Is cybersecurity about more than protection?

Global Information Security Survey
2018-19 results
Internal use only
## Contents

<table>
<thead>
<tr>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
</tr>
<tr>
<td>Demographics</td>
</tr>
<tr>
<td>Section 1: Strategy, innovation and growth</td>
</tr>
<tr>
<td>Section 2: Risk</td>
</tr>
<tr>
<td>Section 3: Technology</td>
</tr>
<tr>
<td>Section 4: People and organization</td>
</tr>
<tr>
<td>Section 5: Finance and legal</td>
</tr>
</tbody>
</table>
EY Global Information Security Survey 2018–19

- The 21st annual edition of EY Global Information Security Survey captures the responses of over 1,400 C-suite leaders and senior information security and IT executives/managers, representing many of the world’s largest and most recognized global organizations.
- The research was conducted between April-July 2018.
- Responses were collected from over 60 countries representing all industry sectors.
Demographics
Respondents by sector

- Automotive & Transportation: 8%
- Banking & Capital Markets: 18%
- Consumer Products & Retail: 19%
- Government & Public Sector: 9%
- Health: 3%
- Insurance: 6%
- Life Sciences: 2%
- Media & Entertainment: 4%
- Mining & Metals: 2%
- Oil & Gas: 3%
- Power & Utilities: 5%
- Professional Firms & Services: 3%
- Real Estate Hospitality & Construction: 4%
- Technology: 8%
- Telecommunications: 4%
- Wealth & Asset Management: 2%
Respondents by EY industry cluster

- Consumer and Mobility: 32%
- Energy: 10%
- Financial Services: 27%
- Government and Public Services and Health: 14%
- TMT: 16%
Respondents by revenue (from the last 12 months in US$)

- Less than $10 million: 19%
- $10 million to $100 million: 21%
- $100 million to $1 billion: 25%
- $1 billion to $10 billion: 24%
- $10 billion or more: 11%
Respondents by company size (based on number of employees)

- Less than 500: 29%
- 501-1000: 12%
- 1001-5000: 28%
- 5001-10000: 10%
- 10001-15000: 5%
- 15001-20000: 3%
- 20001-25000: 2%
- More than 25000: 11%
Respondents by rank

- CISO: 32%
- CIO/IT Director: 27%
- C-suite: 4%
- Internal audit director: 1%
- CRO: 1%
- Global Head of Cybersecurity Governance, Risk & Compliance: 0%
- Other: 35%
Respondents by country

- United States: 16%
- India: 14%
- Brazil: 6%
- China: 6%
- Japan: 4%
- Switzerland: 4%
- Philippines: 4%
- Canada: 3%
- Italy: 3%
- France: 2%
- United Kingdom: 2%
- Oman: 2%
- Colombia: 2%
- Hong Kong: 2%
- Netherlands: 1%
- Sweden: 1%
- South Korea: 1%
- Austria: 1%
- Norway: 1%
- Kuwait: 1%
- Russia: 1%
- Others: 19%
What is your total annual spend on information security (in US$)?

- Nothing: 7%
- Less than or equal to US$100,000: 25%
- Between US$100,000 and US$1 million: 32%
- Between US$1 million and US$10 million: 24%
- Between US$10 million and US$50 million: 7%
- More than US$50 million: 5%
In percentage terms, what is your total spend on information security in relation to your overall IT budget?

- Less than 2%: 22%
- 2-5%: 32%
- 5-10%: 24%
- 10-15%: 9%
- 15-20%: 7%
- More than 20%: 6%
How has your organization's total information security budget changed in the last 12 months?

- Increased by more than 25%: 12%
- Increased between 15% and 25%: 16%
- Increased between 5% and 15%: 25%
- Stayed approximately the same (between +5% and -5%): 40%
- Decreased between 5% and 15%: 4%
- Decreased between 15% and 25%: 1%
- Decreased by more than 25%: 1%
What change to your organization's total information security budget do you expect to see in the next 12 months?

- Will increase by more than 25%: 15%
- Will increase between 15% and 25%: 22%
- Will increase between 5% and 15%: 28%
- Will stay approximately the same (between +5% and 5%): 31%
- Will decrease between 5% and 15%: 2%
- Will decrease between 15% and 25%: 1%
- Will decrease by more than 25%: 1%
How much additional funding is needed to protect the organization? (Select one)

- None: 13%
- Less than 25%: 46%
- 26-50%: 23%
- 51-75%: 6%
- 76-100%: 7%
- Over 100%: 4%
In percentage terms, how many full time employees work solely in cybersecurity, in comparison to the total number of employees in your organization’s IT department?

- Less than 2%: 39%
- 2%–5%: 34%
- 5%–10%: 17%
- 10%–15%: 5%
- 15%–20%: 3%
- More than 20%: 2%
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?

<table>
<thead>
<tr>
<th>Event</th>
<th>Highly unlikely</th>
<th>Unlikely</th>
<th>Likely</th>
<th>Highly likely</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discovery of a breach with, apparently, no harm done.</td>
<td>21%</td>
<td>42%</td>
<td>29%</td>
<td>7%</td>
</tr>
<tr>
<td>Discovery of a breach that resulted in the attackers impacting the organization.</td>
<td>5%</td>
<td>19%</td>
<td>39%</td>
<td>37%</td>
</tr>
<tr>
<td>A Distributed Denial of Service (DDoS) attack.</td>
<td>13%</td>
<td>35%</td>
<td>32%</td>
<td>20%</td>
</tr>
<tr>
<td>A cyber attack on a major competitor.</td>
<td>15%</td>
<td>42%</td>
<td>36%</td>
<td>7%</td>
</tr>
<tr>
<td>A cyber attack on a supplier.</td>
<td>17%</td>
<td>52%</td>
<td>26%</td>
<td>5%</td>
</tr>
<tr>
<td>M&amp;A activity.</td>
<td>25%</td>
<td>43%</td>
<td>26%</td>
<td>6%</td>
</tr>
<tr>
<td>A physical loss of confidential corporate information on a mobile device.</td>
<td>19%</td>
<td>34%</td>
<td>36%</td>
<td>12%</td>
</tr>
<tr>
<td>A physical loss of customer information on a mobile device.</td>
<td>17%</td>
<td>35%</td>
<td>33%</td>
<td>15%</td>
</tr>
</tbody>
</table>

Strategy, innovation and growth

Question: 7
How does information security influence your business strategy and plans?

- Fully and on a regular basis: 18%
- Fully and on a yearly basis: 28%
- Not at all: 7%
- Somewhat: 48%
Section: 2

Risk
What information in your organization is the most valuable to cyber criminals?

- Customers' personal, identifiable information: 17%
- Customers' passwords: 11%
- Research and development (R&D) information: 9%
- Information exchanged during mergers and acquisition (M&A) activities: 8%
- Patented Intellectual Property (IP): 6%
- Non-patented IP: 5%
- Senior executive and board member personal information (including email accounts): 11%
- Financial information of the organization: 12%
- Supplier and vendor identifiable information: 5%
- Supplier and vendor passwords: 3%
- Corporate strategic plans: 12%
Which threats have most increased your risk exposure over the last 12 months?

- Cyber attacks to disrupt or deface the organization: 13%
- Cyber attacks to steal financial information (credit card numbers, bank information, etc.): 12%
- Cyber attacks to steal intellectual property or data: 8%
- Espionage (e.g., by competitors): 2%
- Fraud: 10%
- Internal attacks (e.g., by disgruntled employees): 5%
- Malware (e.g., viruses, worms and Trojan horses): 20%
- Natural disasters (storms, flooding, etc.): 2%
- Phishing: 22%
- Spam: 6%
Which vulnerabilities have most increased your risk exposure over the last 12 months?

- Outdated information security controls or architecture: 26%
- Careless or unaware employees: 34%
- Related to cloud-computing use: 10%
- Related to smartphones, tablets, etc.: 8%
- Related to Internet of Things: 4%
- Related to social media use: 5%
- Unauthorized access (e.g., due to location of data): 13%
Who do you consider to be the most likely source of a cyber attack?

- Malicious employee: 14%
- Careless employee: 22%
- External contractor working on our site: 8%
- Customer: 2%
- Supplier: 5%
- Other business partner: 3%
- Criminal syndicates: 15%
- State sponsored attacker: 8%
- Hacktivists: 12%
- Lone Wolf hacker: 9%
- Other: 1%
How do you ensure that your external partners, vendors, or contractors are protecting your organization's information?

- Accurate inventories of all third party providers, network connections and data are kept: 17%
- All third parties are risk-rated and appropriate diligence is applied: 15%
- Only critical or high-risk third parties are assessed: 12%
- Self-assessments or other certifications are performed by partners, vendors or contractors: 18%
- Assessments are performed by your organization's information security, IT risk, procurement or internal audit function (e.g., questionnaires, site visits, security testing): 22%
- Independent external assessments of partners, vendors or contractors (e.g., SSAE 16, ISAE-3402) are performed: 14%
- Other: 3%
Which risks related to smartphones and tablets apply to your organization?

- The loss of a smart device: 27%
- Devices do not have the same software running on them: 10%
- Hardware interoperability issues of devices: 5%
- Network engineers cannot patch vulnerabilities fast enough: 10%
- Organized cyber criminals sell hardware with Trojans or backdoors already installed: 6%
- Hijacking of devices: 11%
- Poor user awareness and behavior: 29%
- Other: 3%
Which challenges, related to Internet of Things (IoT) apply to your organization?

- Keeping the high number of IoT connected devices updated with the latest version of software: 11%
- Identifying suspicious traffic over the network: 12%
- Finding hidden or unknown zero-day attacks: 10%
- Ensuring that the implemented security controls are meeting the requirements of today: 11%
- Knowing all your assets: 14%
- Managing the growth in access points to your organization: 8%
- Tracking the access to data in your organization: 9%
- Defining and monitoring the perimeters of your business's ecosystem: 7%
- Lack of skilled resources: 10%
- Lack of executive awareness or support: 5%
- Other: 4%
Section: 3

Technology
Which of the following technologies would you define as high, medium or low for your cybersecurity this year?
Compared with last year, are you spending more, less or relatively the same amount on protecting those technologies this year?

<table>
<thead>
<tr>
<th>Technology</th>
<th>Less</th>
<th>Same</th>
<th>More</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud computing</td>
<td>6%</td>
<td>37%</td>
<td>57%</td>
</tr>
<tr>
<td>Mobile computing</td>
<td>7%</td>
<td>58%</td>
<td>35%</td>
</tr>
<tr>
<td>Artificial intelligence</td>
<td>11%</td>
<td>63%</td>
<td>26%</td>
</tr>
<tr>
<td>Robotic process automation</td>
<td>11%</td>
<td>58%</td>
<td>31%</td>
</tr>
<tr>
<td>Machine learning</td>
<td>11%</td>
<td>61%</td>
<td>27%</td>
</tr>
<tr>
<td>Cybersecurity analytics</td>
<td>5%</td>
<td>43%</td>
<td>52%</td>
</tr>
<tr>
<td>Blockchain</td>
<td>15%</td>
<td>69%</td>
<td>15%</td>
</tr>
<tr>
<td>Biometrics</td>
<td>13%</td>
<td>72%</td>
<td>15%</td>
</tr>
<tr>
<td>Internet of Things</td>
<td>9%</td>
<td>61%</td>
<td>29%</td>
</tr>
</tbody>
</table>
Which of the following security functions are you performing in-house or are you outsourcing?

- Security monitoring
  - Outsourced: 35%
  - In-house: 65%

- Vulnerability assessment
  - Outsourced: 48%
  - In-house: 52%

- Self-phishing
  - Outsourced: 39%
  - In-house: 61%

- Vendor risk management
  - Outsourced: 16%
  - In-house: 84%

- Identity and access management
  - Outsourced: 13%
  - In-house: 87%

- Data protection/DLP
  - Outsourced: 18%
  - In-house: 82%

- One-time exercises (e.g., setting up ISMS)
  - Outsourced: 39%
  - In-house: 61%

- Consultancy-specific information security activities
  - Outsourced: 29%
  - In-house: 71%
How would you rate the following information security management processes in your organization in terms of maturity?
Does your company have a Security Operations Center (SOC), whether in-house, outsourced, or a combination of both?

- Yes: 49%
- No: 51%
What functions of your security operations center are outsourced?

- Real-time network security monitoring: 48% outsourced, 52% in-house
- Incident investigation: 48% outsourced, 52% in-house
- Digital and malware forensics: 51% outsourced, 49% in-house
- Threat intelligence collection and feeds: 54% outsourced, 46% in-house
- Threat intelligence analysis: 54% outsourced, 46% in-house
- Cybersecurity exercise creation and delivery: 60% outsourced, 40% in-house
- Vulnerability scanning and management: 61% outsourced, 39% in-house
- Penetration testing: 75% outsourced, 25% in-house
Thinking about the most recent significant cybersecurity incident, how was it discovered?

- Discovered by the SOC: 16%
- Discovered internally by a business function: 24%
- Discovered externally by a third-party: 8%
- Other: 6%
- We have not had a significant incident: 46%
Which statement best describes the maturity of your threat intelligence program?

- We do not have a program: 27%
- We have a formal and up-to-date program: 28%
- We have a formal but obsolete program: 5%
- We have an informal program: 40%
Which statement best describes the maturity of your vulnerability identification capability program?

- We do not have a program: 18%
- We have a formal and up-to-date program: 41%
- We have a formal but obsolete program: 10%
- We have an informal program: 30%
Which statement best describes the maturity of your breach detection program?

- We do not have a program: 20%
- We have a formal and up-to-date program: 36%
- We have a formal but obsolete program: 10%
- We have an informal program: 35%
Which statement best describes the maturity of your incident response capability program?

- We do not have a program: 13%
- We have a formal and up-to-date program: 47%
- We have a formal but obsolete program: 14%
- We have an informal program: 26%
Which statement best describes the maturity of your data protection program?

- We do not have a program: 15%
- We have a formal and up-to-date program: 39%
- We have a formal but obsolete program: 14%
- We have an informal program: 32%
Which statement best describes the maturity of your identity and access management program?

- We do not have a program: 13%
- We have a formal and up-to-date program: 44%
- We have a formal but obsolete program: 19%
- We have an informal program: 24%
Section: 4

People and organization
How effective are your organization’s information security reports?

- I do not receive reports: 21%
- The reports do not meet my expectations: 13%
- The reports meet some of my expectations: 52%
- The reports meet all my expectations: 14%
What information is provided in your organization's information security reports?

<table>
<thead>
<tr>
<th>Information Provided</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>The number of cyber attacks</td>
<td>20%</td>
</tr>
<tr>
<td>The number of cyber attacks successfully defended against</td>
<td>16%</td>
</tr>
<tr>
<td>List of breaches</td>
<td>17%</td>
</tr>
<tr>
<td>The financial impact of every significant breach</td>
<td>5%</td>
</tr>
<tr>
<td>Indication that the regulator needs to be notified of a particular breach</td>
<td>8%</td>
</tr>
<tr>
<td>Areas for improvement</td>
<td>17%</td>
</tr>
<tr>
<td>The overall threat level for the organization</td>
<td>14%</td>
</tr>
<tr>
<td>Other...</td>
<td>3%</td>
</tr>
</tbody>
</table>
Does the board/executive management team of your organization have a comprehensive understanding of information security to fully evaluate the cyber risks the organization is facing and the measures that it is taking?

- Yes: 39%
- Limited: 31%
- No, and no plans to improve: 3%
- No, but they are taking positive steps to improve their understanding: 25%
- Other: 2%
Who is directly responsible for information security in your organization?

- CIO/head of IT: 40%
- CISO/IT Risk/Network Security Officer: 48%
- We do not have anyone who is directly responsible: 4%
- Other...: 7%
Is the person with direct responsibility for information security a member of your organization’s board or executive management team?

- 60% Yes, they are on the board of our organization
- 40% No, they are not on the board of our organization
What is the likelihood of your organization being able to detect a sophisticated cyber attack?

- Very likely: 18%
- Likely: 41%
- Unlikely: 28%
- Very unlikely: 10%
- Don't know: 3%
How would you characterize the extent to which your information security function is meeting the needs of your organization?

- Fully meets needs: 8%
- Partially and plans to improve: 59%
- Partially but no plans to improve: 11%
- To be improved: 18%
- Does not meet needs: 4%
What challenges limit the value that your information security function adds to your organization?

- Lack of skilled resources: 30%
- Budget constraints: 25%
- Lack of executive awareness or support: 11%
- Management and governance issues: 13%
- Lack of quality tools for managing information security: 16%
- Other: 4%
In case of a significant cybersecurity breach, how does your organization perform in the following areas:

- Identification of the breach: 12% Poor, 27% Fair, 33% Good, 22% Very good, 6% Excellent
- Crisis management: 10% Poor, 23% Fair, 36% Good, 23% Very good, 8% Excellent
- Communication internally: 5% Poor, 22% Fair, 38% Good, 25% Very good, 9% Excellent
- Communication externally: 10% Poor, 26% Fair, 36% Good, 21% Very good, 7% Excellent
- Forensics: 21% Poor, 28% Fair, 28% Good, 16% Very good, 7% Excellent
- Returning to business as usual: 5% Poor, 19% Fair, 40% Good, 27% Very good, 9% Excellent
What was the root cause of the latest significant breach at your organization?

- Complex access permissions: 1%
- Improper configuration: 6%
- Known vulnerability/back door: 5%
- Malware: 12%
- Other...: 5%
- Phishing attacks: 11%
- Stolen passwords/credentials: 3%
- Unsecured IoT devices: 1%
- We did not have a significant breach: 54%
- Weak passwords/credentials: 2%
Section: 5

Finance and legal
At what point 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?

<table>
<thead>
<tr>
<th>Action</th>
<th>On day one</th>
<th>Only after all investigations are complete and the issue is closed</th>
<th>Within the first week while investigations continue</th>
<th>Never</th>
<th>Don't know</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notify regulators and compliance organizations</td>
<td>11%</td>
<td>10%</td>
<td>42%</td>
<td>27%</td>
<td>6%</td>
</tr>
<tr>
<td>If customer information affected, notify all customers</td>
<td>15%</td>
<td>17%</td>
<td>36%</td>
<td>15%</td>
<td>6%</td>
</tr>
<tr>
<td>If no customer information affected, notify all customers anyway</td>
<td>15%</td>
<td>9%</td>
<td>15%</td>
<td>6%</td>
<td>17%</td>
</tr>
<tr>
<td>Individually notify only those customers impacted</td>
<td>10%</td>
<td>17%</td>
<td>38%</td>
<td>18%</td>
<td>3%</td>
</tr>
<tr>
<td>Issue a press release and public statement to the media</td>
<td>18%</td>
<td>16%</td>
<td>27%</td>
<td>8%</td>
<td>14%</td>
</tr>
<tr>
<td>If supplier information affected, notify all suppliers</td>
<td>14%</td>
<td>14%</td>
<td>32%</td>
<td>14%</td>
<td>11%</td>
</tr>
<tr>
<td>If no supplier information affected, notify all suppliers anyway</td>
<td>14%</td>
<td>9%</td>
<td>15%</td>
<td>5%</td>
<td>41%</td>
</tr>
<tr>
<td>Individually notify only those suppliers impacted</td>
<td>11%</td>
<td>17%</td>
<td>35%</td>
<td>19%</td>
<td>3%</td>
</tr>
<tr>
<td>Only after all investigations are complete and the issue is closed</td>
<td>10%</td>
<td>17%</td>
<td>38%</td>
<td>18%</td>
<td>14%</td>
</tr>
<tr>
<td>Within the first week while investigations continue</td>
<td>10%</td>
<td>17%</td>
<td>38%</td>
<td>18%</td>
<td>14%</td>
</tr>
<tr>
<td>Never</td>
<td>10%</td>
<td>17%</td>
<td>38%</td>
<td>18%</td>
<td>14%</td>
</tr>
</tbody>
</table>
What is the estimated total financial damage related to information security incidents over the past year at your organization? *(This includes loss of productivity, regulatory fines, etc.; the estimate excludes costs or missed revenue due to brand damage.)*

- Above US$2.5m: 1%
- Between US$1 and US$100,000: 24%
- Between US$100,000 and US$250,000: 6%
- Between US$1m and US$2.5m: 1%
- Between US$250,000 and US$500,000: 3%
- Between US$500,000 and US$1m: 3%
- No financial loss: 62%
What is your current level of interest in cyber insurance?

- We currently have cyber insurance that meets our organization's needs: 35%
- We currently have cyber insurance, but it does not meet our organization's needs: 5%
- We do not have cyber insurance and are actively looking for appropriate cover: 20%
- We do not have cyber insurance and we have no plans to adopt it: 18%
- We have never considered cyber insurance: 16%
- Other: 5%
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.

© 2018 EYGM Limited.
All Rights Reserved.

EYG no. XXXXXX

BMC Advisory
TI0000_00583

ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com