2014 GOVERNANCE OF CYBERSECURITY

ISACA Chapter NL

About ISACA
As an independent, nonprofit, global association, ISACA engages in the development, adoption and use of globally accepted, industry-leading knowledge and practices for information systems. Today, ISACA has more than 110,000 members worldwide. Through more than 200 chapters established in more than 80 countries, ISACA provides its members with education, resource sharing, advocacy, professional networking, and a host of other benefits on a local level. Benefits offered through globally accepted research, certifications and community collaboration result in greater trust in, and value from, information systems.

This survey on the governance of cybersecurity underpins the objective of the ISACA Netherlands chapter to provide member support by leveraging the ISACA strategy and to add some “couleur locale”.

Acknowledgements
ISACA NL would like to express its gratitude to the academic world for their support, especially the University of Amsterdam (VU) and the University of Antwerp (UA).

Development team
Will Franken, Research Director ISACA Netherlands
Michael Fabri, ISACA Netherlands
Kevin Vlaanderen, webmaster University of Utrecht (UU)

Sounding board
KP Meindertsma, Immediate Past President ISACA Netherlands
Fred Steenwinkel, President ISACA Netherlands
Dr. Abbas Shahim, University of Amsterdam (VU)
Prof. Dr. Wim van Grembergen, University of Antwerp (UA)
Ronald Verbeek, Director CIO Platform Nederland

Subject matter reviewers
Hilko Batterink, board member of ISACA Netherlands
Marcel Baveco, ISACA Netherlands
prof.dr.ing. Hans Mulder, executive professor at Antwerp Management School

Will Franken
Research Director ISACA Netherlands

ISACA Netherlands
Gooimeer 4 - 15
1411 DC Naarden
The Netherlands
Email: info@isaca.nl
Website: www.isaca.nl

Provide feedback: info@isaca.nl

Table of Contents

01

Introduction

In recent years Internet technology and cyberspace have had a tremendous impact on all parts of Dutch society. Daily life, social interactions and economic activities all depend on information and communication technology working seamlessly. The Netherlands itself is an international Internet hub and has one of the highest concentrations of online use in the world.

It is widely recognized that cybersecurity is an important precondition to fully capitalize on the opportunities offered by the digital society, and for information and communications technology to sustain the backbone of our economic growth.

Cybersecurity commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cybersecurity strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein.[1] ▶

1 *High Representative of the European Union for Foreign Affairs and Security Policy (2013). Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace p3.*

Companies and institutions must be transparent in their efforts to ensure uninterrupted availability and be accountable for the protection of sensitive data.

The sense of urgency has been widely recognized on different levels. President Obama has stated: “protecting the infrastructure will be a national security priority”. In the EU, the European Commission has issued a Cybersecurity Strategy to “sustain an open, safe and secure cyber space”.

On a national level the second National Cybersecurity Strategy, which was launched in early 2014, states that in order to ensure digital online freedom and to sustain a secure, robust and innovative Internet, the Netherlands will need to further strengthen and combine forces of both public and private parties.

These initiatives acknowledge that governments have a significant role to play in ensuring a free and safe cyberspace. However, the private sector owns and operates significant parts of this cyberspace and so, in addition to protecting their own assets, also has to recognize its leading role in maintaining the reliability and interoperability of the public Internet. For this reason, companies and institutions must be transparent in their efforts to ensure uninterrupted availability and be accountable for the protection of sensitive data. Moreover, as many vital processes are interdependent, a collaborative and cross-organization approach is imperative to respond to a growing cyber threat landscape.

Using three means of control: regulation/ self-regulation, transparency, and developing awareness and knowledge, the Ministry of Safety and Justice calls upon everyone to assume responsibility for their own digital resilience and for society as a whole.[2]

With a strong background in IT governance and information security, and with a strong following amongst over 1500 members in the Netherlands, ISACA NL felt strongly receptive to this call. As an independent, nonprofit association, ISACA NL recognized its role and announced a research project on cybersecurity to assess current governance practices of large organizations and institutions in the Netherlands. The governance of cybersecurity is particularly important because it addresses organizational security with a strong focus on those types of attacks, breaches or incidents that are targeted, sophisticated and extremely difficult to detect or manage.

In its contributing effort, ISACA NL has developed a questionnaire that is aimed to be beneficial to participating organizations in a number of ways, i.e. in identifying areas of strengths and weaknesses in cybersecurity governance and finding ways to incorporate cybersecurity in an organization’s existing governance model. Key benefits also include accommodating cybersecurity governance to support all relevant stakeholders and enhancing cybersecurity to leverage an organization’s risk management and decision-making process. The ultimate goal is to identify and exchange good practices, sharing information and lessons learned cross-industry and between private and public organizations.

In the period from March to June 2014, ISACA NL conducted a survey amongst large Dutch companies and institutions from various economic sectors that provide critical services and infrastructures. The survey’s objective was to assess whether these organizations succeeded in giving adequate attention to cybersecurity in their current governance and management programs. Thirty-two organizations participated in this survey, which took place at a national level.

Participants in alphabetical order

ABN AMRO	Havenbedrijf Rotterdam	Provincie Zuid Holland
Alliander	ING	Rabobank
ASML	Kasbank	Robeco
Atos	KLM	SNS Bank
Belastingdienst	Menzis	RET
Binckbank	Ministerie van Veiligheid en Justitie	UMC Groningen
Centraal Beheer Achmea	NIBC Bank	UMC Utrecht
Credit Europe Bank	NS	USG People
DHL	NXP	van Lanschot Bankiers
Eneco	PGGM	Wolters Kluwer
GE Artesia Bank	ProRail	

Figure 1 Participants

2 *Ministry of Safety and Justice in the Netherlands (2013). Nationale Cybersecurity Strategie 2 - van bewust naar bekwaam p19-20.*

02 Survey Approach *and Methodology*

For this research project, an online survey was used as data collection technique to assess the current status of cybersecurity governance amongst large Dutch companies and institutions. A cybersecurity specific questionnaire was developed in which ISACA's COBIT 5 framework was used as a leading reference, next to guidance and recommendations from other research centers, security industries, and institutions such as ENISA.

Many companies and institutions were invited to participate in this survey, to reflect a representative cross-section of organizations in both private and public sectors. A large proportion of participants were contacted in the finance sector, assuming that these organizations already have made significant progress in cybersecurity governance. Other companies were invited because of their specific focus on protecting certain business-critical processes, infrastructure and/or intellectual properties. Finally, invitations were sent out to organizations that were assumed to be able to benefit from good practices that have already proven to be successful in other parts of the economy.

In view of the focus of this survey, i.e. the governance part of cybersecurity*, respondents were selected amongst sponsors that were positioned as an IT director, CIO, CISO, and/or Audit director. Participants were questioned on seventeen different governance- and management-related topics, primarily on the *perceived* importance for cybersecurity governance of that specific topic. Next, they were requested to provide the *actual* scores for the organization.

* *Technically this survey encompasses both governance and management topics as COBIT 5 makes a clear distinction between governance and management.*

Research topics included, but were not limited to:

- Cybersecurity strategy
- Full end-to-end business and ICT responsibilities of cybersecurity
- Cybersecurity link to the organization's objectives
- Cybersecurity to be part of enterprise risk programs
- Cybersecurity risks effectively translated into adequate security initiatives
- Compliance with relevant laws & regulations as well as contractual requirements and internal policies
- Effective reporting structures in place
- Effective communications in place: internal and external
- Budget space commensurate with current cybersecurity risk profile

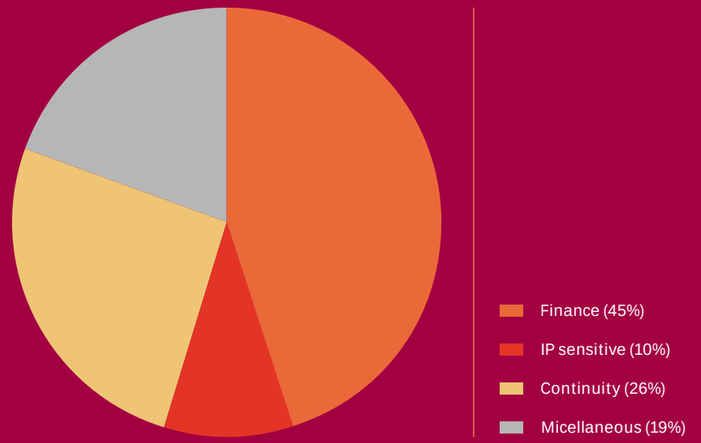


Figure 2 Distribution of participants

For the purpose of analyses, participants were assigned to one of four clusters:

- *Cluster 1*: companies and institutions in the finance sector;
- *Cluster 2*: companies with a strong focus on protecting their Intellectual Property (IP);
- *Cluster 3*: companies with a strong focus on continuity and availability;
- *Cluster 4*: miscellaneous.

The motivation behind this clustering is to distinguish between companies in the finance sector that are confronted with cyber crime, almost on a daily basis, companies that focus on confidentiality to protect their intellectual properties, and companies that have a specific concern for Denial of Service attacks that may jeopardize their on-going operations. ***Figure 2*** shows the distribution of participating organizations across these different clusters.

The results of the survey were analyzed in a number of ways. Respondents were requested to submit their scores on a scale of 1 to 7, 7 being most important or applicable and 1 being least important or applicable. After completing the online survey, participants were given individual feedback on their perceived scores versus actual scores. This overview correlates the organization's security professional expert opinion with the actual status for a specific topic. Upon survey completion, every participant was given feedback on actual scores relative to the consolidated survey average scores.

This publication presents all survey results along with further details on specific observations, on both a consolidated and cluster level.

03 Executive Summary

Established sectors such as finance, health, energy and transport, but also new business models, are built on the uninterrupted availability of ICT and the public Internet. Consequently, the networks and computers we depend on every day should be should be protected from incidents, malicious activities and misuse.

Motivated by the alarming surge in cybersecurity incidents, individual organizations have already intensified their security programs. In addition, for these programs to be effective on an ongoing basis rather than one-off activities, there is a need for strong governance, to operationalize the policies that have been developed, and to better protect businesses and infrastructures against cyber threats.

In this survey, for each participating organization, actual achievements are compared with the expert's opinion of what needs to be in place in the governance and management of cybersecurity. ***Figure 3*** shows that for all topics considered, the perceived importance for what needs to be in place, exceeds what is actually in place. In other words, according to the expert, to some degree, organizations are falling behind in providing the attention to cybersecurity that is required.

Of all the topics covered in this survey, Management commitment, Incident response, Risk management, and Culture, ethics and behavior are perceived to be most important.

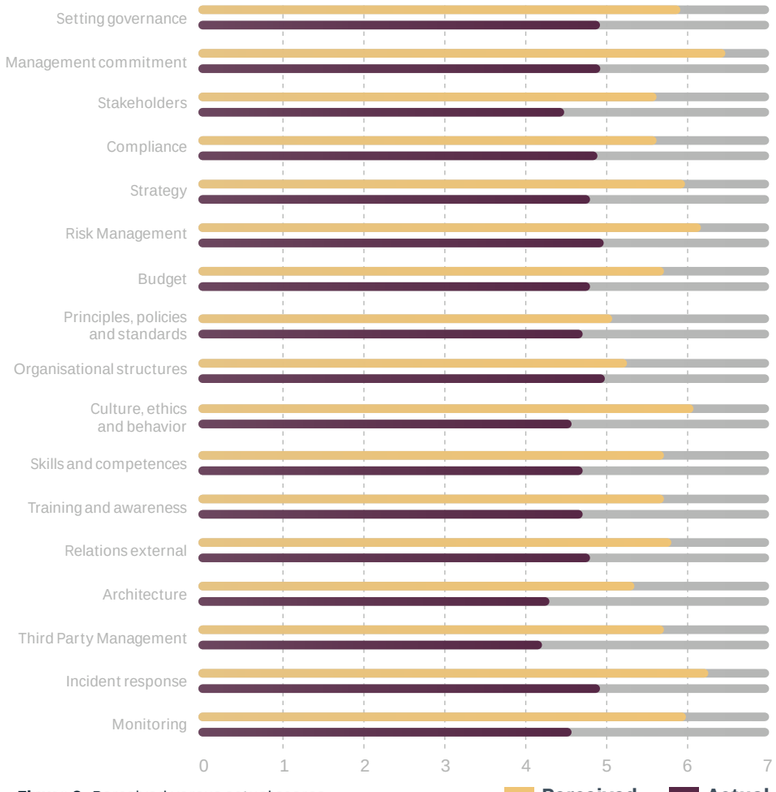


Figure 3 Perceived versus actual scores

The topic of Principles, Policies and Standards is perceived to be least important in cybersecurity governance. So, as an example, with Culture being perceived to be very important for the success of cybersecurity, respondents indicate that organizations are failing to create a culture where people are aware that prevention against cyber threats is almost impossible and that cyber-security should reflect a better balance between prevention and detection.

Looking at figure 4, companies in the Finance sector seem to have established a steady baseline in their governance structures to accommodate cybersecurity. The scores for companies in the IP-sensitive cluster are at a somewhat lower level and show more fluctuation, e.g. on the topic of third-party management. The scores for continuity-sensitive companies are at the lower end of the range but at the same time respondents report many significant deviations in perceived versus actual scores. In other words, according to respondents, their organizations are failing to give adequate attention to topics that they consider are important to cybersecurity. Companies and institutions in the miscellaneous group also are located at the lower range of the spectrum but show fewer deviations toward the perceived importance of cybersecurity.

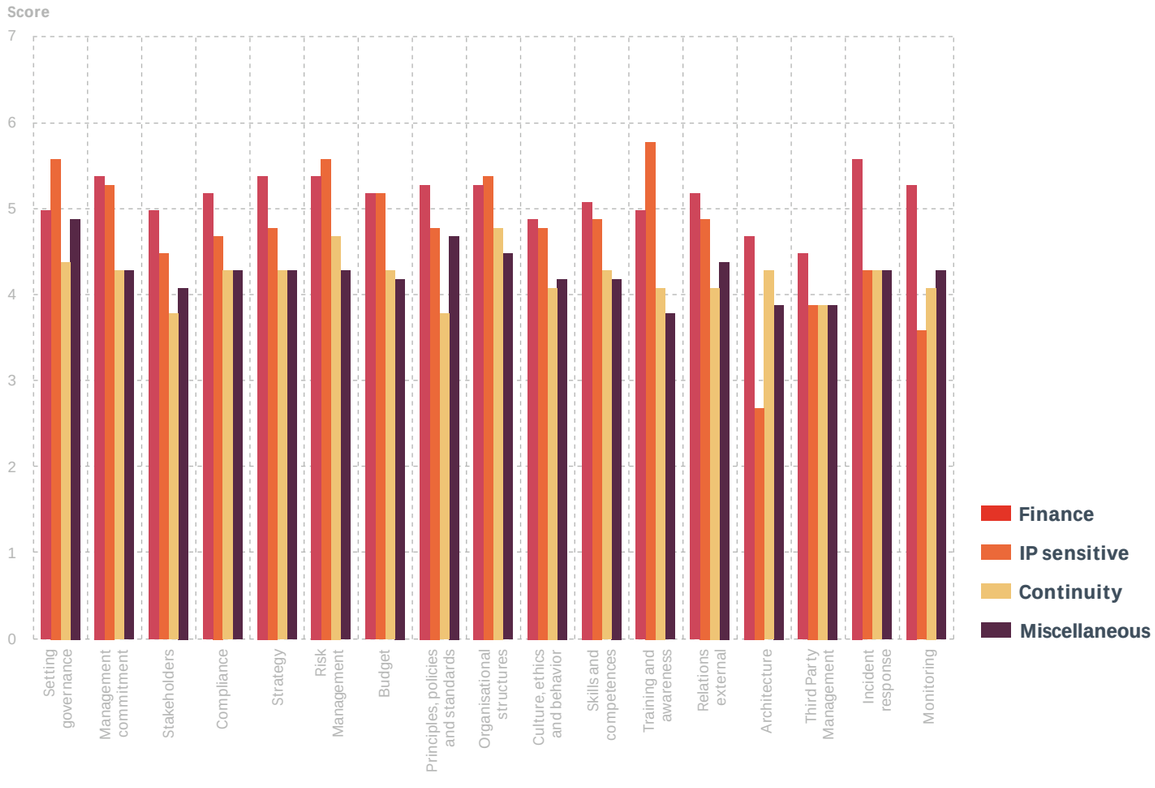


Figure 4 Actual results per cluster

> Emerging technologies and a constantly evolving threat landscape are likely to influence an organization's governance design.

Cybersecurity and third parties
Of all the topics covered in this survey, when it comes to cybersecurity, organizations seem to be struggling most with third-party management. Third parties play a role in many governance topics. In external relations, although suppliers and vendors are referenced as a way of strengthening cybersecurity capabilities, in the survey results they appear to be least recognized as important stakeholders in cybersecurity. Also in compliance, where third parties have to be managed to meet regulatory requirements, assessing and reviewing suppliers for compliance appears to be most challenging. Finally, in risk management, updating risk rating for all third parties subject to cybersecurity requirements proves to be very difficult in third-party management.

Incident response
Incident response is perceived to be very important for cybersecurity in those organizations that have clearly defined objects that require protection. While participants in the Finance-, IP-sensitive- and continuity-sensitive clusters seem to do quite well, organizations in the miscellaneous cluster are clearly struggling with this topic. Although not an explicit part of this survey, this may indicate that institutions in the miscellaneous cluster have not (yet) defined clear objects for protection.

In an effort to limit disruptive effects caused by a significant breach or attack, several items need to be anticipated in an incident response plan. Of all the references suggested in this survey as being part of an incident response plan, establishing interfaces with corporate communication seems to be the most challenging in anticipating communications to all relevant stakeholders in the case of a major cyber incident. The remaining of this publication will give the details for all 17 individual topics.

04 Survey

4.1 | *Governance Setting*

Introduction

Information security governance can be defined in several ways. In general, it is the system by which an organization directs and controls information security. NIST (National Institute of Standards and Technology) refers to information security governance as the process to provide assurance that information security strategies are aligned with – and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility, all in an effort to manage risk. This definition may well encompass cybersecurity, as it protects against all threats that originate from cyber space. However, in contrast to general information security, the focus of cybersecurity is on advanced threats and on vulnerabilities that are neither easily detected nor easily remediated. *It addresses primarily those types of attacks, breaches or incidents that are targeted, sophisticated and difficult to detect or manage.*[3]

Advanced and targeted attacks have become known as APTs (Advanced Persistent Threats). According to NIST, the APT: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives. Since malware such as zero-day exploits for which signatures have not (yet) been provided are extremely difficult to recognize, very unpredictable, and often difficult to trace back to their origins, cybersecurity governance must contain both a preventive and a reactive perspective, as well as a strong focus on detection and acknowledging that some attacks may be - or already have been - successful.

Due to emerging technologies and a constantly evolving threat landscape, cybersecurity-related trends are likely to influence an organization's governance design, be it in defining roles & responsibilities, setting policies, addressing risk & compliance or preparing for incident response in case of major cyber incidents. One of these trends is that organizations are increasingly faced with the daunting task of securing borderless IT environments that embrace enabling technologies in cloud, mobile and social computing. At the same time, the emerging trends in malicious tactics imply that organizations have to defend themselves against a rising tide of increasingly sophisticated cyber attacks.

Participants in this survey were asked to indicate if they think cybersecurity-related trends are important in a governance setting and to what extent these trends are being identified and analyzed in the organization's business environment. For the purpose of this survey, trends have been organized around a limited number of themes: evolving threat landscape, emerging technologies, changes in laws & regulations, sourcing and contractual obligations. Participants were asked to what extent their organization takes these trends into account when setting the governance for cybersecurity.

3 *ISACA (2013). Transforming cybersecurity: using COBIT 5 p29.*

Identify Trends in Setting Governance

Do you think cybersecurity-related trends are important in setting governance?

Perceived versus actual scores

Figure 5 correlates the security expert opinion with the actual status for this topic. From the results it can be concluded that relative to other participants, finance-related organizations perceive taking cybersecurity-related trends into account in setting governance to be most important.

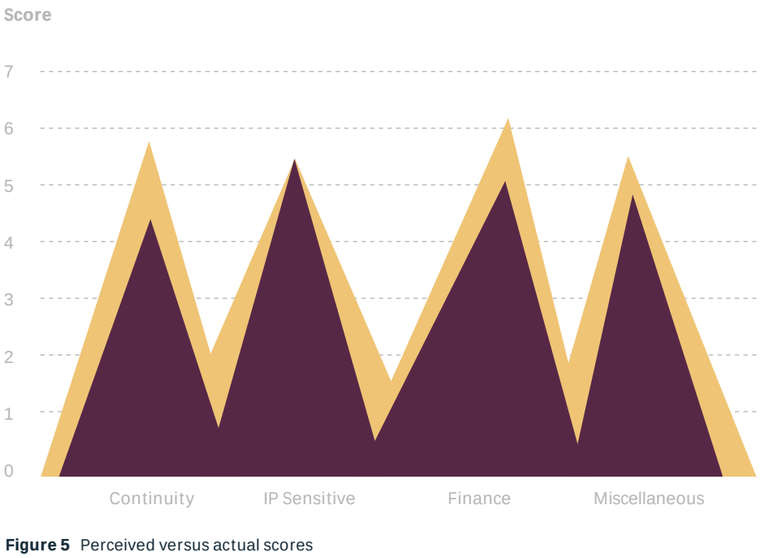


Figure 5 Perceived versus actual scores

> In setting governance dealing with contractual obligations appears to be most difficult.

Relative deviations

Figure 6 shows that, according to the respondents' expectations, finance organizations fail to give adequate attention to this topic of setting governance, with 43% of the responding organizations reporting significant deviations between perceived and actual scores.

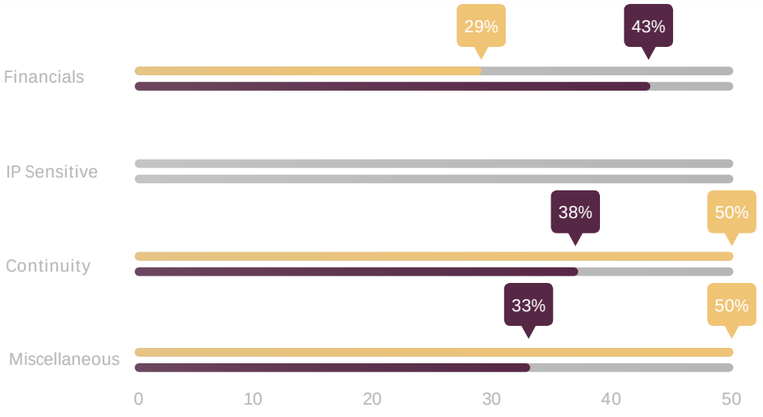


Figure 6 Relative deviations perceived versus actuals

Actual scores per cluster

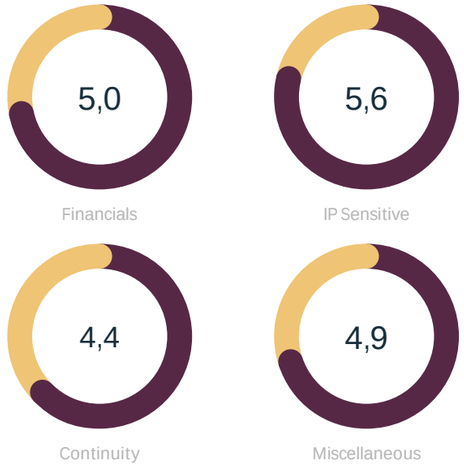


Figure 7 Actual scores per cluster on a scale 1-7

Figure 7 compares the actual scores for this topic. Participants in the IP cluster (companies with a strong focus on the protection of their intellectual properties) are more positive on this topic, relative to other clusters.

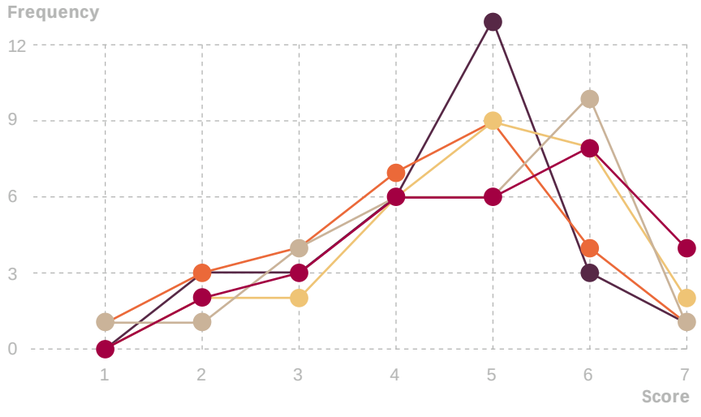


Figure 8 Actual scores per option

Actual scores per option

Figure 8 shows the distribution in scores for each option in this this topic. In this survey, participants indicate that, in setting governance, the impact of contractual obligations is the most difficult item, relative to other items.

- Evolving threat landscape
- Emerging technologies
- Legal & regulatory
- Contractual obligations
- Sourcing

What do leading security bodies say about cyber-security governance?

NIST - Cybersecurity Framework
Recognizing that the national and economic security of the United States depends on the reliable functioning of critical infrastructure, president Obama issued executive order 13636, Improving Critical Infrastructure Cybersecurity, in February 2013.

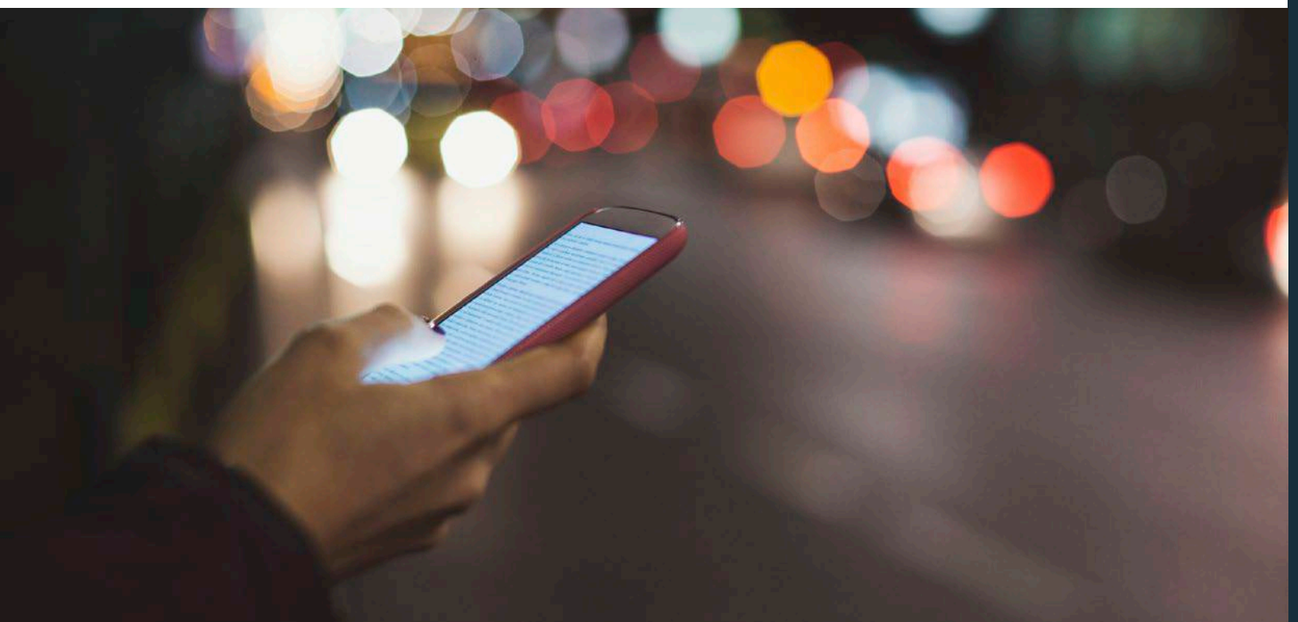
It directed NIST to work with stake-holders to develop a voluntary framework - based on existing standards, guidelines, and practices - for reducing cyber risks to critical infrastructure. NIST released the first version of the Framework for Improving Critical Infrastructure Cybersecurity on February 12th, 2014. In this framework, governance is described as: ensuring that the policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood, and informing the management of cybersecurity risk.

ISACA has written a guide to implement the Cybersecurity Framework (CSF), which will include a toolkit with sample templates for recording profiles and action plans. Using ISACA's industry-based COBIT 5 framework makes it possible to achieve CSF outcomes in an accountable, practical way.

ISF - Threat Horizon 2014
Information Security Forum (ISF) has launched the Threat Horizon 2014 report. This report challenges the traditional approach to managing security risks and recommends that organizations take a much more strategic and business-based approach to risk management.

ISO New Cybersecurity Governance and Risk Management Toolkit
The ISO New Cybersecurity Governance and Risk Management Toolkit provides organizations with a comprehensive set of pre-written and independently developed cybersecurity documents, as well as mapping them across five frameworks, including ISO 55001, ISO 27032, the BIS Ten Steps to Cyber-security, the CSA's Cloud Control Matrix and the new ISO27001: 2013 Standard.

> *To take advantage of technology and cyberspace, organizations must manage new risks beyond those traditionally covered by the information security function, including attacks on reputation and all manner of technology from telephones to industrial control systems.*
>
> *Traditional risk management is insufficiently agile to deal with the risks from activity in cyberspace. Enterprise risk management must be extended to create risk resilience, which must be built on a foundation of preparedness.* [www.securityforum.org]



Survey
4.2 | *Senior Management Commitment*

Introduction

Effective cybersecurity requires commitment and leadership from senior managers in the organization. Leadership in the cyber age requires dynamic, forward thinking to assess an organization's strengths and its limitations. As the threat landscape evolves, it underscores the need for leaders to be visionary, to embrace technological advancements, and to remain competitive in maximizing each advantage while minimizing the risk of emerging technologies. In addition, it is essential that senior management communicate expectations for strong cybersecurity throughout the organization.

Security professionals play an important role in establishing the right sense of urgency for cyber-security. They have to get C-level officers and board members involved and make cybersecurity a priority. Too often, security is a separate function that cannot prevent cybersecurity ending up in an IT- or technology-centric discussion. Failing to get across why a threat actor might be interested in the organization makes it very difficult to think of cybersecurity in a strategic way. So instead of letting cyber-security be downgraded in a way that makes it less important, the security function should come up with a holistic plan with a focus on business objectives. It has to understand the organizations' mission, elicit a dialogue around business risk, and produce a written strategy that is supported and signed off by all stakeholders.

> "It's essential that senior management communicate expectations for strong cybersecurity throughout the organization."

Participants in this survey were asked to indicate whether they think senior management/board level commitment is important for cybersecurity and to what extent this can be demonstrated for their organization. Commitment can be demonstrated in many ways. In this survey, five indicators were used to demonstrate senior management commitment:

- Explicitly recognizing the exposure to cybercrime;
- Itemizing cybersecurity on the board agenda, on a regular basis;
- Communicating expectations for strong cybersecurity throughout the organization;
- Establishing a structure for the implementation of a cyber-security program;
- Having the status of cybersecurity programs reported to the board.

Senior Management Commitment

Do you think senior management/board level commitment and leadership are important to cybersecurity?

Perceived versus actual scores

Figure 9 correlates the security expert opinion with the actual status for this topic. From the results it can be concluded that nearly all participants indicate commitment of senior management to be very important for cybersecurity.

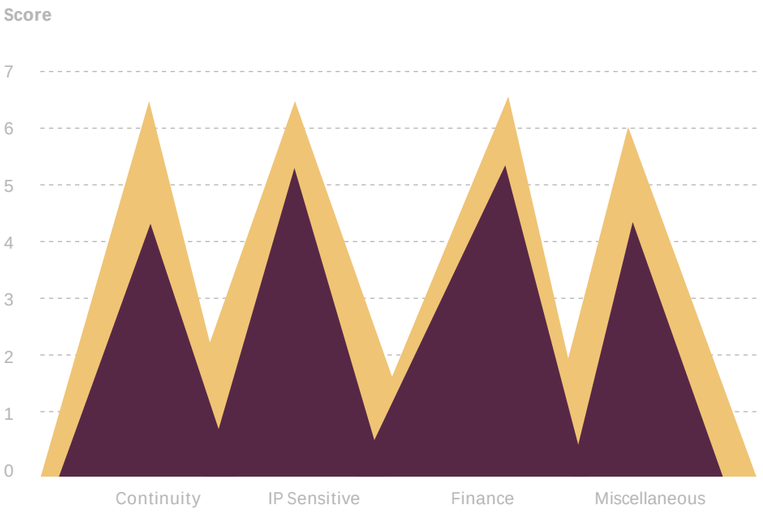


Figure 9 Perceived versus actual scores

> Senior management commitment is demonstrated most in recognizing the exposure to cybercrime.

Actual scores per cluster

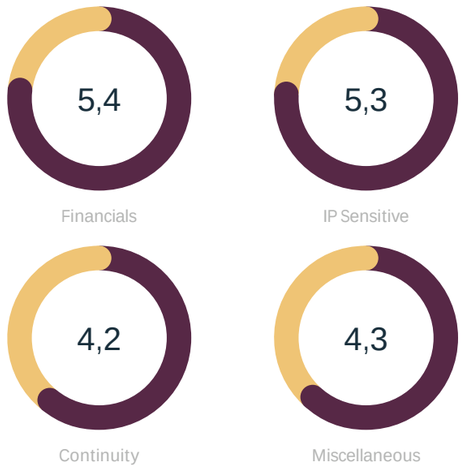


Figure 11 Actual scores per cluster on a scale 1-7

Figure 11 compares the actual scores for this topic. Participants in the Finance and IP clusters are more positive on this topic, relative to other clusters.

Relative deviations

Figure 10 shows expectations are most met in finance- and IP-sensitive organizations, showing the least number of deviations between perceived and actual scores.

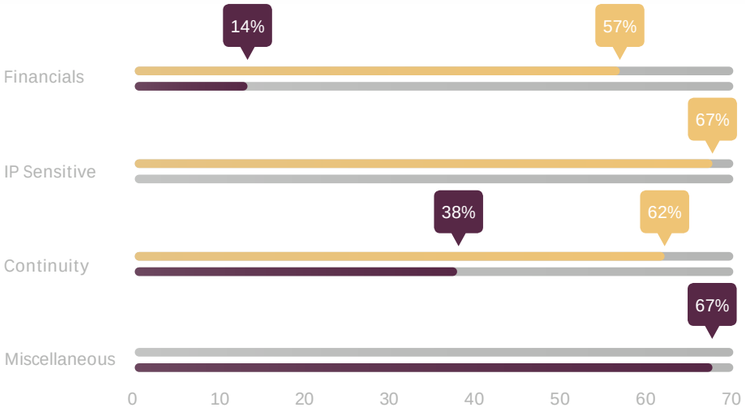


Figure 10 Relative deviations perceived versus actuals

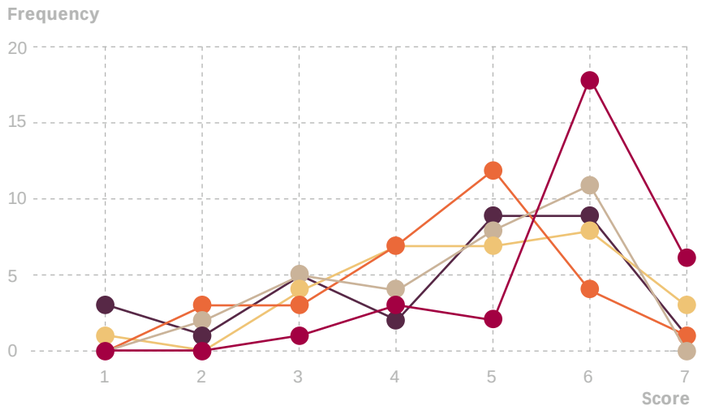


Figure 12 Actual scores per option

Actual scores per option

According to figure 12, senior management commitment is demonstrated most in recognizing the exposure to cybercrime and shows least in having the status of the security program reported to the board.

- Recognizing exposure to cybercrime
- Cybersecurity on the board agenda
- Communicating expectations
- Implementation cybersecurity program
- Status of cybersecurity programs reported

Leadership guidance

According to Gary Cohen, leaders cannot be expected to know everything, especially today. With information accumulating at such a rapid pace and with so many ways to access information, associates routinely know more about their work than their executives do. Asking the right questions about cybersecurity, often to several different people, helps identify vulnerabilities, exposes defects and identifies potential areas of improvement.[4]

The U.S. Department of Homeland Security helps to guide leadership discussions about cybersecurity.[5]

7 questions CEOs should ask about cyber risks:

1. *How is our executive leadership informed about the current level and business impact of cyber risks to our company?*
2. *What is the current level and business impact of cyber risks to our company?*
3. *What is our plan to address identified risks?*
4. *How does our cybersecurity program apply industry standards and best practices?*
5. *How many cyber incidents do we detect in a normal week and what types are they?*
6. *What is the threshold for notifying our executive leadership?*
7. *How comprehensive is our cyber incident response plan? How often is it tested?*

Figure 13 Seven questions CEOs should ask about cyber risks

4 *Garry B. Cohen (2009). Just Ask Leadership: Why Great Managers Always Ask the Right Questions p1.*

5 *U.S. Department of Homeland Security Publication, https://www.us-cert.gov/sites/default/files/publications/DHS-Cybersecurity-Questions-for-CEOs.pdf*

Survey
4.3 | *Stakeholders*

Introduction

Cybersecurity governance is driven by knowing the organization's stakeholders and defining their needs and wants for the purpose of protecting their interests. Amongst these needs, stakeholders should be able to rest assured that adequate protection is in place, commensurate with the level of business or other activities being done over the Internet. In determining reasonable levels of protection, one may find specific cybersecurity-related needs and expectations to be somewhat different from regular information security requirements.

The organization's stakeholders include both internal- and external stakeholders. In an ideal situation all stakeholders should work together and foster rapid information sharing to achieve broader cybersecurity situational awareness.

From an internal perspective, all users can be considered stakeholders in cybersecurity, regardless of their hierarchical level within the organization.

Internal stakeholders include, but are not limited to, end users, IT practitioners, business managers, security experts, audit-, compliance- and risk managers, on- and offsite contractors, and consultants. Relationships between an organization and its associates are important not only to be able to communicate cyber risks internally but also to involve personnel proactively to detect threats and vulnerabilities and to identify cyber issues before they get out of control. In particular, internal relationships between the security function, the IT community and various business stakeholders have to be managed to align both emerging trends in cybersecurity and business expectations of IT.

External stakeholders may include: shareholders, investors, regulatory bodies, customers, suppliers and other business partners. These shareholders are increasingly interested in an organization's current cybersecurity posture including risk profiles, risk tolerances and cyber incidents. They expect an organization to have effective conditions in place to protect their interests by mitigating cyber risks. Moreover, they expect to be adequately informed during crisis situations.

Participants in this survey were asked if they thought it was important to know to what extent cybersecurity is capable of meeting stakeholder needs. To indicate the current situation for their organization, the follow-up question referred to communication with certain groups of stakeholders: investors/shareholders, regulatory bodies, internal stakeholders, customers and suppliers/vendors.

> "All stakeholders should work together and foster rapid information sharing to achieve broader cybersecurity situational awareness."

Stakeholders in Cybersecurity

Do you think it is important to know to what extent cybersecurity is capable of meeting stakeholder needs?

Perceived versus actual scores

Figure 14 correlates the security expert opinion with the actual status for this topic. From the results it can be concluded that relative to other participants, IP-sensitive organizations perceive meeting stakeholder needs to be most important.

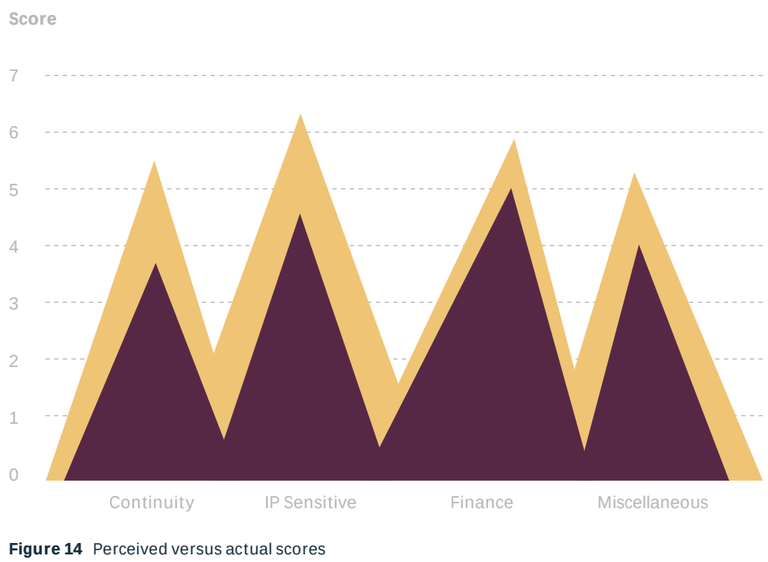


Figure 14 Perceived versus actual scores

> Suppliers and vendors are least recognized as important stake-holders in cybersecurity.

Actual scores per cluster

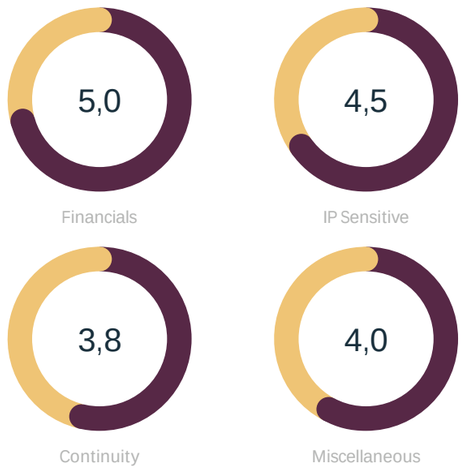


Figure 16 Actual scores per cluster on a scale 1-7

Figure 16 compares the actual scores for this topic. Participants in the finance sector report the highest actual scores, relative to other clusters.

Relative deviations

According to figure 15, continuity-sensitive organizations show the most significant deviations between perceived and actual scores, thus indicating that, according to the respondent's expectations, these organizations fail to give adequate attention to meeting stakeholders needs.

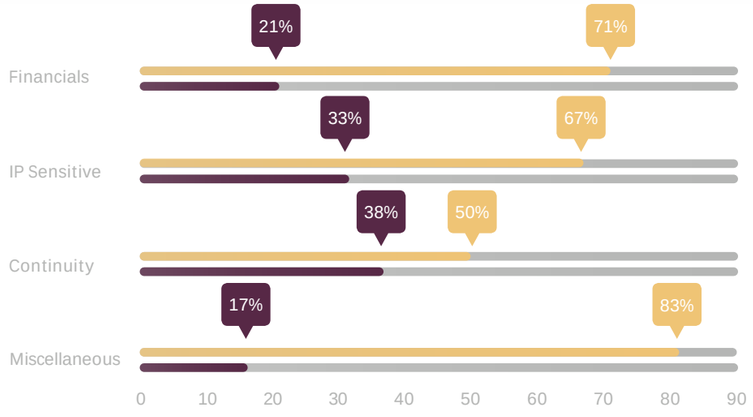


Figure 15 Relative deviations perceived versus actuals

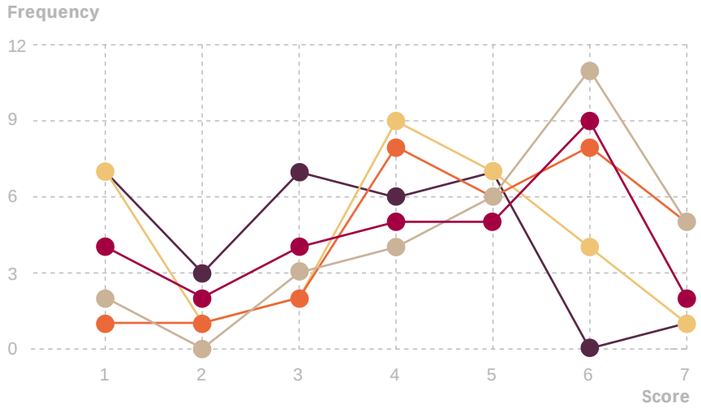


Figure 17 Actual scores per option

Actual scores per option

Figure 17 shows the distribution in scores for each option in this this topic. In this survey, participants indicate that in relative terms, suppliers and vendors are least recognized as important stakeholders in cybersecurity.

- Investors / shareholders
- Regulatory bodies
- Internal stakeholders
- Customers
- Suppliers / Vendors

Communicating with stakeholders in a crisis situation

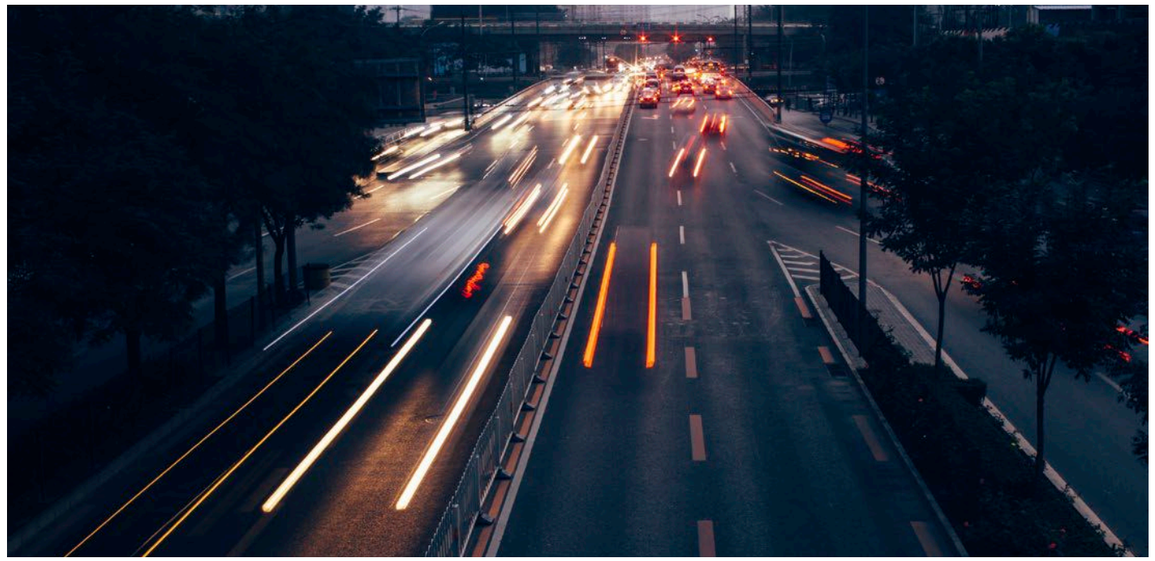
Organizations need to have a plan in place on how to communicate in the event that operations have to take place in a degraded capacity. When confronted by a crisis such as in the case of a cyber attack, it is essential to have open lines of communication with all relevant stakeholders, including customers and business partners. In addition, external relationships with third parties should be anticipated to strengthen cybersecurity capabilities and to help in an adequate response once a breach has occurred. Third-party services include breach investigation and eradication, forensic support, managed services for security monitoring, Denial of Service (DoS) response and malware analysis.

Stakeholders expect their investments to be well protected. In crisis situations they expect to be kept informed in a manner that retains their trust and confidence. Especially critical are the early hours after the event, as is the tone of the communication.

The organization should be prepared to answer a number of key questions, including but not limited to:
- What happened?
- What is the impact?
- What is to be done about it?
- How can we prevent this happening again?
- What have we learned?

Briefings to stakeholders about the results should be well planned and conducted soon after the event. An initial, high-level communication can be issued within one day of the event, followed by a detailed explanation of the activities that took place.

Communication should be clear, concise and focused on problem resolution. It should clearly identify any gaps that remain and propose efforts to mitigate them. It is also important that communications demonstrate lessons learned and identify any new processes created as a result of the effort to make similar eradication events or activities more efficient and less taxing on the organization.[6]



6 *ISACA (2013). Responding to targeted attacks p74.*

Survey
4.4 | *Compliance*

Introduction

The presence of cybercrime has given rise to a vast number of legislative and regulatory initiatives on a global basis. The full impact in a legal and regulatory sense is yet to be seen but cybersecurity is increasingly governed by new mandatory rules that need to be adhered to.[7] As new cybersecurity regulators emerge across the globe, organizations will need to make great efforts to set up the policies, processes and training regimes that will be required to prove compliance.

The legal and regulatory landscape is rather diverse on an international level. Regulators in different countries struggle with privacy considerations that have to be weighed against conflicting legal objectives and the public interest. In some countries, cybersecurity legislation cannot be passed due to political differences concerning how much liability protection to grant businesses in order to get them to share cyber threat information. On the other hand, public authorities need to be able to create cyber awareness and launch defensive cyber operations, which can only happen if there is a high degree of information sharing between the private sector and local government.

Many companies have to comply with e.g. PCI/DSS, HIPAA, and Data Protection Laws, and have numerous security controls in place that can in some way be justified by mandatory legal or regulatory compliance requirements. However, cybersecurity is somewhat different and requires actions that go well beyond the measures required to satisfy compliance demands. Eliminating Advanced Persistent Threat (APT) risk requires levels of security technology, management, education, skills and vigilance that go far beyond the demands of regulatory compliance and everyday information security management. Moreover, regulatory compliance requirements have been progressively forcing enterprises to be more open about their security posture and incidents.

> “Cybersecurity is increasingly governed by new mandatory rules.”

In acknowledging all these trends, companies have to anticipate meeting new compliance needs as they arise in the legal and regulatory landscape.

Participants in this survey were asked if they thought it was important to anticipate new cybersecurity-related regulations in security- and compliance management, and to what extent this could be demonstrated for their organization. Anticipating compliance in this context can be demonstrated in many ways. In this survey five indicators were used to demonstrate that an organization is anticipating cybersecurity:
- Identifying any applicable laws or regulations while reviewing and updating policies and procedures to ensure that IT- and business processes are compliant;
- Setting up the relevant policies, processes and training regimes;
- Assessing the impact on contractual obligations;
- Evaluating the extent to which cybersecurity provisions meet business and compliance/ regulatory needs;
- In vendor management, assessing and reviewing suppliers for cybersecurity compliance.

7 *ISACA (2013). Transforming cybersecurity: using COBIT 5 p26.*

Anticipate Compliance in Cybersecurity

Do you think it is important to anticipate new cybersecurity-related regulations in security- and compliance management?

Perceived versus actual scores

Figure 18 correlates the security expert opinion with the actual status for this topic. From the results it can be concluded that relative to other participants, IP-sensitive organizations perceive anticipating new cybersecurity-related regulations in security- and compliance management to be most important.

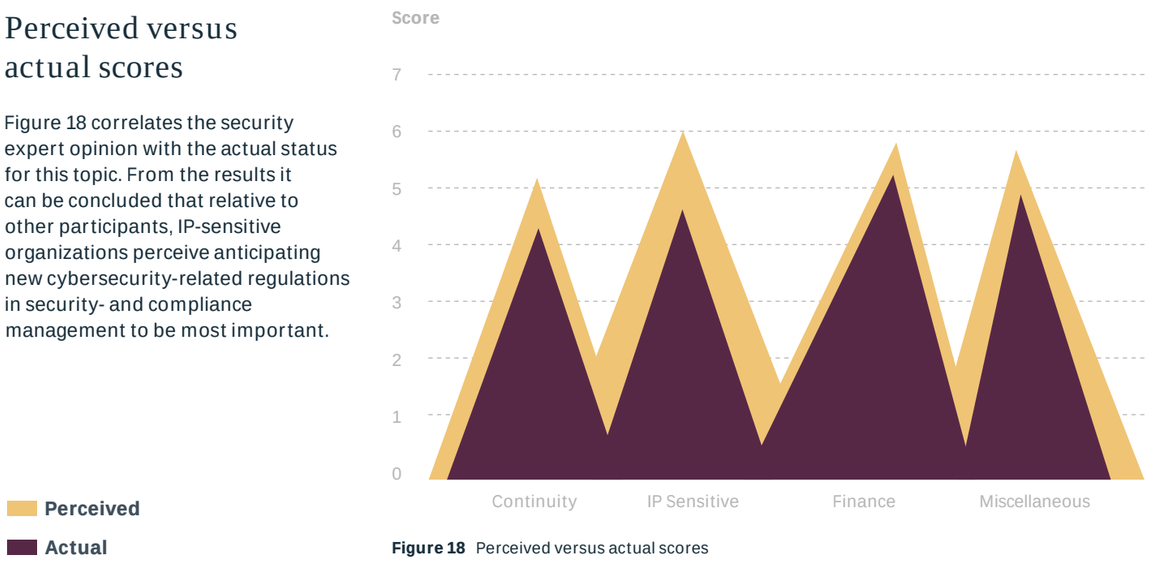


Figure 18 Perceived versus actual scores

> In cybersecurity, assessing and reviewing suppliers for compliance appears to be most difficult.

Actual scores per cluster

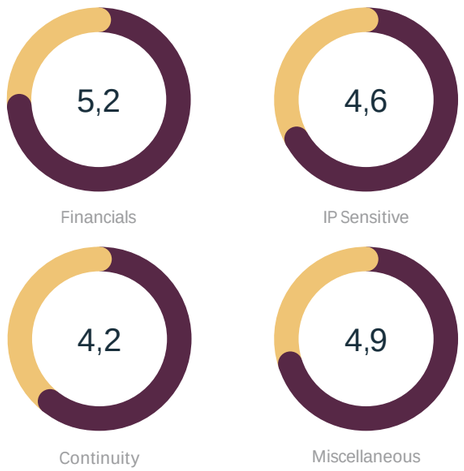


Figure 20 Actual scores per cluster on a scale 1-7

Figure 20 compares the actual scores for this topic. Participants in the finance sector report the highest actual scores, relative to other clusters.

Relative deviations

Figure 19 shows many deviations for IP-sensitive organizations, indicating that on the topic of anticipating new cybersecurity-related regulations much still needs to be done.

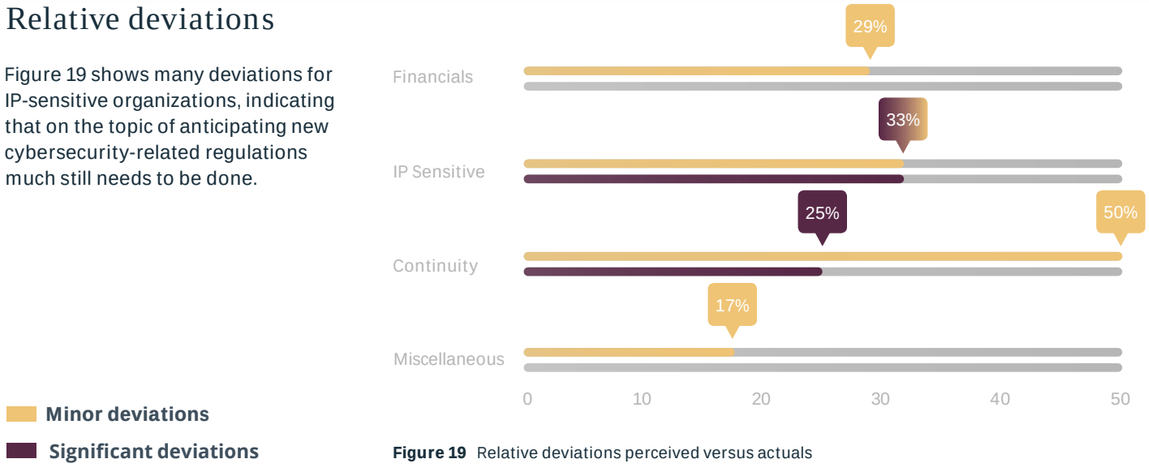


Figure 19 Relative deviations perceived versus actuals

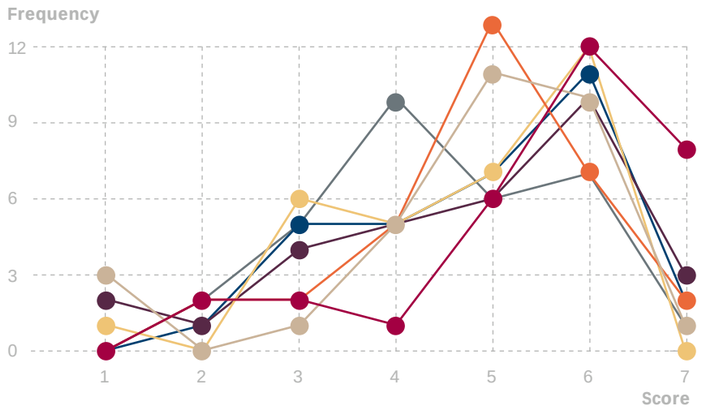
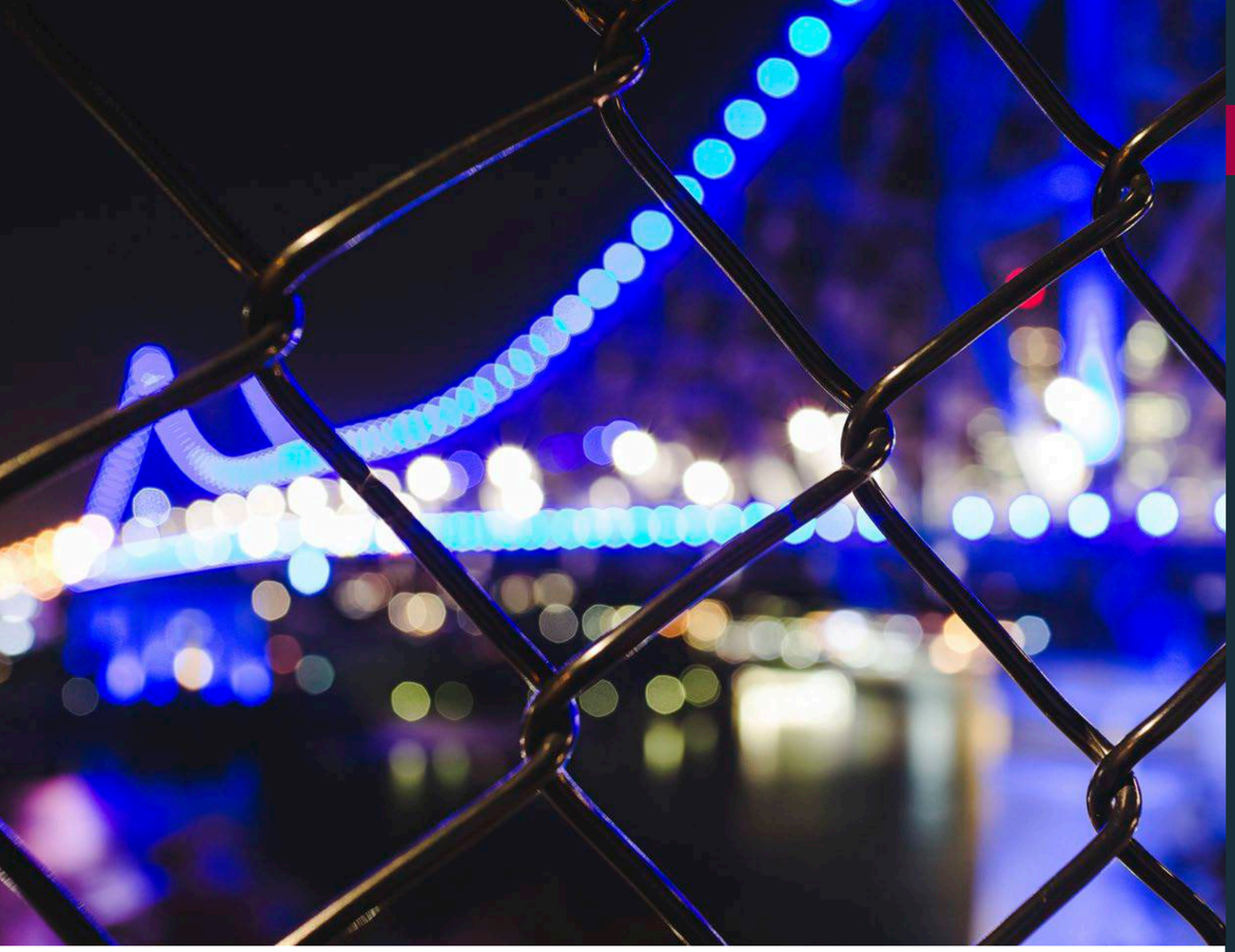


Figure 21 Actual scores per option

Actual scores per option

Figure 21 shows the distribution in scores for each option in this this topic. In this survey, participants indicate that, in anticipating compliance in cybersecurity, assessing and reviewing suppliers for compliance seems to be the most difficult topic.

- Identifying applicable laws or regulations
- Assessing impact on contractual obligations
- Cybersecurity provisions meet business and compliance/regulatory needs
- Setting up the policies, processes and training regimes
- Notify regulators in the event of a data breach
- Creating new processes, acquiring new technology to comply
- Assessing and reviewing suppliers



Regulatory communications

In the US, the Securities and Exchange Commission (SEC) issued "CF Disclosure Guidance: Topic2, cybersecurity" (CF DG2), which is a guideline for businesses on communicating cybersecurity risks. The EU has a different approach: "Given the complexity of the issue and the diverse range of actors involved, centralized, European supervision is not the answer. National governments are best placed to organize the prevention and response to cyber incidents and attacks and to establish contacts and networks with the private sector and the general public across their established policy streams and legal frameworks".[8]
An example is the Dutch initiative: "Responsible Disclosure" that stimulates vigilance and facilitates a secure communication of detected vulnerabilities.

Still, many companies remain reluctant to admit they have been victims of similar attacks, although regulatory compliance requirements have been progressively forcing enterprises to be more open about their security incidents. Companies are caught between informing investors and other stakeholders about the cyber risks to which they are exposed and a number of valid reasons not to disclose cybersecurity risk because of negative effects, e.g.:

- disclosing cybersecurity risk may attract hostile bad actors who will try to exploit vulnerabilities and cause damage;
- loss of investor confidence;
- increased risk of liability lawsuits;
- loss of brand reputation;
- loss of share value.

Companies have to make their own assessment on what cybersecurity information to publicly disclose. Increasingly, major companies such as Google and Amazon are deciding to do so.

8 *High Representative of the European Union for Foreign Affairs and Security Policy (2013). Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace p17.*

Survey
4.5 | *Strategy*

Introduction

A strategy for approaching and managing cybersecurity activities and cyber risks will help target an organization's goals and provide a roadmap for the evolution of an organization's cyber effort. It will provide both a long-term roadmap for technology integration and risk management and assures that an organization remains viable in today's highly competitive business landscape. At the same time, it will include a strategic component that deals with unexpected and unknown threats and contains elements of business continuity and IT service continuity.

In many situations, incorporating cybersecurity into a business strategy is an afterthought. Methods and techniques to create a strategy for cybersecurity are numerous and in most cases describe a way to migrate from an as-is to a to-be situation. While building a strategy for cybersecurity, the following questions may guide the process:

Where are we now?
Where do we want to be?
How do we get there?

In the initial phase the goal is to create a profile that relates to the current cybersecurity posture. Key stakeholders will take a lead in indicating what it takes to attain the mission goals. From this analysis it can be determined which activities, assets and resources in terms of people, processes and technologies are truly mission-critical and have impact on the organization. Understanding the overarching threats to, and vulnerabilities of, those resources and assets helps to establish the current profile.

Assessing "Where do we want to be?" depends on many factors, including type of industry, available resources and risk appetite. Knowing where the organization is today, a number of follow-up questions may help define the to-be state, e.g.:
Does the value of intellectual properties and trade secrets justify significant investments in cybersecurity?
Is the corporate brand enhanced when protected by cybersecurity practices?
How much risk is to be accepted when it comes to cybersecurity?
Are skills and competences sufficiently available to execute cybersecurity in-house?
The next step is to use the current and to-be profiles to create goals and objectives to achieve the desired outcomes. To be effective, cybersecurity needs to be a part in decision-making and all relevant plans, policies and procedures.

"How much protection is needed?"

Participants in this survey were asked if they thought that having a cybersecurity strategy was important. Next they were asked if the organization they represented actually had developed a documented cybersecurity strategy. To be more specific, certain topics were raised that may typically be included in a cybersecurity strategy:

- Providing a link to the organization's objectives;
- Addressing the balance between benefits, costs and risks;
- Meeting business- and compliance/regulatory needs;
- Providing a link to the IT strategy;
- Providing a link to the business continuity plan;
- Providing a link to risk acceptance levels.

Define Cybersecurity Strategy

How do you perceive the importance of having a cybersecurity strategy?

Perceived versus actual scores

Figure 22 correlates the security expert opinion with the actual status for this topic. From the results it can be concluded that relative to other participants, continuity-sensitive organizations perceive cybersecurity strategy to be most important.

Figure 22 Perceived versus actual scores

> Balancing between benefits, costs and risks appears to be the most difficult topic in defining cybersecurity strategy.

Actual scores per cluster

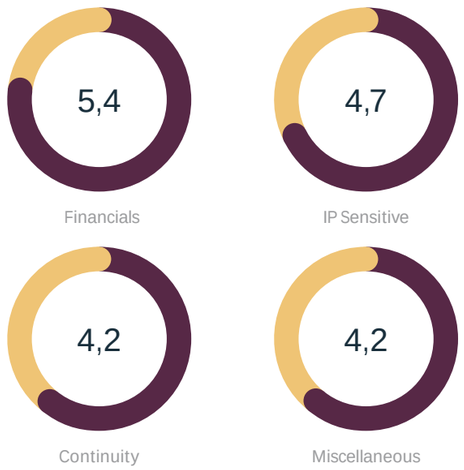


Figure 24 Actual scores per cluster on a scale 1-7

Figure 24 compares the actual scores for this topic. Participants in the finance sector report the highest actual scores on cybersecurity strategy, relative to other clusters.

Relative deviations

Figure 23 shows that, relative to other participants, continuity-sensitive organizations fail to give adequate attention to this topic. In this cluster, half of the responding organizations report significant deviations between perceived and actual scores.

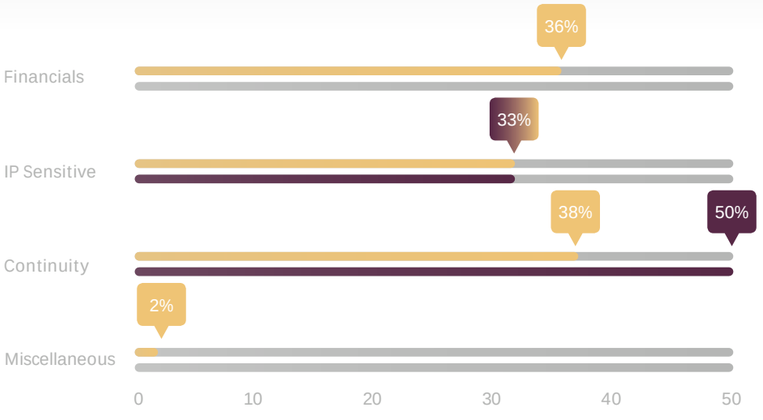


Figure 23 Relative deviations perceived versus actuals

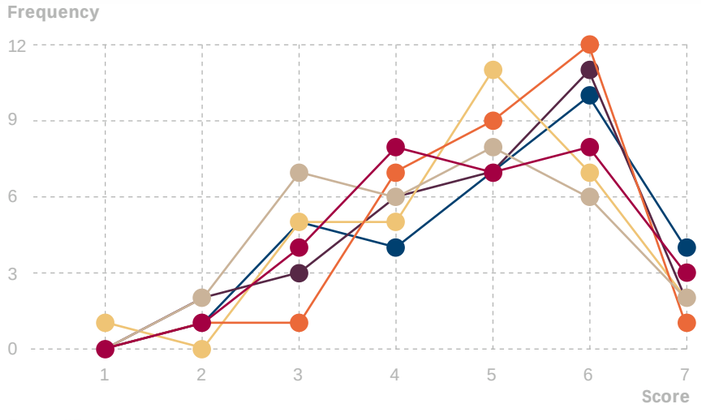


Figure 25 Actual scores per option

Actual scores per option

Figure 25 shows the distribution in scores for each option in this this topic. In this survey, participants indicate that, in cybersecurity strategy, balancing between benefits, costs and risks seems to be the most difficult topic.

- That provides a link to the organization's objectives
- That addresses the balance between benefits, costs and risks
- That addresses meeting business - and compliance/regulatory needs
- That provides a link to the IT strategy
- That provides a link to the business continuity plan
- That provides a link to risk acceptance levels

> The true organization is so prepared for battle that battle has been rendered unnecessary.
>
> *- Sun Tzu -*

Elements to address in a cybersecurity strategy

Goals and objectives are at the heart of cybersecurity planning. An organization's typical goals for cybersecurity may include:

- Reduce exposure to cyber risks;
- Maintain the ability to detect, respond and recover;
- Enable secure information exchange anytime, anywhere by authorized users;
- Maintain the security of information and IT infrastructure;
- Provide IT systems that are reliable and secure;
- Ensure compliance with laws and regulations;
- Control all Internet connections;
- Maintain positive control over all information;
- Ensure all employees are trained in cybersecurity best practices.

From these goals, cybersecurity objectives may be derived to specify specific, measurable and time-relevant statements of what is going to be achieved and when, e.g.:

Goal: Reduce exposure to cyber risks

Objective 1: implement an intrusion detection system by the second quarter of this fiscal year

Objective 2: install security patches within 24 hours of their release from trusted sources

Objective 3: conduct initial cyber-security training for 100% of new employees within three days of employment and before granting access to information systems.[9]

9 Gregory J. Touhill, C. Joseph Touhill (2014). Cybersecurity for Executives - A Practical Guide p110.

Survey
4.6 | *Risk Management*

Introduction

Cyber-resilient organizations that actively integrate cyber risks into their risk programs will consider their risk appetite and tolerance levels, taking a 360-degree risk approach, examining all areas within the organization, prioritizing risks, and developing appropriate strategies to address all risks, including the cyber risk.

Identifying and managing cyber risks is no different than traditional risk management, being a continuous cycle of assessing risks, allocating mitigating controls, implementing remedial actions and monitoring their effectiveness. However, the focus from a cybersecurity perspective is, in the early stages of the risk management process, very much on advanced threats and vulnerabilities that are neither easily detected nor easily remediated. The starting point in every risk management process is to have a clear view on those assets that are truly mission-critical and to understand the corresponding weaknesses as well as the likelihood of someone exploiting potential vulnerabilities. Some of the cybersecurity specific activities include detecting the so-called "tell-tale signs" of an advanced persistent threat (APT) and perform post-mortem analyses of past attacks, incidents and instances of successful breaches. In addition, there are certain times at which a heightened alert is to be considered, e.g. following publicity of new products or services, when entering new markets, when negotiating major contracts, or when following an identified vulnerability.[10]

As independent research initiatives continuously report the majority of breaches to be discovered by external parties, it becomes clear that own (internal) defenses are insufficient to stop a targeted attack. Therefore, verifying external threat sources is an important part of cyber vulnerability assessments. Cyber threat intelligence may be obtained from vendor threat feed subscriptions or from public sources such as the ENISA Threat Landscape or the Verizon annual Data Breach Investigation reports. As to risk mitigation, unfortunately there is no single additional countermeasure, technical or operational, that can be guaranteed to prevent, detect or eradicate an APT infection. The solution from a cybersecurity perspective lies in an holistic approach that combines tighter physical, technical, educational, and operational measures, coordinated through an effective security management system.

In their April 2014 Nexus report, the Atlantic Council/Zurich made a case for cyber risk management in forward-looking organizations to take an holistic view and look beyond the internal IT enterprise for aggregations of risk. They argue that cyber risk is not self-contained within individual enterprises and that advanced organizations should push out their risk horizon and expand their view of risk management, taking into account seven aggregations of risk:

1. Risks from the internal IT enterprise
2. Risks from counterparts and partners
3. Outsourcing- and contractual risks
4. Supply chain risks
5. Upstream infrastructure failures
6. Disruptive technology risks
7. External shocks

For risk managers it may be helpful to visualize the seven aggregations in three distinct zones: "near", "everywhere" and "distant". A corporate risk manager can have the most impact on the "near zone", his influence shifting to assessing contractual relations in the "everywhere zone" and further reducing to acknowledging government initiatives when it comes to the "distant zone".[11]

10 ISACA (2013). Advanced Persistent Threats: How to Manage the Risk to Your Business p72-73.
11 Jason Healy (2014). Beyond data breaches: global interconnections of cyber risk p13.

Manage Cyber Risks

Do you think it is important to integrate cyber risks into an organization's risk program?

Perceived versus actual scores

Figure 26 correlates the security expert opinion with the actual status for this topic. From the results it can be concluded that relative to other participants, IP-sensitive organizations perceive risk management to be most important.

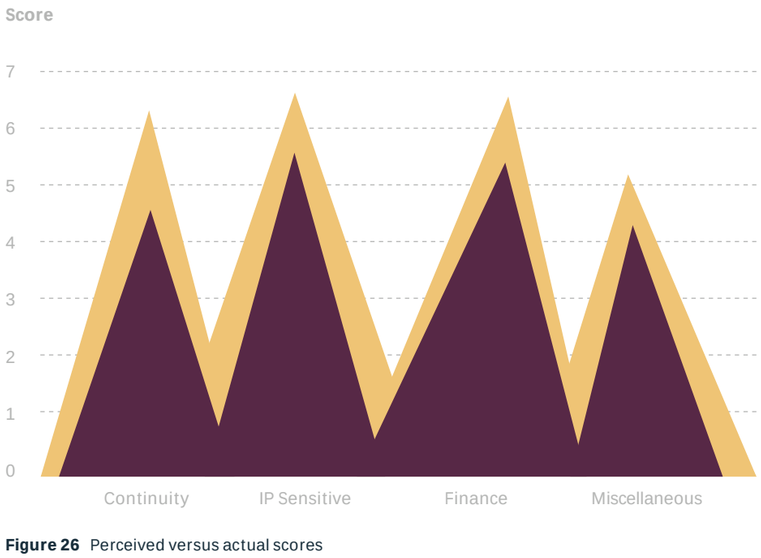


Figure 26 Perceived versus actual scores

> The focus from a cybersecurity perspective is very much on advanced threats and vulnerabilities that are neither easily detected nor easily remediated.

Actual scores per cluster

Figure 28 Actual scores per cluster on a scale 1-7

Figure 28 compares the actual scores for this topic. Participants in the IP cluster (companies with a strong focus on the protection of their intellectual properties) are more positive on this topic, relative to other clusters.

Relative deviations

Figure 27 shows that, according to the respondents' expectations, IP-sensitive organizations seem to do quite well on this topic, reporting the highest scores and showing the least number of deviations between perceived and actual scores.

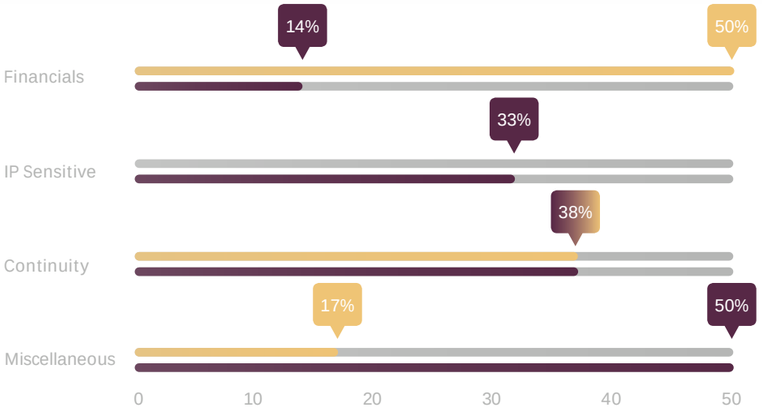


Figure 27 Relative deviations perceived versus actuals

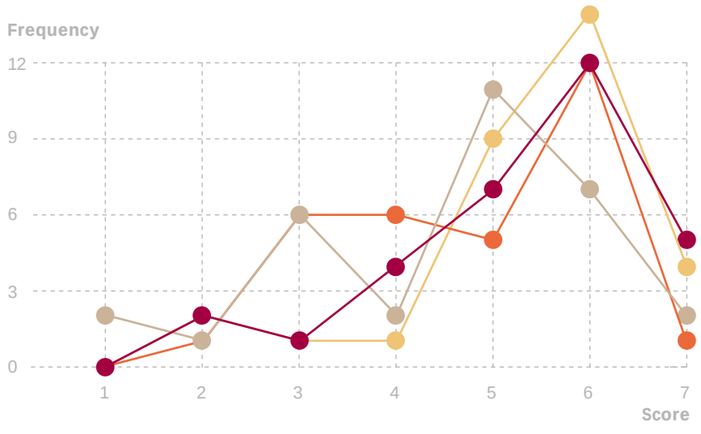


Figure 29 Actual scores per option

Actual scores per option

Figure 29 shows the distribution in scores for each option in this this topic. In this survey, participants indicate that, in cybersecurity risk management, setting priorities, managing investments and measuring progress seem to be most difficult.

- **If critical information is unavailable, compromised or lost**
- **To set priorities, manage investments, measure progress**
- **The consequence of a major cyber security incident**
- **If infrastructure became inoperable**

Focus on Risk Management

In an effort to grow as a risk-aware organization, a cyber-resilient organization anticipates possible cyber threats and rapidly responds to unanticipated events. For the purpose of cyber risk management, many frameworks can be used and there will likely be some overlap between them.

The NIST Cybersecurity Framework (CSF) has been established to leverage existing international approaches, standards, and practices with a focus on risk management. The framework consists of three components: core, tiers and profiles. The core refers to a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. It consists of the five functions Identify, Protect, Detect, Respond and Recover, providing a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk. Framework implementation tiers give information on how to achieve these outcomes/ activities. The profiles are a model to actually record the results and to do risk assessments.

CSF implementation is guided in a seven-step approach:
Step 1 - Prioritize and scope
Step 2 - Orient
Step 3 - Create a current profile
Step 4 - Conduct a risk assessment
Step 5 - Create a target profile
Step 6 - Determine, analyze and prioritize gaps
Step 7 - Implement action plan

Survey
4.7 | *Budget*

Introduction

In many cases an organization considers funding based on next year's security program needs, objectives and planned investments. Organizations rarely or never include a potential loss of revenue caused by a cyber breach when budgeting for security. With cybersecurity, budgeting has to be placed in a wide perspective, as more and more organizations feel the need to prioritize their security spending decisions based on real expectations of the impact on revenue if cyber thieves steal crucial intellectual property (IP) or on major discontinuities due to denial of service attacks.

Intellectual property is hard to value. It gives an organization competitive advantage that translates to increased profits. To calculate possible impact on revenue, this profit value has to be taken into account, along with other cost components such as the cost to develop, maintain and replace information assets, but also the cost if this information is not available.[12]

One difficulty in determining the right amount of spending on cybersecurity lies in quantifying loss estimates based on scale and effect. The cost of malicious cyber activity involves more than the loss of financial assets or intellectual property as it affects competitiveness, pace of innovation and brings damage to brand and reputation. In addition, a loss of confidential information might have considerable negative impact in many areas e.g. in negotiation- and contracting situations.

On the other hand, cyber criminals may take a company's product plans, research results and customer list but this does not mean this information is really lost. The company still has this information and may not even know that it no longer has control over that information. Moreover, stolen IP might not immediately benefit the acquirers as it may take considerable time to create a competing product. The same may apply to the cost of service disruptions. If the website of an online retailer is taken offline, customers may simply defer their purchases.[13]

Finally, the budgeting process might anticipate the cost of "cleaning up after cyber incidents" as well as the cost of increased spending on cybersecurity after a breach has taken place. Several sources may be helpful in defining the cost of a data breach such as the annual Ponemon study on the Cost of Data Breach. To calculate the average cost of a data breach, the Ponemon Institute collects both the direct and indirect expenses incurred by the organization. Direct expenses include engaging forensic experts, outsourcing hotline support and providing free credit monitoring subscriptions and discounts for future products and services. Indirect costs include in-house investigations and communication, as well as the extrapolated value of customer loss resulting from turnover or diminished acquisition rates.

Participants in this survey were asked if they thought budgets were important to accommodate an effective cybersecurity program. Next, they were asked if they thought budget space was sufficient to adequately accommodate cybersecurity programs in the organization they represented. Six items were specified that might be part of such a cybersecurity program:
- Training and awareness campaigns;
- IT capabilities to protect against malware, external attacks and intrusion attempts;
- Process redesign;
- Preparation for incident response;
- Operating expenses;
- Enhancing the Information Security Management System (ISMS).

12 Gregory J. Touhill, C. Joseph Touhill (2014). Cybersecurity for Executives - A Practical Guide p287-288.
13 McAfee (2013). The Economic Impact of Cybercrime and Cyber Espionage p8.

Adequate Budgets to Accommodate Cybersecurity

How important do you think budgets are to accommodate an effective cybersecurity program?

Perceived versus actual scores

Figure 30 correlates the security expert opinion with the actual status for this topic. From the results it can be concluded that relative to other participants, finance organizations perceive budget space for cybersecurity to be most important.

Figure 30 Perceived versus actual scores

> Cyber crime is the greatest transfer of wealth in human history.

Actual scores per cluster

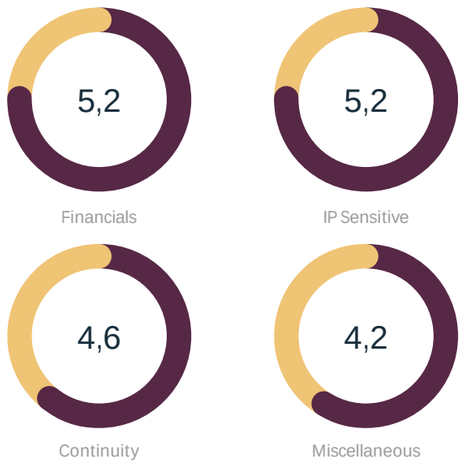


Figure 32 Actual scores per cluster on a scale 1-7

Figure 32 compares the actual scores for this topic. Both participants in the finance sector and in the IP-sensitive cluster report the highest actual scores, relative to other clusters.

Relative deviations

Figure 31 shows that for this topic none of the participants perceive many deviations between perceived and actual scores, thus indicating that, when it comes to cybersecurity budgets, these organizations meet expectations, according to the expert's opinion.

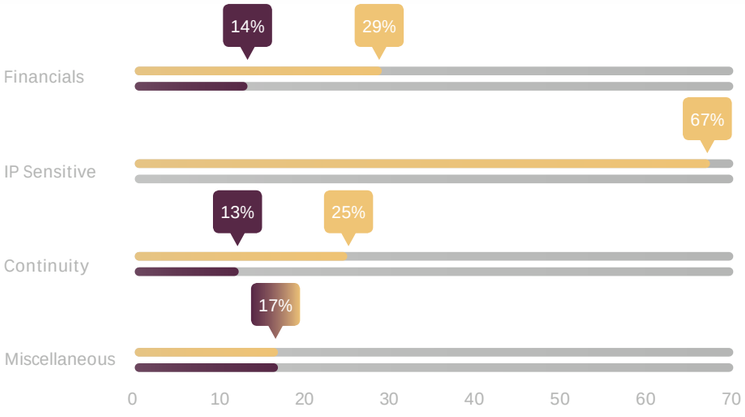


Figure 31 Relative deviations perceived versus actuals

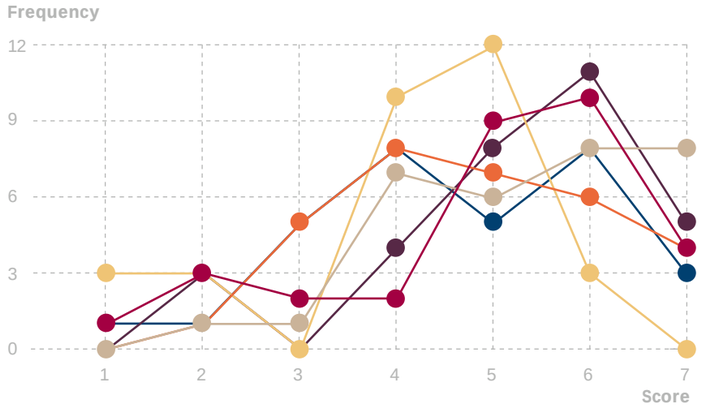
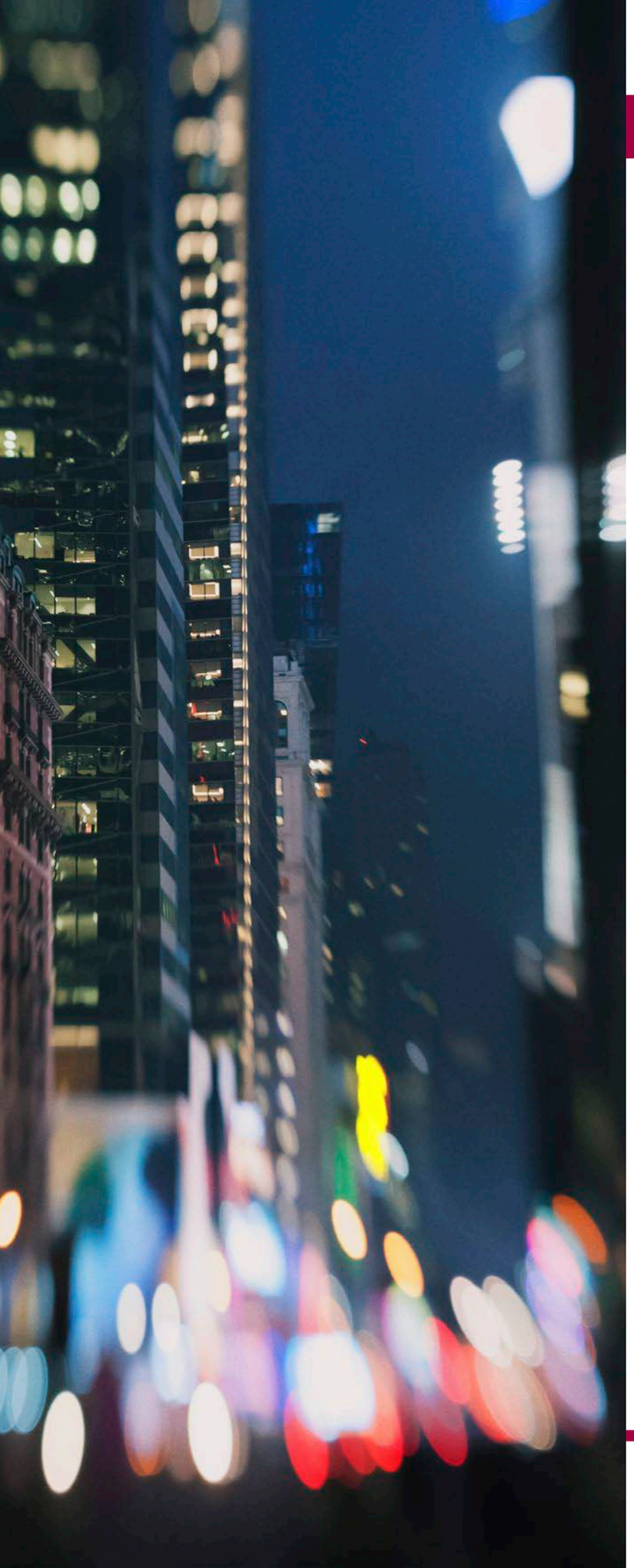


Figure 33 Actual scores per option

Actual scores per option

Figure 33 shows the distribution in scores for each option in this this topic. In this survey, of all reference items, enhancements to the Information Security Management System (ISMS) seems to be the most difficult part in cybersecurity budgeting.

- Training and awareness campaigns
- IT capabilities
- Architectural provisions
- Process redesign
- Preparation for incident response
- Enhancing the ISMS



Cost of cybercrime

In their 2013 study, the Ponemon Institute identified seven factors that influence the cost consequences of a data breach incident:

1. Organizations had a data breach incident management plan in place at the time of the data breach event.
2. The company had a relatively strong security posture at the time of the incident.
3. CISO (or equivalent title) has overall responsibility for enterprise data protection. Organizations have centralized the management of data protection with the appointment of a C-level information security professional.
4. Data was lost due to third-party error. Organizations had a data breach caused by a third party, such as vendors, outsourcers and business partners.
5. The company notified data breach victims quickly. Organizations notified data breach victims and/or regulators within 30 days of the discovery of data loss or theft.
6. Organizations had a data breach as a result of a lost or stolen mobile device, which included laptops, desktops, smartphones, tablets, servers and USB drives containing confidential or sensitive information.
7. Consultants were engaged to help remediate the data breach response and remediation.[14]

14 *Ponemon Institute (2013). Cost of Data Breach Study: Global Analysis p9.*

Survey
4.8 | *Principles, Policies and Standards*

Introduction

The purpose of principles, policies and standards is to clearly and unambiguously express the goals and objectives for security management and security solutions. Information security governance sets the framework and boundaries for security management and related solutions. However, it needs to take into account that a large part of cybersecurity is concerned with handling unexpected events and incidents.

Although many organizations already have extensive policies in place, they may not adequately cover cybersecurity. Against a background of a fast growing and rapidly evolving threat landscape, traditional, standards-based methods for protecting the organization must be augmented and existing policies and standards enhanced.

Principles:
Cybersecurity principles represent a more flexible response to cybercrime, including unpredictable or innovative attacks. A large part of cybersecurity relies on human intelligence to recognize and respond to attacks and incidents.

Policies:
Cybersecurity is a specialized part of general information security and it will inevitably touch on a wide number of other, already existing, policies. Cybersecurity policies should therefore appropriately reference all other relevant policies and standards existing throughout the enterprise. Subsidiary documents, such as a cybersecurity standard, should also contain an appropriate set of cross-references to other pertinent documents.

Standards:
While the cybersecurity policy incorporates information security principles and high-level objectives, the cybersecurity management standards should provide a more detailed overview of management practices, solutions and protective measures to be followed.[15]

Participants in this survey were asked if they thought principles, policies and standards were important to communicate directives in support of cybersecurity governance. Next, they were asked if the organization they represented had principles and policies that supported cybersecurity governance. Nine topics were specified that might be part of a cybersecurity policy document:

- Relationships with business partners, customers and other third parties;
- Compliance with legal and regulatory requirements;
- Adopting a risk-based approach;
- Evaluating current and future threats through cybercrime;
- Creating a realistic outlook on the future of cybersecurity;
- Obtaining external expertise as appropriate;
- Establishing data classification with regard to cybercrime;
- Secure acquisition, system development and maintenance;
- Fostering awareness and rules of behavior about cybersecurity and cybercrime.

15 *ISACA (2013). Transforming cybersecurity: using COBIT 5 p77-90.*

Principles, Policies & Standards to Support Cybersecurity

Do you think principles, policies and standards are important to communicate directives in support of cybersecurity governance?

Perceived versus actual scores

Figure 34 correlates the security expert opinion with the actual status for this topic. From the results it can be concluded that relative to other participants, finance organizations perceive policies and standards for cybersecurity to be most important..

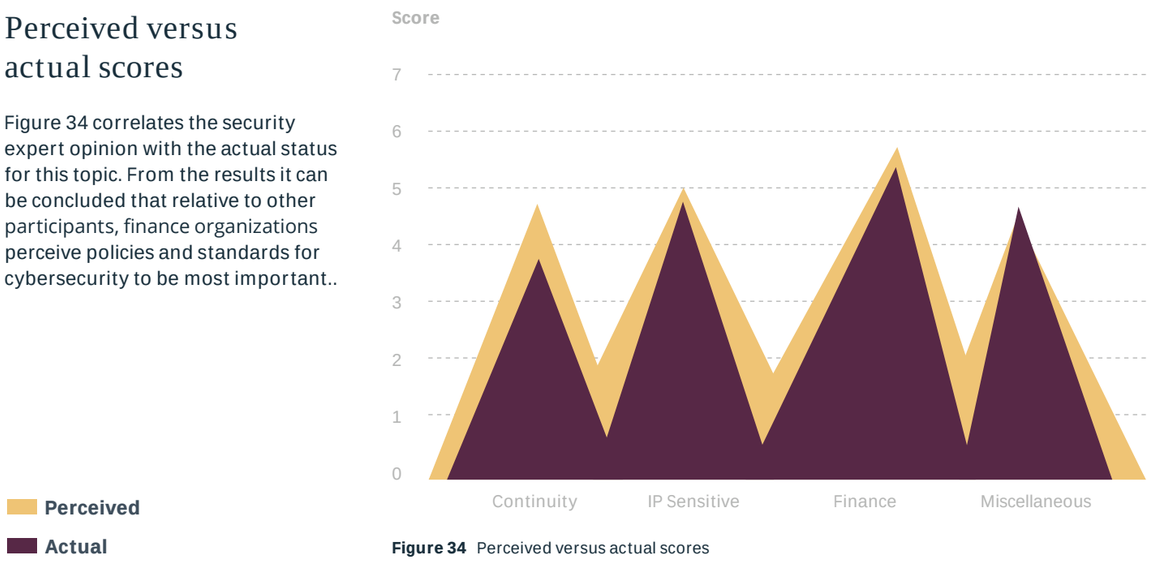


Figure 34 Perceived versus actual scores

Relative deviations

Figure 35 shows that finance organizations do not report many deviations between perceived and actual scores, thus indicating that, when it comes to cybersecurity policies and standards, these organizations meet expectations, according to the expert's opinion. Continuity-sensitive organizations do report some deviations between perceived and actual scores.

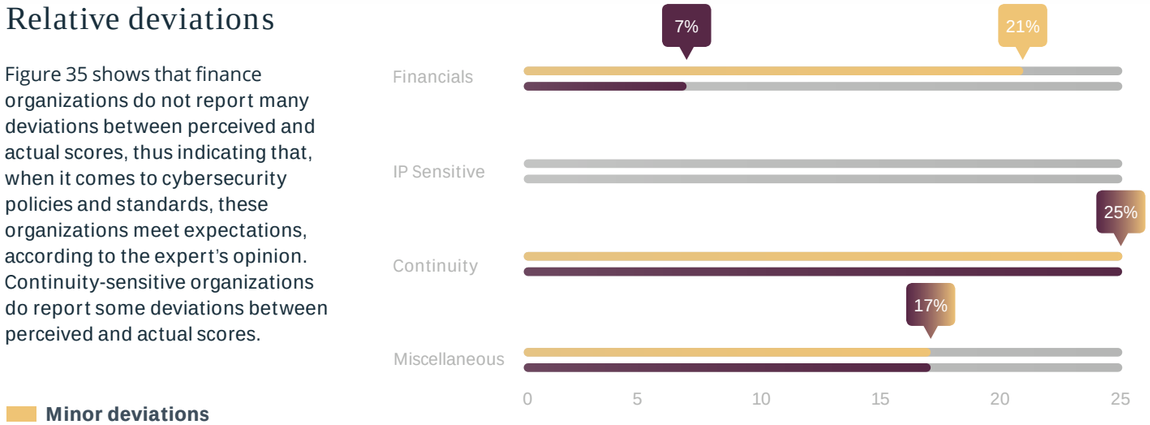


Figure 35 Relative deviations perceived versus actuals

> Cybersecurity is a specialized part of general information security and it will inevitably touch on a wide number of other, already existing, policies.

Actual scores per cluster

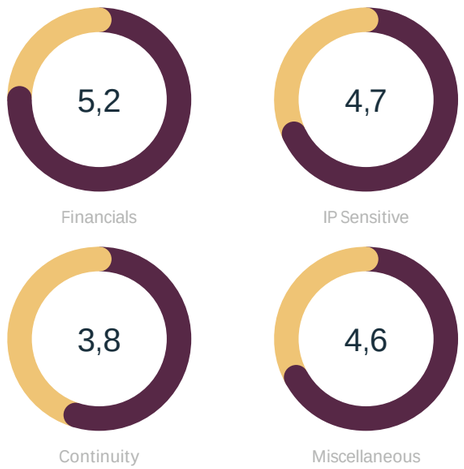


Figure 36 Actual scores per cluster on a scale 1-7

Figure 36 compares the actual scores for this topic. Participants in the finance sector report the highest actual scores, relative to other clusters.

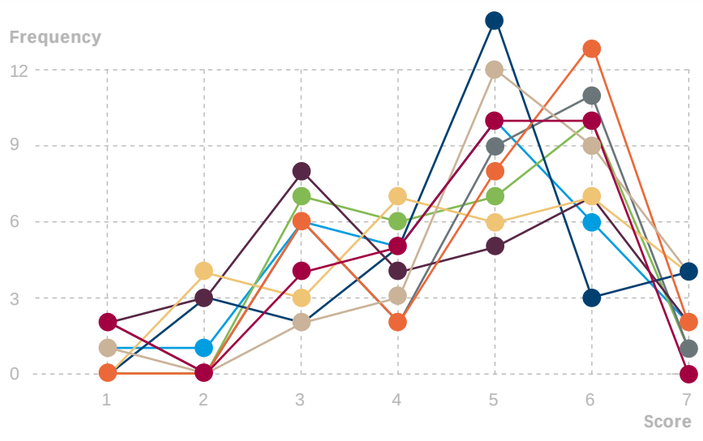
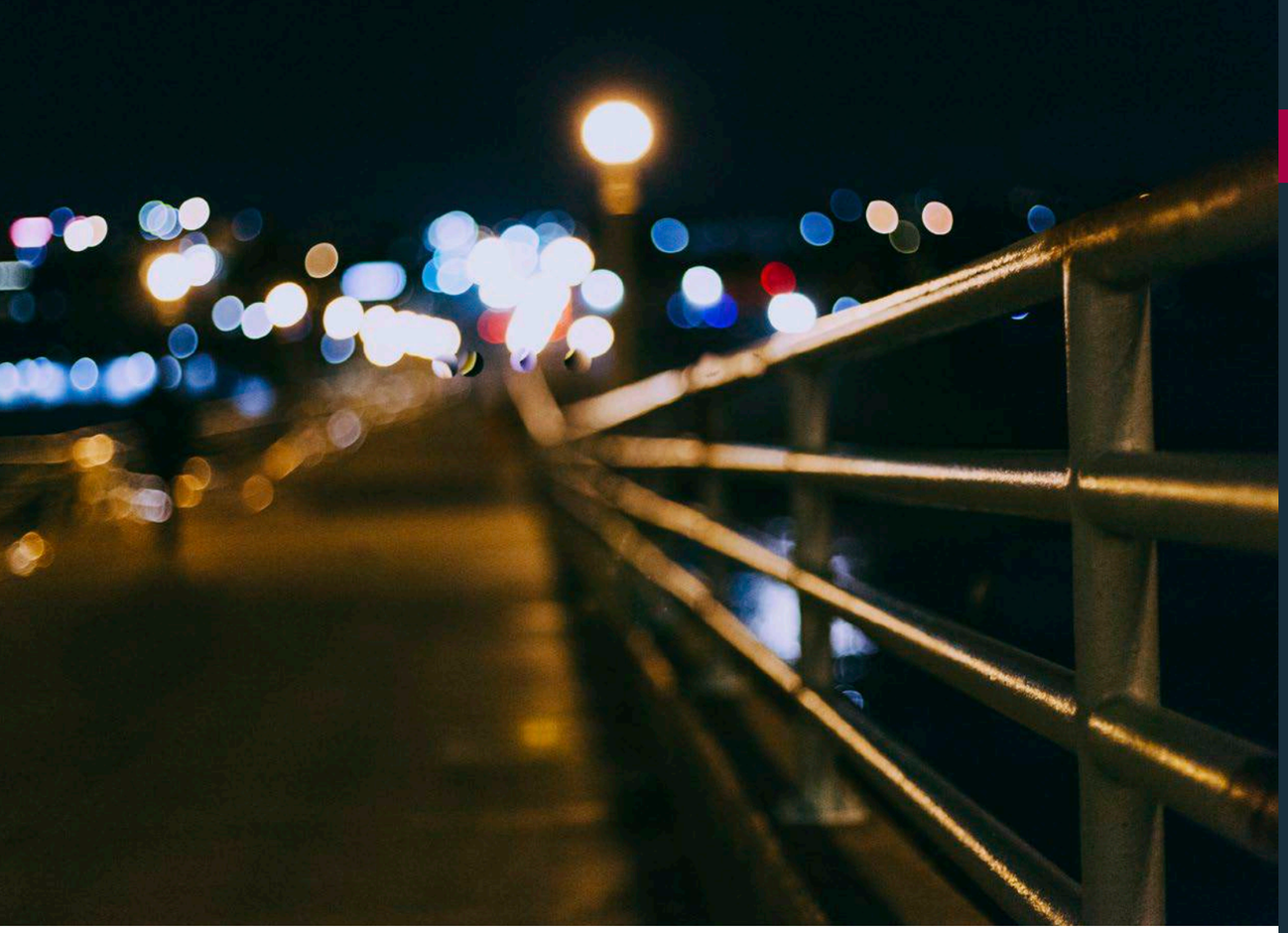


Figure 37 Actual scores per option

Actual scores per option

Figure 37 shows the distribution in scores for each option in this this topic. In this survey, of all reference items, creating a realistic outlook on the future of cybersecurity seems to be the most difficult part in cybersecurity policies and standards.

- Relationships with business partners, customers and other third parties
- Compliance with legal and regulatory requirements
- Adopting a risk-based approach
- Evaluating current and future threats through cybercrime
- Creating a realistic outlook on the future of Cybersecurity
- Obtaining external expertise as appropriate
- Blishing data classification with regard to cybercrime
- Secure acquisition, system development and maintenance
- Fostering awareness and rules of behaviour about Cybersecurity and cybercrime



Security principles

COBIT 5 for Information Security provides a generic catalog of security principles that can be translated for the purposes of cybersecurity:

- Focus on the business > to ensure that information security is integrated into essential business processes.
- Deliver quality and value to stakeholders > to ensure that information security delivers value and meets business requirements.
- Comply with relevant legal and regulatory requirements > to ensure that statutory obligations are met, stakeholder expectations are managed, and civil or criminal penalties are avoided.
- Provide timely and accurate information on information security performance > to support business requirements and manage information risk.
- Evaluate current and future information threats > to analyze and assess emerging information security threats so that informed, timely action to mitigate risk can be taken.
- Promote continuous improvement in information security > to reduce costs, improve efficiency and effectiveness, and promote a culture of continuous improvement in information security.
- Adopt a risk-based approach > to ensure that risk is treated in a consistent and effective manner.
- Protect classified information > to prevent disclosure of classified (e.g., confidential or sensitive) information to unauthorized individuals.
- Concentrate on critical business applications > to prioritize scarce information security resources by protecting the business applications on which an information security incident would have the greatest business impact.
- Develop systems securely > to ensure hat information security-related activities are performed in a reliable, responsible and effective manner.
- Foster an information security-positive culture > to provide a positive information security influence on the behavior of end users, reduce the likelihood of information security incidents occurring, and limit their potential business impact.[16]

16 *ISACA (2012). COBIT 5 for Information Security p61-63.*

Survey
4.9 | *Organizational Structures*

Introduction

The size of the organization, type of industry, its culture and values are key factors in determining the governance structure for cybersecurity. As a discipline, cybersecurity is subject to the management hierarchy and chain of command in information security. However, given the pervasive nature of cyber crime that often contains a significant amount of nontechnical activity (social, human factors, etc.), traditional organizational structures may be insufficient to sustain an effective sociotechnical security management system.

In larger corporate environments, organizational design frequently favors a fairly rigid segregation of duties and creates silos for corporate security, information security and other functions. Without proper communication between the entities, cybersecurity management will be fragmented, leaving gaps that may be successfully exploited.
A secondary risk results from the unevenly distributed IT knowledge and skills needed to prevent, recognize and manage security breaches or incidents. Where only a few people are in a position to fully understand and deal with cybersecurity, it is often difficult to disseminate this knowledge and achieve the desired level of protection and security.[17]

Each organization is different and assigns roles and responsibilities based on several factors including strategy, corporate culture, capabilities and even personalities of their executives. In larger organizational environments, to accommodate cybersecurity, a separate role may be appropriate as well as full end-to-end business and ICT responsibilities. In some organizations the Chief Information Officer (CIO) manages the cybersecurity program while others delegate responsibilities to the Chief Information Security Officer (CISO).

Leadership and ownership at the highest level is vital for companies to recognize that cybersecurity is a board-level issue. Some argue that a Chief Financial Officer (CFO) is best placed to protect a company from future breaches. As the organization seeks growth, through new markets, acquisitions or other means, preventing cyber attacks is one strategy to ensure that the organization's reputation stays intact. CFOs then have a critical role to play to ensure that the board treats cybersecurity as a business issue instead of it being treated as a technological issue.
With the board owning the cybersecurity program and every associate responsible for their part of it, the organization stills needs someone to manage it. The CIO is in all respects the best positioned to manage the cybersecurity program.

Through the creation of plans, policies and procedures, architecture development and the selection of tools, the CIO is at the heart of nearly all business activities. Supported by a competent CISO, and a board that demonstrates commitment to cybersecurity, the CIO has every opportunity to lead an effective cybersecurity team.
Without direct oversight and monitoring of change across processes, systems, devices, applications and third-party engagements, organizations cannot holistically protect themselves against cyber risk. Best practice is to convene a Change Management Board, chaired by the CIO to control and manage the risk introduced by change.

Finally, in many organizations, a Chief Risk Officer and/or Risk Committee are part of the governance structure.

17 *ISACA (2013). Transforming cybersecurity: using COBIT 5 p36.*

Integrate Cybersecurity in Organizational Structures

Do you think it is important to explicitly link cybersecurity activities to established organizational structures?

Perceived versus actual scores

Figure 38 correlates the security expert opinion with the actual status for this topic. From the results it can be concluded that relative to other participants, finance organizations perceive organizational structures to be most important for cybersecurity.

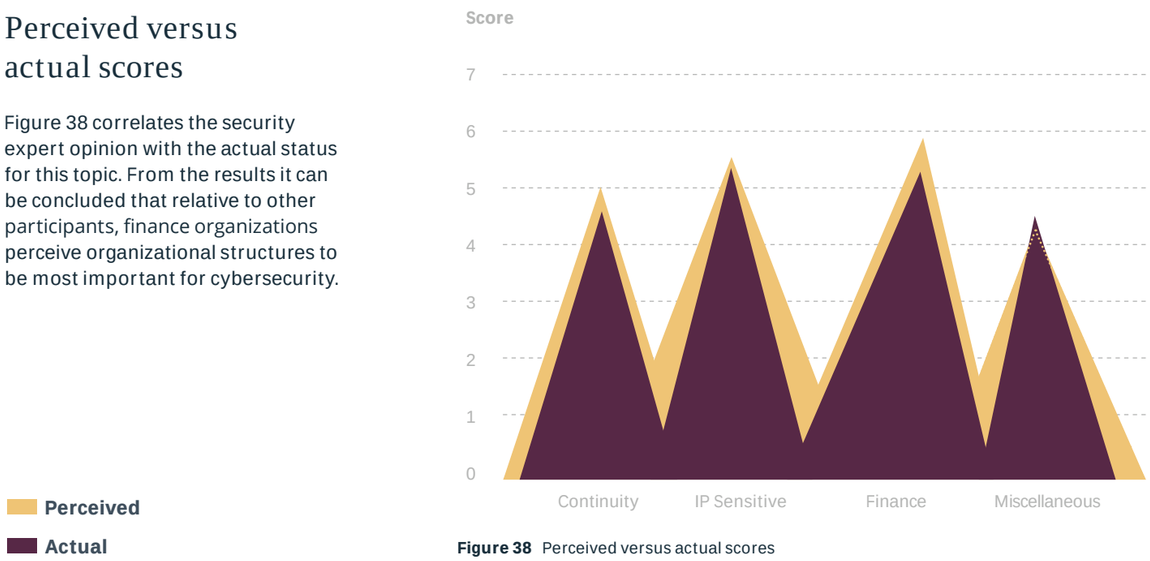


Figure 38 Perceived versus actual scores

Relative deviations

Figure 39 shows that, overall, participating organizations do not report too many deviations between perceived and actual scores, thus indicating that, when it comes to organizational structures, these organizations meet the expert's expectations.

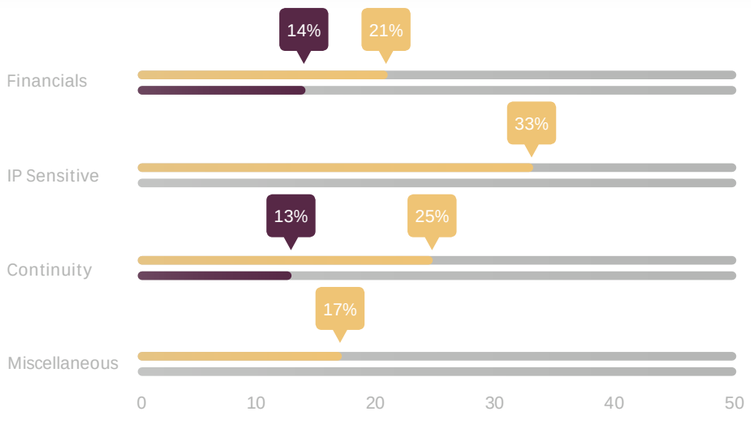


Figure 39 Relative deviations perceived versus actuals

> Without proper communication between the entities, cybersecurity management will be fragmented, leaving gaps that may be successfully exploited.

Actual scores per cluster

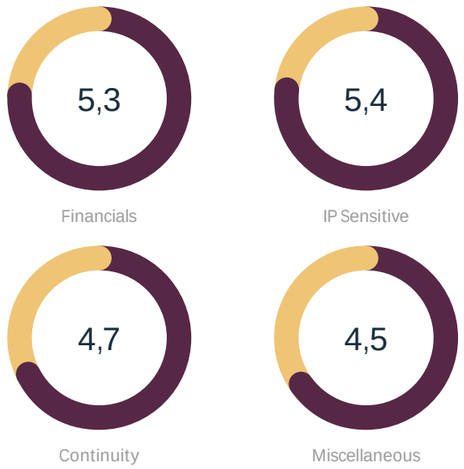


Figure 40 Actual scores per cluster on a scale 1-7

Figure 40 compares the actual scores for this topic. Participants in the IP-sensitive cluster report the highest actual scores, relative to other clusters.

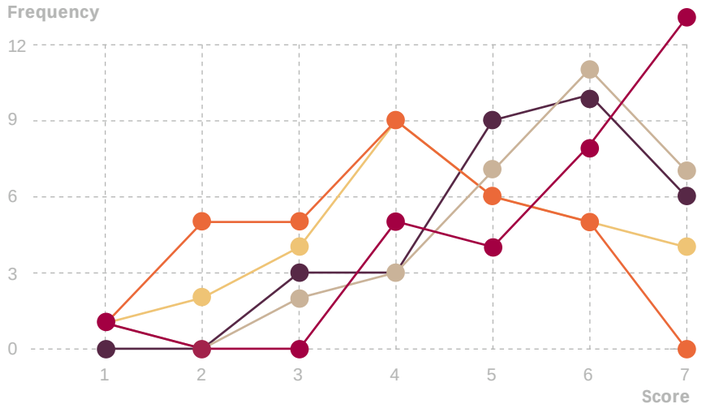


Figure 41 Actual scores per option

Actual scores per option

Figure 41 shows the distribution in scores for each option in this this topic. In this survey, of all reference items, using RACI matrices to specify the level of involvement in cybersecurity seems to be the most difficult part to address in organizational structures.

- **CISO or someone in this position to be charged with cybersecurity**
- **Interfaces between the cyber-security function and other roles**
- **RACI matrices**
- **Appropriate decision making model and authority levels for cybersecurity**
- **Hierarchical escalation paths**

Information security roles and structures

According to COBIT 5, the board of directors carries final accountability for all information security matters. However, considering information security to be a critical business issue, accountability can and should be delegated to a senior manager of the executive management. In addition, the framework describes five typical information security roles and structures that are commonly found in large organizations:

- Chief Information Security Officer (CISO) – overall responsible for the information security program;
- Information Security Steering Committee (ISSC) – responsible that good practices are effectively and consistently applied throughout the organization;
- Information Security Manager (ISM) – overall responsible for the management of information security efforts;
- Enterprise Risk Management (ERM) - responsible for the decision-making to assess, control, optimize, finance and monitor risk;
- Information Custodians/ Business Owners – liaison between the business and information security functions.

Suggested composition of the Information Security Steering Committee: CISO, ISM, information custodians/business owners, IT manager, representatives of specialist functions.

Suggested composition of the Enterprise Risk Management: CISO, C-level officer, process/business owners, audit/compliance, legal representative, CRO.[18]

18 ISACA (2013). COBIT 5 for Information Security p38.

Survey
4.10 | *Culture, Ethics and Behavior*

Introduction

Cybersecurity success, to a large extent, depends on a culture that promotes vigilance and adaptive thinking. The target state requires sense-of-urgency as well as factual and behavioral buy-in from all levels, and in most cases from external business partners as well.

Cultural scans may provide a good starting point in assessing as-is cyber-security culture and may, in some cases, reveal serious misalignments between stakeholders. It is not uncommon for C-level officers to have different views on security issues and priorities, compared to security professionals and employees in the field.

Cybersecurity significantly relies on personal vigilance and the willingness and ability to recognize unusual activity, potential threats and existing vulnerabilities. Security rules are often perceived as inconvenient and cumbersome, making individuals reluctant to accept what they regard as unnecessary constraints to their daily work. Human behavior all together has a profound impact on an organization's cybersecurity posture.

> "Cybersecurity significantly relies on personal vigilance and the willingness and ability to recognize unusual activity, potential threats and existing vulnerabilities."

Human risks include:

- Social media: cyber criminals may use social media to analyze organizations by making hierarchical associations and using the features of the social media tool. Subsequently, this information may be used in their spear-phishing efforts.
- Inadvertent disclosure: employees may inadvertently disclose information without even realizing it.
- Ignorance: can be linked to an uneven distribution of knowledge but also to convenience as a human preference, with resulting vulnerabilities and threats.
- Negligence: a person has acted negligently if he or she departed from the conduct of a reasonable prudent person acting under similar circumstances. Increasingly, lawsuits are emerging against organizations that fail to protect personal identifiable information (PII).
- Lack of leadership: from a cyber-security perspective, organizations and people are most vulnerable where the prevailing leadership style leads to dysfunctional behavior and a corresponding increase in the risk of attacks or breaches.
- Lack of accountability: as cybersecurity has evolved to be a critical business imperative, people must be held accountable for managing and controlling their piece of the cyber risk.

Participants in this survey were asked if they thought culture, ethics and behavior were important for the success of cybersecurity. Next, they were asked if, in the organization they represented, security culture was right for today's threat environment. To support this question, five indicators were given as a reference:

- To be able to view the organization as a high-risk or high-value target;
- To understand that prevention against cyber threats is almost impossible, that the network is already compromised or soon will be;
- To understand that associates are crucial for the success or failure of cybersecurity;
- To understand that the organization must be able to protect its most sensitive information in a compromised environment;
- To be externally aware of what is going on in the cybersecurity space.

Cybersecurity Culture, Ethics and Behavior

Do you think culture, ethics and behavior, including tone at the top, are important for the success of cybersecurity?

Perceived versus actual scores

Figure 42 correlates the security expert opinion with the actual status for this topic. From the results it can be concluded that relative to other participants, finance and continuity sensisitive organizations, perceive culture, ethics and behavior to be most important for the success of cybersecurity.

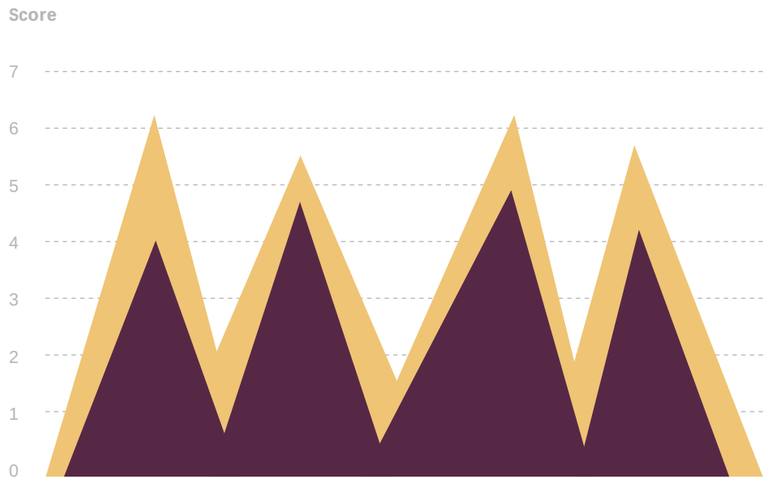


Figure 42 Perceived versus actual scores

Relative deviations

Figure 43 shows that, overall, participating organizations report many deviations between perceived and actual scores, thus indicating that, when it comes to cybersecurity culture, expert's expectations are not met. Continuity-sensitive organizations report the most significant deviations.

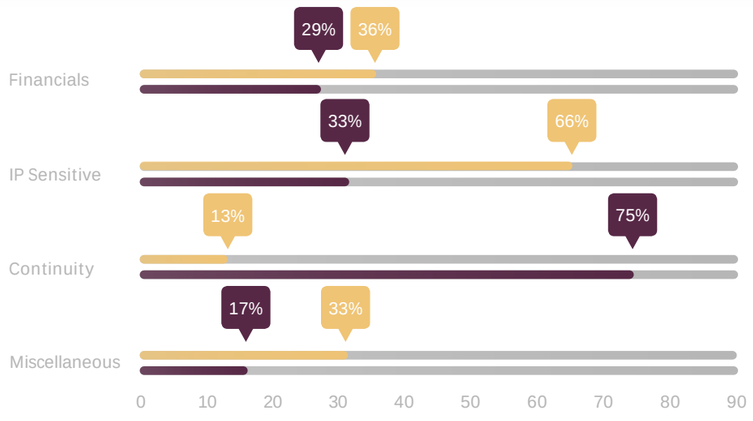


Figure 43 Relative deviations perceived versus actuals

> Cybersecurity significantly relies on personal vigilance and the willingness and ability to recognize unusual activity, potential threats and existing vulnerabilities.

Actual scores per cluster

Figure 44 Actual scores per cluster on a scale 1-7

Figure 44 compares the actual scores for this topic. Participants in the finance cluster report the highest actual scores, relative to other clusters.

Actual scores per option

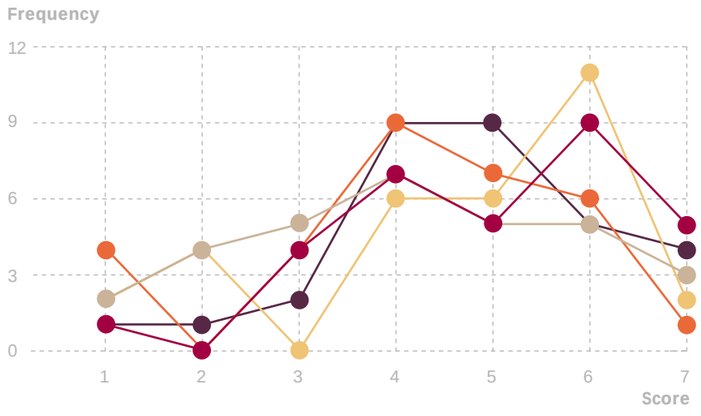


Figure 45 Actual scores per option

Figure 45 shows the distribution in scores for each option in this this topic. In this survey, Of all reference items, understanding that prevention against cyber threats is almost impossible and that the network is already compromised or soon will be, seems to be the most difficult part to grasp in cybersecurity.

- To view itself as a high-risk or high-value target
- To understand that prevention against cyber threats is almost impossible, that the network is already compromised or soon will be
- To understand that associates are crucial for the success or failure of Cybersecurity
- To understand that the organization must be able to protect its most sensitive information in a compromised environment
- To be externally aware of what is going on in the Cybersecurity space

Culture, Ethics and Behavior enabler COBIT 5

The Culture, Ethics and Behavior enabler in COBIT 5 defines a set of model behaviors and cultural values that may be applied to cybersecurity management. Figure 46 gives a high-level overview of the model behaviors defined in the COBIT 5 framework and how they should be applied to cybersecurity management. Every organization will have to align and interpret them in order to match the overall culture of business and security.[19]

COBIT 5 Model Behavior	Application to Cybersecurity
Information security is practiced in daily operations.	- Cybersecurity principles and practices are applied to daily operations. - All associates understand and apply cybersecurity measures completely and in a timely manner.
People respect the importance of information security policies and principles.	- All users understand the defined priorities in cybersecurity and how to apply them in their personal and business IT environment. - All users are aware of, and ideally actively involved in, defining cybersecurity principles and policies. - Cybersecurity principles, policies, standards are updated frequently to reflect day-to-day reality as experienced by the enterprise.
People are provided with sufficient and detailed information security guidance and are encouraged to participate in and challenge the current information security situation.	- Cybersecurity is a transformation process with regular challenges from all parts of the enterprise. - Cybersecurity guidance is simple, to the point and relates to typical day-to-day risk. - The situation with regard to cybersecurity is continuously and jointly assessed by users and security managers.
Everyone is accountable for the protection of information within the enterprise.	- Security managers and users share accountability for cybersecurity. This includes business use, travelling use and home use. - Users have a clear understanding of their accountability and act responsibly. - The enterprise operates a fault/error-tolerant environment and avoids scapegoating.
Stakeholders are aware of how to identify and respond to threats to the enterprise.	- All users are stakeholders in cybersecurity, regardless of their hierarchical level within the enterprise. - User are sufficiently aware of the risk, threats and vulne abilities associated with attacks/breaches. - Response to threats and incidents is well understood, exercised frequently and auditable.
Management proactively supports and anticipates new information security innovations and communicates this to the enterprise. The enterprise is receptive to account for and deal with new information security challenges.	- Security management and end users cooperatively identify, test and adopt innovation in cybersecurity. - Management and end users identify and adopt new business cases for technology, security practices and other types of added value in cybersecurity. - The enterprise explicitly aims at staying in front of the curve in cybersecurity.
Business management engages in continuous cross-functional collaboration to allow for efficient and effective information security programs.	- Cybersecurity programs are in place and form part of the overall innovation strategy. Security innovations are incorporated as key projects. - Business functions cooperate with information security to maximize efficiency and effectiveness of cybersecurity.
Executive management recognizes the business value of information security.	- Executive managers act as end users and recognize the value of cybersecurity. They actively participate in training and awareness activities.

Figure 46 COBIT 5 Model Behaviors in Cybersecurity

19 *ISACA (2013). Transforming cybersecurity: using COBIT 5 p97-98.*

Survey
4.11 | *Skills & Competences*

Introduction

Cybersecurity skills and competences should reflect a good balance of technical and soft skills such as communication, influencing and stakeholder management. Security skills and competences can be acquired through a combination of training and education, on-the-job learning, mentor programs, participation in industry groups, professional networking and continuous study.

Cybersecurity specific skills and competences are not intended to be exclusively for the position of security managers and specialists. Unfortunately, end users are part of many sophisticated attack vectors. Therefore, as a baseline, basic security practices should be part of every user's skill profile, in order to protect them from making avoidable errors.

The strong element of unpredictability that is intrinsic to cybercrime mandates a more comprehensive approach and requires the development or recruitment of specialist skills, sourced either from within the organization or through an external support service. Organizations responding to APT intrusions can gain valuable support and advice from other CERT or CSIRT teams, as well as from security vendors.

According to SANS Critical Security Controls (CSC), the key to upgrading skills is measurement through assessments that show where knowledge is sufficient and where gaps are evident. Once the gaps have been identified, those employees who have the requisite skills and knowledge can be called upon to mentor employees who need to improve their skills. In addition, the organization can develop training plans to fill the gaps and maintain employee readiness. Subsequently, a key way to prioritize training is to focus first on those jobs and roles that are critical to the mission or business outcome of the enterprise.

One way to identify these mission-critical jobs is to reference the list prepared by the Council on CyberSecurity:

- System and Network Penetration Testers;
- Application Penetration Testers;
- Security Monitoring and Event Analysts;
- Incident Responders In-Depth;
- Counter-Intelligence/ Insider Threat Analysts;
- Risk Assessment Engineers;
- Secure Coders and Code Reviewers;
- Security Engineers/Architecture and Design;
- Security Engineers/Operations;
- Advanced Forensics Analysts.

Participants in this survey were asked if they thought people skills and competences were important for the success of cybersecurity. Next, they were asked if skills and competences were readily available in the organization they represented. A number of skills and competences were referenced:

- Ability to formulate cybersecurity strategy components and strategic requirements;
- In-depth understanding of compliance with laws, regulations, directives and standards;
- Ability to establish and maintain a cybersecurity governance framework including supporting processes;
- Strong skills in risk assessment and analysis as well as risk treatment options;
- Extensive technical architecture skills, above-average experience in critical technologies;
- Profound skills and experience in operating security-related IT and processes, covering the organization end-to-end;
- Ability to perform assessments and extensive testing.

Cybersecurity Skills & Competences

Do you think people skills and competences are important for the success of cybersecurity?

Perceived versus actual scores

Figure 47 correlates the security expert opinion with the actual status for this topic. From the results it can be concluded that relative to other participants, continuity-sensitive organizations perceive skills and competences to be most important for the success of cybersecurity.

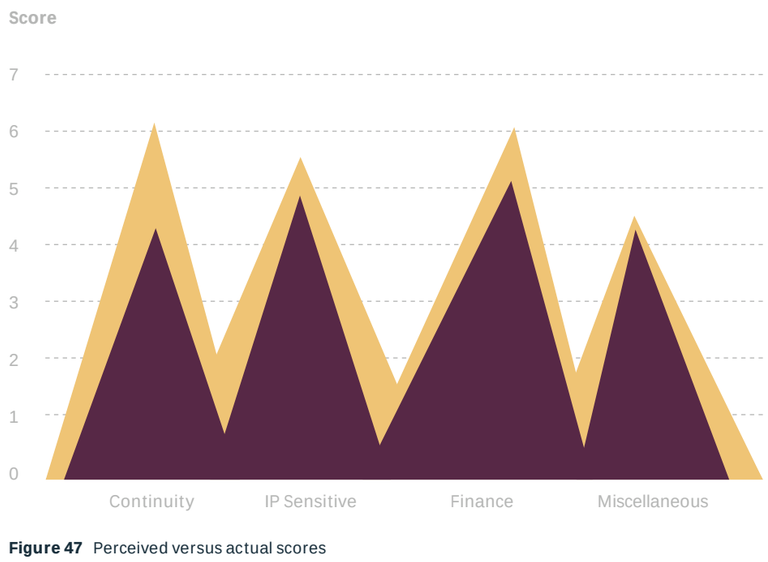


Figure 47 Perceived versus actual scores

> The strong element of unpredictability requires the development or recruitment of specialist skills.

Actual scores per cluster

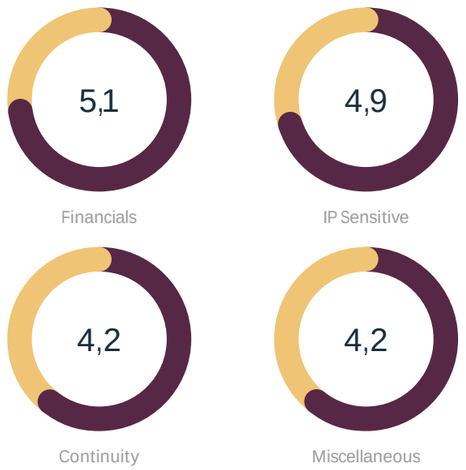


Figure 49 Actual scores per cluster on a scale 1-7

Figure 49 compares the actual scores for this topic. Participants in the finance cluster report the highest actual scores, relative to other clusters.

Relative deviations

Figure 48 shows that, according to the respondents' expectations, continuity-sensitive organizations fail to give adequate attention to this topic. Half of all participants in the continuity cluster report significant deviations.

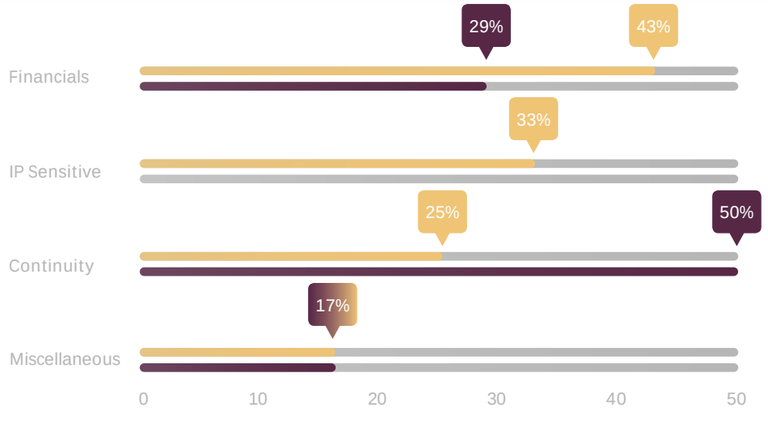


Figure 48 Relative deviations perceived versus actuals

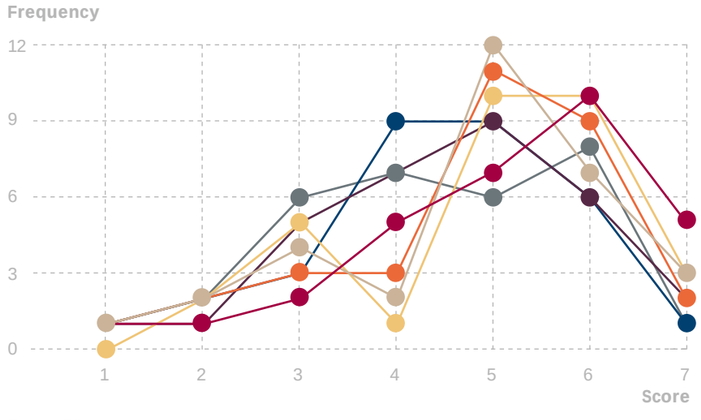


Figure 50 Actual scores per option

Actual scores per option

Figure 50 shows the distribution in scores for each option in this this topic. In this survey, of all cybersecurity skills and competences, the ability to perform assessments and extensive testing seems to be the most difficult to address.

- Allowing for the ability to formulate Cybersecurity strategy components and strategic requirements
- Allowing for in-depth understanding of compliance with laws, regulations, directives and standards
- Allowing for the ability to establish and maintain a Cybersecurity governance framework including supporting processes
- Allowing for strong skills in risk assessment and analysis as well as risk treatment options
- Allowing for extensive technical architecture skills, above-average experience in critical technologies
- Allowing for profound skills and experience in operating security-related IT and processes, covering the organization end-to-end
- Allowing for ability to perform support assessments and extensive testing

Job profiles for Information Security

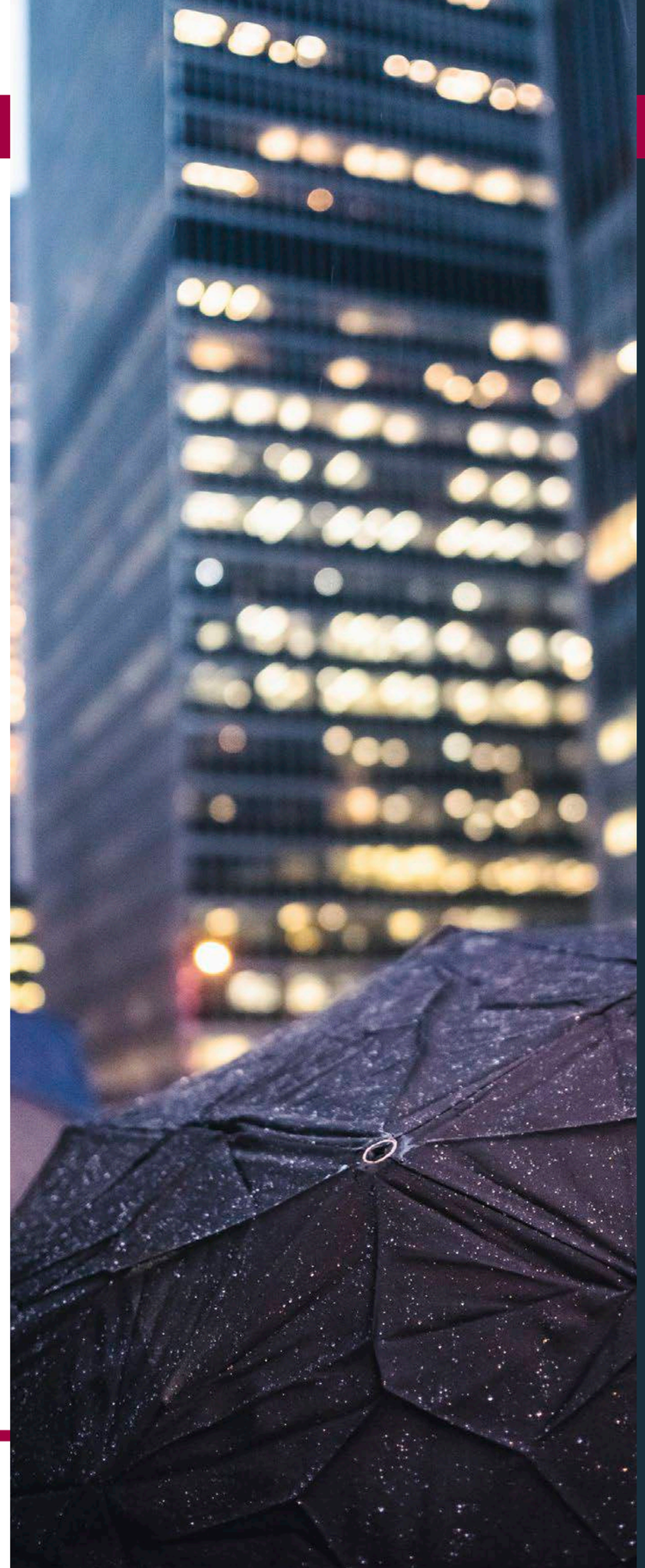
With the emergence of a large number of certificates and job titles that are difficult to compare with each other, it is increasingly difficult for employers to be able to tell if candidates are well-trained and experienced information security professionals. In a recent study the Dutch association for information security professionals (PvIB) made an excellent effort in developing a national qualification scheme, using international standards and framework such as the European E-competence Framework (e-CF).

For a number of professions in information security, competences have been described in so-called job profiles. In the study, four jobs have been identified for which job profiles were described:

- Chief Information Security Officer (CISO)
- Information Security Officer (ISO)
- ICT Security Manager
- ICT Security Specialist

Amongst other elements, each job profile includes: mission, deliverables, main tasks, and competences.[20]

20 *PvIB (2014) Job profiles in Information Security - A Basis for Uniform Qualification of Professionals in Information Security*



Survey
4.12 | *Training & Awareness*

Introduction

A security awareness and education program that keeps pace with ever-evolving cybersecurity demands promotes a culture of vigilance. However, it will not stop determined attackers. Trained and vigilant employees are essential for detecting those attackers that get through the defenses, and for developing systems that are much harder to exploit.

Training is closely tied to policies and awareness. Policies tell people what to do, training provides them the skills to do it, and awareness changes behavior so that people follow policies. An organization should understand the skill gaps within its workforce (and external partners) and plan to fill the gaps through training and awareness.

Most organizations now invest in a basic security training and awareness program. In some cases however, the investment correlates to the more or less immediate experience of a past attack or incident. Subsequently, both awareness and diligence in “living” cybersecurity diminish sharply, until the next attack occurs. In other cases the program is insufficient to mitigate the risk of well-researched social engineering attacks. The scope, intensity and sophistication of the educational program must be aimed at different audiences, focusing in on the managers and staff who are most likely to be targets for such approaches. All employees should receive cybersecurity training so that they have a solid understanding of the threats, vulnerabilities and risks confronting the organization and themselves. If not properly trained they often devise methods and procedures of their own. In addition, if they do not practice cybersecurity methods at home, they are more likely to expose themselves and the organization to risks.

Training and awareness should cover all hierarchical levels, including senior management. The top of the pyramid is where most of the sensitive data is handled on a daily basis. Senior and executive managers that participate in awareness, training and innovation activities will not only strengthen their own base for preventing attacks and breaches, but at the same time the right signals to the organization as a whole will be given.

Training for security professionals will be more frequent and intensive, with regular updates on trends, emerging technologies and risk, covering investigative and forensic treatment of attacks/breaches and new security management practices and techniques. Education will include relevant conferences and workshops and/or industry association participation.

Whaling is a specific kind of malicious hacking within the more general category of phishing, which involves hunting for data that can be used by the hacker. In general, phishing efforts are focused on collecting personal data about users. In whaling, typical targets are high-ranking bankers, executives or others in powerful positions or job titles.

In advanced environments, serious gaming might prove an effective approach to cybersecurity training. These exercises bring IT personnel from different specialties (network, security, virtualization, software, etc.) into color-coded red, white, and blue teams that perform specific roles in attacking and defending IT infrastructures.

Many other user groups need dedicated cybersecurity training including IT operations, security analysts, system developers and programmers. Finally, awareness requires the vigilance of external partners as well. If each organization in a process is considered a link in a chain, then each link needs to be equally strong.

Cybersecurity Training and Awareness

Do you think cybersecurity training- and awareness programs are important to ensure the resilience of an organization?

Perceived versus actual scores

Figure 51 correlates the security expert opinion with the actual status for this topic. From the results it can be concluded that relative to other participants, IP-sensitive organizations perceive training and awareness to be most important to ensure the resilience of an organization.

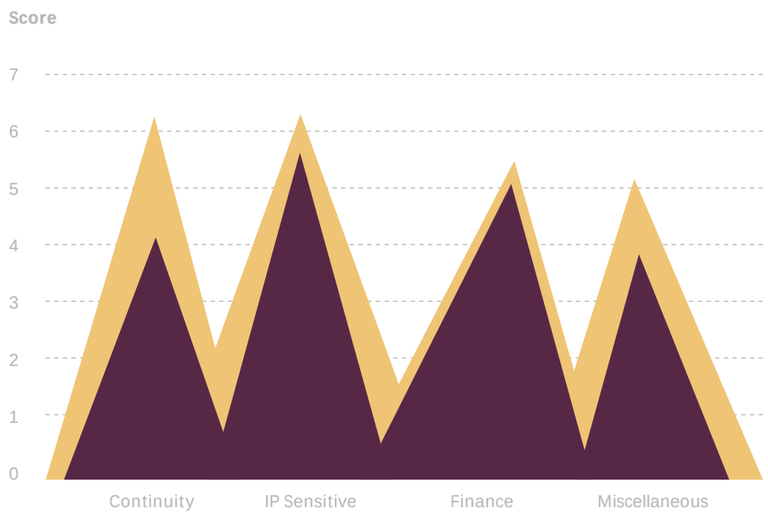


Figure 51 Perceived versus actual scores

> Trained and vigilant employees are essential for detecting those attackers that get through the defences.

Relative deviations

Figure 52 shows that, according to the respondents' expectations, IP-sensitive organizations are most successful in giving adequate attention to this topic, as opposed to continuity-sensitive organizations. They also perceive training and awareness to be important for cybersecurity, although 63% of all participants in the continuity cluster report significant deviations.

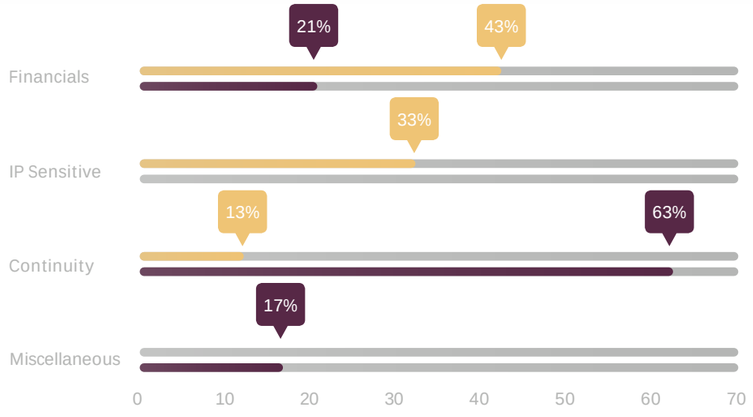


Figure 52 Relative deviations perceived versus actuals

Actual scores per cluster

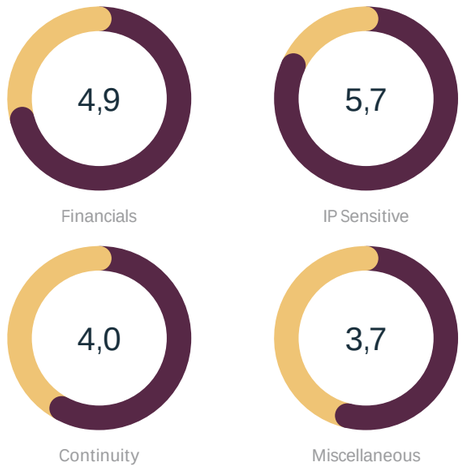


Figure 53 Actual scores per cluster on a scale 1-7

Figure 53 compares the actual scores for this topic. Participants in the IP-sensitive cluster report the highest actual scores, relative to other clusters.

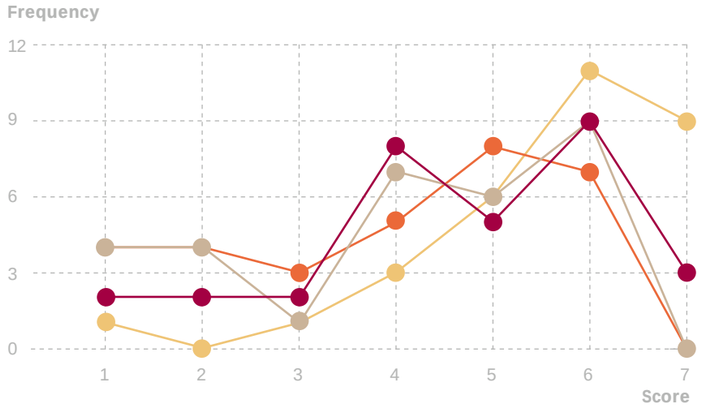


Figure 54 Actual scores per option

Actual scores per option

Figure 54 shows the distribution in scores for each option in this this topic. In this survey, participants indicate that, of all user groups, security managers receive the most in terms of training facilities.

- **End-users receive basic training covering elementary Cybersecurity**
- **Senior managers receive basic training covering elementary Cybersecurity**
- **Business representatives receive training covering business related IT use**
- **Security managers receive training covering advanced skills**

Training and awareness in frameworks

Many frameworks encourage cybersecurity 'best practices' through extensive training, education, and communication, including the SANS CSC, COBIT 5, ISO/IEC 27001:2013 and NIST SP 800-53 Rev. 4.
We include here as an example the SANS Control 9.

SANS Control 9:
Provide clear guidance on training and awareness
For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.
CSC 9-1 Perform gap analysis to see which skills employees need and which behaviors employees are not adhering to, using this information to build a baseline training and awareness roadmap for all employees.
CSC 9-2 Deliver training to fill the skills gap. If possible, use more senior staff to deliver the training. A second option is to have outside teachers provide training onsite so the examples used will be directly relevant. If you have small numbers of people to train, use training conferences or online training to fill the gaps.
CSC 9-3 Implement an online security awareness program that: (1) focuses only on the methods commonly used in intrusions that can be blocked through individual action; (2) is delivered in short online modules convenient for employees; (3) is updated frequently (at least annually) to represent the latest attack techniques; (4) is mandated for completion by all employees at least annually, and; (5) is reliably monitored for employee completion.
CSC 9-4 Validate and improve awareness levels through periodic tests to see whether employees will click on a link from suspicious emails or provide sensitive information on the telephone without following appropriate procedures for authenticating a caller; targeted training should be provided to those who fall victim to the exercise.
CSC 9-5 Use security skills assessments for each of the mission-critical roles to identify skills gaps. Use hands-on, real-world examples to measure mastery. If you do not have such assessments, use one of the available online competitions that simulate real-world scenarios for each of the identified jobs in order to measure skills mastery.

Survey
4.13 | *Relationships External to the Organization*

Introduction

Organizations must actively incorporate customers and business partners to anticipate in the event the organization must operate in a degraded capacity. In addition, external relationships with third parties can be established to strengthen cybersecurity capabilities and/or to help in an adequate response once a breach has occurred.

The challenge for cybersecurity spans the interconnected global business ecosystem. Increasingly, organizations depend on direct interconnections with outside business partners. These connections may include university research partnerships, relationships between competing/cooperating companies, joint ventures and industry associations. On a more contractual basis, organizations relate to external suppliers of services, HR, legal or IT and cloud providers. In addition, they have to rely on partners that play a critical role in the supply stream or upstream infrastructure. Risk-aware organizations anticipate major disruptions to infrastructure, especially in electricity, financial systems, telecommunications and Internet infrastructure, like Internet exchange points and submarine cables.

At the same time, although many public and private organizations have capabilities that are critical in the area of cyber, no single organization - public or private -has sufficient expertise, talent, resources, capabilities, authorities or capacity to act or be successful in isolation.

Security intelligence is one area in which organizations rely on external relations. Cyber threat intelligence (CTI) can be obtained internally, from a community and from external sources. In a community, information is shared via trusted relationships with multiple members with a shared interest. This can be an informal group with member organizations that are in the same industry sector or that have other common interests. There are formal community groups such as the Information Sharing and Analysis Centers (ISACs). The external category includes CTI obtained from sources outside an organization and that are not part of a community group. There are two types of external sources, public and private ones. Public sources are available to anyone and generally there is no cost associated with access. The other type of external CTI source is private. Private sources are typically only available on a paid basis. An organization can subscribe to a threat feed from a vendor to receive regularly updated CTI. These feeds have the advantage in that there may be a service level agreement on data quality.[21]

Participants in this survey were asked if they thought external relationships were important in strengthening cybersecurity capabilities. Next, they were asked if the organization they represented had established external relationships to leverage cybersecurity. As a reference, the survey listed a number of external relations:

- Customers;
- On- and offsite contractors;
- Business partners;
- Third-party providers of security-related services;
- External sources for threat analyses;
- Private - public initiatives;
- Cross-organizational projects.

"The challenge for cybersecurity spans the interconnected global business ecosystem."

21 SANS Institute (2013). Tools and standards for Cyber Threat Intelligence Projects p9-10.

External Relations to Strengthen Cybersecurity

Do you think external relationships are important in strengthening cybersecurity capabilities?

Perceived versus actual scores

Figure 55 correlates the security expert opinion with the actual status for this topic. From the results it can be concluded that nearly all participants indicate that external relations are very important for cybersecurity.

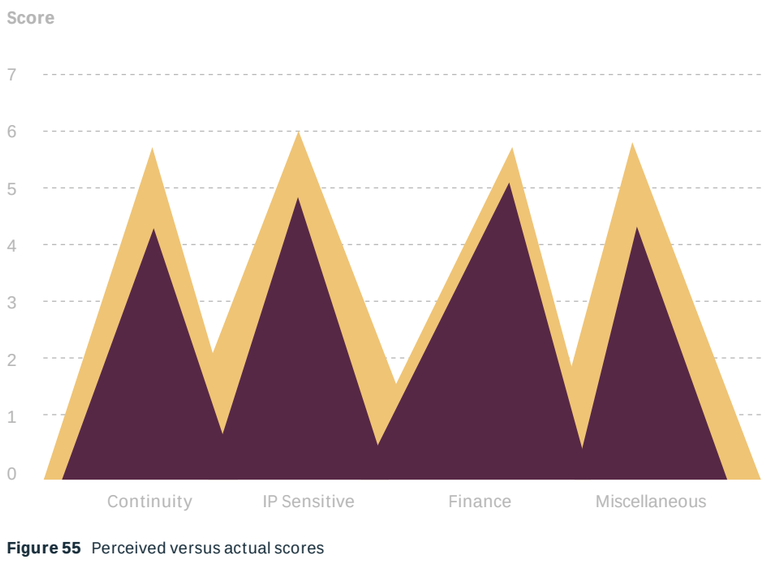


Figure 55 Perceived versus actual scores

Relative deviations

Figure 56 shows that expectations are not fully met, especially not in the continuity-sensitive cluster, showing the largest number of deviations between perceived and actual scores.

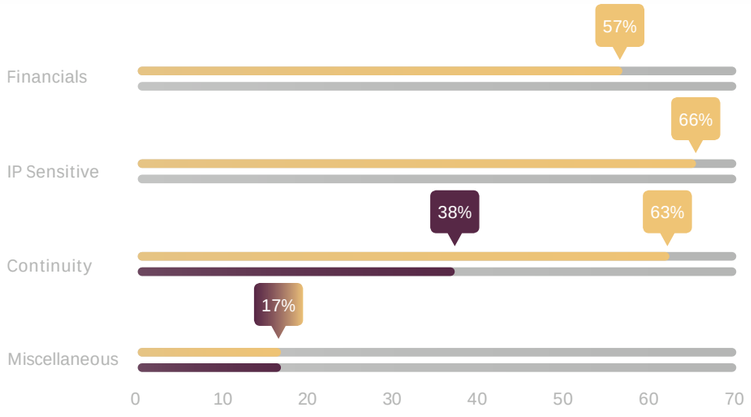


Figure 56 Relative deviations perceived versus actuals

> Of all external relations groups, customers receive the least attention when it comes to cybersecurity.

Actual scores per cluster

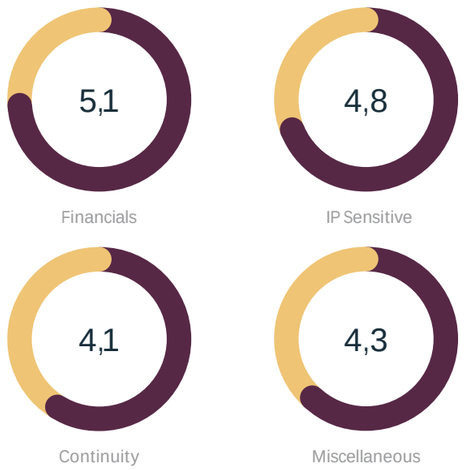


Figure 57 Actual scores per cluster on a scale 1-7

Figure 57 compares the actual scores for this topic. Participants in the finance sector report the highest actual scores, relative to other clusters.

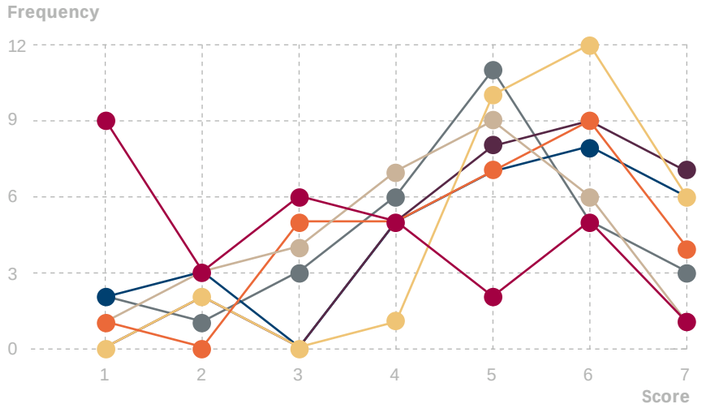


Figure 58 Actual scores per option

Actual scores per option

Figure 58 shows the distribution in scores for each option in this this topic. In this survey, participants indicate that, of all external relations groups, customers receive the least attention when it comes to cybersecurity.

- Customers
- On- and offsite contractors
- Business partners
- Third-party providers of security related services
- External sources for threat analyses
- Private - public initiatives
- Cross organizational projects

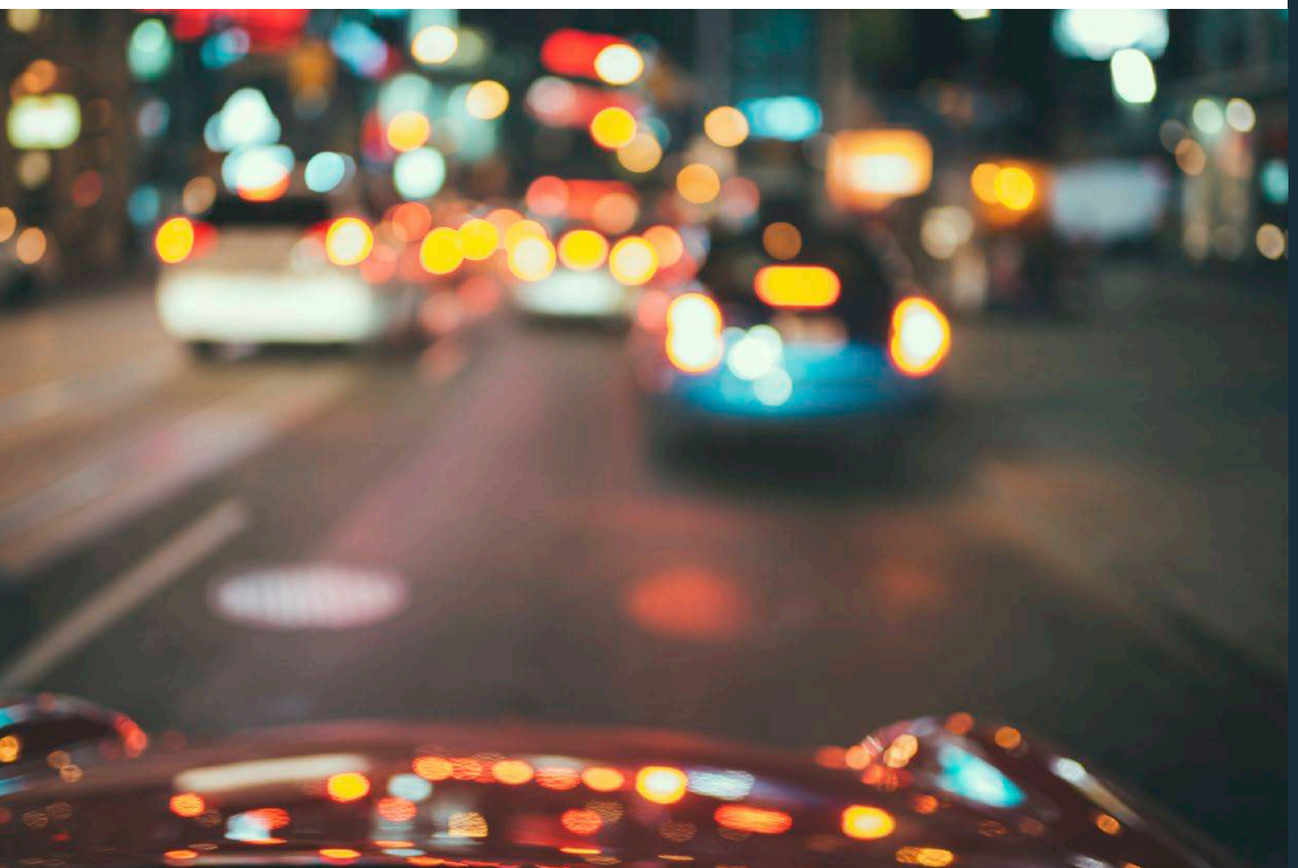
External cyber hubs

Increasingly, organizations benefit from useful hubs for knowledge sharing to strengthen their cybersecurity capabilities.

At a national level, the Hague Security Delta (HSD) brings together companies, governments, and knowledge institutions to work together on innovations and knowledge in the field of cybersecurity. Initiatives include a cybersecurity academy and a research lab for demonstration purposes and serious gaming. In addition, a virtual campus environment has been created for entrepreneurs to develop new cybersecurity-related products and services.

At a European level, the European Union Agency for Network and Information Security (ENISA) provides a hub for the exchange of information, best practices and knowledge in the field of information security. Amongst other activities, ENISA helps facilitate the setting up, training and exercising of CERTs. They also operate a so-called Critical Information Infrastructure Protection (CIIP) and Resilience Unit, responsible for assisting national EU agencies, the private sector and the EU Commission to develop sound and implementable preparedness, response and recovery strategies, policies and measures that fully meet the emerging threats faced by critical information infrastructures today.

Recently, ISACA launched *Cybersecurity Nexus*™ (CSX). CSX is a knowledge platform for cybersecurity professionals, providing a comprehensive set of resources i.e. research, guidance, certificates and certifications, education, mentoring and community facilities. All CSX materials are designed to provide security-related information within the larger business context.
ISACA offers this platform in addition to COBIT, the existing business framework that helps enterprises govern and manage their information and technology.
This way, ISACA provides for a one-stop concept along with complementary knowledge products that relate to governance, risk and compliance.



Survey
4.14 | *Architecture*

Introduction

Where previously the security architecture of an organization regarded the corporate firewall as the known boundary, organizations now have to deal with a problem space that consists of corporate data potentially residing across multiple continents. Also, with traditional security perimeters dissolving, organizations are faced with the task of securing highly virtualized IT environments that embrace the corporate use of mobile devices and the adoption of cloud and social computing technologies.

If cybersecurity is going to effectively protect data and applications across all these virtual pathways, it will need to be embedded in the enterprise architecture and increasingly be viewed as a critical part of business strategy rather than merely as a tactical function.

Mitigating APT risk requires broader use of technologies such as strong authentication and encryption, as well as extensive security monitoring and effective vulnerability management. These requirements will have a significant impact on the information-, IT- and security architectures, which will need to be reviewed to provide stronger protection for intellectual assets.

More mature organizations tend to have a scalable architecture to manage and search logs, thereby enabling correlation and alerting. Increasingly, a Security Information/ Event Management system (SIEM) is an important component in a security architecture. For the purpose of building threat intelligence, a SIEM collects log data, normalizes it into a consistent format and allows for cross-checking of events from multiple systems. SIEM serves two detection functions: as a repository and correlation platform for alerts generated by other means, and as an alerting capability based on network traffic flows and past logs. In addition, these allow for detailed reporting, and the sending of notification with a high degree of confidence. In that respect, SIEM products are rapidly becoming an important part of regulatory compliance monitoring as well.

Participants in this survey were asked if they thought it was important to maintain a reference architecture that described current and target states including a corresponding security architecture. Next, they were asked if the organization they represented maintained a reference architecture that potentially addressed:

- Industry best practices for building a security architecture;
- Clearly defined blueprint and a roadmap that guides from the current state to a desired 'to-be' position;
- Significant parts of the IT architecture being de-parameterized;
- Parts of the IT architecture being operated by third parties;
- Exposed parts of the overall architecture that have high risk/ exposure to attacks and breaches.

> "If cybersecurity is going to effectively protect data and applications across all virtual pathways, it will need to be embedded in the enterprise architecture."

Cybersecurity Embedded in Enterprise Architectures

Do you think it is important to maintain a reference architecture that describes current & target states including a corresponding security architecture?

Perceived versus actual scores

Figure 59 correlates the security expert opinion with the actual status for this topic. From the results it can be concluded that relative to other participants, the IP-sensitive cluster perceive architectures to be a very critical part in cybersecurity.

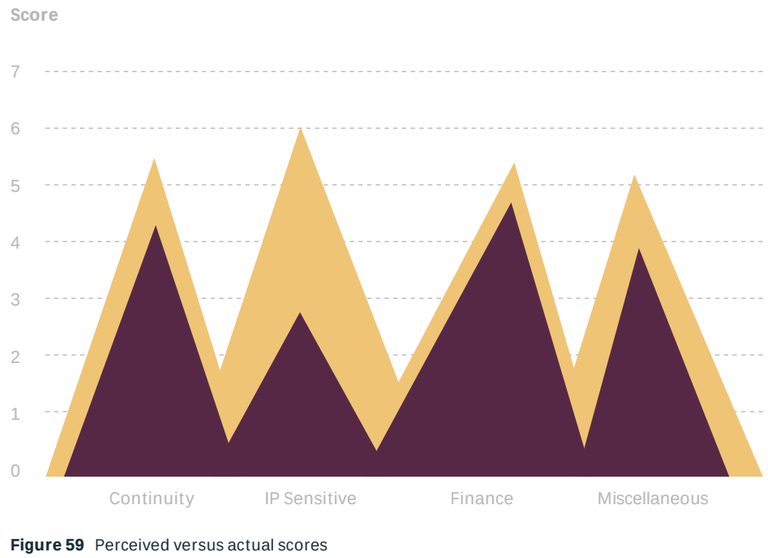


Figure 59 Perceived versus actual scores

Relative deviations

Figure 60 shows that, when it comes to security architectures and road maps, organizations in the IP-sensitive cluster have a great challenge ahead of them.

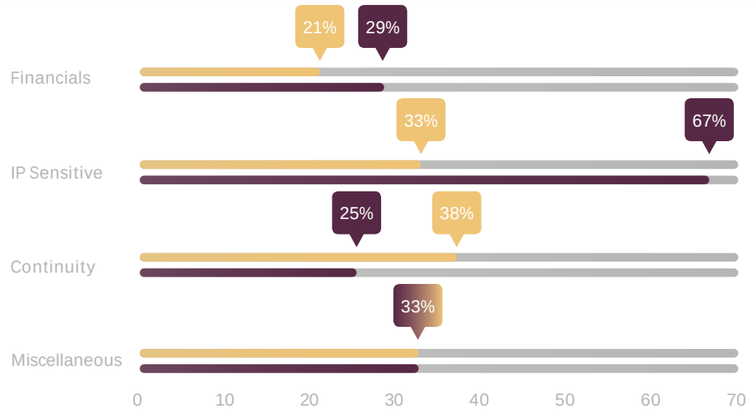


Figure 60 Relative deviations perceived versus actuals

> If cybersecurity is going to effectively protect data and applications across all virtual pathways, it will need to be embedded in the enterprise architecture.

Actual scores per cluster

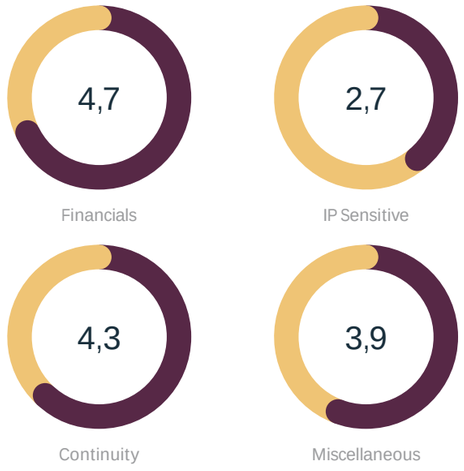


Figure 61 Actual scores per cluster on a scale 1-7

Figure 61 compares the actual scores for this topic. Participants in the finance sector report the highest actual scores, relative to other clusters.

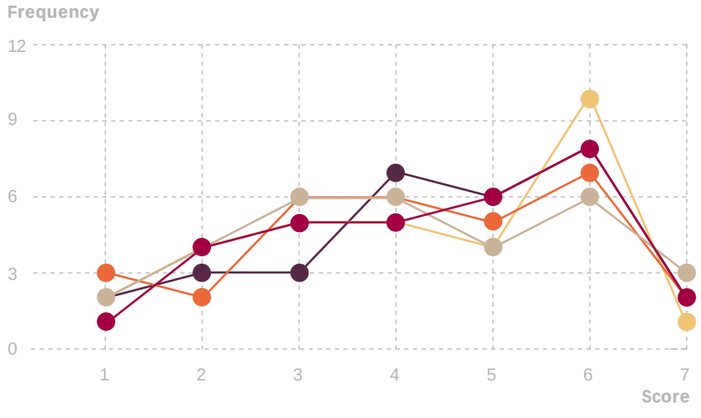


Figure 62 Actual scores per option

Actual scores per option

Figure 62 shows the distribution in scores for each option in this this topic. In this survey, participants indicate that, of all referenced attributes, applying a clearly defined blueprint and a roadmap that guides from the current state to a desired 'to-be' position is the most challenging.

- Covering industry best practices for building a security architecture
- Applying a clearly defined blueprint and a roadmap that guides from the current state to a desired 'to-be' position
- Covering significant parts of the IT architecture being de-perimeterized
- Covering parts of the IT architecture being operated by third parties
- Covering exposed parts of the overall architecture that have high risk/ exposure to attacks and breaches

Survey
4.15 | *Third-Party Management*

Introduction

It is increasingly common for organizations to form a contractual relationship with third parties to handle even business-critical functions. Companies rely on others for software, hardware, ancillary business functions (HR or payroll), or functions that in the past would have been considered business-critical (like order fulfillment, shipping, or even design or manufacturing). Organizations that outsource can fall into the trap of thinking they have transferred cyber risks and other risks, when actually they have retained much of that risk. They may even have added other risks if the outsourcing provider has inadequate security controls or business continuity procedures.

Cyber risks usually are distributed across the value chain, and if each organization, customer, vendor and supplier is considered to be a link in this chain, then each link needs to be equally strong. This is most evident in advanced attacks that often use third-party vendors to deliver malicious software to upstream targets.

Vulnerabilities may also show up in procurement as new products and software may not be sufficiently secure in their design. Suppliers may not face market pressures or requirements to incorporate cybersecurity features in the design of their systems and devices. Organizations may also be subject to malicious manipulation or be compromised by the use of counterfeit parts. The risk presented by substandard products and services may affect an organization's cybersecurity posture. All these issues are further complicated by the global nature of supply chains, which offer multiple possible entry points for cyber attacks. For example, numerous SCADA (Supervisory Control And Data Acquisition) devices are manufactured overseas, including in China, where external cyber threats have originated in the past.

> "Each link needs to be equally strong as cyber risks usually are distributed across the value chain."

In distributed and decentralized IT architectures, the third-party risk is likely to increase, often as a function of moving critical applications, platforms and infrastructure elements into the cloud. Simultaneously, third-party cloud providers are facing an increased risk of attacks and breaches, due to the agglomeration and clustering of sensitive data and information. As we see more and more critical applications being contracted and operated as a cloud service, the third-party risk is likely to increase since clustering of critical data and information in cloud-based repositories increases the attractiveness of such targets.

Another risk concentration occurs when a large number of companies, especially in the same sector, all use the same outsource provider. Once a major client organization has agreed to outsource a service after considerable due diligence, its peers feel justified (or even compelled by cost pressure) to follow its lead. In such circumstances, a failure at the outsourcing company is far more likely to cascade to not just a few companies, but to large segments of a newly dependent sector.

Security architecture

There is growing aspiration amongst organizations to have a clearly defined enterprise security blueprint and a roadmap that takes them from the current state to a desired 'to-be' position. The use of open industry standards like TOGAF and SABSA may prove very effective in creating an enterprise architecture with integrated security.

TOGAF (The Open Group Architecture Framework) is an architecture framework that provides the methods and tools for designing, planning, implementing and governing an enterprise information technology architecture. SABSA (Sherwood Applied Business Security Architecture) is also an open standard but with a strong focus on information security and assurance in developing enterprise architectures. With TOGAF lacking a full security architecture, both frameworks may well complement each other for the purpose of providing a holistic approach to cybersecurity.

Using TOGAF/SABSA, a method for security architecture design will start with gathering input for defining a so-called corporate identity. Strategic business objectives, key business risks, high-level processes, organization charts, available resources, etc. will provide a good starting point for the analyst or enterprise architect.

Amongst other elements, SABSA provides a toolkit for enriching business drivers with attributes from the SABSA library and translating business risks to control objectives for security, thus providing valuable input for establishing a security architecture. Industry standards have a number of advantages: apart from the holistic approach and risk view, they facilitate communications between business and IT, using a common language. In addition, using these standards enables two-way traceability, making it possible for security provisions to always be traced back to the original requirements.

Evaluate Third Parties for Cybersecurity

Do you think it is important to evaluate third-parties against cyber risks?

Perceived versus actual scores

Figure 63 correlates the security expert opinion with the actual status for this topic. From the results it can be concluded that nearly all participants indicate third-party management to be very important for cybersecurity.

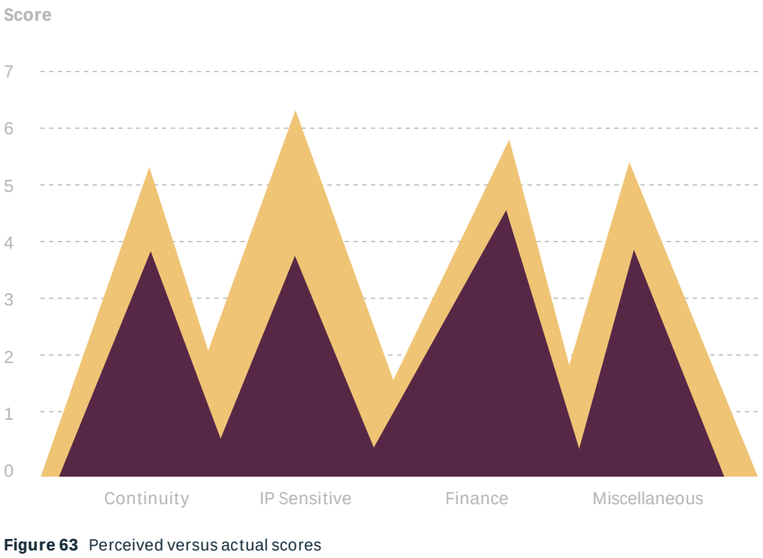


Figure 63 Perceived versus actual scores

Relative deviations

Figure 64 shows that, most respondents report many deviations between perceived and actual scores, indicating that many organizations struggle with this topic. Especially in the IP-sensitive organization, all participants show either significant or minor deviations.

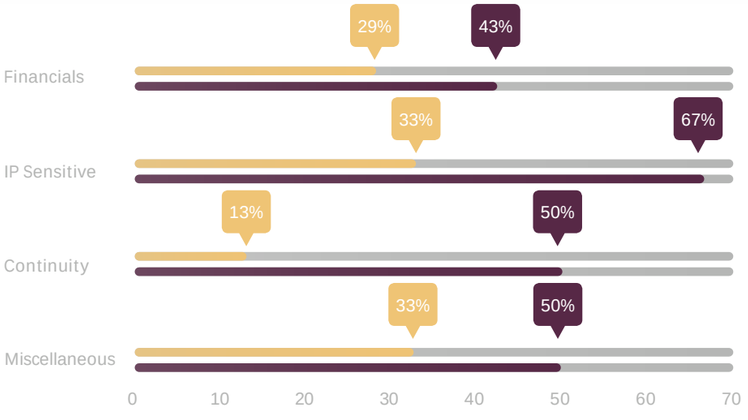


Figure 64 Relative deviations perceived versus actuals

> Updating risk rating for all third parties subject to cybersecurity requirements proves most difficult in third-party management.

Actual scores per cluster

Figure 65 Actual scores per cluster on a scale 1-7

Figure 65 compares the actual scores for this topic participants in the finance sector report the highest actual scores, relative to other clusters.

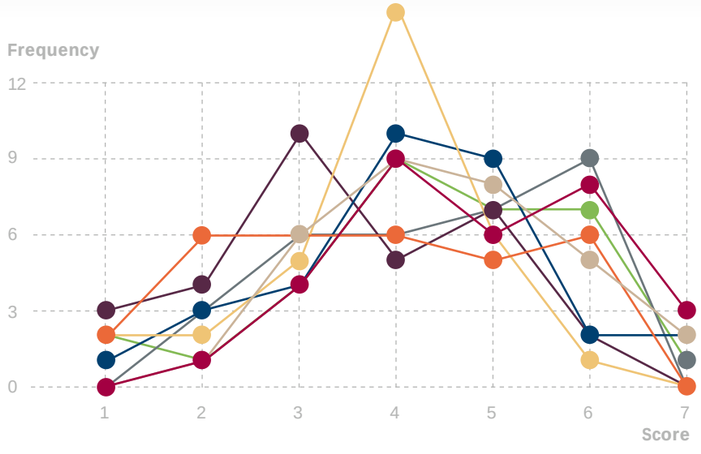


Figure 66 Actual scores per option

Actual scores per option

Figure 66 shows the distribution in scores for each option in this this topic. In this survey, participants indicate that, of all reference items, updating risk rating for all third parties subject to cybersecurity requirements proved most difficult in third-party management.

- In managing third party access to the environment
- In reviewing Cybersecurity-related provisions in contracts as appropriate
- In extending the security awareness program to all contractors, onsite vendors and other external partners
- In engaging with third parties to achieve upstream Cybersecurity controls
- In assessing vendor services and operating levels against criteria and requirements in Cybersecurity
- In updating risk rating for all third parties subject to Cybersecurity requirements
- In assessing and reviewing suppliers for Cybersecurity compliance and performance
- In including Cybersecurity requirements and testing in third-party assurance plans

Lockheed Martin best practices

Lockheed Martin has a very pro-active approach to third-party management, using a variety of methods including supplier briefings, assessments and information-sharing sessions.

Lockheed Martin has developed a supplier cybersecurity questionnaire to provide an initial indication of cybersecurity readiness. They require all suppliers with whom they share sensitive information to complete and maintain a supplier cybersecurity questionnaire. This helps them better understand their supplier's cybersecurity readiness and better manage risks associated with sharing sensitive information. As cybersecurity capabilities evolve, suppliers are requested to update the cybersecurity questionnaire.

In addition, Lockheed Martin organizes supplier briefings to discuss the newest and most pressing cybersecurity threats, cybersecurity best practices, and how to better manage risk. These sessions are collaborative in nature and are helpful in introducing suppliers to organizations and teams that can provide on-going threat- and risk management information.

Also, Lockheed Martin conducts onsite discussions and objective evidence reviews in coordination with suppliers. The assessments look at items like cybersecurity controls, risks, and potential signs of cybersecurity damage in order to help Lockheed Martin and the supplier understand the extent of their cybersecurity capabilities, and their ability to protect sensitive information and deliver secure products and services.

Survey
4.16 | *Incident Response*

Introduction

The threats that organizations face today by being connected to the Internet are evolving at a much faster pace than the information security architectures, technologies and processes they have deployed. No matter the strength of defenses, sophisticated attackers with advanced capabilities have the means and determination to adapt and defeat the most complex prevention- and detection measures the organization might deploy, regardless of size. To ensure resilience, organizations must prepare for an attack and anticipate adequate incident response so that critical business operations can be continued in the event of a significant breach or disruption. In addition, the organization must be able to conduct an investigation of a breach, to execute the remediation/eradication plan to successfully expel the attackers from the environment and, in some cases, enable forensics to be performed within the legal framework.

> "Organizations must anticipate adequate incident response so critical business operations can be continued in the event of a significant breach or disruption."

ISACA has published an excellent paper on incident response: "Responding to Targeted Cyberattacks". Other very good models exist, including models published by NIST and the SANS Institute. Regardless of the model, conceptually the incident response process may cover a number of distinct phases: identification, containment, eradication, recovery and follow-up. This process will come into effect once a breach has occurred. Organizations that have invested time and resources into preparing for a breach will do far better in their response and eradication efforts (also see Belgacom case study).

Several activities may be considered in incident response planning:

1. Establish key relationships: to operate effectively and efficiently during incident response, an organization should establish relationships, both external and internal. External relationships may include business partners, i.e. anyone who would be impacted if the organization is forced to operate in a degraded capacity. In addition, an organization might try to secure internal and external resources to support the investigation and eradication process.
2. Determine authorities: knowing in advance who has the authority to take down networks and systems or otherwise degrade operations will prove invaluable in a crisis situation.
3. Inventorize existing technologies: a well-maintained, actionable inventory of existing technologies and assets aids in conducting an efficient investigation and eradication operation.
4. Establish critical capabilities: a gap analysis of existing capabilities may provide input for a plan to close the gaps so that the organization can better manage a security breach when it occurs. Relevant capabilities may include: malware analysis, digital forensics, host-level- and network-level awareness.
5. Other preparatory activities may be to standardize the investigation process, introduce regular incident response reviews and provide for training and awareness. Also in external relations.[22]

22 ISACA (2013). Responding to targeted attacks.

Incident Response Capabilities

Do you think it is important to have capabilities in place to ensure adequate incident response in the event of a significant breach or disruption?

Perceived versus actual scores

Figure 67 correlates the security expert opinion with the actual status for this topic. From the results it can be concluded that relative to other participants, finance organizations perceive incident response to be most important for the success of cybersecurity.

Figure 67 Perceived versus actual scores

Relative deviations

Figure 68 shows that, especially in the IP-sensitive organization, participants report many significant deviations, indicating their struggle with this topic.

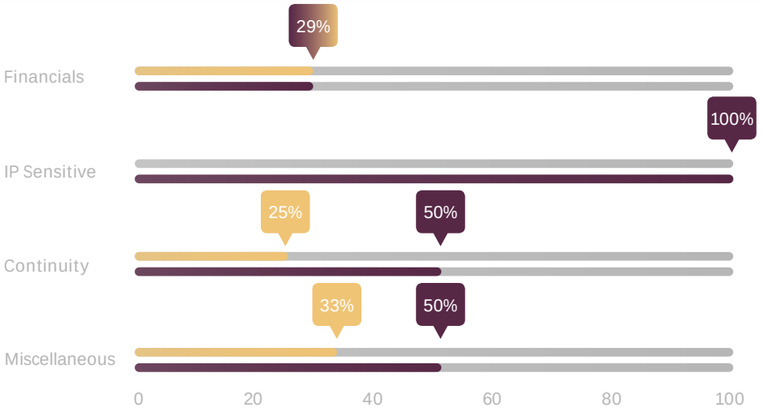


Figure 68 Relative deviations perceived versus actuals

> Establishing interfaces with Corporate Communication appears to be most difficult in incident response.

Actual scores per cluster

Figure 69 Actual scores per cluster on a scale 1-7

Figure 69 compares the actual scores for this topic. Participants in the finance sector report the highest actual scores, relative to other clusters.

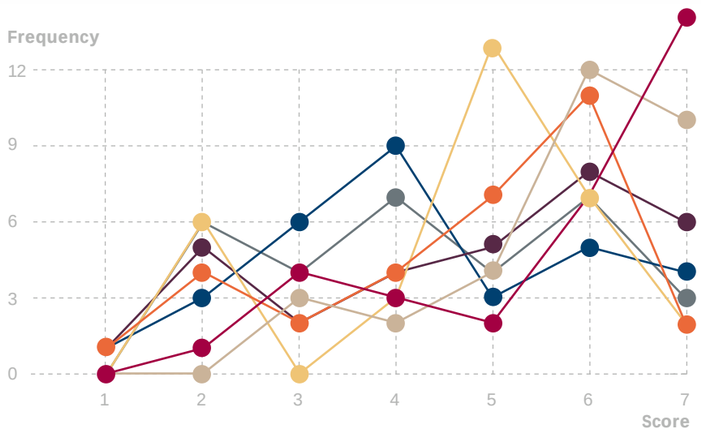


Figure 70 Actual scores per option

Actual scores per option

Figure 70 shows the distribution in scores for each option in this this topic. In this survey, participants indicate that, of all reference items, establishing incident response interfaces with Corporate Communication seems to be most difficult.

- Establishing incident response interfaces with Business Continuity Management (BCM) and crisis management processes
- Establishing incident response interfaces with Corporate Communication
- Establishing relationships with business partners in the event the organization must operate in a degraded capacity
- Establishing relationships with third parties offering professional services in the event of a major breach or disruption
- Establishing a comprehensive contact list of all internal relationships including corresponding authorities and escalation paths
- Relying on a reliable and continually updated computer asset inventory
- Anticipating possible investigations and forensics

Incident Response Investigation

Phase One of the core components of incident response is the collection and analysis of facts during the investigation phase. In the case of cyber attacks, the primary purpose of the investigation is to provide intelligence to the eradication and remediation plan. It is often seen that organizations that have been attacked have generally been notified of the attack by an external source, e.g. a law enforcement or intelligence organization. Organizations have rarely independently detected the attacks, so once an organization understands that it has been attacked, management will have many questions that the investigation will seek to answer, the main ones being: Who has attacked us? When did the attack occur? What did the attackers take from us? Why did they do it?

Eradication is aimed at removing the attackers from the environment. Eradication must be executed with speed and precision. Too often, enterprises rush into eradication activities by blocking an infection vector or point of persistence as soon as it is discovered, before the full scope of the compromise is understood. This approach leaves the enterprise constantly chasing the adversary as the attacker's tactics change in response to the enterprise's poorly planned response. Immediately after a successful completion of the eradication, the organization must continue to operate in a heightened state of alert, as the attacker may try to re-establish. Once all Indicators of Compromise (IOC) have been eradicated and normal operations have resumed, final steps for the incident response team include conducting lessons learned and briefing all relevant stakeholders.[22]

Case study

Friday July 13, 2013, just before lunch, Belgacom IT consultants receive a communication from headquarters. The message doesn't say much, just the request to cancel all appointments. Instead, an emergency conference call will take place. The call takes everyone's breath away. Malware has been discovered on the BICS network, a Belgacom subsidiary. The impact is difficult to comprehend, even for knowledgeable insiders ...

Belgacom International Carrier Services (BICS) operates a network in Belgium that handles telephone traffic, mobile data and Internet. Amongst the customers of BICS are SWIFT, Electrabel, NATO, European Parliament, European Commission etc.

The incident caused great political turmoil. In addition, it appeared to be very difficult to successfully eradicate all malware from the infected network, as can be seen from media reports:

19/07/2013: Belgacom formally reports breach

31/08 – 01/09/2013: Fox-IT first attempts to eradicate malware but doesn't succeed

14-15/09/2013: Fox-IT reports successful eradication

04/10/2013: Newspaper De Standaard reports BICS not getting rid of spyware

17/10/2013: Belgacom admits BICS router still compromised

04/12/2013: Newspaper De Tijd reports: *"Belgacom cannot control hack"*

22 *ISACA (2013). Responding to targeted attacks.*

Survey
4.17 | *Monitoring*

Introduction

To effectively defend against cyber attacks and breaches, both security management and monitoring of the governance system need to be in place to achieve and maintain an adequate level of security.

When it comes to cybersecurity, the concept of monitoring extends beyond the use of technology that looks for signs of malware and detects unauthorized intrusions. Effective monitoring will also have to provide an on-going feedback on meeting strategic security objectives and remaining in compliance with legal and regulatory requirements. The cybersecurity strategy and action plans must contain provisions for monitoring, as well as defined metrics to determine the level of success. In addition, managing and measuring cybersecurity will include policy enforcement, to ensure that the intentions of policies are met. Additionally, it will establish a framework to track the progress of the cybersecurity program, to ensure that planned initiatives are on track to meet defined objectives.

Every organization must choose a set of metrics that is appropriate to measure the effectiveness of their governance system. Key metrics and performance indicators that relate to cybersecurity may include:

- Measuring activities to protect against threats, such as measuring performance of boundary protection, intrusion detection and -prevention devices and antivirus software.
- Vulnerability management that helps to detect flaws and reduces vulnerabilities, e.g. by scheduling regular scans.
- Business drivers: measuring costs, quality and return on investment, to put cybersecurity in a business perspective.
- Comparing to other organizations: understanding how an organization's cybersecurity posture compares with its peers is important not only to understand whether the organization is investing properly but also in understanding its potential risk.
- Compliance: enterprise-specific monitoring processes to ensure compliance and provide on-going feedback on effectiveness.[23]

Participants in this survey were asked if they thought it was important to have mechanisms in place to monitor the effectiveness of the cybersecurity governance system. Next, they were asked if the organization they represented had mechanisms in place to monitor the effectiveness of the cybersecurity governance program. As a reference, eight items were given that may be part of the monitoring process:

- Definition of requirements, indicators, data sets and collection methods for cybersecurity monitoring;
- Implications of the changing threat landscape on the risk profile and corresponding risk appetite;
- Monitoring of the effectiveness of cybersecurity resources (internal and external) against defined security needs, goals and objectives;
- Mechanisms to ensure that the Information Security Management System (ISMS) meets compliance with cybersecurity-related legislation and regulations;
- Operations management;
- Change management, emerging technologies and innovations;
- Structural identification of security weaknesses, exposures, vulnerabilities and threats;
- Security testing and internal and external audits performed on a regular basis.

23 *Gregory J. Touhill, C. Joseph Touhill (2014). Cybersecurity for Executives - A Practical Guide p263.*

Monitoring Cybersecurity Governance

Do you think it is important to have mechanisms in place to monitor the effectiveness of the cybersecurity governance system?

Perceived versus actual scores

Figure 71 correlates the security expert opinion with the actual status for this topic. Participants in the IP-sensitive cluster indicate that, in their view, monitoring is a critical part of cybersecurity governance.

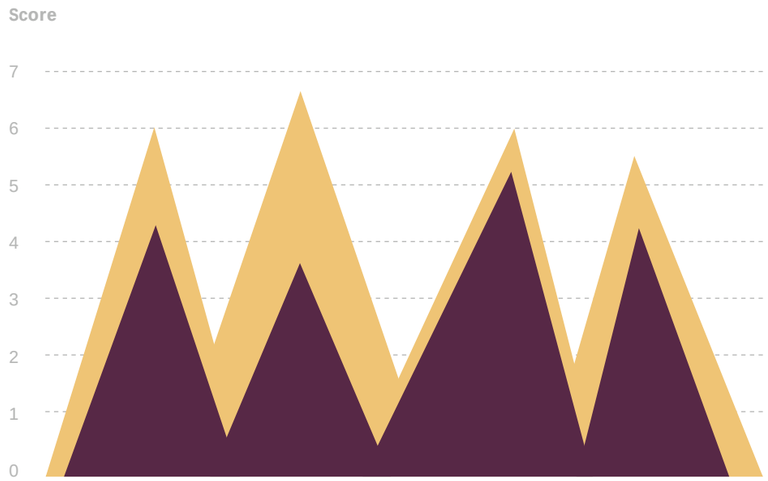


Figure 71 Perceived versus actual scores

Relative deviations

Figure 72 shows that, when it comes to cybersecurity monitoring, organizations in the IP-sensitive cluster have a great challenge ahead of them.

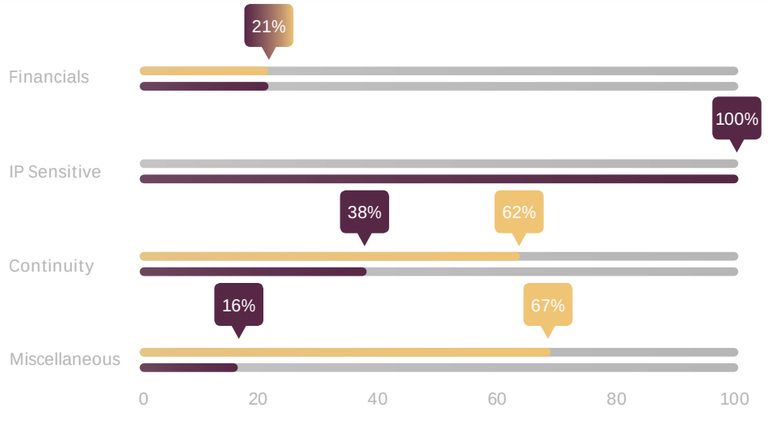


Figure 72 Relative deviations perceived versus actuals

> When it comes to cybersecurity, the concept of monitoring extends beyond the use of technology that looks for signs of malware and detects unauthorized intrusions.

Actual scores per cluster

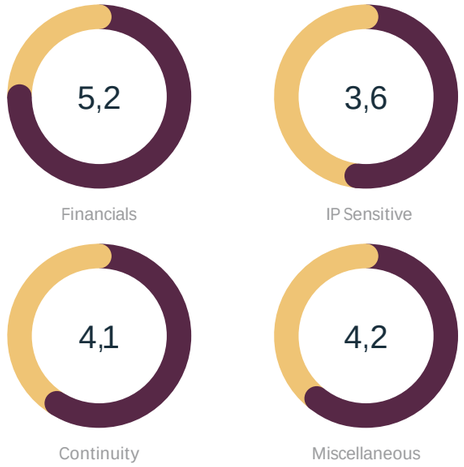


Figure 73 Actual scores per cluster on a scale 1-7

Figure 73 compares the actual scores for this topic. Participants in the finance sector report the highest actual scores, relative to other clusters.

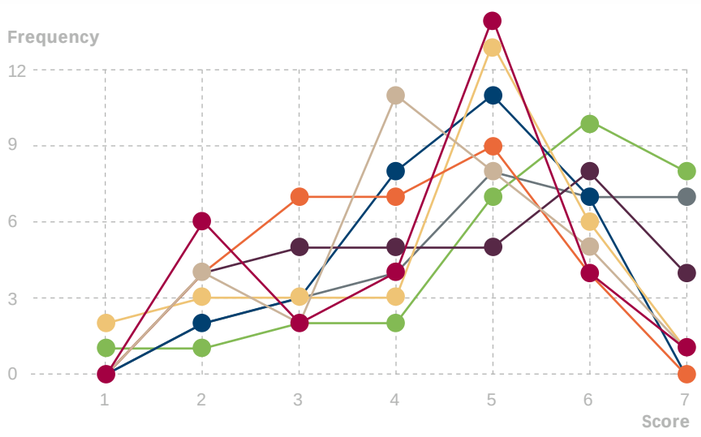


Figure 74 Actual scores per option

Actual scores per option

Figure 74 shows the distribution in scores for each option in this this topic. In this survey, participants indicate that, of all reference items, the most challenging topic in monitoring seems to be security testing and performing internal and external audits on a regular basis.

- Covering the definition of requirements, indicators, data sets and collection methods for Cybersecurity monitoring
- Covering the implications of the changing threat landscape on the risk profile and corresponding risk appetite
- Covering the monitoring of the effectiveness of Cybersecurity resources (internal and external) against defined security needs, goals and objectives
- Covering mechanisms to ensure that the information security management system (ISMS) meets compliance with Cybersecurity related legislation and regulations
- Covering operations management
- Covering change management, emerging technologies and innovations
- Covering the structural identification of security weaknesses, exposures, vulnerabilities and threats
- Covering security testing and internal and external audits be performed on a regular basis

SANS Critical Security Controls metrics

Over the years, many security standards and requirements frameworks have been developed in an attempt to address risks to enterprise systems and the critical data they store. However, most of these efforts have essentially become exercises in reporting on compliance and have actually diverted security program resources from the constantly evolving attacks that must be addressed. In response to this issue, the SANS Institute coordinated the so-called Critical Security Controls. This framework focuses first on prioritizing security functions that are effective against the latest Advanced Targeted Threats, with a strong emphasis on “What Works”.

One of the objectives is for every control to establish common metrics to provide a shared language for executives, IT specialists, auditors, and security officials to measure the effectiveness of security measures within an organization so that required adjustments can be identified and implemented quickly. In the framework, all 20 controls include effectiveness metrics as well as automation metrics to automate the collection of relevant data.

20 Critical Security Controls - Version 5:

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
4. Continuous Vulnerability Assessment and Remediation
5. Malware Defenses
6. Application Software Security
7. Wireless Access Control
8. Data Recovery Capability
9. Security Skills Assessment and Appropriate Training to Fill Gaps
10. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
11. Limitation and Control of Network Ports, Protocols, and Services
12. Controlled Use of Administrative Privileges
13. Boundary Defense
14. Maintenance, Monitoring, and Analysis of Audit Logs
15. Controlled Access Based on the Need to Know
16. Account Monitoring and Control
17. Data Protection
18. Incident Response and Management
19. Secure Network Engineering
20. Penetration Tests and Red Team Exercises

05 Appendices

5.1 | *Questionnaire*

1a. Do you think cybersecurity-related trends are important in setting governance?

1b. Within your organization, to what extent are cybersecurity-related trends being identified in the business environment?

1c. Within your organization, have cybersecurity-related trends in the business environment been analyzed for possible impact on current governance design?
- Concerning the evolving threat landscape?
- Concerning emerging technologies?
- Concerning trends in the legal and regulatory realm?
- Concerning contractual obligations?
- Concerning sourcing?

2a. Do you think senior management/board level commitment and leadership are important to cybersecurity?

2b. Within your organization, how would you rate senior management/board level commitment and leadership to cybersecurity
- In recognizing the exposure to cybercrime?
- In itemizing cybersecurity on the board agenda, on a regular basis?
- In communicating expectations for strong cybersecurity throughout the organization?
- In establishing a structure for the implementation of a cybersecurity program?
- In having the status of cybersecurity programs reported to the board?

3a. Do you think it is important to know to what extent cybersecurity is capable of meeting stakeholder needs?

3b. Within your organization, have stakeholders’ requirements been identified for the purpose of protecting their interests?

3c. Are your organization’s stakeholders being informed about the current status of cybersecurity and cyber risks:
- Investors/shareholders?
- Regulatory bodies?
- Internal stakeholders?
- Customers?
- Suppliers/vendors?

4a. Do you think it is important to anticipate new cybersecurity-related regulations in security- and compliance management?

4b. Does your organization anticipate cybersecurity while reviewing and updating policies and procedures to ensure that IT- and business processes are compliant:
- In identifying any applicable laws or regulations?
- In assessing the impact on contractual obligations?
- In evaluating the extent to which cybersecurity provisions meet the business and compliance/ regulatory needs?
- In setting up the policies, processes and training regimes?
- In vendor management, assessing and reviewing suppliers for cybersecurity compliance? ▸

5a. In general, how do you perceive the importance of having a cybersecurity strategy?

5b. Does your organization have a cybersecurity strategy:
- That provides a link to the organization's objectives?
- That addresses the balance between benefits, costs and risks?
- That addresses meeting business- and compliance/ regulatory needs?
- That provides a link to the IT strategy?
- That provides a link to the business continuity plan?
- That provides a link to risk acceptance levels?

6a. Do you think it is important to integrate cyber risks into an organization's risk program?

6b. Within your organization, are cyber risks being integrated into your risk program and analyzed against risk appetite and tolerance levels:
- To determine if the organization can continue to operate if critical information is unavailable, compromised or lost?
- To set priorities, manage investments, measure progress and make better-informed decisions?
- To determine what the consequence of a major cyber security incident would be in terms of lost revenue, lost customers and investor confidence?
- To determine what the consequences would be if the infrastructure became inoperable?

7a. How important do you think budgets are to accommodate an effective cybersecurity program?

7b. Within your organization, is budget space sufficient to adequately accommodate cybersecurity programs:
- That includes training and awareness campaigns?
- That includes IT capabilities to protect against malware, external attacks and intrusion attempts?
- That includes process redesign?
- That includes preparation for incident response?
- That includes operating expenses?
- That includes enhancing the Information Security Management System (ISMS)?

8a. Do you think principles, policies and standards are important to communicate directives in support of cybersecurity governance?

8b. Does your organization have principles and policies that are used to communicate directives in support of cybersecurity governance? Topics may include but are not limited to:
- Relationships with business partners, customers and other third parties;
- Compliance with legal and regulatory requirements;
- Adopting a risk-based approach;
- Evaluating current and future threats through cybercrime;
- Creating a realistic outlook on the future of cybersecurity;
- Obtaining external expertise as appropriate;
- Establishing data classification with regard to cybercrime;
- Secure acquisition, system development and maintenance;
- Fostering awareness and rules of behavior about cybersecurity and cybercrime.

9a. Do you think it is important to explicitly link cybersecurity activities to established organizational structures?

9b. Does your organization explicitly link cybersecurity activities to established organizational structures:
- Having a CISO or someone in this position to be charged with cybersecurity?
- Having interfaces between the cybersecurity function and other information security and information risk roles to be established organization-wide?
- Having RACI matrices to specify the level of involvement in cybersecurity?
- Having an appropriate decision-making model and authority levels for cybersecurity in place?
- Having hierarchical escalation paths to mandate attack- and incident response?

10a. Do you think culture, ethics and behavior, including tone at the top, are important for the success of cybersecurity? ▸

10b. In your organization, security culture is right for today's threat environment:
- To view itself as a high-risk or high-value target?
- To understand that prevention against cyber threats is almost impossible, that the network is already compromised or soon will be?
- To understand that associates are crucial for the success or failure of cybersecurity?
- To understand that the organization must be able to protect its most sensitive information in a compromised environment?
- To be externally aware of what is going on in the cybersecurity space?

11a. Do you think people skills and competences are important for the success of cybersecurity?

11b. In your organization, skills and competences are readily available to security managers and IT specialists to deal with today's cybersecurity demands:
- Allowing for the ability to formulate cybersecurity strategy components and strategic requirements?
- Allowing for in-depth understanding of compliance with laws, regulations, directives and standards?
- Allowing for the ability to establish and maintain a cybersecurity governance framework including supporting processes?
- Allowing for strong skills in risk assessment and analysis as well as risk treatment options?
- Allowing for extensive technical architecture skills, above-average experience in critical technologies?
- Allowing for profound skills and experience in operating security-related IT and processes, covering the organization end-to-end?
- Allowing for ability to perform assessments and extensive testing?

12a. Do you think cybersecurity training- and awareness programs are important to ensure the resilience of an organization?

12b. In your organization, have training- and awareness programs been put in place, that ensure a security-positive culture and environment:
- End users receive basic training covering elementary cybersecurity?
- Senior managers receive basic training covering elementary cybersecurity?
- Business representatives receive training covering business-related IT use?
- Security managers receive training covering advanced skills?

13a. Do you think external relationships are important in strengthening cybersecurity capabilities?

13b. In your organization, have external relationships been established to leverage cybersecurity
- Customers?
- On- and offsite contractors?
- Business partners?
- Third-party providers of security-related services?
- External sources for threat analyses?
- Private- and public initiatives?
- Cross-organizational projects?

14a. Do you think it is important to maintain a reference architecture that describes current and target states including a corresponding security architecture? ▸

14b. Does your organization maintains a reference architecture that describes current and target states including a corresponding security architecture:
- Covering industry best practices for building a security architecture?
- Applying a clearly defined blueprint and a roadmap that guides from the current state to a desired 'to-be' position?
- Covering significant parts of the IT architecture being de-parameterized?
- Covering parts of the IT architecture being operated by third parties?
- Covering exposed parts of the overall architecture that have high risk/exposure to attacks and breaches?

15a. Do you think it is important to evaluate business partners, assessing third-party contracts and proposals and managing third-party access and performance against cyber risks?

15b. Does your organization actively evaluate, assess and manage third parties to address cybersecurity in contracts, proposals and performance reviews:
- In managing third-party access to the environment?
- In reviewing cybersecurity-related provisions in contracts as appropriate?
- In extending the security awareness program to all contractors, onsite vendors and other external partners?
- In engaging with third parties to achieve upstream cybersecurity controls?
- In assessing vendor services and operating levels against criteria and requirements in cybersecurity?
- In updating risk rating for all third parties subject to cybersecurity requirements?
- In assessing and reviewing suppliers for cybersecurity compliance and performance?
- In including cybersecurity requirements and testing in third-party assurance plans?

16a. Do you think it is important to have capabilities in place to ensure adequate incident response in the event of a significant breach or disruption?

16b. Does your organization provide for capabilities and management practices to ensure adequate incident response in the event of a significant breach or disruption:
- Establishing incident response interfaces with Business Continuity Management (BCM) and crisis management processes?
- Establishing incident response interfaces with Corporate Communication?
- Establishing relationships with business partners in the event the organization has to operate in a degraded capacity?
- Establishing relationships with third parties offering professional services in the event of a major breach or disruption?
- Establishing a comprehensive contact list of all internal relationships including corresponding authorities and escalation paths?
- Relying on a reliable and continually updated computer asset inventory?
- Anticipating possible investigations and forensics?

17a. Do you think it is important to have mechanisms in place to monitor the effectiveness of the cybersecurity governance system?

17b. In an effort to optimize the overall governance system, does your organization have mechanisms in place to monitor the effectiveness of the cybersecurity governance program:
- Covering the definition of requirements, indicators, data sets and collection methods for cybersecurity monitoring?
- Covering the implications of the changing threat landscape on the risk profile and corresponding risk appetite?
- Covering the monitoring of the effectiveness of cybersecurity resources (internal and external) against defined security needs, goals and objectives?
- Covering mechanisms to ensure that the Information Security Management System (ISMS) meets compliance with cybersecurity related legislation and regulations?
- Covering operations management?
- Covering change management, emerging technologies and innovations?
- Covering the structural identification of security weaknesses, exposures, vulnerabilities and threats?
- Covering security testing and internal and external audits being performed on a regular basis?

Appendix
5.2 | *Sources*

1 High Representative of the European Union for Foreign Affairs and Security Policy (2013). Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace p3.

2 Ministry of Safety and Justice in the Netherlands (2013). Nationale Cybersecurity Strategie 2 – van bewust naar bekwaam p19-20.

3 ISACA (2013). Transforming cybersecurity: using COBIT 5 p29.

4 Garry B. Cohen (2009). Just Ask Leadership: Why Great Managers Always Ask the Right Questions p1.

5 U.S. Department of Homeland Security Publication, https://www.us-cert.gov/sites/default/files/publications/DHS-Cybersecurity-Questions-for-CEOs.pdf

6 ISACA (2013). Responding to targeted attacks p74.

7 ISACA (2013). Transforming cybersecurity: using COBIT 5 p26.

8 High Representative of the European Union for Foreign Affairs and Security Policy (2013). Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace p17.

9 Gregory J. Touhill, C. Joseph Touhill (2014). Cybersecurity for Executives - A Practical Guide p110.

10 ISACA (2013). Advanced Persistent Threats: How to Manage the Risk to Your Business p72-73.

11 Jason Healy (2014). Beyond data breaches: global interconnections of cyber risk p13.

12 Gregory J. Touhill, C. Joseph Touhill (2014). Cybersecurity for Executives - A Practical Guide p287-288.

13 McAfee (2013). The Economic Impact of Cybercrime and Cyber Espionage p8.

14 Ponemon Institute (2013). Cost of Data Breach Study: Global Analysis p9.

15 ISACA (2013). Transforming cybersecurity: using COBIT 5 p77-90.

16 ISACA (2012). COBIT 5 for Information Security p61-63.

17 ISACA (2013). Transforming cybersecurity: using COBIT 5 p36.

18 ISACA (2013). COBIT 5 for Information Security p38.

19 ISACA (2013). Transforming cybersecurity: using COBIT 5 p97-98.

20 PviB (2014) Job profiles in Information Security – A Basis for Uniform Qualification of Professionals in Information Security

21 SANS Institute (2013). Tools and standards for Cyber Threat Intelligence Projects p9-10.

22 ISACA (2013). Responding to targeted attacks.

23 Gregory J. Touhill, C. Joseph Touhill (2014). Cybersecurity for Executives - A Practical Guide p263.

Gooimeer 4 - 15 • 1411 DC Naarden • info@isaca.nl • www.isaca.nl