Out of the shadows: CISOs in the spotlight!

2020 CISO's role and responsibilities survey

www.pwc.lu/cyber-security

pwc

clusil
INFORMATION / SECURITY / LUXEMBOURG

Introduction

The Chief Information Security Officer (CISO) position in organisations is becoming more invaluable than ever as cyber-attacks are on the rise. The recent home-based working model of most businesses and institutions, as a result of the pandemic, has even given rise to more cyber-attacks.

Organisations need to rise to the occasion to protect their crown jewels, and this responsibility lies with the CISO to drive initiatives that will protect their organisation's information systems, raise the information security awareness of the employees and ultimately protect the company and its resources from evolving cyber risks.

In this survey, we take a closer look at the role of the CISO and more specifically at the following aspects:

- Typical profile of a CISO;
- The CISO's position and reporting line in the organisation;
- The challenges CISOs face.

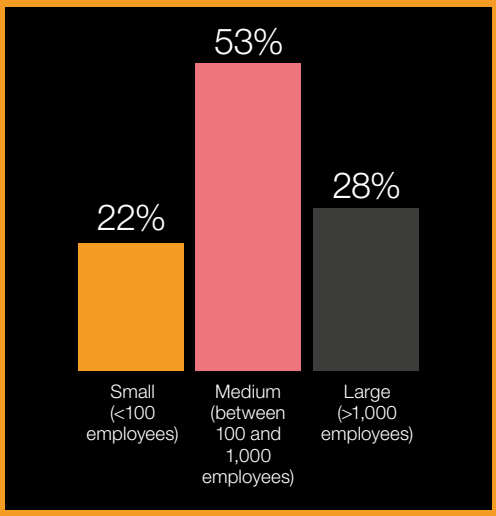
Lastly, based on our experience and best practice, we offer recommendations that would improve the overall experience of the CISO/ISO function in organisations.

The companies we surveyed

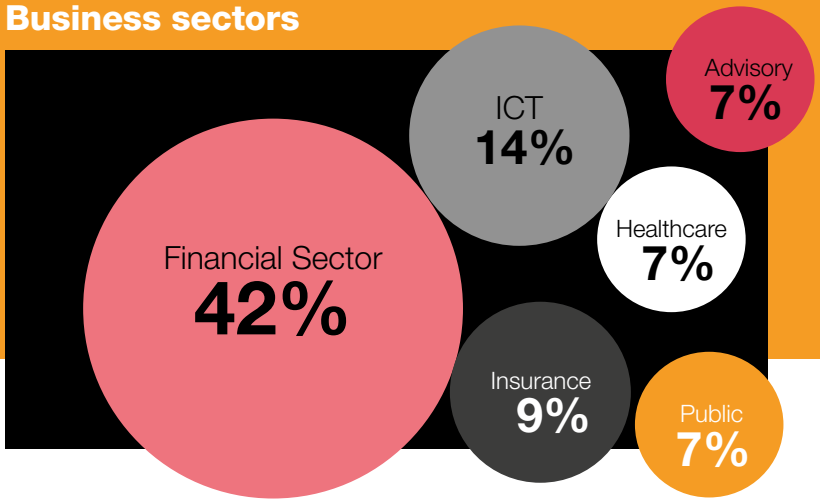
The companies that responded to this edition of our "***Out of the shadows: CISO in the spotlight***" survey, are based in Luxembourg and hence, represent the Luxembourg business landscape.

A total of 45 companies participated, out of which 53% are medium sized enterprises with less than 1000 employees. The majority (42%) of the respondent companies operate in the financial services sector. Other key business sectors such as the insurance, healthcare and public sectors are equally represented.

Company size



Business sectors



The typical CISO/ISO

77%
have a master's degree and above

Education, Skills and Experience

CISOs/ISOs in the contemporary business landscape come from diverse academic backgrounds. However, a large proportion of them will be male (91%), have a master's degree or above (77%), and possess an average of 5.6 years of experience.

Most of the CISOs/ISOs are likely to have attained industry relevant certifications such as the Certified Information Systems Security Professional (CISSP) (56%), ISO/IEC 27001 Information Security Management (54%) and Information Technology Infrastructure Library (ITIL) (37%) three of which seem to be the top industry certifications possessed by CISOs based on this survey.

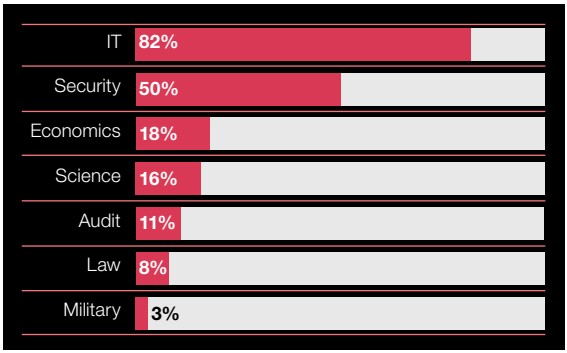
In addition, as the CISOs/ISO role keeps getting more strategic in organisations, other common certifications increasingly picked up by the CISOs/ISOs include the Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA), Certified in Risk and Information Systems Control (CRISC) certifications.

TOP 3 Industry Certifications

54%	56%	37%
ISO 27001	CISSP	ITIL

-1PP	+17PPs	+8PPs
▼	▲	▲

Evolution with respect to 2018 survey



Respondents have an average of about
5.6 years
seniority as a CISO/ISO.

Only about **9%** are of the female gender

The CISO/ISO's position within the company

Full-Time Role

CISOs are increasingly performing their functions in a part time capacity. With a decrease of 12 percentage points from the previous survey conducted in 2018, 64% of the respondents operate as full time CISOs.

Due to the relevance of CISOs' experience, they are taking up additional functions such as the Compliance Officer, Chief Information Officer, Chief Risk Officer, Data Protection Officer.

64%

are full-time in the CISO role

▼ -12PPs

Evolution with respect to 2018 survey

Additional functions or roles CISOs occupy are:

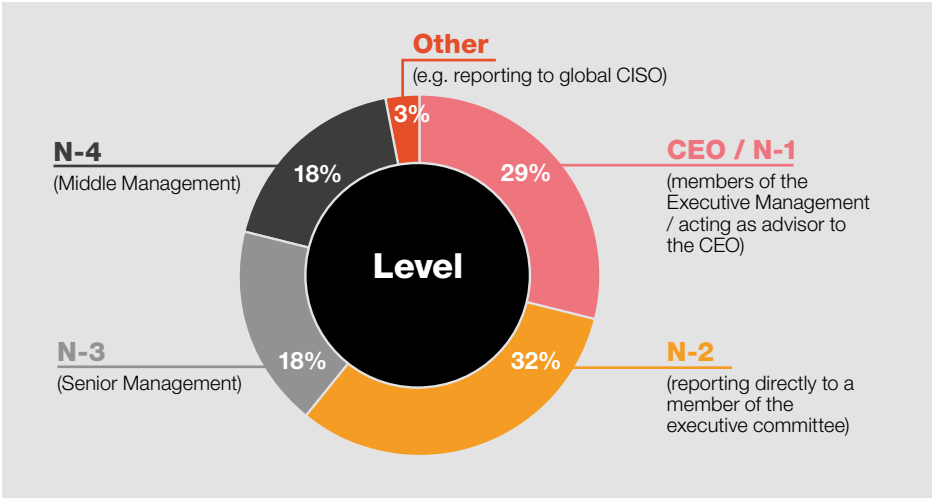
- Compliance Officer
- Chief Information Officer
- Chief Risk Officer
- Data Protection Officer

Reporting Level

CISO/ISO's proximity to the CEO of the company reflects a recognition of the importance of the role and equally expresses the organisation's commitment towards information security.

In contrast to the results of the 2018 survey where no CISO/ISO was part of the Executive Management, the current survey results show that 29% of the CISOs/ISOs are either members of the Executive Management or acting as advisors to the CEO/Executive Management. The rest of the respondents operate at lower management levels that is to say direct report to Executive Management (32%), Senior Management (18%), Middle Management (18%).

A fourth of the respondents do not belong to any committees in the organisation, however the majority of the CISOs belong to the information security committee (86%).



25%

Of respondents DO NOT belong to any committees in the organisation

Committee with CISOs as members:

- Information Security Committee **(86%)**
- Crisis Committee **(48%)**
- Risk Committee(s) **(33%)**
- Management Committee(s) (by delegation from the Executive Committee) **(29%)**

Only 19% are part of the Executive Committee.

Only 29% are part of Project Committee(s).

Management Line

CISOs/ISOs role in companies is spread across four key management lines with the majority (33%) of the respondents residing in the Information Technology (IT) department – an increase of 11 percentage points from the previous survey.

Other management lines where CISOs reside include Risk (30%), Internal Control (11%) and Compliance (4%).

There is still no clear communication link between the entities and their parent companies as about 36% of the CISOs of subsidiaries confirmed that they do not work closely with the CISO of their parent organisation.

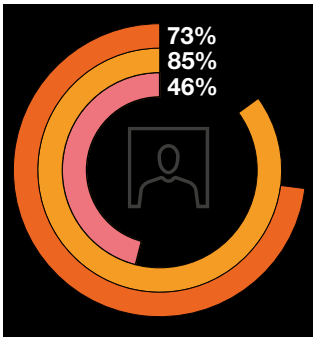
1	33% IT	+11PPs ▲
2	30% Risk	-1PP ▼
3	11% Internal Control	
4	4% Compliance	-9PPs ▼

Evolution with respect to 2018 survey

CISO/ISO's Influence

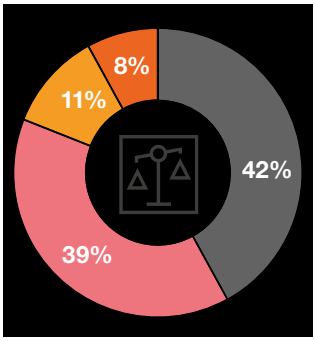
It is interesting to note that the majority of the respondents consider their position to be strategic (73%) and tactical (85%). In addition, almost all of the organisations have a defined information security strategy with about 96% of the respondents affirming this – an increase of 14 percentage points from the previous survey.

CISO's role self consideration



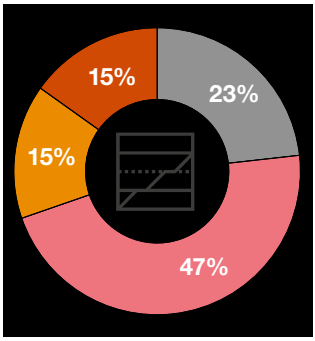
- Strategic
- Tactical
- Operational

CISO's influence self consideration



- Highly influential
- Influential
- Limited influence
- No influence

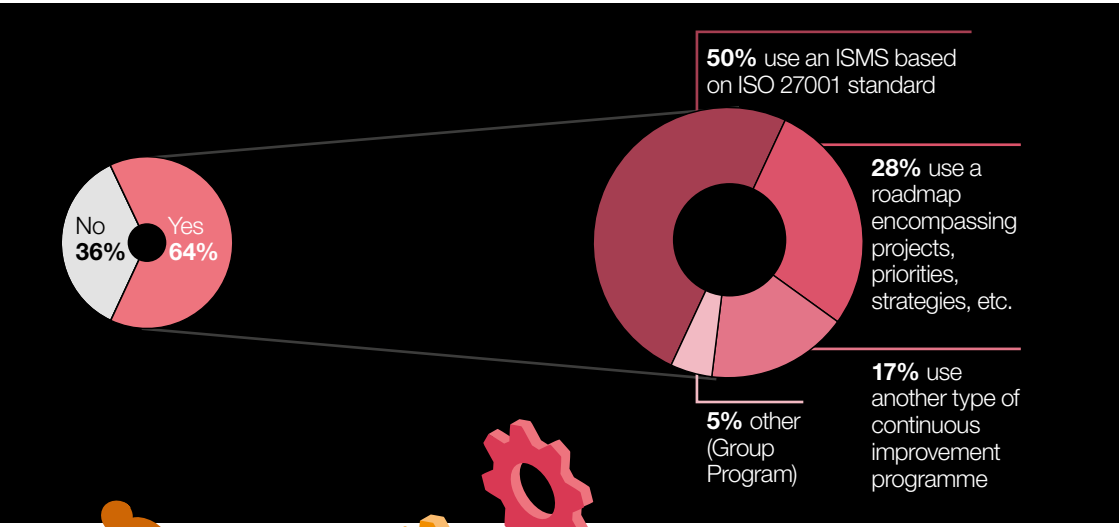
CISO's information security initiatives perception

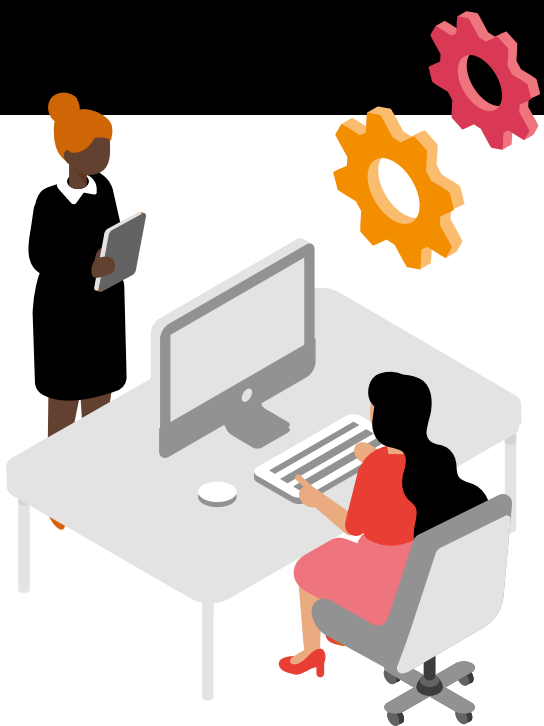


- **Crucial business** enabler and competitive differentiator
- **Vital,** but not an opportunity
- **Unnecessary / excessive** source of cost and constraints
- **Minor** concern

Continuous Improvement Programme

It is a key responsibility of the CISO/ISO to ensure that there is a continuous improvement programme in place to ensure the information security management system is continuously reviewed and updated. 64% of the respondents confirmed having a defined continuous improvement programme based on different approaches.





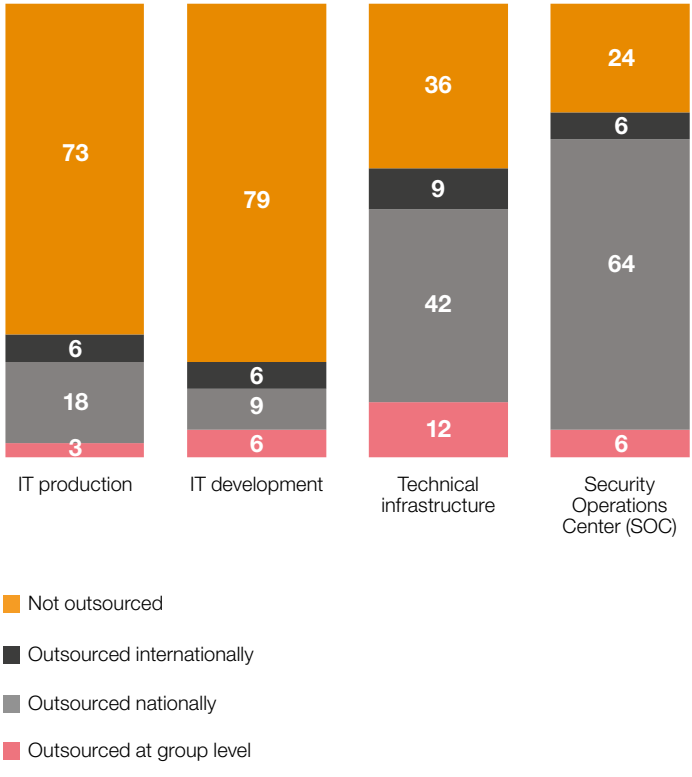
Third Party Risk Management

Outsourced Functions

Organisations are increasingly engaging with external parties to perform all kinds of IT and security services on their behalf. This move is in a bid to save cost, leverage expertise that does not exist internally, be able to diversify and ultimately focus on their core competencies.

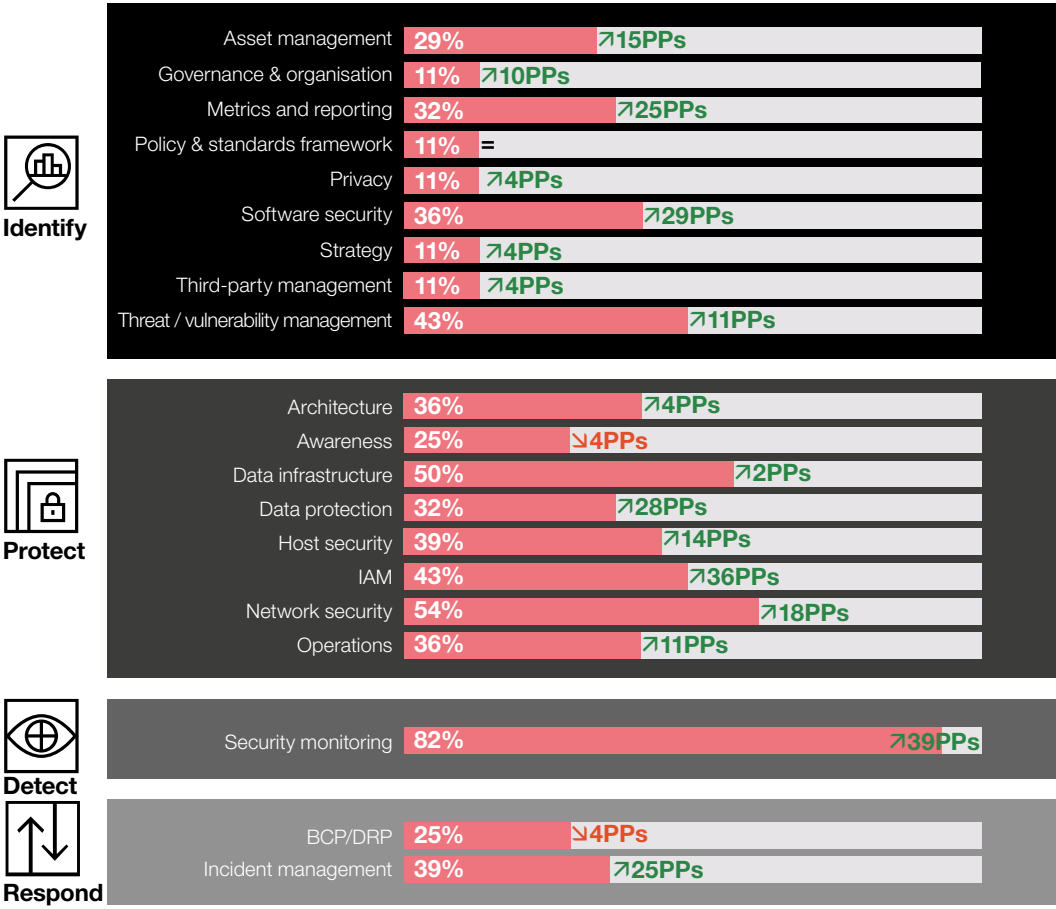
However, organisations need to be reminded that outsourcing activities is not equal to outsourcing the accountability. While the risk is transferred, the ultimate accountability still lies on the organisation and controls need to be put in place to verify the quality (and security) of the service provided.

88%
respondents outsource at least one IT function



Outsourced Information Security Processes

There is clear understanding of the fact that third-party management cannot be outsourced as only 11% of the respondents confirmed that their third-party management process is performed by external parties.



Security Monitoring

There is ample room for improvement in the area of monitoring the functions of third parties. 32% of our respondents confirmed that they do not perform initial internal/external audits on third parties before contracting and 26% do not perform regular internal/external audits throughout the third party's contract life cycle.

Mandatory due diligence exercise is required to be conducted on all third parties before entering into a relationship with them. Furthermore, oversight must be maintained on their activities throughout the lifecycle of the relationship through audits, on site assessments, technical tests and assurance reports.

Use of audit assignments to monitor their third party security

58%

↗9PPs

32%

DO NOT perform initial internal/external audits

26%

DO NOT perform regular audits internal/external audits.

Use of questionnaire / forms to monitor their third party security

70%

↘3PPs

96%

of them use in-house questionnaire

35%

rely on other due-diligence form
(ISAE 3402, ISAE 3000, SOC1, 2, 3, etc.)

CISOs/ISOs challenges

Cyber-Attack Trends and Business Continuity

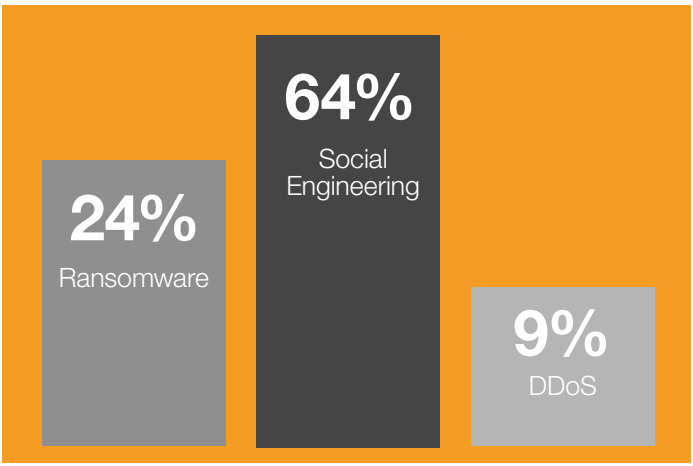
There are numerous challenges that CISOs/ISOs face while performing their functions. The top of this list are the increasing cyber-attacks from both internal and external forces. The CISOs must do their best to keep up with these attacks in order to protect the organisation.

Cyber-attacks are on the rise and the adversaries' tactics are ever evolving. The frequency of these attacks is at an all-time high given the pandemic and employees of most organisations are on an almost 100% remote work model.

The topmost common cyber-attacks in the wild in recent times are Social Engineering, Ransomware and Distributed Denial of Service as observed in the media.

In spite of these, 33% of the CISO respondents have huge concerns that they lack the readiness and resilience capabilities to remain in business in the event of such cyber-attacks.

TOP 3
Cyber Attacks trends observed this year*



*These findings are not extracted from the survey but have been observed in the recent trends on media.

Threat Intelligence

Threat intelligence provides information on cyber threats that could target an organisation. It is a great tool that supports security practitioners including the CISOs/ISOs in their efforts to prepare, identify or prevent cyber-attacks that could have impact on the organisation and its resources.

Regardless of its usefulness, 36% of the respondents confirmed they have not leveraged on external threats intelligence sources. Interestingly, those that do are subscribed to intelligence sources such as CIRCL MISP, ABBL MISP and 81% of them go as far as integrating these sources to their key information security functions such as incident management or vulnerability management processes.

36%

Of respondents DO NOT use external threat intelligence sources

81%

Of the respondents who use intelligence sources also have these sources integrated in their security functions such as incident management or vulnerability management.

Resources and Budget

A lot of money and effort is required when organisations need to recover from information security incidents.

However, it costs way less to take preventive steps by building, operating and maintaining an effective information security management system.

Unfortunately, most organisations still have not identified the need to channel more budget in the information security functions of the organisation.

In light of this, about 40% of the CISOs/ISOs consider their budget as insufficient for performing their functions; and only about the same proportion have seen an increase of over 10% over the last year.

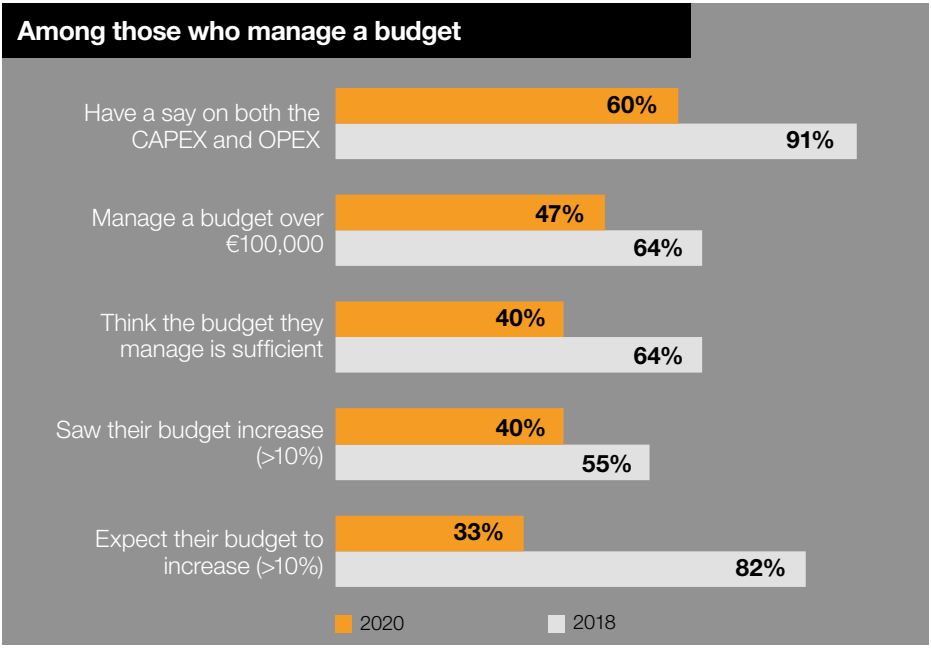
On the contrary, information security staff headcount have been on the increase over the last few years; and over 40% of the respondents expect a similar increase year on year in the future.

42%

DO NOT manage the budget for the purpose of carrying out their role

▼-16PPs

Among those who manage a budget



33% **saw their information security staff count increase over the last few years (40% expect this increase year on year in the future)**

Top Barriers to Success

58% of the CISOs/ISOs consider the complexity of information systems as the top barrier to their success among others such as inadequate budget, political decisions that tend to put individuals' career interests over that of the organisation etc.

Regardless of the inherent difficulty and complexity of the CISO function, 58% consider the role to be the best job they have ever had; they equally see the value they add to the business through their achievements, top of which is, success in raising information security awareness among the company's staff as confirmed by 92% of the respondents.

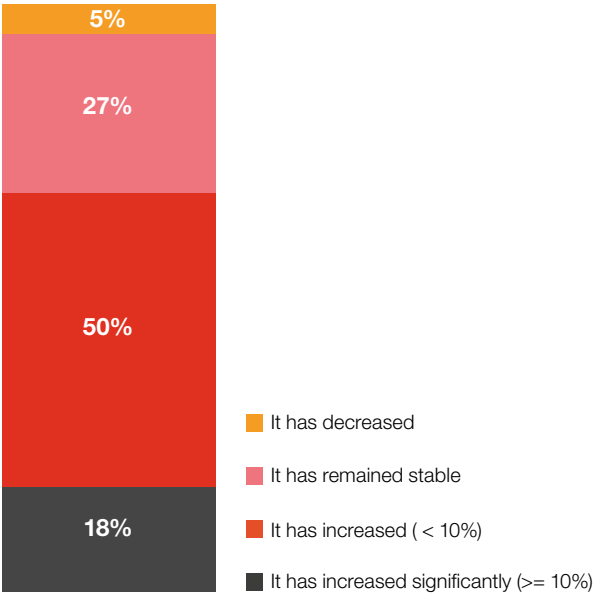
TOP 3 CISO/ISO's achievements		TOP 3 CISO/ISO's barriers to success	
Effectively raising awareness among the company's staff, with visible results	92%	58%	Complexity of IT/ information systems
Enabling the company's staff to be protected against attacks targeting them personally	88%	50%	Lack of an appropriate budget
Formally identifying other vulnerabilities (operational, procedural, cultural, project-specific, governance-related, etc.)	81%	46%	"Political decisions" (i.e. decisions that put individuals' career interests ahead of the company's interests)

CISOs/ISOs' Remuneration

About two thirds of CISO/ISO respondents have a fixed annual salary of over 100,000 Euros per year; and about 32% of the respondents have either had their salary decrease or remain stable over the last year.

2/3

of the respondents have a fixed annual salary (excluding variable components, bonus and benefits) over 100.000€/year



Key Takeaways and Recommendations

Obtain management's support by providing more **adequate budget, resources and time**; and ensure they place top corporate priority on Information security.

This can be done by **increasing your influence** through **active participation** in corporate committees and by **setting up a direct reporting line** with the management.

Align your **Information Security strategy** with the **organisation's strategy** in order to ensure **management support.**

This can be achieved through the **promotion of Information Security** within the company by elevating it as a **market differentiator** place.

Establish a reporting line with the **Risk management function** rather than IT management line in order to ensure **independence** in case of impactful decisions.

This can be reached by **sensitising your management** on Information Security and its **objection with IT interests.**

Place huge focus on **third party risks** and suppliers' security management. Most recent Information Security **incidents** come from third parties and are usually the result of a **poorly managed third-party security**.

Several questionnaires document **points to consider** while contracting with suppliers (ISAE, SOC).

Set up a **strong response** to increasing threats, especially related to **social engineering** and **ransomware**.

This can be done through **employees' awareness** and training on such risks and teaching on **how to react**.

Ensure a **long-term information** security strategy aligned with market best practices.

This is usually achieved by setting up a **continuous improvement programme**. International Standards provide **clear guidance** on the path to follow.

Contacts

About PwC

PwC Luxembourg (www.pwc.lu) is the largest professional services firm in Luxembourg with over 3,000 people employed from 75 different countries. PwC Luxembourg provides audit, tax, and advisory services including management consulting, transaction, financing and regulatory advice. The firm provides advice to a wide variety of clients from local and middle market entrepreneurs to large multinational companies operating from Luxembourg and the Greater Region. The firm helps its clients create the value they are looking for contributing to the smooth operation of the capital markets and providing advice through an industry-focused approach.

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms of 158 countries and 250,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com and www.pwc.lu.

About clusil

CLUSIL a.s.b.l. develops cooperative actions with public authorities, semipublic authorities for the security of information. With about 200 members from all economic sectors, it is a well-established and independent actor among the Information Security Landscape of Luxembourg and the "Greater Region". In more than 20 years we have come a very long way and are very proud of the many achievements. By the members for the members, the collective action is bringing the following capabilities to each member.

Koen Maris
Cybersecurity Leader,
PwC Luxembourg
koen.maris@pwc.com

Maxime Pallez
Cybersecurity Manager,
PwC Luxembourg
maxime.pallez@pwc.com

Daberechi Uwakwe
Senior Associate,
PwC Luxembourg
daberechi.uwakwe@pwc.com

Pascal Steichen
President of Clusil
CEO of SECURITYMADEIN.LU

David Hagen
Honorary President of CLUSIL

Cedric Mauny
Vice-Chairman of the CLUSIL /
Leader of the Think-Tank CISO

info@clusil.lu

© 2020 PricewaterhouseCoopers, Société coopérative. All rights reserved. In this document, "PwC" or "PwC Luxembourg" refers to PricewaterhouseCoopers, Société coopérative which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity. PwC IL cannot be held liable in any way for the acts or omissions of its member firms.