

## ITALY REPORT CARD

Top responses given by survey respondents.

<h3>Fraud</h3>	<p><b>77</b> Percentage of respondents affected by fraud in the past 12 months.</p>	<p>↑ <b>3%</b> points above 2015                  ↓ <b>5%</b> points below global average of 82%</p> <p style="text-align: right;"><small>Global avg.</small></p>															
<h4>MOST COMMON TYPES OF FRAUD</h4>	<table border="1"> <tr> <td>Theft of Physical Assets or Stock</td> <td><b>34%</b></td> <td>29%</td> </tr> <tr> <td>Information theft, loss or attack (e.g., data theft)</td> <td><b>26%</b></td> <td>24%</td> </tr> <tr> <td>Regulatory or compliance breach</td> <td><b>26%</b></td> <td>21%</td> </tr> </table>	Theft of Physical Assets or Stock	<b>34%</b>	29%	Information theft, loss or attack (e.g., data theft)	<b>26%</b>	24%	Regulatory or compliance breach	<b>26%</b>	21%	<p style="text-align: right;"><small>Global avg.</small></p>						
Theft of Physical Assets or Stock	<b>34%</b>	29%															
Information theft, loss or attack (e.g., data theft)	<b>26%</b>	24%															
Regulatory or compliance breach	<b>26%</b>	21%															
<h4>MOST COMMON PERPETRATORS</h4>	<table border="1"> <tr> <td>Junior employees of our own company</td> <td><b>50%</b></td> <td>39%</td> </tr> <tr> <td>Ex-employees</td> <td><b>36%</b></td> <td>27%</td> </tr> <tr> <td>Vendors/suppliers (i.e., a provider of technology or services to your company)</td> <td><b>33%</b></td> <td>26%</td> </tr> <tr> <td>Senior or middle management employees of our own company</td> <td><b>31%</b></td> <td>30%</td> </tr> <tr> <td>Customers</td> <td><b>22%</b></td> <td>19%</td> </tr> </table>	Junior employees of our own company	<b>50%</b>	39%	Ex-employees	<b>36%</b>	27%	Vendors/suppliers (i.e., a provider of technology or services to your company)	<b>33%</b>	26%	Senior or middle management employees of our own company	<b>31%</b>	30%	Customers	<b>22%</b>	19%	
Junior employees of our own company	<b>50%</b>	39%															
Ex-employees	<b>36%</b>	27%															
Vendors/suppliers (i.e., a provider of technology or services to your company)	<b>33%</b>	26%															
Senior or middle management employees of our own company	<b>31%</b>	30%															
Customers	<b>22%</b>	19%															
<h4>MOST COMMON ANTI-FRAUD MEASURES</h4> <p><small>Percentage of respondents who have implemented the anti-fraud measure.</small></p>	<table border="1"> <tr> <td>Assets (physical security systems, stock inventories, tagging, asset register)</td> <td><b>83%</b></td> <td>79%</td> </tr> <tr> <td>Board of director engagement in cyber security policies and procedures</td> <td><b>72%</b></td> <td>75%</td> </tr> <tr> <td>Partners, clients, and vendors (due diligence)</td> <td><b>70%</b></td> <td>77%</td> </tr> <tr> <td>IP (intellectual property risk assessment and trademark monitoring program)</td> <td><b>68%</b></td> <td>75%</td> </tr> </table>	Assets (physical security systems, stock inventories, tagging, asset register)	<b>83%</b>	79%	Board of director engagement in cyber security policies and procedures	<b>72%</b>	75%	Partners, clients, and vendors (due diligence)	<b>70%</b>	77%	IP (intellectual property risk assessment and trademark monitoring program)	<b>68%</b>	75%				
Assets (physical security systems, stock inventories, tagging, asset register)	<b>83%</b>	79%															
Board of director engagement in cyber security policies and procedures	<b>72%</b>	75%															
Partners, clients, and vendors (due diligence)	<b>70%</b>	77%															
IP (intellectual property risk assessment and trademark monitoring program)	<b>68%</b>	75%															
<h4>MOST COMMON MEANS OF DISCOVERY</h4>	<table border="1"> <tr> <td>By a whistle-blower at our company</td> <td><b>53%</b></td> <td>44%</td> </tr> </table>	By a whistle-blower at our company	<b>53%</b>	44%													
By a whistle-blower at our company	<b>53%</b>	44%															
<h3>Cyber Security</h3>	<p><b>79</b> Percentage of respondents that experienced a cyber incident in the past 12 months.</p>	<p>↓ <b>6%</b> points below global average of 85%</p> <p style="text-align: right;"><small>Global avg.</small></p>															
<h4>MOST COMMON TYPES OF CYBER INCIDENT</h4>	<table border="1"> <tr> <td>Data deletion by malicious insider</td> <td><b>30%</b></td> <td>19%</td> </tr> <tr> <td>Email-based phishing attack</td> <td><b>21%</b></td> <td>26%</td> </tr> <tr> <td>Virus/worm infestation</td> <td><b>21%</b></td> <td>33%</td> </tr> </table>	Data deletion by malicious insider	<b>30%</b>	19%	Email-based phishing attack	<b>21%</b>	26%	Virus/worm infestation	<b>21%</b>	33%	<p style="text-align: right;"><small>Global avg.</small></p>						
Data deletion by malicious insider	<b>30%</b>	19%															
Email-based phishing attack	<b>21%</b>	26%															
Virus/worm infestation	<b>21%</b>	33%															
<h4>MOST COMMON PERPETRATORS</h4>	<table border="1"> <tr> <td>Ex-employees</td> <td><b>24%</b></td> <td>20%</td> </tr> </table>	Ex-employees	<b>24%</b>	20%													
Ex-employees	<b>24%</b>	20%															
<h4>MOST COMMON TARGET</h4>	<table border="1"> <tr> <td>Physical assets/money</td> <td><b>38%</b></td> <td>38%</td> </tr> <tr> <td>Customer records</td> <td><b>35%</b></td> <td>51%</td> </tr> <tr> <td>Trade secrets/R&amp;D/IP</td> <td><b>35%</b></td> <td>40%</td> </tr> </table>	Physical assets/money	<b>38%</b>	38%	Customer records	<b>35%</b>	51%	Trade secrets/R&D/IP	<b>35%</b>	40%							
Physical assets/money	<b>38%</b>	38%															
Customer records	<b>35%</b>	51%															
Trade secrets/R&D/IP	<b>35%</b>	40%															
<h4>MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED</h4>	<table border="1"> <tr> <td>Webhosting/website provider</td> <td><b>16%</b></td> <td>9%</td> </tr> </table>	Webhosting/website provider	<b>16%</b>	9%													
Webhosting/website provider	<b>16%</b>	9%															
<h3>Security</h3>	<p><b>68</b> Percentage of respondents that experienced a security incident in the past 12 months.</p>	<p>= equal to global average of 68%</p> <p style="text-align: right;"><small>Global avg.</small></p>															
<h4>MOST COMMON TYPES OF SECURITY INCIDENTS</h4>	<table border="1"> <tr> <td>Theft or loss of intellectual property</td> <td><b>43%</b></td> <td>38%</td> </tr> <tr> <td>Environmental risk (including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)</td> <td><b>21%</b></td> <td>27%</td> </tr> <tr> <td>Workplace violence</td> <td><b>13%</b></td> <td>23%</td> </tr> </table>	Theft or loss of intellectual property	<b>43%</b>	38%	Environmental risk (including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)	<b>21%</b>	27%	Workplace violence	<b>13%</b>	23%	<p style="text-align: right;"><small>Global avg.</small></p>						
Theft or loss of intellectual property	<b>43%</b>	38%															
Environmental risk (including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)	<b>21%</b>	27%															
Workplace violence	<b>13%</b>	23%															
<h4>MOST COMMON PERPETRATORS</h4>	<table border="1"> <tr> <td>Ex-employees</td> <td><b>31%</b></td> <td>23%</td> </tr> </table>	Ex-employees	<b>31%</b>	23%													
Ex-employees	<b>31%</b>	23%															
<h4>RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY RISKS</h4>	<table border="1"> <tr> <td>Workplace violence</td> <td><b>17%</b></td> <td>27%</td> </tr> <tr> <td>Theft or loss of intellectual property</td> <td><b>13%</b></td> <td>19%</td> </tr> <tr> <td>Terrorism (including domestic and international events)</td> <td><b>9%</b></td> <td>18%</td> </tr> </table>	Workplace violence	<b>17%</b>	27%	Theft or loss of intellectual property	<b>13%</b>	19%	Terrorism (including domestic and international events)	<b>9%</b>	18%							
Workplace violence	<b>17%</b>	27%															
Theft or loss of intellectual property	<b>13%</b>	19%															
Terrorism (including domestic and international events)	<b>9%</b>	18%															