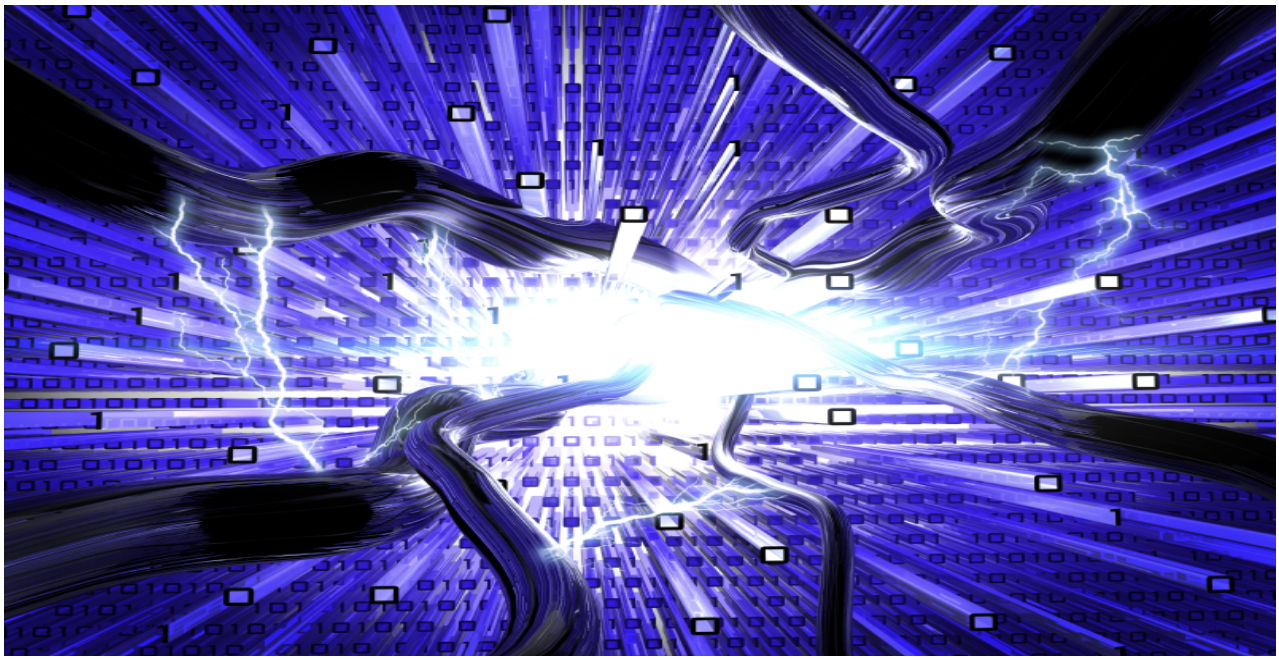


# The Cyber Resilient Organization in Germany: Learning to Thrive against Threats

## Independently conducted by Ponemon Institute LLC

Sponsored by Resilient, an IBM Company

Publication Date: January 2016

# The Cyber Resilient Organization in Germany: 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

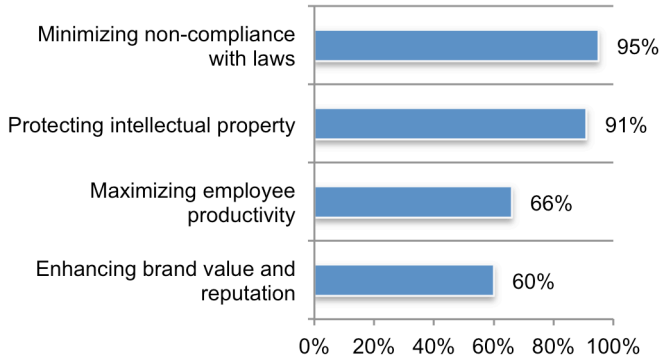
With cyber attacks growing increasingly frequent and complex, cybersecurity strategies are shifting: while prevention is still important, it is more about prevailing. Cyber resilience supports businesses efforts to ensure they'll continue to thrive despite the increased likelihood of a data breach.

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 445 IT and IT security practitioners in Germany about their organizations' approach to becoming resilient to security threats. The findings are presented in the study, *The Cyber Resilient Organization in Germany: 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. Minimizing non-compliance with laws and the protection of high-value intellectual property are best achieved with cyber resilience, according to 95 percent and 91 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 maximize employee productivity (66 percent of respondents) and enhance brand value and reputation (60 percent of respondents).

**Key takeaways include the following:**

**The majority of respondents say the state of cyber resilience in their organizations is considered high.** Fifty-four 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, key components of cyber resiliency are containing and quickly detecting a cyber attack and 63 percent and 56 percent or respondents, respectively rate this ability as high. More than half (51 percent of respondents) rates their organizations ability to recover from a cyber attack as high. Only 46 percent of respondents rate the ability to prevent a cyber attack as high.

**Organizations face a multitude of cyber threats.** By far, respondents say general malware and exploits of existing software vulnerabilities (77 percent and 75 percent of respondents, respectively) are the most frequent threats. Also frequent are web-borne malware attacks (64 percent of respondents) and spear phishing (57 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 organizations' systems or applications from going down according to 66 percent of respondents. It is interesting that only 35 percent of respondents say it is the threat of information loss or theft that influences funding

**Persistent attacks are the enemy of cyber resiliency.** The IT-related threat believed to have the greatest impact on an organization's ability to be cyber resilient are persistent threats. However, the most likely threat to occur are third party glitches. Data exfiltration is also considered a significant threat.

**Planning and preparedness is key to cyber resiliency.** The findings reveal that a lack of knowledgeable staff or enabling technologies arenot as much a hindrance as not devoting the necessary time and resources to planning and preparedness (69 percent of respondents) or complexity of business processes and insufficient risk awareness, analysis and assessments (both 45 percent of respondents).

**The majority of companies are not prepared to respond to a cyber security incident.** Only 21 percent of respondents have a well-defined CSIRP that is applied consistently across the entire enterprise. Despite the importance of preparedness to cyber resilience**,** 52 percent of respondents either say their organization does not have a CSIRP (21 percent of respondents) or it is informal or "ad hoc" (31 percent of respondents).

**A high level of cyber resiliency is difficult to achieve if no one function is responsible.** Only 20 percent of respondents say the business unit leader is accountable for making their organizations resilient to cyber threats. This is followed by 13 percent who say it is the chief information officer (CIO) or no one person has accountability. Ten percent of respondents say the chief information security officer (CISO) has overall responsibility.

Respondents are more certain about who is influential over their organizations' efforts to ensure a high level of cyber resilience. Fifty-seven percent of respondents say it is the chief information officer, 49 percent say it is the CEO and 41 percent of respondents say it is the chief information security officer (CISO).

**Collaboration among business functions is essential to a high level of cyber resilience but it rarely happens.** Only 24 percent of respondents say collaboration is excellent. Seventy-six percent of respondents say collaboration is only adequate (57 percent of respondents) or poor (19 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.

**Organizational factors hinder efforts to achieve a high level of cyber resilience.** Figure 10 shows the organizational factors that affect cyber resilience. Fifty-six percent of respondents say funding for IT security is sufficient to achieve a high level of cyber resilience**.** About half (51 percent of respondents) believe their organizations' leaders recognize that cyber resilience affects enterprise risks and brand image. Fifty-four percent of respondents say management believes cyber resilience affects revenues. Only 47 percent of respondents say staffing for IT security is sufficient to achieve a high level of cyber resilience.

**Preparedness and a knowledgeable staff 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 expert staff and leadership.

**Technologies that enable efficient backup and disaster recovery operations are by far most important to building a cyber resilient enterprise.** Sixty-nine 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 (67 percent of respondents) and those that provide intelligence about the threat landscape (56 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 (52 percent of respondents) and 49 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 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.

**Plans to deal with security incidents and disasters are most important to building a cyber resilient enterprise.** The most important governance practice is to have an incident response management and backup and disaster recovery plan in place, according to 76 percent and 75 percent of respondents, respectively. Also critical are business continuity management plans and expert IT security personnel (74 percent and 68 percent of respondents, respectively).

Understanding risks to the organization should be part of a cyber resilient governance plan. This includes conducting risk assessments to evaluate the organization's IT security posture (63 percent of respondents) and monitoring business partners, vendors and other third parties (56 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.

Also important is adherence to standardized security requirements such as ISO, NIST and others, according to 65 percent of respondents. 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 53 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:

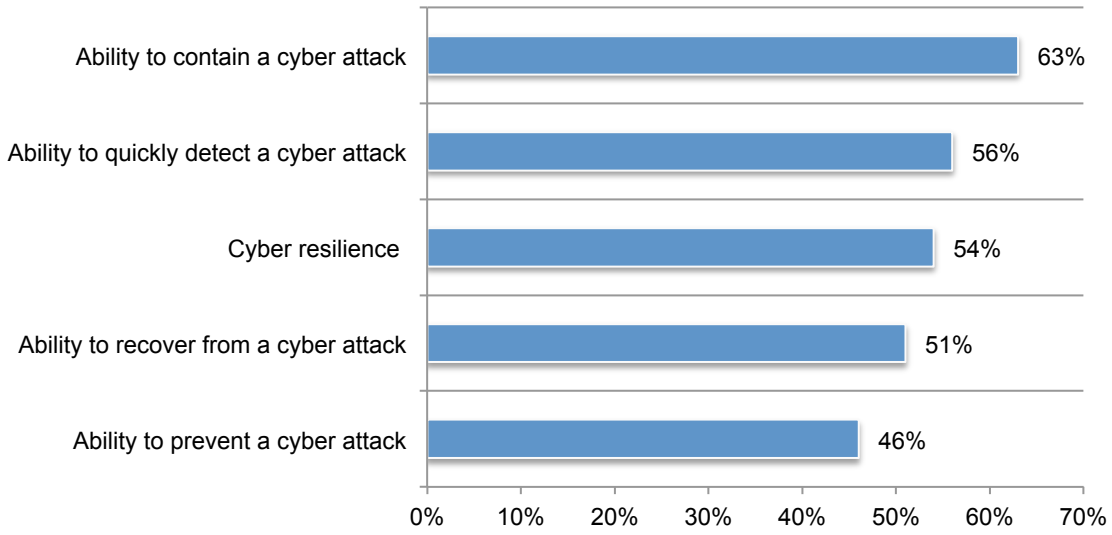
- The state of cyber resilience today
- Barriers to a cyber resilient enterprise
- Roadmap to cyber resilience

### The state of cyber resilience today

**The majority of respondents say the state of cyber resilience in their organizations is considered high.** As shown in Figure 2, 54 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.

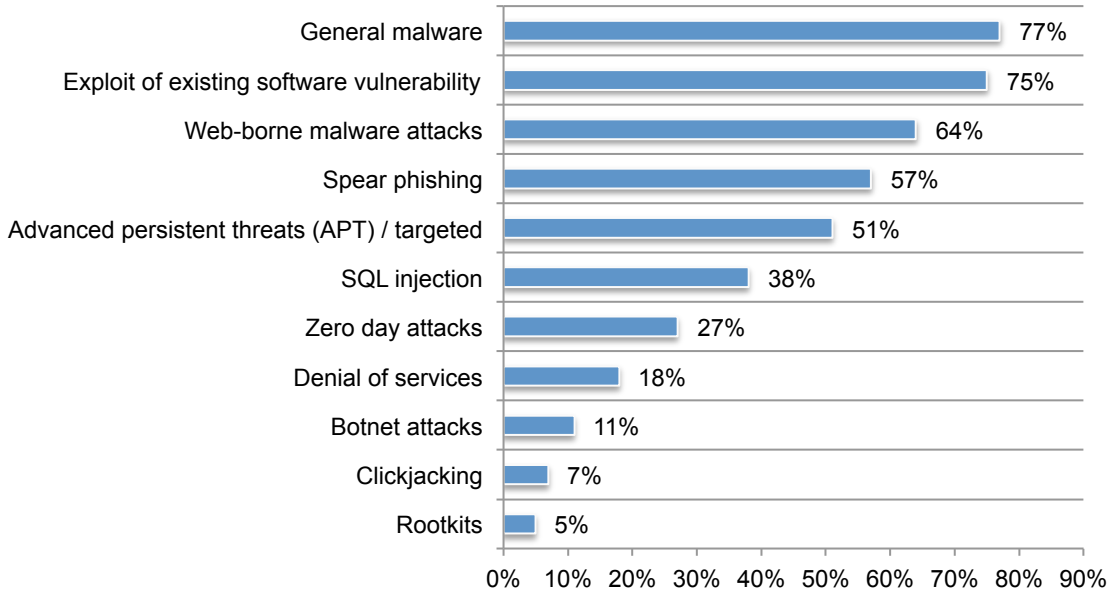
Moreover, key components of cyber resiliency are containing and quickly detecting a cyber attack and 63 percent and 56 percent of respondents, respectively rate this ability as high. More than half (51 percent of respondents) rates their organizations ability to recover from a cyber attack as high. Only 46 percent of respondents rate the ability to prevent a cyber attack as high.

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



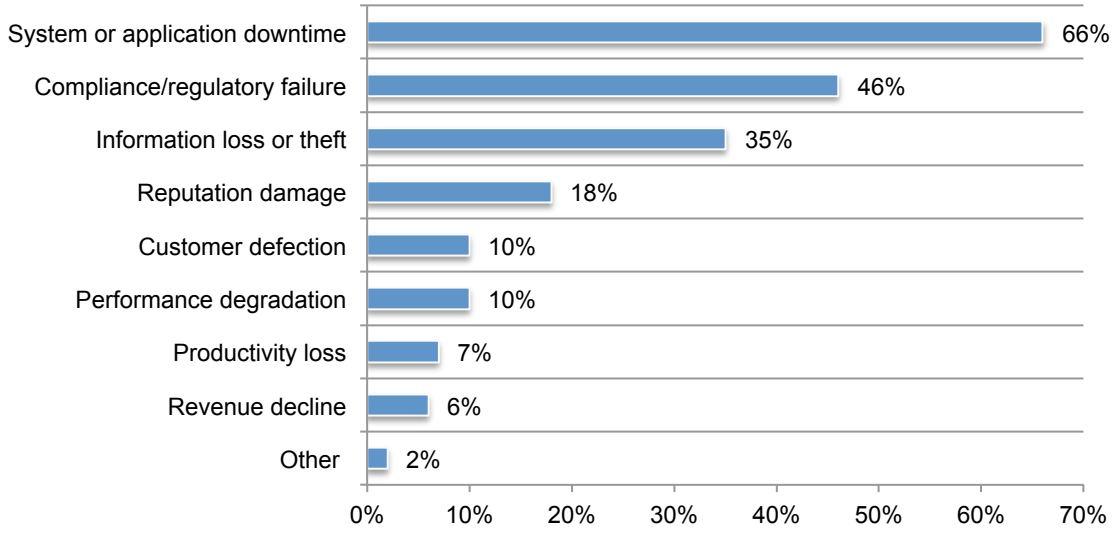
**Organizations face a multitude of cyber threats.** Figure 3 reveals the types of incidents or compromises in IT networks or endpoints causing the most problems for organizations. By far, respondents say general malware and exploits of existing software vulnerabilities (77 percent and 75 percent of respondents, respectively) are the most frequent threats. Also frequent are web-borne malware attacks (64 percent of respondents) and spear phishing (57 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 organizations' systems or applications from going down, according to 66 percent of respondents. It is interesting that only 35 percent of respondents say it is the threat of information loss or theft that influences funding.

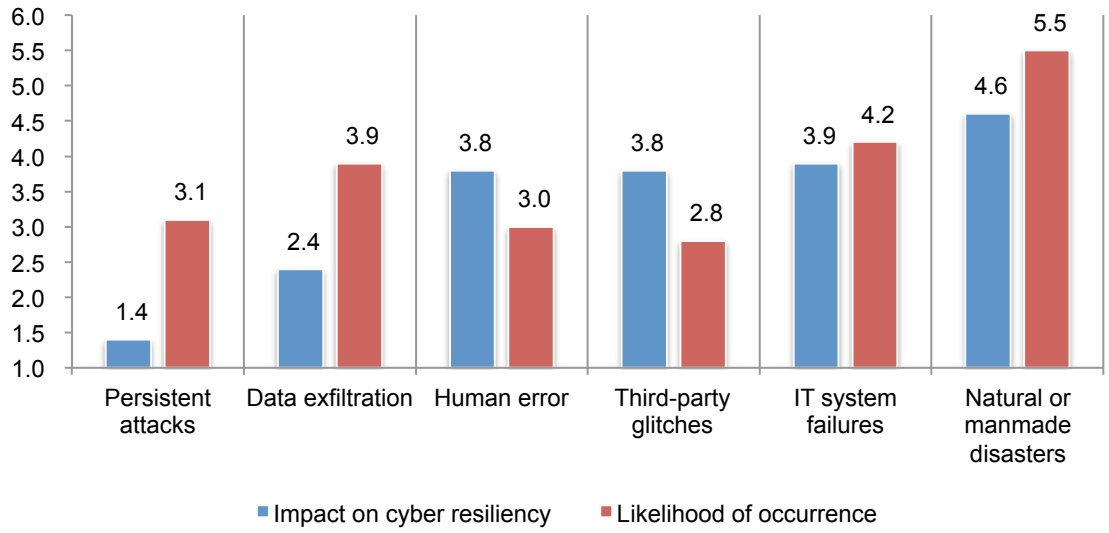
**Figure 4. Factors used to justify the funding of IT security**
Two responses permitted



**Barriers to achieving a cyber resilient enterprise**

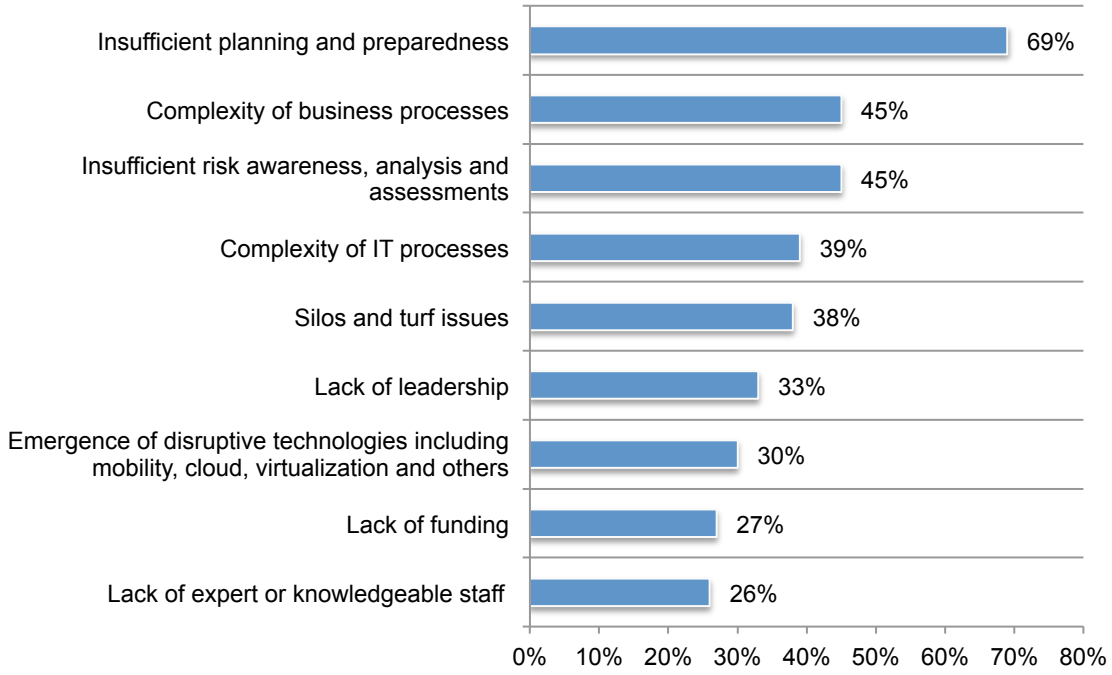
**Persistent attacks are the enemy of cyber resiliency.** As shown in Figure 5, the IT-related threat believed to have the greatest impact on an organization's ability to be cyber resilient are persistent threats. However, the most likely threat to occur are third party glitches. Data exfiltration is also considered a significant threat.

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



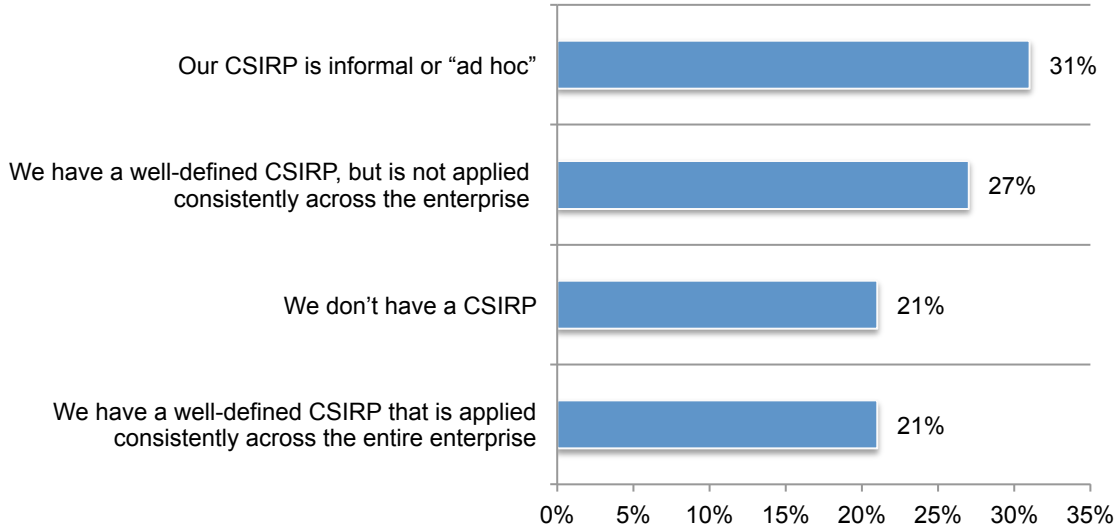
**Planning and preparedness is key to cyber resiliency.** Figure 6 presents the reasons why organizations struggle to achieve a cyber resilient enterprise. It is interesting that a lack of knowledgeable staff or enabling technologies are not as much a hindrance as not devoting the necessary time and resources to planning and preparedness (69 percent of respondents) or complexity of business processes and insufficient risk awareness, analysis and assessments (both 45 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 21 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, 52 percent of respondents either say their organization either does not have a CSIRP (21 percent of respondents) or it is informal or "ad hoc" (31 percent of respondents).

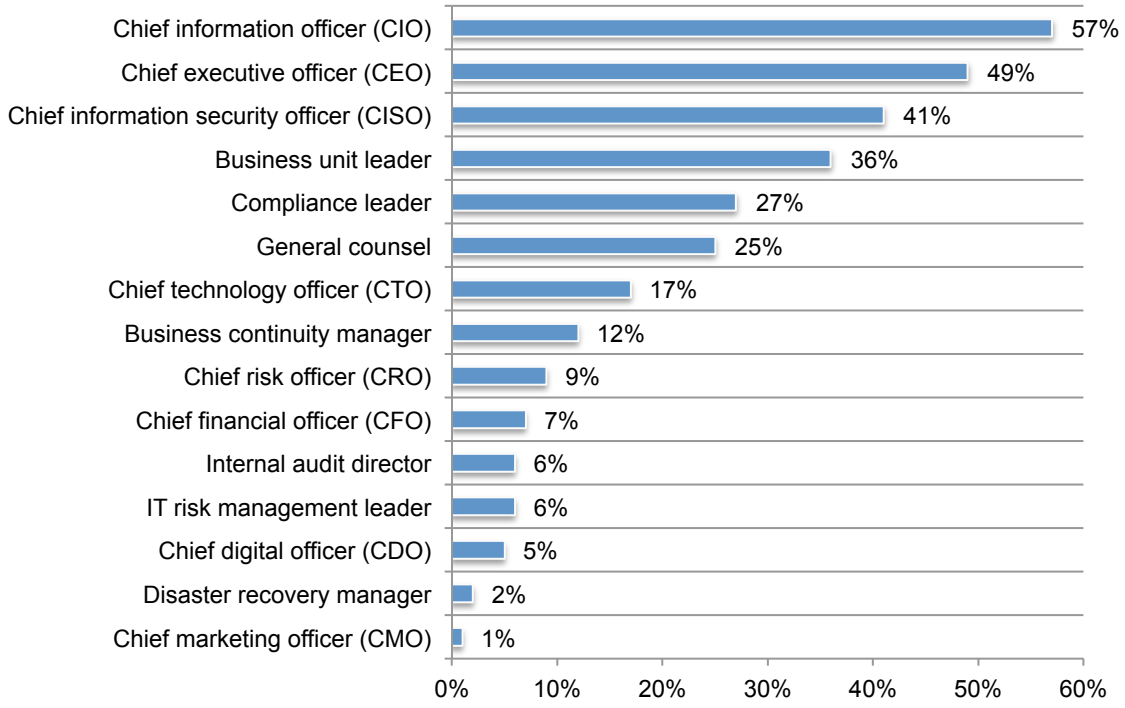
**Figure 7. What best describes your organization's cyber security incident response plan?**



**A high level of cyber resiliency is difficult to achieve if no one function is responsible.** Only 20 percent of respondents say the business unit leader is accountable for making their organizations' resilient to cyber threats. This is followed by 13 percent who say it is the chief information officer (CIO) or no one person has accountability. Ten percent of respondents say the chief information security officer (CISO) has overall responsibility.

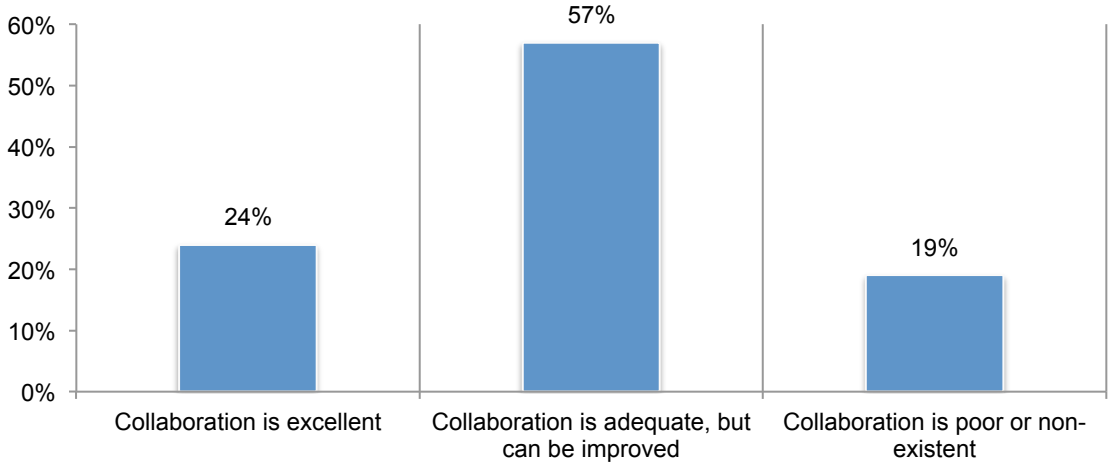
Respondents are more certain about who is influential over their organizations' efforts to ensure a high level of cyber resilience, as shown in Figure 8. Fifty-seven percent of respondents say it is the chief information officer, 49 percent say it is the CEO and 41 percent of respondents say it is the 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 24 percent of respondents say collaboration is excellent. Seventy-six percent of respondents say collaboration is only adequate (57 percent of respondents) or poor (19 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.

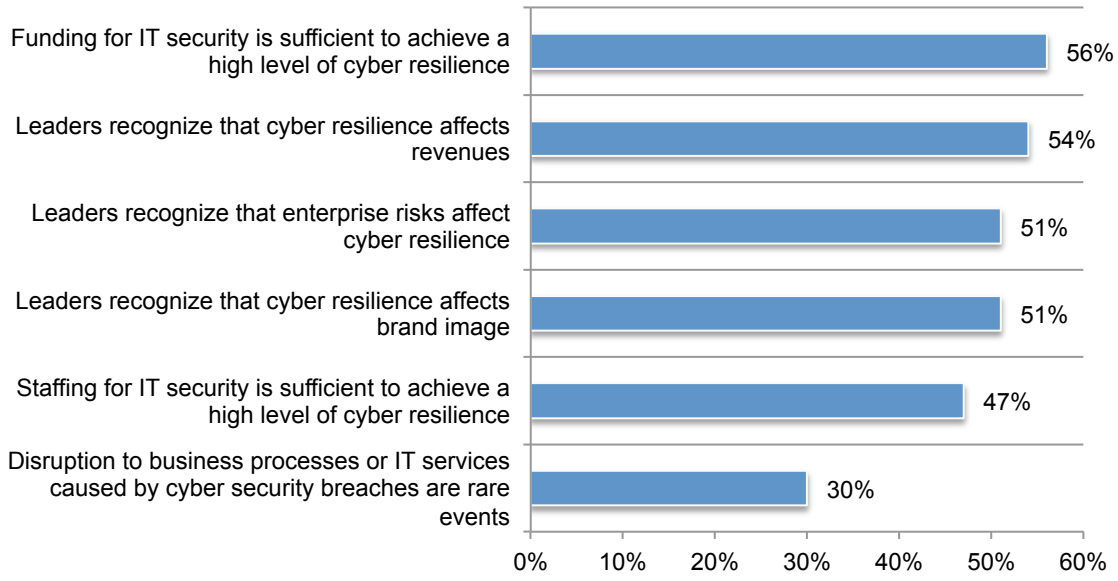
**Figure 9. What is the state of collaboration to support a high level of cyber resilience in your organization?**



**Organizational factors hinder efforts to achieve a high level of cyber resilience.** Figure 10 shows the organizational factors that affect cyber resilience. Fifty-six percent of respondents say funding for IT security is sufficient to achieve a high level of cyber resilience**.** About half (51 percent of respondents) believe their organizations' leaders recognize that enterprise risks affects cyber resilience and cyber resilience affects brand image. Fifty-four percent of respondents say management believes cyber resilience affects revenues. Only 47 percent of respondents say staffing for IT security is sufficient to achieve a high level of cyber resilience.

On average, respondents say their organizations are allocating 23 percent of the IT security budget annually to achieving cyber resilience, which averages about $3.3 million for the organizations represented in this research.

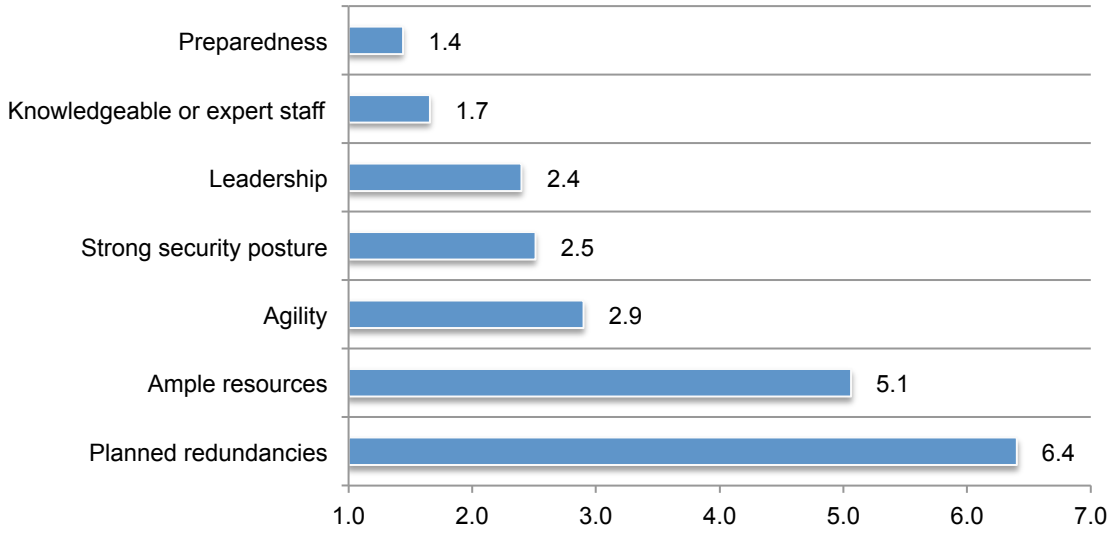
**Figure 10. Organizational factors affect cyber resilience**
Strongly agree and agree responses combined



## Roadmap to cyber resilience

**Preparedness and a knowledgeable staff 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 expert staff and leadership.

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



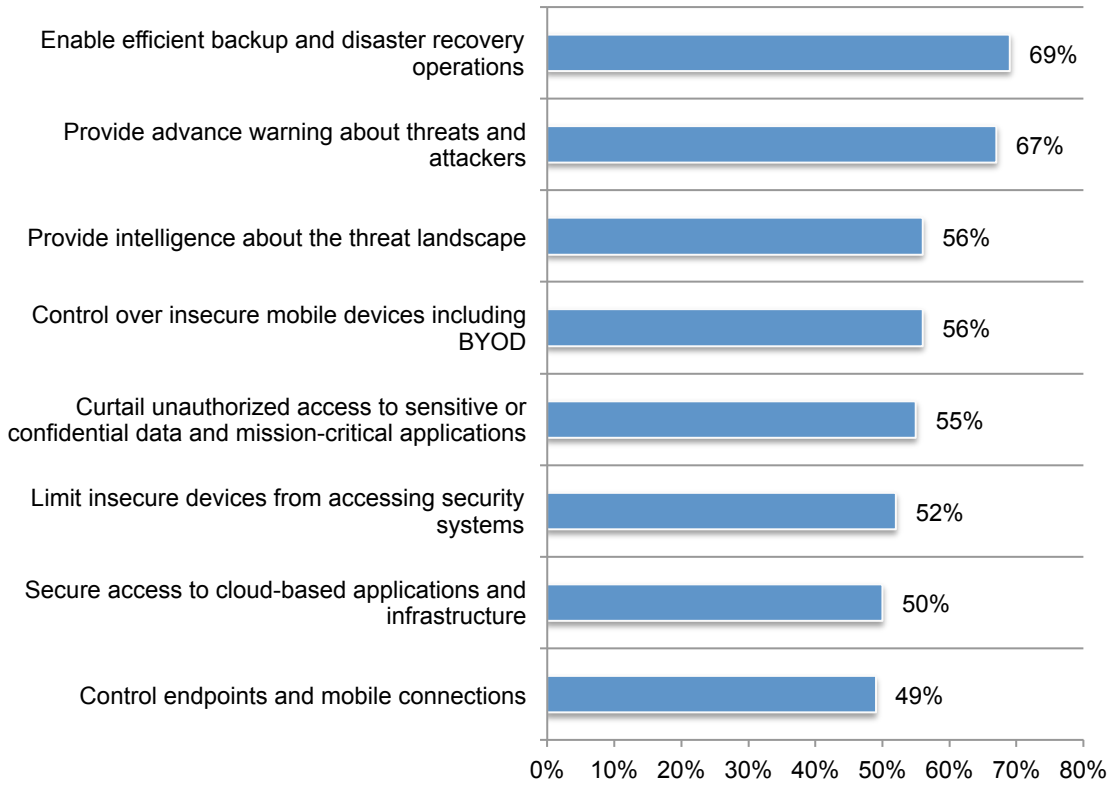
**Technologies that enable efficient backup and disaster recovery operations are by far most important to building a cyber resilient enterprise.** Sixty-nine percent of respondents, as shown in Figure 12, say technologies that support efficient backup and disaster recovery operations are essential or very important. Also important are technologies that provide advance warning about threats and attackers (67 percent of respondents) and those that provide intelligence about the threat landscape (56 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 (52 percent of respondents) and 49 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 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



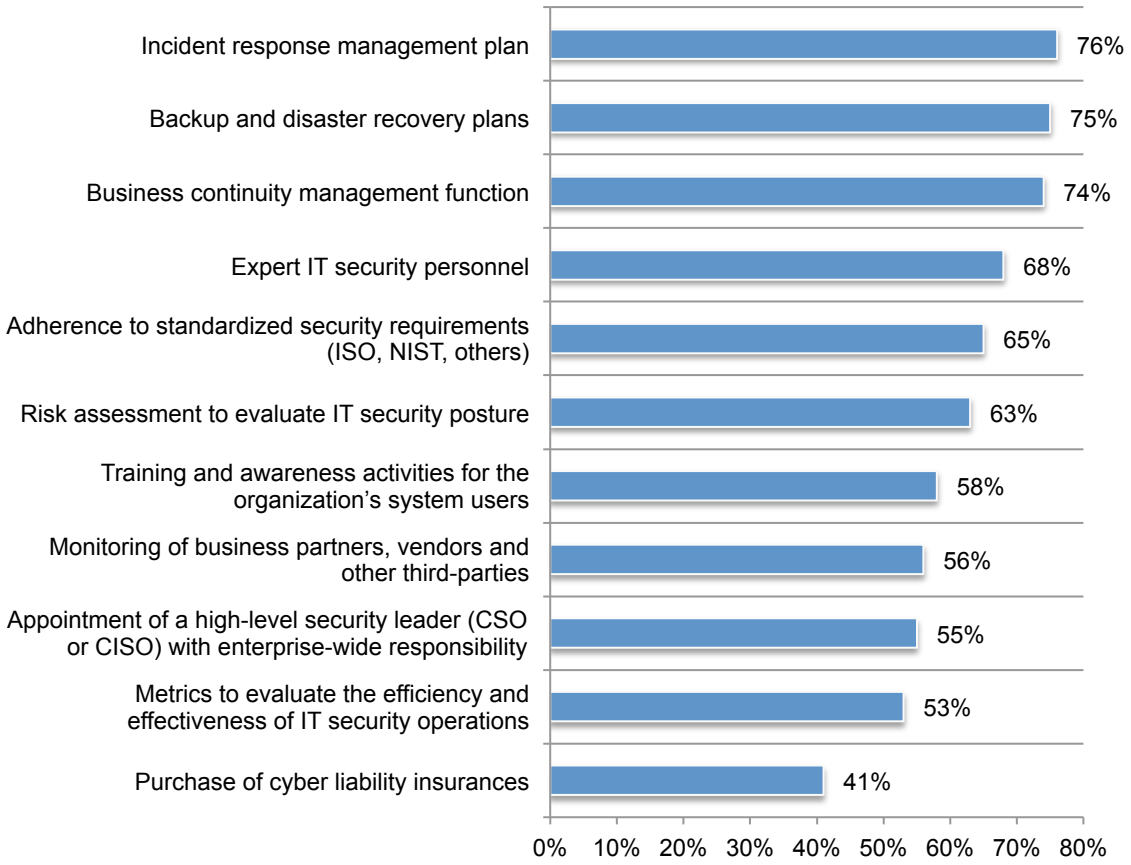
**Plans to deal with security incidents and disasters are most important to building a cyber resilient enterprise.** The most important governance practice is to have an incident response management and backup and disaster recovery plan in place, according to 76 percent and 75 percent of respondents, respectively (Figure 13). Also critical are business continuity management plans and expert IT security personnel (74 percent and 68 percent of respondents, respectively).

Understanding risks to the organization should be part of a cyber resilient governance plan. This includes conducting risk assessments to evaluate the organization's IT security posture (63 percent of respondents) and monitoring business partners, vendors and other third parties (56 percent of respondents). To mitigate the end user risk, 58 percent of respondents say training and awareness activities for system users are essential or very important.

Also important is adherence to standardized security requirements such as ISO, NIST and others, according to 65 percent of respondents. 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 53 percent of respondents.

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

Essential and very important responses combined



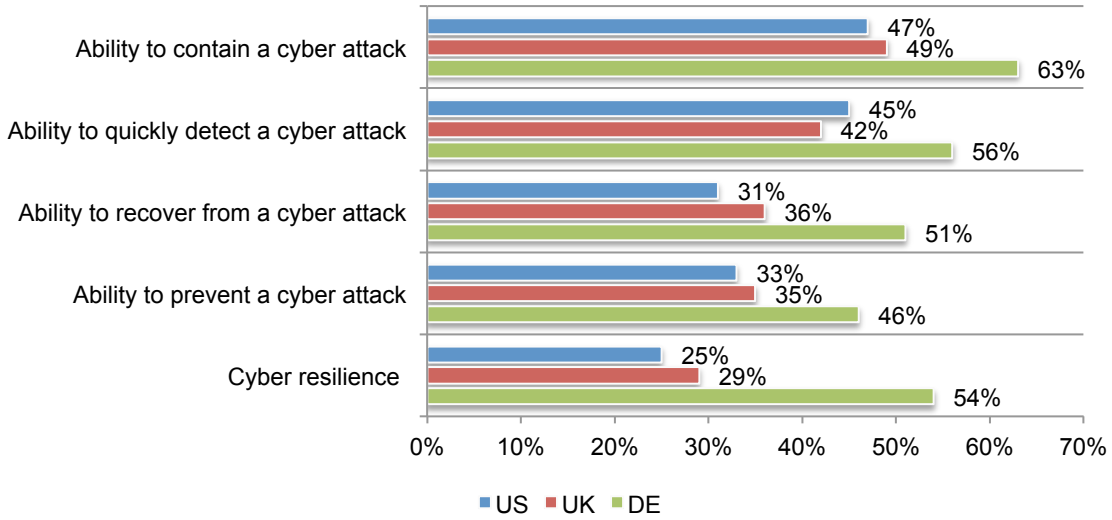
**Part 3. Country Differences**

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 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.

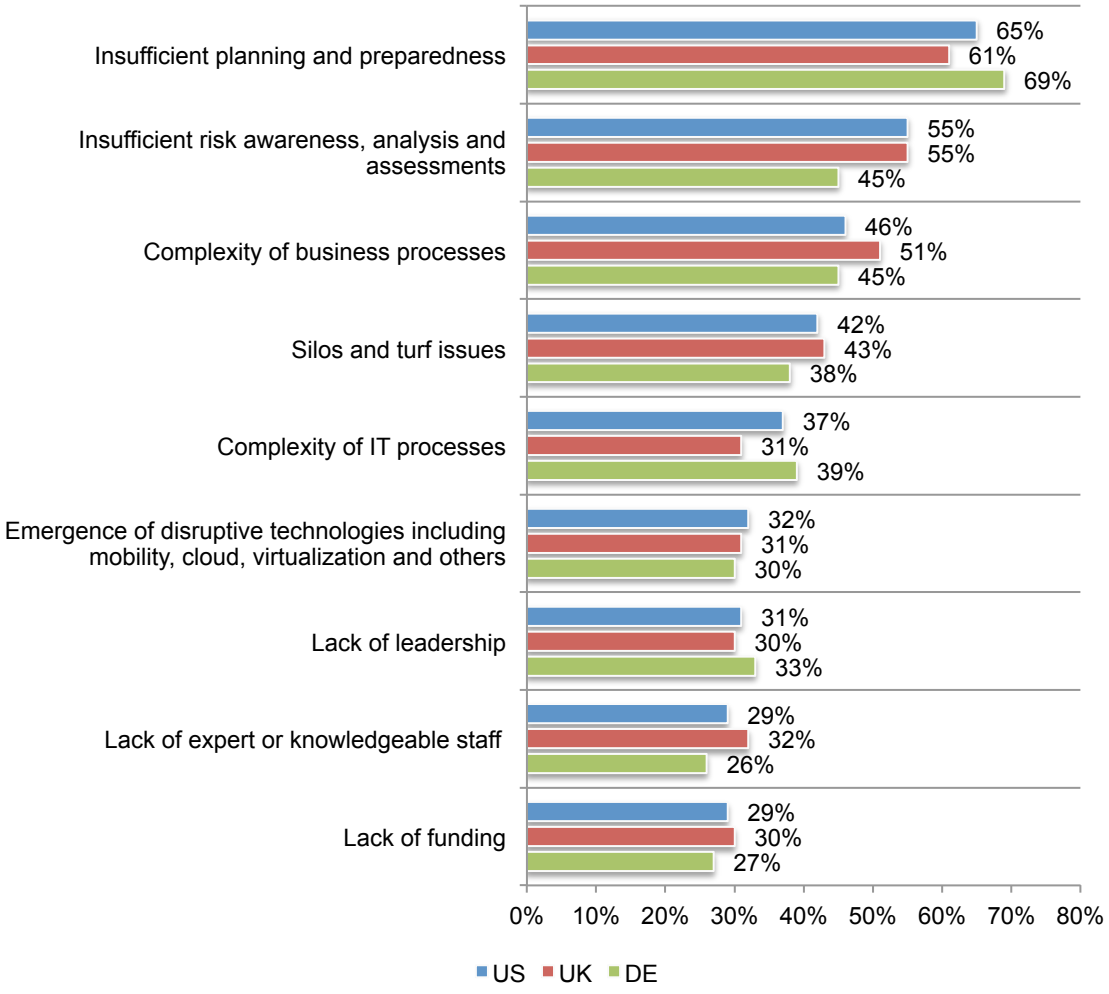
In contrast, only 25 percent of US and 29 percent of UK respondents rank cyber resilience as high in their organizations. Further, 63 percent of German respondents rate their ability to contain a cyber attack as high. US and UK respondents share similar perceptions about their organizations' resilience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



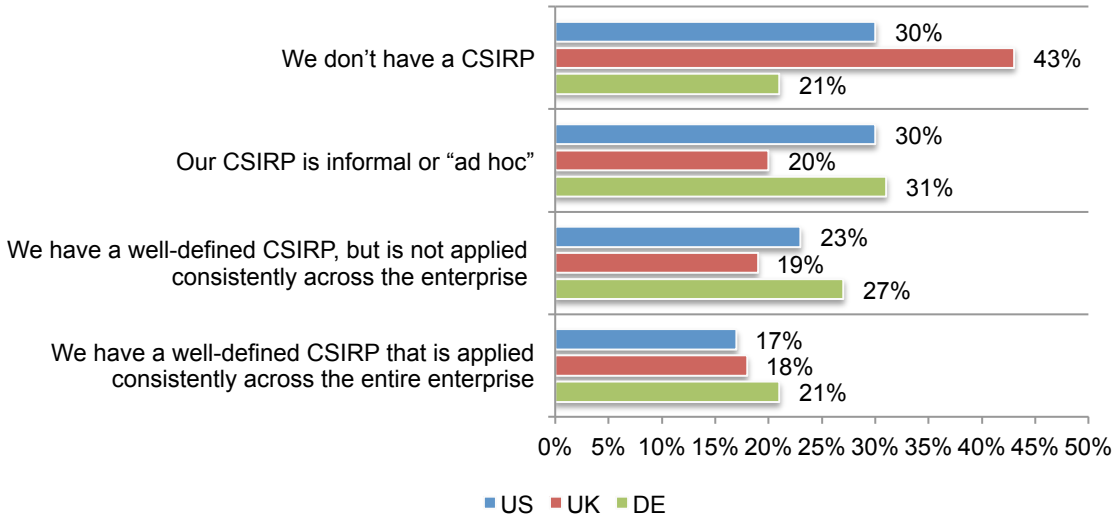
**Respondents in all countries rate insufficient planning and preparedness the biggest barriers to cyber resilient.** According to Figure 15, the majority of respondents in the US, UK and Germany are most concerned about not having adequate planning and preparedness to create an organization that is 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. What are the most significant barriers to achieving a high level of cyber resilience within your organization?**
Four responses permitted



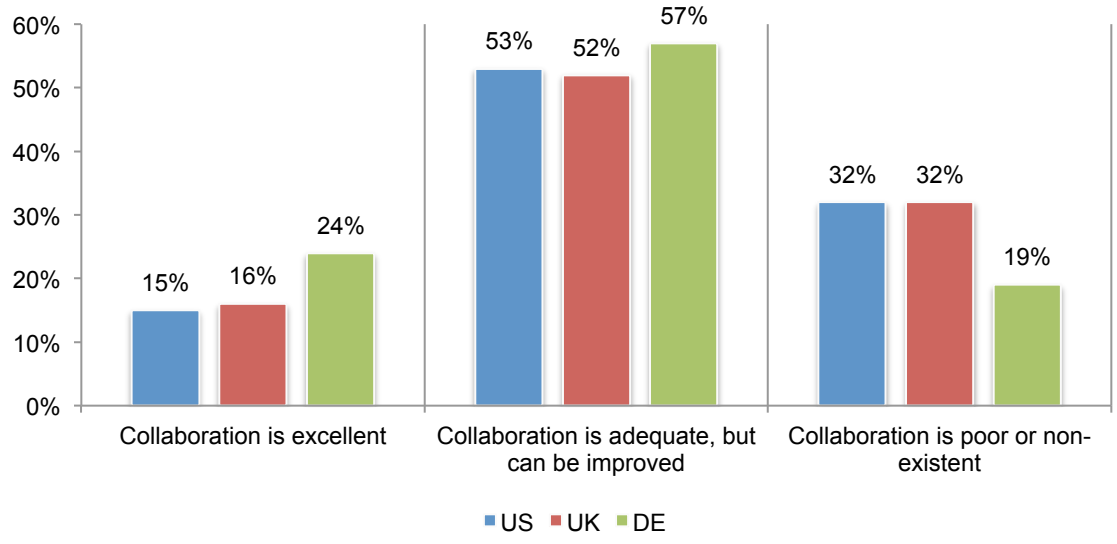
**German respondents are more likely to say their organizations have a cyber security incident response plan (CSIRP).** Sixty-three percent of UK respondents say their organizations do not have a CSIRP (43 percent) or one that is informal or "ad hoc" (20 percent). In contrast, 48 percent of German respondents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



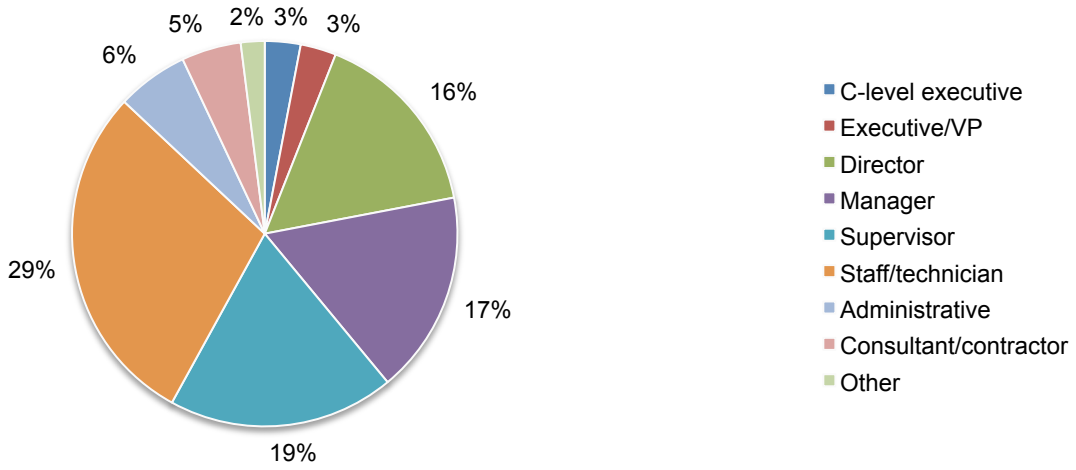
## Part 4. Methods

The sampling frame is composed of 14,005 IT and IT security practitioners located in Germany. As shown in Table 1, 502 respondents completed the survey. Screening removed 57 surveys. The final sample was 445 surveys (or a 3.2 percent response rate).

| Table 1. Sample response | Freq |
|---|---|
| Total sampling frame | 14,005 |
| Total returns | 502 |
| Rejected or screened surveys | 57 |
| Final sample | 445 |
| Response rate | 3.2% |

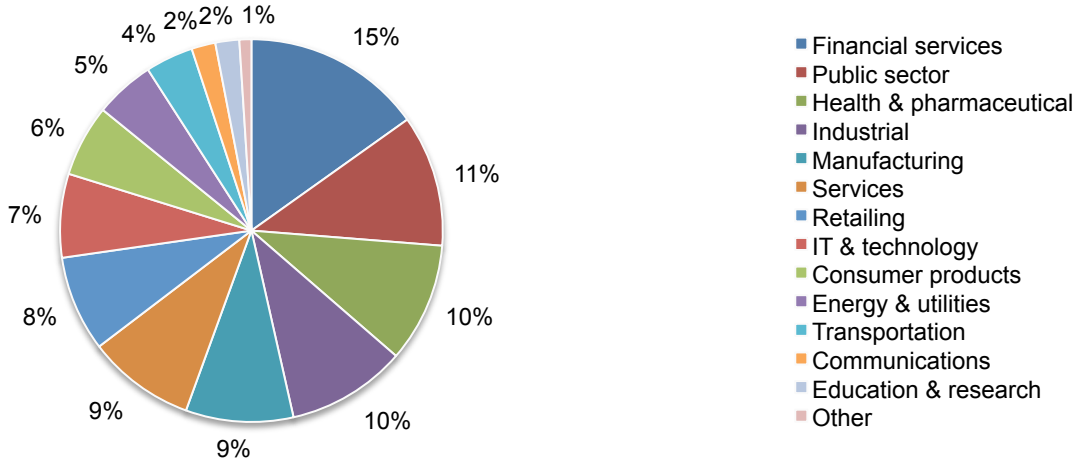
Pie Chart 1 summarizes the approximate position levels of respondents in our study. As can be seen, the majority of respondents (58 percent) are at or above the supervisory level.

**Pie Chart 1. Distribution of respondents according to position level**



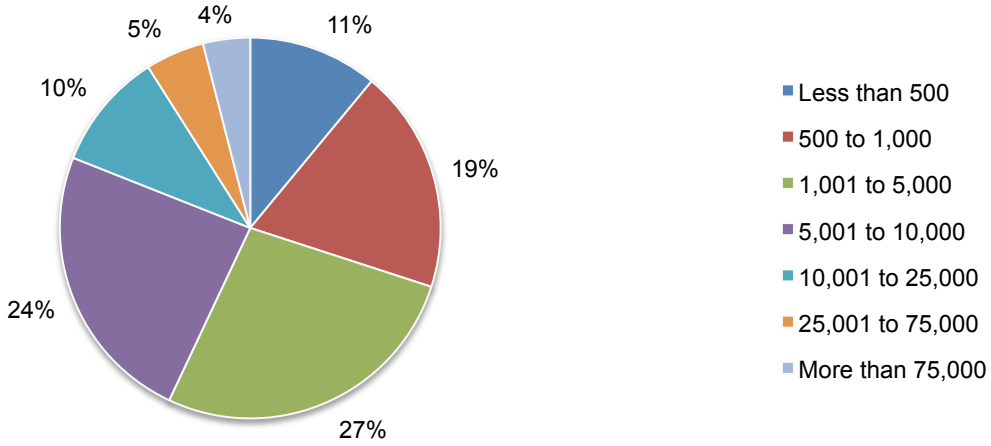

Pie Chart 2 reports the primary industry sector of respondents' organizations. This chart identifies financial services (15 percent) as the largest segment, followed by public sector (11 percent), health & pharmaceuticals (10 percent) and industrial (10 percent).

**Pie Chart 2. Primary industry classification**



According to Pie Chart 4, the majority of respondents (70 percent) are from organizations with a global headcount of more than a 1,000 employees.

**Pie Chart 4. Worldwide headcount of the organization**




## 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 Germany. 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 | DE |
|---|---|
| Total sampling frame | 14,005 |
| Total returns | 502 |
| Rejected or screened surveys | 57 |
| Final sample | 445 |
| Response rate | 3.18% |

**Part 1. Screening**

| S1. What best describes your organizational role or area of focus? | DE |
|---|---|
| IT security operations | 39% |
| IT operations | 37% |
| CSIRT team | 16% |
| 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. | DE |
|---|---|
| Managing budgets | 52% |
| Managing staff | 59% |
| Evaluating vendors | 45% |
| Setting priorities | 34% |
| Securing systems | 63% |
| Ensuring compliance | 48% |
| Ensuring system availability | 40% |
| None of the above (stop) | 0% |
| Total | 369% |

**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. | DE |
|---|---|
| 1 or 2 | 8% |
| 3 or 4 | 14% |
| 5 or 6 | 24% |
| 7 or 8 | 21% |
| 9 or 10 | 33% |
| Total | 100% |
| Extrapolated value | 6.64 |

| Q2. Using the following 10-point scale, please rate your organization's ability to **prevent** a cyber attack from 1 = low to 10 = high. | DE |
|---|---|
| 1 or 2 | 8% |
| 3 or 4 | 19% |
| 5 or 6 | 27% |
| 7 or 8 | 21% |
| 9 or 10 | 25% |
| Total | 100% |
| Extrapolated value | 6.22 |

| 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. | DE |
|---|---|
| 1 or 2 | 10% |
| 3 or 4 | 14% |
| 5 or 6 | 20% |
| 7 or 8 | 27% |
| 9 or 10 | 29% |
| Total | 100% |
| Extrapolated value | 6.52 |

| Q4. Using the following 10-point scale, please rate your organization's ability to **contain** a cyber attack from 1 = low to 10 = high. | DE |
|---|---|
| 1 or 2 | 7% |
| 3 or 4 | 11% |
| 5 or 6 | 19% |
| 7 or 8 | 33% |
| 9 or 10 | 30% |
| Total | 100% |
| Extrapolated value | 6.86 |

| 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. | DE |
|---|---|
| 1 or 2 | 6% |
| 3 or 4 | 11% |
| 5 or 6 | 32% |
| 7 or 8 | 27% |
| 9 or 10 | 24% |
| Total | 100% |
| Extrapolated value | 6.54 |

| Q6. What best describes the maturity level of your organization's **cyber security** program or activities today? | DE |
|---|---|
| Early stage – most program activities have not as yet been deployed | 10% |
| Middle stage – most program activities are only partially deployed | 26% |
| Late-middle stage – most program activities are fully deployed | 41% |
| Mature stage – all program activities are fully deployed | 23% |
| 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. | DE |
|---|---|
| Agility | 2.9 |
| Preparedness | 1.4 |
| Planned redundancies | 6.4 |
| Strong security posture | 2.5 |
| Knowledgeable or expert staff | 1.7 |
| Ample resources | 5.1 |
| Leadership | 2.4 |

| 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. | DE |
|---|---|

| | |
|---|---|
| Persistent attacks | 1.4 |
| IT system failures | 3.9 |
| Data exfiltration | 2.4 |
| Human error | 3.8 |
| Natural or manmade disasters | 4.6 |
| Third-party glitches | 3.8 |

| 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. | DE |
|---|---|
| Persistent attacks | 3.1 |
| IT system failures | 4.2 |
| Data exfiltration | 3.9 |
| Human error | 3.0 |
| Natural or manmade disasters | 5.5 |
| Third-party glitches | 2.8 |

| 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. | DE |
|---|---|
| Advanced persistent threats (APT) / targeted attacks | 51% |
| Botnet attacks | 11% |
| Clickjacking | 7% |
| Denial of services | 18% |
| Exploit of existing software vulnerability | 75% |
| General malware | 77% |
| Rootkits | 5% |
| Spear phishing | 57% |
| SQL injection | 38% |
| Web-borne malware attacks | 64% |
| Zero day attacks | 27% |
| Total | 430% |

**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. | DE |
| Strongly agree | 23% |
| Agree | 28% |
| Unsure | 33% |
| Disagree | 11% |
| Strongly disagree | 5% |
| Total | 100% |

| Q10b. My organization's leaders recognize that cyber resilience affects revenues. | DE |
|---|---|
| Strongly agree | 24% |
| Agree | 30% |
| Unsure | 32% |
| Disagree | 8% |
| Strongly disagree | 6% |
| Total | 100% |

| Q10c. My organization's leaders recognize that cyber resilience affects brand image. | DE |
|---|---|
| Strongly agree | 25% |
| Agree | 26% |
| Unsure | 35% |
| Disagree | 11% |
| Strongly disagree | 3% |
| Total | 100% |

| Q10d. In my organization, **funding** for IT security is sufficient to achieve a high level of cyber resilience | DE |
|---|---|
| Strongly agree | 26% |
| Agree | 30% |
| Unsure | 34% |
| Disagree | 5% |
| Strongly disagree | 5% |
| Total | 100% |

| Q10e. In my organization, **staffing** for IT security is sufficient to achieve a high level of cyber resilience | DE |
|---|---|
| Strongly agree | 20% |
| Agree | 27% |
| Unsure | 38% |
| Disagree | 7% |
| Strongly disagree | 8% |
| Total | 100% |

| Q10f. In my organization, disruption to business processes or IT services caused by cyber security breaches are rare events. | DE |
|---|---|
| Strongly agree | 14% |
| Agree | 16% |
| Unsure | 17% |
| Disagree | 37% |
| Strongly disagree | 16% |
| Total | 100% |

**Part 4. Cyber Resilience**

| Q11. What factors justify the funding of your organization's IT security? Please select your top two choices. | DE |
|---|---|
| System or application downtime | 66% |
| Information loss or theft | 35% |
| Performance degradation | 10% |
| Productivity loss | 7% |
| Revenue decline | 6% |
| Reputation damage | 18% |
| Customer defection | 10% |
| Compliance/regulatory failure | 46% |
| Other (please specify) | 2% |
| 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 | DE |
| Very important | 11% |
| Important | 37% |
| Not important | 52% |
| Total | 100% |

| Q12b. Maximizing customer acquisition | DE |
|---|---|
| Very important | 9% |
| Important | 42% |
| Not important | 49% |
| Total | 100% |

| Q12c. Minimizing non-compliance with laws | DE |
|---|---|
| Very important | 55% |
| Important | 40% |
| Not important | 5% |
| Total | 100% |

| Q12d. Maximizing employee productivity | DE |
|---|---|
| Very important | 12% |
| Important | 54% |
| Not important | 34% |
| Total | 100% |

| Q12e. Increasing revenues and positive cash flow | DE |
|---|---|
| Very important | 13% |
| Important | 41% |
| Not important | 46% |
| Total | 100% |

| Q12f. Expanding into new global markets | DE |
|---|---|
| Very important | 8% |
| Important | 25% |
| Not important | 67% |
| Total | 100% |

| Q12e. Protecting intellectual property | DE |
|---|---|
| Very important | 76% |
| Important | 15% |
| Not important | 9% |
| Total | 100% |

| Q12f. Enhancing brand value and reputation | DE |
|---|---|
| Very important | 21% |
| Important | 39% |
| Not important | 40% |
| 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. | DE |
|---|---|
| Business continuity manager | 8% |
| Disaster recovery manager | 4% |
| IT risk management leader | 7% |
| Business unit leader | 20% |
| Chief executive officer (CEO) | 8% |
| Chief financial officer (CFO) | 0% |
| Chief information officer (CIO) | 13% |
| Chief technology officer (CTO) | 6% |
| Chief marketing officer (CMO) | 0% |
| Chief risk officer (CRO) | 3% |
| Chief information security officer (CISO) | 10% |
| Chief digital officer (CDO) | 0% |
| Compliance leader | 5% |
| Internal audit director | 1% |
| General counsel | 2% |
| No one person has overall responsibility | 13% |
| Total | 100% |

| Q13b. Who has **"influence"** over your organization's efforts to ensure a high level of cyber resilience? Please check three top choices. | DE |
|---|---|
| Business continuity manager | 12% |
| Disaster recovery manager | 2% |
| IT risk management leader | 6% |
| Business unit leader | 36% |
| Chief executive officer (CEO) | 49% |
| Chief financial officer (CFO) | 7% |
| Chief information officer (CIO) | 57% |
| Chief technology officer (CTO) | 17% |
| Chief marketing officer (CMO) | 1% |
| Chief risk officer (CRO) | 9% |
| Chief information security officer (CISO) | 41% |
| Chief digital officer (CDO) | 5% |
| Compliance leader | 27% |
| Internal audit director | 6% |
| General counsel | 25% |
| Total | 300% |

| Q14. What one statement best describes how various functions within your organization work together to support a high level of cyber resilience? | DE |
|---|---|
| Collaboration is excellent | 24% |
| Collaboration is adequate, but can be improved | 57% |
| Collaboration is poor or non-existent | 19% |
| Total | 100% |

| Q15. Please check one statement that best describes your organization's cyber security incident response plan (CSIRP). | DE |
|---|---|
| We have a well-defined CSIRP that is applied consistently across the entire enterprise | 21% |
| We have a well-defined CSIRP, but is not applied consistently across the enterprise | 27% |
| Our CSIRP is informal or "ad hoc" | 31% |
| We don't have a CSIRP | 21% |
| 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. | DE |
|---|---|
| Lack of funding | 27% |
| Lack of leadership | 33% |
| Lack of expert or knowledgeable staff | 26% |
| Lack of enabling technologies | 23% |
| Silos and turf issues | 38% |
| Insufficient planning and preparedness | 69% |
| Insufficient risk awareness, analysis and assessments | 45% |
| Complexity of business processes | 45% |
| Complexity of IT processes | 39% |
| Interconnected business and IT processes with partners, vendors and other third parties | 23% |
| Emergence of disruptive technologies including mobility, cloud, virtualization and others | 30% |
| Other (please specify) | 2% |
| 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 | DE |
| Essential | 12% |
| Very important | 25% |
| Important | 30% |
| Not important | 15% |
| Irrelevant | 18% |
| Total | 100% |

| Q17b. Provide advance warning about threats and attackers | DE |
|---|---|
| Essential | 30% |
| Very important | 37% |
| Important | 20% |
| Not important | 10% |
| Irrelevant | 3% |
| Total | 100% |

| Q17c. Enable adaptive perimeter controls | DE |
|---|---|
| Essential | 11% |
| Very important | 21% |
| Important | 29% |
| Not important | 25% |
| Irrelevant | 14% |
| Total | 100% |

| Q17d. Provide intelligence about the threat landscape | DE |
|---|---|
| Essential | 19% |
| Very important | 37% |
| Important | 25% |
| Not important | 13% |
| Irrelevant | 6% |
| Total | 100% |

| Q17e. Enable efficient patch management | DE |
|---|---|
| Essential | 19% |
| Very important | 29% |
| Important | 39% |
| Not important | 11% |
| Irrelevant | 2% |
| Total | 100% |

| Q17f. Capture information about attackers (honey pot/hack back) | DE |
|---|---|
| Essential | 8% |
| Very important | 18% |
| Important | 35% |
| Not important | 31% |
| Irrelevant | 8% |
| Total | 100% |

| Q17g. Prioritize threats, vulnerabilities and attacks | DE |
|---|---|
| Essential | 16% |
| Very important | 29% |
| Important | 39% |
| Not important | 13% |
| Irrelevant | 3% |
| Total | 100% |

| Q17h. Control over insecure mobile devices including BYOD | DE |
|---|---|
| Essential | 25% |
| Very important | 32% |
| Important | 29% |
| Not important | 10% |
| Irrelevant | 4% |
| Total | 100% |

| Q17i. Limit insecure devices from accessing security systems | DE |
|---|---|
| Essential | 27% |
| Very important | 25% |
| Important | 36% |
| Not important | 7% |
| Irrelevant | 5% |
| Total | 100% |

| Q17j. Effort to reduce footprint of sensitive or confidential data | DE |
|---|---|
| Essential | 18% |
| Very important | 28% |
| Important | 35% |
| Not important | 11% |
| Irrelevant | 8% |
| Total | 100% |

| Q17k. Curtail unauthorized sharing of sensitive or confidential data | DE |
|---|---|
| Essential | 10% |
| Very important | 26% |
| Important | 38% |
| Not important | 17% |
| Irrelevant | 9% |
| Total | 100% |

| Q17l. Curtail unauthorized access to sensitive or confidential data and mission-critical applications | DE |
|---|---|
| Essential | 19% |
| Very important | 36% |
| Important | 34% |
| Not important | 9% |
| Irrelevant | 2% |
| Total | 100% |

| Q17m. Curtail end-user access to insecure Internet sites and web applications | DE |
|---|---|
| Essential | 24% |
| Very important | 28% |
| Important | 32% |
| Not important | 12% |
| Irrelevant | 4% |
| Total | 100% |

| Q17n. Control endpoints and mobile connections | DE |
|---|---|
| Essential | 23% |
| Very important | 26% |
| Important | 30% |
| Not important | 17% |
| Irrelevant | 4% |
| Total | 100% |

| Q17o. Limit the loss or theft of portable data-bearing devices such as laptops, smartphones and others | DE |
|---|---|
| Essential | 11% |
| Very important | 25% |
| Important | 37% |
| Not important | 15% |
| Irrelevant | 12% |
| Total | 100% |

| Q17p. Enable efficient backup and disaster recovery operations | DE |
|---|---|
| Essential | 34% |
| Very important | 35% |
| Important | 18% |
| Not important | 10% |
| Irrelevant | 3% |
| Total | 100% |

| Q17q. Establish metrics for upstream reporting | DE |
|---|---|
| Essential | 12% |
| Very important | 20% |
| Important | 45% |
| Not important | 15% |
| Irrelevant | 8% |
| Total | 100% |

| Q17r. Conduct surveillance of system users | DE |
|---|---|
| Essential | 8% |
| Very important | 14% |
| Important | 41% |
| Not important | 22% |
| Irrelevant | 15% |
| Total | 100% |

| Q17s. Secure access to cloud-based applications and infrastructure | DE |
|---|---|
| Essential | 22% |
| Very important | 28% |
| Important | 27% |
| Not important | 17% |
| Irrelevant | 6% |
| Total | 100% |

| Q17t. Secure data stored in clouds | DE |
|---|---|
| Essential | 21% |
| Very important | 29% |
| Important | 24% |
| Not important | 22% |
| Irrelevant | 4% |
| 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 | DE |
| Essential | 36% |
| Very important | 32% |
| Important | 23% |
| Not important | 9% |
| Irrelevant | 0% |
| Total | 100% |

| Q18b. Clearly defined IT security policies | DE |
|---|---|
| Essential | 12% |
| Very important | 25% |
| Important | 28% |
| Not important | 20% |
| Irrelevant | 15% |
| Total | 100% |

| Q18c. Backup and disaster recovery plans | DE |
|---|---|
| Essential | 37% |
| Very important | 38% |
| Important | 10% |
| Not important | 9% |
| Irrelevant | 6% |
| Total | 100% |

| Q18d. Business continuity management function | DE |
|---|---|
| Essential | 37% |
| Very important | 37% |
| Important | 11% |
| Not important | 9% |
| Irrelevant | 6% |
| Total | 100% |

| Q18e. Incident response management plan | DE |
|---|---|
| Essential | 42% |
| Very important | 34% |
| Important | 12% |
| Not important | 12% |
| Irrelevant | 0% |
| Total | 100% |

| Q18f. Background checks of system users | DE |
|---|---|
| Essential | 11% |
| Very important | 34% |
| Important | 37% |
| Not important | 12% |
| Irrelevant | 6% |
| Total | 100% |

| Q18g. Specialized training for IT security personnel | DE |
|---|---|
| Essential | 12% |
| Very important | 17% |
| Important | 39% |
| Not important | 20% |
| Irrelevant | 12% |
| Total | 100% |

| Q18h. Training and awareness activities for the organization's system users | DE |
|---|---|
| Essential | 25% |
| Very important | 33% |
| Important | 24% |
| Not important | 16% |
| Irrelevant | 2% |
| Total | 100% |

| Q18i. Monitoring of business partners, vendors and other third-parties | DE |
|---|---|
| Essential | 27% |
| Very important | 29% |
| Important | 23% |
| Not important | 13% |
| Irrelevant | 8% |
| Total | 100% |

| Q18j. Internal or external audits of security and IT compliance practices | DE |
|---|---|
| Essential | 6% |
| Very important | 18% |
| Important | 29% |
| Not important | 26% |
| Irrelevant | 21% |
| Total | 100% |

| Q18k. Segregation of duties between IT and business functions | DE |
|---|---|
| Essential | 5% |
| Very important | 16% |
| Important | 24% |
| Not important | 33% |
| Irrelevant | 22% |
| Total | 100% |

| Q18l. Risk assessment to evaluate IT security posture | DE |
|---|---|
| Essential | 29% |
| Very important | 34% |
| Important | 19% |
| Not important | 16% |
| Irrelevant | 2% |
| Total | 100% |

| Q18m. Adherence to standardized security requirements (ISO, NIST, others) | DE |
|---|---|
| Essential | 26% |
| Very important | 39% |
| Important | 19% |
| Not important | 15% |
| Irrelevant | 1% |
| Total | 100% |

| Q18n. Appointment of a high-level security leader (CSO or CISO) with enterprise-wide responsibility | DE |
|---|---|
| Essential | 19% |
| Very important | 36% |
| Important | 21% |
| Not important | 16% |
| Irrelevant | 8% |
| Total | 100% |

| Q18o. Appointment of high-level leader (CPO) accountable for information protection and privacy | DE |
|---|---|
| Essential | 20% |
| Very important | 36% |
| Important | 29% |
| Not important | 10% |
| Irrelevant | 5% |
| Total | 100% |

| Q18p. Upstream communication channel from the security leader to the CEO and board of directors | DE |
|---|---|
| Essential | 14% |
| Very important | 26% |
| Important | 25% |
| Not important | 25% |
| Irrelevant | 10% |
| Total | 100% |

| Q18q. Creation of a security program charter approved by executive management | DE |
|---|---|
| Essential | 8% |
| Very important | 16% |
| Important | 26% |
| Not important | 36% |
| Irrelevant | 14% |
| Total | 100% |

| Q18r. Regularly scheduled presentation on the state of security to the board of directors | DE |
|---|---|
| Essential | 13% |
| Very important | 29% |
| Important | 27% |
| Not important | 27% |
| Irrelevant | 4% |
| Total | 100% |

| Q18s. Process for self-reporting compliance violations to appropriate authorities | DE |
|---|---|
| Essential | 6% |
| Very important | 15% |
| Important | 24% |
| Not important | 40% |
| Irrelevant | 15% |
| Total | 100% |

| Q18t. Purchase of cyber liability insurances | DE |
|---|---|
| Essential | 18% |
| Very important | 23% |
| Important | 16% |
| Not important | 30% |
| Irrelevant | 13% |
| Total | 100% |

| Q18u. Metrics to evaluate the efficiency and effectiveness of IT security operations | DE |
|---|---|
| Essential | 25% |
| Very important | 28% |
| Important | 19% |
| Not important | 18% |
| Irrelevant | 10% |
| 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**? | DE* |
|---|---|
| < $1 million | 0% |
| $1 to 5 million | 9% |
| $6 to $10 million | 26% |
| $11 to $15 million | 41% |
| $16 to $20 million | 9% |
| $21 to $25 million | 8% |
| $26 to $50 million | 4% |
| > $50 million | 3% |
| Total | 100% |
| Extrapolated value ($millions) | $14.5 |
| *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? | DE |
|---|---|
| < 2% | 0% |
| 2% to 5% | 2% |
| 6% to 10% | 9% |
| 11% to 20% | 34% |
| 21% to 30% | 32% |
| 31% to 40% | 15% |
| 41% to 50% | 6% |
| 51% to 60% | 1% |
| 61% to 70% | 1% |
| 71% to 80% | 0% |
| 81% to 90% | 0% |
| 91 to 100% | 0% |
| Total | 100% |
| Extrapolated value (percentage) | 23% |

**Part 8. Organizational and Respondents' Demographics**

| D1. What best describes your position level within the organization? | DE |
|---|---|
| C-level executive | 3% |
| Executive/VP | 3% |
| Director | 16% |
| Manager | 17% |
| Supervisor | 19% |
| Staff/technician | 29% |
| Administrative | 6% |
| Consultant/contractor | 5% |
| Other (please specify) | 2% |
| Total | 100% |

| D2. What best describes your organization's primary industry classification? | DE |
|---|---|
| Agriculture & food services | 0% |
| Communications | 2% |
| Consumer products | 6% |
| Defense & aerospace | 0% |
| Education & research | 2% |
| Energy & utilities | 5% |
| Entertainment & media | 1% |
| Financial services | 15% |
| Health & pharmaceutical | 10% |
| Hospitality | 1% |
| Industrial | 10% |
| IT & technology | 7% |
| Logistics & distribution | 0% |
| Manufacturing | 9% |
| Public sector | 11% |
| Retailing | 8% |
| Services | 9% |
| Transportation | 4% |
| Other (please specify) | 0% |
| Total | 100% |

| D3. What range best describes the full-time headcount of your global organization? | DE |
|---|---|
| Less than 500 | 11% |
| 500 to 1,000 | 19% |
| 1,001 to 5,000 | 27% |
| 5,001 to 10,000 | 24% |
| 10,001 to 25,000 | 10% |
| 25,001 to 75,000 | 5% |
| More than 75,000 | 4% |
| Total | 100% |
| Extrapolated value (headcount) | 10,230 |

**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.