KASPERSKY lab

What It Takes to Be a CISO: Success and Leadership in Corporate IT Security

www.kaspersky.com
#truecybersecurity

Contents

What It Takes to Be a CISO: Success and Leadership in Corporate IT Security

Introduction

As it becomes increasingly critical for businesses to stay connected to their ecosystems, their reliance on IT rises. The role of the Chief Information Security Officer (CISO) therefore also grows in importance.

But what makes a CISO successful? What does a typical CISO profile look like? Is the typical CISO part of the board? How is IT security structured?

This study "The Chief Information Security Officer Survey 2018" seeks to answer these questions, and more. Carried out by PAC on behalf of Kaspersky Lab, it analyzes the status quo and future developments worldwide with regard to the CISO's role and organization. It is based on a CATI survey of 250 companies around the world with CISOs or their equivalent, as well as 11 expert interviews. This study is the first of its kind, was completed in summer 2018, and will be repeated on an annual basis.

Key findings – take-aways

Professional qualifications and certifications are important

CISOs should make sure that they and their key employees have at least basic formal professional qualifications, e.g. CISSP (46% of the CISOs) or CISM (37% of the CISOs), as well as the certifications that accompany the tools and solutions used. For example, an ISO 27001 certification of the department/company can help during budget negotiations as well as for compliance issues.

Most CISOs are not part of the board, and only a few of them want to change that

Only 26% of CISOs surveyed are members of the board and only 25% of those not on the board think they should be. Formal board membership is one thing, another is the ability to work with different lines of business (LoBs) on specific topics and be involved at a time when direction can be given without slowing the projects down. This is not linked to a formal hierarchical position but to attitude.

Collaboration with IT and LoBs is key

IT security is rarely an isolated topic. Collaboration with IT departments is essential, but cooperation with other LoBs is also crucial and should not be limited to concrete projects in which IT security-related compliance rules and policies need to be met – it should also happen during daily business. The more normal the interaction between IT security and the LoBs, the better the collaboration will work during projects and in cases where IT security has to get involved with a live project.

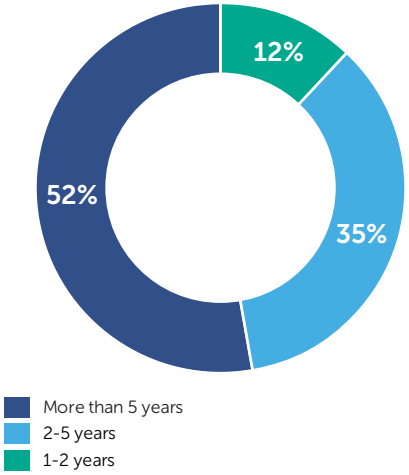
Budgeting: regulations have a growing impact on budget processes

ROI calculations are not necessarily the best way to justify budgets and essential projects, as they are usually complex and depend heavily on weak assumptions, making them hard to defend. More persuasive are evaluations of damage done to the company by past attacks. Presenting arguments related to mandatory regulations is even better, and already done by 38% of CISOs.

Tech trends and technologies: adaptation is critical

Even though most CISOs are not part of the IT department, they should have a clear opinion on tech trends as well as the impact that major new technologies (that are already available or on their way to maturity) are having on IT security. For example, quantum computing, which is currently not much more than scientific research, will change encryption as we know it completely, possibly in the next two years, but most probably in five to 10 years.

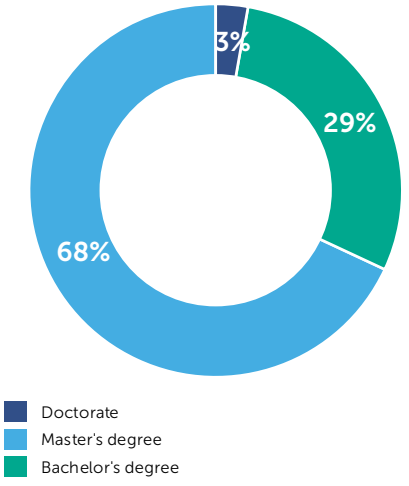
How long have you been in your current position?



"I have an MBA, which was sponsored by my previous organization. Overall, I have more than 15 years of experience in this field. I have the relevant security certifications such as CISM, CISSP, and in the area of project management PMP, Prince2, Six Sigma, ITIL. On the technical side, I have Microsoft certifications."

(CISO at an IT services provider, UK)

What is your highest educational qualification?



The CISO profile and role: in the driving seat for IT security

The role of a CISO embraces information security in its entirety, across the enterprise and its ecosystem. Accordingly, CISOs should collaborate with all departments and, of course, IT, in all IT-related projects. Cybersecurity managers must have the capacity to enforce their policies and have influence over other senior managers, including those working in IT. To do so, the CISO must be at senior management level.

Most CISOs fulfill the following tasks:

- Development and definition of security-relevant, business-specific objectives, threats and risks, as well as the resulting security goals
- Establishment and operation of an organizational unit to implement these security objectives
- Creation and update of processes, security manuals, and security guidelines on an organizational and technical level
- Performance of advisory role to the other business units, consulting with them, as well as with relevant external sources and experts
- Auditing of functional units on the state of implementation and further development of security regulations
- Creation of employee security awareness through training and campaigns
- Definition of security-relevant business processes and selection of security services and solutions
- Management of cybersecurity operations

Qualifications and experience

In order to fulfill the Chief Information Security Officer position, the CISO must know the company's processes, internal culture, and key employees, and be involved in all projects that might influence the security exposure of the company. The results seem to indicate it is an advantage to have a CISO who has has been in place for a while. We cannot formally establish a causal relationship, but this can be seen in the survey as well. 52% of the CISOs surveyed have been in their position for more than 5 years, with only 12% stating 1-2 years. Differences between the regions are noticeable, but follow the same trend. In North America 64% of the CISOs have held their position for more than five years, while in the Middle East & Africa it is only 33% (53% have held their position for two to five years). Another trend is that the larger the company, the greater the number of CISOs who have held their position for more than five years. An important point: 64% of CISOs who have held their position for more than five years think they are adequately involved in business decision-making, while 36% of CISOs who have held their position for that length of time do not share this impression. From this it can be deduced that experience on the job leads to more involvement, and that for most cybersecurity professionals, experience is key.

From an academic point of view, most CISOs surveyed (68%) hold a master's degree. The longer the CISOs surveyed have held their current position, the more likely they are to have a master's degree. The shorter the time in their current position, the more likely they are to have a bachelor's degree. Consequently, it appears that the minimum qualification for this position has been lowered recently due to a scarcity of talent. Only small differences in terms of academic qualification can be found when it comes to involvement in business decisions.

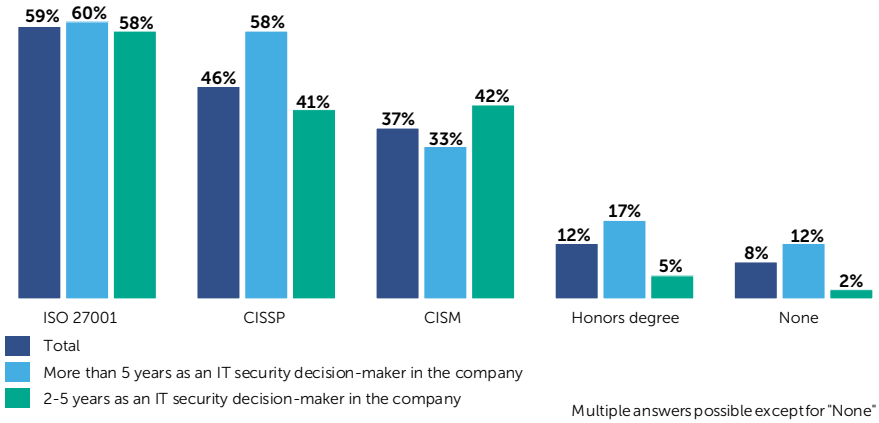
11%
of European CISOs surveyed hold a doctorate; in North America, none do.

50%
of CISOs surveyed from the CIS region hold a bachelor's degree.

Only 46% of the CISOs surveyed hold any formal professional qualification. The lowest level can be found in the Middle East & Africa (33%), the highest in CIS (60%). The most important professional qualifications are ISO 27001 (although this is not a personal qualification, the CISO as the top security manager plays a vital role in the certification process), Certified Information Systems Security Professional (CISSP), and Certified Information Security Manager (CISM). According to the survey results, long-term CISOs are more likely to be CISSP-certified than the more recent CISOs, while CISM certifications are less common. Both CISSP and CISM require theoretical IT security knowledge and practical experience in the field of IT security.

A recent development observed by PAC is that CISOs increasingly hold an MBA in addition to their technical degrees to be able to better understand their businesses' needs. Insights gained from these degrees help them better protect their businesses as well as better advise the board and LoBs about various business risks and impacts. This is especially true if the CISO is aiming for the board and/or for risk management roles or for the more management-oriented role of the Chief Information Security Officer.

Do you have any professional qualifications, e.g. CISSP, ISO27001?



Multiple answers possible except for "None"

The role of the CISO

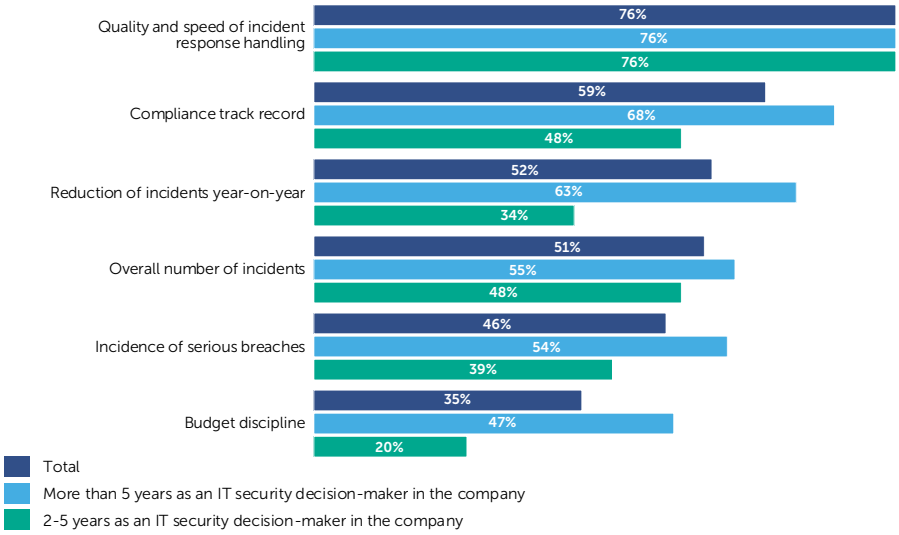
"The CISO can be a simple pawn sacrifice in the event of a breach – even if it is not their fault."

(CISO from a bank, France)

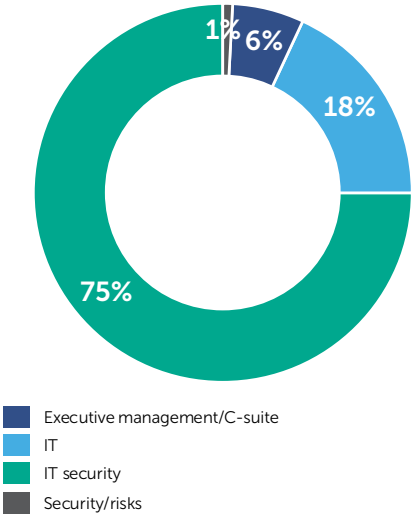
The role of the CISOs surveyed within their respective companies can be characterized based on the KPIs they are measured by, the department they are working for, and their most important tasks.

Those KPIs reflect the priorities of the CISOs: protecting the company from cyber threats and their impact, reducing vulnerabilities, addressing compliance issues, and keeping budgets on track.

How is your performance in your role measured (KPIs)?



Which of the following best describes the department you work in?



Looking at the way CISOs' performance is measured, significant differences can be seen in their KPIs, depending on the CISO's length of time in the role. It is interesting to see that shorter-tenured CISOs are rated less across all KPIs. This can be seen as an indication that, overall, they simply do not feel their job performance is really measured. Due to the business impact cybersecurity breaches now have, the quality and speed of incident response handling is very important for most of the CISOs, while track records and yearly improvements gain in importance over time. Budget discipline is clearly the least relevant KPI. Cybersecurity is now such a priority, reinforced by compliance issues that companies are less strict on spending for cybersecurity than for other IT-related projects.

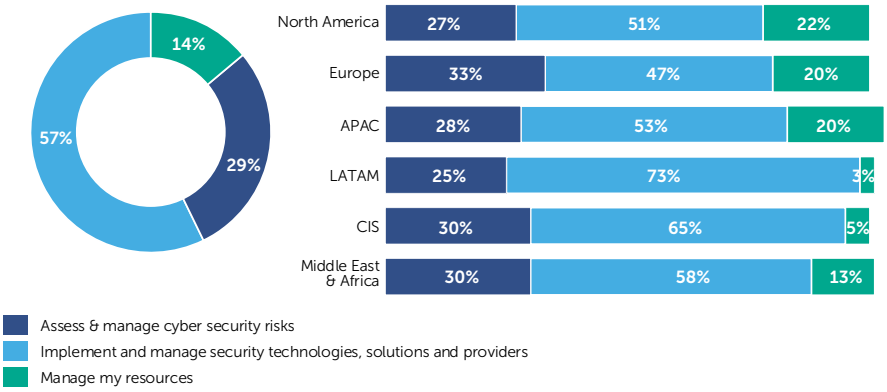
The differences between geographies are significant. For example, the quality and speed of incident response handling is a KPI for 80% of the CISOs surveyed in APAC, while only 68% of the CISOs in Latin America are measured against this KPI.

CISOs who think they are not adequately involved in business decisions are measured 9% less often against the incidence of serious breaches and 10% less against compliance track record. This seems to reflect the lower level of involvement in business decisions granted to them by their enterprise.

This can also be seen in terms of the department that CISOs surveyed are working in. 6% of CISOs are part of executive management, while 75% work in IT security. Special security/risk departments, covering IT and non-IT security matters, are still extremely rare and can only be found in APAC, CIS, and Europe, even though they are generally regarded as a cybersecurity best practice.

From an organizational point of view, having a CISO manage an IT security department is fine, but having the position at a senior executive level would be better in order to encourage their involvement and lower the risk of them being bypassed in projects and processes where cybersecurity issues are critical.

What is the most important part of your role?



"My role actually consists of one very simple paradigm: minimizing cybersecurity risks for the group. Furthermore, when it comes to the more 'human' part of my role, I'm a manager of very talented cybersecurity specialists, who are targets of multiple head hunters at the moment."

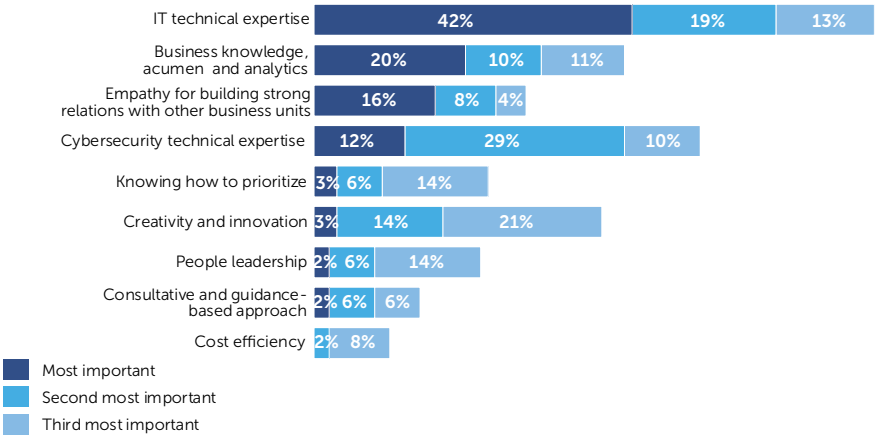
(CISO from a construction company, Switzerland)

The most important part of a CISO's role is to implement and manage security technologies, solutions, and providers. In PAC's view, CISOs do not see themselves as the typical C level executive, but as a group or department manager who is still close to the daily business and the hands-on work to be done. The differences between the observed geographies is significant, but the main trend is the same. In North America and Europe, the role is seen as a slightly more strategic.

Skills set and reasons to be a CISO

In line with the most important tasks of the CISOs surveyed, IT technical expertise is considered the top skill. Cybersecurity expertise is perceived as important, as well as business knowledge.

What are the top skills you must have to be a successful CISO? (Please select the 3 most important aspects)



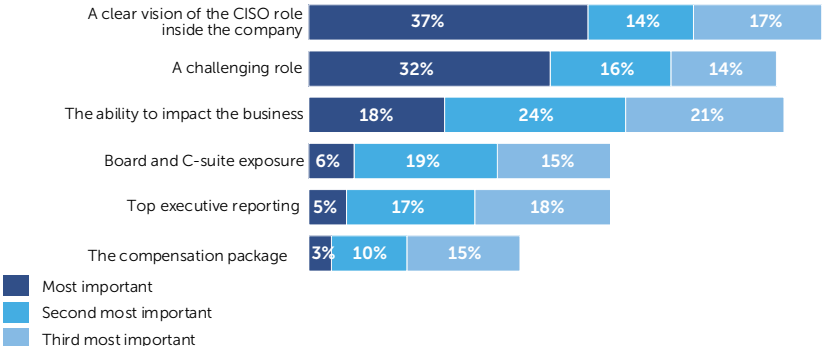
Only 2%

of the CISOs surveyed find people leadership the most important skill of a CISO. Another indication that CISOs are still more experts than managers.

The differences between the observed geographies are significant. For example, in North America, 27% of the CISOs surveyed think that cybersecurity technical expertise is most important, while in the Middle East & Africa no one selected that answer. This means that CISOs' understanding of their role is pretty diverse across the different geographies.

The reason why a potential CISO takes the role is because it is a challenging job. Most importantly, the role has to be well defined in advance. Most medium-sized and large companies know they need a CISO, but they first need to define what that person will do. There are differences between the observed geographies, but the main trends are the same. CISOs who think they are adequately involved in business decision-making ask 12% more often for a clearly defined CISO role than CISOs who do not share this view. Also, CISOs intending to increase their overall involvement with LoBs and departments ask 15% more often for a clearly defined CISO role. This reflects the higher profiles of those types of CISOs and/or the higher cybersecurity maturity of their organizations.

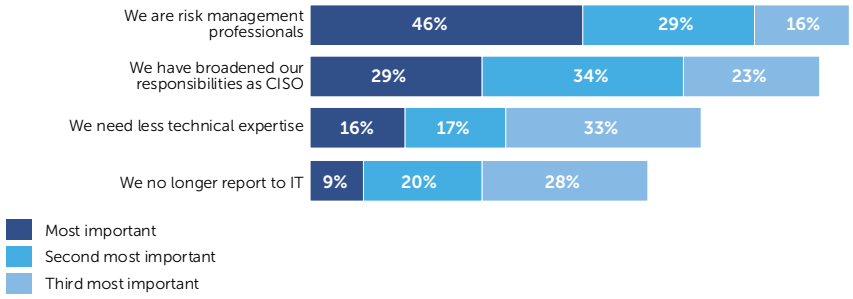
What are the top reasons for you to work in a company as CISO? (Please select the three most important aspects)



External factors impacting the CISO's role

Even though CISOs are asking for a clear vision of their role in the company, there are some changes taking place in the role and its perception. While in the early days of IT security, technical literacy was key – and is still very important – risk management is now a big part of the CISO role. In fact, the CISO is now a cyber risk manager. It is apparent, therefore, that responsibilities have been broadened and the role now requires less technical expertise.

What has changed most for CISOs in the last few years? (Please select the three most important aspects)



"The most important thing which has changed is visibility. As a cybersecurity professional, I was not really visible in my organization a few years back. Due to innovation and new technology, the game has completely changed now."

(CISO from a payment service company, India)

"Also, the complexity of our IT and OT is always worth reflecting."

(CISO from a construction company, Switzerland)

One of the best practices in cybersecurity is that the CISO does not report to the CIO. This is essentially because these two roles should be peers that both report to the CEO.

The reporting structure differs significantly by geography. In North America, only 2.2% of the CISOs surveyed find it most important to no longer report to IT, while in CIS and APAC 15% share this view. The amount of time spent in the position also has some impact on opinions here. While 5% of the CISOs surveyed who have been in their role for more than five years feel it isimportant not to report to IT, 13% of the CISOs with two to five years on the job feel that way.

In addition to internal factors, there are also external situations that put pressure on CISOs. Most important is the complexity of IT architectures, which are becoming increasingly complicated due to additional technologies and IT layers. The handling of personal data and sensitive information is also important and an increasing source of pressure due to ever stricter regulations such as NIS, GDPR, etc. In addition, the increasing number of cyberattacks puts additional pressure on the CISOs.

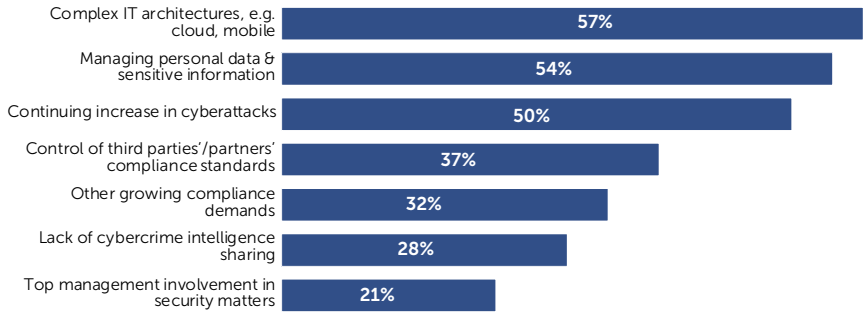
Top management involvement in security matters is considered an additional pressure by 21% of the CISOs surveyed. Usually one would assume that this involvement concerns the strategic and budgetary part of IT security (see the section IT security budgeting).

"CxO awareness is much better now than two years ago, as some executives have been fired because of the gravity of the cybersecurity issues and the arrival of GDPR."

(CISO from a bank, France)

Remarkable here are the differences between regions. While in Europe and CIS the management of personal data and sensitive information is only seen by one out of three of CISOs surveyed as the source of greatest pressure, in all other geographies two out of three CISOs specified this. Growing compliance demands are especially seen as a source of pressure in APAC.

What puts the most pressure on CISOs?



The state of IT security: cybersecurity has an increasing impact on the business, but the CISO is still not a regular member of the executive board

IT security is under a lot of pressure due to:

- the increasing openness of IT infrastructures,
- digital transformation,
- the increasing number, sophistication, and gravity of cyberattacks,
- and industry bodies and governments tightening compliance regulations.

Since essentially all business processes depend on IT systems, these security threats can potentially affect a whole company and make it liable vis-a-vis its partners and clients.

Due to the critical importance of IT security, the IT security manager should be elevated to a real, fully capacitated CISO role and be part of senior management. Unfortunately, this is still not always the case.

58%

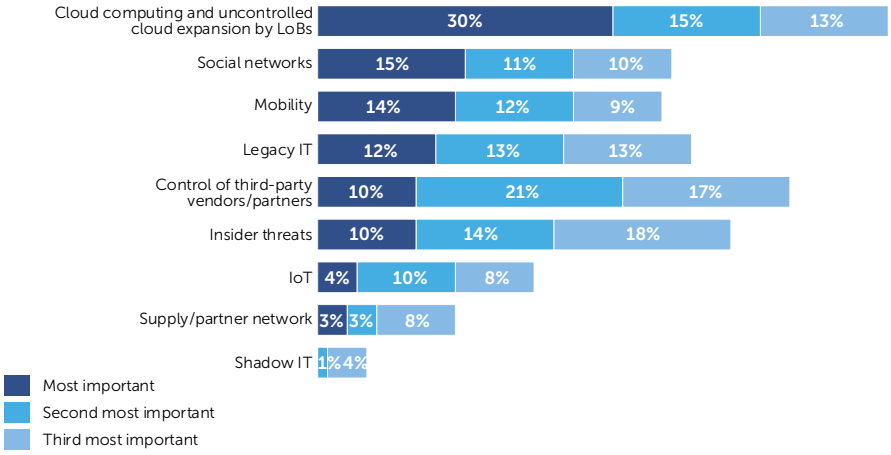
of the CISOs surveyed think cloud computing and uncontrolled cloud expansion by LoBs are important cyber-risks.

IT security risks

When it comes to IT security, there are a myriad potential risks. For the CISOs surveyed, one particular security risk is clearly the most worrying: cloud computing and uncontrolled cloud expansion by LoBs, an effect regarded as part of 'shadow IT' (even if it is not recognized as such in this survey). This is valid for all observed geographies, but especially for North America, where 36% of the CISOs surveyed selected cloud computing and cloud expansion by LoBs as the most worrying security risk – in the region that nonetheless has the highest cloud adoption rate in the world!

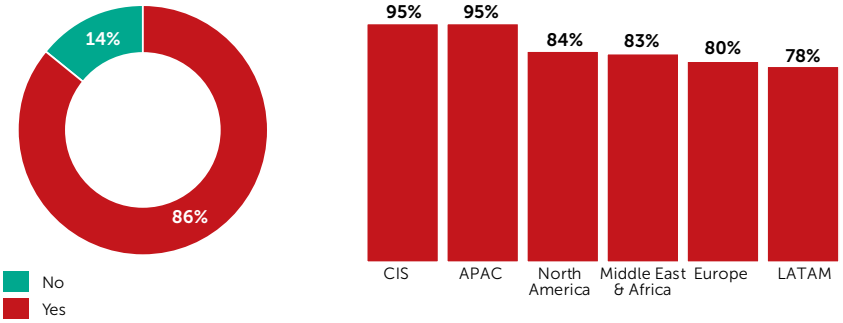
Another security risk which has often been played down in the past is that of insider threats. That is, threats by employees or third parties with access to systems who may intentionally or through negligence steal sensitive information or download malware. This worrisome security risk is mainly seen in the Middle East & Africa and Latin America, where 20% of the CISOs surveyed mention it as the number one threat, while in APAC no respondents cited this concern.

What are the top three security risks you are most worried about? (Please rank three)



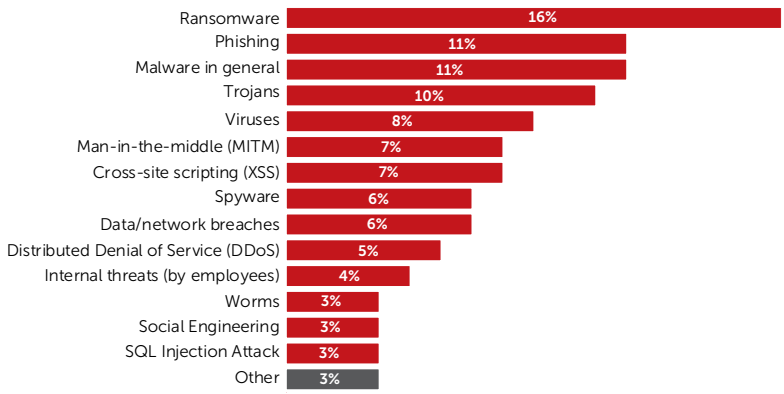
There are no 100% guarantees when it comes to IT security, and most of the CISOs surveyed think that cybersecurity breaches are inevitable. On the one hand, this is being realistic, while on the other, it shows a need to focus actions and resources on the assets which really need security.

Are cybersecurity breaches inevitable?



The differences between the observed geographies are significant, but the main trend is common. The same is valid for the different company sizes and sectors. 89% of the CISOs surveyed who intend to increase their overall involvement with LoBs and departments think that cybersecurity breaches are inevitable, while only 78% of the other CISOs share this view.

What is the most difficult type of attack to respond to?



16%

of the CISOs surveyed in North America and Europe are most worried by legacy IT security risks.

"What makes a CISO successful?

1. **That the sky does not fall on my head! I mean no successful attack that damages the company**
2. **HR management**
3. **Collaboration."**

(CISO from a construction company, Switzerland)

When it comes to specific types of attacks, WannaCry is still top of mind for many CISOs. A closer look reveals that the assessment of "which kind of attack is most difficult to respond to" is highly dependent on geography. In North America, data and network breaches are mentioned by 16% of the CISOs surveyed. In Europe, viruses are top with 21% of the CISOs mentioning them. In APAC (16%) and CIS (28%) it is ransomware, while in Latin America it is malware in general and Trojans, both 18%. In the Middle East & Africa, malware in general and phishing are top with 18% of the CISOs mentioning these topics.

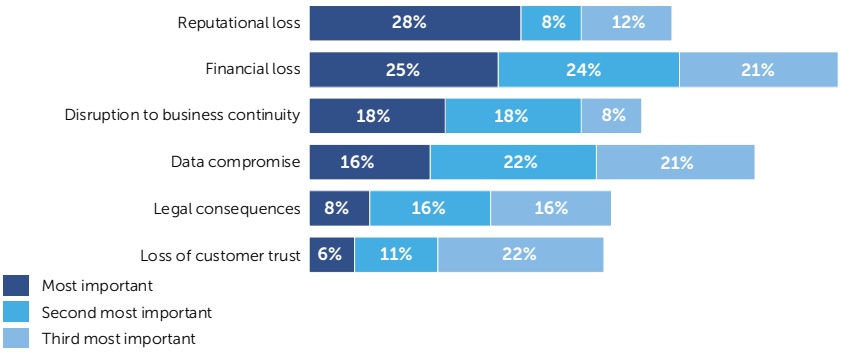
The whole organization is affected

When it comes to the consequences of security breaches, two connected questions come to mind. What are the biggest risks to the organization after a breach and to whom can these breaches be attributed?

The biggest risks to an organization after a breach can be divided into two groups. The external consequences such as reputational loss, financial loss, legal consequences etc., and the internal consequences such as the impact on business continuity.

Again, the assessment of the biggest risks is highly dependent on geography. While in North America (27% of the CISOs surveyed) and CIS (50%) financial losses are seen as the biggest risk, in Europe (27%), APAC (35%), Latin America (35%), and the Middle East & Africa (35%), it is reputational loss (27%).

What are the biggest risks to the organization after a breach? (Please rank three)



CISOs' perceptions of the biggest IT security risks to their organizations in terms of attribution are very clear and consistent across geography, company size, and observed sectors.

40%

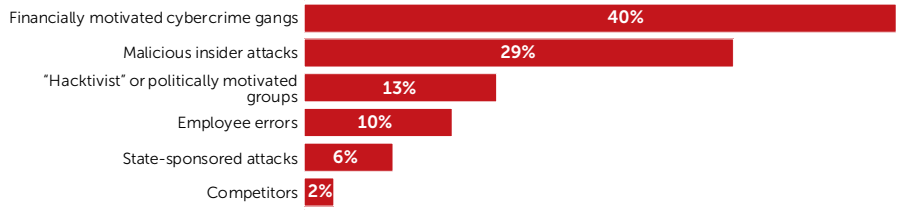
of the CISOs surveyed perceive financially motivated cybercrime gangs as the biggest IT security risk to their organization.

Financially motivated cybercrime gangs are the biggest security risk in terms of attribution according to 40% of the CISOs surveyed. These groups are usually highly motivated, professional, well equipped, and trained for what they are being paid to do – either hampering business operations or stealing information for financial gain.

Almost one third of the CISOs surveyed think that malicious insider attacks are the biggest security risk in terms of attribution. These groups of insiders can either be paid by an external party or be acting on their own initiative for some personal motive.

Hacktivists are considered to be especially relevant in Latin America (23%), but not in CIS and the Middle East & Africa (both 8%).

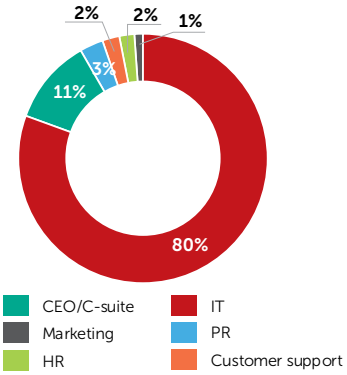
What do you perceive as the biggest IT security risks to your organization in terms of attribution?

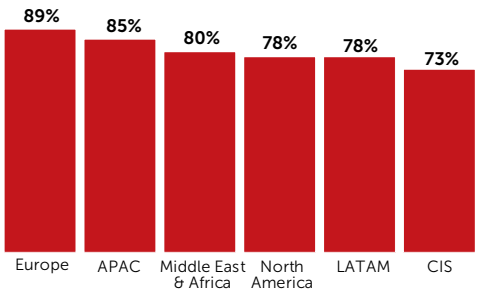


The command structure

Although most CISOs do not report to IT anymore, if things go wrong IT is the first department to be informed. The reasons for this are manifold. Firstly, IT is the most affected. Secondly, it is also the IT department that needs to stop the threat from spreading in some cases, while security operations usually need a certain degree of support from IT. The significance of the other departments depends on geography. While the C-suite is not usually first in line to be informed in North America (7%) and Europe (4%), it is more likely to be so in Latin America (15%) and CIS (23%). While nobody in Europe would inform PR in the first instance, 5% of the CISOs would do it in APAC.

After a security breach, which department do you inform first?





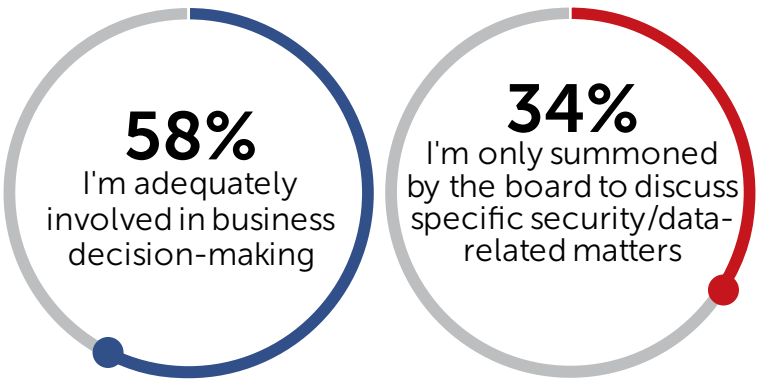
The influence of the CISO in the organization

In order to adequately fulfill the IT security mission at all levels, the CISO and their organization should be involved in all business decisions and resulting projects in order to influence processes and technologies early enough to find the most secure ways to perform a given task. For that to happen, it is important for a CISO to be involved in business decision-making processes.

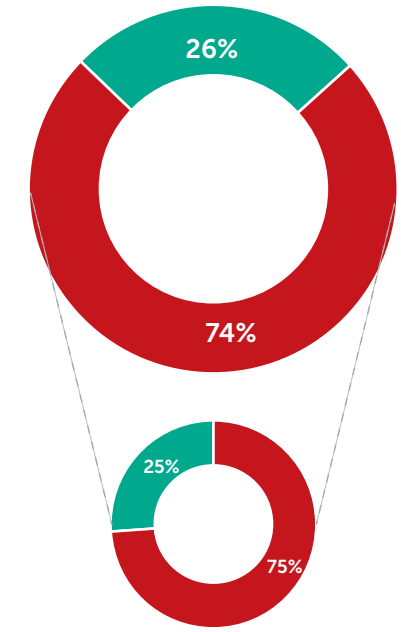
"I am very much involved in implementing security strategies within my organization, and also I am very much involved with the board as well for implementing different strategies. When it comes to influencing the board regarding the implementation of certain technology in the organization, then we go by the use case, sharing instances of threats which have affected other organizations as well."

(CISO from an IT service provider, USA)

How do you measure your influence in your organization?



Are you part of the board and do you attend all meetings? If you are not part of the board, do you think you should be?



Breakdown of responses from respondents who are not part of the board, in %

No
Yes

While involvement is one thing, organizational hierarchy is another topic. Usually, a Chief Information Security Officer would be expected in the C-suite alongside the CEO, COO, CFO, CMO, CIO, and other C-suite members. However, only 26% of the CISOs surveyed are part of the board and attend all meetings. Having a CISO at executive level normally only happens in highly digitalized enterprises, highly sensitive ones, and in very large organizations. This is often synonymous with high cybersecurity maturity. Only 58% of the CISOs surveyed think that they are adequately involved in business decision-making.

From a geographical perspective, there are two distinct groups: North America (40% C-suite), and then the rest of the world with much lower proportions. CIS has the lowest C-suite proportion of 5% compared to the worldwide figure. A closer look by geography shows that the CISOs in Europe (64%) and APAC (65%) are far more often adequately involved than their colleagues from North America and the Middle East & Africa (both 53%). This reveals a clear difference in CISOs' perceptions in the different geographies. While differentiation by sector is less interesting, differentiation by tenure is revealing. CISOs with more than five years on the job are much more often adequately involved (71%) than their peers with less experience on the job (47%), which is pretty normal as they usually grow their role internally. Logically, CISOs who intend to increase their overall involvement with LoBs and departments are, with 62%, more involved than their colleagues who do not (48%).

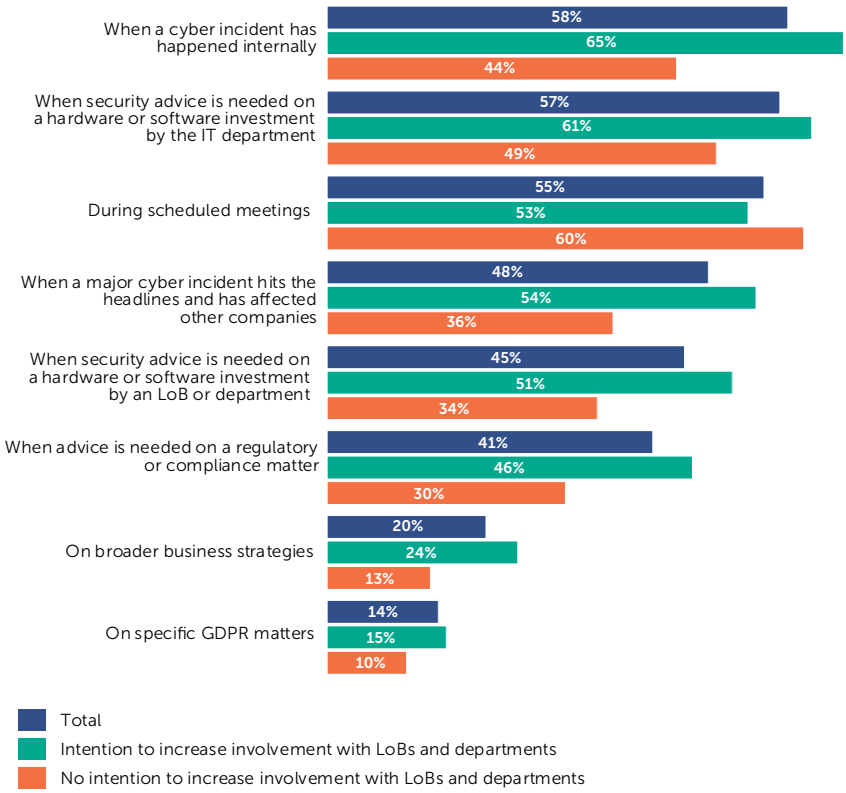
Only 25% of CISOs surveyed who are not part of the board think they should be. The others are happy with the position they currently have. In Europe, 41% of the CISOs who are not part of the board think they should be, whereas only 13% of the CISOs surveyed in CIS who are not part of the board think they should be.

One finding of this study is that a large majority of the CISOs do not see themselves as business managers, something that is normally a key part of a CxO level role, but rather as domain experts. Cybersecurity managers are among the most technical roles in the enterprise, and that is how they are evaluated. However, cybersecurity teams are growing over time and the impacts of breaches are increasingly business impacts, so we see a need for CISOs who are able to talk as equals with other CxO roles. The CISO is a relatively new role in the enterprise and mostly associated with the role of a cybersecurity manager. Yet, cybersecurity managers often struggle to rise to CISO status, as they are not trained and prepared to be in the C- suite, while others underestimate their ability to succeed in this role.

Whether they are part of the board or not, from time to time the board seeks advice from the CISO. When it comes to asking for this advice, it is interesting to note how the board treats CISOs who intend to increase their involvement with LoBs differently from those CISOs who do not.

Specifically, CISOs who want to increase their involvement with the LoBs are more often asked for advice by the board than CISOs who do not. CISOs who have a good network in their organization and are willing to work with the different LoBs are perceived as a more valuable source of advice than their peers without that level of engagement. This is a future trend in CISO profiles, as they have to be more business friendly and focus on business risks. Some major companies already have a CISO who is not from the IT department.

When does the board seek your advice?



The organization – resources, budgets, and collaboration

In order to cope with the most urgent IT security challenges, the IT security department first has to tackle the lack of resources and then improve collaboration within the IT department and with partners. Budgets are less of an issue.

Security professionals are rare and difficult to recruit

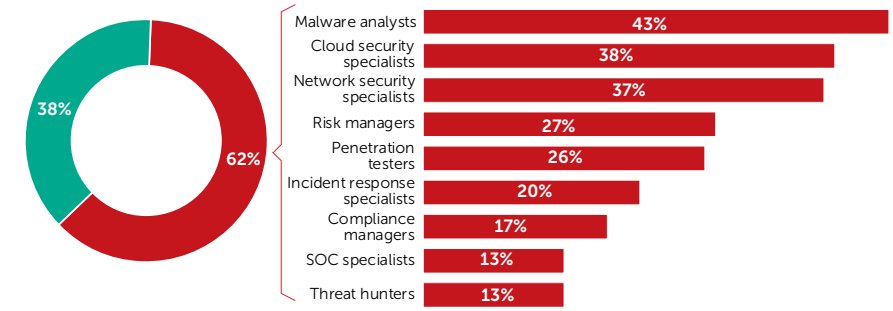
For many cybersecurity managers, this is one, if not the, key issue. All actors in the market are looking for cybersecurity resources, and this scarcity affects cybersecurity projects and makes resources ever more expensive to obtain and use.

62% of the CISOs surveyed find it hard to hire new security talent. This problem seems to be lower in North America (38%), while in CIS it is especially challenging (85%).

61%

of CISOs from APAC find it hard to source new network security talent.

Do you find it hard to source skilled cybersecurity professionals for your organization? If yes, which of the following skills are the hardest to recruit?



Breakdown of responses from companies, that find it hard to source skilled professionals, expressed in %

No
Yes

When it comes to the specific skills that are hard to recruit, the differences by geography are huge. For example, malware analysts are hard to recruit for only 24% of European CISOs, while 59% of North American CISOs experience difficulties here. When it comes to cloud security specialists, only 27% of CISOs in the Middle East & Africa find it a challenge to hire new talent, while 53% of the North American CISOs see this as an issue.

The good news – regardless of geography or industry sector (which has no significant influence anyway) – is that a significant portion of the new talent needed in the future will be in software (and those products can be sourced). In other words, artificial intelligence-based solutions will widely be deployed in the next five years to reduce the amount of standard tasks for human employees and give them time for strategic and value-creating tasks.

IT security budgeting

IT security budgeting is a bit like personal liability insurance – if nothing happens, the premium is wasted. The budgeting situation has become a little easier over the last few years with the rising number of attacks, their growing impact, the surge of compliance rules, and, last but not least, the fact that senior management could be held responsible for security breaches if they did not pay enough attention to IT security and did not allocate it enough budget.

If you do not get the budget you require, what are the reasons?

45%

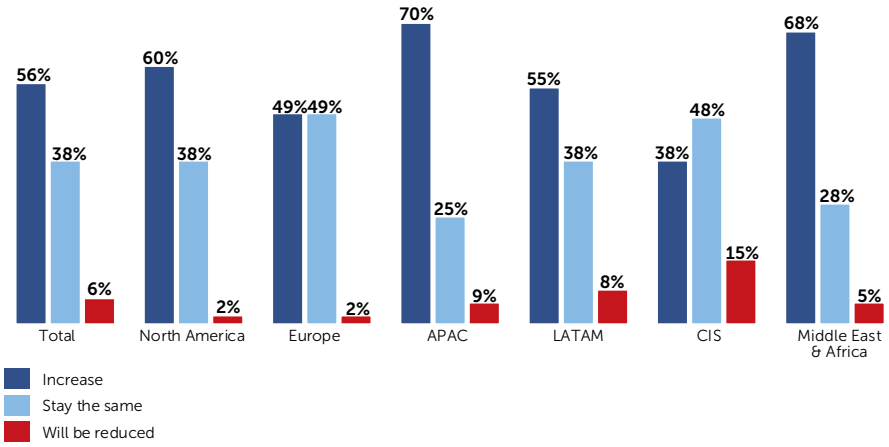
of enterprises worldwide will raise their cybersecurity budgets.

CxO 3000 Survey, PAC 2018

Nevertheless, CISOs find themselves having to fight for budgets every year. The biggest barriers to getting the right budgets apply to all geographies. The key point is that regardless of the amount of money spent on security, there will always be the risk of a security breach happening. Another approach by senior management is to include the IT security budget in the IT budget. When this happens, PAC's experience shows that IT security has to compete with IT operations for part of the budget, leading to long and usually fruitless discussions.

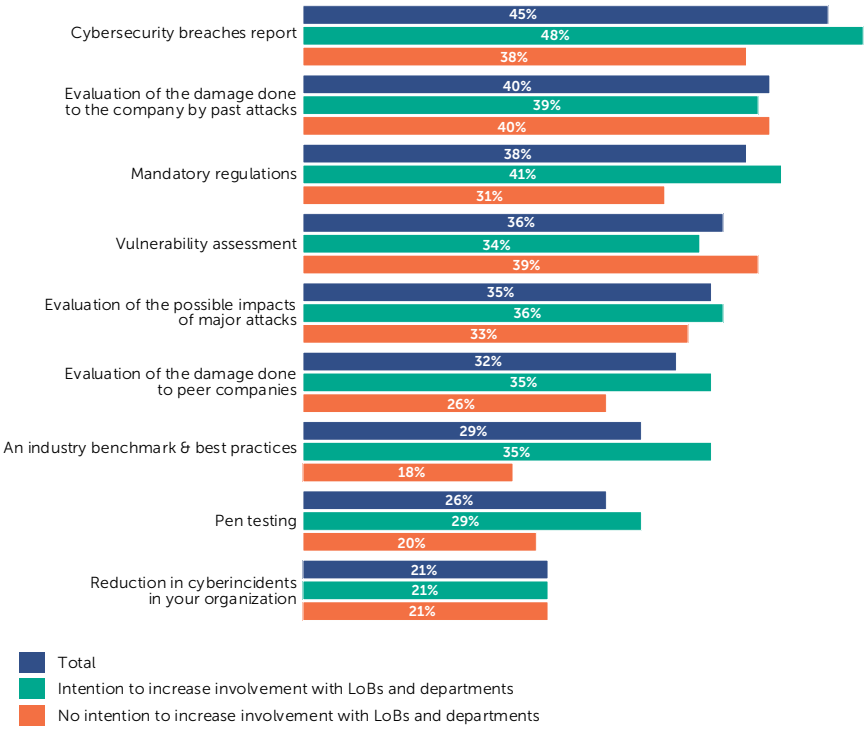
On the other hand, if we take a closer look at IT security budget developments, most CISOs manage to get increasing budgets regardless of the maturity of security markets or the economic situation in their geography. The situation is only worrisome in CIS, where 15% of the CISOs surveyed report declining budgets.

Will your IT security budget increase, stay the same or be reduced in the next financial year?



The return on investment (ROI) of IT security expenditure is always hard to argue. Most calculations include probabilities and assumptions on breaches, their damage and the costs associated with reputational losses, direct financial losses, etc. That is why many CISOs have to justify their budget without a clear ROI.

Without a clear ROI, how do you justify your budget?



"I do not lack in any authority here, and since I have been associated with this firm for quite a long time, they trust me, and I do not see any trouble in proving ROI."

(CISO from a bank, USA)

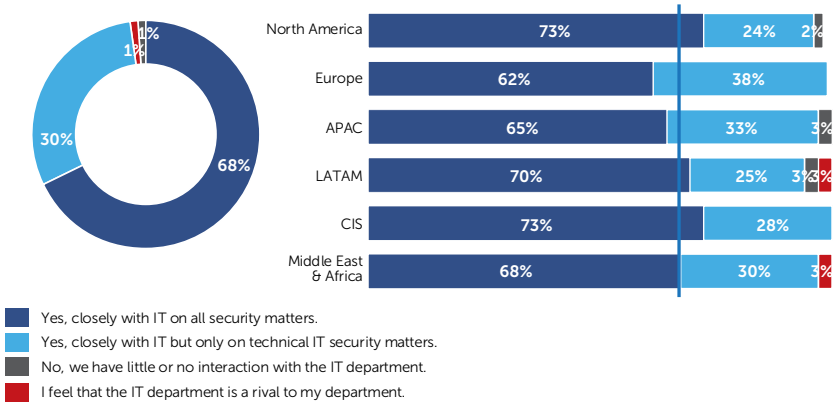
When it comes to justifying budgets, it helps to be involved with the LoBs, as it increases the CISO's standing within the company. The different means of justification heavily depend on geography and are only influenced to a limited extent by the size of the company or its sector. Cybersecurity breach reports, for example, are extensively used in Latin America and the Middle East & Africa (both 55%), North America (49%), and APAC (48%), while in CIS (38%) and Europe (27%) these are not seen as helpful. In CIS, the evaluation of the damage done to the company by past attacks is more persuasive (43%). The same applies to Europe (47%).

Relationship with the wider organization

IT security is usually closely related to IT systems and applications, as protecting them is a key IT security goal. Consequently, it is almost mandatory that IT security works closely with the IT department and with other LoBs in order to get early involvement in new processes and systems or applications.

Fortunately, practically all CISOs surveyed work closely with the IT department, either on all security matters or at least on technical IT security matters. The differences between the different geographies are negligible. It is only in Latin America and the Middle East & Africa that a few CISOs do not work with the IT department.

Do you work closely with the IT department when formulating IT security strategies, on recruitment and investment?



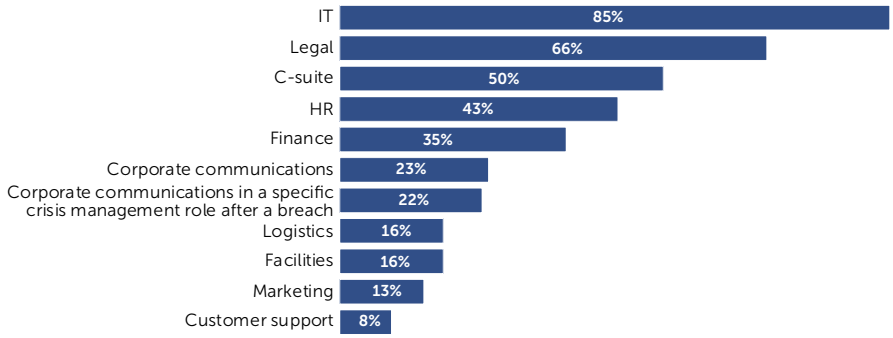
"Before introducing any new technology in any department, I conduct meetings with those departments to ensure that their changes are not going against our security norms. Then we make the required changes so as to have proper integration with our network."

(CISO from an automotive company, India)

Those CISOs with more than five years on the job work significantly more often with IT in all matters (74%) than CISOs with two to five years on the job (61%). Experience leads to more collaboration. CISOs who intend to increase their overall involvement with LoBs and departments work much more often with IT on all IT security matters (77%) than CISOs who do not. These CISOs work much more with IT on technical matters only (44%).

When it comes to IT security strategy, recruitment, or investments, IT security needs to work with other departments as well. The CISOs surveyed work most often with IT (85%), followed by Legal (66%) and the C-suite (50%). The role of the legal department has been reinforced lately by new compliance regulations. HR remains quite important as well, as the IT security department often works with HRon identity and access management.

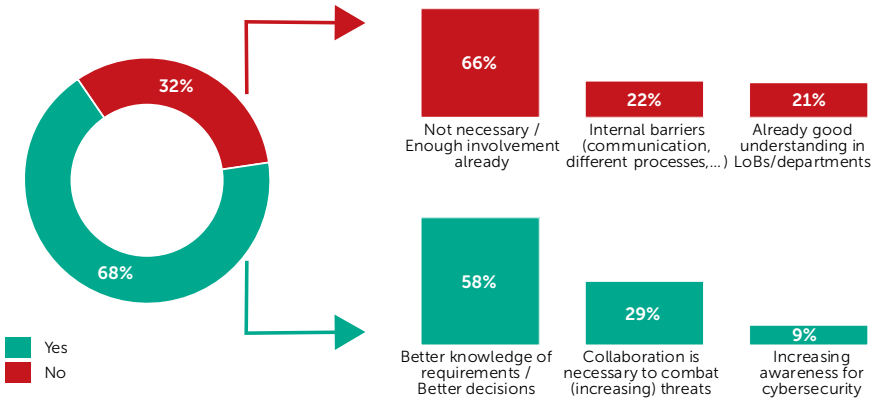
What other departments do you work closely with when formulating IT security strategies or on recruitment and investment?



Collaboration with other departments such as Logistics or Marketing falls short currently. However, two thirds of CISOs surveyed intend to increase their overall involvement with LoBs and departments, mainly to better understand their needs and make better decisions. 74% of CISOs who think that they are adequately involved in business decision-making want to increase their overall involvement with LoBs and departments even further in order to expand their knowledge in these areas.

One third of CISOs surveyed are not looking for more involvement with LoBs and departments. One out of three consider it a necessity to be able to better combat threats In all cases, more collaboration is nearly always a good idea and stands out as one of cybersecurity's best practices.

Do you intend to increase your overall involvement with LoBs and departments? Please state why.



Future trends impacting IT security

Changing environments lead to different IT architectures and applications, which in turn can affect IT security requirements and risk profiles.

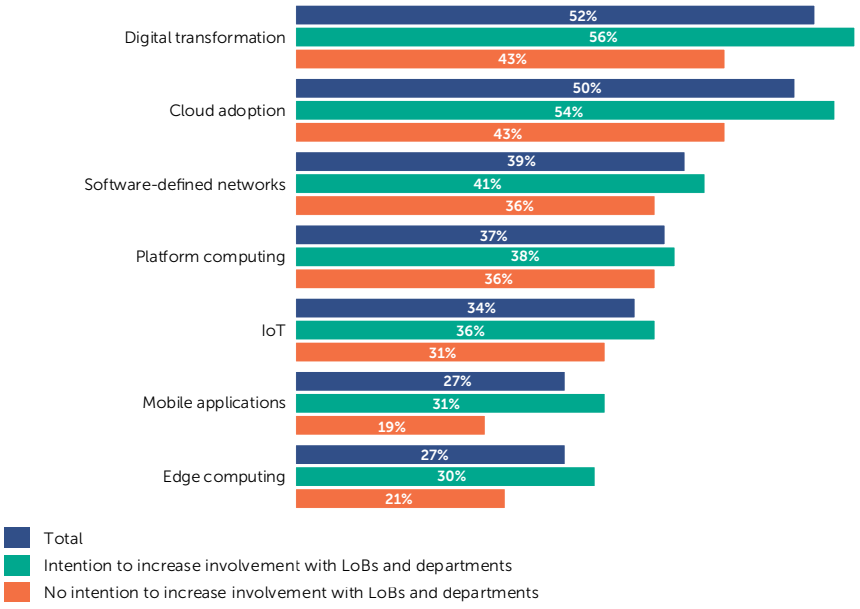
In the early days of the CISO role, when IT security was mainly part of IT, many CISOs' reactions to changes in technologies or to new ones was a simple rejection. Times, however, have changed. LoBs have to be more agile, and they have the power to pressure the IT and IT security departments into providing the environment they need (or at least think they need). Cybersecurity must accompany LoBs and new IT architectures in order to manage risks and secure operations as much as possible. At the same time, businesses have started to realize that without cybersecurity they will not succeed in their digital transformation. IT security is no longer a blockade, but rather a catalyst for digital transformation.

Digital transformation and its related IT architecture, cloud computing, seem to be the main tech trends that will have the biggest impacts on IT security. In fact, the other tech trends are ultimately also digital transformation trends (IoT, mobile applications, platform computing etc.), based on a cloud architecture, or subsets of a cloud architecture (software-defined networks, edge computing etc.).

Consequently, CISOs must have a clear picture on tech trends and their impact on the IT security of their organization over the next five years. CISOs who intend to increase their overall involvement with LoBs and departments see greater impact from the different tech trends than CISOs with no intention to increase their involvement.

Looking at the geography shows some significant differences. Digitalization is viewed as having the biggest impact in the Middle East & Africa (63% of the CISOs surveyed). IoT is not seen by North American CISOs as having a big impact, while for 50% of CISOs in APAC it is. European CISOs (16%) are relaxed when it comes to edge computing, while CISOs in the Middle East & Africa have much greater concerns about this topic. Cloud adoption has the biggest impact for APAC CISOs (73%).

Which of the following tech trends will have the biggest impact on the IT security of your organization in the next five years?



"The arrival of cloud technologies has changed a lot of stuff and we have to change our cybersecurity defenses to a defense-in-depth concept rather than perimeter security. Industry 4.0 is another cloud-related challenge that gives me headaches. Both increase complexity and make my job more difficult."

(CISO from a construction company, Switzerland)

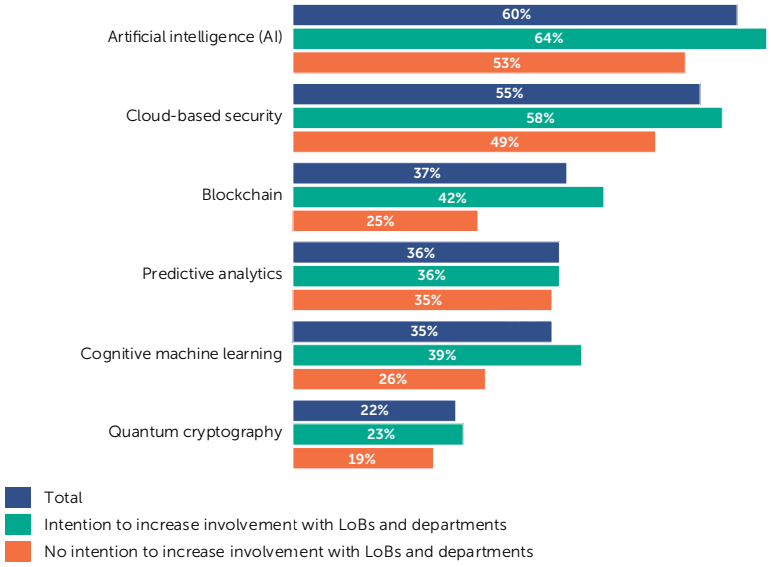
Globally, AI is leading the way. Cybersecurity happens to be one of the technology segments where the likely impact of AI will be the highest. Many users are already convinved of the benefits of e.g. behavioral/contextual analysis or machine learning, AI's main applied concepts. Cloud-based security closely follows AI, as it is one of the best ways to automate and share rare and expensive cybersecurity resources. It is also the enabling architecture for the rest of these future technologies. Blockchain, with its huge potential for securing transactions – by providing proof of authenticity – is the third technology on the podium.

Artificial intelligence is recognized as the technology with the biggest impact in Latin America, with 70% of CISOs surveyed mentioning it. In fact, PAC expects that artificial intelligence will be the leading source of innovation in the IT security software space and one of the answers to the skills shortage for the time being.

Cloud-based security is recognized as the technology with the biggest impact in APAC, with 78% of the CISOs surveyed stating this.

Blockchain is recognized as the technology with the biggest impact in Latin America, with 45% of the CISOs surveyed mentioning this.

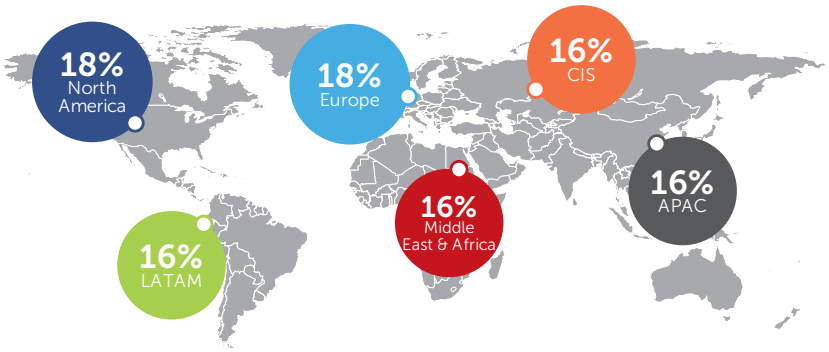
Which technology will have the biggest impact on IT security in the next five years?

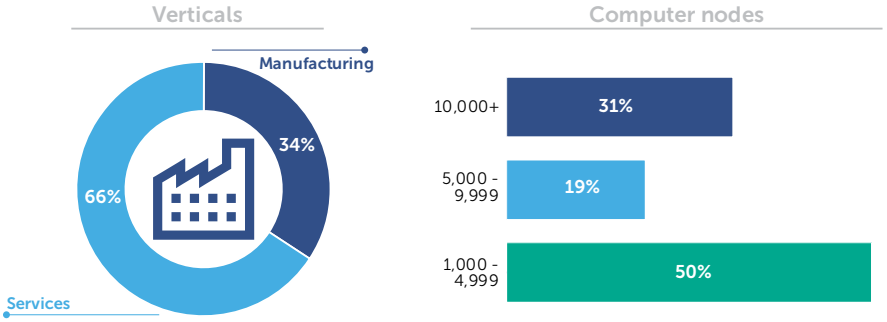


Appendix

Methodology

From May until the beginning of July, PAC interviewed 250 IT security decision-makers (CISOs, directors and heads of IT security, and others) in both the Manufacturing and Services sectors. Based on a CATI (computer-assisted telephone interview) approach, professionals from North America, Europe, APAC, LATAM, and CIS along with the Middle East & Africa took part in this study.





In addition to the quantitative study, 11 qualitative expert interviews were conducted. The quotations given within this report are an (anonymized) excerpt and are intended to substantiate study results.

Disclaimer, usage rights, independence, and data protection

The creation and distribution of this study was supported by Kaspersky Lab.

For more information, please visit www.pac-online.com.

Disclaimer

The contents of this study were compiled with the greatest possible care. However, no liability for their accuracy can be assumed. Analyses and evaluations reflect the state of our knowledge in September 2018 and may change at any time. This applies in particular, but not exclusively, to statements made about the future. Names and designations that appear in this study may be registered trademarks.

Usage rights

Independence and data protection

This study was produced by Pierre Audoin Consultants (PAC – a CXP Group Company). Kaspersky Lab had no influence on the analysis of the data and the production of the study.

The participants in the study were assured that the information they provided would be treated confidentially. No statement enables conclusions to be drawn about individual companies and no individual survey data was passed to Kaspersky Lab or any other third party. All participants in the study were selected at random. There is no connection between the production of the study and any commercial relationship between the respondents and Kaspersky Lab.

Kaspersky Lab AO
39A/3 Leningradskoe Shosse
Moscow, 125212
Russian Federation
Tel.: +7-495-797-8700
info@kaspersky.com
www.kaspersky.com

About Kaspersky Lab

Kaspersky Lab is a global cybersecurity company which has been operating in the market for over 20 years. Kaspersky Lab's deep threat intelligence and security expertise is constantly transforming into next generation security solutions and services to protect businesses, critical infrastructure, governments, and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky Lab technologies and we help 270,000 corporate clients protect what matters most to them.

Learn more at: www.kaspersky.com

Contact: info@kaspersky.com

Follow us: https://twitter.com/Kaspersky

A CXP GROUP COMPANY

PAC – a CXP Group Company
Holzstr. 26
80469 Munich, Germany
Tel.: +49 (0)89 23 23 68 0
info-germany@pac-online.com
www.pac-online.com

About PAC

Founded in 1976, Pierre Audoin Consultants (PAC) is part of CXP Group, the leading independent European research and consulting firm for the software, IT services, and digital transformation industry.

CXP Group offers its customers comprehensive support services for the evaluation, selection, and optimization of their software solutions and for the evaluation and selection of IT services providers, and accompanies them in optimizing their sourcing and investment strategies. As such, CXP Group supports ICT decision-makers in their digital transformation journey.

Further, CXP Group assists software and IT services providers in optimizing their strategies and go-to-market approaches with quantitative and qualitative analyses as well as consulting services. Public organizations and institutions equally base the development of their IT policies on our reports.

Capitalizing on 40 years of experience, based in 8 countries (with 17 offices worldwide) and with 140 employees, CXP Group provides its expertise every year to more than 1,500 ICT decision-makers and the operational divisions of large enterprises as well as mid-market companies and their providers. CXP Group consists of three branches: Le CXP, BARC (Business Application Research Center), and Pierre Audoin Consultants (PAC).

For more information please visit: www.pac-online.com

PAC's latest news: www.pac-online.com/blog

Follow us on Twitter: @CXPgroup

Kaspersky Lab
Cyber Threats News: **www.securelist.com**
IT Security News: **business.kaspersky.com/**

#truecybersecurity
#HuMachine

www.kaspersky.com