



**Marketing**

Marketing Research

# **Nationwide Cyber Security Survey**

**Presented by Harris Poll**

July 2015

## Executive Summary: Cyber-Security

---

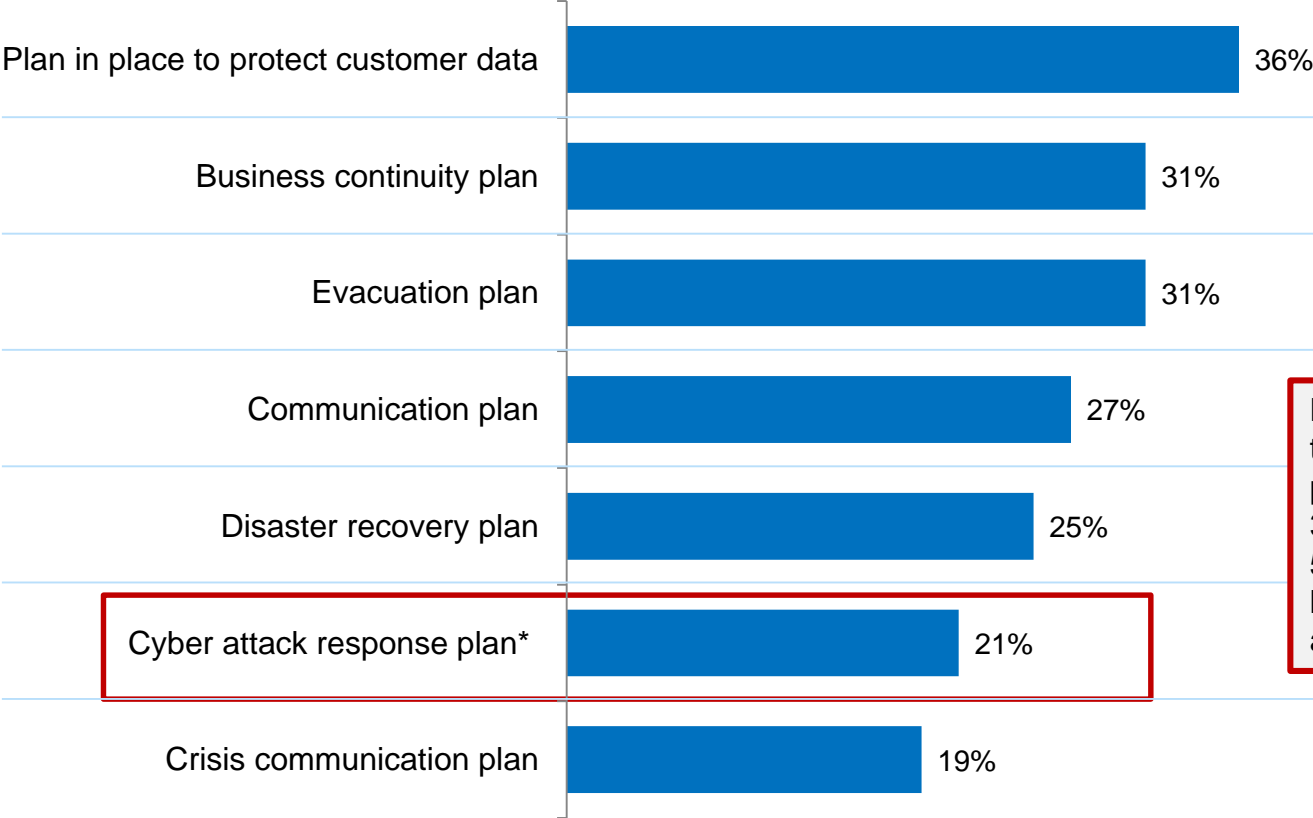
- **Cyber-security is a low priority for many because the threat is not palpable**

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



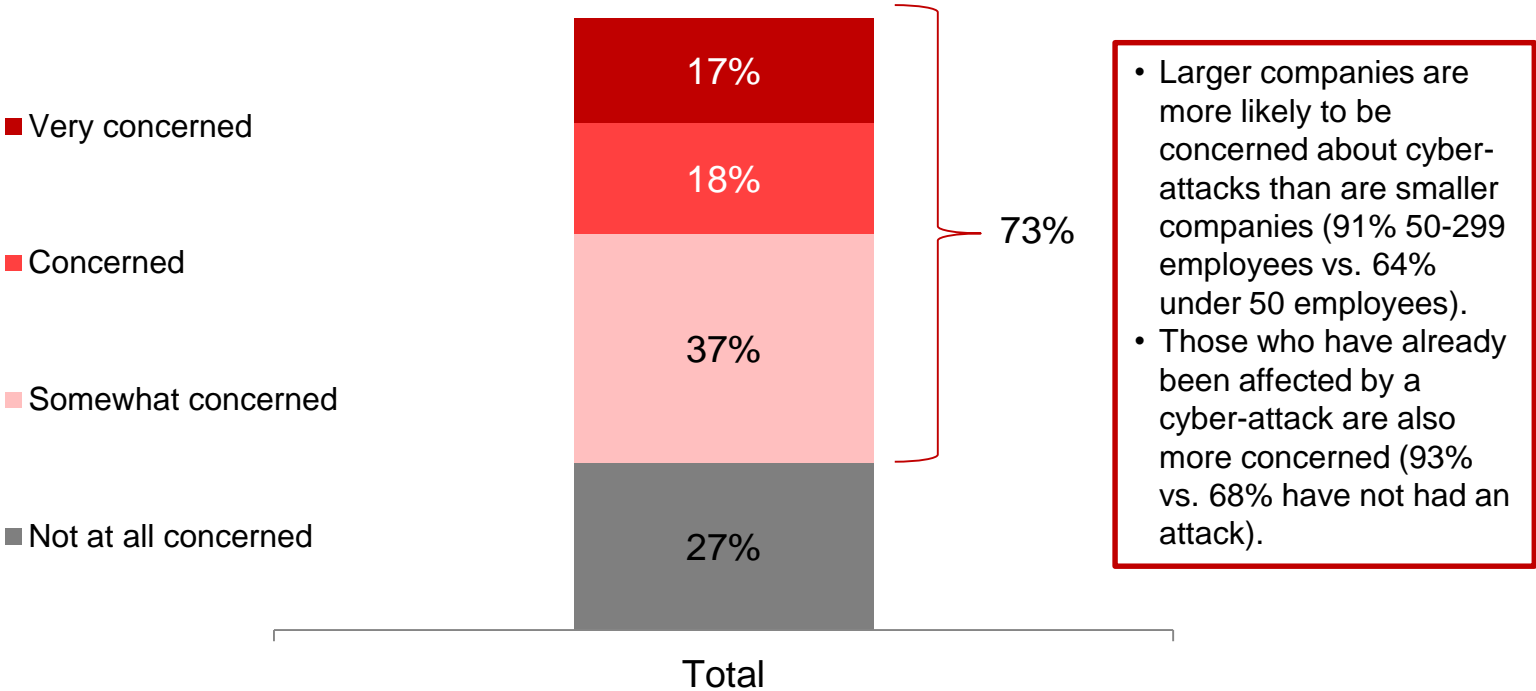
Larger companies are more likely to have a cyber-attack response plan (42% 100-299 employees, 39% 50-99 employees, 12% under 50 employees), as are those who have been affected by a cyber-attack (43% vs. 17% not affected).

\*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

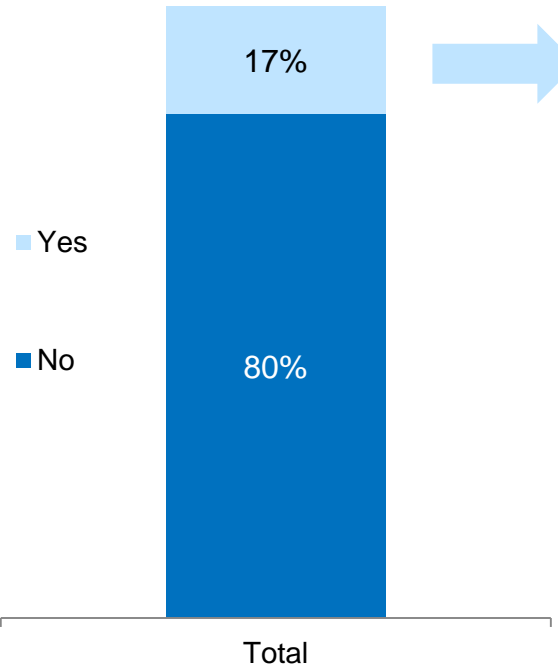
Level of Concern With a Potential Cyber-Attack on Business



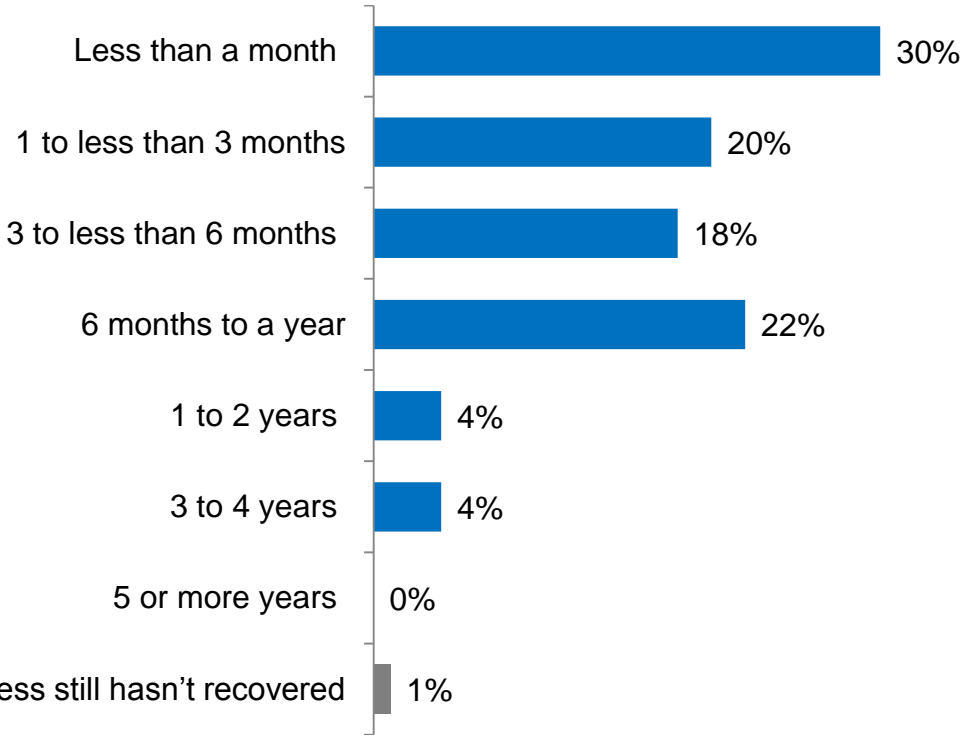
Base: ALL QUALIFIED RESPONDENTS (n=500)  
Q14 How concerned are you with a potential cyber-attack affecting your business?

# Cyber-attacks are not usual, but half took over three months to recover from

Has Company Been Affected by Cyber-Attack



Time it Took Company to Recover from Cyber-Attack



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).

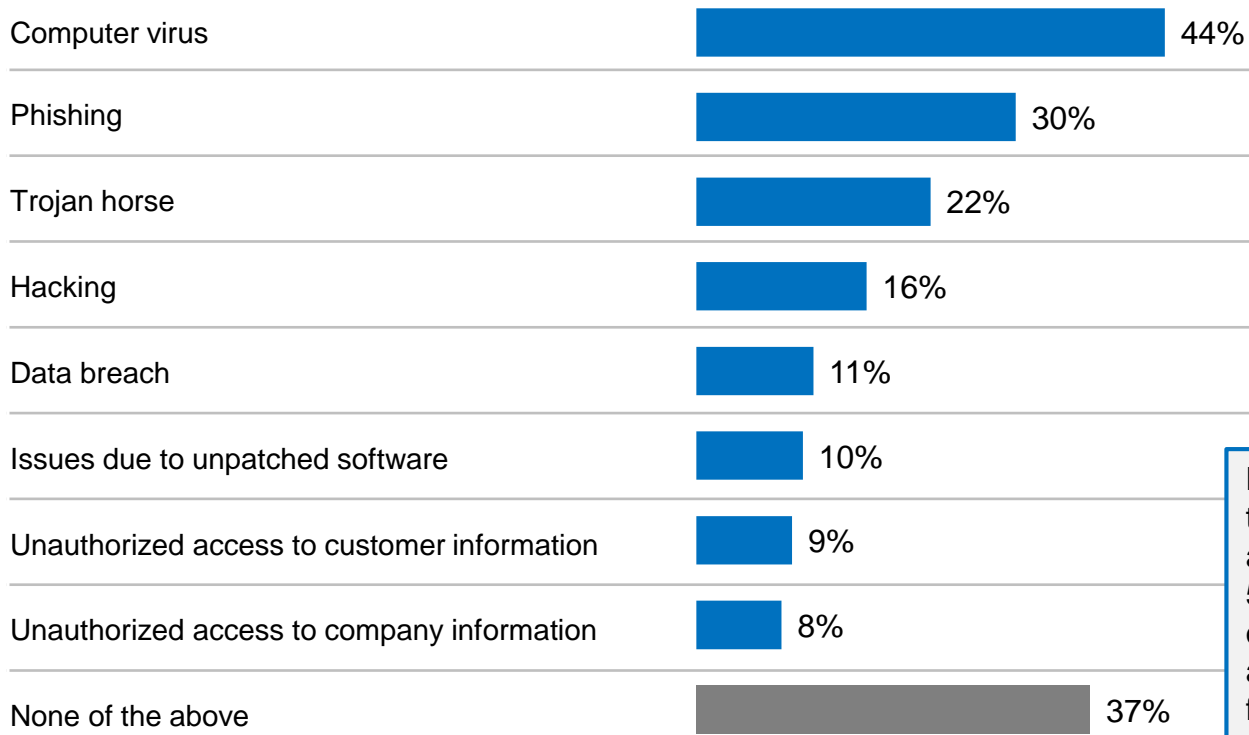
BASE: ALL QUALIFIED RESPONDENTS (n=500)/ENCOUNTERED CYBER-ATTACK (n=128)

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.

**Types of Attacks Ever Happen to Company**



63% were victim to at least one type of attack.

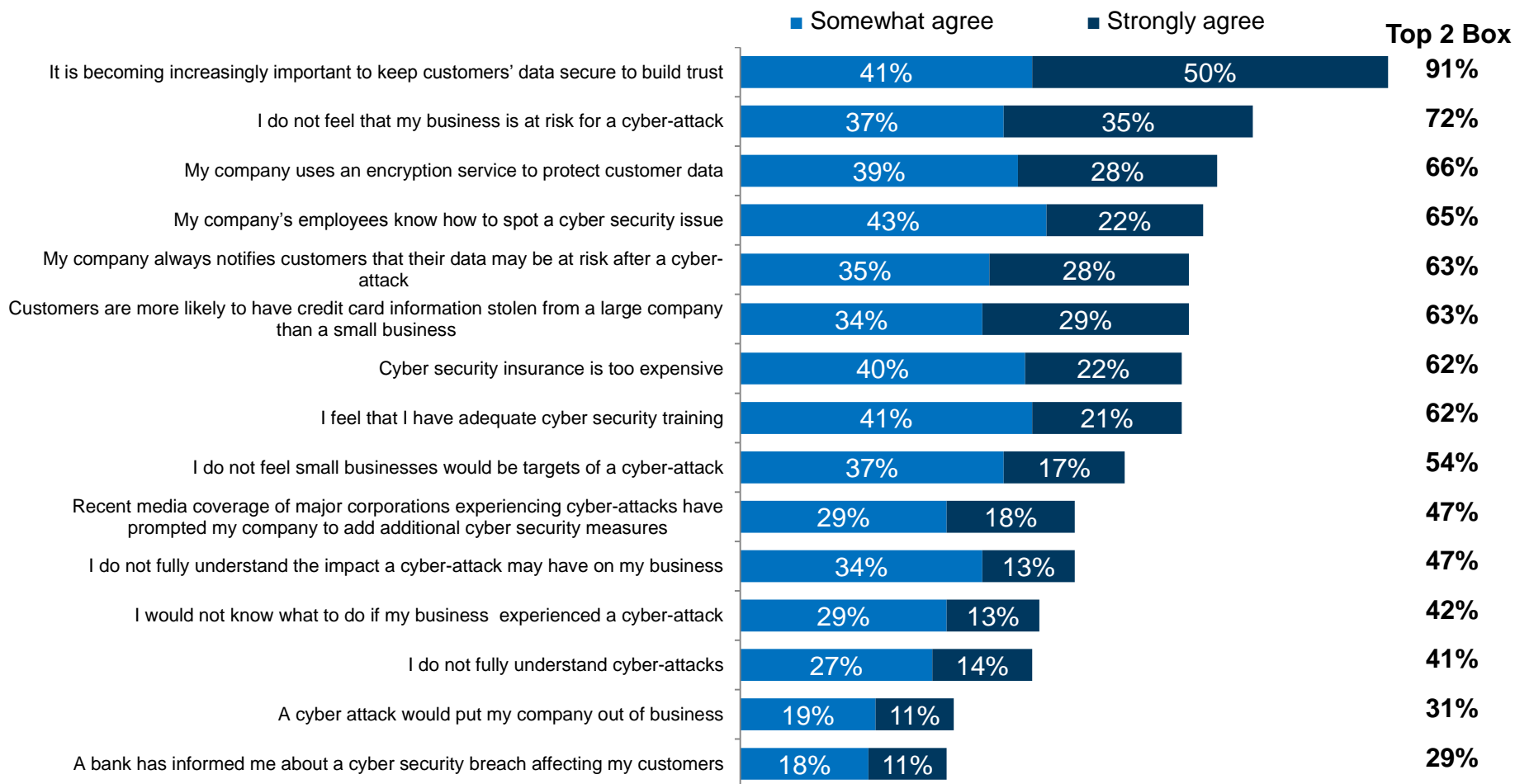
Larger companies are more likely to have been a victim of a cyber-attacks (80% of companies with 50 – 299 employees were a victim of at least one of these types of attacks vs. 55% for those with fewer than 50 employees).

BASE: QUALIFIED RESPONDENTS (n=500)

Q19 Have any of the following ever happened to your company? Please select all that apply.

# 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%).



Base: ALL QUALIFIED RESPONDENTS (n=500)

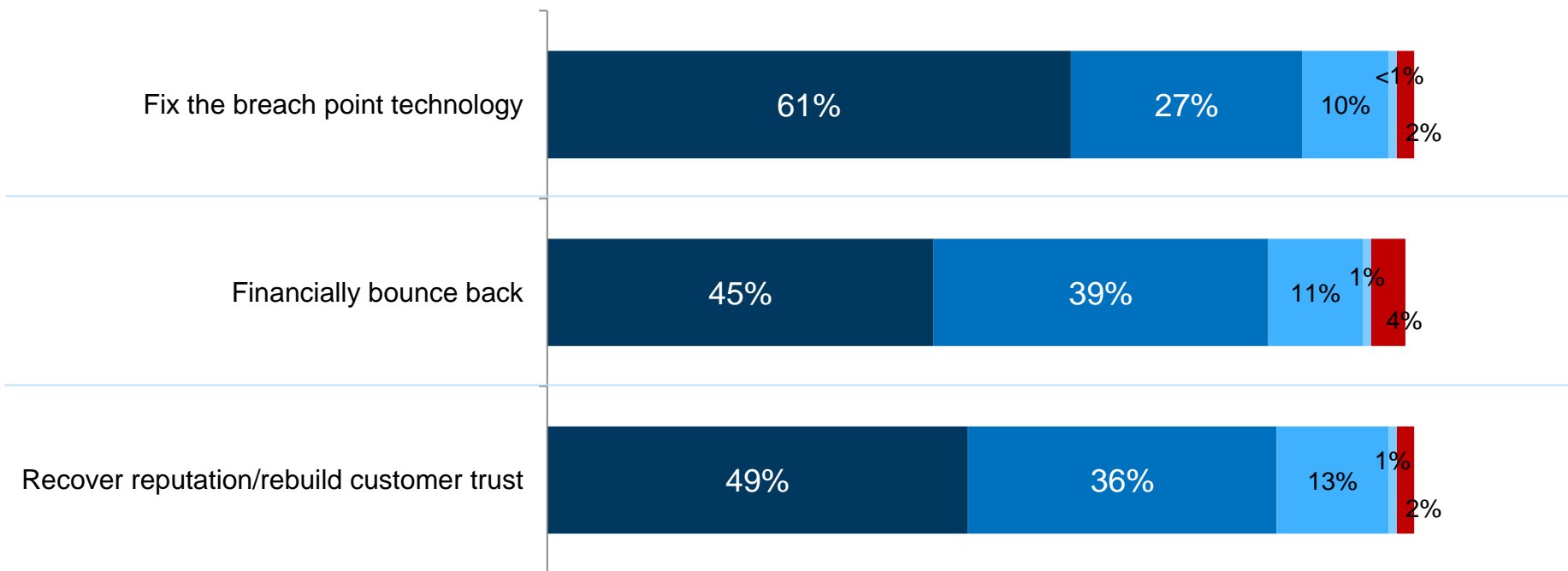
Q24 Please tell me if you agree or disagree with the following statements.

# 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**

■ Less than 3 months   ■ 3 - 11 months   ■ 1 - 4 years   ■ 5+ years   ■ I do not think my business would ever recover



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.