Nationwide Cyber Security Survey

Presented by Harris Poll

July 2015
Executive Summary: Cyber-Security

- **Cyber-security is a low priority for many because the threat is not palpable**
  Eight in ten (79%) have no cyber-attack plan in place. When asked why not:
  - 46% feel their current software is secure enough and
  - 40% do not feel their company will be affected by a cyber-attack.

- **Perceived ease of recovery also contributes to the deprioritization of cyber-security**
  - Virtually all SBOs (95%) are at least somewhat confident they'll recover from an attack
  - Of the 80% who have never been affected by a cyber-attack, over half (53%) think the recovery would take *less than a month*.
  - However, of the 17% who were actually affected by a cyber-attack, just 30% say it took *less than a month* to recover.
  - In the aftermath of a breach, there’s overall agreement that the actual *data breach* is quicker to fix (61% say it would take less than 3 months) than either *financial* (45% say less than three months) or *reputation/trust* (49%) damages.
Few SBOs have a cyber attack response plan

### Types of Plans Company Currently Has in Place

<table>
<thead>
<tr>
<th>Type of Plan</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plan in place to protect customer data</td>
<td>36%</td>
</tr>
<tr>
<td>Business continuity plan</td>
<td>31%</td>
</tr>
<tr>
<td>Evacuation plan</td>
<td>31%</td>
</tr>
<tr>
<td>Communication plan</td>
<td>27%</td>
</tr>
<tr>
<td>Disaster recovery plan</td>
<td>25%</td>
</tr>
<tr>
<td>Cyber attack response plan*</td>
<td>21%</td>
</tr>
<tr>
<td>Crisis communication plan</td>
<td>19%</td>
</tr>
</tbody>
</table>

Larger companies are more likely to have a cyber-attack response plan (42% 100-299 employees, 39% 50-99 employees, 12% under 50 employees), as are those who have been affected by a cyber-attack (43% vs. 17% not affected).  

*An attack, via cyberspace, targeting an enterprise’s use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.*

**BASE:** ALL QUALIFIED RESPONDENTS (n=500)  
**Q12** Which of the following types of plans does your company currently have in place? Please select all that apply.
Nearly three-quarters are at least somewhat concerned about a cyber attack

Level of Concern With a Potential Cyber-Attack on Business

- **Very concerned**: 17%
- **Concerned**: 18%
- **Somewhat concerned**: 37%
- **Not at all concerned**: 27%

Total: 73%

- Larger companies are more likely to be concerned about cyber-attacks than are smaller companies (91% 50-299 employees vs. 64% under 50 employees).
- Those who have already been affected by a cyber-attack are also more concerned (93% vs. 68% have not had an attack).

Base: ALL QUALIFIED RESPONDENTS (n=500)
Q14 How concerned are you with a potential cyber-attack affecting your business?
Cyber-attacks are not usual, but half took over three months to recover from

**Has Company Been Affected by Cyber-Attack**

- Yes: 17%
- No: 80%
- Total: 100%

**Time it Took Company to Recover from Cyber-Attack**

- Less than a month: 30%
- 1 to less than 3 months: 20%
- 3 to less than 6 months: 18%
- 6 months to a year: 22%
- 1 to 2 years: 4%
- 3 to 4 years: 4%
- 5 or more years: 0%
- My business still hasn't recovered: 1%

Larger companies are more likely to have been affected by a cyber-attack (45% 100-299 employees, 23% 50-99 employees, 8% under 50 employees).

**BASE:** ALL QUALIFIED RESPONDENTS (n=500)/ENCOUNTERED CYBER-ATTACK (n=128)

**Q16** Has your company ever been affected by a cyber-attack?

**Q17** How long did it take your company to recover from a cyber-attack?
SBOs admit they have been a victim of computer viruses and phishing attempts

While some have experienced a Trojan horse (22%) or hacking attack (16%), over a third (37%) say they have not been attacked.

<table>
<thead>
<tr>
<th>Types of Attacks Ever Happen to Company</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer virus</td>
<td>44%</td>
</tr>
<tr>
<td>Phishing</td>
<td>30%</td>
</tr>
<tr>
<td>Trojan horse</td>
<td>22%</td>
</tr>
<tr>
<td>Hacking</td>
<td>16%</td>
</tr>
<tr>
<td>Data breach</td>
<td>11%</td>
</tr>
<tr>
<td>Issues due to unpatched software</td>
<td>10%</td>
</tr>
<tr>
<td>Unauthorized access to customer information</td>
<td>9%</td>
</tr>
<tr>
<td>Unauthorized access to company information</td>
<td>8%</td>
</tr>
<tr>
<td>None of the above</td>
<td>37%</td>
</tr>
</tbody>
</table>

Larger companies are more likely to have been a victim of a cyber-attacks (80% of companies with 50 – 299 employees were a victim of at least one of these types of attacks vs. 55% for those with fewer than 50 employees).

63% were victim to at least one type of attack.
SBOs acknowledge customer data security as increasingly essential to customer trust

Even so, most still feel they are not at risk for a cyber-attack (72%) and are confident in their company’s encryption service (66%) and employees’ knowledge of spotting a cyber security issue (65%).

It is becoming increasingly important to keep customers’ data secure to build trust
- Somewhat agree: 41%
- Strongly agree: 50%
- Top 2 Box: 91%

I do not feel that my business is at risk for a cyber-attack
- Somewhat agree: 37%
- Strongly agree: 35%
- Top 2 Box: 72%

My company uses an encryption service to protect customer data
- Somewhat agree: 39%
- Strongly agree: 28%
- Top 2 Box: 66%

My company’s employees know how to spot a cyber security issue
- Somewhat agree: 43%
- Strongly agree: 22%
- Top 2 Box: 65%

My company always notifies customers that their data may be at risk after a cyber-attack
- Somewhat agree: 35%
- Strongly agree: 28%
- Top 2 Box: 63%

Customers are more likely to have credit card information stolen from a large company than a small business
- Somewhat agree: 34%
- Strongly agree: 29%
- Top 2 Box: 63%

Cyber security insurance is too expensive
- Somewhat agree: 40%
- Strongly agree: 22%
- Top 2 Box: 62%

I feel that I have adequate cyber security training
- Somewhat agree: 41%
- Strongly agree: 21%
- Top 2 Box: 62%

I do not feel small businesses would be targets of a cyber-attack
- Somewhat agree: 37%
- Strongly agree: 17%
- Top 2 Box: 54%

Recent media coverage of major corporations experiencing cyber-attacks have prompted my company to add additional cyber security measures
- Somewhat agree: 29%
- Strongly agree: 18%
- Top 2 Box: 47%

I do not fully understand the impact a cyber-attack may have on my business
- Somewhat agree: 34%
- Strongly agree: 13%
- Top 2 Box: 47%

I would not know what to do if my business experienced a cyber-attack
- Somewhat agree: 29%
- Strongly agree: 13%
- Top 2 Box: 42%

I do not fully understand cyber-attacks
- Somewhat agree: 27%
- Strongly agree: 14%
- Top 2 Box: 41%

A cyber attack would put my company out of business
- Somewhat agree: 19%
- Strongly agree: 11%
- Top 2 Box: 31%

A bank has informed me about a cyber security breach affecting my customers
- Somewhat agree: 18%
- Strongly agree: 11%
- Top 2 Box: 29%

Base: ALL QUALIFIED RESPONDENTS (n=500)
Q24 Please tell me if you agree or disagree with the following statements.

July 2015
Financial and reputational recovery may take longer than fixing a cybersecurity breach

Six in ten (61%) say the data breach would be corrected in fewer than three months; but over half believe their reputation (51%) or finances (55%) would suffer for a longer period of time.

**Time It Would Take for Business to Recover From Incidents**

<table>
<thead>
<tr>
<th>Time Frame</th>
<th>Fix the breach point technology</th>
<th>Financially bounce back</th>
<th>Recover reputation/rebuild customer trust</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 3 months</td>
<td>61%</td>
<td>45%</td>
<td>49%</td>
</tr>
<tr>
<td>3 - 11 months</td>
<td>27%</td>
<td>39%</td>
<td>36%</td>
</tr>
<tr>
<td>1 - 4 years</td>
<td>10%</td>
<td>11%</td>
<td>13%</td>
</tr>
<tr>
<td>5+ years</td>
<td>&lt;1%</td>
<td>1%</td>
<td>1%</td>
</tr>
<tr>
<td>I do not think my business would ever recover</td>
<td>2%</td>
<td>4%</td>
<td>2%</td>
</tr>
</tbody>
</table>

Smaller companies (under 50 employees) expect a shorter time to fix and recover from a breach: 71% of those with fewer than 50 employees say fixing the breach would take fewer than 3 months, compared to 41% among those with 50-99 employees and 40% among 100-299.

**BASE:** ALL QUALIFIED RESPONDENTS (n=500)

Q27 How long do you think it would take your business to recover in each of the following ways? By recover, we mean return to pre-incident status.
Methodology

The Small Business Owner Study was conducted online from June 8 - 19, 2015. Respondents comprised 500 U.S. small business owners, defined as companies with less than 300 employees.

- Results are weighted to be representative of small business owners in the U.S.
- Research participants were drawn from the Harris Poll Online (HPOL) research panel and partner sample. Because the sample is based on those who were invited to participate in the HPOL panel, estimates of theoretical sampling error cannot be calculated.
- Percentages were rounded to the nearest whole percent. Differences in the sums of combined categories/answers are due to rounding.

Throughout the report, we have called out differences between relevant subgroups if they are statistically significant at the 95% confidence level.