

Out of the shadows: CISO is in the spotlight!

2018 CISO's role and responsibility survey



Introduction

Failing to keep their information secure and not being compliant to regulations exposes organisations to severe operational, legal, financial and reputational risk. There are business benefits from embedding security consciousness in the organisational culture, and making it a core competency.

In this survey conducted by the Collège des Professionnels de la Sécurité de l'Information (CPSI) and PwC Luxembourg, the second since 2016, we assess market practices regarding the roles and responsibilities of the Chief Information Security Officer (CISO) or Information Security Officer (ISO), and in particular:

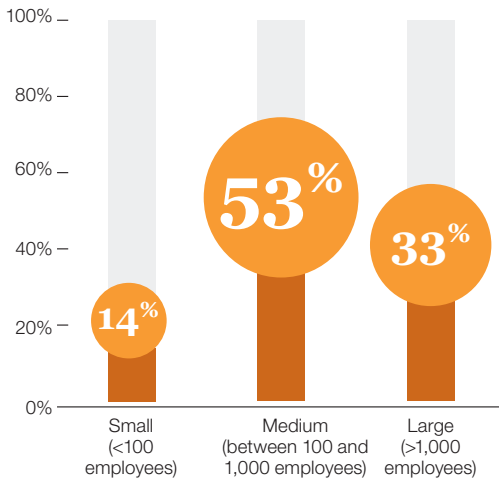
- Their place in the corporate hierarchy
- How their role has evolved since 2016
- What is involved as part of their daily work
- Their challenges with respect to local and international regulations



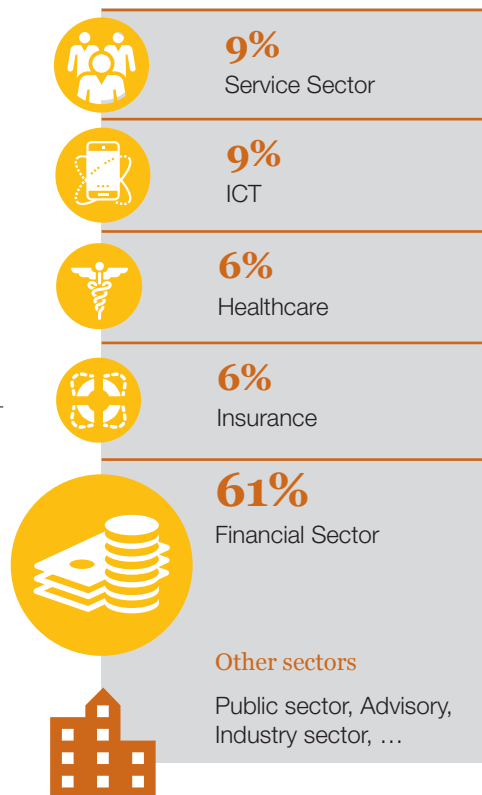
The companies we surveyed

The companies that responded to our invitation to participate in this survey are based in Luxembourg, and are representative of the Luxembourg economic landscape. The majority (67%) are Small and Medium-sized Enterprises (SMEs) with less than 1,000 employees. Many (61%) serve the financial sector. 50 people from these companies participated in this survey.

Company size



Business sector



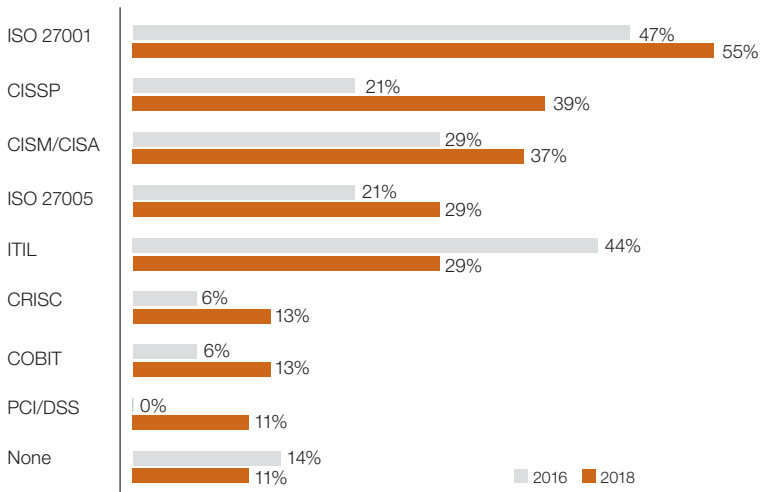
The typical CISO/ISO



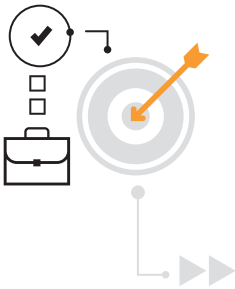
If you meet a CISO or an ISO today, the chances are that he will be male with a higher degree and a background in IT and security. He will have been in his role for just over six years, and been trained in ISO/IEC 27001 Information Security Management and have IT-based certifications, such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) and Certified Information Systems Auditor (CISA).

Interestingly, since 2016, there has been a drop in the number of CISOs reporting ITIL certifications, but there has been an uptick in those with backgrounds in law and economics, and with credentials such as Certified Risk and Information Systems Control (CRISC). This reflects the trend of positioning the CISO from a strongly technical to more of an enterprise-level business risk and strategic management role. This positive trend can be perceived as very slow considering how information and cyber security grows in strategic importance for most organisations.

Certifications



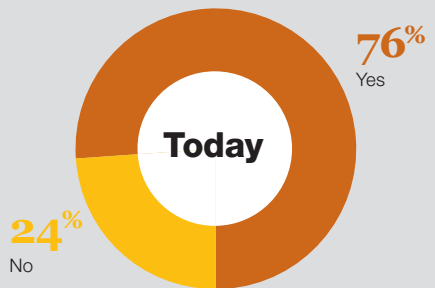
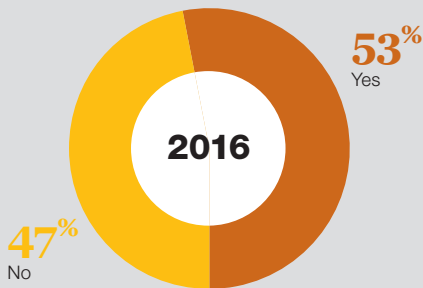
The CISO/ISO's role



There has been a growing recognition of allocating a full-time role for the CISO/ISO position. In 2016, just over half of the respondents reported that CISO/ISO roles were full-time. Today, over three quarters consider it to be a distinct, full-time job.

SMEs may not always have the capacity to support a full-time CISO/ISO role. CISO/ISOs that are not in a full-time role reported their additional function as being either CIOs, Risk, Compliance, Business Continuity, Disaster Recovery or Data Privacy Officers. Some of these combinations, beyond the fact that they could lead to conflict of interest, could be very difficult to handle on a day-to-day basis and should be challenged by governance bodies.

CISO/ISO: a full-time role?



The CISO/ISO's position in the company







Whereas in 2016 no CISO/ISOs reported working at that level, today 13% report to the CEO. Taking into account the next rung in the hierarchy, the N-2 Level, nearly two thirds of the CISO/ISOs have close access to the top. Proximity to the CEO reflects the growing recognition of the CISO/ISO as being an executive level contributor, and the organisational seriousness towards information security.

Most CISO/ISOs lead the company Information Security Committee, but only half are represented on Project Steering Committees. There is an opportunity to increase their involvement in projects to ensure that project teams conduct the proper security assessments before introducing work practice changes into the organisation.

Of the company lines of business, the highest number of CISO/ISOs were appropriately in the Risk Management area. The next area of congregation for CISO/ISOs was in IT. This is symptomatic of information security being coupled with information technology. The future trend is for information security to be framed as an enterprise-wide risk management, compliance type of role. The CISO/ISOs need to hold an independent role that affords them objectivity in safeguarding corporate interests outside of pressures from individual projects.

Position within the company

CEO		Executive Committee	
N-1			28%*
N-2			34%
N-3			16%
N-4			19%

*N-1 level: includes CISO/ISOs who are members of the executive management as well as those acting as advisors to the CEO

Management's perception of information security



For nearly all companies, information security is a priority. Although some (8%) consider it to be excessively costly, others (23%) see it as a key differentiator and business enabler. Many (65%), however, see it as being necessary, but do not see it as holding much opportunity.

Companies that see information security as an enabler also value the opinion of their CISO/ISOs and take it into account for decision making. CISO/ISOs from one of five respondents believe that they are not considered to be very influential or worth taking into account.

Management's perception of information security



Business enabler, key differentiator

23%



Vital, but not an opportunity

65%



Not a priority

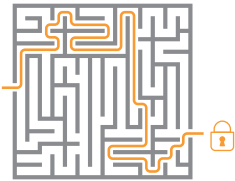
4%



Source of excessive cost

8%

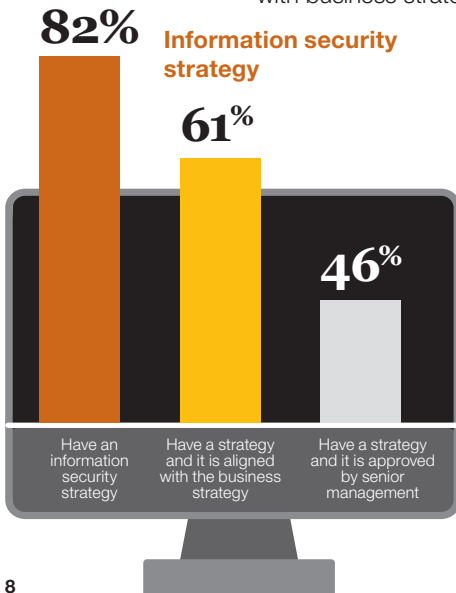
CISO/ISO visible influence to their company



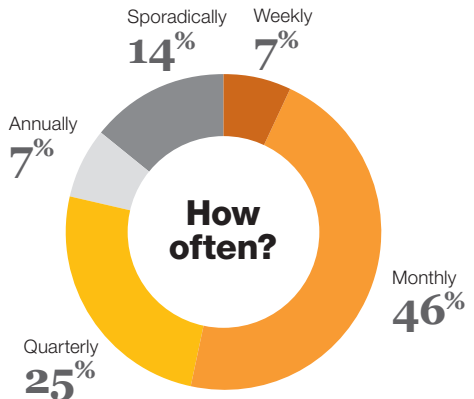
Most (82%) of the surveyed companies have an information security strategy. Of these, many (61%) are aligned with business strategies, but only about half (46%) of the information strategies are approved by senior management.

Many (61%) companies have a continuous improvement programme. Approximately half (47%) of them rightly base the programme on a recognised Information Security Management System (ISMS) framework, for example ISO 27001. Others base their improvement programme on 'internal methods'.

Nearly half (46%) of those who maintain KPIs and metrics report them on a monthly basis. However, many (36%) do not report the metrics to management. Showcasing the positive impact of the strategy should be used as a pro-active and positive approach to get management's involvement, leading to a crucial alignment with business strategy.

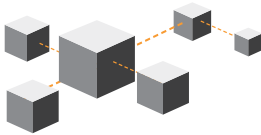


Use of metrics (KPIs, dashboards, etc)



Third Party Risk

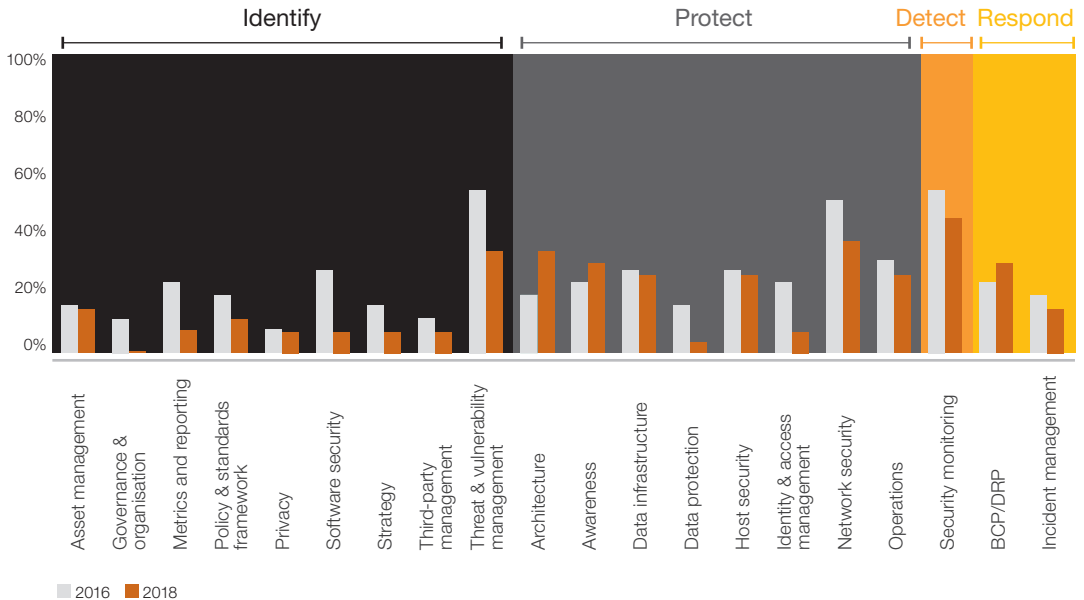
Outsourced Security related Processes



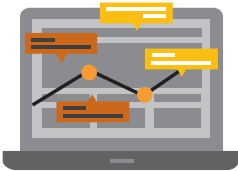
Other than in the cases of seeking third party advice on creating security architectures, conducting awareness programmes and ensuring Business Continuity and Disaster Recovery, the general overall trend since 2016 is for companies to lower their dependency on third parties for information security related activities.

Companies are taking greater ownership of developing their own strategic governance agendas and capabilities, and doing more internally. Where it does make sense for them to outsource is for specialist technical expertise on penetration testing for example.

Cases where the process is outsourced (either partially or totally)



Monitoring third parties



As part of risk and vendor management, it is a good practice to actively monitor third parties. On-site audits provide the most immediate and hands-on assessment.

Half (49%) of the respondents perform audits. Many (63%) perform an initial on-site, due diligence, audit and continue with regular annual audits. Most (75%) just audit who they consider to be their most critical providers.

Many (73%) respondents rely on provider responses to questionnaires. The questionnaires generally are home grown, while some (29%) also use International Standard for Assurance Engagements (ISAE) due diligence forms to assess the provider maturity.

Use of
questionnaires

73%

Use of
audit

49%

Among the CISO/ISOs using questionnaires to monitor third parties:

- All of them use in-house questionnaires;
- 29% also use due diligence forms (ISAE3402, ISAE3000, etc.).

Among the CISO/ISOs performing audits on third parties:

- 63% perform regular audits (on an annual basis, in most cases), not just an initial one;
- 75% conduct audits only on critical providers.

No increase compared to the 2016 results

Main challenges



Resources

Less than half (42%) of CISO/ISOs manage their own budget. Of these, many (64%), although less than in 2016, think that their budget is sufficient, and most (82%) expect it to increase.

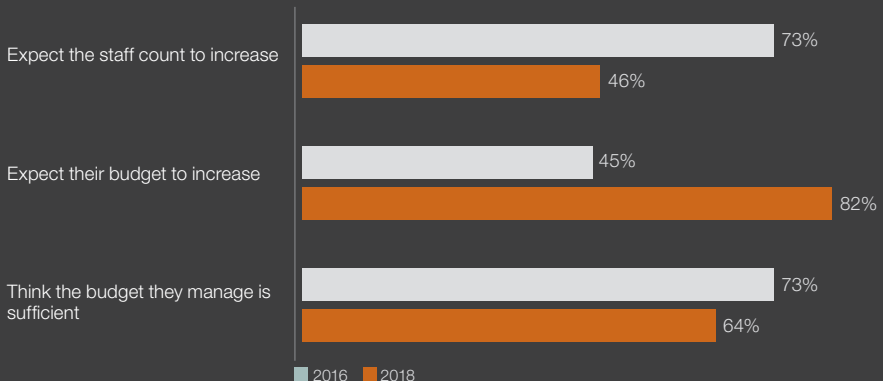
Most (91%) CISO/ISOs have a say on Capital Expenditures that may be directed to buying security-related tools, but much fewer (46%) are consulted on Operating Expenses.

Although less than in 2016, nearly half (46%) of the respondents expect their staff count to increase.

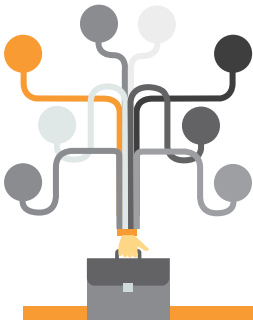
58%

Do not manage a budget

Among those who manage a budget



Job complexity



Even though most (85%) CISO/ISOs think that their jobs have become more complex than they were in 2016, they believe that they receive a fair compensation, and half consider it to be the best job that they have ever had!

Their jobs have become more complex as our world has become more interconnected and dependent on the cloud. Meanwhile, hackers have become even more audacious. Greater regulations and safeguards are imposed by regulations from various levels (European, country, industry, etc.).

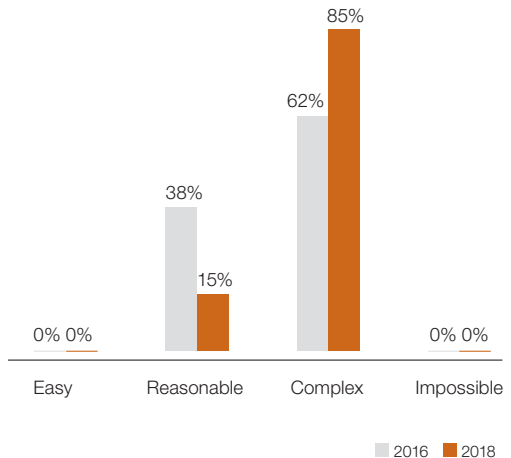
Despite this complexity:

92%

of respondents think their job is a great job

46% being their best job!

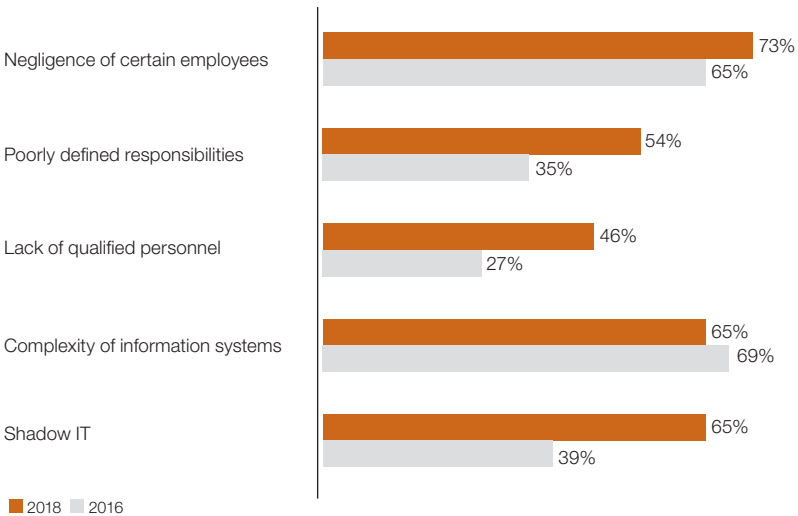
Complexity of the job



One of the key preoccupations of CISO/ISOs is the human factor in cybersecurity. The lack of security qualified professionals, negligent employees without clearly defined responsibilities working in a complex IT environment are prone to cause a lot of damage. They often fall short, to make their life easier, when it comes to complying with, and even circumvent rules and secure practices.

Companies, for their own sustainability, need to promote a security culture where everyone has the responsibility to observe and promote clear and simple security practices and more importantly, to behave in a conscious way which is in alignment with the company's information security strategy. Companies need to disclose and encourage the good behaviours, instead of blaming. Keeping a positive mindset is key.

Main barriers to success



Key takeaways and recommendations



Our recommendations to the CISO/ISO community following the survey are to:

1. Better manage third party risk
2. Test, monitor and improve your security controls on a regular basis
3. Convince your management of the need for you as CISO/ISO to be influential and sufficiently independent
4. Educate your employees about the latest security threats and help them understand how their behaviour can positively support the protection of the company's information

Better manage third party risk

Build a comprehensive inventory of your third parties, and classify them according to the various dimensions of your Enterprise Risk Management framework, including level of exposure and security risk. With that in place, define minimum security requirements to be included in each and all contracts. Develop a strategy to monitor third parties, including regular audits while concentrating your efforts on high-risk suppliers. Develop metrics to report the overall performance of your third parties.

Test, monitor and improve your security controls on a regular basis

Define a programme on how to continually improve and refine your security controls. Identify lessons learned after each incident, and put measures in place to prevent them from occurring again. Plan how frequently you will review your security controls. Draw up metrics to track changes in your security capabilities and identify areas for improvement. They need to understand the good behaviours that will make a difference. Don't use fear but encouragement.

Management needs independent and influential CISO/ISOs

Discuss with your management that, as CISO/ISO, you need to be involved in strategic information security-related decision-making. Raise the issue of independence with your management, especially if the current configuration affects your ability to raise security concerns freely and without fear of negative consequences.

Educate your employees

Use multiple communication channels (training classes, newsletters, flyers, etc.) to educate your workforce on cybersecurity risks. Ensure that employees understand their responsibilities and obligations regarding cybersecurity (i.e. complying with security procedures, reporting anything suspicious, etc.). Take the opportunity to introduce unpredictability into these tests scenarios and be ready to discover the unknown. If you are precise in the test scenario, it means that you know what you are looking for and therefore how you can improve.

Contacts



About PwC

PwC Luxembourg (www.pwc.lu) is the largest professional services firm in Luxembourg with 2,870 people employed from 76 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 by 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 in 158 countries with over 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 CPSI

Founded in June 2010, The College of Information Security Professionals (CPSI) aims to promote the profession of Chief Information Security Officer, to recognise individuals having CISO expertise and to develop these skills.

The CPSI wants to:

- Promote the profession of chief information security officer (CISO).
- Recognise the people having CISO expertise.
- Develop the competences needed by chief information security officers.

Greg Pitzer

Cybersecurity Leader, PwC
greg.pitzer@lu.pwc.com

Maxime Pallez

Cybersecurity Manager, PwC
maxime.pallez@lu.pwc.com

Rodolphe Mans

Chairman, CPSI
rodolphe@mans.lu

Ludovic Raymond

Member, CPSI
ludovic.raymond@bil.com