2016 全球网络安全保障报告

2016 全球网络安全保障报告

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	2016 Global Cybersecurity Assurance Report Card		
原文作者	CyberEdge	**原文发布日期**	2016 年 2 月
作者简介	CyberEdge 集团对安全供应商和服务供应商提供信息服务。该集团成立于 2012 年，总部设在马里兰州安纳波利斯，CyberEdge 由于其久经考验的研究方法和和无与伦比的客观性和综合性迅速成为了自定义安全研究的主要供应商。		
原文发布单位	CyberEdge		
原文出处	http://whitepapers.theregister.co.uk/paper/view/4435/2016-global-cybersecurity-assurance-report-card.pdf		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

tenable network security

简介

在过去的一年里，我们看到了攻击者针对世界各地各行各业的企业发动了破坏性的网络攻击。随着攻击者对世界各地的防御系统展开随心所欲地攻击，企业的防御能力受到了质疑。公民的私有数据，数十亿美元的国际业务收入和国家的安全都处于危险之中。鉴于这些潜在的危险，企业要知道他们的安全计划的哪些部分是有效的，哪些部分有短板。

本研究的目的是衡量企业 IT 安全专业人士如何看待企业评估网络安全风险，并缓解可以利用这些风险的威胁的能力。根据研究结果，Tenable 发布了该行业的第一份全球网络安全保障报告。

为了了解世界各地的企业是如何评估和缓解网络风险的，2015 年 8 月，Tenable 对 504 位就职于员工人数超过 1,000 人的企业的 IT 安全专业人员进行了调查。调查问卷包含 12 个基于 web 的问题（见附录 3）。调查问卷要求被调查者对每个问题进行 5 分制评分。通过将两个分值最高的得分相加，然后求相关问题的平均值，得到两个指数，具体如下：

73%

风险评估指数

代表企业评估 IT 基础设施的 10 大关键组件网络安全风险的能力

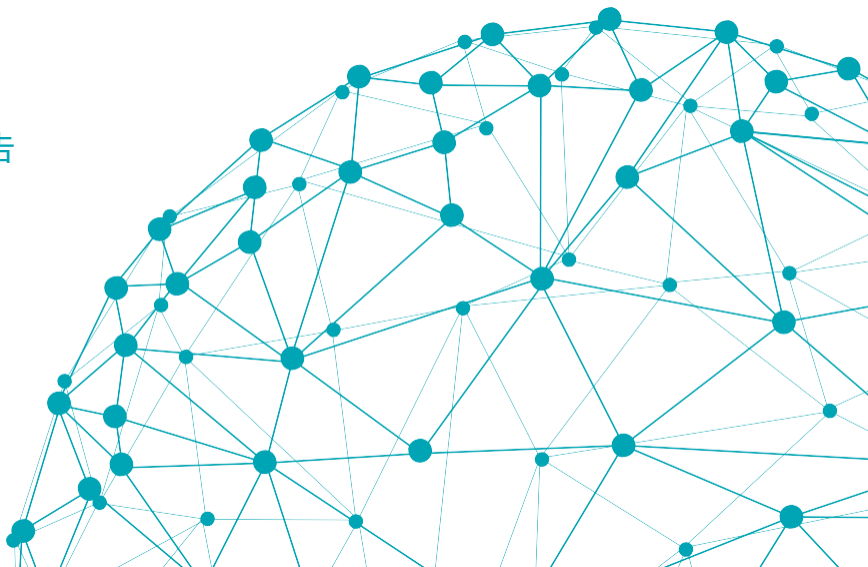
79%

风险评估指数

代表企业通过检测安全基础设施，缓解威胁的能力

76%

全球网络安全保险报告



tenable network security

执行摘要

“C.” 在美国，拿到“C”常常意味着不及格，而这正是 2016 年全球网络安全保障报告的调查数据结果，根据对这 504 位安全从业人员的调查结果（73%的风险评价指标和 79%的安全保障指数）。这两个数字平均一下为 76% ，换算之后为“C”。

本报告对 IT 安全专业人士如何评估和缓解网络安全风险进行了阐述。这些内容分为三个部分：全球洞察，地理见解和行业洞察。以下为这三部分的主要内容：

1 **人无完人。** 按照国家和行业来评估，部分国家和行业的得分为“B-”，而大部分的得分为“C”和“D”。这意味着，超过 20%的企业对响应和缓解网络风险没有信息。

2 **陷入云中。** 受访者一致认为云应用程序（D+）和云基础设施（D）是评估网络安全风险中三项最具挑战性的 IT 组件中的两项。根据调查结果，评估安全风险时最具挑战性的 IT 组件是云基础设施（IaaS，PaaS）。

3 **移动设备带来了困扰。** 根据调查结果，移动设备（D）也为评估风险带来了挑战。在第一时间检测到临时的移动设备是安全人员面临的另一个巨大的挑战（C）。

4 **未被调查的董事会成员。** 好的一面是，受访者大多认为他们已经得到了合适工具，以衡量整体安全有效性（B-），并向安全风险管理人员和董事会成员报告了安全风险（B）。然而，受访者也对高管和董事会成员是否完全了解这些安全风险（C+），并就缓解风险进行足够的投资提出了质疑（C）。

5 **美国州国家的得分最高。** 虽然加拿大的安全保险评分比美国高，但是，这样不足以超越美国的风险评估得分。

6 **澳大利亚的困扰。** 虽然澳大利亚的风险评估分数与德国和新加坡的不相上下，但其安全保障得分是所有国家中最低的。

7 **金融，电信/技术行业的得分高居榜首。** 金融服务业，电信/科技产业的网络安全保障报告最高分。金融服务业在风险评估中得分最高分，而电信与技术在安全保障方面得分最高。

8 **教育行业要提高威胁意识。** 被调查的七大代表性行业中，教育行业的整体得分最低，其安全保险指数最低，风险评估指数倒数第二。

在本报告的其余部分提供了风险评估指标和安全保障指数结果和分析的详细内容，以及对企业提出的建议，以帮助企业最小化网络安全风险。

风险评估报告

如在基于 web 的调查（见附录 3）中的问题 6，以及图 1 和图 2 所示，风险评估指标指代一个企业针对 10 项关键基础设施组件评估网络安全风险的能力。图 1 为各国风险评估指数得分。图 2 是按照行业进行评估各行业的得分。

	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+**

图 1 各国风险评估指数得分

	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**

图 2: *各行业风险评估指数得分*

安全保险报告

该安全保险指数代表各行业缓解风险的能力（见附录 3 中的问题 5,6,8,9,10,11）

	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+**

图 3: *安全保险报告（各国）*

	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**

图 4: *安全保险报告（各行业）*

最终得分

风险评估和安全保障（与相同比重）分数总和的平均值就是各国和各行业在网络安全保险报告中的得分和级别（见图 5,6）。图 5 中的第一列为所有六个国家和所有行业的总得分。

	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+

图 5: 网络安全保险报告（各国）

	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

图 6: 网络安全保险报告（各行业）

各国解析

以下就按照国家对风险评估和安全保险进行解析：

UNITED STATES

RISK ASSESSMENT
77% (#1 of 6)

SECURITY ASSURANCE
83% (#2 of 6)

AVERAGE SCORE
80% (#1 of 6)

AVERAGE GRADE
B-

虽然得分为 B-，但也没什么可炫耀的，来自美国的受访者明显对其企业评估风险的能力最有信心。

优势

1. 向董事会成员和高管报告风险(B)
2. 行政人员和董事会了解风险(B)
3. 衡量 安全投资的有效性(B)

弱点

1. 就风险性对移动设备进行评估 (D)
2. 就风险性对云基础设施(IaaS, PaaS)进行评估 (D+)
3. 就风险性对云应用程序(SaaS)进行评估 (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)*

加拿大的受访者对其企业缓解风险的能力表现出了最大的信心，然而，加拿大的受访者对评估网络安全风险的信心为第三名。

优势

1. 检测企业内部存在的网络威胁(A-)
2. 向董事会成员和高管报告风险(B+)
3. 探测和评估临时的移动设备(B)

弱点

1. 就风险性对云基础设施(IaaS, PaaS)进行评估(F)
2. 就风险性对云应用程序(SaaS)进行评估(D+)
3. 就风险进行 DMZ 评估 (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)*

就风险评估和安全保险两项而言，英国的受访者的得分都处于中等水平。

优势

1. 就风险对台式机进行评估 (B)
2. 就风险进行 DMZ 评估(B-)
3. 向董事会成员和高管报告风险(B-)

弱点

1. 就风险性对移动设备进行评估(F)
2. 探测和评估临时的移动设备(D)
3. 就风险性对云基础设施(IaaS, PaaS)进行评估(D)

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)*

根据对来自新加坡的受访者进行调查，他们对每项内容都不是很有信心，没有超过 C+的得分。然而，他们的也没有拿到低于 D 的得分，使得新加坡位于受访国家中的第四名。

优势

1. 用数据中心的物理服务器评估风险(C+)
2. 用数据中心的虚拟服务器评估风险(C+)
3. 衡量安全投资的有效性 (C+)

弱点

1. 就风险性对云基础设施(IaaS, PaaS)进行评估(D)
2. 就风险性对云应用程序(SaaS)进行评估(D)
3. 就风险性对云应用程序(SaaS)进行评估(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)*

德国的受访者给出的答复差异较大。得分从 B 至 F 都有。

优势

1. 用数据中心的虚拟服务器评估风险(B)
2. 用数据中心的物理服务器评估风险(B-)
3. 向董事会成员和高管报告风险(B-)

弱点

1. 就风险性对移动设备进行评估(F)
2. 就风险性对客户网站应用程序进行评估(F)
3. 就风险进行 DMZ 评估(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)*

澳大利亚的受访者在调查期间的信心受到了打击，澳大利亚受访者对风险评估和安全保险的信心都为最低。

优势

1. 就安全风险对笔记本和电脑进行评估 (B+)
2. 就安全风险对台式机进行评估(B-)
3. 检测来自内部的网络威胁 (C)

弱点

1. 就风险性对云基础设施(IaaS, PaaS)进行评估(F)
2. 就风险性对客户网站应用程序进行评估(D-)
3. 检测和评估临时的移动设备(D-)

行业洞察

以下内容为就行业对风险评估和安全保险进行分析:

FINANCIAL SERVICES

RISK ASSESSMENT
79% (#1 of 7)

SECURITY ASSURANCE
84% (#2 of 7)

OVERALL SCORE
81% (Tied #1 of 7)

OVERALL GRADE
B-

金融服务业胜过电信业，排到了第一名。

优势

1. 鉴于风险评估网络基础设施组件 (A)
2. 管理人员和董事会成员了解风险 (B)
3. 就安全风险对台式机进行评估(B)

弱点

1. 就风险性对云基础设施(IaaS, PaaS)进行评估(D+)
2. 就风险性对云应用程序(SaaS)进行评估(C-)
3. 就风险性对移动设备进行评估(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-

虽然电信业的整体排名为第二位，但就安全保险得分来看，电信业的排名高于金融服务业。

优势

1. 管理人员和董事会成员了解风险(B)
2. 管理人员和董事会成员对 IT 安全负责 (B)
3. 对安全投资的有效性进行评估 (B)

弱点

1. 就风险性对云应用程序(SaaS)进行评估(D+)
2. 就风险性对云基础设施(IaaS, PaaS)进行评估(C-)
3. 就风险性对移动设备进行评估(C-)

RETAIL

RISK ASSESSMENT
75% (#3 of 7)

SECURITY ASSURANCE
79% (#4 of 7)

OVERALL SCORE
77% (#3 of 7)

OVERALL GRADE
C+

整体上，零售行业的风险评估和安全保险的得分都高于平均分，这可能是由于近几年该行业在经历了若干高调的网络攻击之后对安全投资有所增加的原因。

优势

1. 鉴于风险评估网络基础设施组件 (A-)
2. 对数据中心的虚拟服务器进行评估 (B)
3. 检测来自内部的网络威胁 (C)

弱点

1. 就风险性对移动设备进行评估(D)
2. 就风险进行 DMZ 评估(D)
3. 就风险性对云基础设施(IaaS, PaaS)进行评估(C-)

MANUFACTURING

RISK ASSESSMENT
72% (Tied #4 of 7)

SECURITY ASSURANCE
80% (#3 of 7)

OVERALL SCORE
76% (#4 of 7)

OVERALL GRADE
C

尽管针对 SCADA（数据采集与监控系统）和 ICS（互联网连接共享）的国际性恶意软件攻击有所增加，但是，制造业的受访者取得了的成绩达到了平均值。

优势

1. 就风险对台式机进行评估 (B)
2. 向管理人员和董事会成员报告风险 (B)
3. 对安全投资的有效性进行评估(B)

弱点

1. 就风险性对移动设备进行评估(D)
2. 就风险性对云基础设施(IaaS, PaaS)进行评估(D)
3. 就风险性对云应用程序(SaaS)进行评估(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

医疗保健行业的受访者的成绩略低于平均成绩。它也是唯一一个在 DMZ 风险评估这一项取得不错成绩的行业。

优势

1. 向管理人员和董事会成员报告风险 (B)
2. 就风险进行 DMZ 评估(B-)
3. 对安全投资的有效性进行评估(B-)

弱点

1. 就风险性对移动设备进行评估(F)
2. 检测和评估临时移动设备(D-)
3. 就风险性对云基础设施(IaaS, PaaS)进行评估(D)

GOVERNMENT

RISK ASSESSMENT
63% (#7 of 7)

SECURITY ASSURANCE
70% (#6 of 7)

OVERALL SCORE
66% (#6 of 7)

OVERALL GRADE
D

对美国人事管理局办公室的攻击使得政府安全受到了关注。尽管纳税人提供资金以确保政府系统和更好地保护公民的数据，但是，调查反馈表明，政府的 IT 安全专业人员对其评估和缓解安全风险的能力缺乏信心。

优势

1. 向管理人员和董事会成员报告风险(B)
2. 管理人员和董事会成员了解风险(B)
3. 对安全投资的有效性进行评估(B-)

弱点

1. 就风险性对移动设备进行评估(F)
2. 就风险性对云基础设施(IaaS, PaaS)进行评估(F)
3. 就风险性对云应用程序(SaaS)进行评估(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

本次调查中为自己所处行业评分最低的行业是教育行业。在评估云的风险和检测临时移动设备中面临的挑战是其垫底的主要原因。

优势

1. 就风险对网络基础设施组件进行评估(B)
2. 就风险对数据中心的物理服务器进行评估 (C+)
3. 向管理人员和董事会成员报告风险(C+)

弱点

1. 就风险性对云基础设施(IaaS, PaaS)进行评估(F)
2. 就风险性对云应用程序(SaaS)进行评估(F)
3. 检测和评估临时设备 (F)

预见未来

为了对受访者的心态进行进一步洞察，Tenable 询问了受访者两个与该报告无关的问题。第一个问题是：“与去年的这时候相比，你认为你所在企业防御网络攻击的能力是提升了还是你仍持悲观的态度？”受访者的答复如图 7 所示。

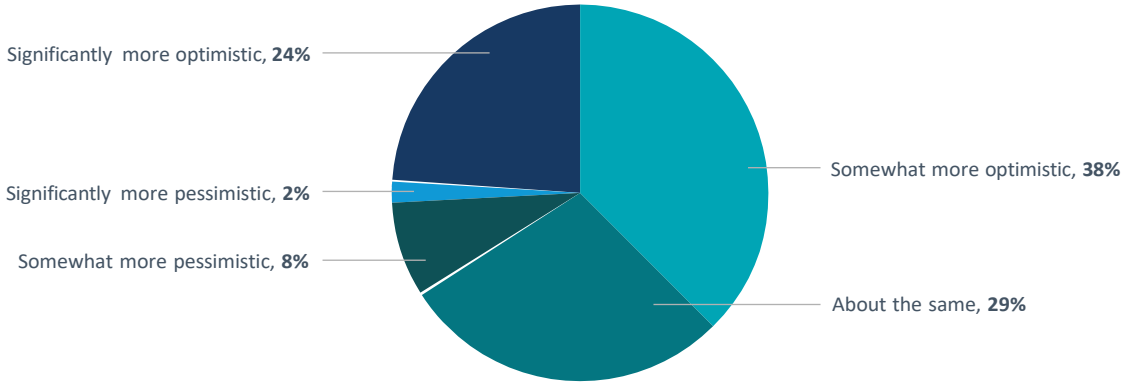


图 7: *与一年前相比对企业防御能力的态度。*

鉴于全球 72%d 的受访者都顺利地完成了所有调查问题，因此，这些结果足以说明问题。

这两个额外问题的第二个问题就哪些因素可能阻止了 IT 安全专业人士提高抵御网络威胁的成功率的提升进行了探讨，问题是：“分数为 1 分至 5 分，以 5 分为最高，为当今的 IT 专业人员面临的挑战进行打分。”得分结果如图 8 所示。

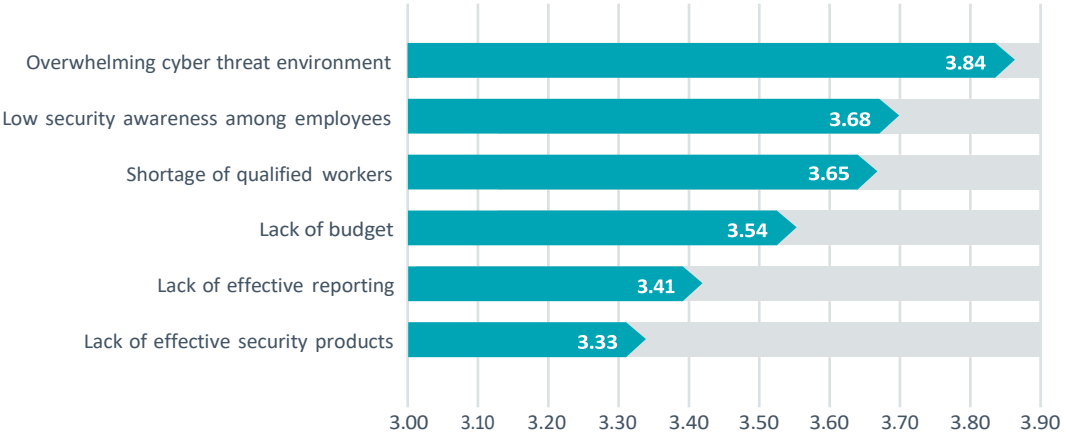


图 8: *IT 专业人员面临的主要挑战*

那么，IT 安全企业应怎么提高其评估和缓解网络安全风险的能力呢？以下为几条建议：

1 **提升攻击者发动攻击的成本。** 针对网络攻击的最好的威慑是把重点放在基本问题上。通过坚持一些基本做法，安全团队能有效提高攻击者发动攻击的成本。首先，了解企业网络的一切;第二，不断删除漏洞和错误配置;第三，利用现有的技术，以防止或侦测恶意行为（例如，下一代防火墙和终端保护平台）;第四，对管理权限进行管理，确保用户只能访问他们所需要的东西;第五，积极搜寻恶意软件和入侵者。网络安全的基本原理几十年来都没有改变，但正如 2015 年几起高调的攻击所展示，许多企业仍然没有抽出时间或者投资安全防御的提升。

2 **获取董事会级的参与。**本次调查数据显示，受访者认为其所在企业的董事会成员并没有对安全给予足够的重视，并且也不完全了解企业所面临的网络风险。董事会的参与对企业 IT 安全项目的成功至关重要。首席信息安全官及其安全团队必须学会讲业务语言，以清楚地同董事会就整体安全态势进行交流。如果没有企业最高级别人员的参与，企业很难进步。

3 **部署被动扫描以缩小安全差距。**当今的企业网络在不断演变。主机频繁更替，移动设备和虚拟化技术的扩散一直推动者变革。依赖于定期漏洞评估的企业对其网络安全风险有准备的认识。通过采用被动扫描解决方案作为一个连续的网络监控解决方案的一部分，IT 安全团队可以获得对一年之中其他 353 天安全的完全可视化。

4 **拥抱云。**将应用程序和 IT 基础架构转向云可以加强业务优势。但它也引发了新的风险和不确定性。眼不见不意味着心不烦。不要妄想你的云服务供应商已实施了足够的安全保护。保护基于云的资产是您的责任-不是他们的。

5 **检测内部威胁。** 当今的网络犯罪分子资金雄厚，干劲十足，而且比以往任何时候都更加复杂。高级威胁攻击者不断开发新的方法来规避外围防御。随着笔记本电脑和移动设备在工作中的使用越来越多，企业员通常会在周末用电脑进行娱乐之后将威胁带入企业。由于这些原因，企业不能完全依赖边界安全设备和传统的终端防御。精明的首席信息安全官会投资可以检测内部威胁的技术。

附录 1: 调查对象

国家

504 位受访者中，有 60%来自北美（美国&加拿大），25%来自欧洲（英国&德国），15%来自亚洲太平洋地区（澳大利亚&新加坡）。图 9 显示了来自各地区受访者所占比重。

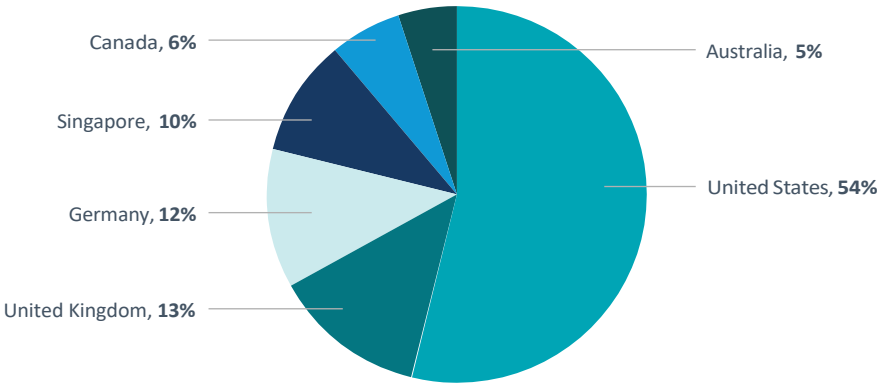


图 9: *受访者的国家分布*

IT 安全角色

504 位受访者中有三分之二的受访者在企业担任经理，主管或高管一职。图 10 显示了各职位受访者比重。

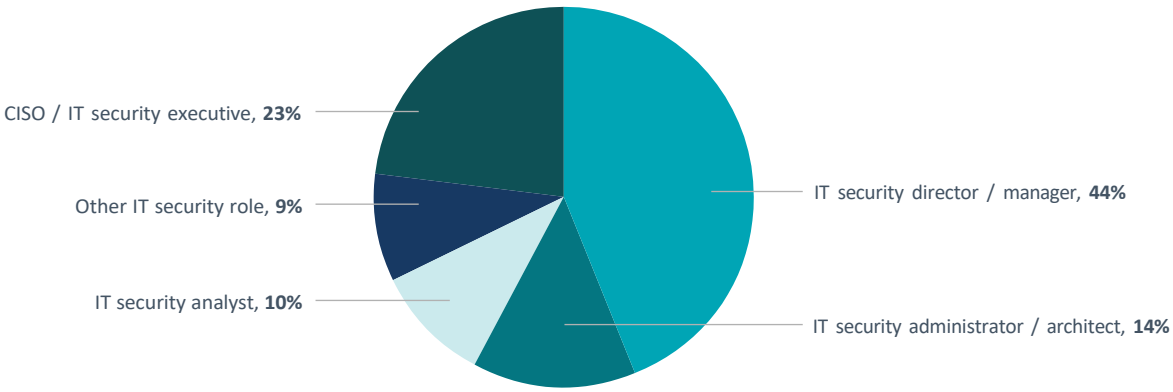


图 10: *受访者的职位*

企业规模

504 位受访者中超过三分之一（38%）来自员工人员超过 10,000 人的企业。图 11 显示了受访者所在企业的规模比。

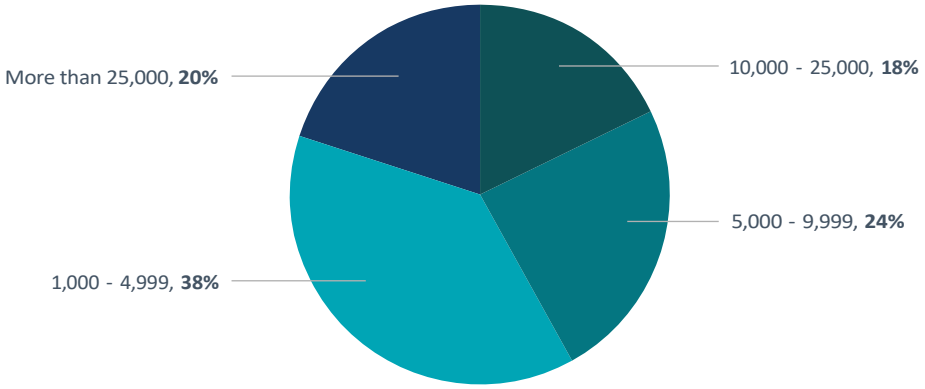


图 11: *受访企业规模比*

行业

虽然受访者来自 19 种行业，来自前 7 大行业的受访者占 73%。图 12 显示了受访者所属行业比。

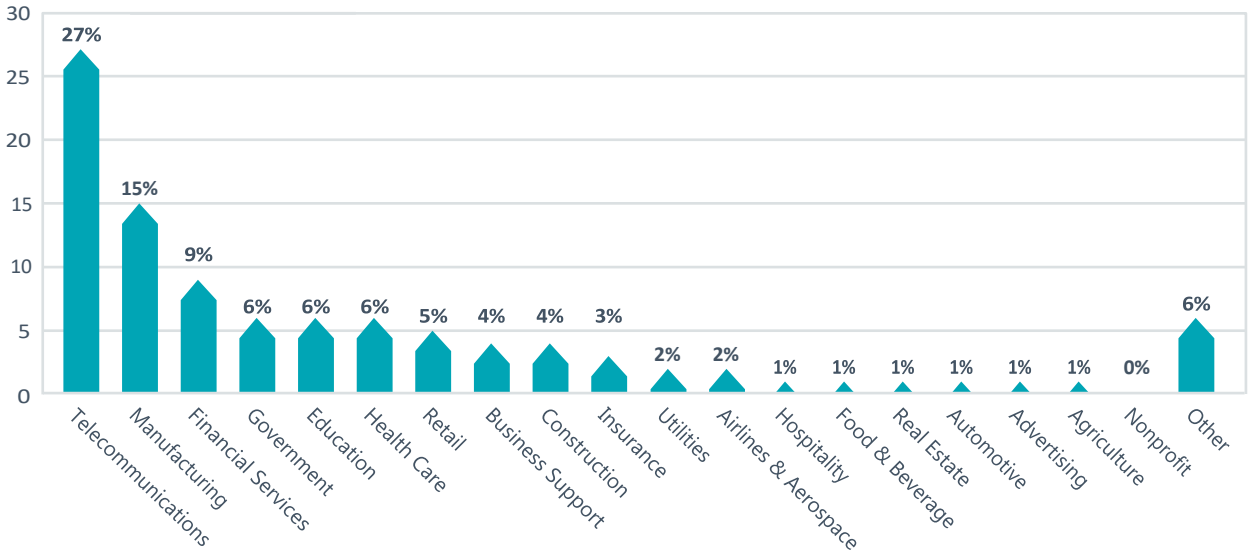


图 12: *受访者所属行业比*

附录 2: 研究方法

CyberEdge 集团与 Tenable 一道设计了包含 10 个问题的基于 web 的调查工具。这项调查针对六个国家的信息安全专业人员展开。针对德国的调查被翻译成了德文。其他国家的受访者用英语完成了调查。

在线调查于 2015 年 8 月进行。每个受访者都要回答两个统计问题：（1）受雇于全球员工总数超过 1,000 人的企业和（2）从事 IT 安全。未能满足这些条件之一的受访者会从调查中筛除。

样本规格

受访者来自 19 个行业，六个国家。来自每个国家和每个行业的受访者至少有 25 人。行业受访人数少于 25 人的会做个整体报告。

以下为各国受访者占比的递减排序：

全球: 504 (100%)
美国: 272 (54%)
英国: 67 (13%)
德国: 61 (12%)
新加坡: 50 (10%)
加拿大: 29 (6%)
澳大利亚: 25 (5%)

以下为各行受访者占比的递减排序：

电信，科技，互联网和电子: 137 (27%)
制造业: 75 (15%)
金融及金融服务: 43 (9%)
政府部门: 30 (6%)
教育: 30 (6%)
医疗保健&制药业: 28 (6%)
零售业&消费品业: 25(5%)

分析

通过将相关联的两个得分最高的问题的总体比重相加得到最后分数。风险评估成绩与问题 5 中所示的 10 个 IT 组件相关（见附件 3）。安全保证得分与问题 4，5，7，8，9，和 10 有关。

典型的美国成绩按照以下比例被分配到各指数得分：

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%

质量控制

每个（非人口统计）调查问题都包括“不知道”选项，尽量减少受访者在回答他们各自的专长或责任区以外的问题时有困难。本报告中的所有调查结果都是在筛除了“不知道”的回答后所得，从而减少每个问题的答复的样本规模。

我们对所有合格的调查回复都进行了检查，以确保调查回复的有效性。无效回复结果将不予采用。

附录 3: 在线调查问题

以下即要求 504 位受访者在线回答的问题：

1 请选择您在企业中的职位。
- a CISO / IT 安全高管
- b IT 安全主管 / 经理
- c IT 安全管理员
- d IT 安全分析师
- e 其他 IT 人员
- f 我的工作不涉及 IT 安全

2 贵司的员工数是多少?
- a 超过 25,000
- b 10,000-25,000
- c 5,000-9,999
- d 1,000-4,999
- e 不到 1,000

3 贵司所属行业为哪类?
- a 广告与营销
- b 农业
- c 航空&航天
- d 汽车行业
- e 业务支持和物流
- f 建筑，机械
- g 教育
- h 金融及金融服务
- i 食品和饮料
- j 政府
- k 医疗保健&制药业
- l 酒店，娱乐，休闲
- m 保险业
- n 制造业
- o 非营利机构
- p 零售&消费品
- q 房地产
- r 通讯，科技，互联网和电子
- s 公用事业，能源
- t 其他（请注明）

4 与去年的此时相比，您对企业防御网络攻击的能力持更加积极的或是消极的态度？
- a 明显更加积极
- b 更加积极
- c 没变化
- d 更加消极
- e 明显更加消极
- f 不知道

5 您是否同意以下说法：“我所在企业可以准确评估安全投资的整体有效性。”
- a 非常同意
- b 同意
- c 不同意也不反对
- d 不同意
- e 强烈反对
- f 不知道

6 您是否同意以下说法：“我所在企业有检测临时设备的工具，并可以准确评估其安全风险。”
- a 非常同意
- b 同意
- c 不同意也不反对
- d 不同意
- e 强烈反对
- f 不知道

7 请为您所在企业评估与以下 IT 组件有关的风险的能力打分，分值为 1-5 分，5 分最高：
- a 云应用程序(SaaS)
- b 云基础设施(IaaS, PaaS)
- c 数据中心/物理服务器
- d 数据中心/虚拟服务器
- e 台式机(PCs)
- f 笔记本电脑
- g 移动设备
- h 网络边界/ DMZ
- i Web 应用程序
- j 网络基础设施组件

8 您是否同意以下说法：“我所在企业的管理团队和董事会完全了解我司所面临的网络安全威胁。”

- a 非常同意
- b 同意
- c 不同意也不反对
- d 不同意
- e 强烈反对
- f 不知道

9 您是否同意以下说法：“我所在企业有可以准确地向管理团队和董事会传送信息的工具。”

- a 非常同意
- b 同意
- c 不同意也不反对
- d 不同意
- e 强烈反对
- f 不知道

10 您是否同意以下说法：“我所在企业有可以准确地检测来自内部网络的威胁的工具。”

- a 非常同意
- b 同意
- c 不同意也不反对
- d 不同意
- e 强烈反对
- f 不知道

11 您是否同意以下说法：“我所在企业的管理团队和董事会对 IT 安全给予了应有的重视。”

- a 非常同意
- b 同意
- c 不同意也不反对
- d 不同意
- e 强烈反对
- f 不知道

12 为以下当今 IT 专业人员面临的挑战打分，分值为 1-5 分，5 分最高：

- a 缺乏预算
- b 缺乏有效的报告
- c 缺乏有效的安全产品
- d 合格的工人的短缺
- e 网络威胁环境的压制
- f 员工的安全意识低
- g 无法监控安全投资的有效性
- h 不知道