64%	-13%
Datacenter / virtual servers	76%	65%	-11%
Desktops (PCs)	78%	64%	-14%
DevOps environments	-	57%	
Laptops / notebooks	77%	62%	-15%
Mobile devices	65%	57%	-8%
Network infrastructure	73%	64%	-9%
Network perimeter / DMZ	72%	62%	-10%
Web applications	80%	62%	-18%

FIGURE 1: Global Risk Assessment Index scores for 2016 and 2017

As is evident in this year’s results, information security professionals are more concerned today with their organizations’ ability to assess security risks across nearly all facets of the IT infrastructure than they were last year.

The Global Cybersecurity Assurance Report Card is intended to measure the human IT landscape and was designed to gauge the attitudes and beliefs of IT security professionals, not the actual effectiveness of their security defenses. While it might be difficult to nail down any single cause, one thing is clear — the overall decline in Risk Assessment confidence is real.

The marked decline in global confidence levels indicates that security professionals may be experiencing a drop in morale as a result of near-daily data breach headlines, compounded by fatigue as a result of the uphill battle to keep pace with emerging technologies and proliferating threats. Despite spending tens of billions of dollars on security products and services each year, organizations around the world continue to be affected by data breaches. And security professionals are wondering whether their organizations will be next, and are doubting their readiness despite feeling like they have the funding and tools they need (see Figure 10).

Of notable concern are the failing grades for containerization platforms (52%), DevOps environments (57%) and mobile devices (57%).

First, although containerization delivers numerous benefits, it also introduces new security risks, which are impossible to identify using traditional security tools. The rapid development and deployment of containers, combined with their relatively short life cycles, make it difficult for security teams to effectively monitor and detect container-based vulnerabilities.

Second, the emergence of DevOps processes in the world's enterprises has fundamentally changed the way security should be implemented. The goal of DevOps is to change and improve the relationship between development and operations to create a seamless and streamlined process; however, if security is not incorporated into the build cycle, it could be treated as an afterthought or cut out of the loop entirely. Similar to containerization, the use of DevOps platforms presents new risks that many organizations struggle to proactively identify and remediate.

Third, mobile devices continue to be a weak point for IT security professionals. Users want to access corporate applications and data using their personal tablets and smartphones, but implementing a bring-your-own-device (BYOD) policy can leave IT environments vulnerable, unless these devices are properly secured. IT security professionals continue to struggle with not only securing mobile devices, but also assessing their security risks.

The biggest Risk Assessment score drop in the 2017 report is web applications, which fell 18% this year (from 80% in 2016 to 62% in 2017). The ability to access these services online and from mobile phones puts them right at users' fingertips. From Google Docs and email to maps, games and news, applications are used to streamline productivity and stifle boredom. More alarming is what this could mean for the future. As confidence in the ability to secure web apps falls, the accelerating migration of IT operations and infrastructure to the cloud means the traditional approach to security must evolve beyond perimeter defenses and endpoint solutions, placing application security high on the list of critical priorities.

See Figure 2 below for a look at how each of the nine surveyed countries fared. Overall score changes from 2016 to 2017 for each country are depicted in the "Final Grades" section.

	GLOBAL		USA		CANADA		UK		GERMANY		FRANCE		AUSTRALIA		SINGAPORE		JAPAN		INDIA	
	%	Grade	%	Grade	%	Grade	%	Grade	%	Grade	%	Grade	%	Grade	%	Grade	%	Grade	%	Grade
Cloud environments	60%	D-	71%	C-	69%	D+	58%	F	56%	F	64%	D	62%	D-	71%	C-	43%	F	76%	C
Containerization platforms	52%	F	59%	F	46%	F	42%	F	47%	F	66%	D	59%	F	60%	D-	40%	F	68%	D+
Datacenter / physical servers	64%	D	73%	C	69%	D+	65%	D	50%	F	68%	D+	66%	D	69%	D+	47%	F	76%	C
Datacenter / virtual servers	65%	D	75%	C	66%	D	69%	D+	43%	F	67%	D+	67%	D+	65%	D	54%	F	72%	C-
Desktops (PCs)	64%	D	74%	C	79%	C+	67%	D+	46%	F	73%	C	71%	C-	65%	D	42%	F	76%	C
DevOps environments	57%	F	65%	D	69%	D+	51%	F	33%	F	59%	F	56%	F	72%	C-	38%	F	68%	D+
Laptops / notebooks	62%	D-	73%	C	69%	D+	61%	D-	50%	F	73%	C	64%	D	65%	D	40%	F	58%	F
Mobile devices	57%	F	66%	D	69%	D+	57%	F	53%	F	57%	F	59%	F	71%	C-	39%	F	72%	C-
Network infrastructure	64%	D	75%	C	66%	D	60%	D-	34%	F	73%	C	65%	D	69%	D+	43%	F	84%	B
Network perimeter / DMZ	62%	D-	71%	C-	66%	D	58%	F	35%	F	75%	C	67%	D+	71%	C-	44%	F	76%	C
Web applications	62%	D-	71%	C-	66%	D	56%	F	38%	F	68%	D+	67%	D+	69%	D+	45%	F	72%	C-
AVERAGE	61%	D-	70%	C-	67%	D+	59%	F	44%	F	67%	D+	64%	D	68%	D+	43%	F	73%	C

FIGURE 2: Risk Assessment Index scores by country

The following are 2017 Risk Assessment Index scores by industry:

	EDUCATION		FINANCIAL SVS.		GOVERNMENT		HEALTH CARE		MANUFACT'ING		RETAIL		TELECOM	
	%	Grade	%	Grade	%	Grade	%	Grade	%	Grade	%	Grade	%	Grade
Cloud environments	50%	F	59%	F	49%	F	51%	F	63%	D	80%	B-	57%	F
Containerization platforms	55%	F	52%	F	55%	F	42%	F	41%	F	63%	D	52%	F
Datacenter / physical servers	81%	B-	59%	F	71%	C-	53%	F	59%	F	55%	F	66%	D
Datacenter / virtual servers	67%	D+	53%	F	71%	C-	71%	C-	68%	D+	59%	F	64%	D
Desktops (PCs)	69%	D+	56%	F	61%	D-	58%	F	63%	D	63%	D	67%	D+
DevOps environments	50%	F	58%	F	52%	F	39%	F	56%	F	65%	D	58%	F
Laptops / notebooks	56%	F	67%	D+	56%	F	60%	D-	59%	F	76%	C	64%	D
Mobile devices	60%	D-	60%	D-	55%	F	47%	F	57%	F	65%	D	54%	F
Network infrastructure	69%	D+	67%	D+	69%	D+	60%	D-	59%	F	57%	F	62%	D-
Network perimeter / DMZ	86%	B	61%	D-	60%	D-	51%	F	55%	F	74%	C	61%	D-
Web applications	66%	D	61%	D-	54%	F	57%	F	71%	C-	65%	D	57%	F
AVERAGE	64%	D	59%	F	59%	F	54%	F	59%	F	66%	D	60%	D-

FIGURE 3: Risk Assessment Index scores by industry

The forthcoming “Geographical Insights” and “Industrial Insights” sections provide insights on results by country and industry, respectively.

Security Assurance Index

The Security Assurance Index conveys an organization’s ability to mitigate threats by investing in security infrastructure fueled by executive and board-level commitment. Questions 7-12 of the web-based survey (see Appendix 3) are associated with Security Assurance Index scores. Three of the six questions carried over from 2016 (questions 7, 11, and 12) while three questions are new (questions 8, 9, and 10).

Figure 4 depicts the global Security Assurance scores for 2016 and 2017, and the score changes for those three topics carried over from last year.

	2016	2017	Change
Security Assurance Index (Global)			
Measuring security effectiveness	81%	83%	2%
View network risks continuously	-	79%	
Aggregate risk intelligence	-	73%	
Align security with business	-	79%	
Conveying risks to execs and board	83%	80%	-3%
Exec and board-level commitment	76%	77%	1%

FIGURE 4: Global Security Assurance Index scores for 2016 and 2017

Even with three new questions, the 2017 Security Assurance Index was relatively unchanged compared to last year. Security practitioners expressed the least confidence in their ability to aggregate risk intelligence at 73% (C). This is consistent with the findings that security practitioners struggle with accurately assessing risk posture across the enterprise.

The Security Assurance data also show that information security as a profession is maturing. Security pros are confident in their ability to measure security effectiveness at 83% (B) and also in their ability to convey risks to executives and the board — 80% (B-). Despite confidence in their own abilities, security teams remain unimpressed with executive and board-level commitment, which was up just one point to 77% (C+) in 2017.

In almost every country, with the exception of Singapore, Security Assurance led Risk Assessment, with scores indicating that security teams feel comfortable measuring and reporting on what they know they can see, but acknowledge that there are critical gaps in security visibility — a theme reflected later in this report (see Figure 10).

Figure 5 depicts global Security Assurance Index scores and country scores.

	GLOBAL		USA		CANADA		UK		GERMANY		FRANCE		AUSTRALIA		SINGAPORE		JAPAN		INDIA	
	%	Grade	%	Grade	%	Grade	%	Grade	%	Grade	%	Grade	%	Grade	%	Grade	%	Grade	%	Grade
Measuring security effectiveness	83%	B	91%	A-	87%	B+	81%	B-	80%	B-	83%	B	80%	B-	71%	C-	52%	F	100%	A+
View network risks continuously	79%	C+	85%	B	87%	B+	76%	C	84%	B	79%	C+	82%	B-	55%	F	52%	F	92%	A-
Aggregate risk intelligence	73%	C	80%	B-	77%	C+	67%	D+	69%	D+	79%	C+	78%	C+	47%	F	48%	F	96%	A
Align security with business	79%	C+	86%	B	87%	B+	66%	D	82%	B-	83%	B	74%	C	66%	D	56%	F	96%	A
Conveying risks to execs and board	80%	B-	88%	B+	80%	B-	78%	C+	84%	B	77%	C+	80%	B-	62%	D-	52%	F	96%	A
Exec and board-level commitment	77%	C+	82%	B-	83%	B	70%	C-	78%	C+	80%	B-	76%	C	60%	D-	53%	F	96%	A
AVERAGE	79%	C+	85%	B	83%	B	73%	C	79%	C+	80%	B-	78%	C+	60%	D-	52%	F	96%	A

FIGURE 5: Security Assurance Report Cards by country

Figure 6 depicts Security Assurance Index scores by industry.

	EDUCATION		FINANCIAL SVS.		GOVERNMENT		HEALTH CARE		MANUFACT'ING		RETAIL		TELECOM	
	%	Grade	%	Grade	%	Grade	%	Grade	%	Grade	%	Grade	%	Grade
Measuring security effectiveness	75%	C	88%	B+	81%	B-	80%	B-	89%	B+	84%	B	88%	B+
View network risks continuously	58%	F	85%	B	78%	C+	80%	B-	83%	B	92%	A-	83%	B
Aggregate risk intelligence	58%	F	83%	B	44%	F	67%	D+	80%	B-	86%	B	72%	C-
Align security with business	69%	D+	86%	B	62%	D-	78%	C+	86%	B	84%	B	80%	B-
Conveying risks to execs and board	58%	F	86%	B	72%	C-	82%	B-	87%	B+	88%	B+	84%	B
Exec and board-level commitment	58%	F	83%	B	67%	D+	67%	D+	88%	B+	84%	B	77%	C+
AVERAGE	63%	D	85%	B	67%	D+	76%	C	86%	B	86%	B	81%	B-

FIGURE 6: Security Assurance Report Cards by industry

The forthcoming “Geographical Insights” and “Industrial Insights” sections provide insights on results by country and industry, respectively.

Overall Cybersecurity Assurance

The combination of Risk Assessment and Security Assurance scores (with equal weighting) yields the overall Global Cybersecurity Assurance Report Card score. Figure 7 compares the global and per-country scores from 2016 and 2017, while depicting the score changes for the six countries that were also part of the 2016 report.






		2016	2017	Change
Global				
	Risk Assessment	73%	61%	-12%
	Security Assurance	79%	79%	NC
	Overall Score	76%	70%	-6%
	Overall Grade	C	C-	▼
India				
	Risk Assessment	-	73%	
	Security Assurance	-	96%	
	Overall Score	-	84%	
	Overall Grade	-	B	
United States				
	Risk Assessment	77%	70%	-7%
	Security Assurance	83%	85%	2%
	Overall Score	80%	78%	-2%
	Overall Grade	B-	C+	▼
Canada				
	Risk Assessment	70%	67%	-3%
	Security Assurance	84%	83%	-1%
	Overall Score	77%	75%	-2%
	Overall Grade	C+	C	▼
France				
	Risk Assessment	-	67%	
	Security Assurance	-	80%	
	Overall Score	-	74%	
	Overall Grade	-	C	
Australia				
	Risk Assessment	69%	64%	-5%
	Security Assurance	69%	78%	9%
	Overall Score	69%	71%	2%
	Overall Grade	D+	C-	▲
United Kingdom				
	Risk Assessment	73%	59%	-14%
	Security Assurance	74%	73%	-1%
	Overall Score	74%	66%	-8%
	Overall Grade	C	D	▼
Singapore				
	Risk Assessment	69%	68%	-1%
	Security Assurance	75%	60%	-15%
	Overall Score	72%	64%	-8%
	Overall Grade	C-	D	▼
Germany				
	Risk Assessment	69%	44%	-25%
	Security Assurance	74%	79%	5%
	Overall Score	72%	62%	-10%
	Overall Grade	C-	D-	▼
Japan				
	Risk Assessment	-	43%	
	Security Assurance	-	52%	
	Overall Score	-	48%	
	Overall Grade	-	F	

FIGURE 7: Cybersecurity Assurance Report Cards by country

Figure 8 compares the scores from the 2016 and 2017 reports, while depicting the score changes for all seven industries.








		2016	2017	Change
Retail				
	Risk Assessment	75%	66%	-9%
	Security Assurance	79%	86%	7%
	Overall Score	77%	76%	-1%
	Overall Grade	C+	C	▼
Financial Services				
	Risk Assessment	79%	59%	-20%
	Security Assurance	84%	85%	1%
	Overall Score	81%	72%	-9%
	Overall Grade	B-	C-	▼
Manufacturing				
	Risk Assessment	72%	59%	-13%
	Security Assurance	80%	86%	6%
	Overall Score	76%	72%	-4%
	Overall Grade	C	C-	▼
Telecom				
	Risk Assessment	77%	60%	-17%
	Security Assurance	85%	81%	-4%
	Overall Score	81%	70%	-11%
	Overall Grade	B-	C-	▼
Health Care				
	Risk Assessment	72%	54%	-18%
	Security Assurance	75%	76%	1%
	Overall Score	73%	65%	-8%
	Overall Grade	C	D	▼
Education				
	Risk Assessment	65%	64%	-1%
	Security Assurance	64%	63%	-1%
	Overall Score	64%	64%	NC
	Overall Grade	D	D	NC
Government				
	Risk Assessment	63%	59%	-4%
	Security Assurance	70%	67%	-3%
	Overall Score	66%	63%	-3%
	Overall Grade	D	D	NC

FIGURE 8: Cybersecurity Assurance Report Cards by industry

Geographical Insights

The following are Risk Assessment and Security Assurance insights by country:



Making its Global Cybersecurity Assurance Report Card debut in first place overall, India earned the only "A" in the entire 2017 report with its Security Assurance score, which was also the highest score recorded for any geography or industry. India's security pros felt the most confident in their ability to measure security effectiveness and align security to business objectives. This confidence combined with an above average Risk Assessment score placed India firmly ahead of everyone and six points higher than second-place United States.

Strengths

- 1 Measuring security effectiveness (A+)
- 2 Aggregating risk intelligence (A)
- 3 Aligning security with the business (A)

Weaknesses

- 1 Assessing laptops and notebooks (F)
- 2 Assessing containerization platforms (D+)
- 3 Assessing DevOps environments (D+)



Although the United States' overall score dropped by two points, it is still well above the 70% global average. The United States scored second-highest on Risk Assessment and Security Assurance, behind India.

Strengths

- 1 Measuring security effectiveness (A-)
- 2 Conveying risks to executives and board members (B+)
- 3 Viewing network risks continuously (B)

Weaknesses

- 1 Assessing containerization platforms (F)
- 2 Assessing DevOps environments (D)
- 3 Assessing mobile devices (D)



Canada's scores showed the least variance between 2016 and 2017. Its overall score was third best, behind India and the United States. Like most countries, it struggled with assessing risks in container and DevOps environments.

Strengths

- 1 Measuring security effectiveness (B+)
- 2 Viewing network risks continuously (B+)
- 3 Aligning security with the business (B+)

Weaknesses

- 1 Assessing containerization platforms (F)
- 2 Assessing virtual servers in datacenters (D)
- 3 Assessing DevOps environments (D+)



FRANCE

RISK ASSESSMENT
67%

SECURITY ASSURANCE
80%

AVERAGE SCORE
74%

AVERAGE GRADE
C *(Satisfactory in France)*

For its debut in the Global Cybersecurity Assurance Report Card, France's overall scores were above average and respondents in the country felt particularly confident in their ability to align security with the business.

Strengths

- 1 Measuring security effectiveness (B)
- 2 Aligning security with the business (B)
- 3 Executive and board-level commitment (B-)

Weaknesses

- 1 Assessing mobile devices (F)
- 2 Assessing DevOps environments (F)
- 3 Assessing cloud environments (D)



AUSTRALIA

RISK ASSESSMENT
64% (-5%)

SECURITY ASSURANCE
78% (+9%)

AVERAGE SCORE
71% (+2%)

AVERAGE GRADE
C- *(Pass in Australia)*

Australia is the only entity (country or industry) to achieve a higher overall score in this year's report. Although its Risk Assessment score dropped five points to 64% (D), its Security Assurance score rose to 78% (C+) — the most improved score of any country or industry.

Strengths

- 1 Viewing network risks continuously (B-)
- 2 Measuring security effectiveness (B-)
- 3 Conveying risks to executives and board members (B-)

Weaknesses

- 1 Assessing DevOps environments (F)
- 2 Assessing physical servers in datacenters (D)
- 3 Assessing mobile devices (F)



UNITED KINGDOM

RISK ASSESSMENT
59% (-14%)

SECURITY ASSURANCE
73% (-1%)

AVERAGE SCORE
66% (-8%)

AVERAGE GRADE
D *(Fail in UK)*

Compared to its middle-of-the-road scores from last year, the United Kingdom's confidence is down this year, with a 14-point drop in Risk Assessment. However, the UK maintained about the same level of Security Assurance.

Strengths

- 1 Measuring security effectiveness (B-)
- 2 Conveying risks to executives and board members (C+)
- 3 Viewing network risks continuously (C)

Weaknesses

- 1 Assessing containerization platforms (F)
- 2 Assessing DevOps environments (F)
- 3 Assessing web applications (F)



SINGAPORE

RISK ASSESSMENT

68% (-1%)

SECURITY ASSURANCE

60% (-15%)

AVERAGE SCORE

64% (-8%)

AVERAGE GRADE

D (D in Singapore)

Although Singapore excelled in measuring security effectiveness, it suffered a 15-point drop in Security Assurance — the largest of any country surveyed — to earn a 64% (D) overall, a full letter grade lower than last year. Interestingly, Singapore ranked much higher than average in three areas that challenged other 2017 respondents.

Strengths

- 1 Assessing DevOps environments (C-)
- 2 Assessing cloud environments (C-)
- 3 Assessing mobile devices (C-)

Weaknesses

- 1 Aggregating risk intelligence (F)
- 2 Viewing network risks continuously (F)
- 3 Conveying risks to executives and board members (D-)



GERMANY

RISK ASSESSMENT

44% (-25%)

SECURITY ASSURANCE

79% (+5%)

AVERAGE SCORE

62% (-10%)

AVERAGE GRADE

D- (4- in Germany)

Germany suffered the most pronounced single-score drop of any country or industry surveyed for 2017. Germany's Risk Assessment score plunged 25 points from 69% (D+) to 44% (F). Security Assurance rose by five points to 79% (C+). Its overall 2017 score is 62% (D-), which is well below the global average and a full grade lower than last year.

Strengths

- 1 Viewing network risks continuously (B)
- 2 Conveying risks to executives and board members (B)
- 3 Aligning security with the business (B-)

Weaknesses

- 1 Assessing DevOps environments (F)
- 2 Assessing network infrastructure (F)
- 3 Assessing the network perimeter/DMZ (F)



JAPAN

RISK ASSESSMENT

43%

SECURITY ASSURANCE

52%

AVERAGE SCORE

48%

AVERAGE GRADE

F (Fail in Japan)

Japan is new to this year's survey, but failing scores across the board indicate that there is much work to be done as they continue to address emerging security challenges. Security practitioners in Japan assigned themselves the lowest Security Assurance score by eight points at 52% (F) — 27 points lower than the global average.

Strengths

- 1 No passing scores

Weaknesses

- 1 Assessing DevOps environments (F)
- 2 Assessing mobile devices (F)
- 3 Assessing containerization platforms (F)

Industrial Insights

The following are Risk Assessment and Security Assurance insights by industry:



RETAIL

RISK ASSESSMENT

66% (-9%)

SECURITY ASSURANCE

86% (+7%)

OVERALL SCORE

76% (-1%)

OVERALL GRADE

C

With an overall report card score of 76% (C), Retail sits in first place among industries surveyed. Although the Risk Assessment confidence levels of Retail infosec pros dropped nine points to 66% (D), survey respondents felt more confident this year in their ability to assess risks in the cloud, giving Retail an 80% (B-).

Strengths

- 1 Viewing network risks continuously (A-)
- 2 Conveying risks to executives and board members (B+)
- 3 Assessing cloud environments (B-)

Weaknesses

- 1 Assessing physical servers in datacenters (F)
- 2 Assessing network infrastructure (F)
- 3 Assessing virtual servers in datacenters (F)



FINANCIAL SERVICES

RISK ASSESSMENT

59% (-20%)

SECURITY ASSURANCE

85% (+1%)

OVERALL SCORE

72% (-9%)

OVERALL GRADE

C-

Financial Services took the second-biggest hit of any industry with an overall score of 72% (C-), which was good enough to be tied with Manufacturing for second place, but down nine points from 2016 when Financial Services was tied for first place with Telecom. Driving the sharp decline was the single-largest Risk Assessment drop of the year — down 20 points to 59% (F).

Strengths

- 1 Measuring security effectiveness (B+)
- 2 Aligning security with the business (B)
- 3 Conveying risks to executives and board members (B)

Weaknesses

- 1 Assessing containerization platforms (F)
- 2 Assessing virtual servers in datacenters (F)
- 3 Assessing desktops / PCs (F)



MANUFACTURING

RISK ASSESSMENT

59% (-13%)

SECURITY ASSURANCE

86% (+6%)

OVERALL SCORE

72% (-4%)

OVERALL GRADE

C-

A sharp 13-point decline in Risk Assessment was partially offset by a modest six-point increase in Security Assurance to earn Manufacturing an overall 2017 report card score of 72% (C-) — enough to be tied with Financial Services for second place.

Strengths

- 1 Measuring security effectiveness (B+)
- 2 Executive and board-level commitment (B+)
- 3 Conveying risks to executives and board members (B+)

Weaknesses

- 1 Assessing containerization platforms (F)
- 2 Assessing the network perimeter/DMZ (F)
- 3 Assessing DevOps environments (F)



TELECOM

RISK ASSESSMENT

60% (-17%)

SECURITY ASSURANCE

81% (-4%)

OVERALL SCORE

70% (-11%)

OVERALL GRADE

C-

Tied with Financial Services for first place last year, Telecom did not feel as confident this year in its ability to assess risks, and had the biggest drop in overall report card score for any industry, sliding 11 points to fourth place with a 70% (C-).

Strengths

- 1 Measuring security effectiveness (B+)
- 2 Conveying risks to executives and board members (B)
- 3 Viewing network risks continuously (B)

Weaknesses

- 1 Assessing containerization platforms (F)
- 2 Assessing mobile devices (F)
- 3 Assessing cloud environments (F)



HEALTH CARE

RISK ASSESSMENT

54% (-18%)

SECURITY ASSURANCE

76% (+1%)

OVERALL SCORE

65% (-8%)

OVERALL GRADE

D

Health Care security professionals reported less confidence in their ability to assess security risk this year, awarding their industry a 54% (F) — 18 points lower than 2016. A negligible increase in Security Assurance netted Health Care an eight-point drop for an overall report card score of 65% (D).

Strengths

- 1 Conveying risks to executives and board members (B-)
- 2 Measuring security effectiveness (B-)
- 3 Viewing network risks continuously (B-)

Weaknesses

- 1 Assessing DevOps environments (F)
- 2 Assessing containerization platforms (F)
- 3 Assessing mobile devices (F)



EDUCATION

RISK ASSESSMENT

64% (-1%)

SECURITY ASSURANCE

63% (-1%)

OVERALL SCORE

64% (no change)

OVERALL GRADE

D

Education's overall score was unchanged year-over-year, but that was good enough to bump it out of last place this year with a 64% (D). Education security professionals reported the lowest 2017 Security Assurance score of any industry with 63% (D).

Strengths

- 1 Assessing the network perimeter/DMZ (B)
- 2 Assessing physical servers in the datacenter (B-)
- 3 Measuring security effectiveness (C)

Weaknesses

- 1 Assessing cloud environments (F)
- 2 Conveying risks to executives and board members (F)
- 3 Executive and board-level commitment (F)



GOVERNMENT

RISK ASSESSMENT

59% (-4%)

SECURITY ASSURANCE

67% (-3%)

OVERALL SCORE

63% (-3%)

OVERALL GRADE

D

Government fell three points to land in last place this year with an overall report card score of 63% (D), just one point lower than Education.

Strengths

- 1 Measuring security effectiveness (B-)
- 2 Viewing network risks continuously (C+)
- 3 Conveying risks to executives and board members (C-)

Weaknesses

- 1 Aggregating risk intelligence (F)
- 2 Assessing cloud environments (F)
- 3 Assessing DevOps environments (F)

The Road Ahead

To provide additional insight into the mindset of security professionals, respondents were asked two questions not associated with the Risk Assessment or Security Assurance indices. The first question asked the following: “Compared to this time last year, do you feel more optimistic or pessimistic about your organization’s ability to defend itself against cyber attacks?” The responses are depicted in Figure 9 below.

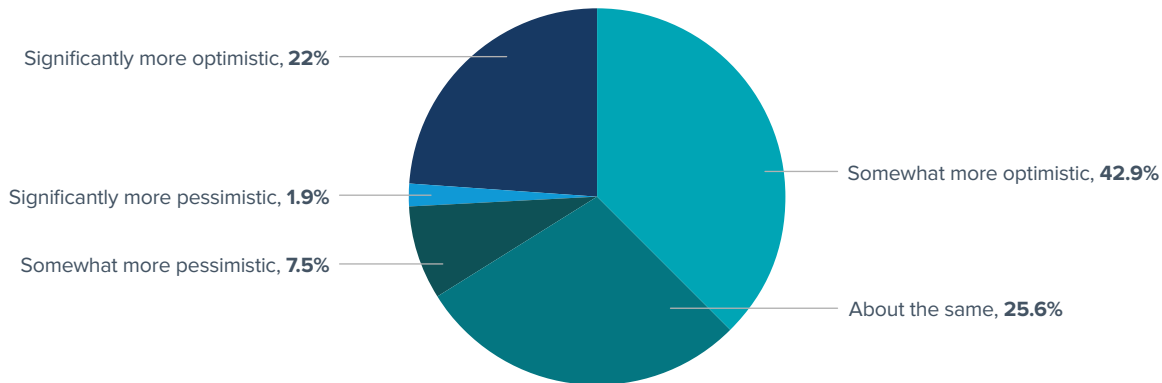


FIGURE 9: *Optimism now versus one year ago for defending against cyber attacks*

Optimism among IT security professionals in 2017 is similar to last year’s findings. Despite the number of data breach headlines, and present concern about the inability to properly assess IT security risks brought on by new and emerging technologies, respondents are generally optimistic about the future, perhaps fueled by new investments in people and/or technology, and the concerted effort to make security a boardroom-level issue.

The second question posed the following: “On a scale of 1 to 5, with 5 being highest, rate each of the following challenges facing IT security professionals today.” The results are depicted in Figure 10.

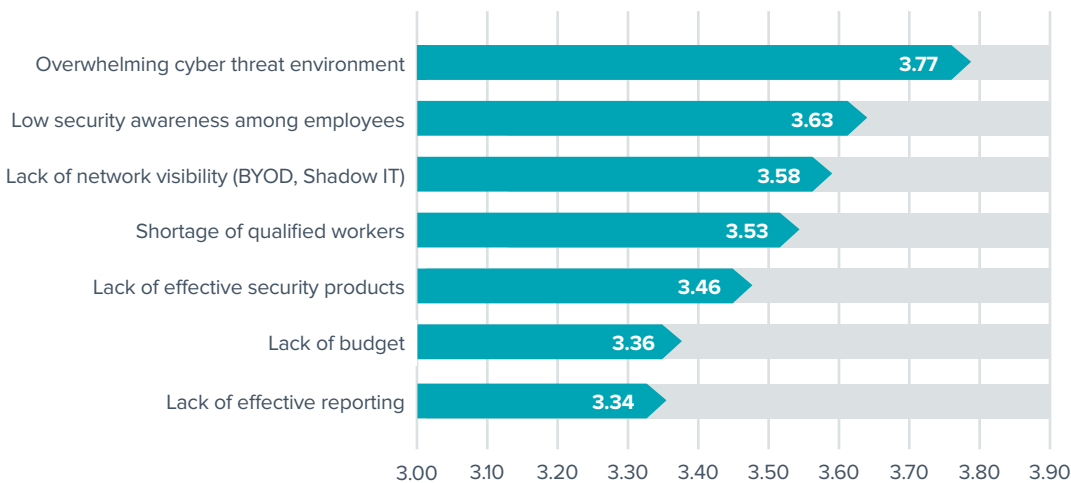


FIGURE 10: *Top challenges facing IT security professionals*

The top two most common responses — overwhelming cyber threat environment and low security awareness among employees — are the same top responses from last year. However, a new survey response, lack of network visibility, was added this year and was the third biggest challenge for organizations.

There's no question that BYOD and shadow IT cause headaches among security professionals. Both trends bring unapproved and non-secure devices onto corporate networks, making it nearly impossible for security teams to detect them. Both scenarios bring substantial risk to an already risk-heavy environment.

Based off the findings of the 2017 Global Cybersecurity Assurance Report Card, what can security professionals and organizations, alike, do to improve their Risk Assessment and Security Assessment scores? Here are some suggestions to get started:

- 1 Know Yourself** You can't secure what you can't see. These days this not only means having continuous visibility into cloud, hybrid and on-premises environments, but organizations also have to stay ahead of security challenges that accompany new trends and technologies.

This year, visibility is more important than ever. Now, alongside cloud, mobile, BYOD and shadow IT, DevOps and containerization are forcing security pros to once again re-think the approach to information security.

Continuous visibility equals rapid detection of threats and vulnerabilities, which is why active scanning — even if frequent — is no longer enough. Organizations need passive vulnerability scanning and log correlation to achieve true continuous and pervasive monitoring. The combination of active, passive and log/event correlation drastically reduces the attack surface and helps detect threats faster and with greater accuracy by continuously uncovering and tracking users, applications, cloud environments, and mobile devices. This also allows organizations to perform continuous vulnerability assessment across all network assets.

- 2 Define and Convey Success** With nation-state cyber attacks and massive data breaches in the news every day, cybersecurity is now firmly in the spotlight and security pros are being held accountable to the business in ways they haven't before. As the cybersecurity industry matures, there are higher expectations for security teams to contribute meaningfully to board-level decision making. Knowing themselves is a good start, but today's security teams must also be able to convey that sense of self to others.

This year's survey results show executive and board-level commitment lagging behind the abilities of the world's security professionals to measure security effectiveness and convey risks up the chain. Executive-level reporting on organizational risk posture enables the kind of informed decision making senior business leaders need to meet the technology challenges of tomorrow. Having the right metrics is crucial to convincing senior executives that cybersecurity should be taken as a high-level business concern, but it is up to the security practitioners to make these metrics readily available and easily digestible for people without in-depth security expertise.

- 3 A Balanced Approach to Security** Threats evolve and most security vendors have been slow to adapt. There is a better way, one that is simpler and more intuitive, and can help organizations achieve security balance with less resources.

The days of buying and managing 80 or 90 “best-of-breed” layered security products from dozens of different vendors are over. Organizations need a balanced approach to security investment with solutions that — even if from different vendors — are still part of a security ecosystem where everything works together — seamlessly and intelligently — to deliver comprehensive protection from threats and vulnerabilities and, through risk prioritization and actionable insights, helps answer the question: “What can I do right now to improve security for my organization today?”

Appendix 1: Survey Demographics

Countries

Of the 700 respondents, 43% were based in North America (U.S. & Canada), 32% in Europe (U.K., Germany & France), and 25% in Asia Pacific (Australia, Singapore, Japan & India). Figure 11 depicts the breakdown of respondents by country.

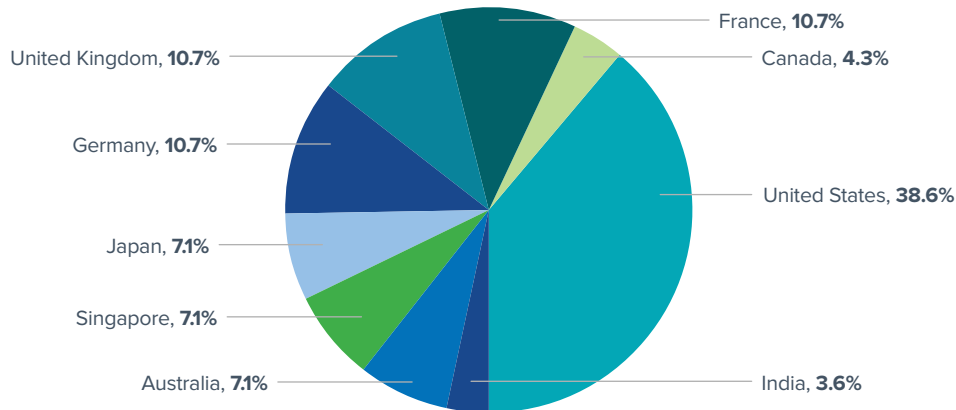


FIGURE 11: Respondents by country

IT Security Roles

Of the 700 respondents, three-quarters (combined 75%) held manager, director, or executive leadership roles. Figure 12 depicts the breakdown of respondents by IT security role.

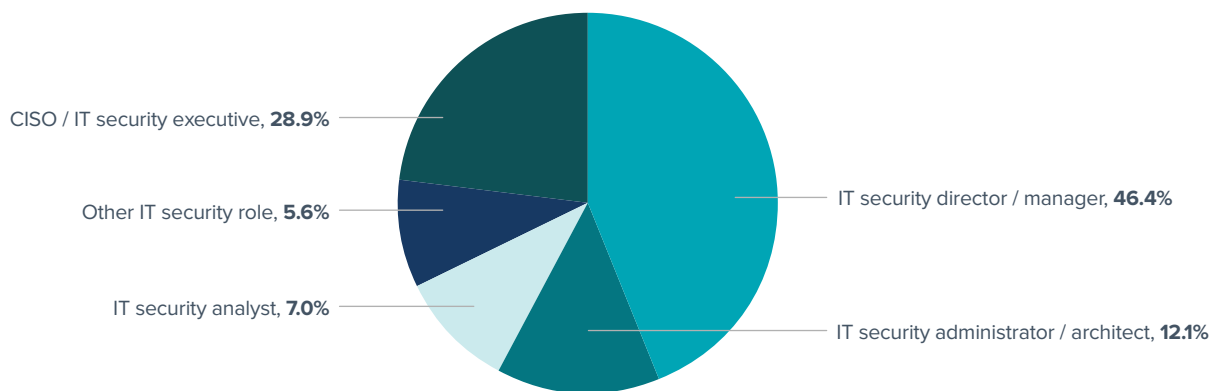


FIGURE 12: Respondents by IT security role

Organization Size

Of the 700 respondents, more than one-third (combined 35%) were employed by organizations with 10,000 or more employees worldwide. Figure 13 depicts the breakdown of respondents by organization size (i.e., worldwide employee count).

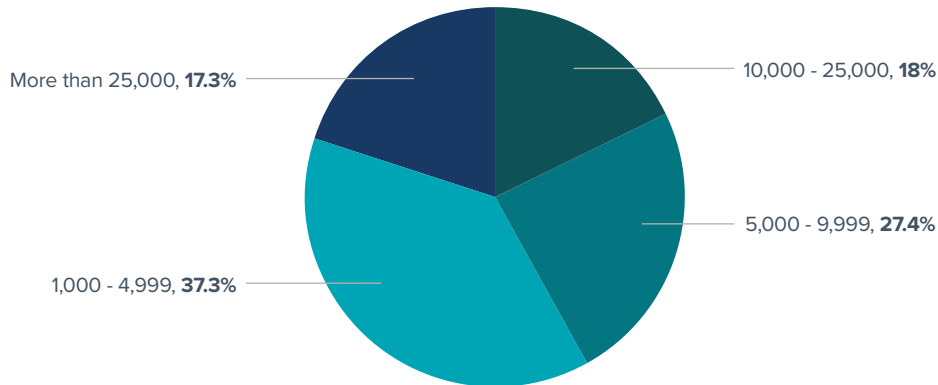


FIGURE 13: Respondents by organization's worldwide employee count

Industries

IT security professionals from 19 industries participated in this year's study, with no more than 15% derived from any single industry. Figure 14 depicts the breakdown of responses by industry (see question 3 in Appendix 3 for a list of full industry descriptions).

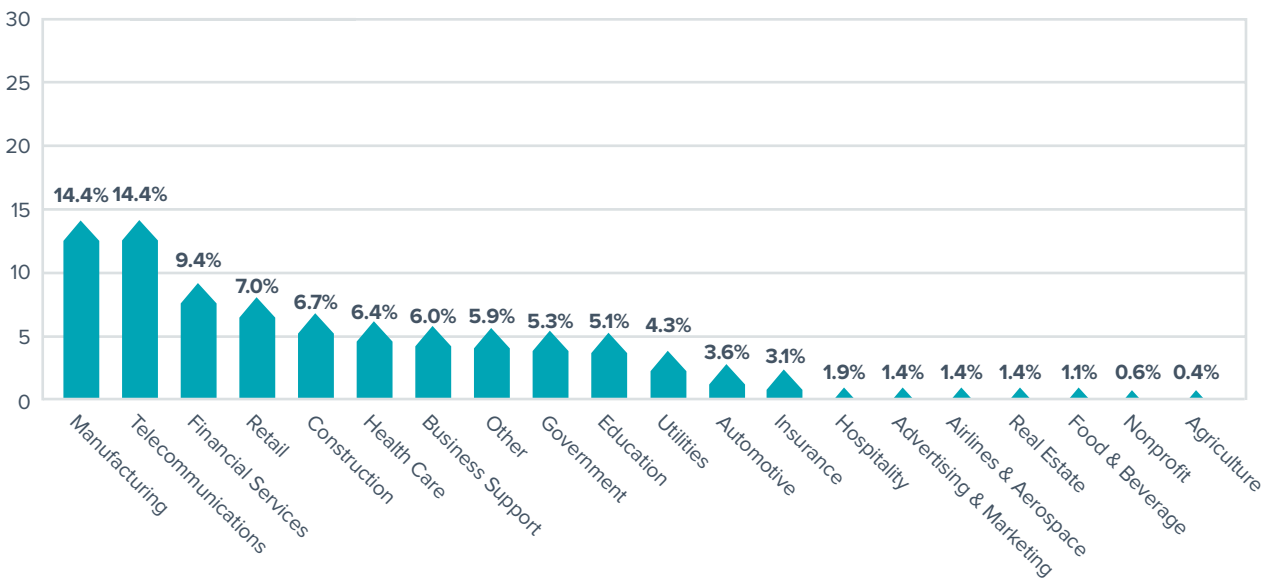


FIGURE 14: Respondents by industry

Appendix 2: Research Methodology

CyberEdge Group developed a 12-question web-based survey instrument in partnership with Tenable Network Security. The survey was promoted to information security professionals across nine countries and three geographic regions — United States and Canada (North America), United Kingdom, Germany, and France (Europe), and Australia, Singapore, Japan, and India (Asia Pacific). The survey was translated for all non-English-speaking target audiences.

The online survey was conducted in October 2016. Each respondent met two demographic requirements: (1) employed for an organization with 1,000+ employees globally and (2) held an IT security position (i.e., not an IT generalist). Respondents that failed to meet either of these criteria were exited from the survey.

Sample Sizes

Respondents were derived from 19 industries and nine countries. Each country and industry referenced in this report included a minimum of 25 responses. Responses from industries with fewer than 25 responses were reported in the aggregate, globally and by country.

The following are sample sizes by geography in decreasing order:

- ▶ Global: 700 (100%)
- ▶ United States: 270 (38.6%)
- ▶ United Kingdom: 75 (10.7%)
- ▶ Germany: 75 (10.7%)
- ▶ France: 75 (10.7%)
- ▶ Australia: 50 (7.1%)
- ▶ Singapore: 50 (7.1%)
- ▶ Japan: 50 (7.1%)
- ▶ Canada: 30 (4.3%)
- ▶ India: 25 (3.6%)

The following are sample sizes by industry in decreasing order:

- ▶ Manufacturing: 101 (14.4%)
- ▶ Telecom, Technology, Internet, and Electronics: 101 (14.4%)
- ▶ Finance & Financial Services: 66 (9.4%)
- ▶ Retail & Consumer Durables: 49 (7.0%)
- ▶ Health Care & Pharmaceuticals: 45 (6.4%)
- ▶ Government: 37 (5.3%)
- ▶ Education: 36 (5.1%)

Analysis

Each score was derived by adding together the percentages of the two most-favorable responses of associated questions. Risk Assessment scores are associated with 11 IT components depicted in question 6 (see Appendix 3). Security Assurance scores are associated with questions 7-12.

Typical American grades were assigned to each index score (along with international grades for high-level index scores for non-U.S. countries) using the following scale:

GRADE	RANGE
A+	100%
A	93-99%
A-	90-92%
B+	87-89%
B	83-86%
B-	80-82%
C+	77-79%
C	73-76%
C-	70-72%
D+	67-69%
D	63-66%
D-	60-62%
F	< 60%

Quality Control

Each (non-demographic) survey question included a “Don’t know” response, minimizing the potential for respondents to over-reach by answering questions outside their respective areas of expertise or responsibility. All findings within this report were derived after “Don’t know” response counts were excluded, thus slightly decreasing the sample size of responses for each question by country and industry.

All qualified survey responses were inspected for potential survey “cheaters,” meaning survey takers that responded to questions in a consistent pattern (e.g., all “A” responses, repeating A-B-C-A-B-C responses) and/or completed the survey in a fraction of the median survey completion time in an attempt to complete the survey quickly. Suspected cheater survey responses were deleted from the pool of responses.

Appendix 3: Online Survey Questions

The following questions were asked of 700 security professionals employed by organizations with 1,000+ employees worldwide:

Demographics

- 1 Select the option that best describes **your role** in your organization's **IT security** department.
 - a CISO / IT security executive
 - b IT security director / manager
 - c IT security administrator / architect
 - d IT security analyst
 - e Other IT security role
 - f I do not work in IT security
- 2 How many individuals are **employed** by your organization **worldwide**?
 - a More than 25,000
 - b 10,000-25,000
 - c 5,000-9,999
 - d 1,000-4,999
 - e Less than 1,000
- 3 Which best describes your employer's **primary industry**?
 - a Advertising & Marketing
 - b Agriculture
 - c Airlines & Aerospace (including Defense)
 - d Automotive
 - e Business Support & Logistics
 - f Construction, Machinery, and Homes
 - g Education
 - h Finance & Financial Services
 - i Food & Beverages
 - j Government
 - k Health Care & Pharmaceuticals
 - l Hospitality, Entertainment, and Leisure
 - m Insurance
 - n Manufacturing
 - o Nonprofit
 - p Retail & Consumer Durables
 - q Real Estate
 - r Telecommunications, Technology, Internet, and Electronics
 - s Utilities, Energy, and Extraction
 - t Other (please specify)

Optimism & Challenges

- 4 **Compared to this time last year**, do you feel **more optimistic or pessimistic** about your **organization's ability to defend itself** against cyber attacks?
 - a Significantly more optimistic
 - b Somewhat more optimistic
 - c About the same
 - d Somewhat more pessimistic
 - e Significantly more pessimistic
 - f Don't know
- 5 On a scale of 1 to 5, with 5 being highest, rate each of the following **challenges facing IT security professionals today**:
 - a Lack of budget
 - b Lack of effective reporting
 - c Lack of effective security products
 - d Lack of network visibility (BYOD, Shadow IT)
 - e Low security awareness among employees
 - f Overwhelming cyber threat environment
 - g Shortage of qualified workers

Risk Assessment

- 6 On a scale of 1 to 5, with 5 being highest, rate your organization's **ability to assess risks** (vulnerabilities and security misconfigurations) associated with each of the following IT components:
 - a Cloud environments (SaaS, IaaS, PaaS)
 - b Containerization platforms (Docker, CoreOS)
 - c Datacenter / physical servers
 - d Datacenter / virtual servers
 - e Desktops (PCs)
 - f DevOps environments
 - g Laptops / notebooks
 - h Mobile devices (smartphones, tablets)
 - i Network infrastructure components (routers, firewalls)
 - j Network perimeter / DMZ (web servers)
 - k Web applications (custom built)

Security Assurance

- 7 Describe your agreement with the following statement: "My organization has the **tools necessary** to **accurately measure the overall effectiveness** of our **security investments**?"
- a Strongly agree
 - b Somewhat agree
 - c Neither agree nor disagree
 - d Somewhat disagree
 - e Strongly disagree
 - f Don't know
- 8 Describe your agreement with the following statement: "My organization has the **tools necessary** to **continuously view network assets** and their **inherent security risks** in real time."
- a Strongly agree
 - b Somewhat agree
 - c Neither agree nor disagree
 - d Somewhat disagree
 - e Strongly disagree
 - f Don't know
- 9 Describe your agreement with the following statement: "My organization has the **tools necessary** to **aggregate real-time risk intelligence** from disparate sources into a **unified security platform**."
- a Strongly agree
 - b Somewhat agree
 - c Neither agree nor disagree
 - d Somewhat disagree
 - e Strongly disagree
 - f Don't know
- 10 Describe your agreement with the following statement: "My company's **IT executives** (CIO/CISO) properly **align IT security initiatives** with **key business objectives**."
- a Strongly agree
 - b Somewhat agree
 - c Neither agree nor disagree
 - d Somewhat disagree
 - e Strongly disagree
 - f Don't know
- 11 Describe your agreement with the following statement: "My organization has the **tools necessary** to **accurately convey information security risks** to our company's **executive team and board of directors**."
- a Strongly agree
 - b Somewhat agree
 - c Neither agree nor disagree
 - d Somewhat disagree
 - e Strongly disagree
 - f Don't know
- 12 Describe your agreement with the following statement: "My company's **executive team and board of directors** are **giving IT security the attention it deserves**."
- a Strongly agree
 - b Somewhat agree
 - c Neither agree nor disagree
 - d Somewhat disagree
 - e Strongly disagree
 - f Don't know

Appendix 4: About CyberEdge Group

CyberEdge Group is an award-winning research, marketing, and publishing firm serving the needs of information security vendors and service providers. Founded in 2012 and headquartered in Annapolis, Maryland, CyberEdge has rapidly become the pre-eminent provider of custom security research backed by proven methodologies, broad geographic reach, and unparalleled integrity and objectivity.

CyberEdge is widely regarded for its annual Cyberthreat Defense Report (CDR), which has garnered wide-scale attention by dozens of business and technology media outlets, including USA Today, Bloomberg, CNBC, SC Magazine, Information Week, and others. CyberEdge's uncanny ability to harvest keen insights from research data has elevated CyberEdge to become a true thought leader in the information security industry.

For more information on CyberEdge's research, marketing, and publishing services, contact the company at info@cyber-edge.com or **800-327-8711**. Or connect to CyberEdge's website at cyber-edge.com.