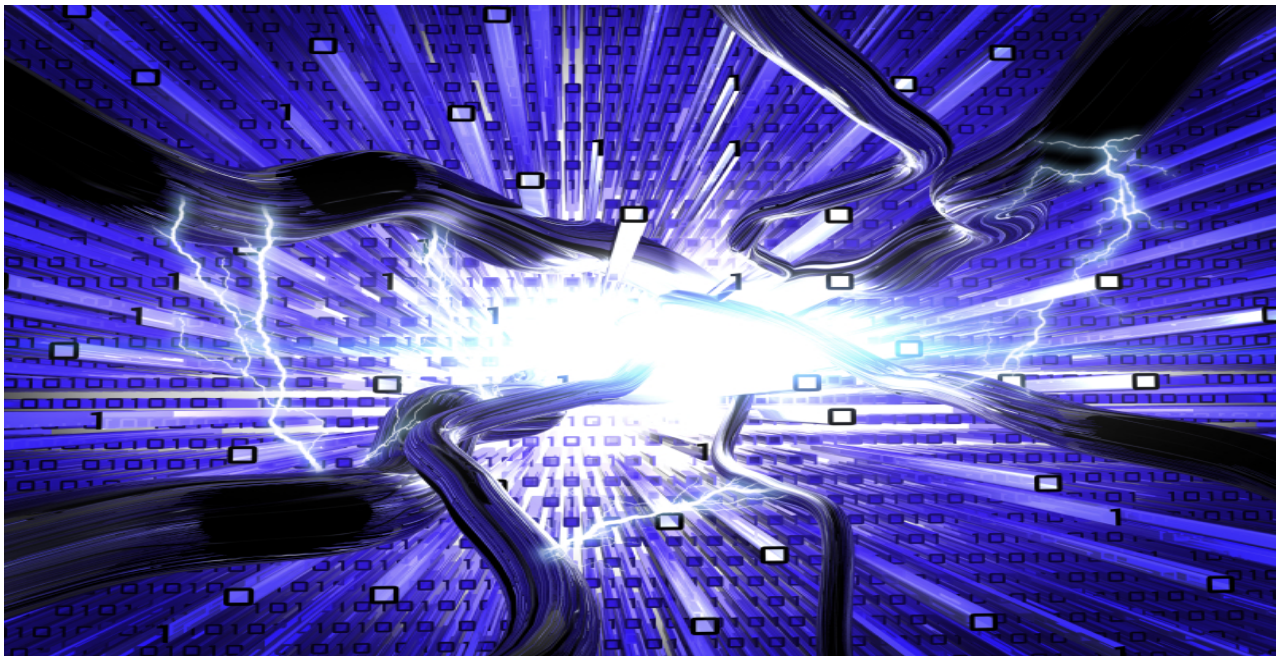


The Cyber Resilient Organisation in the United Kingdom: Learning to Thrive against Threats

Independently conducted by Ponemon Institute LLC

Sponsored by Resilient, an IBM Company

Publication Date: January 2016

The Cyber Resilient Organisation in the United Kingdom: Learning to Thrive against Threats

Ponemon Institute, January 2016

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 450 IT and IT security practitioners in the United Kingdom about their organisations' approach to becoming resilient to security threats. The findings are presented in the study, *The Cyber Resilient Organisation in the United Kingdom: Learning to Thrive against Threats.*

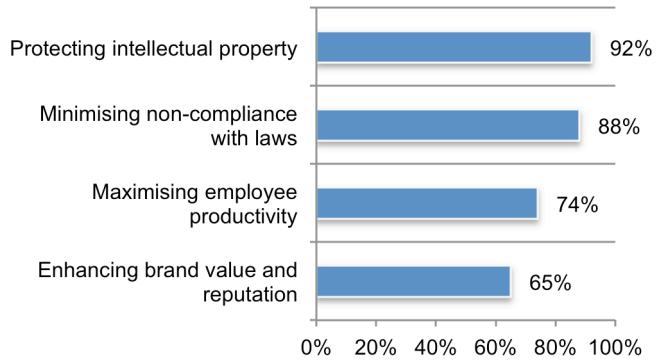
In the context of this research, we define cyber resilience as the capacity of an enterprise to maintain its core purpose and integrity in the face of cyberattacks. A cyber resilient enterprise is one that can prevent, detect, contain and recover from a plethora of serious threats against data, applications 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 92 percent and 88 percent of respondents, respectively.

Cyber resilience also is considered to maximise employee productivity (74 percent of respondents) and enhance brand value and reputation (65 percent of respondents)

Figure 1. The importance of cyber resilience to achieving certain business goals

Very important and important responses combined



Key takeaways include the following:

The state of cyber resilience needs improvement. Only 29 percent of respondents rate their organisations' 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, key components of cyber resiliency are the ability to contain and detect a cyber attack and 49 percent and 42 percent of respondents rate this as high, respectively. Prevention is rated fairly low at 35 percent of respondents.

Organisations face a multitude of cyber threats. By far, respondents say exploits of existing software vulnerabilities (90 percent of respondents) are the most frequent threat. Also frequent are web-borne malware attacks (59 percent of respondents), general malware (55 percent of respondents) and spear phishing (50 percent of respondents).

System or application downtime is most often used to justify the funding of IT security initiatives. The primary reason that triggers funding for IT security investments is to keep the organisations' systems or applications from going down according to 64 percent of respondents. It is interesting that only 36 percent of respondents say it is the threat of information loss or theft that influences funding.

Human error is the enemy of cyber resiliency. The IT-related threat believed to have the greatest impact on an organisation'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.

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 to achieving cyber resiliency as not devoting the necessary time and resources to planning and preparedness (61 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. Only 18 percent of respondents have a well-defined CSIRP that is applied consistently across the entire enterprise. Despite the importance of preparedness to cyber resilience**,** 63 percent of respondents either say their organisation does not have a CSIRP (43 percent of respondents) or it is informal or "ad hoc" (20 percent of respondents).

A high level of cyber resiliency is difficult to achieve if no one function clearly owns the responsibility. Only 19 percent of respondents say the Chief Information Officer (CIO) is accountable for making their organisations resilient to cyber threats. This is followed by 17 percent who say it is the business unit leader and 14 percent who say no one person has overall responsibility. Respondents are more certain about who is influential over their organisations' efforts to ensure a high level of cyber resilience. Fifty-nine percent of respondents say it is the business unit leader, 50 percent say it is the Chief Information Officer (CIO) and 49 percent say it is the CEO.

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.

Organisational factors hinder efforts to achieve a high level of cyber resilience. The importance of cyber resilience is often not recognised by senior management**.** Only 44 percent of respondents believe their organisations' leaders recognise that cyber resilience affects enterprise risks and 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.

A knowledgeable staff and preparedness 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. Expertise and preparedness to deal with cyber threats is critical followed by 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).

Mobile security in the workplace is also a factor contributing to cyber resilience. Fifty-three 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 (55 percent of respondents) and 51 percent of respondents believe technologies that control endpoints and mobile connections are important.

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

Plans to deal with security incidents and disasters are most important to building a cyber resilient enterprise. Consistent with the findings above, the most important governance practice is to have an incidence response plan, according to 76 percent of respondents. Also critical are backup and disaster recovery plans and expert security personnel (75 percent and 69 percent of respondents, respectively). As part of being prepared, 63 percent of respondents say business continuity management is critical as well as the appointment of a high-level security leader (CISO or CSO), according to 56 percent of respondents.

Understanding risks to the organisation should be part of a cyber resilient governance plan. This includes conducting risk assessments to evaluate the organisation's IT security posture (58 percent of respondents) 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 organisation is on the right path to achieving cyber resilience, metrics to evaluate the efficiency and effectiveness of security operations is key, according to 62 percent of respondents. Important, but less so, is adherence to standardised security requirements such as ISO, NIST and others (56 percent of respondents).

Part 2. Key Findings

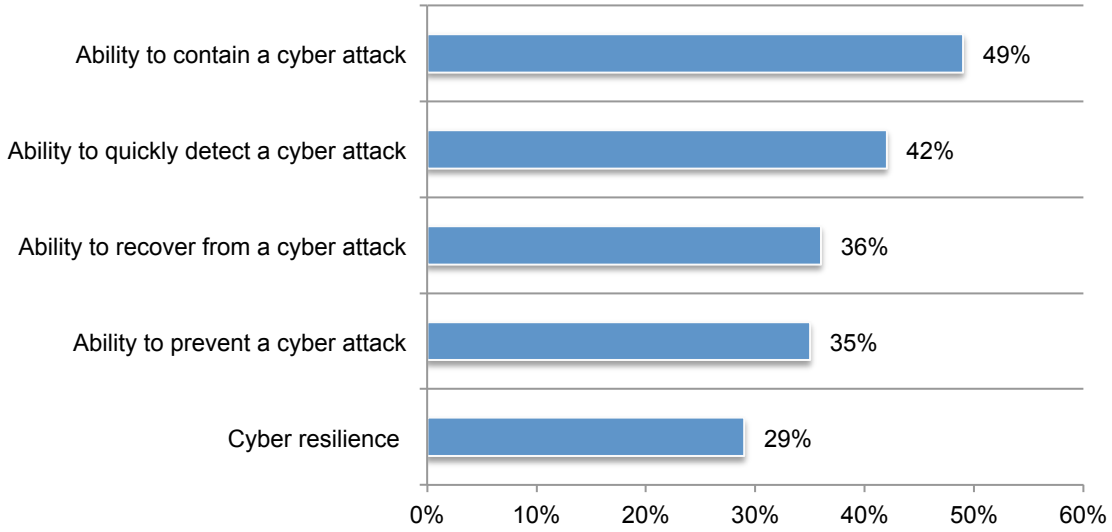
In this section, we provide an analysis of the key findings. The complete audited findings are presented in the appendix of this report. The report is organised according to the following topics:

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

The state of cyber resilience today

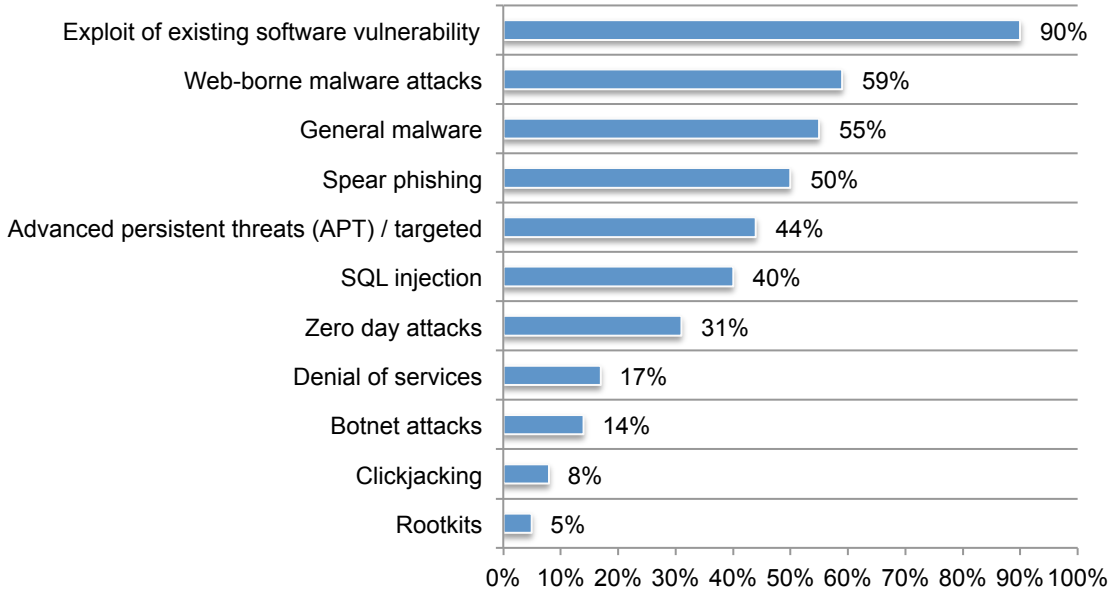
The state of cyber resilience needs improvement. As shown in Figure 2, only 29 percent of respondents rate their organisations' cyber resilience as high (7+ on a scale of 1 = low resilience to 10 = high resilience) based on the definition described in the introduction. Moreover, key components of cyber resiliency are the ability to contain and detect a cyber attack and 49 percent and 42 percent of respondents rate this as high, respectively. Prevention is rated fairly low at 35 percent of respondents.

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



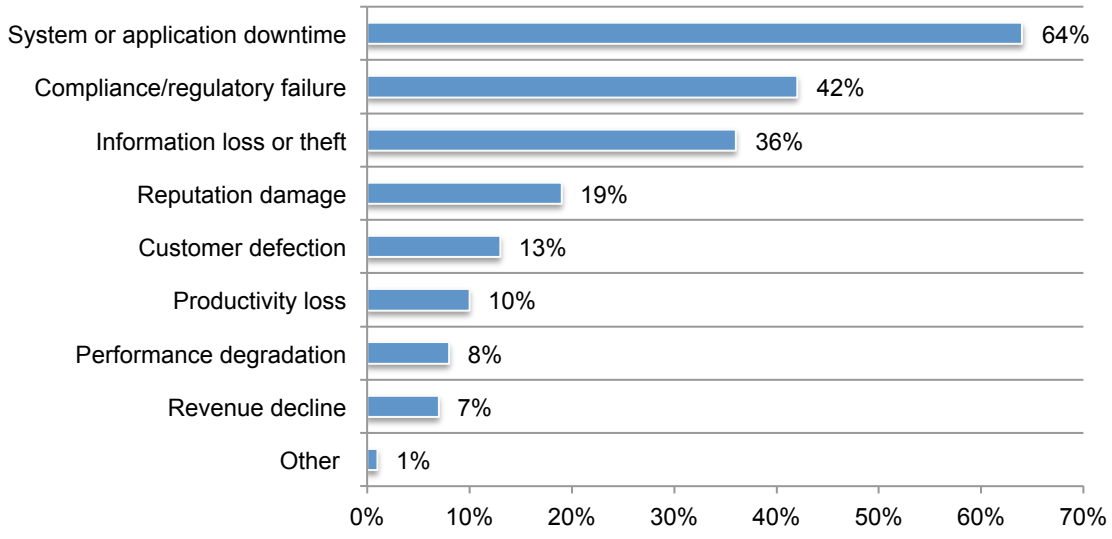
Organisations face a multitude of cyber threats. Figure 3 reveals the types of incidents or compromises in IT networks or endpoints causing the most problems for organisations. By far, respondents say exploits of existing software vulnerabilities (90 percent of respondents) are the most frequent threat. Also frequent are web-borne malware attacks (59 percent of respondents), general malware (55 percent of respondents) and spear phishing (50 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 primary reason that triggers funding for IT security investments is to keep the organisations' systems or applications from going down according to 64 percent of respondents. It is interesting that only 36 percent of respondents say it is the threat of information loss or theft that influences funding.

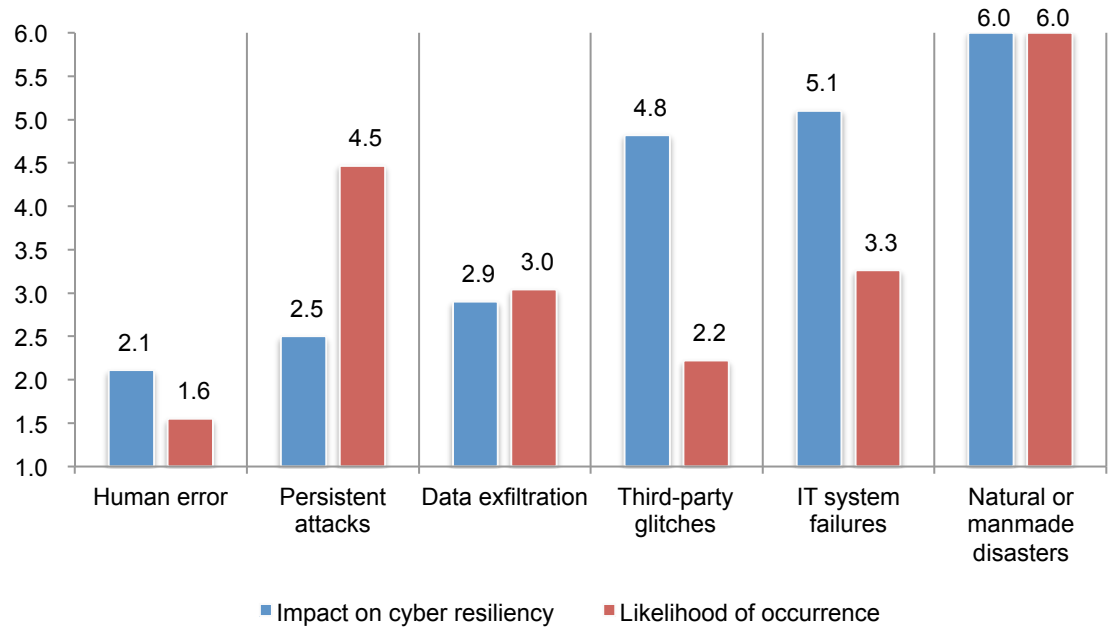
Figure 4. Factors used to justify the funding of IT security
Two responses permitted



Barriers to achieving a cyber resilient enterprise

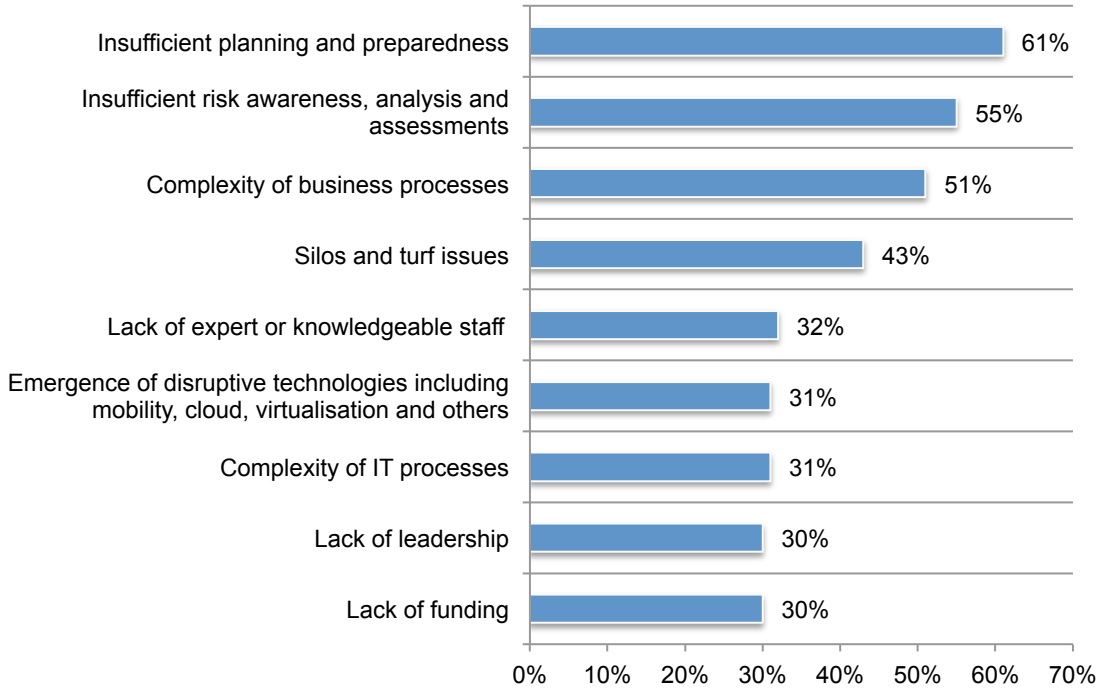
Human error is the enemy of cyber resiliency. As shown in Figure 5, the IT-related threat believed to have the greatest impact on an organisation's ability to be cyber resilient and the most likely to occur is human error. Persistent attacks are considered to have the second greatest impact on cyber 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



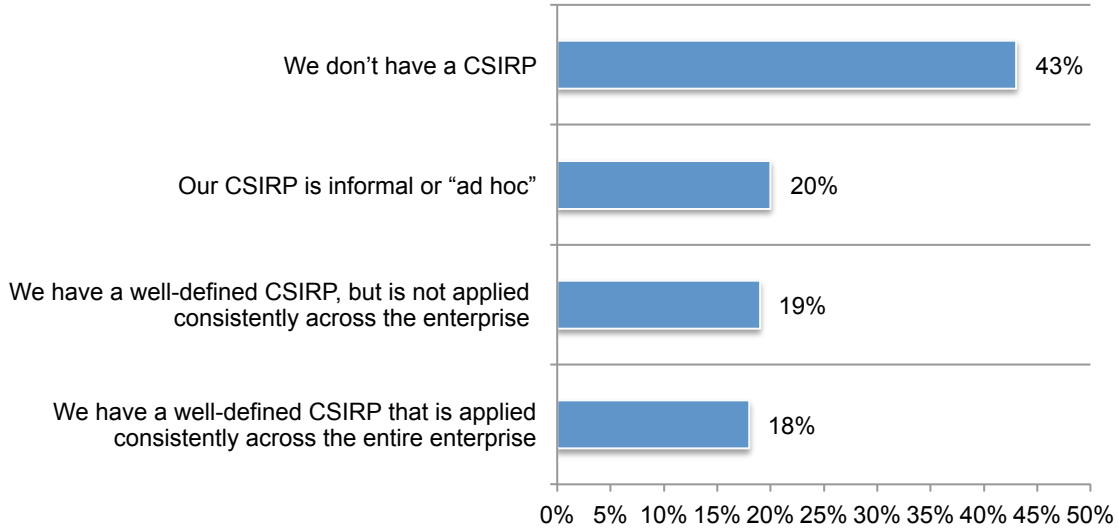
Planning and preparedness is key to cyber resiliency. Figure 6 presents the reasons why organisations struggle to achieve a cyber resilient enterprise. It is interesting that a lack of knowledgeable staff or enabling technologies is not as much a hindrance to achieving cyber resiliency as not devoting the necessary time and resources to planning and preparedness (61 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 organisation
Four responses permitted



The majority of companies are not prepared to respond to a cyber security incident. Only 18 percent of respondents have a well-defined CSIRP that is applied consistently across the entire enterprise. Despite the importance of preparedness to cyber resilience, according to Figure 7, 63 percent of respondents either say their organisation does not have a CSIRP (43 percent of respondents) or it is informal or "ad hoc" (20 percent of respondents).

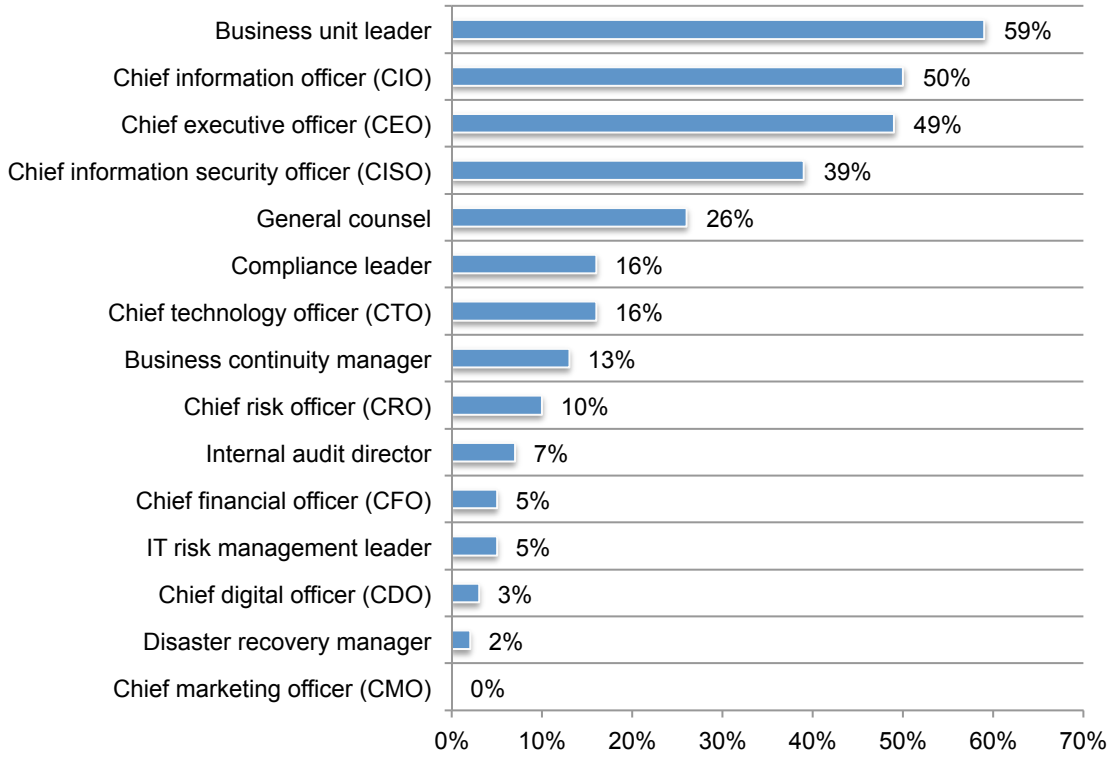
Figure 7. What best describes your organisation's cyber security incident response plan?



A high level of cyber resiliency is difficult to achieve if no one function clearly owns the responsibility. Only 19 percent of respondents say the Chief Information Officer (CIO) is accountable for making their organisations resilient to cyber threats. This is followed by 17 percent who say it is the business unit leader and 14 percent who say no one person has overall responsibility.

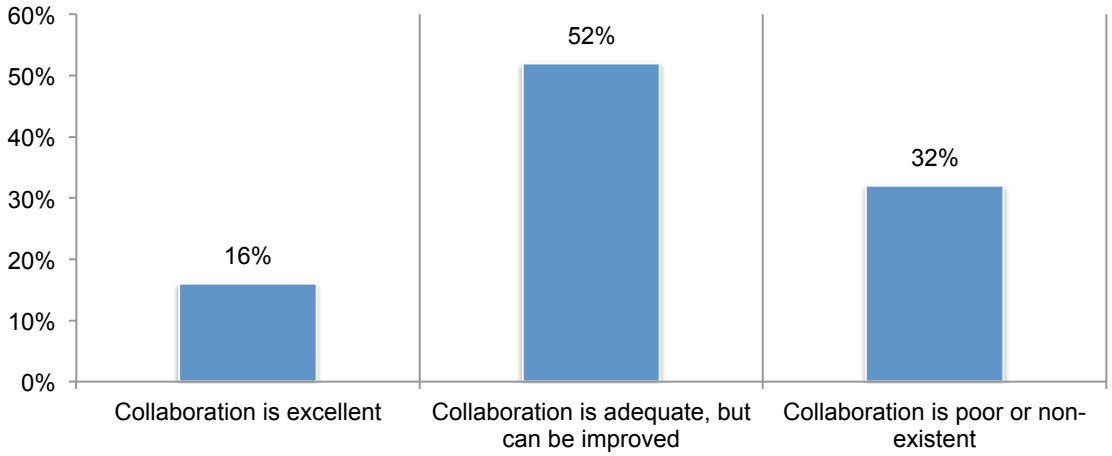
Respondents are more certain about who is influential over their organisations' efforts to ensure a high level of cyber resilience, as shown in Figure 8. Fifty-nine percent of respondents say it is the business unit leader, 50 percent say it is the Chief Information Officer (CIO) and 49 percent say it is the CEO.

Figure 8. Who has influence over your organisation'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 16 percent of respondents say collaboration is excellent. Eighty-four percent of respondents say collaboration is only adequate (52 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.

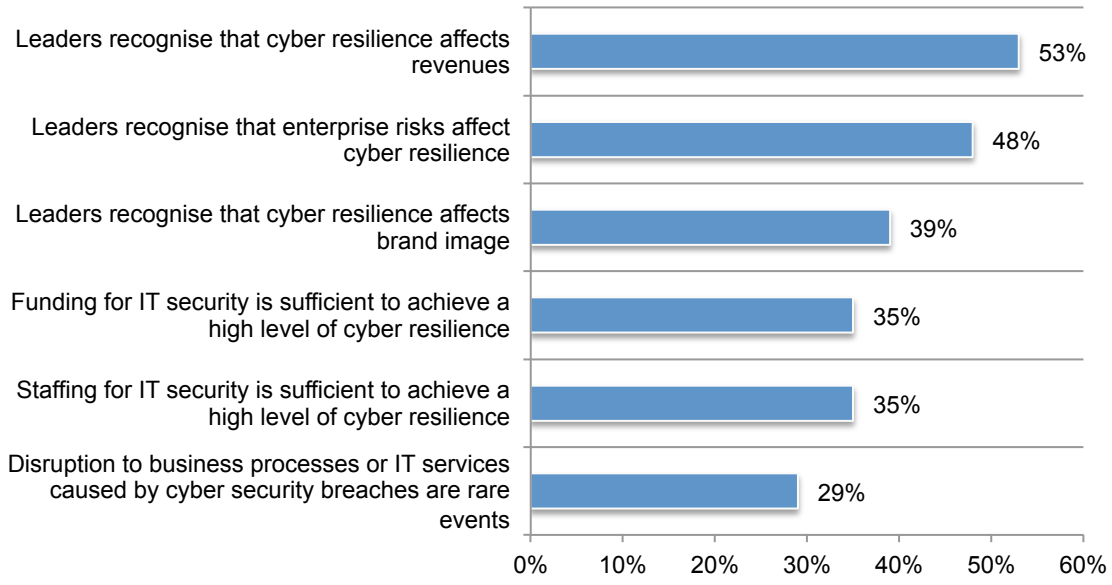
Figure 9. What is the state of collaboration to support a high level of cyber resilience in your organisation?



Organisational factors hinder efforts to achieve a high level of cyber resilience. Figure 10 shows the organisational factors that affect cyber resilience. The importance of cyber resilience is often not recognised by senior management**.** Fifty-three percent of respondents believe their organisations' leaders recognise that cyber resilience affects revenues and about half (48 percent of respondents) say leaders recognise that enterprise risks affect cyber resilience. Other factors that are a hindrance are insufficient funding and staffing. Only 35 percent of respondents say funding and staffing is adequate to achieve cyber resilience.

On average, respondents say their organisations are allocating 23 percent of the IT security budget annually to achieving cyber resilience, which averages about $3.1 million for the organisations represented in this research.

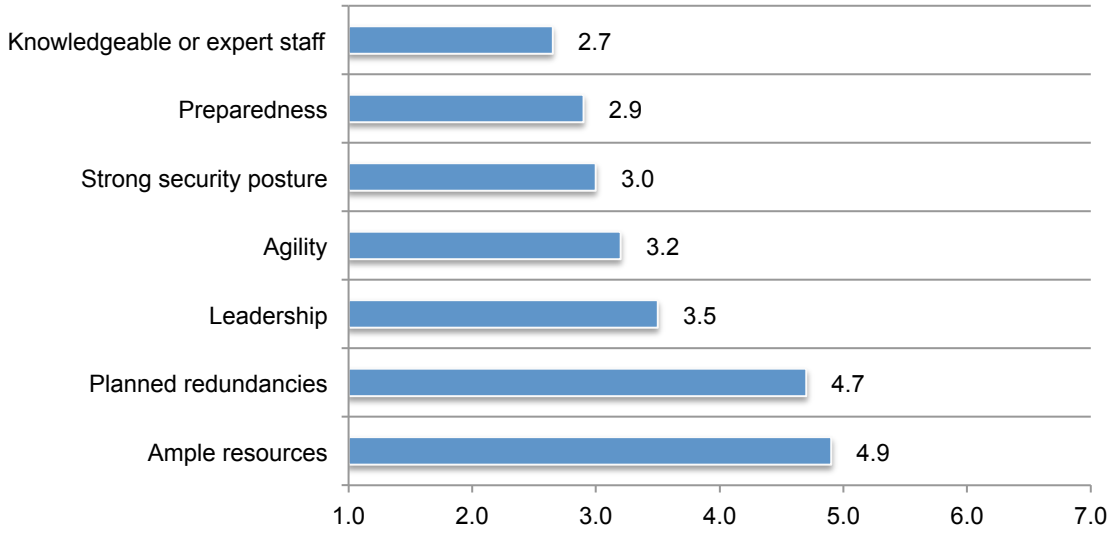
Figure 10. Organisational factors affect cyber resilience
Strongly agree and agree responses combined



Roadmap to cyber resilience

Knowledgeable staff and preparedness 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 knowledgeable staff and preparedness to deal with cyber threats is critical. Based on these findings, ample resources does not seem to be a factor when striving for a high level of cyber resilience.

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

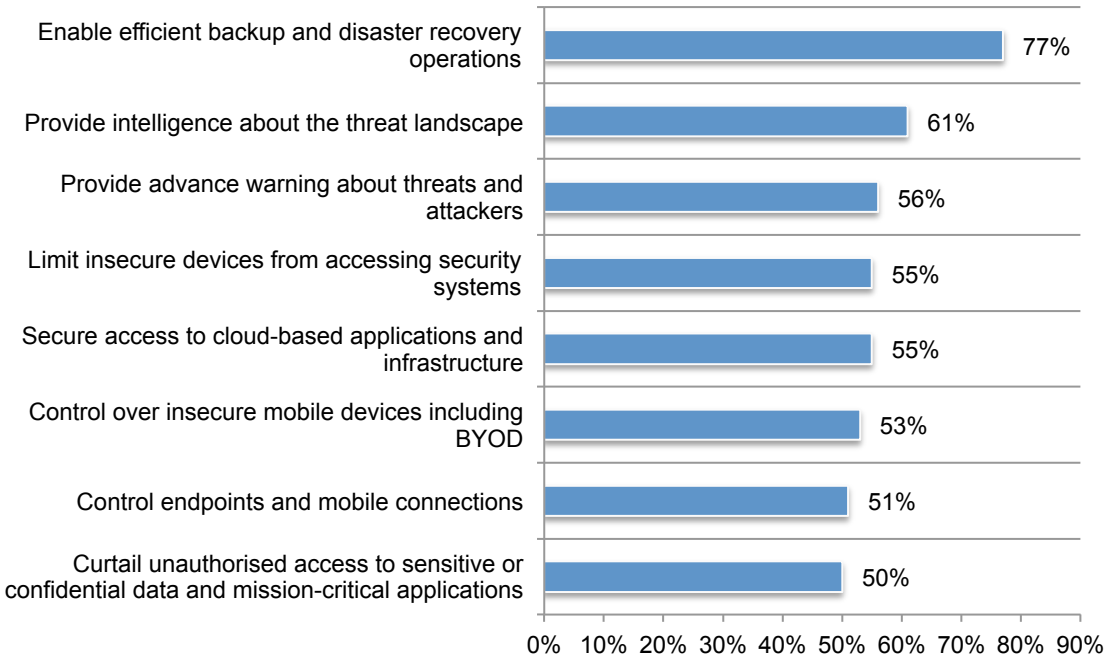


Technologies that enable efficient backup and disaster recovery operations are by far most important to building a cyber resilient enterprise. Seventy-seven percent of respondents, as shown in Figure 12, say technologies that support efficient backup and disaster recovery operations are essential or very important. Also important are technologies that provide intelligence about the threat landscape (61 percent of respondents) and advance warnings about the threat landscape (56 percent of respondents).

Mobile security in the workplace is also a factor contributing to cyber resilience. Fifty-three 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 (55 percent of respondents) and 51 percent of respondents believe technologies that control endpoints and mobile connections are important.

Finally, end user control is critical. Fifty-five percent of respondents say technologies that secure access to cloud-based applications and infrastructure is important and 50 percent of respondents say technologies that curtail unauthorised access to sensitive or confidential data and mission-critical applications 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



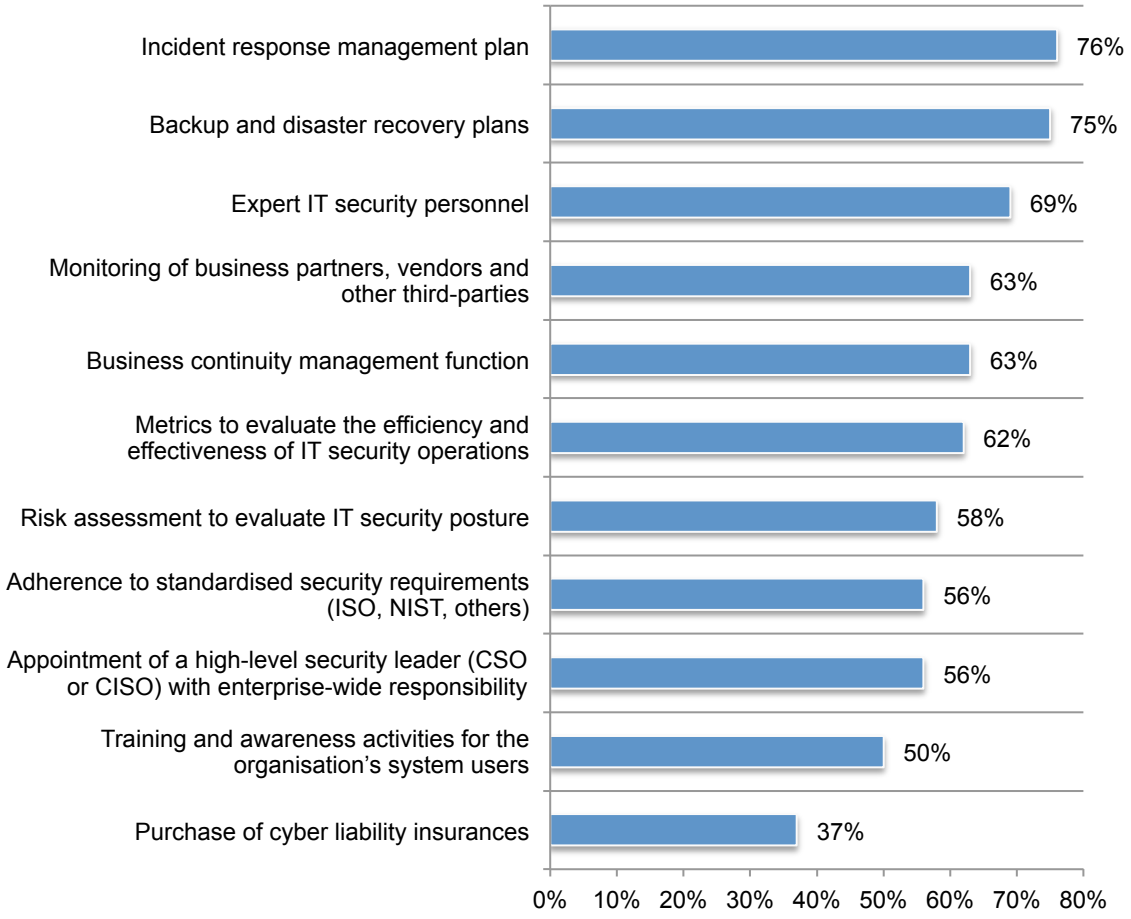
Plans to deal with security incidents and disasters are most important to building a cyber resilient enterprise. Consistent with the findings above, the most important governance practice is to have an incidence response plan, according to 76 percent of respondents (Figure 13). Also critical are backup and disaster recovery plans and expert security personnel (75 percent and 69 percent of respondents, respectively). As part of being prepared, 63 percent of respondents say business continuity management is critical as well as the appointment of a high-level security leader (CISO or CSO), according to 56 percent of respondents.

Understanding risks to the organisation should be part of a cyber resilient governance plan. This includes conducting risks assessments to evaluate the organisation's IT security posture (58 percent of respondents0 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 organisation is on the right path to achieving cyber resilience, metrics to evaluate the efficiency and effectiveness of security operations is key, according to 62 percent of respondents. Important, but less so, is adherence to standardised security requirements such as ISO, NIST and others (56 percent of respondents).

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

Essential and very important responses combined



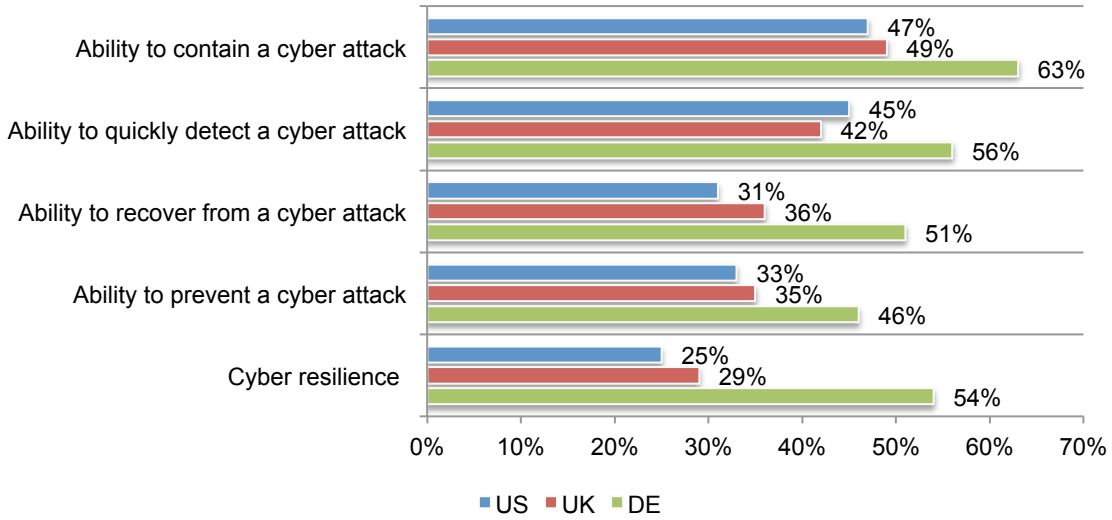
Part 3. Country differences

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 organisations are significantly more positive about the state of cyber resilience in their organisations. Fifty-four percent of German respondents rate their organisations' cyber resilience as high.

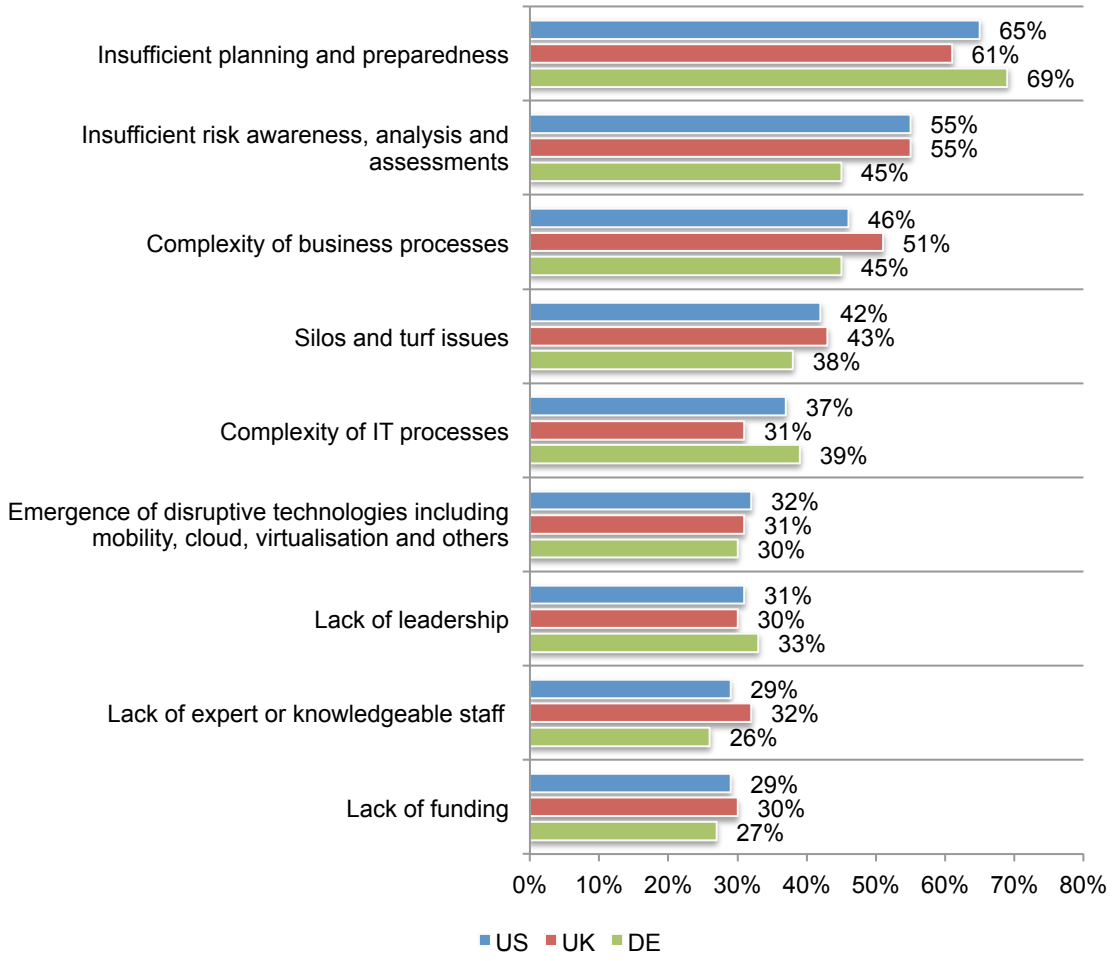
In contrast, only 25 percent of US and 29 percent of UK respondents rate cyber resilience as high in their organisation. Further, 63 percent of German respondents rate their ability to contain a cyber attack as high. US and UK respondents share similar perceptions about their organisations' resilience to cyber attacks and both lag significantly behind German respondents in how they rate their organisations resilience to cyber attacks.

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



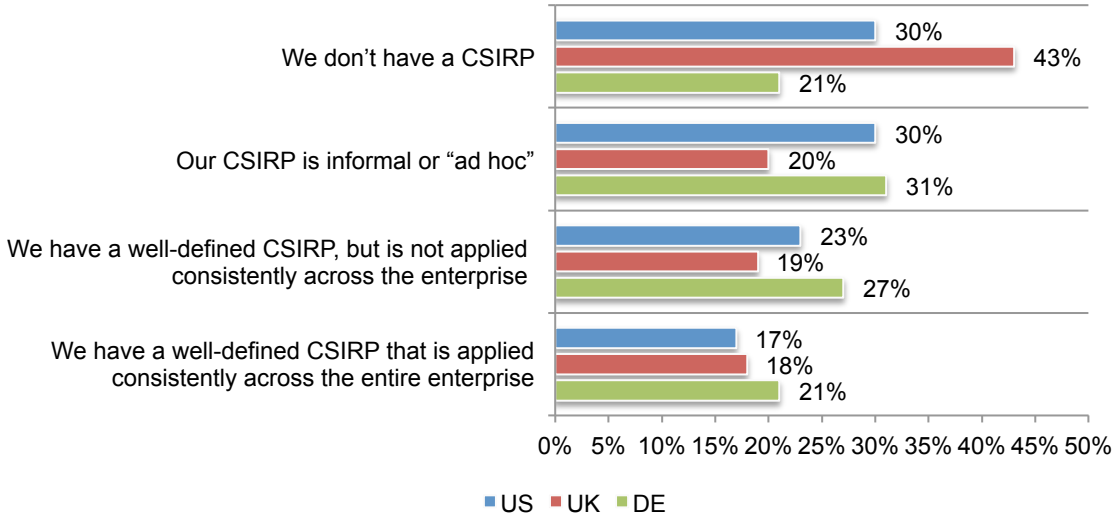
Respondents in all countries rate insufficient planning and preparedness the biggest barriers to cyber resilient. According to Figure 15, the majority of respondents in the US, UK and Germany are most concerned about not having adequate planning and preparedness to create an organisation that is resilient 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 organisation
Four responses permitted



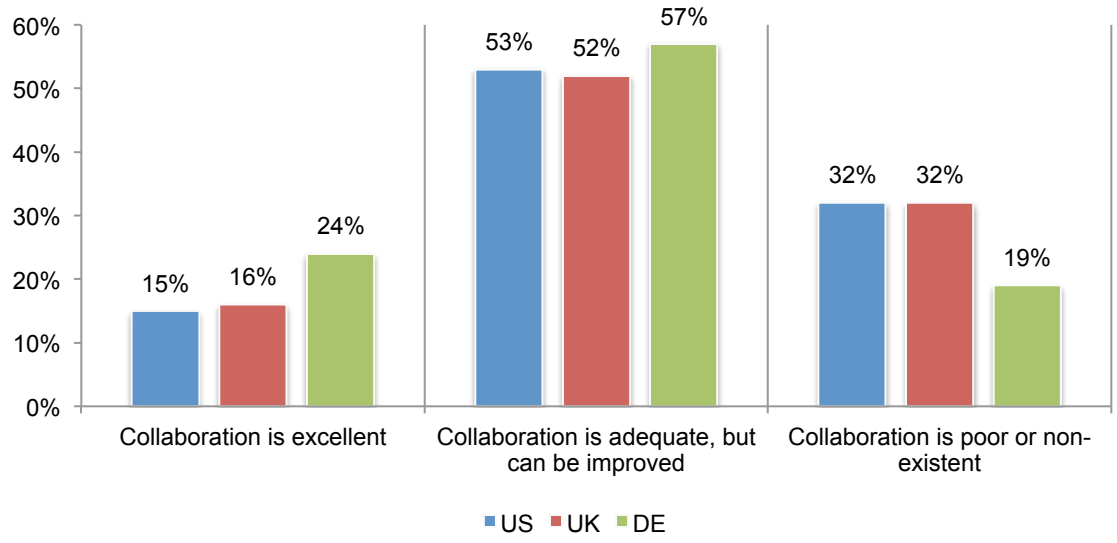
German respondents are more likely to say their organisations have a cyber security incident response plan (CSIRP). Sixty-three percent of UK respondents say their organizations do not have a CSIRP (43 percent) or one that is informal or "ad hoc" (20 percent). In contrast, 48 percent of German respondents 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 organisation's cyber security incident response plan?



German organisations 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 organisation?



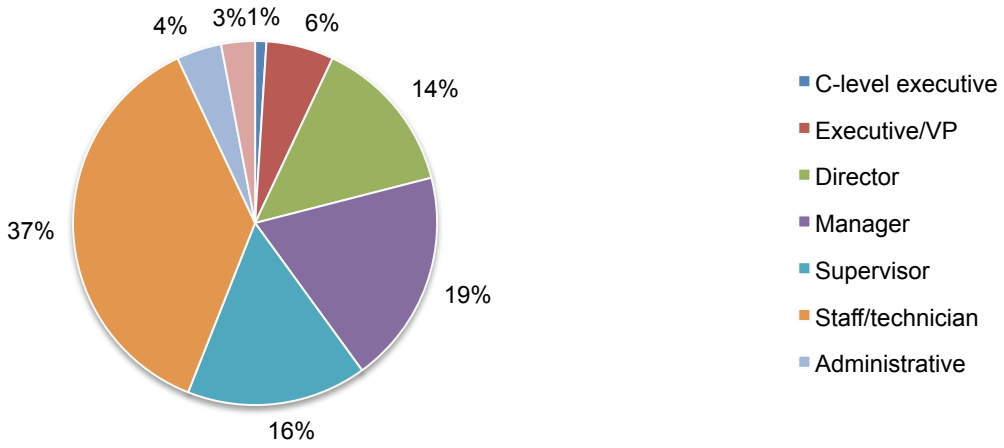
Part 4. Methods

The sampling frame is composed of 13,992 IT and IT security practitioners located in the United Kingdom. As shown in Table 1, 525 respondents completed the survey. Screening removed 75 surveys. The final sample was 450 surveys (or a 3.2 percent response rate).

Table 1. Sample response	Freq
Total sampling frame	13,992
Total returns	525
Rejected or screened surveys	75
Final sample	450
Response rate	3.2%

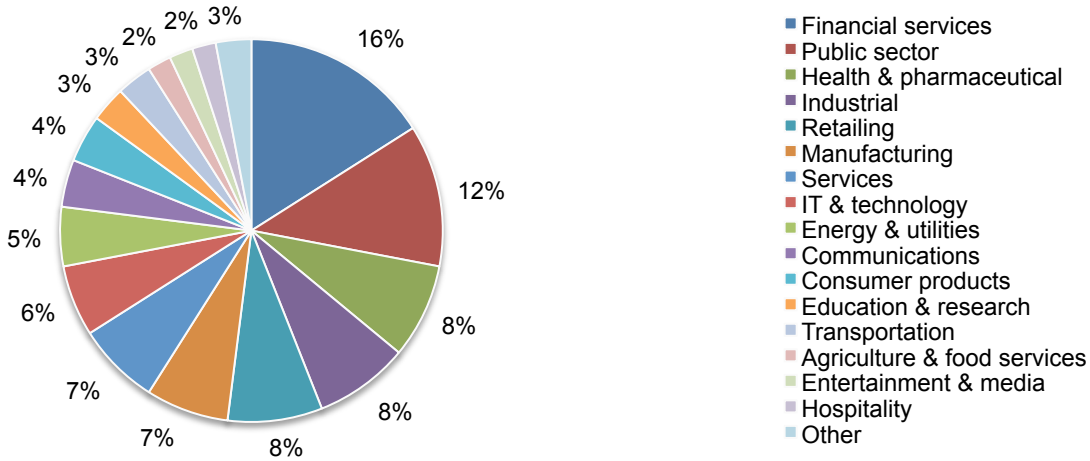
Pie Chart 1 summarises the approximate position levels of respondents in our study. As can be seen, the majority of respondents (56 percent) are at or above the supervisory level.

Pie Chart 1. Distribution of respondents according to position level



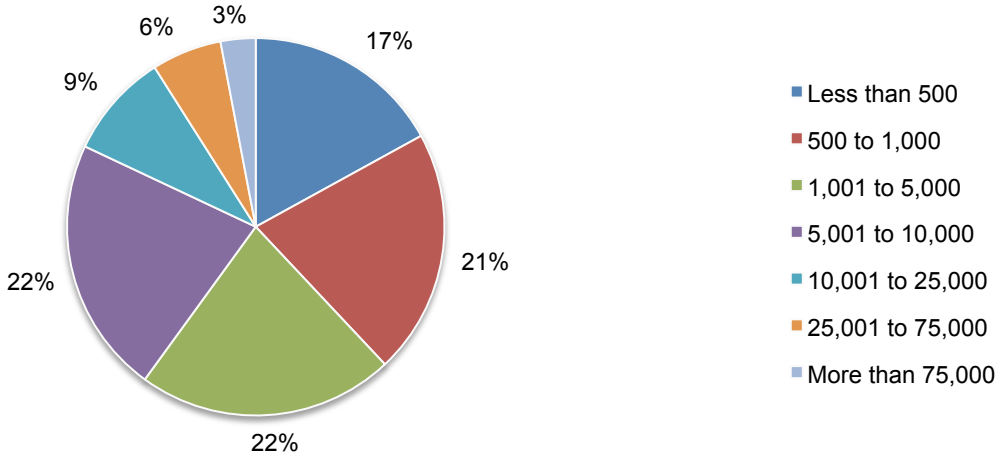
Pie Chart 2 reports the primary industry sector of respondents' organisations. This chart identifies financial services (16 percent) as the largest segment, followed by public sector (12 percent), health & pharmaceuticals (8 percent) and industrial (8 percent).

Pie Chart 2. Primary industry classification



According to Pie Chart 4, the majority of respondents (62 percent) are from organisations with a global headcount of more than a 1,000 employees.

Pie Chart 4. Worldwide headcount of the organisation



Part 4. 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 Kingdom. 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	**UK**
Total sampling frame	13,992
Total returns	525
Rejected or screened surveys	75
Final sample	450
Response rate	3.22%

Part 1. Screening

S1. What best describes your organisational role or area of focus?	UK
IT security operations	33%
IT operations	39%
CSIRT team	21%
Business continuity management	7%
None of the above (stop)	0%
Total	100%

S2. Please check all the activities that you see as part of your job or role.	UK
Managing budgets	44%
Managing staff	60%
Evaluating vendors	48%
Setting priorities	32%
Securing systems	71%
Ensuring compliance	40%
Ensuring system availability	38%
None of the above (stop)	0%
Total	300%

Part 2. Background Questions

Q1. Using the following 10-point scale, please rate your organisation's cyber resilience from 1 = low resilience to 10 = high resilience.	UK
1 or 2	10%
3 or 4	20%
5 or 6	41%
7 or 8	20%
9 or 10	9%
Total	100%
Extrapolated value	5.46

Q2. Using the following 10-point scale, please rate your organisation's ability to **prevent** a cyber attack from 1 = low to 10 = high.	UK
1 or 2	13%
3 or 4	22%
5 or 6	30%
7 or 8	24%
9 or 10	11%
Total	100%
Extrapolated value	5.46

Q3. Using the following 10-point scale, please rate your organisation's ability to quickly **detect** a cyber attack from 1 = low to 10 = high.	UK
1 or 2	10%
3 or 4	19%
5 or 6	29%
7 or 8	22%
9 or 10	20%
Total	100%
Extrapolated value	5.96

Q4. Using the following 10-point scale, please rate your organisation's ability to **contain** a cyber attack from 1 = low to 10 = high.	UK
1 or 2	5%
3 or 4	19%
5 or 6	27%
7 or 8	25%
9 or 10	24%
Total	100%
Extrapolated value	6.38

Q5. Using the following 10-point scale, please rate your organisation's ability to **recover** from a cyber attack from 1 = low to 10 = high.	UK
1 or 2	9%
3 or 4	24%
5 or 6	31%
7 or 8	28%
9 or 10	8%
Total	100%
Extrapolated value	5.54

Q6. What best describes the maturity level of your organisation's **cyber security** program or activities today?	UK
Early stage – most program activities have not as yet been deployed	12%
Middle stage – most program activities are only partially deployed	34%
Late-middle stage – most program activities are fully deployed	39%
Mature stage – all program activities are fully deployed	15%
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.	UK
Agility	3.2
Preparedness	2.9
Planned redundancies	4.7
Strong security posture	3.0
Knowledgeable or expert staff	2.7
Ample resources	4.9
Leadership	3.5

Q8a. Following are 6 common IT-related threats that may impact the cyber resilience within your organisation. Please rank order the following threats in terms of their **impact** on your organisation's cyber resiliency. 1 = Most significant impact to 6 = least significant impact.	UK
Persistent attacks	2.5
IT system failures	5.1
Data exfiltration	2.9
Human error	2.1
Natural or manmade disasters	6.0
Third-party glitches	4.8

Q8b. Please rank order the following six common IT-related threats in terms their likelihood of occurrence in your organisation. 1 = Most likely to 6 = least likely.	UK
Persistent attacks	4.5
IT system failures	3.3
Data exfiltration	3.0
Human error	1.6
Natural or manmade disasters	6.7
Third-party glitches	2.2

Q9. Which of these types of incidents or compromises are you seeing frequently in your organisation's IT networks or endpoints? Please check all that apply.	UK
Advanced persistent threats (APT) / targeted attacks	44%
Botnet attacks	14%
Clickjacking	8%
Denial of services	17%
Exploit of existing software vulnerability	90%
General malware	55%
Rootkits	5%
Spear phishing	50%
SQL injection	40%
Web-borne malware attacks	59%
Zero day attacks	31%
Total	413%

Part 3. Attributions

Please express your opinion about each one of the following statements using the five-point scale below each item.

Q10a. My organisation's leaders recognise that enterprise risks affect cyber resilience.	UK
Strongly agree	22%
Agree	26%
Unsure	28%
Disagree	13%
Strongly disagree	11%
Total	100%

Q10b. My organisation's leaders recognise that cyber resilience affects revenues.	UK
Strongly agree	26%
Agree	27%
Unsure	26%
Disagree	12%
Strongly disagree	9%
Total	100%

Q10c. My organisation's leaders recognise that cyber resilience affects brand image.	UK
Strongly agree	19%
Agree	20%
Unsure	31%
Disagree	19%
Strongly disagree	11%
Total	100%

Q10d. In my organisation, **funding** for IT security is sufficient to achieve a high level of cyber resilience	UK
Strongly agree	18%
Agree	17%
Unsure	29%
Disagree	24%
Strongly disagree	12%
Total	100%

Q10e. In my organisation, **staffing** for IT security is sufficient to achieve a high level of cyber resilience	UK
Strongly agree	16%
Agree	19%
Unsure	30%
Disagree	28%
Strongly disagree	7%
Total	100%

Q10f. In my organisation, disruption to business processes or IT services caused by cyber security breaches are rare events.	UK
Strongly agree	13%
Agree	16%
Unsure	18%
Disagree	36%
Strongly disagree	17%
Total	100%

Part 4. Cyber Resilience

Q11. What factors justify the funding of your organisation's IT security? Please select your top two choices.	UK
System or application downtime	64%
Information loss or theft	36%
Performance degradation	8%
Productivity loss	10%
Revenue decline	7%
Reputation damage	19%
Customer defection	13%
Compliance/regulatory failure	42%
Other (please specify)	1%
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	UK
Very important	10%
Important	39%
Not important	51%
Total	100%

Q12b. Maximizing customer acquisition	UK
Very important	9%
Important	32%
Not important	59%
Total	100%

Q12c. Minimizing non-compliance with laws	UK
Very important	49%
Important	39%
Not important	12%
Total	100%

Q12d. Maximizing employee productivity	UK
Very important	19%
Important	55%
Not important	26%
Total	100%

Q12e. Increasing revenues and positive cash flow	UK
Very important	8%
Important	36%
Not important	56%
Total	100%

Q12f. Expanding into new global markets	UK
Very important	8%
Important	29%
Not important	63%
Total	100%

Q12e. Protecting intellectual property	UK
Very important	71%
Important	21%
Not important	8%
Total	100%

Q12f. Enhancing brand value and reputation	UK
Very important	26%
Important	39%
Not important	35%
Total	100%

Q13a. Who has overall responsibility or **'owns"** your organisation's efforts to ensure a high level of cyber resilience? Please check only one top choice.	UK
Business continuity manager	6%
Disaster recovery manager	5%
IT risk management leader	7%
Business unit leader	17%
Chief executive officer (CEO)	9%
Chief financial officer (CFO)	0%
Chief information officer (CIO)	19%
Chief technology officer (CTO)	6%
Chief marketing officer (CMO)	0%
Chief risk officer (CRO)	3%
Chief information security officer (CISO)	8%
Chief digital officer (CDO)	0%
Compliance leader	4%
Internal audit director	0%
General counsel	2%
No one person has overall responsibility	14%
Total	100%

Q13b. Who has **"influence"** over your organisation's efforts to ensure a high level of cyber resilience? Please check three top choices.	UK
Business continuity manager	13%
Disaster recovery manager	2%
IT risk management leader	5%
Business unit leader	59%
Chief executive officer (CEO)	49%
Chief financial officer (CFO)	5%
Chief information officer (CIO)	50%
Chief technology officer (CTO)	16%
Chief marketing officer (CMO)	0%
Chief risk officer (CRO)	10%
Chief information security officer (CISO)	39%
Chief digital officer (CDO)	3%
Compliance leader	16%
Internal audit director	7%
General counsel	26%
Total	300%

Q14. What one statement best describes how various functions within your organisation work together to support a high level of cyber resilience?	UK
Collaboration is excellent	16%
Collaboration is adequate, but can be improved	52%
Collaboration is poor or non-existent	32%
Total	100%

Q15. Please check one statement that best describes your organisation's cyber security incident response plan (CSIRP).	UK
We have a well-defined CSIRP that is applied consistently across the entire enterprise	18%
We have a well-defined CSIRP, but is not applied consistently across the enterprise	19%
Our CSIRP is informal or "ad hoc"	20%
We don't have a CSIRP	43%
Total	100%

Q16. What do you see as the most significant barriers to achieving a high level of cyber resilience within your organisation? Please provide four top choices.	UK
Lack of funding	30%
Lack of leadership	30%
Lack of expert or knowledgeable staff	32%
Lack of enabling technologies	25%
Silos and turf issues	43%
Insufficient planning and preparedness	61%
Insufficient risk awareness, analysis and assessments	55%
Complexity of business processes	51%
Complexity of IT processes	31%
Interconnected business and IT processes with partners, vendors and other third parties	10%
Emergence of disruptive technologies including mobility, cloud, virtualisation and others	31%
Other (please specify)	1%
Total	400%

Part 5. Security Enabling Technologies

Q17. Following are cyber security technology features considered important by many organisations. 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	UK
Essential	15%
Very important	17%
Important	31%
Not important	20%
Irrelevant	17%
Total	100%

Q17b. Provide advance warning about threats and attackers	UK
Essential	23%
Very important	33%
Important	26%
Not important	12%
Irrelevant	6%
Total	100%

Q17c. Enable adaptive perimeter controls	UK
Essential	7%
Very important	16%
Important	34%
Not important	28%
Irrelevant	15%
Total	100%

Q17d. Provide intelligence about the threat landscape	UK
Essential	18%
Very important	43%
Important	20%
Not important	11%
Irrelevant	8%
Total	100%

Q17e. Enable efficient patch management	UK
Essential	21%
Very important	32%
Important	35%
Not important	11%
Irrelevant	1%
Total	100%

Q17f. Capture information about attackers (honey pot/hack back)	UK
Essential	16%
Very important	29%
Important	43%
Not important	10%
Irrelevant	2%
Total	100%

Q17g. Prioritise threats, vulnerabilities and attacks	UK
Essential	17%
Very important	35%
Important	31%
Not important	14%
Irrelevant	3%
Total	100%

Q17h. Control over insecure mobile devices including BYOD	UK
Essential	22%
Very important	31%
Important	28%
Not important	13%
Irrelevant	6%
Total	100%

Q17i. Limit insecure devices from accessing security systems	UK
Essential	23%
Very important	32%
Important	34%
Not important	5%
Irrelevant	6%
Total	100%

Q17j. Effort to reduce footprint of sensitive or confidential data	UK
Essential	7%
Very important	25%
Important	41%
Not important	16%
Irrelevant	11%
Total	100%

Q17k. Curtail unauthorised sharing of sensitive or confidential data	UK
Essential	9%
Very important	30%
Important	42%
Not important	15%
Irrelevant	4%
Total	100%

Q17l. Curtail unauthorised access to sensitive or confidential data and mission-critical applications	UK
Essential	25%
Very important	25%
Important	36%
Not important	11%
Irrelevant	3%
Total	100%

Q17m. Curtail end-user access to insecure Internet sites and web applications	UK
Essential	19%
Very important	25%
Important	30%
Not important	15%
Irrelevant	11%
Total	100%

Q17n. Control endpoints and mobile connections	UK
Essential	24%
Very important	27%
Important	30%
Not important	12%
Irrelevant	7%
Total	100%

Q17o. Limit the loss or theft of portable data-bearing devices such as laptops, smartphones and others	UK
Essential	14%
Very important	23%
Important	36%
Not important	15%
Irrelevant	12%
Total	100%

Q17p. Enable efficient backup and disaster recovery operations	UK
Essential	38%
Very important	39%
Important	8%
Not important	11%
Irrelevant	4%
Total	100%

Q17q. Establish metrics for upstream reporting	UK
Essential	9%
Very important	17%
Important	57%
Not important	13%
Irrelevant	4%
Total	100%

Q17r. Conduct surveillance of system users	UK
Essential	16%
Very important	33%
Important	35%
Not important	12%
Irrelevant	4%
Total	100%

Q17s. Secure access to cloud-based applications and infrastructure	UK
Essential	25%
Very important	30%
Important	25%
Not important	16%
Irrelevant	4%
Total	100%

Q17t. Secure data stored in clouds	UK
Essential	18%
Very important	29%
Important	22%
Not important	23%
Irrelevant	8%
Total	100%

Part 6. Governance & Controls

Q18. Following are governance and control practices considered important by many organisations. 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	UK
Essential	39%
Very important	30%
Important	23%
Not important	8%
Irrelevant	0%
Total	100%

Q18b. Clearly defined IT security policies	UK
Essential	10%
Very important	23%
Important	30%
Not important	24%
Irrelevant	13%
Total	100%

Q18c. Backup and disaster recovery plans	UK
Essential	35%
Very important	40%
Important	13%
Not important	9%
Irrelevant	3%
Total	100%

Q18d. Business continuity management function	UK
Essential	28%
Very important	35%
Important	12%
Not important	15%
Irrelevant	10%
Total	100%

Q18e. Incident response management plan	UK
Essential	39%
Very important	37%
Important	12%
Not important	11%
Irrelevant	1%
Total	100%

Q18f. Background checks of system users	UK
Essential	11%
Very important	33%
Important	41%
Not important	13%
Irrelevant	2%
Total	100%

Q18g. Specialised training for IT security personnel	UK
Essential	11%
Very important	22%
Important	38%
Not important	19%
Irrelevant	10%
Total	100%

Q18h. Training and awareness activities for the organisation's system users	UK
Essential	22%
Very important	28%
Important	24%
Not important	18%
Irrelevant	8%
Total	100%

Q18i. Monitoring of business partners, vendors and other third-parties	UK
Essential	27%
Very important	36%
Important	21%
Not important	12%
Irrelevant	4%
Total	100%

Q18j. Internal or external audits of security and IT compliance practices	UK
Essential	9%
Very important	20%
Important	30%
Not important	28%
Irrelevant	13%
Total	100%

Q18k. Segregation of duties between IT and business functions	UK
Essential	5%
Very important	17%
Important	24%
Not important	28%
Irrelevant	26%
Total	100%

Q18l. Risk assessment to evaluate IT security posture	UK
Essential	29%
Very important	29%
Important	21%
Not important	16%
Irrelevant	5%
Total	100%

Q18m. Adherence to standardised security requirements (ISO, NIST, others)	UK
Essential	27%
Very important	29%
Important	24%
Not important	15%
Irrelevant	5%
Total	100%

Q18n. Appointment of a high-level security leader (CSO or CISO) with enterprise-wide responsibility	UK
Essential	24%
Very important	32%
Important	25%
Not important	11%
Irrelevant	8%
Total	100%

Q18o. Appointment of high-level leader (CPO) accountable for information protection and privacy	UK
Essential	19%
Very important	24%
Important	30%
Not important	17%
Irrelevant	10%
Total	100%

Q18p. Upstream communication channel from the security leader to the CEO and board of directors	UK
Essential	12%
Very important	24%
Important	31%
Not important	22%
Irrelevant	11%
Total	100%

Q18q. Creation of a security program charter approved by executive management	UK
Essential	9%
Very important	16%
Important	20%
Not important	42%
Irrelevant	13%
Total	100%

Q18r. Regularly scheduled presentation on the state of security to the board of directors	UK
Essential	15%
Very important	26%
Important	26%
Not important	28%
Irrelevant	5%
Total	100%

Q18s. Process for self-reporting compliance violations to appropriate authorities	UK
Essential	5%
Very important	17%
Important	25%
Not important	37%
Irrelevant	16%
Total	100%

Q18t. Purchase of cyber liability insurances	UK
Essential	12%
Very important	25%
Important	18%
Not important	30%
Irrelevant	15%
Total	100%

Q18u. Metrics to evaluate the efficiency and effectiveness of IT security operations	UK
Essential	29%
Very important	33%
Important	20%
Not important	13%
Irrelevant	5%
Total	100%

Part 7. Budget for Cyber Resilience

Q19. Approximately, what is the dollar range that best describes your organisation's **IT/cyber security budget for 2015**?	UK*
< $1 million	0%
$1 to 5 million	11%
$6 to $10 million	39%
$11 to $15 million	30%
$16 to $20 million	9%
$21 to $25 million	6%
$26 to $50 million	5%
> $50 million	0%
Total	100%
Extrapolated value ($millions)	$12.3
*Scale converted from GBP and Euros to US Dollars	

Q20. Approximately, what percentage of the **2015 IT/cyber security budget** will go to cyber resilience-related activities?	UK
< 2%	1%
2% to 5%	0%
6% to 10%	5%
11% to 20%	29%
21% to 30%	35%
31% to 40%	23%
41% to 50%	6%
51% to 60%	2%
61% to 70%	0%
71% to 80%	0%
81% to 90%	0%
91 to 100%	0%
Total	101%
Extrapolated value (percentage)	25%

Part 8. Organisational and Respondents' Demographics

D1. What best describes your position level within the organisation?	UK
C-level executive	1%
Executive/VP	6%
Director	14%
Manager	19%
Supervisor	16%
Staff/technician	37%
Administrative	4%
Consultant/contractor	3%
Other (please specify)	0%
Total	100%

D2. What best describes your organisation's primary industry classification?	UK
Agriculture & food services	2%
Communications	4%
Consumer products	4%
Defence & aerospace	1%
Education & research	3%
Energy & utilities	5%
Entertainment & media	2%
Financial services	16%
Health & pharmaceutical	8%
Hospitality	2%
Industrial	8%
IT & technology	6%
Logistics & distribution	0%
Manufacturing	7%
Public sector	12%
Retailing	8%
Services	7%
Transportation	3%
Other (please specify)	2%
Total	100%

D3. What range best describes the full-time headcount of your global organisation?	UK
Less than 500	17%
500 to 1,000	21%
1,001 to 5,000	22%
5,001 to 10,000	22%
10,001 to 25,000	9%
25,001 to 75,000	6%
More than 75,000	3%
Total	100%
Extrapolated value (headcount)	9,485

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 organisations.

As a member of the **Council of American Survey Research Organisations (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.