REPORT

The State of Enterprise Security Resilience

Executive Summary

Ixia, an international leader in application performance and security resilience technology, conducted a survey to better understand how network security resilience solutions and techniques are used within the modern enterprise. While information exists on security products and threats, very little is available on how it is actually being used and the techniques and technology to ensure that security is completely integrated into the corporate network structure. This report presents the research we uncovered.

During this survey, there were three areas of emphasis exploring security and visibility architectures. One portion of the survey focused on understanding the product types and use. The second area of emphasis was on understanding the processes in use. The final area of emphasis was on understanding the people components of typical architectures.

This report features several key findings that include the following:

- Many enterprises and carriers are still highly vulnerable to the effects of a security breach. This is due to concerns with lack of following best practices, process issues, lack of awareness, and lack of proper technology.
- Lack of knowledge, not cost, is the primary barrier to security improvements. However, typical annual spend on network security is less than $100K worldwide.

KEYSIGHT TECHNOLOGIES

- Security resilience approaches are growing in worldwide adoption. A primary contributor is the merge of visibility and security architectures. Additional data shows that life-cycle security methodologies and security resilience testing are also positive contributors.
- The top two main security concerns for IT are data loss and malware attacks.

These four key findings confirm that while there are still clear dangers to network security in the enterprise, there is some hope for improvement. The severity of the risk has not gone away, but it appears that some are managing it with the right combination of investment in technology, training, and processes.

Survey Conclusions

Ixia conducted a survey to better understand the state of security resilience within the enterprise. While traditional surveys have focused on threat vectors, breach losses, and defensive postures, the primary purpose for this survey was to discover the pervasiveness of security resilience solutions in the enterprise market space.

This survey uncovered the following key findings, which we will discuss in more detail in the following pages:

- Many enterprises and carriers are still highly vulnerable to the effects of a security breach
- Lack of knowledge, not cost, is the primary barrier to security improvements
- Security resilience approaches are growing in worldwide adoption
- The top two main security concerns for IT are data loss and malware attacks

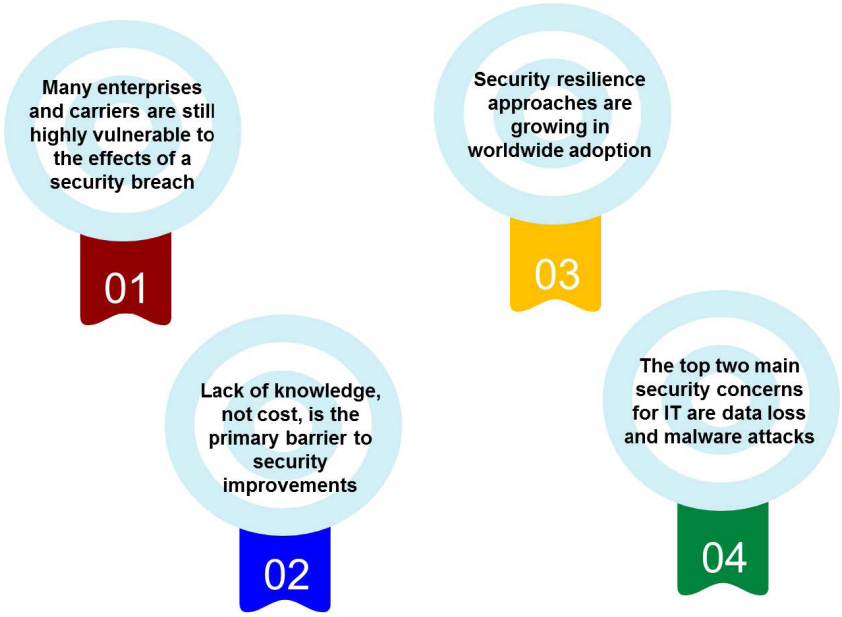


Figure 1: Survey Conclusions

1. Many enterprises and carriers are still highly vulnerable to the effects of a security breach

To come to the conclusion that many enterprises are still highly vulnerable to the effects of a security breach, the responses to the following questions (listed in the Detailed Survey Responses section) were analyzed: Question 1, Question 2, Question 3, Question 8, Question 9, Question 13, Question 15, and Question 18.

In regards to Question 1 "Does your company have a visibility (monitoring) architecture integrated with your security architecture to recognize and record any security attacks?", while 59% of respondents have started to integrate their security and visibility architectures, approximately 26% of respondents have not. Without proper visibility into the network, there is no good way to really understand if a network has been breached, much less how and where. This alone makes at least 1/4 of enterprises moderately vulnerable.

Question 2 asked "How often does your company actively test your architecture and upgrades for security issues BEFORE you deploy them into the live network?" While 20% of companies are following best practices and test their architectures and upgrades all the time, about 1/3 of the respondents perform little to no testing. When combined with Question 1, this survey result ensures that there is high vulnerability for the companies that are not trying to routinely validate their architectures, especially when they have not implemented a proper visibility architecture to see problems.

In response to Question 3 "Does your company currently deploy any of the following in-line security/monitoring solutions?", only about 20% of companies have deployed in-line tools and packet brokers. This means that most companies will need to be reactionary to security attacks and will not be able to thwart attacks in real-time or even near real-time. Companies in Europe/Middle East seemed to especially lag behind the Americas and Asia Pacific by at least 7%. Future plans to deploy in-line capabilities in Europe/Middle East don't look too promising either, with their plans to use in-line lagging over 10% behind the other two regions. One good piece of news was that almost 1/3 have deployed in-line taps. Without the proper tools deployed in-line though, this doesn't mean much.

Question 8 asked "If not, what is preventing your company from conducting network security readiness/resilience testing?" In this question, 19% of respondents indicated that the security architecture didn't need testing because vendors already test their products. Asia Pacific had the strongest response here with 33% of respondents having that sentiment versus only 10% for the Americas. Another 10% indicated that the network didn't need to be tested because it was already tested in previous years. And an additional 10% indicated that management didn't support this type of effort.

All three response categories indicate that there is a definite education problem in terms of security best practices. Just because the network was tested once, doesn't mean it is still secure, especially if there have been any (even the slightest) changes to it.

Question 9 "Which of the following does your company perform annually?" investigated the use of security best practices further. While the answers to question 9 had some positive news as far as companies performing different types of test activities, about 12.5% of respondents indicated that their companies conduct no employee network security training (not even for IT) or response plan reviews. This means that of those 12.5% of respondents, basically none of them are prepared to respond to any type of serious security issue. Even for the rest of the respondents, only about 1/2 conduct security training activities and about 1/4 conduct response plan reviews. These all indicate problems with company processes.

Question 13 asked "Does your company have the following (different types of security plans)?" About 18% of respondents indicated that this question wasn't applicable to them. This is a further indicator of an education problem and a probable security architecture risk for these companies. The further implication to those companies is that they will probably experience costlier breaches than the more prepared companies.

Question 15 "How concerned are you about a network breach?" indicated that a little over 15% aren't too concerned about a security breach. The Americas were about 10% more concerned than Europe/Middle East and Asia Pacific. With the rising velocity and severity of security attacks, everyone should be concerned – as a significant security breach can be financially catastrophic for a small to mid-size enterprise and painful for a large enterprise.

Question 18 "Was your corporate network ever down due to a security attack (e.g. DDoS, malware)?" demonstrated that about 1/4 of the respondents indicated that their network has, in fact, been brought down by a security breach. The Americas were slightly under this average while both Asia Pacific and Europe/Middle East were almost 10% higher than the Americas. This is an alarming statistic. It's one thing to incur a breach and stay operational. It's another when your network comes to a grinding halt for a period of time. Productivity and brand value can become impacted.

The resulting surface-level conclusion is that some IT managers are still not taking network security seriously. A summary of the alarming results are as follows:

- 26% of respondents have no integrated visibility and security architecture
- 1/3 don't test their architecture or upgrades before deploying
- Only 20% have the ability to respond in real-time to an attack
- 40% have a lack of understanding basic security best practices
- 12.5% of companies conduct no readiness training
- Only about 1/2 conduct security training activities and about 1/4 conduct response plan review – indicating problems with company processes
- 18% don't conduct any contingency planning for security breaches
- 15% are unconcerned about a security breach
- 25% of security defenses are defeated so badly that the corporate network crashes and becomes unusable until the problem is remediated

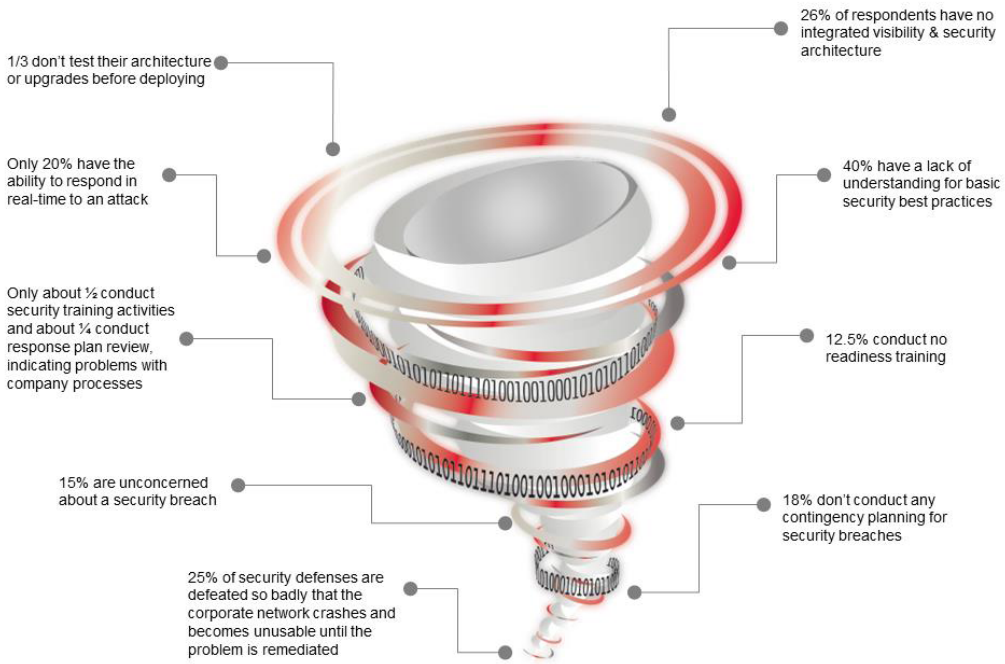


Figure 2: Many enterprises and carriers are still highly vulnerable to the effects of a security breach

2. Lack of knowledge, not cost, is the primary barrier to security improvements

The second conclusion from this study is that there is a lack of knowledge around how to properly implement security and visibility architectures – which is the primary barrier to security improvements. This is especially true for in-line security deployments. At the same, the typical average spend on network security is less than $100K annually. This conclusion was reached by studying the answers to the following questions: Question 3, Question 5, Question 6, Question 7, Question 8, and Question 15.

As mentioned earlier, Question 3 “Does your company currently deploy any of the following in-line security/monitoring solutions?” showed that only 20% of respondents are using in-line tools. A second question, Question 5 “If your company isn’t deploying in-line security solutions, what is preventing it from doing so?", explained this by showing that 24% are not deploying in-line tools because of a lack of experience/ knowledge with these solutions. The Americas were a little more confident at about 19%, while Asia Pacific (about 30%) and Europe/Middle East (about 30%) were less confident. Responses also showed concerns that in-line solutions would fail or introduce new security flaws were 7% and 12.5% lower, respectively. Cost, as a reason for not implementing in-line security, was only identified by 3.5% of respondents.

While cost is not a direct reason for lack of security investments, according to Question 6 “How much does your company spend annually on security investments?”, the highest category for spending (20%) was for less than $25K for the year. Another 14% plan on spending up to $100K. This means that about 34% plan on spending $100K or less on annual improvements. After that, all categories drop to single digits for responses. An interesting note is that about 16% plan to spend between $100K and $500K and about 10% plan to spend over $1M on annual security investments.

Question 7 “Does your company currently conduct any of the following testing for the different network life-cycle stages?” showed that only about 1/3 of respondents are following best practices and testing their networks during pre-production, production, and upgrade lifecycle phases. This leaves about 50% (removing answers for those not involved with this type of security effort) conducting little to no testing. Out of that number, almost half confirm that they are not testing at all. From a regional perspective, Europe/Middle East were performing the best for pre-production and production testing activities. The Americas were conducting the least amount of testing in those areas. One interesting note was that while Europe/Middle East led in those two categories, they conducted the least amount of testing for upgrades.

Question 8 “If not, what is preventing your company from conducting network security readiness/resilience testing?” confirmed that there is a lack of knowledge. As mentioned previously, 19% of respondents don’t perform security readiness testing because the vendor already tests their products. This shows a clear lack of understanding as to how vendors test products and what they test. The vendor testing cannot be assumed as a replacement for network testing. Configuration changes can create brand new security holes that need routine security integrity validation.

Question 15 “How concerned are you about a network breach?” went on to show that 15% are unconcerned about a breach. As stated in Conclusion 1, this shows a clear lack of understanding regarding the security risks that all companies face.

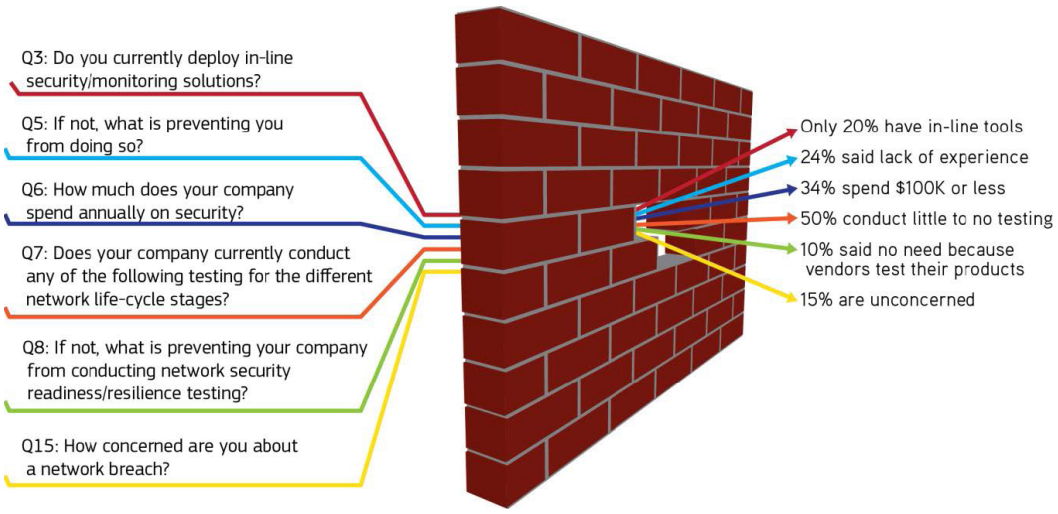


Figure 3: Lack of knowledge, not cost, is the primary barrier to security improvements

3. Security resilience approaches are showing significant worldwide adoption

On a positive note, the survey confirmed that security resilience approaches are growing in worldwide adoption. This conclusion was based upon responses to Question 1, Question 2, Question 7, Question 9, Question 10, Question 12, and Question 13.

While Question 1 “Does your company have a visibility (monitoring) architecture integrated with your security architecture to recognize and record any security attacks?” showed an architecture flaw for some enterprises, the question also revealed that 59% of businesses are actually merging visibility and security architectures. This is a very positive architectural improvement. There will be always be some security risk, so managing that risk to make it as small as possible is the clear path forward for enterprises.

Respondents were also looking at the different phases of the life of their network and implementing products and processes accordingly. Evidence of a life cycle approach starts with Question 2 “How often does your company actively test your architecture and upgrades for security issues BEFORE you deploy them into the live network?” and shows that respondents are trying to validate the initial designs and upgrades for their network. Of the responses, 20% test any changes all the time and another 21% test them most of the time.

Question 7 “Does your company currently conduct any of the following testing for the different network life-cycle stages?” follows up with a direct question on test efforts. Here are the results per lifecycle stage:

Life-Cycle Stage Testing Activity	Percent
Pre-deployment load testing	32%
Pre-deployment security resilience testing	36%
Production security resilience testing	38%
Hardware upgrade security resilience testing	29%
Software upgrade security resilience testing	32%

Question 9 “Which of the following does your company perform annually?” and Question 13 “Does your company have the following?” asked further questions on different types of activities that can be assigned to a life-cycle stage. The following responses show the percentage of respondents that are conducting these activities.

Life-Cycle Stage Testing Activity	Percent
Penetration testing	42%
Network security threat/resilience testing	44%
Red Flag testing	15%
Response plan review	28%
IT employee security training	47%

Life-Cycle Stage Testing Activity	Percent
Cyber range training	14%
Business continuity plan	56%
Chief Information Security Officer	52%
Network security architecture baseline	45%
Network security remediation/escalation plan	41%
Network security test plan	36%

For Question 10 “Does your company have a cyber range?”, the average number of respondents saying that they have a cyber range was 22%. From a regional perspective, Europe/Middle East/Africa (EMEA) and Asia Pacific (APAC) had almost double the amount of cyber ranges as the Americas. Support for cyber range training is a good indicator of personnel training in the operational phase.

Question 12 “Has your company seen less of any of these network problems due to network readiness/resilience testing?” asked whether individuals had seen any evidence of improvements due to resilience testing. The answer was yes. Over 32% had seen less network failures and 26% had seen fewer breaches.

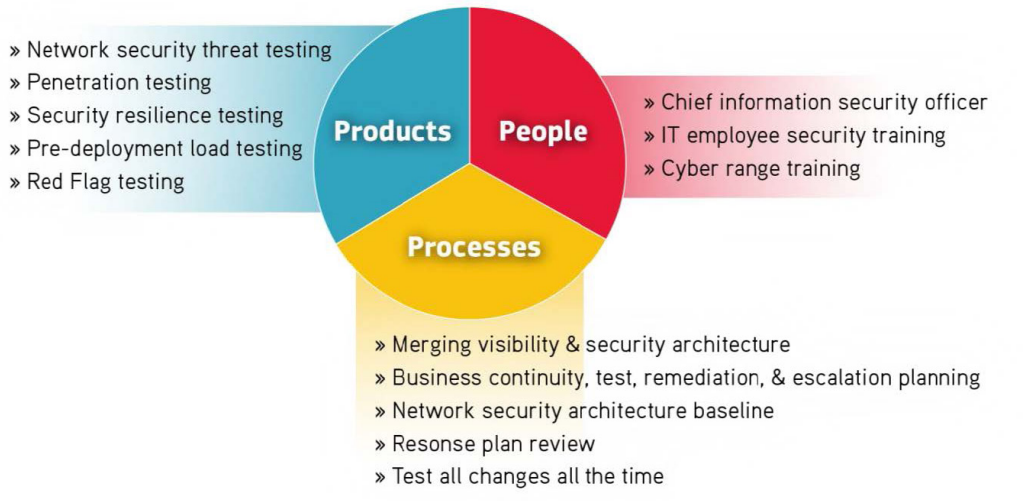


Figure 4: Security resilience approaches are showing significant worldwide adoption

4. Top two main security concerns are data loss and malware attacks

The survey also asked respondents what their top security concerns were. The two highest concerns were data loss and malware attacks. This conclusion was based upon responses to Question 16 “What is your company’s main security threat/emerging risk (that you know you have)?”. There were 145 individual responses collected to this question.

A summary of the detailed results is as follows:

- Data loss (information leaks, DLP) / breach of information = 22
- Malware attack (worm, virus, botnet) = 19
- DDoS attacks = 18
- General Cyber Attack (hacking, cyber terrorism) = 16
- Application Vulnerability (attacks, backdoors, SQL, client, Zero Day vulnerabilities) =10
- Insider threats (others, people, employees, USB copying of files) = 10
- Negligence or human error (gen. passwords, emp. awareness) = 8
- Phishing, SPAM, emails = 8
- Lack of Defenses (old equipment, authentication) = 5
- Other (client loss, growth, public exposure, phone fraud) = 5
- Nation State hacking = 4
- Advanced persistent threats = 4
- Availability (physical network or cloud service down) = 4
- Mobile devices =3
- End point security = 3
- Updates & upgrades = 2
- Customer & Partner Vulnerabilities (IaaS, outside breaches) = 2
- Physical data center security =1
- PCI, Financial transactions =1

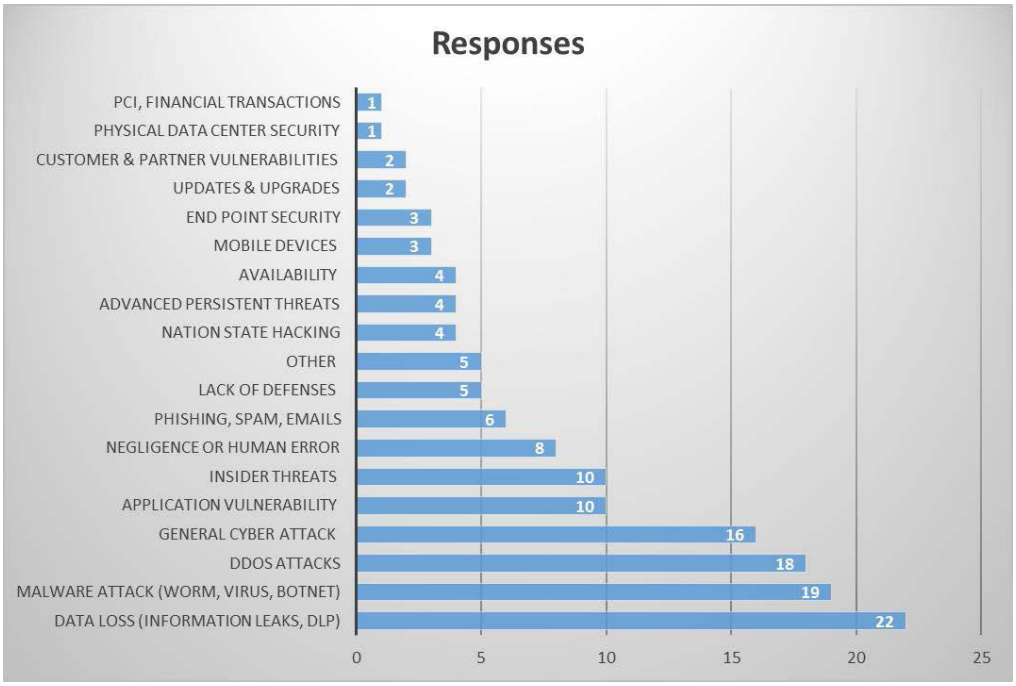


Figure 5: Top two main concerns are data loss and malware attacks

Survey Result Highlights

In addition to the key findings, other useful insights are available from the survey data. These are summarized as follows:

1. Enterprises are embracing the integration of visibility architectures with security architectures. 59% have already done this. From a regional perspective, here is the breakdown for the respondents who answered yes: Americas = 56%, Asia Pacific = 55%, Europe/Middle East = 68%. (Question 1)

2. About 1/4 of enterprises and carriers are still highly vulnerable to the effects of a security breach since they lack core capabilities to spot and control the damage. (Question 1)

3. Over 1/3 of enterprises and carriers are not following best practices when it comes to system updates and upgrades. Of the 20% of respondents that are following best practices, here is the regional breakdown for those that said they follow best practices all of the time: Americas = 23%, Asia Pacific = 19%, and for Europe/Middle East = 17%. (Question 2)

4. Approximately 20% of companies have deployed in-line security tools and 54% are using taps and bypass switches. A regional deployment of in-line tools is as follows: Americas = 22%, Asia Pacific = 24%, and for Europe/Middle East = 15%. (Question 3)

5. About 33% of respondents plan to deploy more security tools in the next year. 31% also plan to deploy taps and bypass switches. A regional breakdown for those that have plans to deploy in-line NPBs is as follows: Americas = 15.5%, Asia Pacific = 17%, and Europe/Middle East = 4.4%. (Question 4)

6. Cost isn't a major barrier for deploying in-line security solutions, its lack of experience according to 1/4 of the respondents. The regional breakdown of answers for lack of experience is as follows: Americas = 19%, Asia Pacific = 28%, and Europe/Middle East = 30%. (Question 5)

7. The typical annual spend on network security is less than $100K. (Question 6)

8. When it comes to testing, the Americas perform the lowest amount of pre-deployment testing, while Europe/Middle East perform the highest amount of pre-deployment testing (but also the lowest amount of upgrade testing). Europe/Middle East perform the highest amount of production network testing. (Question 7)

9. About 30% of companies are following some form of a life-cycle approach to network security. (Question 7)

10. A lack of understanding about security threats is leaving companies vulnerable:
    - About 43% of companies are performing security threat and resilience testing. (Question 9)
    - 51% don't see a need for network readiness/resilience testing because the network was either tested in previous years, they use a pen tester or assume products are already tested by vendor (Question 8)
    - 20% don't have budget for network readiness/resilience testing (Question 8)
    - 17% don't have time for network readiness/resilience testing (Question 8)
    - 12% of companies don't do annual security preparedness (pen test, threat test, response planning, Red Flag testing, cyber range training, IT security training, etc.) (Question 9)

11. Asia Pacific has the highest belief that vendors test products (33%) so there is no need to test them, while the Americas has the lowest belief in this concept (10%). (Question 8)

12. Europe/Middle East perform the most pen testing at 54%. (Question 9)

13. Cyber range training is consistent across all 3 regions at approximately 15%. (Question 9)

14. Approximately 22% of companies have a cyber range. Europe/Middle East and Asia Pacific have almost double the amount of cyber ranges that the Americas has. (Question 10)

15. Companies are realizing benefits from network resilience testing. Network failures are down 36.5% and security breaches are down 26%. Specifically, Europe/Middle East (48%) have seen less network failures than Asia Pacific (38%) and the Americas (33%). (Question 12)

16. The following is a summary of the responses to Question 13:
    - Business continuity plan = Asia Pacific (65%), Americas (59%), Europe/Middle East (45%)
    - CISO = Europe/Middle East (61%), Americas (51%), Asia Pacific (44%)
    - Architecture baseline = Europe/Middle East (55%), Asia Pacific (47%), Americas (40%)
    - Remediation and escalation plan = Asia Pacific (50%), Americas (43%), Europe/Middle East (32%)
    - Testing plan = Asia Pacific (44%), Americas (42%), Europe/Middle East (26%)
17. The following is a summary of attacks/breaches for 2014 (Question 14):
    - 19% had 0
    - 20% had 5 or more
    - 40% had 1 or more
    - 5+ Europe/Middle East = 32%, Americas = 23%, Asia Pacific = 15%
    - 0 Europe/Middle East = 23%, Americas = 17%, Asia Pacific = 12%
18. The following data summarizes the response to the question of how concerned the respondents were about a future breach (Question 15):
    - 34% are extremely concerned
    - 60% are extremely or very concerned
    - 15% aren't that concerned
    - The Americas are more concerned (38%) with this topic than Asia Pacific & Europe/Middle East (both around 29%)
    - Over half were very or extremely concerned across all three regions
19. When a breach did occur, most companies experienced multiple types of losses (monetary, IP, etc.). (Question 17)
20. When asked about specific types of losses, the respondents indicated the following (Question 17):
    - Asia Pacific experienced the most types of monetary financial loss (30%) vs. the Americas (21%) and Europe/Middle East (6.5%)
    - Asia Pacific experienced the most types of IP loss (47%) vs. the Americas (24%) and Europe/Middle East (29%)
    - Asia Pacific experienced the most types of PII loss (62%) vs. the Americas (26%) and Europe/Middle East (32%)
    - Asia Pacific's largest loss was in IP. The Americas highest loss was in productivity. Europe/Middle East lost the most in productivity.
    - Asia Pacific experienced more amounts of loss in every category compared to the Americas and Europe/Middle East

21. Question 18 asked what percentage of companies lost network uptime as part of a security attack. The averaged answer was 25% with a regional breakdown as follows: Americas = 22%, Asia Pacific = 30%, and the Europe/Middle East = 32%.

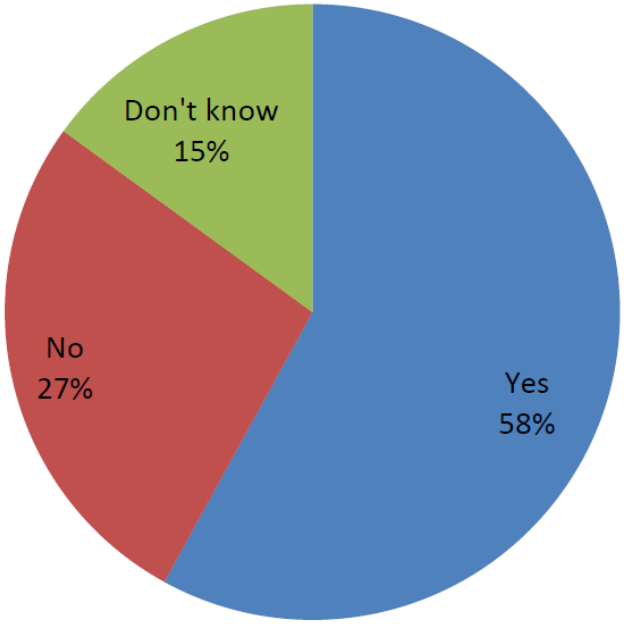
22. The average amount of time a network was down due to a security attack was 5 to 30 minutes. (Question 19)

23. Question 20 asked what the financial impact of a breach was to the respondents. A summary is as follows:
    - Most don't know the cost of a breach (over 54%)
    - The highest response category (16%) indicated that total average losses were less than $25K worldwide
    - A little over 30% experienced a loss of $500K or less
    - Almost 4% experienced a breach of over $50M
    - Europe/Middle East and Asia Pacific average losses were less than $25K per company
    - The average losses for the Americas were between $100K - $500K

Detailed Survey Responses

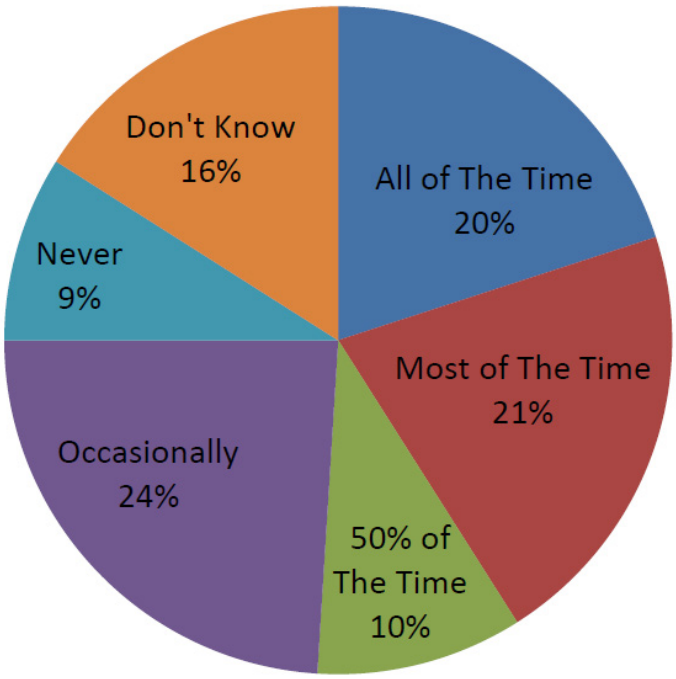
These results were compiled on June 5, 2015.

1. Does your company have a visibility (monitoring) architecture integrated with your security architecture to recognize and record any security attacks?



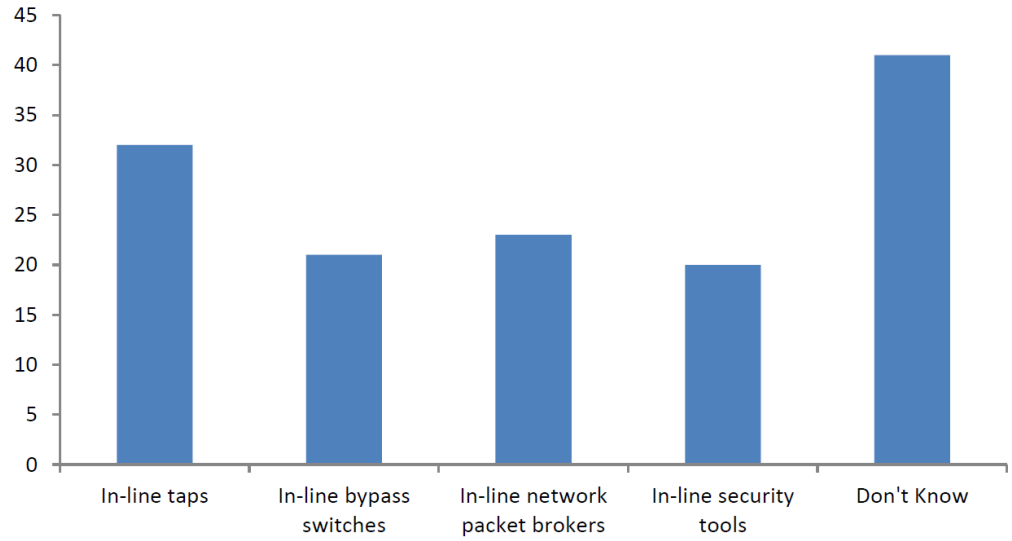
Value	Percent	Count
Yes	58.2%	153
No	26.6%	70
Don't know	15.2%	40
Total		263

2. How often does your company actively test your architecture and upgrades for security issues BEFORE you deploy them into the live network?



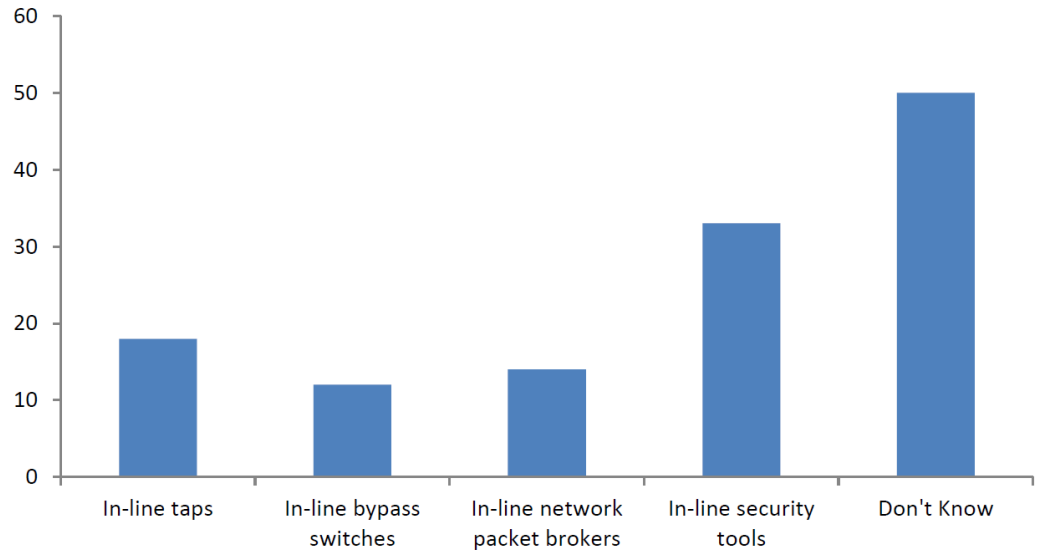
Value	Percent	Count
All of The Time	20.3%	53
Most of The Time	20.7%	54
50% of The Time	10.0%	26
Occasionally	23.8%	62
Never	8.8%	23
Don't Know	16.5%	43
Total		261

3. Does your company currently deploy any of the following in-line security/monitoring solutions? (select all that apply)



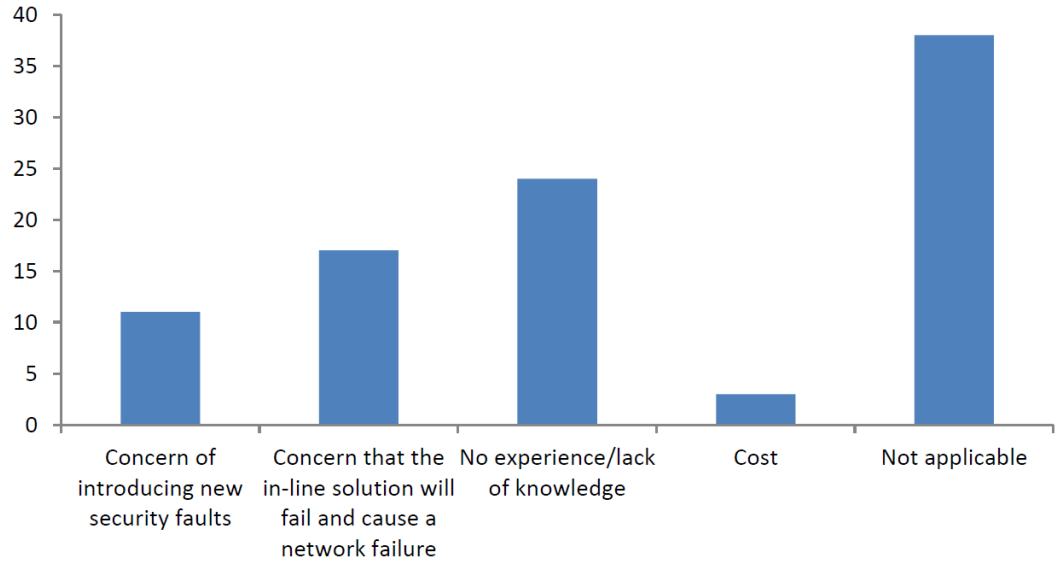
Value	Percent	Count
In-line taps	32.2%	84
In-line bypass switches	21.1%	55
In-line network packet brokers	23.4%	61
In-line security tools	19.5%	51
Don't Know	41.4%	108
Total		261

4. Does your company have plans to deploy in-line security/monitoring solutions during the next year? (select all that apply)



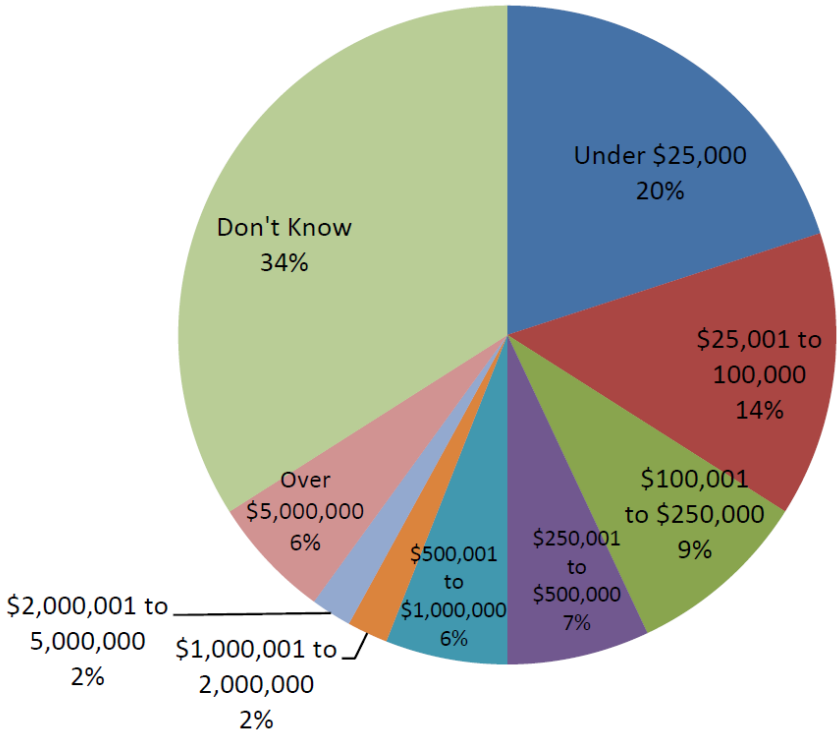
Value	Percent	Count
In-line taps	18.1%	47
In-line bypass switches	12.3%	32
In-line network packet brokers	14.2%	37
In-line security tools	33.1%	86
Don't Know	50.4%	131
Total		260

5. If your company isn't deploying in-line security solutions, what is preventing it from doing so? (select all that apply)



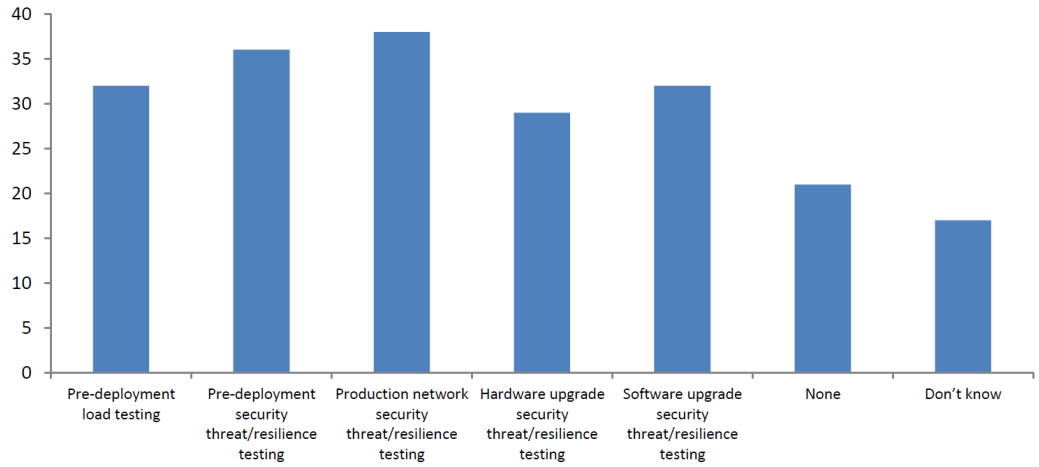
Value	Percent	Count
Concern of introducing new security faults	11.5%	30
Concern that the in-line solution will fail and cause a network failure	16.9%	44
No experience/lack of knowledge	23.8%	62
Cost	3.5%	9
Not applicable	38.3%	100
Total		261

6. How much does your company spend annually on security investments (assume USD)?



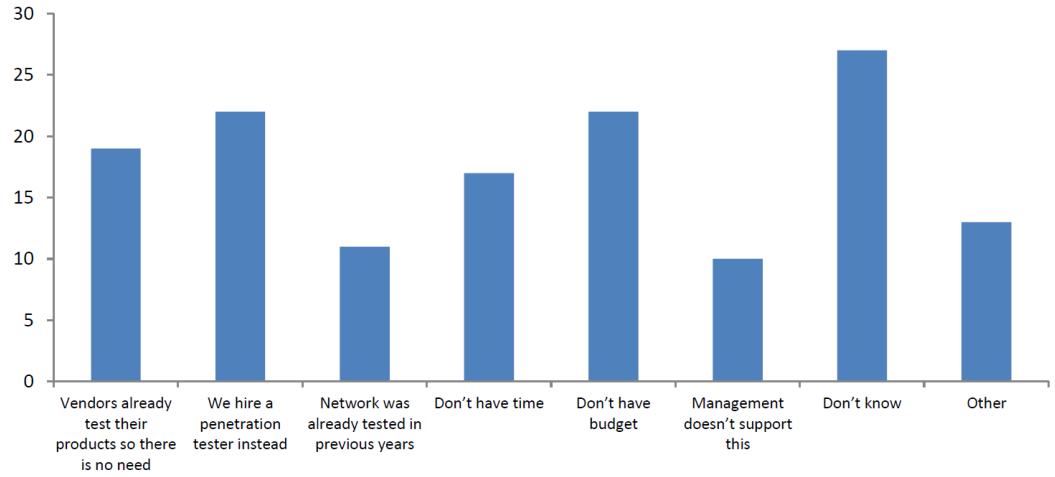
Value	Percent	Count
Under $25,000	20.3%	53
$25,001 to 100,000	14.2%	37
$100,001 to $250,000	8.8%	23
$250,001 to $500,000	6.9%	18
$500,001 to $1,000,000	5.8%	15
$1,000,001 to 2,000,000	1.9%	5
$2,000,001 to 5,000,000	2.3%	6
Over $5,000,000	5.8%	15
Don't Know	34.1%	89
Total		261

7. Does your company currently conduct any of the following testing for the different network life-cycle stages? (select all that apply)



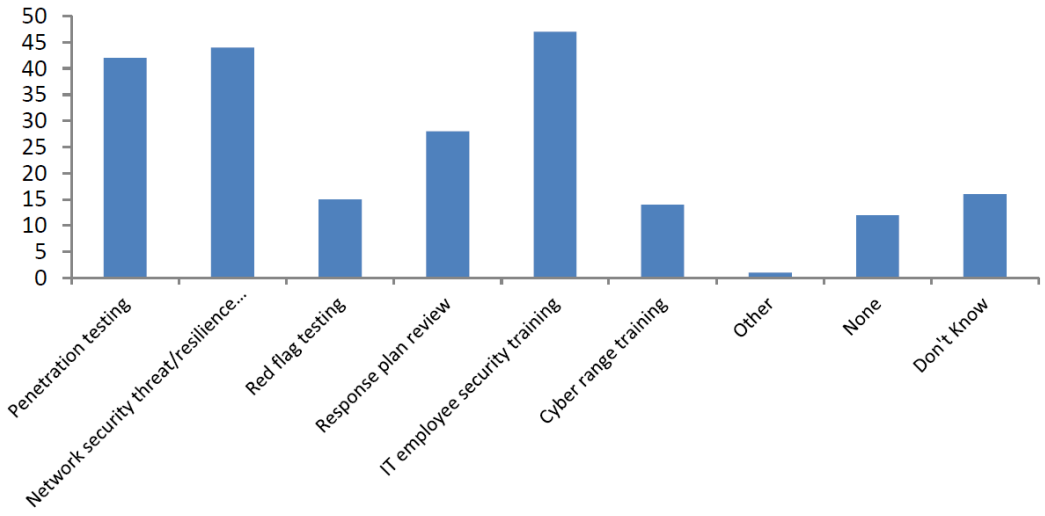
Value	Percent	Count
Pre-deployment load testing	31.8%	64
Pre-deployment security threat/ resilience testing	36.3%	73
Production network security threat/ resilience testing	38.3%	77
Hardware upgrade security threat/ resilience testing	29.4%	59
Software upgrade security threat/ resilience testing	32.3%	65
None	20.9%	42
Don't know	17.4%	35
Total		201

8. If not, what is preventing your company from conducting network security readiness/resilience testing? (select all that apply)



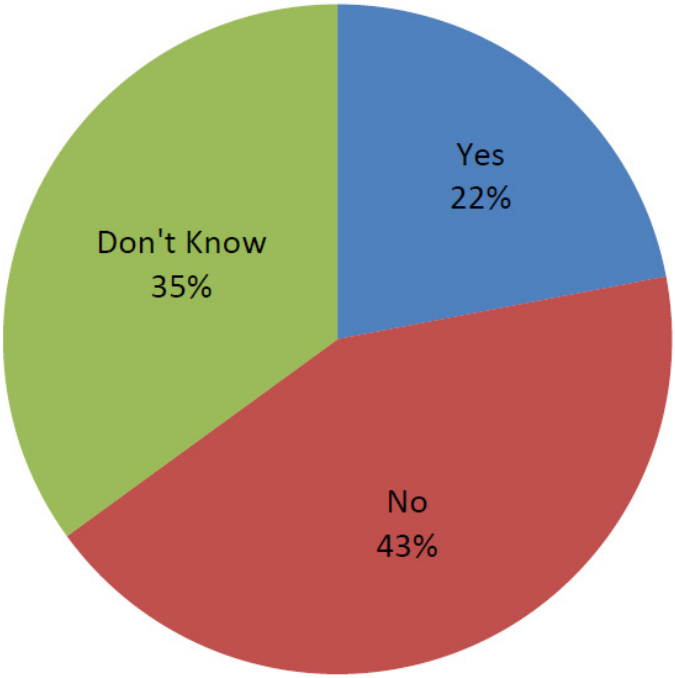
Value	Percent	Count
Vendors already test their products so there is no need	19.0%	38
We hire a penetration tester instead	22.0%	44
Network was already tested in previous years	10.5%	21
Don't have time	17.0%	34
Don't have budget	22.0%	44
Management doesn't support this	9.5%	19
Don't know	26.5%	53
Other	12.5%	25
Total		200

9. Which of the following does your company perform annually? (select all that apply)



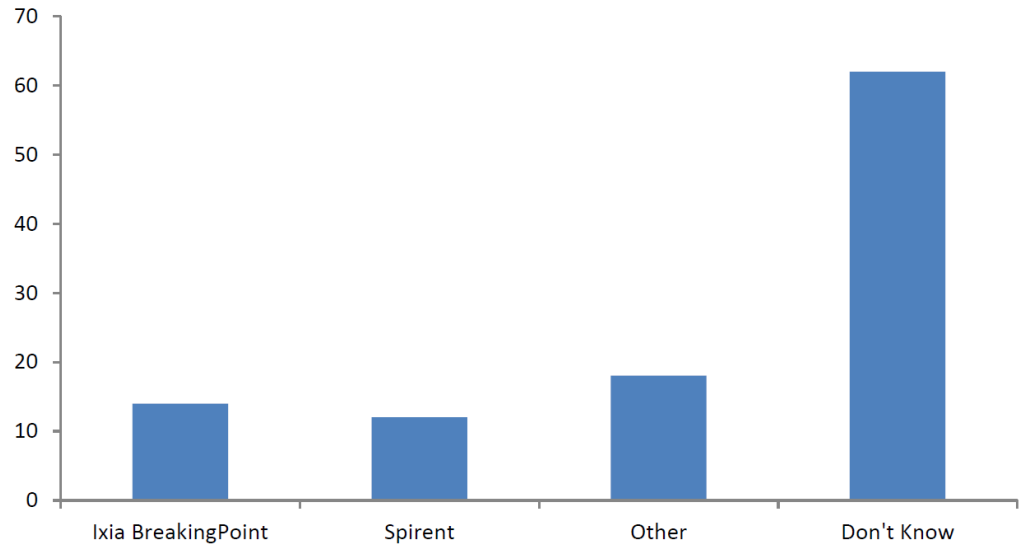
Value	Percent	Count
Penetration testing	42.1%	85
Network security threat/resilience testing	44.1%	89
Red flag testing	15.4%	31
Response plan review	27.7%	56
IT employee security training	46.5%	94
Cyber range training	14.4%	29
Other	0.5%	1
None	12.4%	25
Don't Know	16.3%	33
Total		202

10. Does your company have a cyber range?



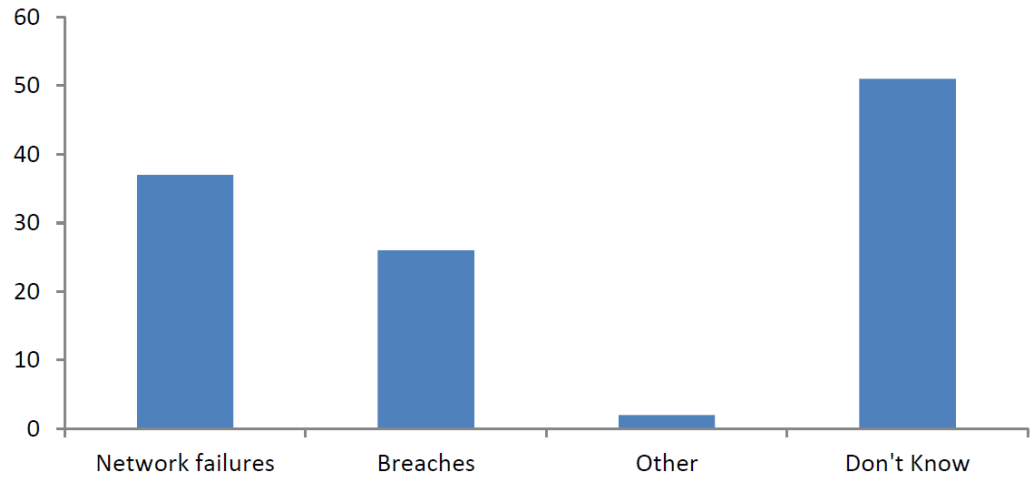
Value	Percent	Count
Yes	22.4%	45
No	42.8%	86
Don't Know	34.8%	70
Total		201

11. What tools does your company use to test your network security readiness/ resilience with? (select all that apply)



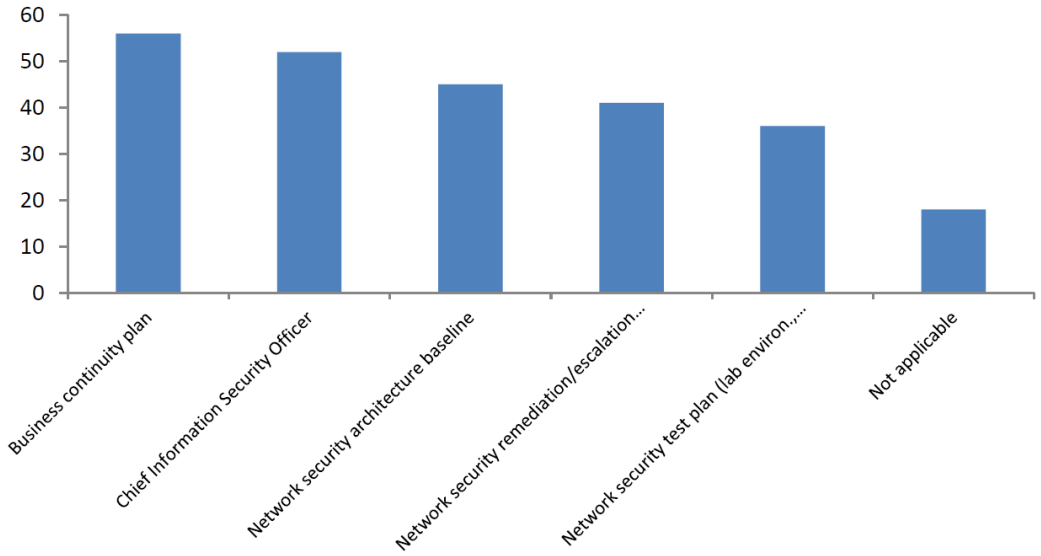
Value	Percent	Count
Ixia BreakingPoint	14.4%	29
Spirent	11.9%	24
Other	17.9%	36
Don't Know	61.7%	124
Total		201

12. Has your company seen less of any of these network problems due to network readiness/resilience testing? (select all that apply)



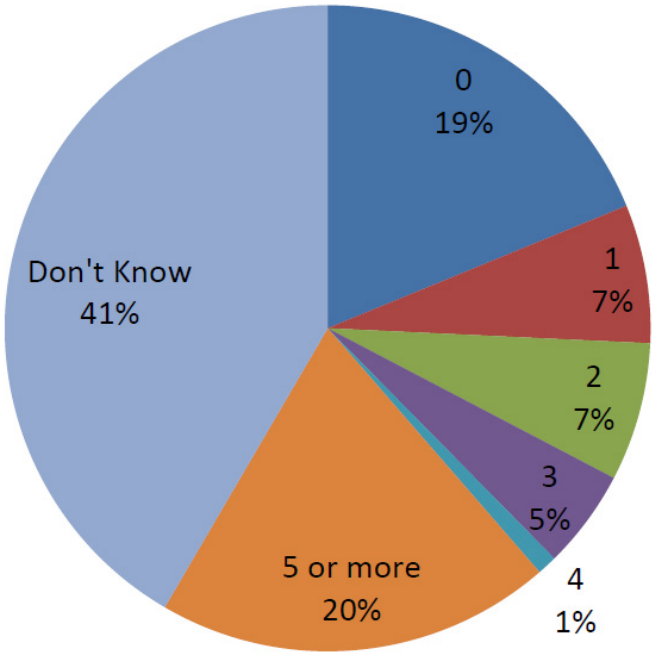
Value	Percent	Count
Network failures	37.2%	64
Breaches	26.2%	45
Other	2.3%	4
Don't Know	50.6%	87
Total		172

13. Does your company have the following? (select all that apply)



Value	Percent	Count
Business continuity plan	56.4%	97
Chief Information Security Officer	51.7%	89
Network security architecture baseline	44.8%	77
Network security remediation/ escalation plan	40.7%	70
Network security test plan (lab environ., production environ., or upgrades)	36.1%	62
Not applicable	18.0%	31
Total		172

14. How many security attacks/breaches did your company experience in 2014?

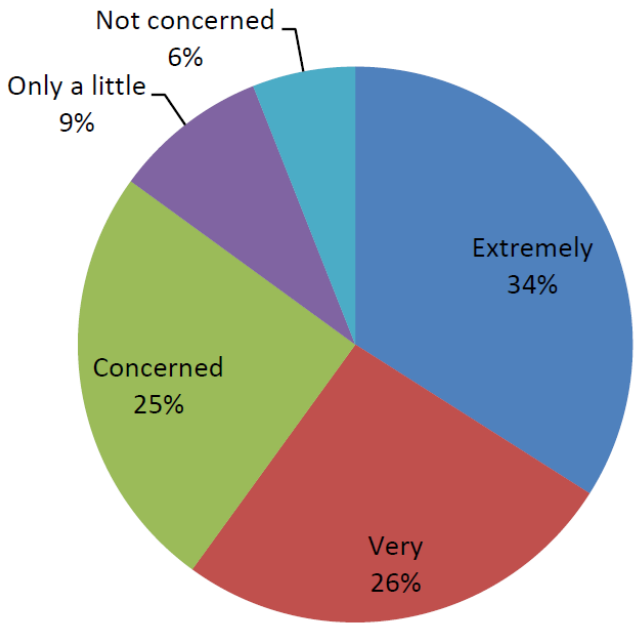


Value	Percent	Count
0	18.6%	32
1	7.0%	12
2	7.0%	12
3	4.7%	8
4	1.2%	2
5 or more	19.8%	34
Don't Know	41.9%	72
Total		172

Statistics

Total Responses	172
Sum	238.0
Average	2.4
StdDev	2.1

15. How concerned are you about a network breach?

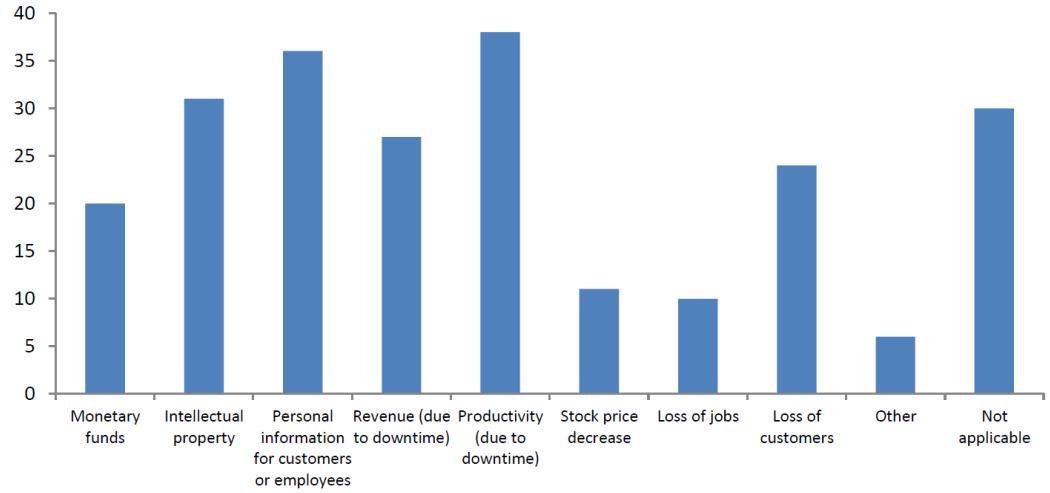


Value	Percent	Count
Extremely	33.7%	58
Very	26.2%	45
Concerned	25.0%	43
Only a little	8.7%	15
Not concerned	6.4%	11
Total		172

16. What is your company's main security threat/emerging risk (that you know you have)?

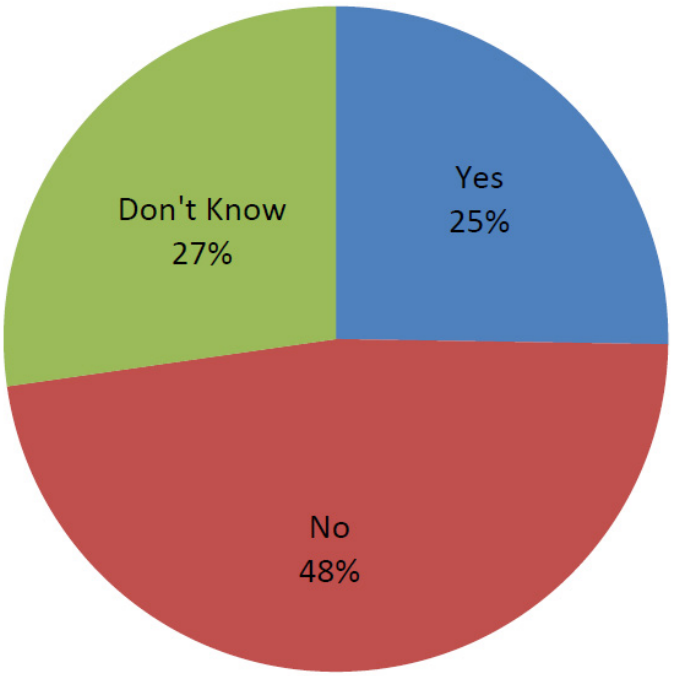
Count	Response
22	Data loss (information leaks, DLP) / breach of information
19	Malware attack (worm, virus, Botnet)
18	DDoS attacks
16	General Cyber Attack (hacking, cyber terrorism)
10	Application Vulnerability (attacks, backdoors, SQL, client, Zero Day vulnerabilities)
10	Insider threats (others, people, employees, USB copying of files)
8	Negligence or Human error (gen. passwords, emp. awareness)
8	Phishing, SPAM, emails
5	Lack of Defenses (old equipment, authentication)
5	Other (client loss, growth, public exposure, phone fraud)
4	Nation State hacking
4	APT
4	Availability (physical network or cloud service down)
3	Mobile devices
3	End point security
2	Updates & upgrades
2	Customer & Partner Vulnerabilities (IaaS, outside breaches)
1	Physical data center security
1	PCI, Financial transactions
11	Not applicable for my team
31	Don't know

17. If your company experienced a breach, what types of loss were experienced? (select all that apply)



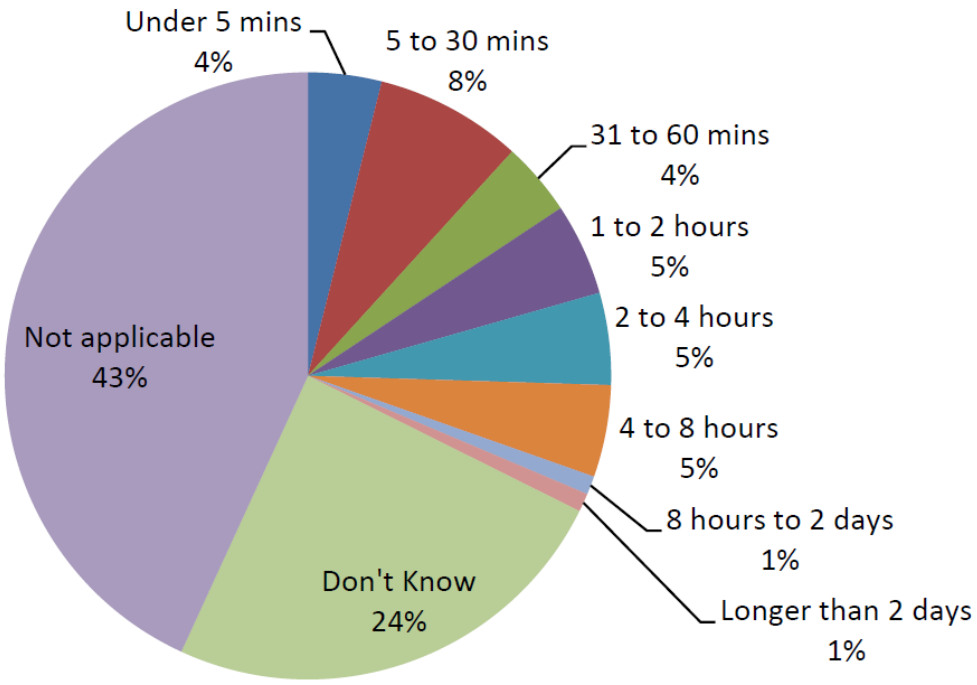
Value	Percent	Count
Monetary funds	19.8%	34
Intellectual property	31.4%	54
Personal information for customers or employees	36.1%	62
Revenue (due to downtime)	27.3%	47
Productivity (due to downtime)	38.4%	66
Stock price decrease	11.1%	19
Loss of jobs	9.9%	17
Loss of customers	24.4%	42
Other	5.8%	10
Not applicable	30.2%	52
Total		172

18. Was your corporate network ever down due to a security attack (e.g. DDoS, malware)?



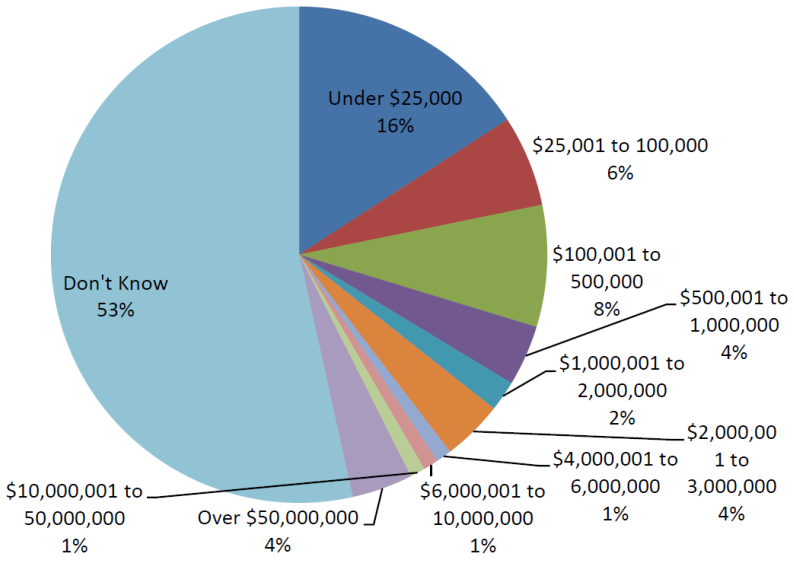
Value	Percent	Count
Yes	25.2%	43
No	47.4%	81
Don't Know	27.5%	47
Total		171

19. If so, how long?



Value	Percent	Count
Under 5 mins	3.5%	6
5 to 30 mins	7.7%	13
31 to 60 mins	3.5%	6
1 to 2 hours	4.7%	8
2 to 4 hours	4.7%	8
4 to 8 hours	4.7%	8
8 hours to 2 days	1.2%	2
Longer than 2 days	1.2%	2
Don't Know	24.7%	42
Not applicable	44.1%	75
Total		170

20. What is the financial impact of a breach for your company (assume USD)?



Value	Percent	Count
Under $25,000	15.8%	27
$25,001 to 100,000	6.4%	11
$100,001 to 500,000	8.2%	14
$500,001 to 1,000,000	4.1%	7
$1,000,001 to 2,000,000	1.8%	3
$2,000,001 to 3,000,000	3.5%	6
$3,000,001 to 4,000,000	0.0%	0
$4,000,001 to 6,000,000	0.6%	1
$6,000,001 to 10,000,000	1.2%	2
$10,000,001 to 50,000,000	0.6%	1
Over $50,000,000	3.5%	6
Don't Know	54.4%	93
Total		171

Methodology and Scope

Survey invitations were sent out to thousands of targeted individuals worldwide. This included engineering teams, product management teams, sales and sales engineering, and management teams. The survey was localized by region with three separate regions being created: the Americas (North and South America), Europe/Middle East (including African countries), and Asia Pacific (included mainland Asia, Indonesia, Australia, etc.). Germany was excluded from the survey due to SPAM laws.

A total of 263 surveys were returned. Of this number, there were 154 complete responses and 109 partial responses (where the respondent answered yes but did not complete all questions). The Americas had the largest number of responses (approximately 60%) with the other two regions both around 25% of the total responses.

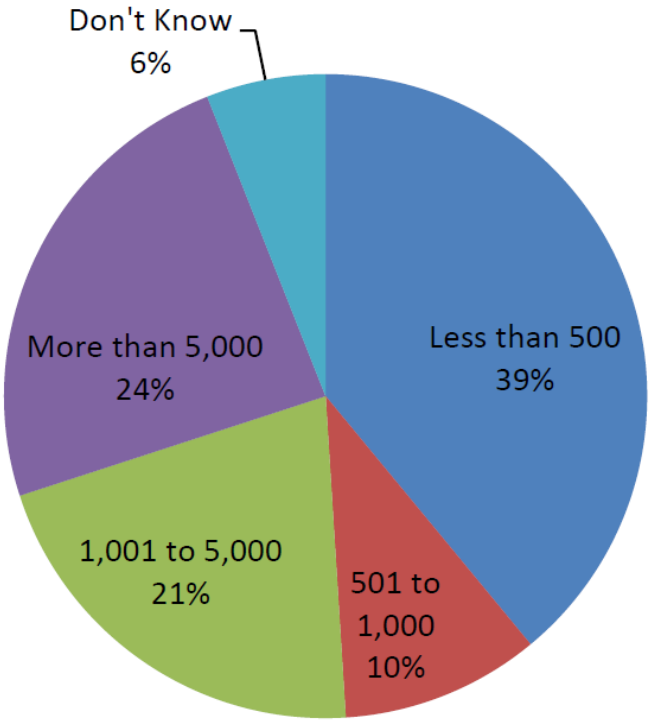
The exact breakdown of the responses by region is as follows:

- North and South America (60.1%) = 93 completed, 65 partial responses
- Europe, Middle East, and Africa (20.9%) = 29 completed, 26 partial responses
- Asia Pacific (19.0%) = 32 completed, 18 partial responses

Survey Demographic Information

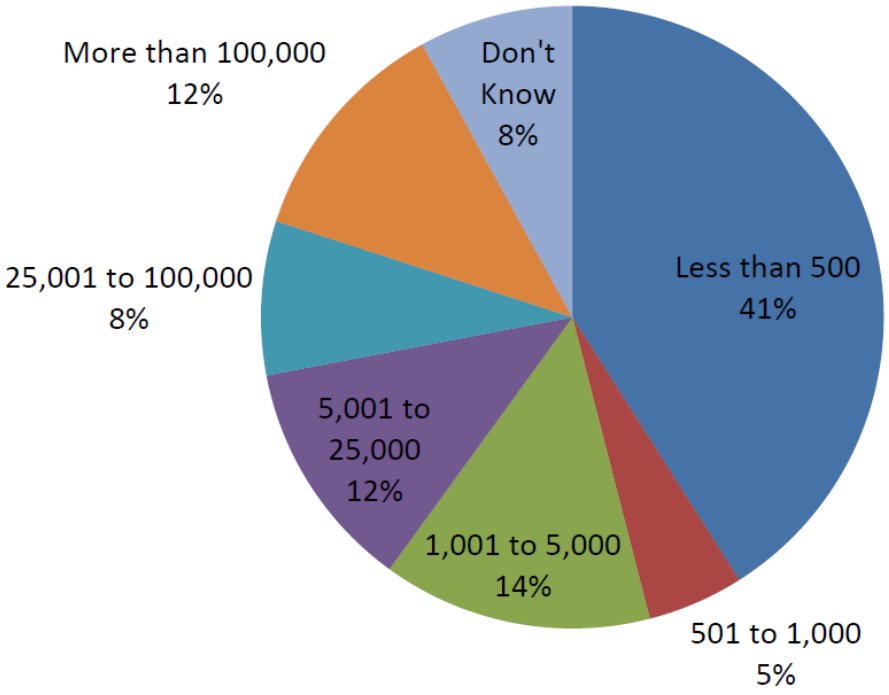
Company demographic size split fairly evenly across all three regions between SMB (less than 500 employees), small enterprise (500 to 5,000 employees), and large enterprise (over 5,000 employees). There was a slightly larger amount of SMB respondents. The exact split was as follows: SMB = 39%, small enterprise = 31%, and large enterprise = 24%. There was about 6% that did not know. However, both Asia Pacific and Europe/Middle East had more responses from the SMB segment with 40% of respondents for Asia Pacific and 50% of respondents for Europe/Middle East.

21. How many employees does your company have?



Value	Percent	Count
Less than 500	38.8%	64
501 to 1,000	10.3%	17
1,001 to 5,000	21.2%	35
More than 5,000	23.6%	39
Don't Know	6.1%	10
Total		165

22. How many people does your company network support?

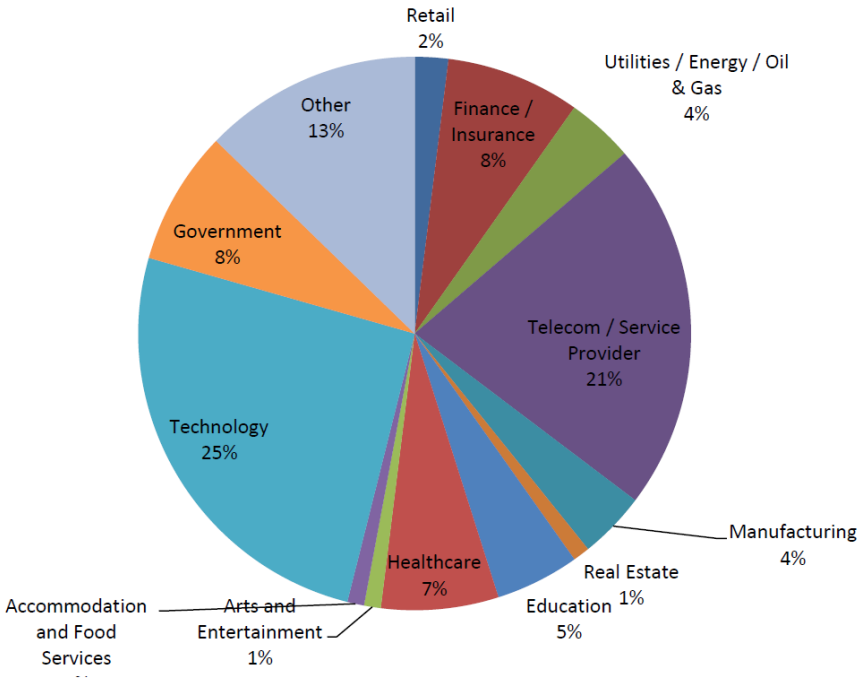


Value	Percent	Count
Less than 500	40.6%	67
501 to 1,000	5.5%	9
1,001 to 5,000	13.9%	23
5,001 to 25,000	11.5%	19
25,001 to 100,000	7.9%	13
More than 100,000	12.1%	20
Don't Know	8.5%	14
Total		165

Responses by Market Segment

The top responding market segments were as follows: Technology (26.1%), Telecom/ Service Provider (21.8%), Finance/Insurance (7.9%), Government (7.9%), and Healthcare (6.7%). The following chart shows a detailed breakdown.

23. Which of the following best describes your company's business?



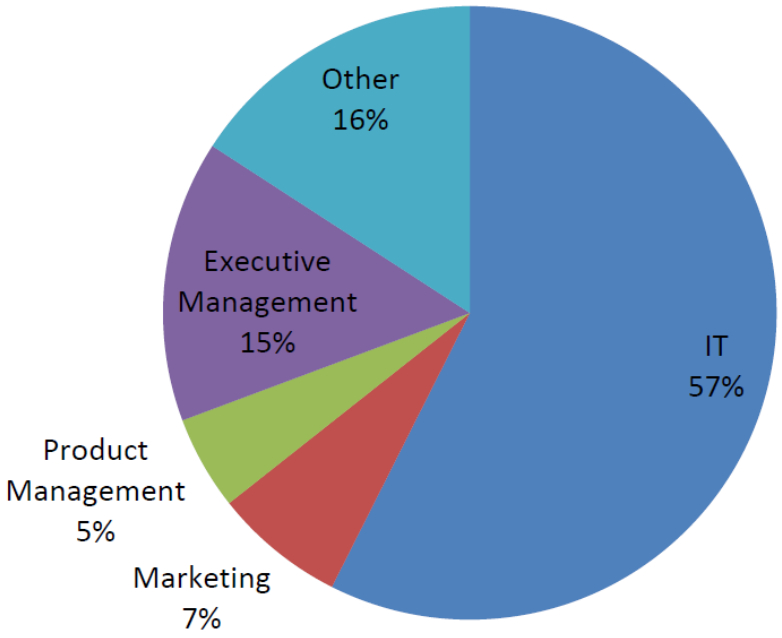
Value	Percent	Count
Retail	1.8%	3
Finance / Insurance	7.9%	13
Utilities / Energy / Oil & Gas	3.6%	6
Telecom / Service Provider	21.8%	36
Manufacturing	3.6%	6
Construction	0.0%	0
Transportation	0.0%	0
Real Estate	0.6%	1

Value	Percent	Count
Real Estate	0.6%	1
Education	5.5%	9
Healthcare	6.7%	11
Arts and Entertainment	1.2%	2
Accommodation and Food Services	0.6%	1
Technology	26.1%	43
Government	7.9%	13
Other	12.7%	21
Total		165

Responses by Role

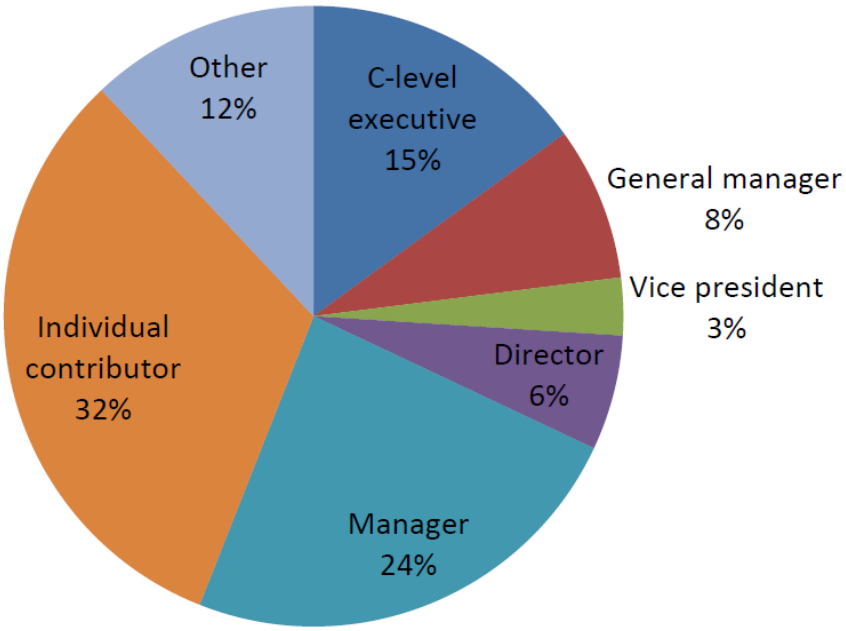
The roles of respondents varied. 57% of respondents were in IT. Another 15% of respondents were executives. The other category mainly comprised technical personnel such as architects, engineers, sales engineering, project management, and consultants.

24. What is your role within your company?



Value	Percent	Count
IT	57.6%	95
Marketing	7.3%	12
Product Management	4.9%	8
Executive Management	14.6%	24
Other	15.8%	26
Total		165

25. My responsibilities in my organization can be best described as:



Value	Percent	Count
C-level executive	14.6%	24
General manager	8.5%	14
Vice president	3.0%	5
Director	6.1%	10
Manager	23.6%	39
Individual contributor	32.1%	53
Other	12.1%	20
Total		165

Responses by Country

Information on responses by country was also captured. The top reporting countries were: United States of America (43.7%), India (8.7%), China (3.9%), and Malaysia (3.5%). A detailed breakdown is provided as follows:

Value	Percent	Count
Argentina	0.4%	1
Australia	1.2%	3
Belgium	0.4%	1
Bulgaria	0.4%	1
Canada	2.8%	7
Chile	0.4%	1
China	3.9%	10
Colombia	0.8%	2
Croatia	0.4%	1
Czech Republic	0.4%	1
France	1.6%	4
Germany	0.8%	2
Greece	0.4%	1
Hong Kong	1.2%	3
Hungary	0.8%	2
India	8.7%	22
Indonesia	2.0%	5
Ireland	0.4%	1
Israel	0.8%	2

Value	Percent	Count
Italy	0.4%	1
Japan	1.6%	4
Korea, Republic of	2.8%	7
Malaysia	3.5%	9
Mexico	1.2%	3
Netherlands	1.2%	3
New Zealand	0.4%	1
Norway	0.8%	2
Pakistan	0.4%	1
Philippines	1.2%	3
Portugal	0.8%	2
Qatar	0.4%	1
Romania	2.4%	6
Russian Federation	1.2%	3
Saudi Arabia	0.4%	1
Singapore	1.2%	3
Spain	1.6%	4
Sweden	1.2%	3
Switzerland	0.8%	2
Taiwan	0.4%	1
Thailand	0.4%	1

Value	Percent	Count
Turkey	0.8%	2
United Arab Emirates	0.8%	2
United Kingdom	2.4%	6
United States	43.7%	111
Vietnam	0.4%	1
Yemen	0.4%	1
Total		254

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus

KEYSIGHT TECHNOLOGIES