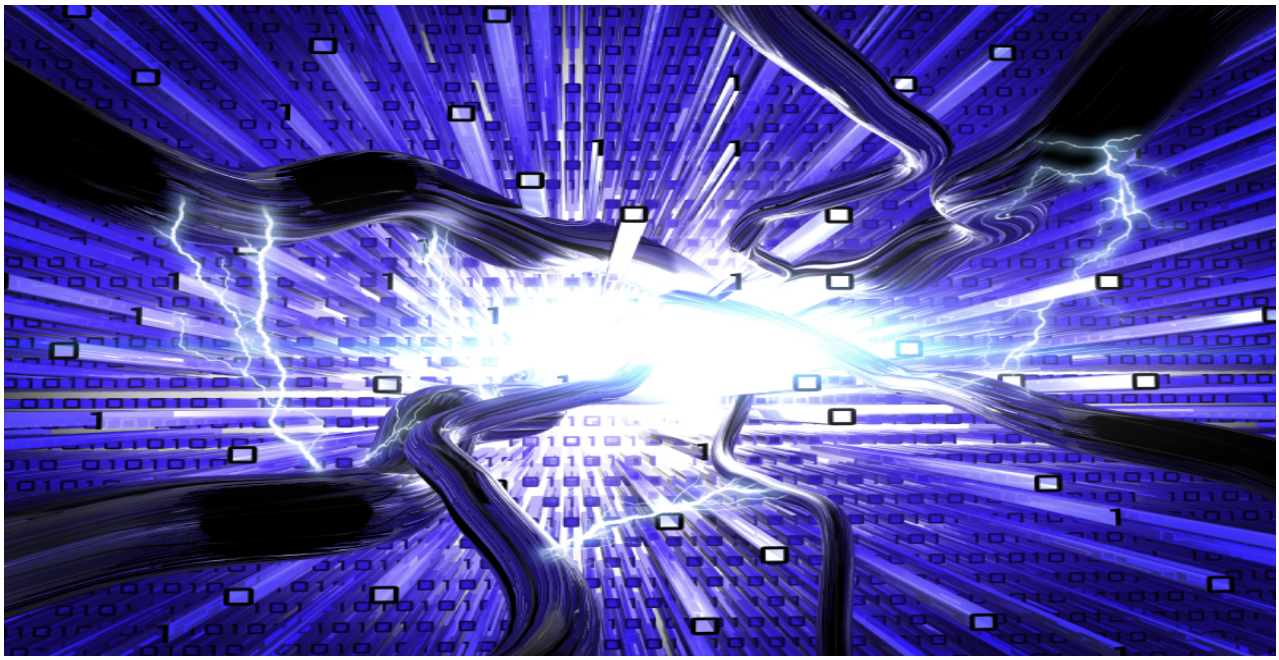


The Cyber Resilient Organization: Learning to Thrive against Threats

Independently conducted by Ponemon Institute LLC

Sponsored by Resilient, an IBM Company

Publication Date: September 2015

The Cyber Resilient Organization: Learning to Thrive against Threats

Ponemon Institute, September 2015

Cy-ber Re-sil-ience *(ˈsībə rəˈzilyəns) n. – The capacity of an enterprise to maintain its core purpose and integrity in the face of cyberattacks.*

Part 1. Introduction

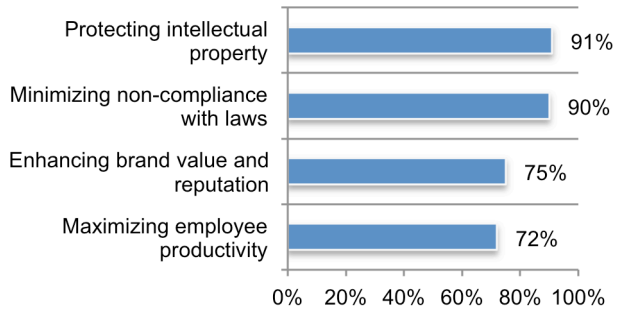
With cyber attacks growing increasingly frequent and complex, cybersecurity strategies are shifting: while prevention is still important, it is more about prevailing. Cyber resilience supports businesses efforts to ensure they'll continue to thrive despite the increased likelihood of a data breach.

That's the essence of cyber resilience – aligning prevention, detection, and response capabilities to manage, mitigate, and move on from cyberattacks. But are businesses ready today to face cyber threats head on? To find out, Ponemon Institute, with sponsorship from Resilient, an IBM Company, surveyed 623 IT and IT security practitioners about their organizations' approach to becoming resilient to security threats. The findings are presented in the study, *The Cyber Resilient Organization: Learning to Thrive against Threats.*

In the context of this research, we define cyber resilience as the capacity of an enterprise to maintain its core purpose and integrity in the face of cyberattacks. A cyber resilient enterprise is one that can prevent, detect, contain and recover from a plethora of serious threats against data, applications and IT infrastructure. A cyber resilient enterprise successfully aligns continuity management and disaster recovery with security operations in a holistic fashion.

Figure 1 shows why cyber resilience is emerging as the standard for which to strive. The protection of high-value intellectual property and compliance with laws and regulations are best achieved with cyber resilience, according to 91 percent and 90 percent of respondents, respectively.

Figure 1. The importance of cyber resilience to achieving certain business goals
Very important and important responses combined



Cyber resilience also is considered to enhance brand value and reputation (75 percent of respondents) and maximize employee productivity (72 percent of respondents).

Key takeaways include the following:

The state of cyber resilience needs improvement. Only 25 percent of respondents rate their organizations' cyber resilience as high (7+ on a scale of 1 = low resilience to 10 = high resilience) based on the definition described in the introduction. Moreover, a key component of cyber resiliency is the ability to recover from a cyber attack and only 31 percent rate this as high. Prevention is also rated fairly low at 33 percent. The ability to detect and contain cyber attacks is rated much higher by 45 percent and 47 percent of respondents, respectively.

Only 25 percent of respondents rate their organizations' cyber resilience as high based on the definition described in the introduction. Moreover, a key component of cyber resiliency is the ability to recover from a cyber attack and only 32 percent rate this as high. Prevention is also rated fairly low. The ability to detect and contain cyber attacks are rated much higher by 44 percent and 47 percent of respondents, respectively.

Human error is the enemy of cyber resiliency. The IT-related threat believed to have the greatest impact on an organization's ability to be cyber resilient and the most likely to occur is human error. Persistent attacks are considered to have the second greatest impact on cyber resiliency but are less likely to occur.

Planning and preparedness is key to cyber resiliency. It is interesting that a lack of knowledgeable staff or enabling technologies is not as much a hindrance as not devoting the necessary time and resources to planning and preparedness (65 percent of respondents) or insufficient risk awareness, analysis and assessments (55 percent of respondents).

The majority of companies are not prepared to respond to a cyber security incident. Despite the importance of preparedness to cyber resilience**,** 60 percent of respondents either say their organization does not have a cybersecurity incident response plan (CSIRP) (30 percent of respondents) or it is informal or "ad hoc" (30 percent of respondents). Only 17 percent of respondents have a well-defined CSIRP that is applied consistently across the entire enterprise.

A high level of cyber resiliency is difficult to achieve if no one function clearly owns the responsibility. Only 24 percent of respondents say the Chief Information Officer (CIO) is accountable for making their organizations' resilient to cyber threats. This is followed by 20 percent who say it is the business unit leader and 10 percent who say no one person has overall responsibility.

Collaboration among business functions is essential to a high level of cyber resilience but it rarely happens. Only 15 percent of respondents say collaboration is excellent. Almost one-third of respondents (32 percent of respondents) say collaboration is poor or non-existent. Leadership and responsibility are critical to improving collaboration.

Organizational factors hinder efforts to achieve a high level of cyber resilience. The importance of cyber resilience is often not recognized by senior management**.** Only 44 percent of respondents believe their organizations' leaders recognize that enterprise risks affects cyber resilience and 42 percent believe cyber resilience affects brand image. About half (50 percent of respondents) say cyber resilience does affect revenues. Other factors that are a hindrance are insufficient funding and staffing.

Preparedness and agility are most important to achieving a high level of cyber resilience. Respondents were asked to rank those factors considered important to achieving a high level of cyber resilience. Once again preparedness to deal with cyber threats is critical followed by agility and a strong security posture.

Technologies that enable efficient backup and disaster recovery operations are by far most important to building a cyber resilient enterprise. Seventy-seven percent of respondents say technologies that support efficient backup and disaster recovery operations are essential or very important. Also important are technologies that provide advance warning about threats and attackers (59 percent of respondents) and those that provide intelligence about the threat landscape (58 percent of respondents).

Part 2. Key Findings

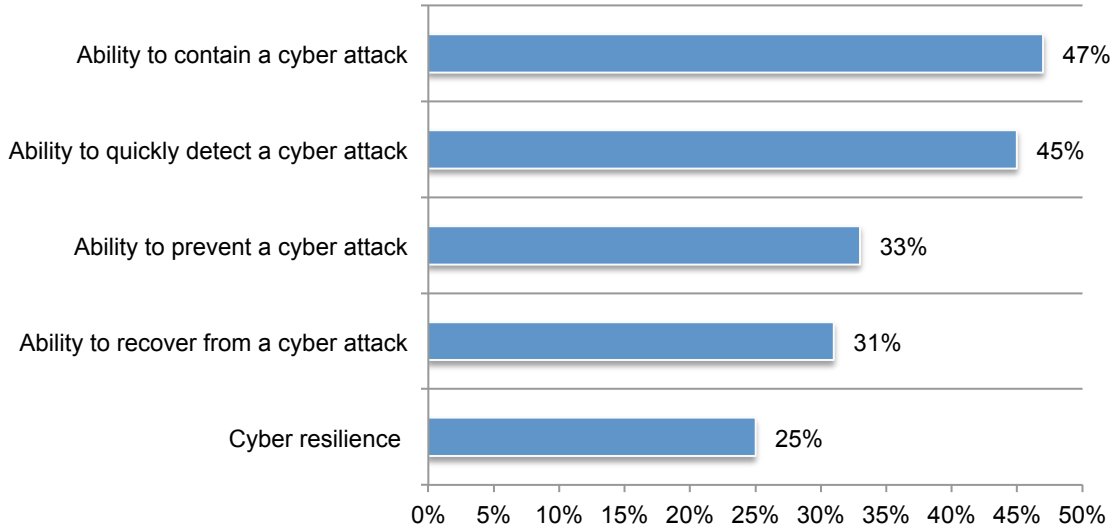
In this section, we provide an analysis of the key findings. The complete audited findings are presented in the appendix of this report. The report is organized according to the following topics:

- The state of cyber resilience today
- Barriers to a cyber resilient enterprise
- Roadmap to cyber resilience

The state of cyber resilience today

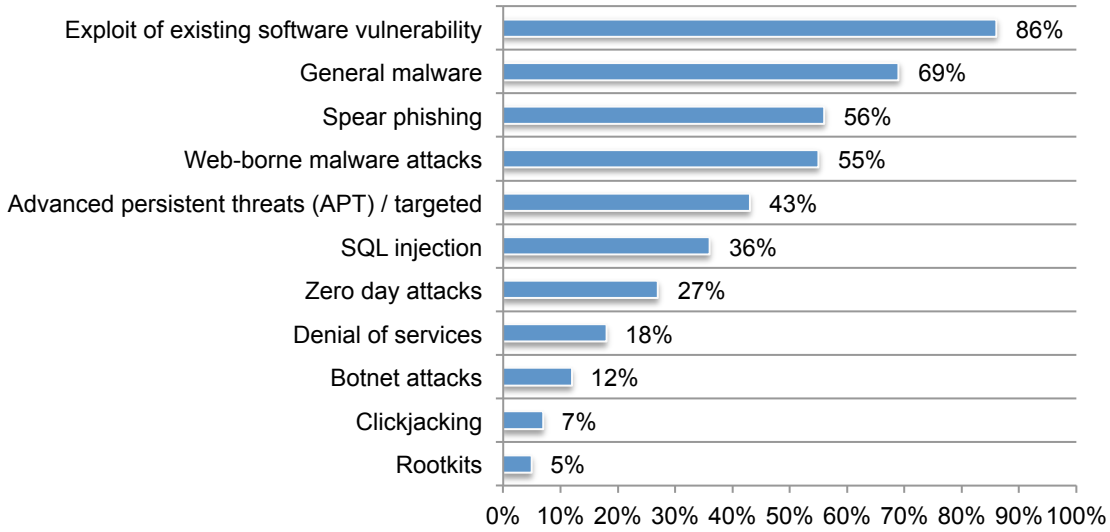
The state of cyber resilience needs improvement. As shown in Figure 2, only 25 percent of respondents rate their organizations' cyber resilience as high (7+ on a scale of 1 = low resilience to 10 = high resilience) based on the definition described in the introduction. Moreover, a key component of cyber resiliency is the ability to recover from a cyber attack and only 31 percent rate this as high. Prevention is also rated fairly low at 33 percent. The ability to detect and contain cyber attacks is rated much higher by 45 percent and 47 percent of respondents, respectively.

Figure 2. How companies rate their resilience to cyber attacks
7 + responses combined from a scale of 1 = low resilience to 10 = high resilience



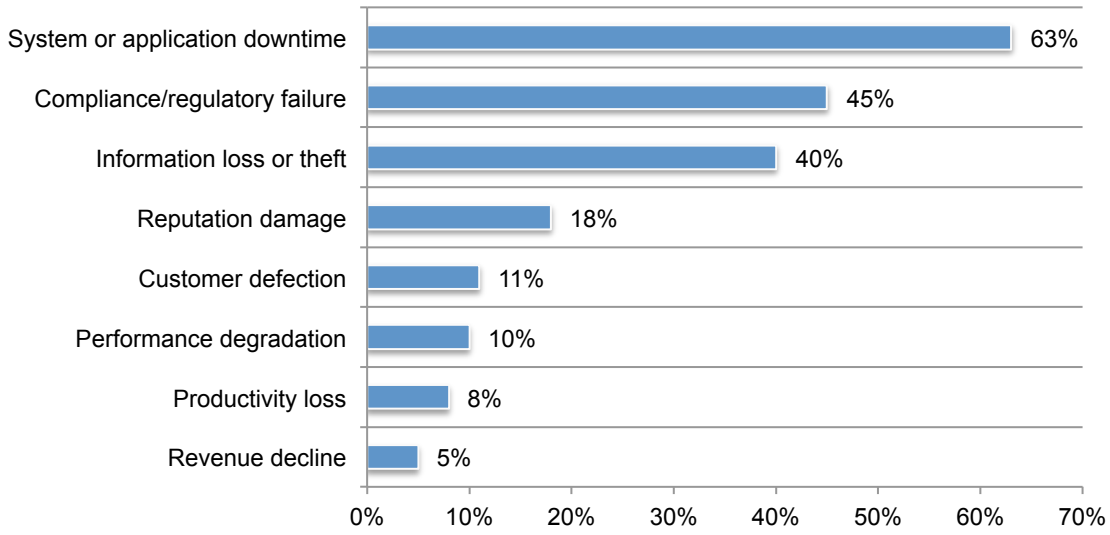
Organizations face a multitude of cyber threats. Figure 3 reveals the types of incidents or compromises in IT networks or endpoints causing the most problems for organizations. By far, respondents say exploits of existing software vulnerabilities (86 percent of respondents) are the most frequent threat. Also frequent are general malware (69 percent of respondents), spear phishing (56 percent of respondents) and web-borne malware attacks (55 percent of respondents).

Figure 3. Types of incidents or compromises most often seen in IT networks or endpoints
More than one response permitted



System or application downtime is most often used to justify the funding of IT security initiatives. According to Figure 4, the reasons that trigger funding for IT security investments is to keep the organizations' systems or applications from going down according to 63 percent of respondents. It is interesting that only 40 percent of respondents say it is the threat of information loss or theft that influences funding.

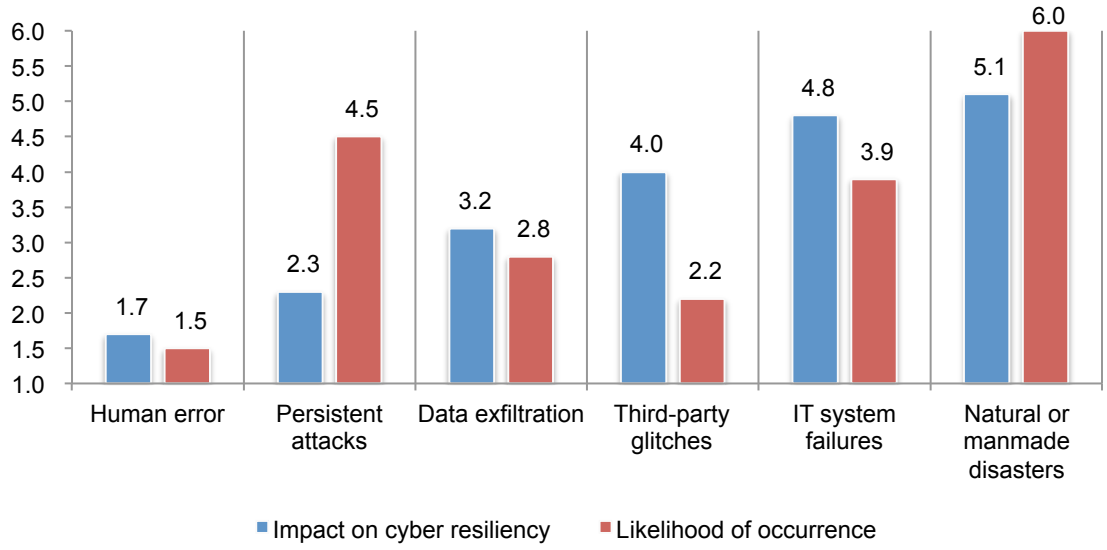
Figure 4. Factors used to justify the funding of IT security
Two responses permitted



Barriers to achieving a cyber resilient enterprise

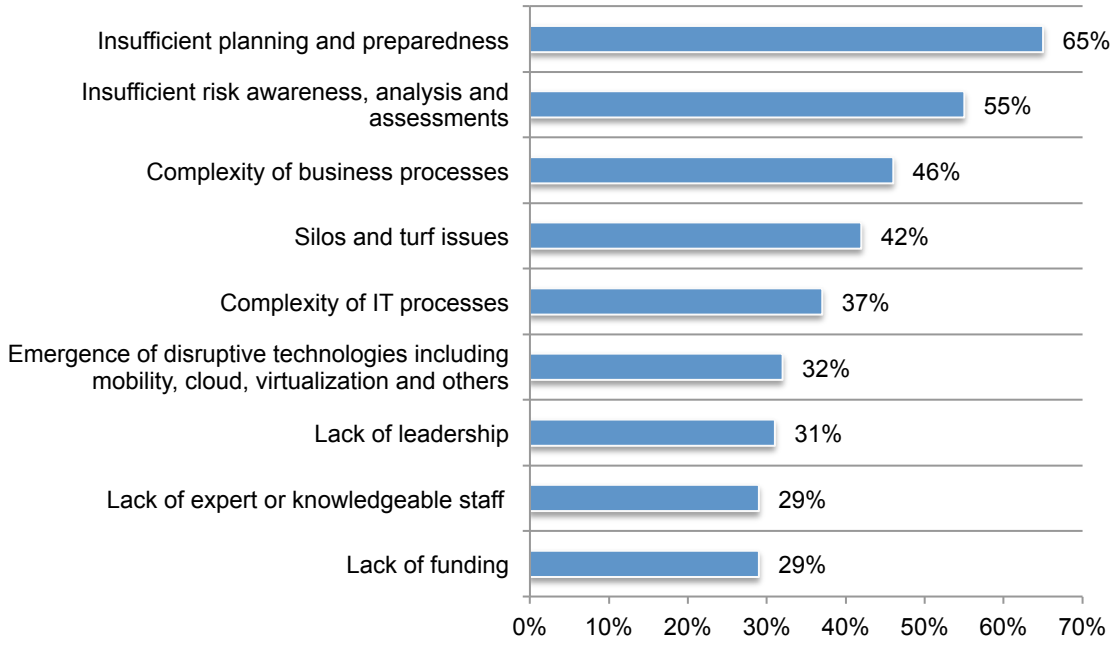
Human error is the enemy of cyber resiliency. As shown in Figure 5, the IT-related threat believed to have the greatest impact on an organization's ability to be cyber resilient and the most likely to occur is human error. Persistent attacks are considered to have the second greatest impact on cyber resiliency but are less likely to occur. Third-party glitches are likely to occur but in contrast are not seen as having the highest impact on cyber resiliency.

Figure 5. IT-related threats impacting cyber resiliency and most likely to occur
1 = Most significant impact to 6 = least significant impact



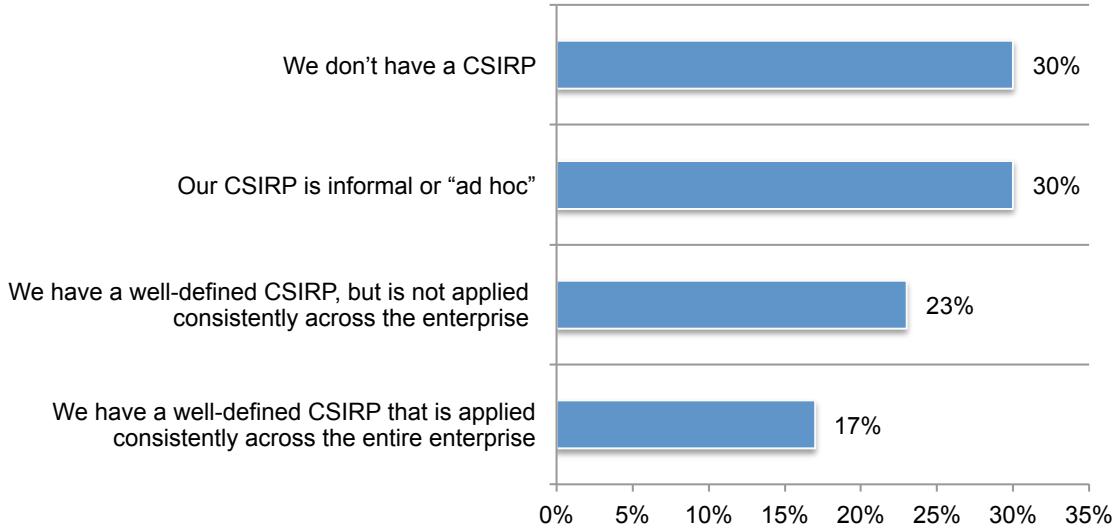
Planning and preparedness is key to cyber resiliency. Figure 6 presents the reasons why organizations struggle to achieve a cyber resilient enterprise. It is interesting that a lack of knowledgeable staff or enabling technologies is not as much a hindrance as not devoting the necessary time and resources to planning and preparedness (65 percent of respondents) or insufficient risk awareness, analysis and assessments (55 percent of respondents).

Figure 6. The most significant barriers to achieving a high level of cyber resilience within your organization
Four responses permitted



The majority of companies are not prepared to respond to a cyber security incident. Only 17 percent of respondents have a well-defined CSIRP that is applied consistently across the entire enterprise. Despite the importance to preparedness to cyber resilience, according to Figure 7, 60 percent of respondents either say their organization does not have a CSIRP (30 percent of respondents) or it is informal or "ad hoc" (30 percent of respondents).

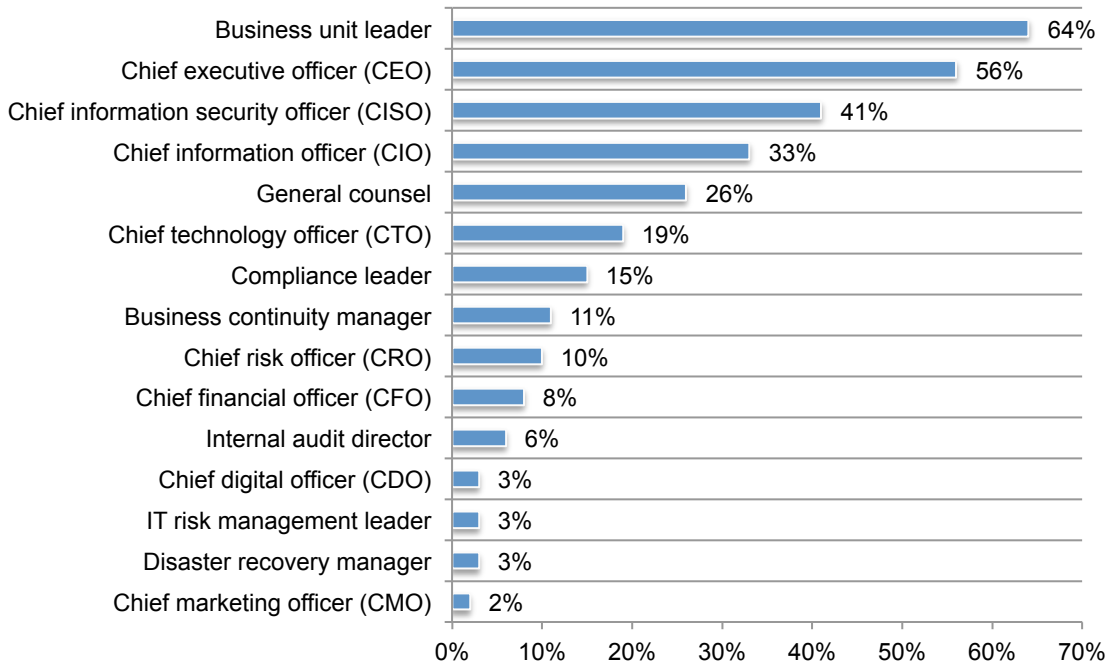
Figure 7. What best describes your organization's cyber security incident response plan?



A high level of cyber resiliency is difficult to achieve if no one function clearly owns the responsibility. Only 24 percent of respondents say the Chief Information Officer (CIO) is accountable for making their organizations' resilient to cyber threats. This is followed by 20 percent who say it is the business unit leader and 10 percent who say no one person has overall responsibility.

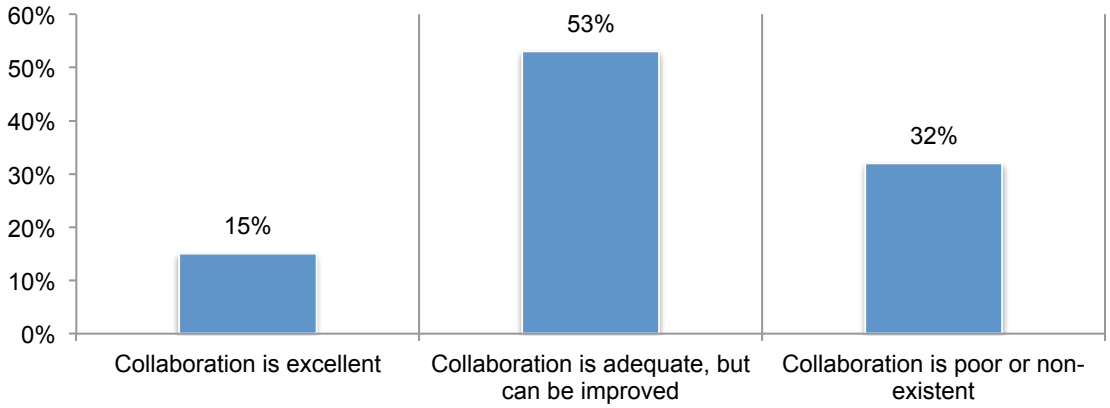
Respondents are more certain about who is influential over their organizations' efforts to ensure a high level of cyber resilience, as shown in Figure 8. Sixty-four percent of respondents say it is the business unit leader, 56 percent say it is the CEO and 41 percent say it is the Chief Information Security Officer (CISO).

Figure 8. Who has influence over your organization's efforts to ensure a high level of cyber resilience?



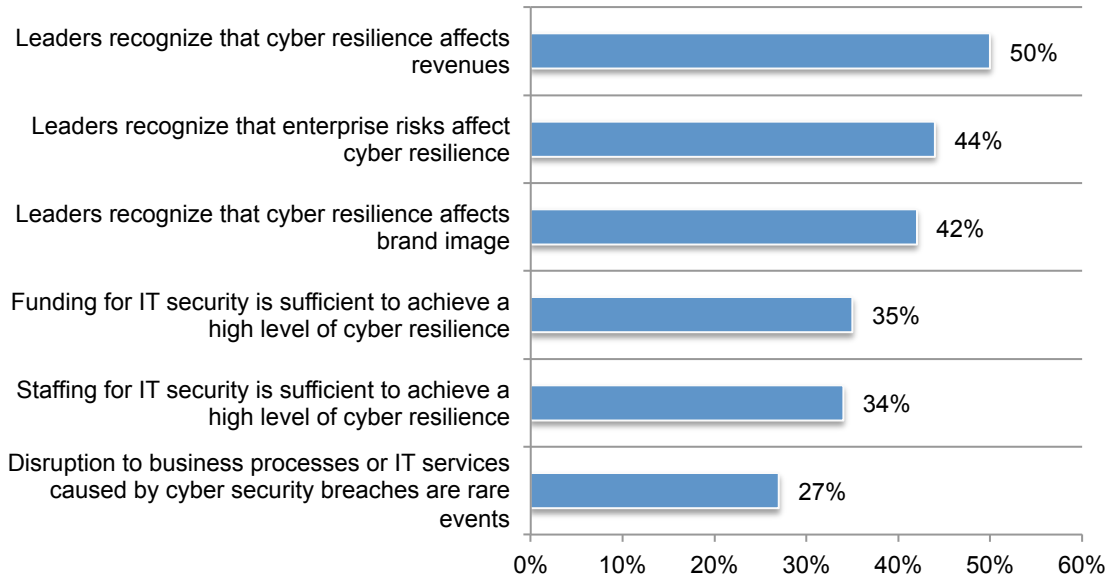
Collaboration among business functions is essential to a high level of cyber resilience but it rarely happens. According to Figure 9, only 15 percent of respondents say collaboration is excellent. Eighty-five percent of respondents say collaboration is only adequate (53 percent of respondents) or poor (32 percent of respondents). Leadership and responsibility are critical to improving collaboration. As discussed above, while there are "influencers," there are few individuals who are being held responsible for ensuring a high level of cyber resilience.

Figure 9. What is the state of collaboration to support a high level of cyber resilience in your organization?



Organizational factors hinder efforts to achieve a high level of cyber resilience. Figure 10 shows the organizational factors that affect cyber resilience. The importance of cyber resilience is often not recognized by senior management**.** Only 44 percent of respondents believe their organizations' leaders recognize that enterprise risks affects cyber resilience and 42 percent believe cyber resilience affects brand image. About half (50 percent of respondents) say cyber resilience does affect revenues. Other factors that are a hindrance are insufficient funding and staffing. On average, respondents say their organizations are allocating 30 percent of the IT security budget annually to achieving cyber resilience, which averages about $5.3 million for the organizations represented in this research.

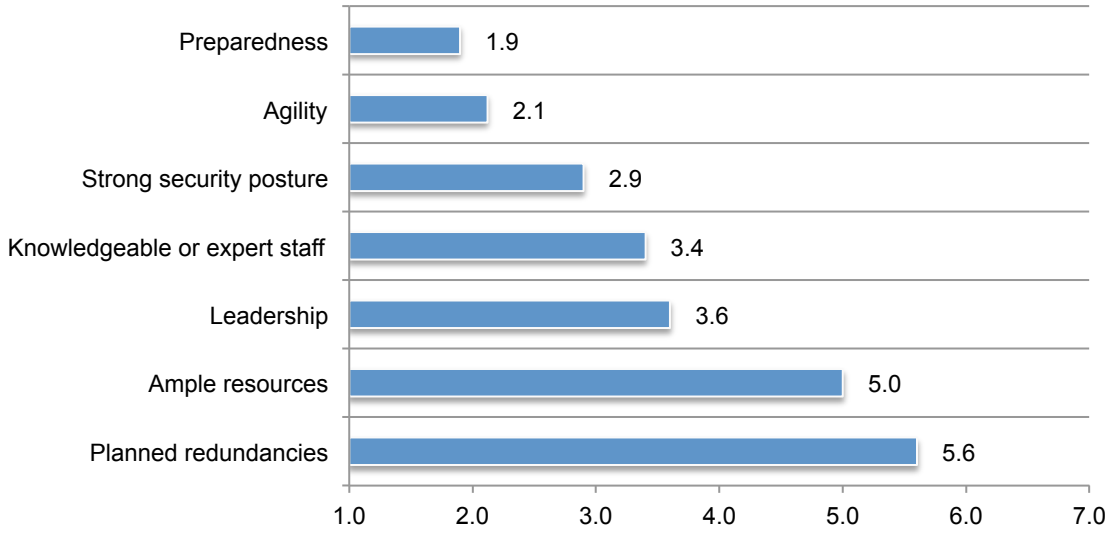
Figure 10. Organizational factors affect cyber resilience
Strongly agree and agree responses combined



Roadmap to cyber resilience

Preparedness and agility are most important to achieving a high level of cyber resilience. Respondents were asked to rank those factors considered important to achieving a high level of cyber resilience. Figure 11 reveals once again preparedness to deal with cyber threats is critical followed by agility and a strong security posture.

Figure 11. Seven factors considered important in achieving a high level of cyber resilience
1 = most important to 7 = least important

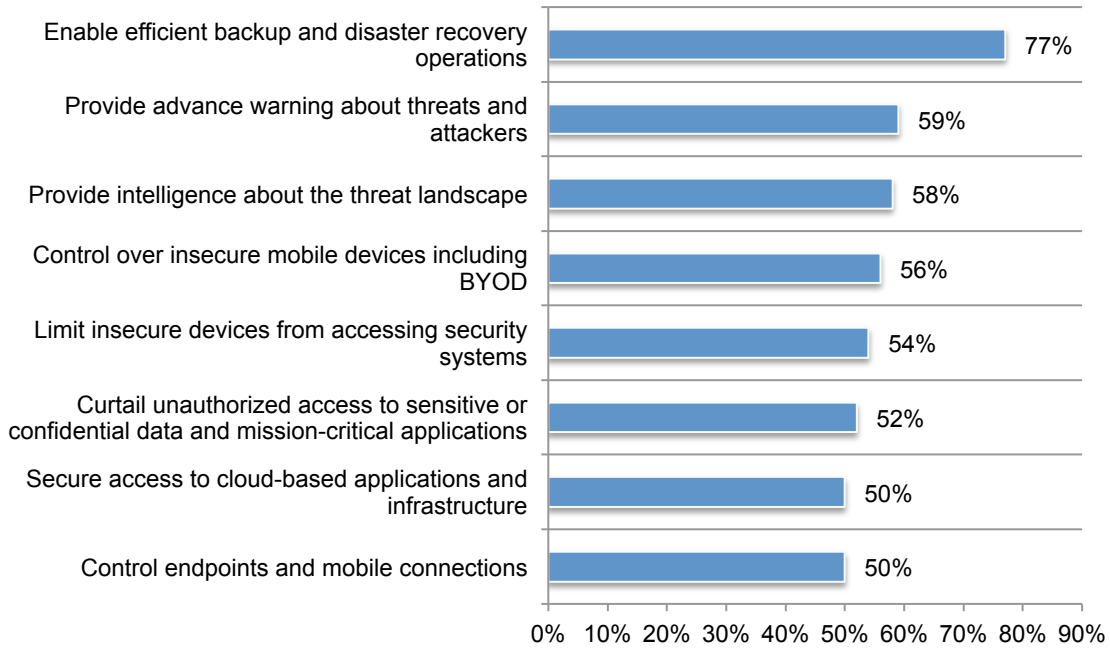


Technologies that enable efficient backup and disaster recovery operations are by far most important to building a cyber resilient enterprise. Seventy-seven percent of respondents, as shown in Figure 12, say technologies that support efficient backup and disaster recovery operations are essential or very important. Also important are technologies that provide advance warning about threats and attackers (59 percent of respondents) and those that provide intelligence about the threat landscape (58 percent of respondents).

Mobile security in the workplace is also a factor contributing to cyber resilience. Fifty-six percent of respondents say technologies that enable control over insecure mobile devices including BYOD are critical as well as those that limit insecure devices from accessing security systems (54 percent of respondents) and 50 percent of respondents believe technologies that control endpoints and mobile connections are important.

Finally, end user control is critical. Fifty-two percent of respondents say technologies that curtail unauthorized access to sensitive or confidential data and mission-critical applications and secure access to cloud-based applications and infrastructure (50 percent of respondents) would support a high level of cyber resilience.

Figure 12. Security enabling technologies important to achieving a high level of cyber resilience
Essential and very important responses combined



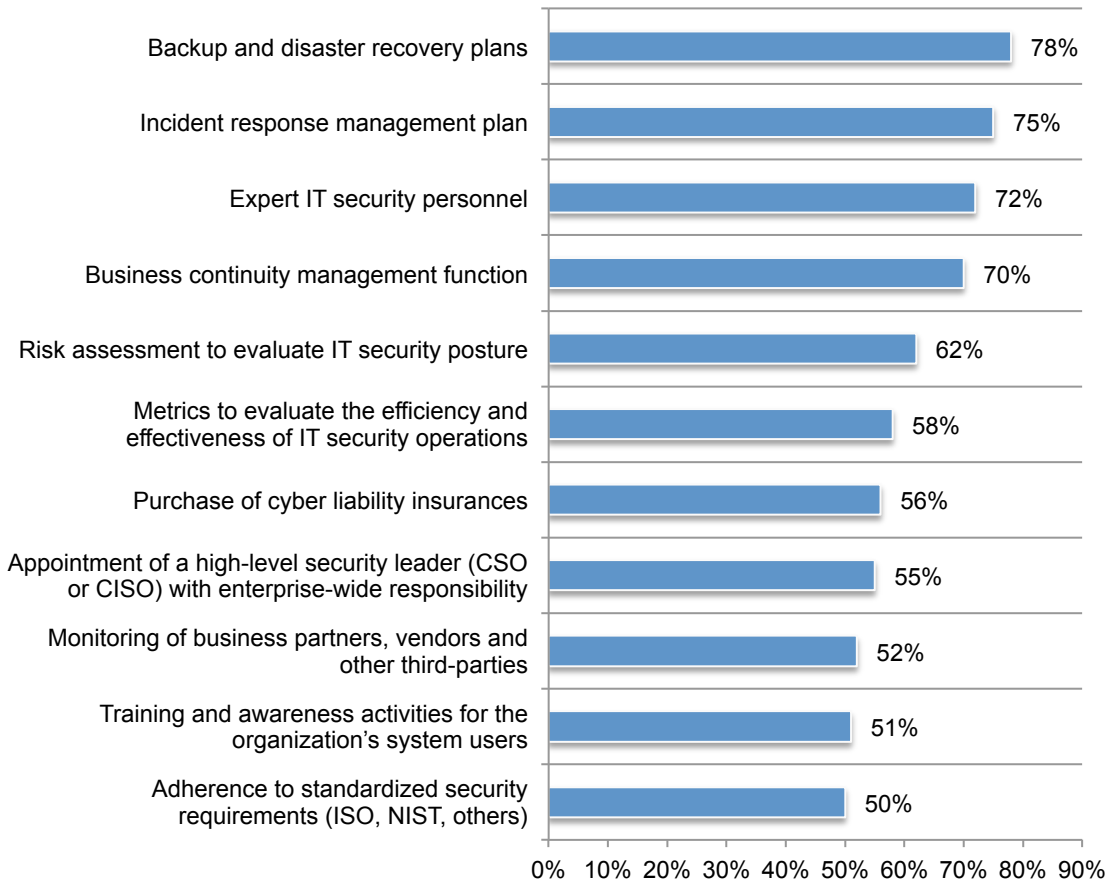
Plans to deal with disasters, security incidents and business continuity are most important to building a cyber resilient enterprise. Consistent with the findings above, the most important governance practice is to have a backup and disaster recover plan in place, according to 78 percent of respondents (Figure 13). Also critical are incident response management plans and a business continuity management plan (75 percent and 70 percent of respondents, respectively). As part of being prepared, 56 percent of respondents say the purchase of cyber liability insurance should be considered.

Expert IT security personnel are critical to cyber resiliency, according to 72 percent of respondents as well as the appointment of a high-level security leader (CISO or CSO), according to 55 percent of respondents.

Understanding risks to the organization should be part of a cyber resilient governance plan. This includes conducting risks assessments to evaluate the organization's IT security posture and monitoring business partners, vendors and other third parties (both 62 percent of respondents). To mitigate the end user risk, 51 percent of respondents say training and awareness activities for system users are essential or very important.

To understand if the organization is on the right path to achieving cyber resilience, metrics to evaluate the efficiency and effectiveness of security operations is key, according to 58 percent of respondents. Important, but less so, is adherence to standardized security requirements such as ISO, NIST and others.

Figure 13. Governance and control practices important to achieving a high level of cyber resilience
Essential and very important responses combined

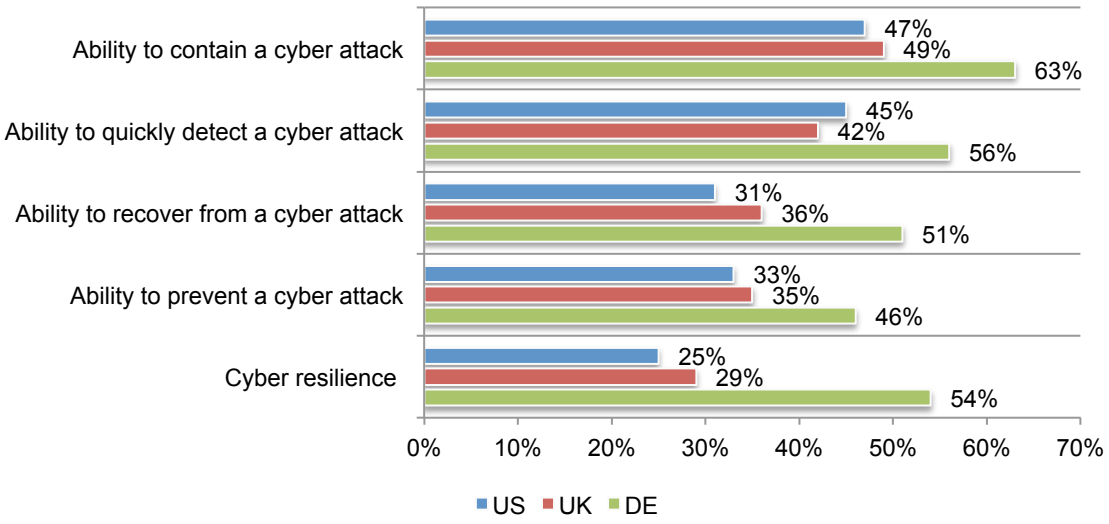


Part 3. Country differences

In this section, we provide the most interesting differences among the countries represented in this research.

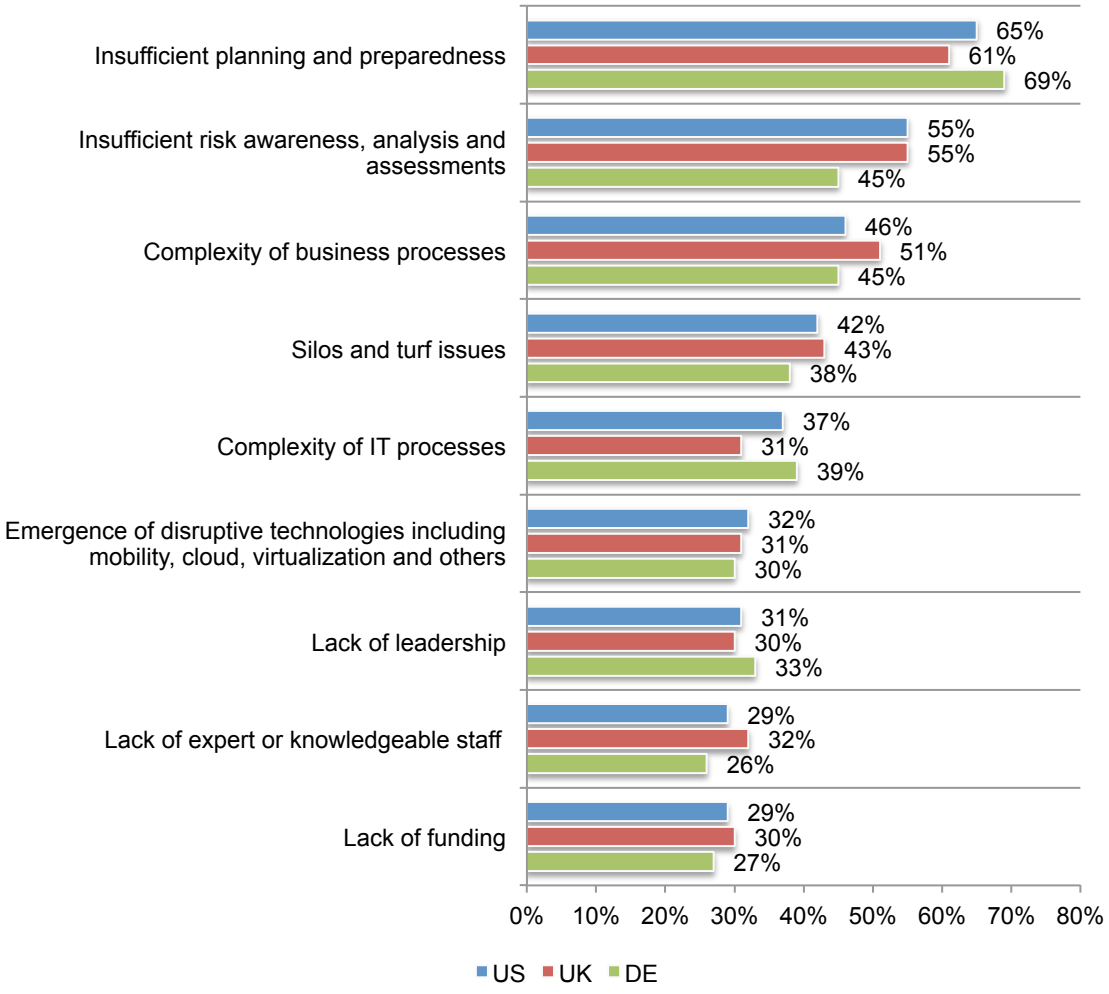
German respondents are more confident in their ability to withstand cyber attacks. As shown in Figure 14, respondents in German organizations are significantly more positive about the state of cyber resilience in their organizations. Fifty-four percent of German respondents rate their organizations' cyber resilience as high. Further, 63 percent of German respondents rate their ability to contain a cyber attack as high. US and UK respondents have similar perceptions about their organizations' resilience to cyber attacks and lag significantly behind German respondents.

Figure 14. How companies rate their resilience to cyber attacks
7 + responses combined from a scale of 1 = low resilience to 10 = high resilience



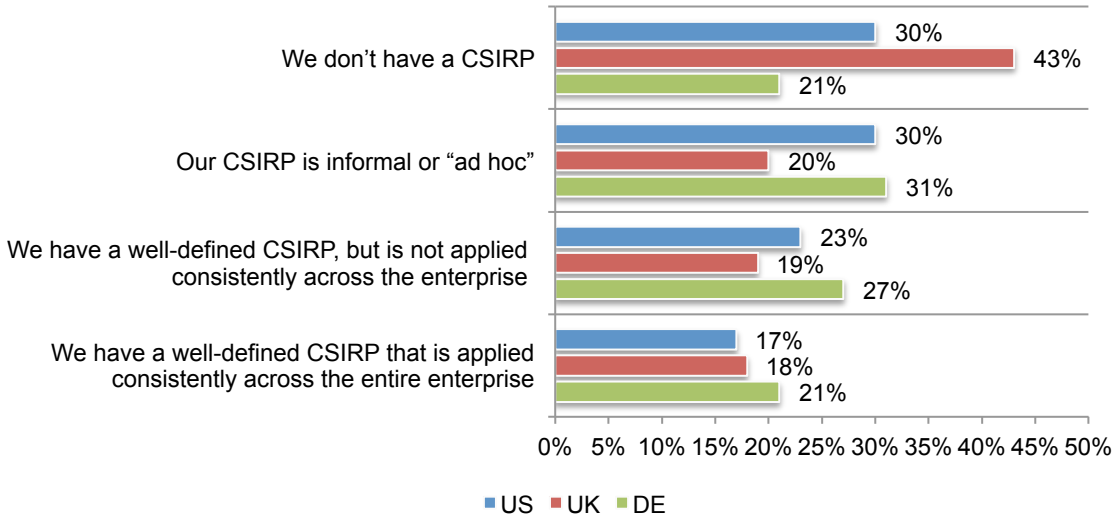
Respondents in all countries rate insufficient planning and preparedness the biggest barriers to cyber resilient. According to Figure 15, the majority of respondents in the US, UK and Germany are most concerned about not having adequate planning and preparedness to create an organization that is resilient to cyber attacks. US and UK respondents are more likely to consider insufficient risk awareness, analysis and assessments as barriers to achieving a high level of cyber resilience.

Figure 15. The most significant barriers to achieving a high level of cyber resilience within your organization
Four responses permitted



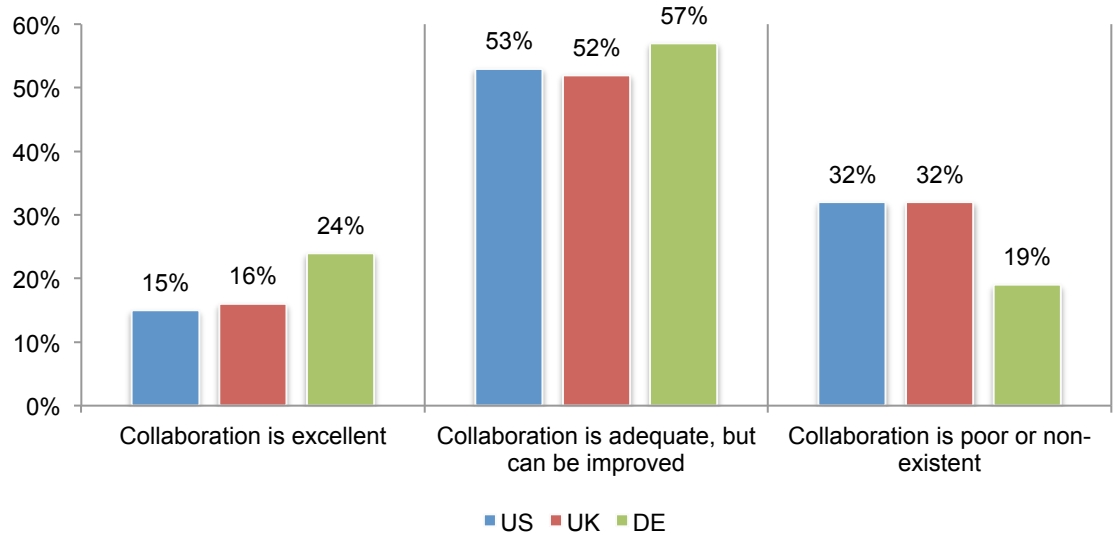
German respondents are more likely to say their organizations have a cyber security incident response plan (CSIRP). Sixty-three percent of UK respondents say their organizations do not have a CSIRP (43 percent) or one that is informal or "ad hoc" (20 percent). In contrast, 48 percent of German respondents say they have a well-defined CSIRP but not applied consistently across the enterprise (27 percent) or they have a well-defined CSIRP applied consistently across the entire enterprise (21 percent).

Figure 16. What best describes your organization's cyber security incident response plan?



German organizations are more likely to have an excellent or adequate state of collaboration to support cyber resilience. Only 19 percent of German respondents say collaboration is poor or non-existent in contrast to 32 percent of US and UK respondents who rate their collaboration as poor.

Figure 17. What is the state of collaboration to support a high level of cyber resilience in your organization?



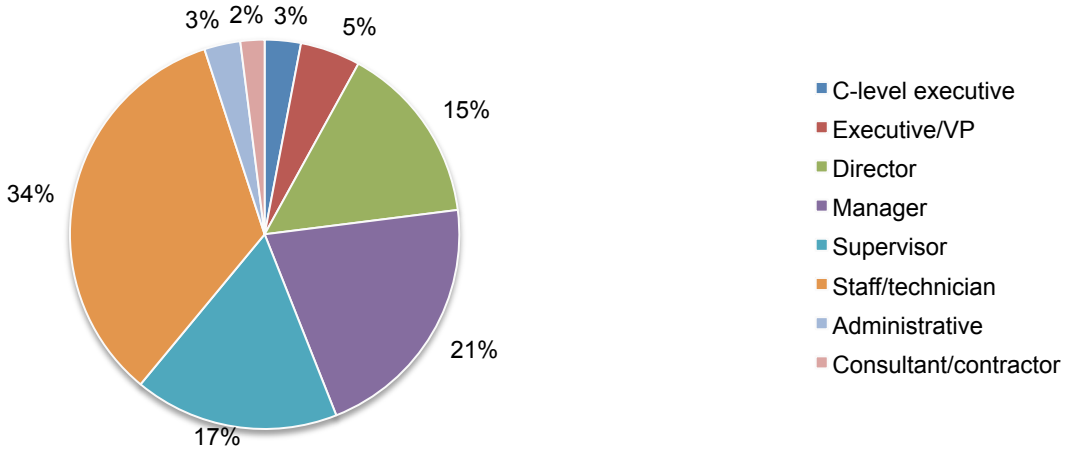
Part 4. Methods

The sampling frame is composed of 18,823 IT and IT security practitioners located in the United States. As shown in Table 1, 718 respondents completed the survey. Screening removed 95 surveys. The final sample was 623 surveys (or a 3.3 percent response rate).

Table 1. Sample response	Freq
Total sampling frame	18,823
Total returns	718
Rejected or screened surveys	95
Final sample	623
Response rate	3.3%

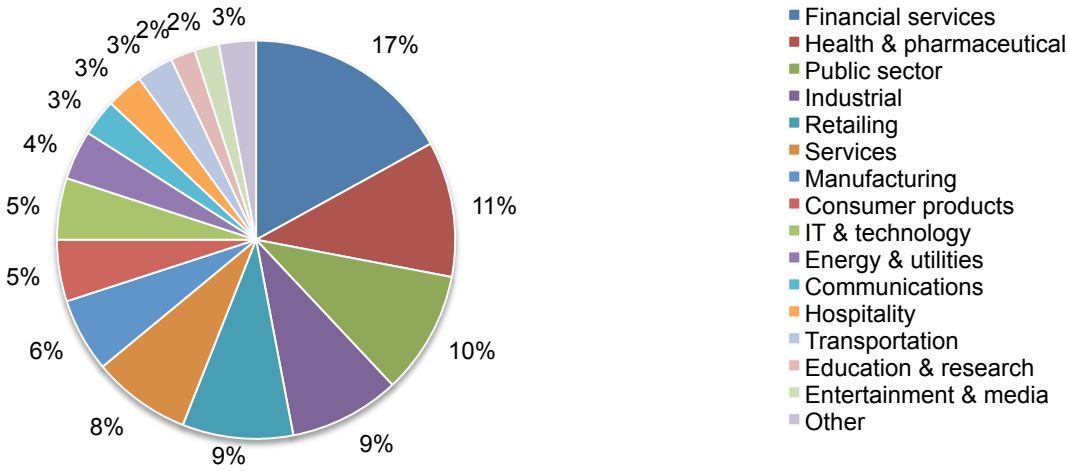
Pie Chart 1 summarizes the approximate position levels of respondents in our study. As can be seen, the majority of respondents (61 percent) are at or above the supervisory level.

Pie Chart 1. Distribution of respondents according to position level



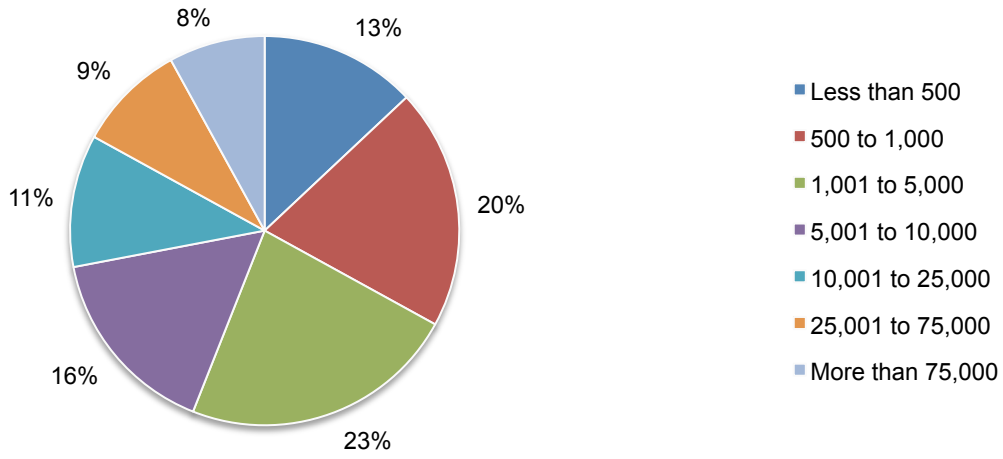
Pie Chart 2 reports the primary industry sector of respondents' organizations. This chart identifies financial services (17 percent) as the largest segment, followed by health & pharmaceuticals (11 percent) and public sector (10 percent).

Pie Chart 2. Primary industry classification



According to Pie Chart 4, the majority of respondents (67 percent) are from organizations with a global headcount of 1,000 or more employees.

Pie Chart 4. Worldwide headcount of the organization



Part 5. Caveats

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

Sampling frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or IT security practitioners located in the United States. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by compensating subjects to complete this research within a specified time period.

Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured in May 2015.

Survey response	Freq.
Total sampling frame	18,823
Total returns	718
Rejected or screened surveys	95
Final sample	623
Response rate	3.31%

Part 1. Screening

S1. What best describes your organizational role or area of focus?	Pct%
IT security operations	33%
IT operations	41%
CSIRT team	18%
Business continuity management	8%
None of the above (stop)	0%
Total	100%

S2. Please check all the activities that you see as part of your job or role.	Pct%
Managing budgets	51%
Managing staff	56%
Evaluating vendors	47%
Setting priorities	34%
Securing systems	63%
Ensuring compliance	50%
Ensuring system availability	39%
None of the above (stop)	0%
Total	340%

Part 2. Background Questions

Q1. Using the following 10-point scale, please rate your organization's cyber resilience from 1 = low resilience to 10 = high resilience.	Pct%
1 or 2	12%
3 or 4	22%
5 or 6	41%
7 or 8	17%
9 or 10	8%
Total	100%
Extrapolated value	5.24

Q2. Using the following 10-point scale, please rate your organization's ability to prevent a cyber attack from 1 = low to 10 = high.	Pct%
1 or 2	12%
3 or 4	18%
5 or 6	37%
7 or 8	21%
9 or 10	12%
Total	100%
Extrapolated value	5.56

Q3. Using the following 10-point scale, please rate your organization's ability to quickly detect a cyber attack from 1 = low to 10 = high.	Pct%
1 or 2	10%
3 or 4	15%
5 or 6	30%
7 or 8	23%
9 or 10	22%
Total	100%
Extrapolated value	6.14

Q4. Using the following 10-point scale, please rate your organization's ability to contain a cyber attack from 1 = low to 10 = high.	Pct%
1 or 2	6%
3 or 4	19%
5 or 6	28%
7 or 8	27%
9 or 10	20%
Total	100%
Extrapolated value	6.22

Q5. Using the following 10-point scale, please rate your organization's ability to recover from a cyber attack from 1 = low to 10 = high.	Pct%
1 or 2	9%
3 or 4	25%
5 or 6	35%
7 or 8	27%
9 or 10	4%
Total	100%
Extrapolated value	5.34

Q6. What best describes the maturity level of your organization's cyber security program or activities today?	Pct%
Early stage – most program activities have not as yet been deployed	9%
Middle stage – most program activities are only partially deployed	31%
Late-middle stage – most program activities are fully deployed	35%
Mature stage – all program activities are fully deployed	25%
Total	100%

Q7. Following are 7 factors considered important in achieving a high level of cyber resilience. Please rank order each factor from 1 = most important to 7 = least important.	Average rank
Agility	2.1
Preparedness	1.9
Planned redundancies	5.6
Strong security posture	2.9
Knowledgeable or expert staff	3.4
Ample resources	5.0
Leadership	3.6

Q8a. Following are 6 common IT-related threats that may impact the cyber resilience within your organization. Please rank order the following threats in terms of their impact on your organization's cyber resiliency. 1 = Most significant impact to 6 = least significant impact.	Average rank
Persistent attacks	2.3
IT system failures	4.8
Data exfiltration	3.2
Human error	1.7
Natural or manmade disasters	5.1
Third-party glitches	4.0

Q8b. Please rank order the following six common IT-related threats in terms their likelihood of occurrence in your organization. 1 = Most likely to 6 = least likely.	Average rank
Persistent attacks	4.5
IT system failures	3.9
Data exfiltration	2.8
Human error	1.5
Natural or manmade disasters	6.0
Third-party glitches	2.2

Q9. Which of these types of incidents or compromises are you seeing frequently in your organization's IT networks or endpoints? Please check all that apply.	Pct%
Advanced persistent threats (APT) / targeted attacks	43%
Botnet attacks	12%
Clickjacking	7%
Denial of services	18%
Exploit of existing software vulnerability	86%
General malware	69%
Rootkits	5%
Spear phishing	56%
SQL injection	36%
Web-borne malware attacks	55%
Zero day attacks	27%
Total	414%

Part 3. Attributions

Please express your opinion about each one of the following statements using the five-point scale below each item.	
Q10a. My organization's leaders recognize that enterprise risks affect cyber resilience.	Pct%
Strongly agree	21%
Agree	23%
Unsure	27%
Disagree	15%
Strongly disagree	14%
Total	100%

Q10b. My organization's leaders recognize that cyber resilience affects revenues.	Pct%
Strongly agree	24%
Agree	26%
Unsure	26%
Disagree	13%
Strongly disagree	11%
Total	100%

Q10c. My organization's leaders recognize that cyber resilience affects brand image.	Pct%
Strongly agree	18%
Agree	24%
Unsure	30%
Disagree	18%
Strongly disagree	10%
Total	100%

Q10d. In my organization, funding for IT security is sufficient to achieve a high level of cyber resilience	Pct%
Strongly agree	16%
Agree	19%
Unsure	27%
Disagree	25%
Strongly disagree	13%
Total	100%

Q10e. In my organization, staffing for IT security is sufficient to achieve a high level of cyber resilience	Pct%
Strongly agree	15%
Agree	19%
Unsure	28%
Disagree	26%
Strongly disagree	12%
Total	100%

Q10f. In my organization, disruption to business processes or IT services caused by cyber security breaches are rare events.	Pct%
Strongly agree	12%
Agree	15%
Unsure	19%
Disagree	33%
Strongly disagree	21%
Total	100%

Part 4. Cyber Resilience

Q11. What factors justify the funding of your organization's IT security? Please select your top two choices.	Pct%
System or application downtime	63%
Information loss or theft	40%
Performance degradation	10%
Productivity loss	8%
Revenue decline	5%
Reputation damage	18%
Customer defection	11%
Compliance/regulatory failure	45%
Other (please specify)	0%
Total	200%

Q12. The following table contains 8 common business objectives critical to the success for most companies. Using the adjacent three-point scale, please rate the importance of cyber resilience for achieving each stated objective.	
Q12a. Minimizing customer defection	Pct%
Very important	11%
Important	38%
Not important	51%
Total	100%

Q12b. Maximizing customer acquisition	Pct%
Very important	9%
Important	35%
Not important	56%
Total	100%

Q12c. Minimizing non-compliance with laws	Pct%
Very important	51%
Important	39%
Not important	10%
Total	100%

Q12d. Maximizing employee productivity	Pct%
Very important	19%
Important	53%
Not important	28%
Total	100%

Q12e. Increasing revenues and positive cash flow	Pct%
Very important	14%
Important	35%
Not important	51%
Total	100%

Q12f. Expanding into new global markets	Pct%
Very important	9%
Important	28%
Not important	63%
Total	100%

Q12e. Protecting intellectual property	Pct%
Very important	70%
Important	21%
Not important	9%
Total	100%

Q12f. Enhancing brand value and reputation	Pct%
Very important	32%
Important	43%
Not important	25%
Total	100%

Q13a. Who has overall responsibility or 'owns" your organization's efforts to ensure a high level of cyber resilience? Please check only one top choice.	Pct%
Business continuity manager	5%
Disaster recovery manager	2%
IT risk management leader	6%
Business unit leader	20%
Chief executive officer (CEO)	8%
Chief financial officer (CFO)	0%
Chief information officer (CIO)	24%
Chief technology officer (CTO)	5%
Chief marketing officer (CMO)	0%
Chief risk officer (CRO)	3%
Chief information security officer (CISO)	9%
Chief digital officer (CDO)	0%
Compliance leader	5%
Internal audit director	1%
General counsel	2%
No one person has overall responsibility	10%
Other (please specify)	0%
Total	100%

Q13b. Who has "influence" over your organization's efforts to ensure a high level of cyber resilience? Please check three top choices.	Pct%
Business continuity manager	11%
Disaster recovery manager	3%
IT risk management leader	3%
Business unit leader	64%
Chief executive officer (CEO)	56%
Chief financial officer (CFO)	8%
Chief information officer (CIO)	33%
Chief technology officer (CTO)	19%
Chief marketing officer (CMO)	2%
Chief risk officer (CRO)	10%
Chief information security officer (CISO)	41%
Chief digital officer (CDO)	3%
Compliance leader	15%
Internal audit director	6%
General counsel	26%
Other (please specify)	0%
Total	300%

Q14. What one statement best describes how various functions within your organization work together to support a high level of cyber resilience?	Pct%
Collaboration is excellent	15%
Collaboration is adequate, but can be improved	53%
Collaboration is poor or non-existent	32%
Total	100%

Q15. Please check one statement that best describes your organization's cyber security incident response plan (CSIRP).	Pct%
We have a well-defined CSIRP that is applied consistently across the entire enterprise	17%
We have a well-defined CSIRP, but is not applied consistently across the enterprise	23%
Our CSIRP is informal or "ad hoc"	30%
We don't have a CSIRP	30%
Total	100%

Q16. What do you see as the most significant barriers to achieving a high level of cyber resilience within your organization? Please provide four top choices.	Pct%
Lack of funding	29%
Lack of leadership	31%
Lack of expert or knowledgeable staff	29%
Lack of enabling technologies	25%
Silos and turf issues	42%
Insufficient planning and preparedness	65%
Insufficient risk awareness, analysis and assessments	55%
Complexity of business processes	46%
Complexity of IT processes	37%
Interconnected business and IT processes with partners, vendors and other third parties	9%
Emergence of disruptive technologies including mobility, cloud, virtualization and others	32%
Other (please specify)	0%
Total	400%

Part 5. Security Enabling Technologies

Q17. Following are cyber security technology features considered important by many organizations. What is the relative importance of each feature for achieving a high level of cyber resilience? Please use the five-point scale provided below each item.	
Q17a. Pinpoints anomalies in network traffic	Pct%
Essential	11%
Very important	21%
Important	34%
Not important	18%
Irrelevant	16%
Total	100%

Q17b. Provide advance warning about threats and attackers	Pct%
Essential	23%
Very important	36%
Important	24%
Not important	12%
Irrelevant	5%
Total	100%

Q17c. Enable adaptive perimeter controls	Pct%
Essential	6%
Very important	17%
Important	35%
Not important	27%
Irrelevant	15%
Total	100%

Q17d. Provide intelligence about the threat landscape	Pct%
Essential	19%
Very important	39%
Important	23%
Not important	12%
Irrelevant	7%
Total	100%

Q17e. Enable efficient patch management	Pct%
Essential	16%
Very important	29%
Important	41%
Not important	12%
Irrelevant	2%
Total	100%

Q17f. Capture information about attackers (honey pot/hack back)	Pct%
Essential	16%
Very important	29%
Important	41%
Not important	12%
Irrelevant	2%
Total	100%

Q17g. Prioritize threats, vulnerabilities and attacks	Pct%
Essential	16%
Very important	30%
Important	38%
Not important	13%
Irrelevant	3%
Total	100%

Q17h. Control over insecure mobile devices including BYOD	Pct%
Essential	24%
Very important	32%
Important	30%
Not important	11%
Irrelevant	3%
Total	100%

Q17i. Limit insecure devices from accessing security systems	Pct%
Essential	25%
Very important	29%
Important	34%
Not important	6%
Irrelevant	6%
Total	100%

Q17j. Effort to reduce footprint of sensitive or confidential data	Pct%
Essential	9%
Very important	27%
Important	44%
Not important	12%
Irrelevant	8%
Total	100%

Q17k. Curtail unauthorized sharing of sensitive or confidential data	Pct%
Essential	10%
Very important	27%
Important	41%
Not important	15%
Irrelevant	7%
Total	100%

Q17l. Curtail unauthorized access to sensitive or confidential data and mission-critical applications	Pct%
Essential	20%
Very important	32%
Important	32%
Not important	10%
Irrelevant	6%
Total	100%

Q17m. Curtail end-user access to insecure Internet sites and web applications	Pct%
Essential	16%
Very important	28%
Important	32%
Not important	14%
Irrelevant	10%
Total	100%

Q17n. Control endpoints and mobile connections	Pct%
Essential	23%
Very important	27%
Important	33%
Not important	11%
Irrelevant	6%
Total	100%

Q17o. Limit the loss or theft of portable data-bearing devices such as laptops, smartphones and others	Pct%
Essential	11%
Very important	25%
Important	35%
Not important	16%
Irrelevant	13%
Total	100%

Q17p. Enable efficient backup and disaster recovery operations	Pct%
Essential	39%
Very important	38%
Important	9%
Not important	9%
Irrelevant	5%
Total	100%

Q17q. Establish metrics for upstream reporting	Pct%
Essential	11%
Very important	19%
Important	50%
Not important	12%
Irrelevant	8%
Total	100%

Q17r. Conduct surveillance of system users	Pct%
Essential	16%
Very important	29%
Important	41%
Not important	12%
Irrelevant	2%
Total	100%

Q17s. Secure access to cloud-based applications and infrastructure	Pct%
Essential	22%
Very important	28%
Important	25%
Not important	18%
Irrelevant	7%
Total	100%

Q17t. Secure data stored in clouds	Pct%
Essential	21%
Very important	28%
Important	26%
Not important	19%
Irrelevant	6%
Total	100%

Part 6. Governance & Controls

Q18. Following are governance and control practices considered important by many organizations. What is the relative importance of each practice to achieving a high level of cyber resilience? Please use the five-point scale provided below each item.	
Q18a. Expert IT security personnel	Pct%
Essential	42%
Very important	30%
Important	21%
Not important	7%
Irrelevant	0%
Total	100%

Q18b. Clearly defined IT security policies	Pct%
Essential	11%
Very important	23%
Important	27%
Not important	22%
Irrelevant	17%
Total	100%

Q18c. Backup and disaster recovery plans	Pct%
Essential	38%
Very important	40%
Important	11%
Not important	8%
Irrelevant	3%
Total	100%

Q18d. Business continuity management function	Pct%
Essential	34%
Very important	36%
Important	12%
Not important	12%
Irrelevant	6%
Total	100%

Q18e. Incident response management plan	Pct%
Essential	43%
Very important	32%
Important	13%
Not important	12%
Irrelevant	0%
Total	100%

Q18f. Background checks of system users	Pct%
Essential	12%
Very important	30%
Important	39%
Not important	13%
Irrelevant	6%
Total	100%

Q18g. Specialized training for IT security personnel	Pct%
Essential	11%
Very important	19%
Important	37%
Not important	19%
Irrelevant	14%
Total	100%

Q18h. Training and awareness activities for the organization's system users	Pct%
Essential	22%
Very important	29%
Important	25%
Not important	17%
Irrelevant	7%
Total	100%

Q18i. Monitoring of business partners, vendors and other third-parties	Pct%
Essential	30%
Very important	32%
Important	22%
Not important	11%
Irrelevant	5%
Total	100%

Q18j. Internal or external audits of security and IT compliance practices	Pct%
Essential	8%
Very important	18%
Important	29%
Not important	29%
Irrelevant	16%
Total	100%

Q18k. Segregation of duties between IT and business functions	Pct%
Essential	5%
Very important	16%
Important	25%
Not important	31%
Irrelevant	23%
Total	100%

Q18l. Risk assessment to evaluate IT security posture	Pct%
Essential	29%
Very important	33%
Important	20%
Not important	15%
Irrelevant	3%
Total	100%

Q18m. Adherence to standardized security requirements (ISO, NIST, others)	Pct%
Essential	18%
Very important	32%
Important	25%
Not important	16%
Irrelevant	9%
Total	100%

Q18n. Appointment of a high-level security leader (CSO or CISO) with enterprise-wide responsibility	Pct%
Essential	21%
Very important	34%
Important	23%
Not important	16%
Irrelevant	6%
Total	100%

Q18o. Appointment of high-level leader (CPO) accountable for information protection and privacy	Pct%
Essential	21%
Very important	24%
Important	31%
Not important	15%
Irrelevant	9%
Total	100%

Q18p. Upstream communication channel from the security leader to the CEO and board of directors	Pct%
Essential	13%
Very important	26%
Important	28%
Not important	24%
Irrelevant	9%
Total	100%

Q18q. Creation of a security program charter approved by executive management	Pct%
Essential	9%
Very important	16%
Important	20%
Not important	39%
Irrelevant	16%
Total	100%

Q18r. Regularly scheduled presentation on the state of security to the board of directors	Pct%
Essential	15%
Very important	30%
Important	26%
Not important	25%
Irrelevant	4%
Total	100%

Q18s. Process for self-reporting compliance violations to appropriate authorities	Pct%
Essential	5%
Very important	15%
Important	23%
Not important	41%
Irrelevant	16%
Total	100%

Q18t. Purchase of cyber liability insurances	Pct%
Essential	20%
Very important	36%
Important	19%
Not important	18%
Irrelevant	7%
Total	100%

Q18u. Metrics to evaluate the efficiency and effectiveness of IT security operations	Pct%
Essential	28%
Very important	30%
Important	18%
Not important	16%
Irrelevant	8%
Total	100%

Part 7. Budget for Cyber Resilience

Q19. Approximately, what is the dollar range that best describes your organization's IT/cyber security budget for 2015?	Pct%
< $1 million	1%
$1 to 5 million	11%
$6 to $10 million	23%
$11 to $15 million	28%
$16 to $20 million	12%
$21 to $25 million	10%
$26 to $50 million	8%
> $50 million	7%
Total	100%
Extrapolated value ($millions)	$13.32

Q20. Approximately, what percentage of the 2015 IT/cyber security budget will go to cyber resilience-related activities?	Pct%
< 2%	2%
2% to 5%	1%
6% to 10%	4%
11% to 20%	16%
21% to 30%	34%
31% to 40%	21%
41% to 50%	14%
51% to 60%	5%
61% to 70%	3%
71% to 80%	0%
81% to 90%	0%
91 to 100%	0%
Total	100%
Extrapolated value (percentage)	30%

Part 8. Organizational and Respondents' Demographics

D1. What best describes your position level within the organization?	Pct%
C-level executive	3%
Executive/VP	5%
Director	15%
Manager	21%
Supervisor	17%
Staff/technician	34%
Administrative	3%
Consultant/contractor	2%
Other (please specify)	0%
Total	100%

D2. What best describes your organization's primary industry classification?	Pct%
Agriculture & food services	1%
Communications	3%
Consumer products	5%
Defense & aerospace	1%
Education & research	2%
Energy & utilities	4%
Entertainment & media	2%
Financial services	17%
Health & pharmaceutical	11%
Hospitality	3%
Industrial	9%
IT & technology	5%
Logistics & distribution	1%
Manufacturing	6%
Public sector	10%
Retailing	9%
Services	8%
Transportation	3%
Other (please specify)	0%
Total	100%

D3. What range best describes the full-time headcount of your global organization?	Pct%
Less than 500	13%
500 to 1,000	20%
1,001 to 5,000	23%
5,001 to 10,000	16%
10,001 to 25,000	11%
25,001 to 75,000	9%
More than 75,000	8%
Total	100%
Extrapolated value (headcount)	14,898

For more information about this study, please contact Ponemon Institute by sending an email to research@ponemon.org or calling us at 1.800.887.3118.

Ponemon Institute

Advancing Responsible Information Management

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

As a member of the **Council of American Survey Research Organizations (CASRO)**, we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.