2016 Global Cybersecurity Assurance Report Card

tenable®
network security

tenable network security

Introduction

Over the last twelve months the world has seen costly and destructive cyberattacks target organizations of all sizes regardless of industry or geography. With attackers breaching the world's cyber defenses seemingly at will, the ability of organizations to successfully defend themselves against a proliferating threat environment has become uncertain. At risk are the private data of citizens, billions in international business revenue and the security of nations. With so much at stake, organizations need to know where their security programs are effective and where they are falling short.

The objective of this inaugural Tenable Network Security research study is to measure how enterprise IT security professionals view their organization's ability to assess cybersecurity risks and to mitigate threats that can exploit those risks. In doing so, Tenable has developed the industry's first Global Cybersecurity Assurance Report Card, which assigns indices and grades to responding organizations globally, by country, and by industry based on the responses of the security practitioners themselves.

To uncover just how well organizations across the globe are able to assess and mitigate cyber risk, Tenable surveyed 504 IT security professionals employed by organizations with 1,000+ employees in August 2015. A 12-question web-based survey was developed (see Appendix 3). Survey questions asked respondents to provide a rating on a 5-point scale. By adding together the two most-favorable responses (e.g., Strongly agree + Somewhat agree) for each question, and then averaging together associated responses, two summary indices were derived, as follows:

73%

Risk Assessment Index

Represents the organization's ability to assess cybersecurity risks across 10 key components of enterprise IT infrastructure

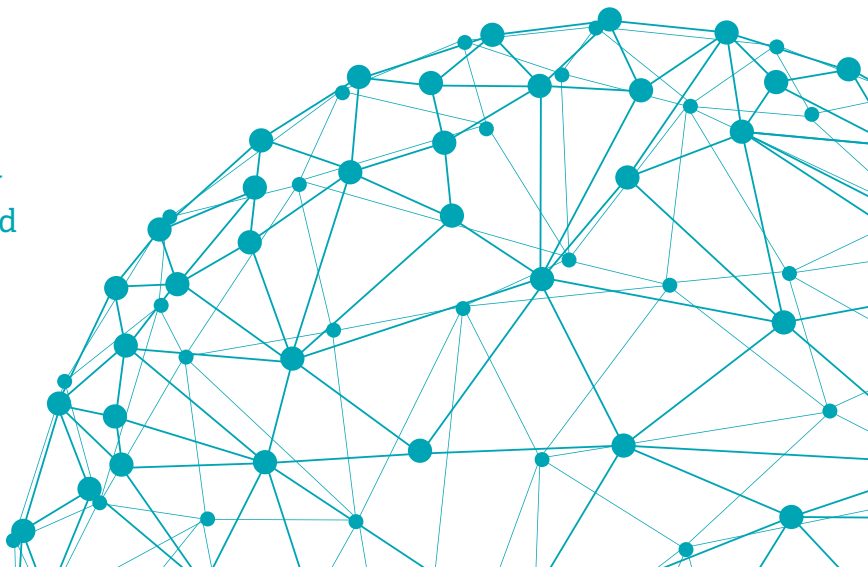
79%

Risk Assessment Index

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

76%

Global Cybersecurity Assurance Report Card



tenable network security

Executive Summary

In the United States, a "C" grade is commonly viewed as underachieving, and that is what the 2016 Global Cybersecurity Assurance Report Card survey data reflect. Worldwide, the 504 security practitioners surveyed collectively reported just 73% on the Risk Assessment Index and 79% on the Security Assurance Index. These two figures average to 76%— earning an unremarkable "C."

This inaugural report yielded dozens of insights into how IT security professionals assess and mitigate cybersecurity risks. These insights are depicted within three sections of this report: Global Insights, Geographical Insights, and Industrial Insights. The following are some of the key takeaways:

1. **Nobody's perfect.** The highest overall grade by country and by industry is a "B-," with most falling into the "C" and "D" ranges. This means that more than 20% of responding organizations are not confident in their abilities to assess and mitigate cybersecurity risks. In today's challenging cyberthreat environment, these scores point to much room for improvement.

2. **Stuck in the cloud.** Respondents consistently cited cloud applications (D+) and cloud infrastructure (D) as two of the three most challenging IT components for assessing cybersecurity risks. According to survey results, the most challenging IT component for assessing security risks is cloud infrastructure (IaaS, PaaS). No other areas across all 16 aspects of the survey gave IT security respondents more trouble.

3. **A mobile dilemma.** Rounding out the bottom three, mobile devices (D) also were reported as being particularly challenging for assessing risks. An inability to even detect transient mobile devices in the first place was another big challenge (C).

4. **Uninvested board members.** On the upside, respondents largely believe they've got the tools in place to measure overall security effectiveness (B-) and to convey security risks to executives and board members (B). On the downside, respondents question whether their executives and board members fully understand those security risks (C+) and are investing enough to mitigate them (C).

5. **North Americans earn top marks.** The United States nudged out Canada to earn the highest Global Cybersecurity Assurance Report Card score of any country surveyed. Although Canada achieved a slightly higher Security Assurance score than its neighbor to the south, it wasn't enough to overcome the United States' stronger Risk Assessment score.

6. **Trouble down under.** Although Australia's Risk Assessment score was comparable to Germany and Singapore, its Security Assurance score was the lowest of all, earning Australia a last place finish among the six countries surveyed.

7. **Finance and Telecom/Tech tied at the top.** The Financial Services and Telecommunications & Technology industries both earned the highest Cybersecurity Assurance Report Card score. Financial Services scored top marks in Risk Assessment while Telecom & Tech took first place for Security Assurance.

8. **Education industry has lessons to learn.** Among the seven most common industries represented, the Education industry trails the pack with overall lowest score, lowest Security Assurance Index score, and second-lowest Risk Assessment Index score.

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 improve your organization's ability to minimize cybersecurity risks.

tenable network security

Risk Assessment Report Cards

The Risk Assessment Index conveys an organization's ability to assess cybersecurity risks across 10 key IT infrastructure components, as shown in question 6 of the web-based survey (see Appendix 3) and in Figures 1 and 2 below (in abbreviated form). Figure 1 represents global scores followed by scores for each country in decreasing order of average score. Figure 2 depicts scores by industry, also in decreasing order of average score.

	GLOBAL		USA		UK		CANADA		GERMANY		AUSTRALIA		SINGAPORE	
	%	Grade	%	Grade	%	Grade	%	Grade	%	Grade	%	Grade	%	Grade
Cloud Apps (Saas)	69%	D+	72%	C-	69%	D+	67%	D+	71%	C-	67%	D+	63%	D
Cloud Infrastructure (IaaS)	64%	D	67%	D+	66%	D	59&	F	69%	D+	50%	F	63%	D
Datacenter / Physical Servers	77%	C+	80%	B-	75%	C	79%	C+	81%	B-	68%	D+	79%	C+
Datacenter / Virtual Servers	76%	C	79%	C+	74%	C	71%	C-	83%	B	72%	C-	78%	C+
Desktops (PCs)	78%	C+	81%	B-	85%	B	68%	D+	69%	D+	80%	B-	70%	C-
Laptops / Notebooks	77%	C+	79%	C+	77%	C+	68%	D+	71%	C-	88%	B+	73%	C
Mobile Devices	65%	D	66%	D	59%	F	79%	C+	57%	F	68%	D+	65%	D
Network Perimeter / DMZ	72%	C-	77%	C+	73%	C	67%	D+	65%	D	76%	C	65%	D
Web Applications	80%	B-	78%	C+	73%	C	68%	D+	59%	F	60%	D-	63%	D
Network Infrastructure	73%	C	86%	B	82%	B-	71%	C-	67%	D+	64%	D	71%	C-
AVERAGE	**73%**	**C**	**77%**	**C+**	**73%**	**C**	**70%**	**C-**	**69%**	**D+**	**69%**	**D+**	**69%**	**D+**

FIGURE 1: *Risk Assessment Index scores by country*

	FINANCIAL SVS.		TELECOM		RETAIL		HEALTH CARE		MANUFACT'ING		EDUCATION		GOVERNMENT	
	%	Grade	%	Grade	%	Grade	%	Grade	%	Grade	%	Grade	%	Grade
Cloud Apps (Saas)	72%	C-	68%	D+	71%	C-	64%	D	63%	D	52%	F	57%	F
Cloud Infrastructure (IaaS)	67%	D+	72%	C-	71%	C-	64&	D	63%	D	38%	F	46%	F
Datacenter / Physical Servers	84%	B	83%	B	75%	C	79%	C+	73%	C	79%	C+	67%	D+
Datacenter / Virtual Servers	79%	C+	78%	C+	83%	B	71%	C-	78%	C+	68%	D+	67%	D+
Desktops (PCs)	86%	B	83%	B	75%	C	75%	C	85%	B	75%	C	63%	D
Laptops / Notebooks	84%	B	80%	B-	71%	C-	79%	C+	81%	B-	61%	D-	67%	D+
Mobile Devices	70%	C-	72%	C-	63%	D	50%	F	65%	D	57%	F	50%	F
Network Perimeter / DMZ	77%	C+	77%	C+	67%	D	81%	B-	68%	D+	67%	D+	77%	C+
Web Applications	81%	B-	75%	C	79%	C+	73%	C	70%	C-	63%	D	59%	F
Network Infrastructure	93%	A	81%	B-	92%	A-	81%	B-	77%	C+	86%	B	72%	C-
AVERAGE	**79%**	**C+**	**77%**	**C+**	**75%**	**C**	**72%**	**C-**	**72%**	**C-**	**69%**	**D**	**63%**	**D**

FIGURE 2: *Risk Assessment Index scores by industry*

tenable network security

Security Assurance Report Cards

The Security Assurance Index conveys an organization's ability to mitigate threats by investing in security infrastructure fueled by executive- and board-level commitment (see Appendix 3 to view questions 5, 6, 8, 9, 10, and 11).

	GLOBAL		CANADA		USA		UK		SINGAPORE		GERMANY		AUSTRALIA	
	%	Grade	%	Grade	%	Grade	%	Grade	%	Grade	%	Grade	%	Grade
Measuring Effectiveness	81%	B-	79%	C+	86%	B	79%	C+	78%	C+	74%	C	72%	C-
Detecting Transient Devices	75%	C	86%	B	79%	C+	63%	D	70%	C-	72%	C-	60%	D-
Detecting Internal Threats	83%	B	90%	A-	87%	B+	76%	C	72%	C-	77%	C+	76%	C
Board-level Understanding	77%	C+	82%	B-	80%	B-	70%	C-	76%	C	70%	C-	68%	D+
Conveying Risks to Board	83%	B	89%	B+	86%	B	82%	B-	76%	C	80%	B-	72%	C-
Board-level Commitment	76%	C	79%	C+	77%	C+	77%	C+	76%	C	70%	C-	68%	D+
AVERAGE	**79%**	**C+**	**84%**	**B**	**83%**	**B**	**74%**	**C**	**75%**	**C**	**74%**	**C**	**69%**	**D+**

FIGURE 3: *Security Assurance Report Cards by country*

	GOVERNMENT		TELECOM		MANUFACT'ING		EDUCATION		HEALTH CARE		RETAIL		FINANCIAL SVS.	
	%	Grade	%	Grade	%	Grade	%	Grade	%	Grade	%	Grade	%	Grade
Measuring Effectiveness	85%	B	84%	B	83%	B	80%	B-	81%	B-	80%	B-	67%	D+
Detecting Transient Devices	84%	B	86%	B	77%	C+	76&	C	61%	D-	59%	F	53%	F
Detecting Internal Threats	83%	B	84%	B	84%	B	80%	B-	86%	B	83%	B	77%	C+
Board-level Understanding	84%	B	84%	B	78%	C+	80%	B-	71%	C-	60%	D-	55%	F
Conveying Risks to Board	86%	B	86%	B	81%	B-	76%	C	79%	C+	83%	B	76%	C
Board-level Commitment	85%	B	79%	C+	75%	C	80%	B-	71%	C-	57%	F	57%	F
AVERAGE	**85%**	**B**	**84%**	**B**	**80%**	**B-**	**79%**	**C+**	**75%**	**C**	**70%**	**C-**	**64%**	**D**

FIGURE 4: *Security Assurance Report Cards by industry*

Final Grades

Averaging together overall Risk Assessment and Security Assurance scores (with equal weighting) yields an overall Cybersecurity Assurance Report Card score and grade for each country (Figure 5) and each industry (Figure 6). The global score and grade across all six countries and all seven industries is depicted in the first column of Figure 5.

	GLOBAL	USA	CANADA	UK	SINGAPORE	GERMANY	AUSTRALIA
Risk Assessment	73%	77%	70%	73%	69%	69%	69%
Security Assurance	79%	83%	84%	74%	75%	74%	69%
Overall Score	76%	80%	77%	74%	72%	72%	69%
Overall Grade	C	B-	C+	C	C-	C-	D+

FIGURE 5: *Cybersecurity Assurance Report Cards by country*

	FINANCIAL SVS.	TELECOM & TECHNOLOGY	RETAIL	MANUFACT'ING	HEALTH CARE	GOVERNMENT	EDUCATION
Risk Assessment	79%	77%	75%	72%	72%	63%	65%
Security Assurance	84%	85%	79%	80%	75%	70%	64%
Overall Score	81%	81%	77%	76%	73%	66%	64%
Overall Grade	B-	B-	C+	C	C	D	D

FIGURE 6: *Cybersecurity Assurance Report Cards by industry*

Geographical Insights

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

UNITED STATES

RISK ASSESSMENT
77% (#1 of 6)

SECURITY ASSURANCE
83% (#2 of 6)

AVERAGE SCORE
80% (#1 of 6)

AVERAGE GRADE
B-

Although achieving a B- is nothing to brag about, survey respondents from the United States clearly felt the most confident about their organizations' abilities to assess risk across the ten key IT infrastructure domains.

Strengths

1. Conveying risks to executives and board members (B)
2. Executive- and board-level understanding of risks (B)
3. Measuring effectiveness of security investments (B)

Weaknesses

1. Assessing mobile devices for risks (D)
2. Assessing cloud infrastructure (IaaS, PaaS) for risks (D+)
3. Assessing cloud applications (SaaS) for risks (C-)

CANADA

RISK ASSESSMENT
70% (#3 of 6)

SECURITY ASSURANCE
84% (#1 of 6)

AVERAGE SCORE
77% (#2 of 6)

AVERAGE GRADE
C+ *(B+ in Canada)*

Canadian respondents led the Security Assurance pack in having the highest confidence for mitigating risks fueled by executive- and board-level commitment. However, Canadian respondents are third overall in confidence for assessing network security risks.

Strengths

1. Detecting cyber threats emanating from within (A-)
2. Conveying risks to executives and board members (B+)
3. Detecting and assessing transient mobile devices (B)

Weaknesses

1. Assessing cloud infrastructure (IaaS, PaaS) for risks (F)
2. Assessing cloud applications (SaaS) for risks (D+)
3. Assessing assets at the perimeter / DMZ for risks (D+)

UNITED KINGDOM

RISK ASSESSMENT
73% (#3 of 6)

SECURITY ASSURANCE
74% (Tied #4 of 6)

AVERAGE SCORE
74% (#3 of 6)

AVERAGE GRADE
C *(Third Class in UK)*

British respondents achieved middle-of-the-road scores for both Risk Assessment and Security Assurance. The Achilles heal in the UK is clearly detecting and assessing mobile devices.

Strengths

1. Assessing desktops / PCs for risks (B)
2. Assessing assets at the perimeter / DMZ for risks (B-)
3. Conveying risks to executives and board members (B-)

Weaknesses

1. Assessing mobile devices for risks (F)
2. Detecting and assessing transient mobile devices (D)
3. Assessing cloud infrastructure (IaaS, PaaS) for risks (D)

Singaporeans struggled to convey confidence across all aspects of the online survey,

SINGAPORE

RISK ASSESSMENT
69% (Tied #4 of 6)

SECURITY ASSURANCE
75% (#3 of 6)

AVERAGE SCORE
72% (Tied #4 of 6)

AVERAGE GRADE
C- *(A2 in Singapore)*

never scoring higher than a C+ in any single area. However, as they had no marks lower than a D, Singapore is positioned in fourth place among the six countries.

Strengths

1. Assessing risks with physical servers in datacenters (C+)
2. Assessing risks with virtual servers in datacenters (C+)
3. Measuring effectiveness of security investments (C+)

Weaknesses

1. Assessing cloud infrastructure (IaaS, PaaS) for risks (D)
2. Assessing cloud applications (SaaS) for risks (D)
3. Assessing cloud applications (SaaS) for risks (D)

GERMANY

RISK ASSESSMENT
69% (Tied #4 of 6)

SECURITY ASSURANCE
74% (Tied #4 of 6)

AVERAGE SCORE
72% (Tied #4 of 6)

AVERAGE GRADE
C- *(3 in Germany)*

Responses from German survey takers varied significantly across the 16 report card data points. Marks varied from B to F, with responding German IT security organizations particularly struggling to assess network security risks outside the datacenter.

Strengths

1. Assessing risks with virtual servers in datacenters (B)
2. Assessing risks with physical servers in datacenters (B-)
3. Conveying risks to executives and board members (B-)

Weaknesses

1. Assessing mobile devices for risks (F)
2. Assessing custom web applications for risks (F)
3. Assessing assets at the perimeter / DMZ for risks (D)

AUSTRALIA

RISK ASSESSMENT
69% (Tied #4 of 6)

SECURITY ASSURANCE
69% (#6 of 6)

AVERAGE SCORE
69% (#6 of 6)

AVERAGE GRADE
D+ *(Band 3 in Australia)*

Australian respondents were challenged in conveying confidence with any aspect of the survey. Australians self-reported among the lowest scores for confidence in Risk Assessment and are in dead last for Security Assurance.

Strengths

1. Assessing laptops and notebooks for security risks (B+)
2. Assessing desktop PCs for risks (B-)
3. Detecting cyber threats emanating from within (C)

Weaknesses

1. Assessing cloud infrastructure (IaaS, PaaS) for risks (F)
2. Assessing custom web applications for risks (D-)
3. Detecting and assessing transient mobile devices (D-)

Industrial Insights

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

FINANCIAL SERVICES

RISK ASSESSMENT
79% (#1 of 7)

SECURITY ASSURANCE
84% (#2 of 7)

OVERALL SCORE
81% (Tied #1 of 7)

OVERALL GRADE
B-

Financial Services respondents tied those from Telecom & Technology for first place in their overall confidence for assessing risks and mitigating threats. Financial Services nudged out Telecom & Technology for first place in Risk Assessment.

Strengths

1. Assessing network infrastructure components for risks (A)
2. Executive- and board-level understanding of risks (B)
3. Assessing desktop PCs for risks (B)

Weaknesses

1. Assessing cloud infrastructure (IaaS, PaaS) for risks (D+)
2. Assessing cloud applications (SaaS) for risks (C-)
3. Assessing mobile devices for risks (C-)

TELECOM & TECH

RISK ASSESSMENT
77% (#2 of 7)

SECURITY ASSURANCE
85% (#1 of 7)

OVERALL SCORE
81% (Tied #1 of 7)

OVERALL GRADE
B-

Telecommunications & Technology tied Financial Services for first place overall, and it came in ahead of Financial Services, ranking first place in Security Assurance.

Strengths

1. Executive- and board-level understanding of risks (B)
2. Executive- and board-level commitment to IT security (B)
3. Measuring effectiveness of security investments (B)

Weaknesses

1. Assessing cloud applications (SaaS) for risks (D+)
2. Assessing cloud infrastructure (IaaS, PaaS) for risks (C-)
3. Assessing mobile devices for risks (C-)

RETAIL

RISK ASSESSMENT
75% (#3 of 7)

SECURITY ASSURANCE
79% (#4 of 7)

OVERALL SCORE
77% (#3 of 7)

OVERALL GRADE
C+

The Retail industry on the whole gave itself above average marks for both Risk Assessment and Security Assurance, potentially due to increased security investments in recent years following numerous high-profile cyberattacks against retail chains.

Strengths

1. Assessing risks in network infrastructure components (A-)
2. Assessing risks in virtual servers within datacenters (B)
3. Detecting cyber threats emanating from within (C)

Weaknesses

1. Assessing mobile devices for risks (D)
2. Assessing assets at the perimeter / DMZ for risks (D)
3. Assessing cloud infrastructure (IaaS, PaaS) for risks (C-)

MANUFACTURING

RISK ASSESSMENT
72% (Tied #4 of 7)

SECURITY ASSURANCE
80% (#3 of 7)

OVERALL SCORE
76% (#4 of 7)

OVERALL GRADE
C

Despite a rise in international malware attacks targeting SCADA and ICS systems, Manufacturing industry respondents achieved average grades, matching the industry's overall score with that of the Global Cybersecurity Assurance Report Card score.

Strengths

1. Assessing desktop PCs for risks (B)
2. Conveying risks to executives and board members (B)
3. Measuring effectiveness of security investments (B)

Weaknesses

1. Assessing mobile devices for risks (D)
2. Assessing cloud infrastructure (IaaS, PaaS) for risks (D)
3. Assessing cloud applications (SaaS) for risks (D)

HEALTH CARE

RISK ASSESSMENT
72% (Tied #4 of 7)

SECURITY ASSURANCE
75% (#5 of 7)

OVERALL SCORE
73% (#5 of 7)

OVERALL GRADE
C

Health Care industry respondents achieved slightly below average results, landing this industry in fifth place out of seven. It's also the only industry that fared well in assessing assets in the perimeter / DMZ for risks.

Strengths

1. Conveying risks to executives and board members (B)
2. Assessing assets at the perimeter / DMZ for risks (B-)
3. Measuring effectiveness of security investments (B-)

Weaknesses

1. Assessing mobile devices for risks (F)
2. Detecting and assessing transient mobile devices (D-)
3. Assessing cloud infrastructure (IaaS, PaaS) for risks (D)

GOVERNMENT

RISK ASSESSMENT
63% (#7 of 7)

SECURITY ASSURANCE
70% (#6 of 7)

OVERALL SCORE
66% (#6 of 7)

OVERALL GRADE
D

The Office of Personnel Management breach in the United States put government security under intense scrutiny worldwide in 2015. Despite taxpayer funding to secure government systems and better protect citizen data, survey responses reveal that government IT security professionals lack confidence in their ability to assess and mitigate security risks.

Strengths

1. Conveying risks to executives and board members (B)
2. Executive- and board-level understanding of risks (B)
3. Measuring effectiveness of security investments (B-)

Weaknesses

1. Assessing mobile devices for risks (F)
2. Assessing cloud infrastructure (IaaS, PaaS) for risks (F)
3. Assessing cloud applications (SaaS) for risks (F)

tenable network security

EDUCATION

RISK ASSESSMENT
65% (#6 of 7)

SECURITY ASSURANCE
64% (#7 of 7)

OVERALL SCORE
64% (#7of 7)

OVERALL GRADE
D

The industry that assigned itself the worst scores in this inaugural research study is the industry most accustomed to assigning grades to others. Challenges with assessing risks in the cloud and detecting transient mobile devices placed education at the bottom of the class.

Strengths

1. Assessing network infrastructure components for risks (B)
2. Assessing physical servers in the datacenter for risks (C+)
3. Conveying risks to executives and board members (C+)

Weaknesses

1. Assessing cloud infrastructure (IaaS, PaaS) for risks (F)
2. Assessing cloud applications (SaaS) for risks (F)
3. Detecting and assessing transient mobile devices (F)

The Road Ahead

To provide additional insight into the mindset of survey respondents, Tenable asked two additional questions not associated with the Risk Assessment or Security Assurance report cards. The first of the two 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 cyberattacks?" The responses are depicted in Figure 7 below.

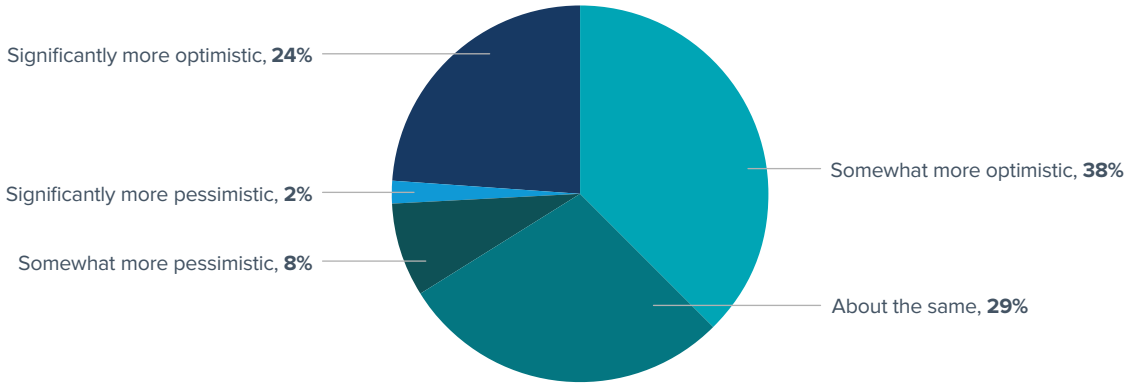


FIGURE 7: *Optimism now versus one year ago for defending against cyberattacks*

Given that 72% of global survey respondents, on average, responded favorably to the 16 Risk Assessment and Security Assurance questions in the survey, these results intuitively make sense. However, they also reiterate a key theme present throughout this report – there is still much work to be done.

The second of the two additional questions explored what might be keeping IT security professionals from being more successful at stopping cyberthreats, reading: "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 8.

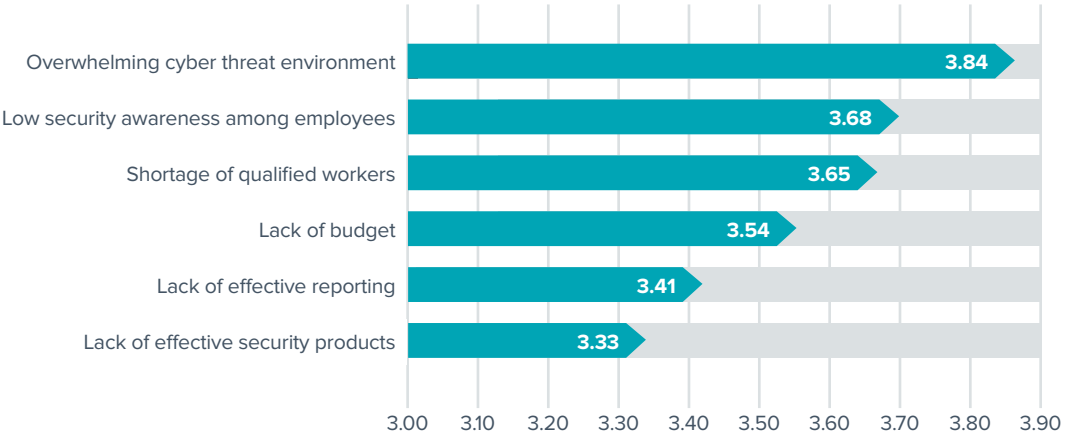


FIGURE 8: *Top challenges facing IT security professionals*

So what can IT security organizations do to improve their abilities to assess and mitigate network security risks? Here are a few suggestions to get started:

1 **Raise the cost for an attacker.** The best deterrence against cyberattacks is to focus on the basics. By adhering to a few fundamental practices, security teams can effectively raise the cost for an attacker to the point that the payoff isn't worth the effort. First, know everything on your network; second, continuously remove vulnerabilities and misconfigurations; third, make use of available technologies to prevent or detect malicious activity (e.g., next-generation firewalls and endpoint protection platforms); fourth, manage admin privileges and ensure users can only access what they need; and fifth, actively hunt for malware and intruders. The fundamentals of cybersecurity haven't changed in decades, but as the high-profile breaches of 2015 show, many organizations still are not taking the time or spending the money to position themselves for success.

2 **Gain board-level buy-in.** The survey data show that practitioners believe their board members aren't giving security the attention it deserves and don't fully understand the cyber risks facing their organizations. Board-level involvement is critical to the long-term success of any enterprise IT security program. CISOs and their security teams must learn to speak the language of business and construct reports that bridge the technical knowledge gap so they can clearly communicate the overall security status of their organization. Without buy-in at the highest levels of an organization, progress will be hard to achieve.

3 **Deploy passive scanning to close security gaps.** Today's corporate networks are constantly evolving. New hosts frequently come and go, fueled by the proliferation of mobile devices and virtualization. Organizations that rely on periodic vulnerability assessments alone have an accurate depiction of their network security risks about once per month. By employing passive scanning solutions as part of a continuous network monitoring solution, IT security teams gain full visibility into security risks during the other 353 days of the year.

4 **Embrace the cloud.** Transitioning applications and IT infrastructure to the cloud yields compelling business advantages. But it also introduces new risks and uncertainties. Out of sight should never mean out of mind. Don't assume your cloud service provider has implemented adequate security protections. The onus of securing your cloud based assets falls on your shoulders – not theirs. Be sure to embrace a unified risk management platform that continuously monitors for security risks with IT components located on-premises and in the cloud.

5 **Detect threats from within.** Today's cybercriminals are well funded, highly motivated, and more sophisticated than ever. Advanced threat actors constantly develop new ways to circumvent perimeter defenses. And with the use of laptops and mobile devices on a seemingly permanent upward trend, employees often hand carry threats into the office after surfing the web over the weekend. For these reasons, organizations can't afford to rely exclusively on perimeter security devices and traditional endpoint defenses. Smart CISOs are investing in technologies that continuously search for threats from the inside.

Appendix 1: Survey Demographics

Countries

Of the 504 respondents, 60% were based in North America (U.S. & Canada), 25% in Europe (U.K. & Germany), and 15% in Asia Pacific (Australia & Singapore). Figure 9 depicts the breakdown of respondents by country.

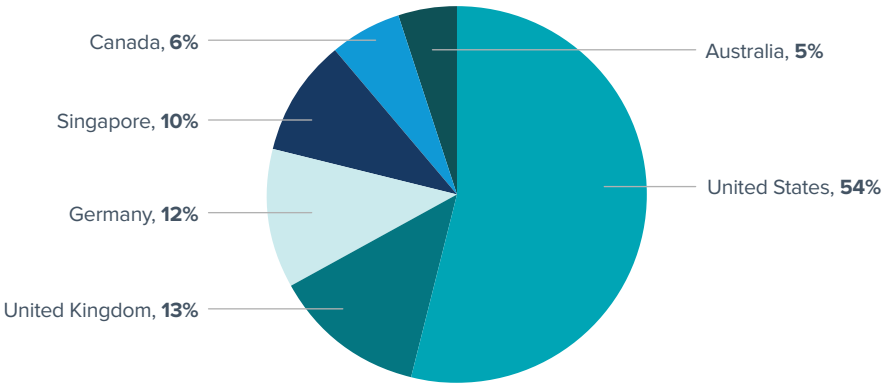


FIGURE 9: *Respondents by country*

IT Security Roles

Of the 504 respondents, two-thirds (combined 67%) held manager, director, or executive leadership roles. Figure 10 depicts the breakdown of respondents by IT security role.

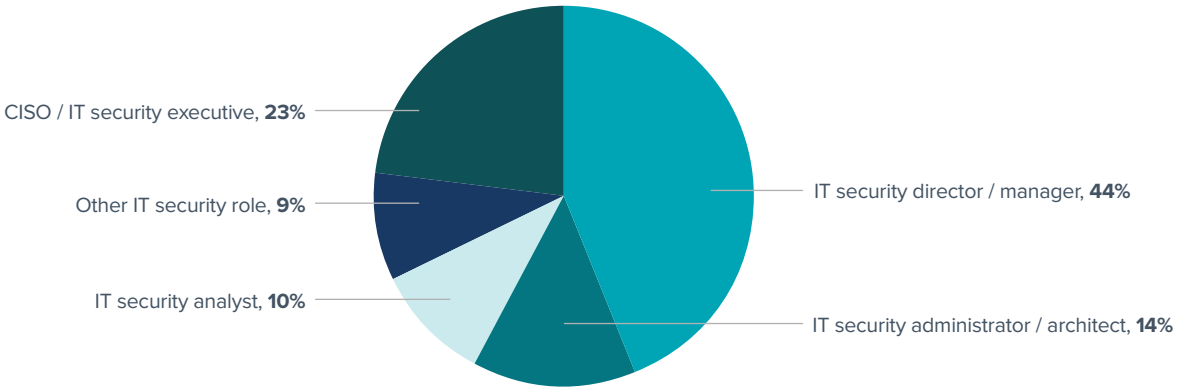


FIGURE 10: *Respondents by IT security role*

Organization Size

Of the 504 respondents, more than one-third (combined 38%) were employed by organizations with 10,000 or more employees worldwide. Figure 11 depicts the breakdown of respondents by organization size (i.e., worldwide employee count).

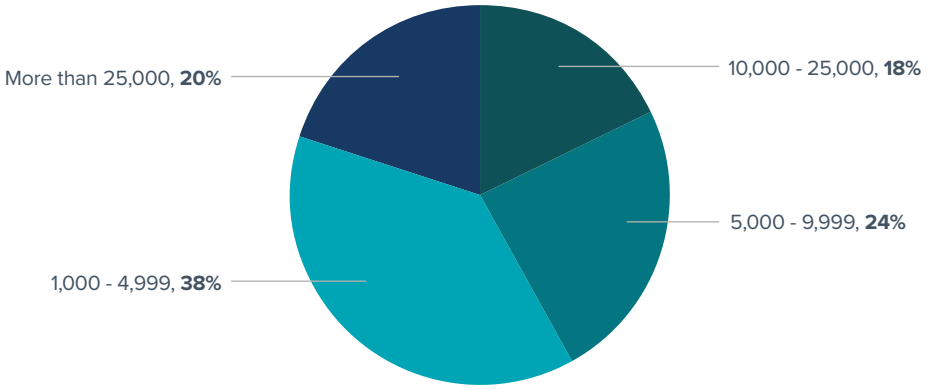


FIGURE 11: *Respondents by organization worldwide employee count*

Industries

Although responses from 19 industries were collected, the top seven industries account for 73% of the responses. Figure 12 depicts the breakdown of responses by industry (see question 3 in Appendix 3 for a list of full industry descriptions).

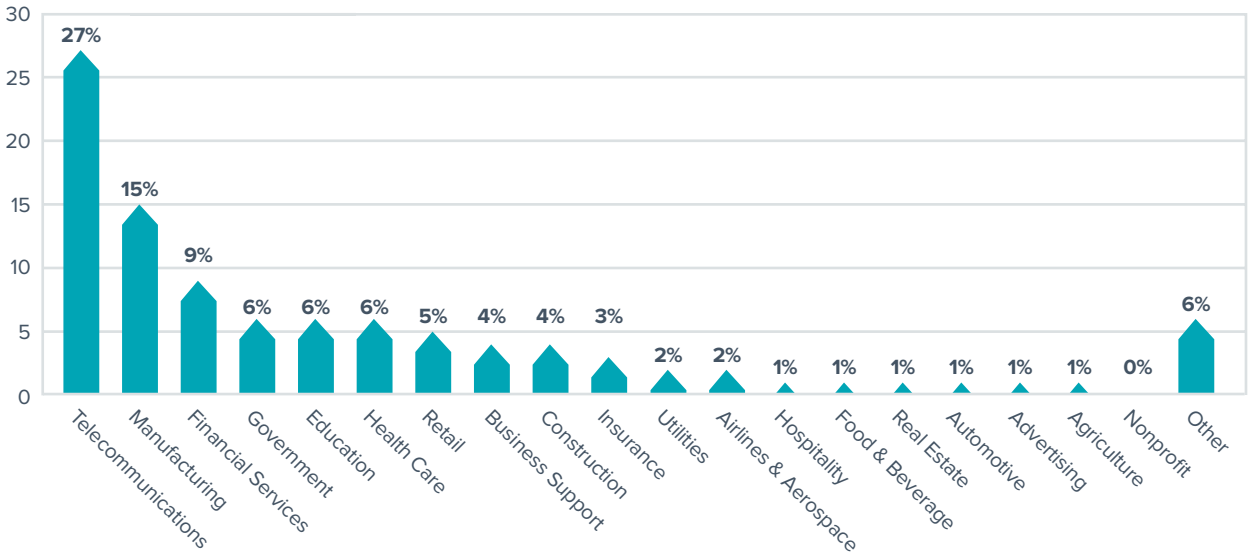


FIGURE 12: *Respondents by industry*

Appendix 2: Research Methodology

CyberEdge Group developed a 10-question web-based survey instrument in partnership with Tenable Network Security. The survey was promoted to information security professionals across six countries and three geographic regions—United States and Canada (North America), United Kingdom and Germany (Europe), and Australia and Singapore (Asia Pacific). The survey was translated into German for those respondents targeted in Germany. All other respondents completed the survey in English.

The online survey was conducted in August 2015. 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 six 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: 504 (100%)
- United States: 272 (54%)
- United Kingdom: 67 (13%)
- Germany: 61 (12%)
- Singapore: 50 (10%)
- Canada: 29 (6%)
- Australia: 25 (5%)

The following are sample sizes by industry in decreasing order:

- Telecom, Technology, Internet, and Electronics: 137 (27%)
- Manufacturing: 75 (15%)
- Finance & Financial Services: 43 (9%)
- Government: 30 (6%)
- Education: 30 (6%)
- Health Care & Pharmaceuticals: 28 (6%)
- Retail & Consumer Durables: 25(5%)

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 ten IT components depicted in question 5 (see Appendix 3). Security Assurance Scores are associated with questions 4, 5, 7, 8, 9, and 10.

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%

GRADE	RANGE
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.

tenable network security

Appendix 3: Online Survey Questions

The following questions were asked of 504 security professionals employed by organizations with 1,000+ employees worldwide:

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)

4 ***Compared to this time last year***, do you feel ***more optimistic or pessimistic*** about your ***organization's ability to defend itself*** against cyberattacks?
- **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 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

6 Describe your agreement with the following statement: "My organization has the tools necessary to ***detect transient mobile devices*** (smartphones and tablets) and ***accurately assess their security risks***."
- **a** Strongly agree
- **b** Somewhat agree
- **c** Neither agree nor disagree
- **d** Somewhat disagree
- **e** Strongly disagree
- **f** Don't know

7 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 applications (SaaS)
- **b** Cloud infrastructure (IaaS, PaaS)
- **c** Datacenter / physical servers
- **d** Datacenter / virtual servers
- **e** Desktops (PCs)
- **f** Laptops / notebooks
- **g** Mobile devices (smartphones, tablets)
- **h** Network perimeter / DMZ (web servers)
- **i** Web applications (custom built)
- **j** Network infrastructure components (routers, firewalls)

tenable network security

8 Describe your agreement with the following statement: "My company's ***executive team and board of directors*** fully understand the ***cyber security risks*** our company is facing."

- **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 ***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

10 Describe your agreement with the following statement: "My organization has the ***tools necessary*** to ***detect cyber threats emanating from inside our corporate network***."

- **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 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

12 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** Shortage of qualified workers
- **e** Overwhelming cyber threat environment
- **f** Low security awareness among employees
- **g** Inability to monitor the effectiveness of security investments
- **h** 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 **www.cyber-edge.com**.