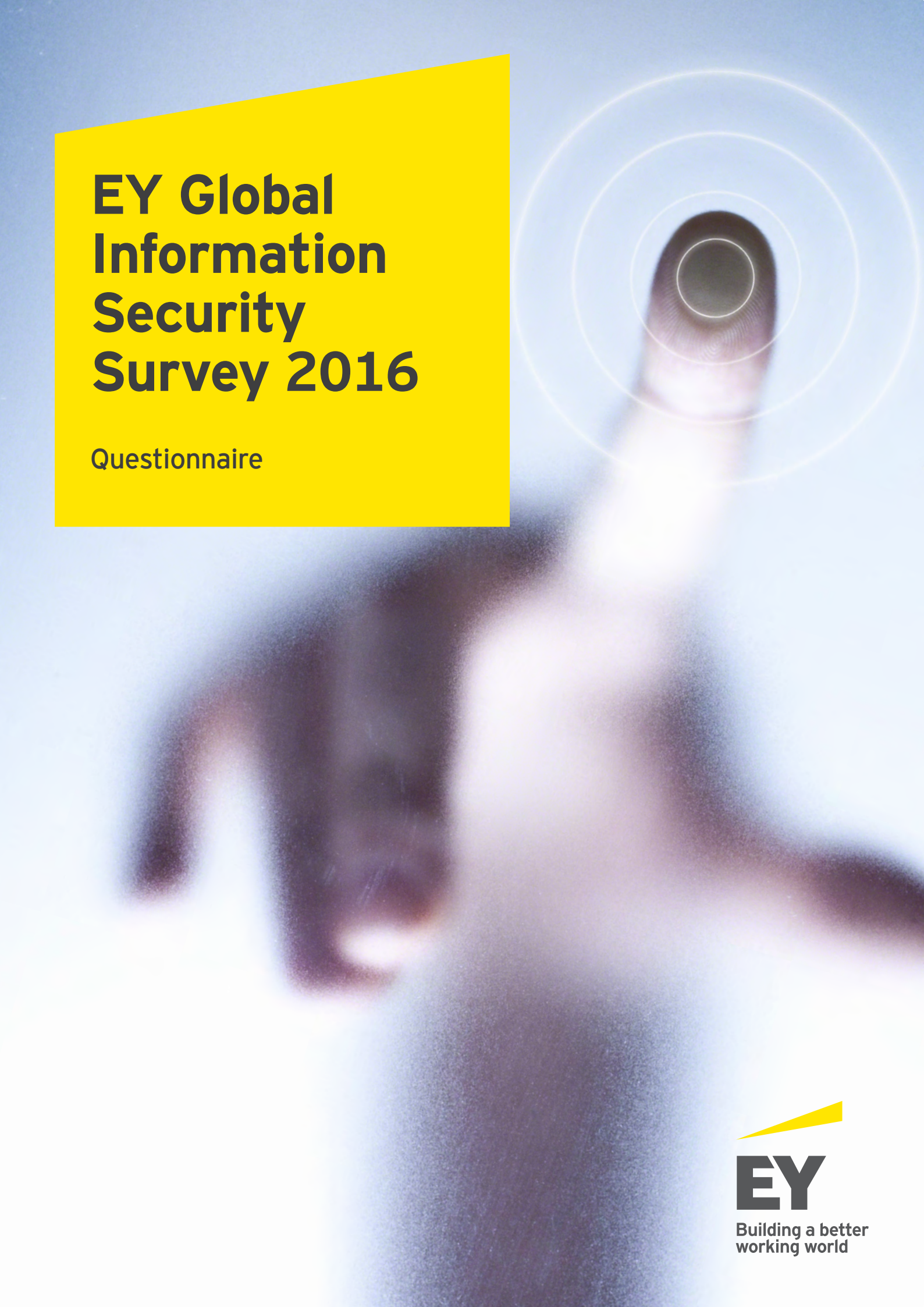
EY Global Information Security Survey 2016

Questionnaire



Building a better working world

EY Global Information Security Survey 2016

Questionnaire

The questionnaire is divided into sections that relate to different dimensions of an enterprise:

SECTION 1

Strategy, innovation and growth

1 What is your organization's total annual spend on information security (approximately, including people, process and technology costs)? *(Select one)*

- Less than US$1 million ☐
- Between US$1 million and US$2 million ☐
- Between US$2 million and US$10 million ☐
- Between US$10 million and US$50 million ☐
- Between US$50 million and US$100 million ☐
- Between US$100 million and US$250 million ☐
- More than US$250 million ☐
- Don't know ☐

2 Which of the following describes the change in your organization's total information security budget over the last 12 months? *(Select one)*

- Increased by more than 25% ☐
- Increased between 15% and 25% ☐
- Increased between 5% and 15% ☐
- Stayed approximately the same (between +5% and -5%) ☐
- Decreased between 5% and 15% ☐
- Decreased between 15% and 25% ☐
- Decreased by more than 25% ☐
- Don't know ☐

3 Which of the following describes the change in your organization's total information security budget in the coming 12 months? *(Select one)*

- Will increase by more than 25% ☐
- Will increase between 15% and 25% ☐
- Will increase between 5% and 15% ☐
- Will stay approximately the same (between +5% and 5%) ☐
- Will decrease between 5% and 15% ☐
- Will decrease between 15% and 25% ☐
- Will decrease by more than 25% ☐
- Don't know ☐

4 How much additional funding is needed to protect the company, in line with management's risk tolerance? *(Select one)*

0-25%	☐
26-50%	☐
51-75%	☐
76 -100%	☐
Over 100%	☐
Don't know	☐

5 How likely is it that any of the following events would encourage your organization to increase your information security budget in the coming 12 months?
(Select one response for each topic)

	Highly unlikely: (0-20% likelihood)	Unlikely: 20-50% likelihood)	Likely: (50-80% likelihood)	Highly likely: (80-100% likelihood)
Discovery of a breach with, apparently, no harm done	☐	☐	☐	☐
Discovery of a breach that resulted in the attackers impacting the organization	☐	☐	☐	☐
A DDoS attack	☐	☐	☐	☐
A cyber attack on a major competitor	☐	☐	☐	☐
A cyber attack on a supplier	☐	☐	☐	☐
M&A activity	☐	☐	☐	☐
A physical loss of confidential corporate information on a mobile device	☐	☐	☐	☐
A physical loss of customer information on a mobile device	☐	☐	☐	☐
Other *(please specify)*	☐	☐	☐	☐

6 How does information security inform your organization's strategy and plans? *(Select the answer that best describes your current situation)*

- We have fully considered the information security implications of our current strategy and plans. Our cyber threats, vulnerabilities and risks are included in the risk landscape and monitored. We are satisfied with our assessments, and our strategy and plans are unchanged. ☐
- We have somewhat considered the information security implications of our current strategy and plans. Our cyber threats, vulnerabilities and risks are somewhat included in the risk landscape and monitored, and we are planning a more thorough consideration. In the meantime, our current strategy and plans are unchanged. ☐
- We have somewhat considered the information security implications of our current strategy and plans. Our cyber threats, vulnerabilities and risks are somewhat included in the risk landscape and monitored. We have no plans to expand our consideration of information security risks at this current time. ☐
- We plan to include a consideration of the information security implications of our strategy and plans, when we undertake our next strategy review, and not before. ☐
- Concerns have been growing and we are just about to embark on an unscheduled consideration of the information security implications of our current strategy and plans. Our cyber threats, vulnerabilities and risks will be included in the risk landscape and monitored. ☐
- We recently made a significant change to our organization's strategy and plans as a result of cyber threats, vulnerabilities and risks being identified, which exposed the organization to too much risk. ☐
- We do not believe we have a full enough appreciation of the current information security implications, cyber threats, vulnerabilities and risks, and therefore cannot decide what impact this could have on our strategy and plans. ☐

SECTION 2 Risk

7 What information in your organization do you consider is the most valuable to cyber criminals *(Select the top 5 you consider most valuable for your organization, and rank them from 1 as the most valuable, to 5 as less valuable)*

	Rank
Customer personal, identifiable information	
Customer passwords	
Research and development (R&D) information	
Information exchanged during mergers and acquisition (M&A) activities	
Patented Intellectual Property (IP)	
Non-patented IP	
Senior executive / Board member personal information (inc. email accounts)	
Company financial information	
Supplier / vendor identifiable information	
Supplier / vendor passwords	
Corporate strategic plans	
Don't know	
Other *(please specify)*	

8 Which **threats*** and **vulnerabilities**** have most increased your risk exposure over the last 12 months? *(Rate all of these items, with 1 as the highest priority, down to 5 as your lowest priority)*

	Threats and vulnerabilities Top five
Vulnerability – outdated information security controls or architecture	☐
Vulnerability – careless or unaware employees	☐
Vulnerability – related to cloud computing use	☐
Vulnerability – vulnerabilities related to mobile computing use	☐
Vulnerability – related to social media use	☐
Vulnerability – unauthorized access (e.g., due to location of data)	☐
Threat – cyber attacks to disrupt or deface the organization	☐
Threat – cyber attacks to steal financial information (credit card numbers, bank information, etc.)	☐
Threat – cyber attacks to steal intellectual property or data	☐
Threat – espionage (e.g., by competitors)	☐
Threat – fraud	☐
Threat – internal attacks (e.g., by disgruntled employees)	☐
Threat – malware (e.g., viruses, worms and Trojan horses)	☐
Threat – natural disasters (storms, flooding, etc.)	☐
Threat – phishing	☐
Threat – spam	☐
Threat – zero-day attacks	☐

**Threat is defined as the potential for a hostile action from actors in the external environment*
*** Vulnerability is defined as exposure to the possibility of being attacked or harmed exists*

9 Who or what do you consider the most likely source of an attack? *(Select all that apply)*

- Malicious employee ☐
- Careless employee ☐
- External contractor working on our site ☐
- Customer ☐
- Supplier ☐
- Other business partner ☐
- Criminal syndicates ☐
- State sponsored attacker ☐
- Hacktivists ☐
- Lone Wolf hacker ☐
- Other *(please specify)* ☐

10 How do you ensure that your external partners, vendors or contractors are protecting your organization's information? *(Select all that apply)*

- Accurate inventory of all third-party providers, network connections and data ☐
- Fourth parties (also known as sub-service organizations) are identified and assessments performed (e.g., questionnaires issued, reliance placed on your vendor's assessment processes) ☐
- All third parties are risk-rated and appropriate diligence is applied ☐
- Only critical or high-risk third parties are assessed ☐
- Self-assessments or other certifications performed by partners, vendors or contractors ☐
- Assessments performed by your organization's information security, IT risk, procurement or internal audit function (e.g., questionnaires, site visits, security testing) ☐
- Independent external assessments of partners, vendors or contractors *(e.g., SSAE 16, ISAE-3402)* ☐
- Other *(please specify)* ☐
- *Don't know* ☐

11 What are the main risks associated with the growing use of mobile devices (e.g., laptops, tablets, smartphones) in your organization? *(Select all that apply)*

- The loss of a single smart device not only means the loss of information, but increasingly it also leads to a loss of identity ☐
- Devices do not have the same firmware or software running on them ☐
- Hardware interoperability issues of devices ☐
- Network engineers cannot patch vulnerabilities fast enough ☐
- Organized cyber criminals sell hardware with Trojans or backdoors already installed ☐
- Hijacking of devices ☐
- Poor user awareness / behavior ☐
- Other *(please specify)* ☐

12 What do you consider to be the information security challenges of the Internet of Things (IoT) for your organization? *(Select all that apply)*

- [ ] Keeping the high number of IoT connected devices updated with the latest version of code and security bug free
- [ ] Identifying suspicious traffic over the network
- [ ] Finding hidden or unknown zero-day attacks
- [ ] Ensuring that the implemented security controls are meeting the requirements of today
- [ ] Knowing all your assets
- [ ] Managing the growth in access points to your organization
- [ ] Tracking the access to data in your organization
- [ ] Defining and monitoring the perimeters of your businesses ecosystem
- [ ] Other *(please specify)*
- [ ] Don't know

13 What do you consider to be the main obstacles that need to be overcome to enable the wider adoption of IoT devices in your organization? *(Select all that apply)*

- [ ] Lack of skilled resources
- [ ] Budget constraints
- [ ] Lack of executive awareness or support
- [ ] Management of governance issues
- [ ] Lack of quality controls
- [ ] Privacy concerns of employees
- [ ] Other *(please specify)*

SECTION 3 Technology

14a Which of the following information security areas would you define as "High, Medium or Low priorities" for your organization over the coming 12 months? *(Select one response for each topic)*

	High	Medium	Low
Business continuity / disaster recovery resilience	☐	☐	☐
Cloud computing	☐	☐	☐
Data leakage / data loss prevention	☐	☐	☐
Forensics support	☐	☐	☐
Fraud support	☐	☐	☐
Identity and access management	☐	☐	☐
Incident response capabilities	☐	☐	☐
Information security transformation (fundamental redesign)	☐	☐	☐
Insider risk / threats	☐	☐	☐
Intellectual property (IP)	☐	☐	☐
IT security and operational technology integration	☐	☐	☐
Mobile devices	☐	☐	☐
Offshoring / outsourcing security activities, including third-party supplier risk	☐	☐	☐
Privacy measures	☐	☐	☐
Privileged access management	☐	☐	☐
Robotic process automation	☐	☐	☐
Securing connected devices on the IoT	☐	☐	☐
Securing cryptocurrencies (e.g., Bitcoin)	☐	☐	☐
Securing emerging technologies (e.g., advanced machine learning, ambient user experience, 3D printing materials)	☐	☐	☐
Security architecture redesign	☐	☐	☐
Security awareness and training	☐	☐	☐
Security incident and event management (SIEM) and Security Operations Center (SOC)	☐	☐	☐
Security operations (e.g., antivirus, patching, encryption)	☐	☐	☐
Security testing (e.g., attack and penetration)	☐	☐	☐
Social media	☐	☐	☐
Third-party risk management	☐	☐	☐
Threat and vulnerability management (e.g., security analytics, threat intelligence)	☐	☐	☐
Other *(please specify)*	☐	☐	☐

14b Compared to the previous year, does your organization plan to spend more, less or relatively the same amount over the coming year for the following activities?
(Select one response for each topic)

	Spend more	Spend less	Same or constant
Business continuity / disaster recovery resilience	☐	☐	☐
Cloud computing	☐	☐	☐
Data leakage / data loss prevention	☐	☐	☐
Forensics support	☐	☐	☐
Fraud support	☐	☐	☐
Identity and access management	☐	☐	☐
Incident response capabilities	☐	☐	☐
Information security transformation (fundamental redesign)	☐	☐	☐
Insider risk / threats	☐	☐	☐
Intellectual property (IP)	☐	☐	☐
IT security and operational technology integration	☐	☐	☐
Mobile devices	☐	☐	☐
Offshoring / outsourcing security activities, including third-party supplier risk	☐	☐	☐
Privacy measures	☐	☐	☐
Privileged access management	☐	☐	☐
Robotic process automation	☐	☐	☐
Securing connected devices on the IoT	☐	☐	☐
Securing cryptocurrencies (e.g., Bitcoin)	☐	☐	☐
Securing emerging technologies (e.g., advanced machine learning, ambient user experience, 3D printing materials)	☐	☐	☐
Security architecture redesign	☐	☐	☐
Security awareness and training	☐	☐	☐
Security incident and event management (SIEM) and Security Operations Center (SOC)	☐	☐	☐
Security operations (e.g., antivirus, patching, encryption)	☐	☐	☐
Security testing (e.g., attack and penetration)	☐	☐	☐
Social media	☐	☐	☐
Third-party risk management	☐	☐	☐
Threat and vulnerability management (e.g., security analytics, threat intelligence)	☐	☐	☐
Other *(please specify)*	☐	☐	☐

15 What Information Security functions are you outsourcing? *(Select all that apply)*

- Security monitoring ☐
- Vulnerability assessment ☐
- Self-phishing ☐
- Vendor risk management ☐
- IT security helpdesk ☐
- One time exercises (e.g., setting up ISMS) ☐
- Consultancy specific information security activities ☐
- Other *(please specify)* ☐

16 Please rate the following information security management processes in your organization in terms of maturity *(Select on a scale of 1 to 5, where 1 is non-existent and 5 is very mature)*. **Refer to 'Appendix' for details**

	Non-existent 1	2	3	4	Very mature 5
Architecture	☐	☐	☐	☐	☐
Asset management	☐	☐	☐	☐	☐
Awareness	☐	☐	☐	☐	☐
BCP / DR	☐	☐	☐	☐	☐
Data infrastructure	☐	☐	☐	☐	☐
Data protection	☐	☐	☐	☐	☐
Governance and organization	☐	☐	☐	☐	☐
Host security	☐	☐	☐	☐	☐
Identity and access management	☐	☐	☐	☐	☐
Incident management	☐	☐	☐	☐	☐
Metrics and reporting	☐	☐	☐	☐	☐
Network security	☐	☐	☐	☐	☐
Operations	☐	☐	☐	☐	☐
Policy and standards framework	☐	☐	☐	☐	☐
Privacy	☐	☐	☐	☐	☐
Security monitoring	☐	☐	☐	☐	☐
Software security	☐	☐	☐	☐	☐
Strategy	☐	☐	☐	☐	☐
Third-party management	☐	☐	☐	☐	☐
Threat and vulnerability management	☐	☐	☐	☐	☐
Other *(please specify)*	☐	☐	☐	☐	☐

17 What functions of your Security Operations Center (SOC) are outsourced? *(Select all that apply)*
(If your organization does not have a Security Operations Center (SOC) , please skip to Q19)

- [ ] We do not have a SOC
- [ ] Real time network security monitoring
- [ ] Incident investigation
- [ ] Digital / malware forensics
- [ ] Threat intelligence collection / feeds
- [ ] Threat intelligence analysis
- [ ] Cybersecurity exercise creation and delivery
- [ ] Vulnerability scanning and management
- [ ] Penetration testing
- [ ] We fulfill all functions in-house
- [ ] Other *(please specify)*
- [ ] Don't know

18 How does your SOC keep up to date with the latest threats? *(Select all that apply)*

- [ ] Our SOC collaborates and shares data with other public SOCs
- [ ] Our SOC collaborates and shares data with others in our industry
- [ ] Our SOC has analysts that read and subscribe to specific open source resources
- [ ] Our SOC has a paid subscription to cyber threat intelligence feeds
- [ ] Our SOC has dedicated individual(s) focusing solely on cyber threat intelligence
- [ ] None of the above
- [ ] Don't know

19 Thinking about the most recent significant cybersecurity incident, how was it discovered? *(Select one)*

- [ ] We have not had a significant incident
- [ ] Discovered by the SOC
- [ ] Discovered internally by a business function
- [ ] Discovered externally by a third-party
- [ ] Other *(please specify)*

20 Which statement best describes the maturity of your **threat intelligence** program? *(Select one)*

- We do not have a threat intelligence program ☐
- We have an informal threat intelligence program that incorporates information from trusted third parties and email distribution lists ☐
- We have a formal threat intelligence program that includes subscription threat feeds from external providers and internal sources, such as a security incident and event management tool ☐
- We have a threat intelligence team that collects internal and external threat and vulnerability feeds to analyze for credibility and relevance in our environment ☐
- We have an advanced threat intelligence function with internal and external feeds, dedicated intelligence analysts and external advisors that evaluate information for credibility, relevance and exposure against threat actors ☐

21 Which statement best describes the maturity of your **vulnerability identification** capability? *(Select one)*

- We do not have a vulnerability identification program ☐
- We have an informal vulnerability identification program and perform automated testing on a regular basis ☐
- We use a variety of review approaches, including social engineering and manual testing ☐
- We have a formal vulnerability intelligence function with a program of assessments based on business threats utilizing deep dive attack and penetration testing of suppliers, periodical testing of business processes, and project testing, (e.g., new systems) ☐
- We have an advanced vulnerability intelligence function and conduct risk-based assessments with results and remediation agreed with the risk function throughout the year ☐

22 Which statement best describes the maturity of your **breach detection** program? *(Select one)*

- We do not have a detection program ☐
- We have perimeter network security devices (i.e., IDS) ☐
- We do not have formal processes in place for response and escalation ☐
- We utilize a security information and event management (SIEM) solution to actively monitor network, IDS / IPS and system logs ☐
- We have an informal response and escalation processes in place ☐
- We have a formal detection program that leverages modern technologies (host-based and network-based malware detection, behavioral anomaly detection, etc.) to monitor both internal and external traffic ☐
- We use ad hoc processes for threat collection, integration, response and escalation ☐
- We have a formal and advanced detection function that brings together each category of modern technology (host-based malware detection, antivirus, network-based malware detection, DLP, IDS, next-gen firewalls, log aggregation) and use sophisticated data analytics to identify anomalies, trends and correlations ☐
- We have formal processes for threat collection, dissemination, integration, response, escalation and prediction of attacks ☐

23 Which statement best describes the maturity of your **incident response** capability? *(Select one)*

- [ ] We do not have an incident response capability
- [ ] We have an incident response plan through which we can recover from malware and employee misbehavior. Further investigations into root causes are not conducted.
- [ ] We have a formal incident response program and conduct investigations following an incident
- [ ] We have a formal incident response program and established arrangements with external vendors for more complete identity response services and investigations
- [ ] We have a robust incident response program that includes third parties and law enforcement and is integrated with our broader threat and vulnerability management function. We build playbooks for potential incidents and test those playbooks via table-top exercises regularly.

24 Which statement best describes the maturity of your **data protection** program? *(Select one)*

- [ ] We do not have a data protection program
- [ ] Data protection policies and procedures are informal or ad-hoc policies are in place
- [ ] Data protection policies and procedures are defined at the business unit level
- [ ] Data protection policies and procedures are defined at the group level
- [ ] Data protection policies and procedures are defined at the group level with corporate oversight and communicated through the business, with specific business unit exceptions documented, tracked and annually reviewed

25 Which statement best describes the maturity of your **identity and access management** program? *(Select one)*

- [ ] We do not have an identity and access management program
- [ ] A team with oversight of access management processes and central repository conducts reviews yet not formally established
- [ ] A formal team provides oversight on defined access management processes although largely manual; a central directory is in place yet interacts with a limited number of applications and not regularly reviewed
- [ ] A formal team interacts with business units in gaining oversight with well-defined processes, limited automated workflows, single source sign-on on for most applications and regular reviews

26 Which statement best describes the maturity of your **robotic process automation capability**? *(Select one)*

- [ ] We do not have a robotic process automation capability
- [ ] We have a robotic process automation capability, but do not yet have a governance process in place
- [ ] We have a robotic process automation capability with a governance process outside of IT
- [ ] We have a robotic process automation capability that sits within IT governance
- [ ] We have a robotic process automation capability that sits within IT governance and the robot is specifically protected against hacking
- [ ] We have a robotic process automation capability that sits within IT governance; the robot is specifically protected against hacking and the robot is able to change the rules definition

27 Do you consider that the security of blockchains offers a realistic choice of payment method for your organization? *(Select one)*

- [ ] Not at all aware of blockchains and their function
- [ ] Have some awareness of blockchains, but not enough knowledge to properly evaluate
- [ ] Blockchains have potential, but will not consider it for at least another year
- [ ] We are actively considering blockchains, but have no plans to implement yet
- [ ] We are actively considering blockchains and are developing plans to implement within the next 2 years
- [ ] Do not believe in the security of blockchains
- [ ] Other *(please specify)*

SECTION 4 People and organization

28 How does your Information Security function interface outside of IT? *(Select all that apply)*

- Directly reports outside of IT ☐
- Places dedicated business line security officers in key lines of business ☐
- Provides ad hoc reports on request to the Board / audit committee level stakeholders ☐
- Sometimes produces scheduled reports (2-6x/year) to Board / audit committee level stakeholders ☐
- Regularly produces scheduled reports (>6x/year) to Board / audit committee level stakeholders ☐
- Specifically identifies non-IT "crown jewels" and differentially protects those information assets ☐
- None of the above ☐
- Other *(please specify)* ☐

29 If, in your role, you receive reports on your organization's information security, how effective are they? *(Select all that apply)*

- I do not receive reports on the organization's information security ☐
- The reports provide metrics on the number of cyber attacks made on the organization ☐
- The reports provide metrics on the number of cyber attacks successfully defended against ☐
- The reports provide information on every attack where a breach occurred ☐
- The reports evaluate the financial impact of every significant breach ☐
- The reports evaluate whether a regulator needs to be notified of a particular breach ☐
- The reports identify areas where improvement is needed ☐
- The reports provide an overall threat level for the organization ☐
- The reports I receive are very informative and inspire confidence ☐
- The reports I receive are not informative enough and do not fully inspire confidence ☐
- None of the above ☐
- Other *(please specify)* ☐

30 How knowledgeable do you feel the whole Board is on the topic of information security? *(Select the response that most closely describes the current situation)*

- The Board has sufficient knowledge of information security to fully evaluate the effectiveness of the risks the organization is facing and the measures the organization is taking ☐
- The Board does not have sufficient knowledge of information security to fully evaluate the effectiveness of the risks the organization is facing and the measures the organization is taking ☐
- The Board does not have sufficient knowledge of information security to fully evaluate the effectiveness of the risks the organization is facing and the measures the organization is taking. They are taking positive steps to improve their understanding. ☐
- The Board does not have sufficient knowledge of information security to fully evaluate the effectiveness of the risks the organization is facing and the measures the organization is taking. This has resulted in incorrect decision-making. ☐
- Don't know ☐
- Other *(please specify)* ☐

31a Who is directly responsible for information security? *(Select one)*

The CIO / Head of IT is directly responsible	☐ Go to Q31b
The CISO / IT Risk / Network Security Officer is directly responsible	☐ Go to Q31b
Information security is the direct responsibility of another role *(please specify role)*	☐ Go to Q31b
We do not have anyone who is directly responsible	☐ Go to Q32
Direct responsibility for our information security lies outside of our organization	☐ Go to Q32

31b What is their position in relation to the Board?

Is on the Board of our organization	☐
Is not on the Board of our organization	☐

32 In your opinion, what is the likelihood of your organization being able to detect a sophisticated cyber attack? *(Select one)*

We have not had a significant incident	☐
Very Likely **(80-100% likelihood)**	☐
Likely **(50-80% likelihood)**	☐
Unlikely **(20-50% likelihood)**	☐
Highly unlikely **(0-20% likelihood)**	☐

33 How would you characterize the extent to which the Information Security function is meeting the needs of your organization? *(Select one)*

Fully meets the organizational needs	☐
Partially meets the organizational needs and improvement is underway	☐
Partially meets the organizational needs and there are no agreed plans for improvement	☐
It does not meet the organizational needs but improvement is underway	☐
It does not meet the organizational needs and there are no agreed plans for improvement	☐

34 What are the main obstacles or reasons that challenge your Information Security operation's contribution and value to the organization? *(Select all that apply)*

- Lack of skilled resources ☐
- Budget constraints ☐
- Lack of executive awareness or support ☐
- Management and governance issues ☐
- Lack of quality tools for managing information security ☐
- Fragmentation of compliance / regulation ☐
- Other *(please specify)* ☐

35a Does your organization have an agreed-upon communications strategy or plan in place in the event of a significant cyber attack taking place and data being compromised?

- Yes ☐ Go to Q35b
- No ☐ Go to Q36

35b Considering the following scenarios, at what point in time would your organization be most likely to communicate that a significant cyber attack has taken place and that data in your organization has definitely been compromised? *(Select a response for each statement)*

	On day1	Within the first week while investigations continue	Within the first month while investigations continue	Only after all investigations are complete and the issue is closed	Never	Don't know
Notify regulators / compliance organizations	☐	☐	☐	☐	☐	☐
If customer information affected, notify all customers	☐	☐	☐	☐	☐	☐
If no customer information affected, notify all customers anyway	☐	☐	☐	☐	☐	☐
Individually notify only those customers impacted	☐	☐	☐	☐	☐	☐
Issue a press release / public statement to the media	☐	☐	☐	☐	☐	☐
If supplier information affected, notify all suppliers	☐	☐	☐	☐	☐	☐
If no supplier information affected, notify all suppliers anyway	☐	☐	☐	☐	☐	☐
Individually notify only those suppliers impacted	☐	☐	☐	☐	☐	☐
Other *(please specify)*	☐	☐	☐	☐	☐	☐

36 What was the primary control or process failure that lead to your most significant cyber breach(es) in the last year? *(Select one)*

- ☐ Lack of multi-factor authentication for remote users
- ☐ Poorly secured internet-facing systems and / or applications
- ☐ End user awareness, exploited via phishing
- ☐ Lack of network segmentation to prevent attacker moving from internet to "crown jewel"
- ☐ Lack of security leadership (e.g., no CISO)
- ☐ Outdated / unpatched systems
- ☐ Inability to identify/contain breaches before they increased in significance
- ☐ Other *(please specify)*
- ☐ Don't know

37 What benchmarking information is most useful? *(Rank from 1 to 5, with 1 being most important).*

- ☐ Information security maturity of peer organizations by sector
- ☐ Effectiveness of a given technology class (e.g., DLP, end-point protection, perimeter detection, SOC/SIEM)
- ☐ Internal reporting structure for the information security function
- ☐ Funding amount and allocation across security function
- ☐ Effectiveness of threat intelligence sources
- ☐ None of the above
- ☐ Not interested in peer comparisons or benchmarking
- ☐ Other *(please specify)*

38 Do you have a role or department in your Information Security function focusing on the following technologies and their impact on your organization's information security? *(Select a response for each topic)*

	Yes	No, but planning to implement	No	Don't know	Technology is not applicable
IoT connected devices	☐	☐	☐	☐	☐
Blockchains and cryptocurrencies	☐	☐	☐	☐	☐
Robotic process automation	☐	☐	☐	☐	☐
Advanced machine learning / artificial intelligence	☐	☐	☐	☐	☐

SECTION 5

Finance and legal

39 What is your estimate of the total financial damage related to information security incidents over the past year (this includes loss of productivity, regulatory fines, etc.; the estimate excludes costs or missed revenue due to brand damage)? *(Select one)*

- Between US$0 and US$100,000 ☐
- Between US$100,000 and US$250,000 ☐
- Between US$250,000 and US$500,000 ☐
- Between US$500,000 and US$1 million ☐
- Between US$1 million and US$2.5 million ☐
- Above US$2.5 million ☐
- Had no information security incidents that resulted in any financial damage ☐
- Don't know ☐

40 What is your current level of interest in cyber insurance? *(Select one)*

- We currently have cyber insurance that meets our organization's needs ☐
- We currently have cyber insurance, but it does not meet our organization's needs ☐
- We do not have cyber insurance and are actively looking for appropriate cover ☐
- We do not have cyber insurance and we have no plans to adopt it ☐
- We have never considered cyber insurance ☐
- Other *(please specify)* ☐

Thank you for your participation!

Appendix (for Q.16)

Domain	Areas in scope for domain
Architecture	This domain reconciles business requirements with solutions, including component selection and implementation, to provide a coherent framework for identifying security needs in an organization, and putting systems and processes in place to meet those needs. In a mature organization, the architecture function is used to manage the information security solutions and technologies that promote interoperability and manageability while meeting the organization's risk management needs. The architecture may include a core set of design principles that support the information security program goals. The technology components of architecture typically include network, host, application and data. Architecture processes in an organization include governance and standards functions.
Asset management	IT asset management (ITM) encompasses the infrastructure and processes necessary for the effective management, control and protection of the hardware and software assets within an organization, throughout all stages of their lifecycle.
Awareness	The scope for a security awareness program consists of all staff within an organization, including self-employed staff, contractors and third party service providers. Special attention is given to employees with security responsibilities as for example developers, service desk personnel, control room personnel, physical security guards, receptionists, information security and IT security staff, and management. Security awareness is typically a program with a long-term shift and direction following a wave-pattern: on a regular basis new trainings and campaigns are launched, as people typically require repetition to learn. It is important to protect information throughout its lifecycle: creation, distribution, storage, usage, and destruction should receive equal attention.
BCP/DR	This domain covers business continuity and disaster recovery concepts such as senior management support for BCM, adequate skilled resources, process definition, business impact analysis, testing of plans, and metrics reporting.
Data infrastructure	Data repositories, warehouses, and systems to support a classic business intelligence function within security operations.
Data protection	EY takes a holistic view of data security. While data governance and management are foundational elements, the business is the driver for these elements. Security's focus is on protecting and a major component of this view relates to DLP with the program's goal to effectively manage data loss risks. Data includes, for example, intellectual property, customer data, transaction data, privacy data as well as client specific sensitive data. DLP is concerned with data throughout the data lifecycle; Data at Rest, Data in Motion and Data in Use. DLP requires an understanding of what data you have, the value of that data, your obligations to protect that data, where the data resides, who access the data, where the data is going, how you protect the data, the gaps and risks in your current protection and how you respond to data leaks.
Governance and organization	This domain covers the information security program governance structure (including defined roles and responsibilities), business alignment, executive engagement and support, and monitoring and oversight of the information security function.

continues

Appendix (For Q.16) *(continued)*

Domain	Areas in scope for Domain
Host security	This domain covers the protection mechanisms and controls in place at the host level. Topics in scope for this section are: – Anti-virus – Full disk encryption – Malware protection – Hardware access control – Patch management
Identity and access management	Identity and access management (IAM) can be described by defining its core components, identity management and access management. **Identity management** refers to the processes associated with managing the entire lifecycle of digital identities and profiles for people, processes, and technology. It typically includes: – Establishing unique identities and associated authentication credentials – Provisioning new user accounts – Managing identity data and credentials (e.g., self-service password reset) – Creating workflow processes for approving account creation and modification – Providing the ability to modify, suspend, or remove accounts – Auditing and reporting of user identity information. **Access management** refers to the processes used to control who has access to specific information assets, including: – Providing the capability to request specific entitlements and/or roles – Implementing workflow processes for approving the granting of entitlements and/or roles to a user – Providing the ability to modify or remove the entitlements and/or roles assigned to a user – Managing the association of entitlements to roles – Associating entitlements and roles to job functions – Providing the ability to review, remove, approve, and certify the entitlements and / or roles assigned to users – Providing the ability to review and audit historical access – Identifying, reporting and preventing inappropriate combinations of access.
Incident management	Incident management is defined as the formal function for reporting and responding to incidents that may adversely impact the organization's assets, operations, reputation, financial position, intellectual capital, or confidential information. It serves as a critical component of an organization's overall information security structure, and provides a foundation for identifying and responding to incidents in a consistent and well-organized manner.
Metrics and reporting	The metrics and reporting domain encompasses any defined, repeatable measurement activity that aids the organization in understanding the various components within their information security program, and how the program supports the business strategy. The domain includes analyzing the information security goals set by the business, and defining repeatable methods of measurement to show effectiveness, or progress in meeting those desired goals. Dependent domain(s): All domains within the framework could have inputs into the metrics and reporting domain. A mature metrics program will inherently measure and report on strategic goals, but the inclusion of "Services" domains into the metrics program will depend on applicability to the organization.

continues

Appendix (for Q.16) *(continued)*

Domain	Areas in scope for domain
Network security	The network security domain captures the policies, processes, tools, and technologies that are used to maintain security at the network level, and includes access management (e.g., network devices, remote access, access to logs, third-party access), vulnerability management, incident identification and notification, device configuration and patch management, and network architecture, including wireless networks. Although there is an overlap, we have attempted to not include topics related to host security, non-network architecture, security monitoring, and threat and vulnerability management.
Operations	The Operations scope for the SPM framework is: 1. Change management 2. Configuration management 3. Communications and operations management 4. Backup 5. Physical and environment security 6. System planning and acceptance 7. Operations access control
Policy and standards framework	This domain encompasses the formal development, documentation, review, and approval of the information security policies, standards, and guidelines that defines the information security requirements, processes and controls to be implemented for protection of an organization's information and IT assets. This domain also includes periodic review of PSGs, lifecycle management processes, IT and business stakeholder engagement, and compliance monitoring for PSGs.
Privacy	In today's digital world, personal identifiable information is being gathered on a vast scale and organizations need to focus on abiding by the ever growing weight of regulation, as well as find more and more secure ways of keeping this information safe from cyber attackers.
Security monitoring	The capabilities to successfully capture and monitor logs from network devices, hosts, files, databases, and privileged user access so as to identify or be alerted of events that require further investigation due to the potential of being security events that may need to trigger the incident response process.
Software security	Software security focuses on the development of software and information security's role in that. This covers both internal and external software development and SDLC process and controls. However, the process of identifying and managing vulnerabilities is managed through threat and vulnerability (TVM) management.
Strategy	Strategy focuses primarily on the information security related goals for the organization, as well as how these have been defined and communicated, and how often they are reviewed. A key element of this is alignment to organizational objectives to ensure strategic priorities are met. Strategy is also inclusive of high level planning for information security, including budget.
Third-party management	The process for managing third-parties, and the transfer and exchange to, or storage of information/data by the third-parties. This domain includes, contract requirements and obligations with third-parties, monitoring processes, and compliance/audit checks for third-parties.
Threat and vulnerability management	Threat and vulnerability management (TVM) is the programmatic approach for an organization to predict threats, identify and remediate vulnerabilities, detect and respond to attacks, and strategically develop counter measures. Functionally TVM should include APT, threat intelligence, vulnerability identification, remediation, detection, response, and countermeasure planning.

If you were under cyber attack, would you ever know?

As many organizations have learned, sometimes the hard way, cyber attacks are no longer a matter of if, but when. Hackers are increasingly relentless. When one tactic fails, they will try another until they breach an organization's defenses. At the same time, technology is increasing an organization's vulnerability to attack through increased online presence, broader use of social media, mass adoption of mobile devices, increased usage of cloud services, and the collection and analysis of big data. Our ecosystems of digitally connected entities, people and data increase the likelihood of exposure to cybercrime in both the work and home environment. Even traditionally closed operational technology systems are now being given IP addresses, enabling cyber threats to make their way out of backoffice systems and into critical infrastructures such as power generation and transportation systems.

Anticipating cyber attacks is the only way to be ahead of cyber criminals. With our focus on you, we ask better questions about your operations, priorities and vulnerabilities. We then collaborate with you to create innovative answers that help you activate, adapt and anticipate cybercrime. Together, we help you design better outcomes and realize long-lasting results, from strategy to execution.

We believe that when organizations manage cybersecurity better, the world works better.

So, if you were under cyber attack, would you ever know? Ask EY.

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

ey.com/cybersecurity

About EY's Advisory Services

In a world of unprecedented change, EY Advisory believes a better working world means helping clients solve big, complex industry issues and capitalize on opportunities to grow, optimize and protect their businesses.

Through a collaborative, industry-focused approach, EY Advisory combines a wealth of consulting capabilities – strategy, customer, finance, IT, supply chain, people advisory, program management and risk – with a complete understanding of a client's most complex issues and opportunities, such as digital disruption, innovation, analytics, cybersecurity, risk and transformation. EY Advisory's high-performance teams also draw on the breadth of EY's Assurance, Tax and Transaction Advisory service professionals, as well as the organization's industry centers of excellence, to help clients realize sustainable results.

True to EY's 150-year heritage in finance and risk, EY Advisory thinks about risk management when working on performance improvement, and performance improvement is top of mind when providing risk management services. EY Advisory also infuses analytics, cybersecurity and digital perspectives into every service offering.

EY Advisory's global connectivity, diversity and collaborative culture inspires its consultants to ask better questions. EY consultants develop trusted relationships with clients across the C-suite, functions and business unit leadership levels, from Fortune 100 multinationals to leading disruptive innovators. Together, EY works with clients to create innovative answers that help their businesses work better.

The better the question. The better the answer. The better the world works.

Our Risk Advisory Leaders are:

EY Global Risk Leader		
Paul van Kessel	+31 88 40 71271	paul.van.kessel@nl.ey.com
EY Area Risk Leaders		
Americas		
Amy Brachio	+1 612 371 8537	amy.brachio@ey.com
EMEIA		
Jonathan Blackmore	+971 4 312 9921	jonathan.blackmore@ae.ey.com
Asia-Pacific		
Iain Burnet	+61 8 9429 2486	iain.burnet@au.ey.com
Japan		
Yoshihiro Azuma	+81 3 3503 1100	azuma-yshhr@shinnihon.or.jp

Our Cybersecurity Leaders are:

EY Global Cybersecurity Leader		
Ken Allan	+44 20 795 15769	kallan@uk.ey.com
EY Area Cybersecurity Leaders		
Americas		
Bob Sydow	+1 513 612 1591	bob.sydow@ey.com
EMEIA		
Scott Gelber	+44 207 951 6930	sgelber@uk.ey.com
Asia-Pacific		
Paul O'Rourke	+65 8691 8635	paul.o'rourke@sg.ey.com
Japan		
Shinichiro Nagao	+81 3 3503 1100	nagao-shnchr@shinnihon.or.jp