PulseReport
GATEPOINT RESEARCH

Web Threat Detection Trends in E-Commerce

RSA®

Summary Results • April 2016

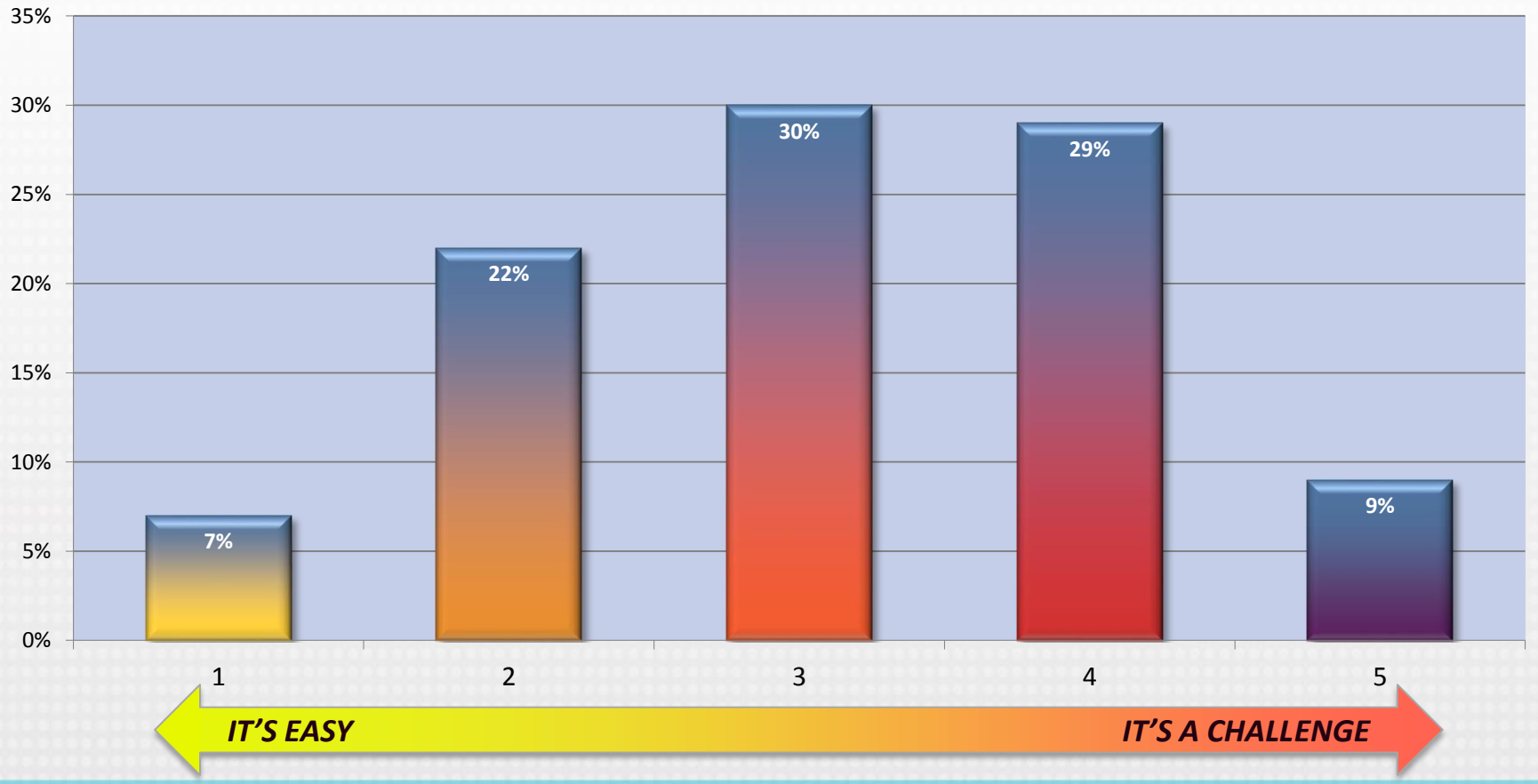
Program Overview

- Between January and April 2016, Gatepoint Research invited selected IT executives to participate in a survey themed ***Web Threat Detection Trends in E-Commerce***.
- Candidates were invited via email and 100 executives have participated to date.
- Management levels represented are predominantly senior decision makers: 12% hold the title CxO, 7% are VPs, 27% are Directors, and 51% are Managers.
- 66% of survey participants work in retail trade (the survey was focused on this industry). Other industry sectors also represented in the survey include general and primary manufacturing, wholesale trade, financial services, business services, and public administration .
- Almost two-thirds of respondents (61%) work in Fortune 1000 companies with revenues over $1.5 billion. Other revenue levels were also represented:
  - 17% work in Large firms whose revenues are between $500 million and $1.5 billion;
  - 10% work in Mid-Market firms with $250 million to $500 million in revenues;
  - 12% work in Small companies with less than $250 million in revenues.
- 100% of responders participated voluntarily; none were engaged using telemarketing.

Observations and Conclusions

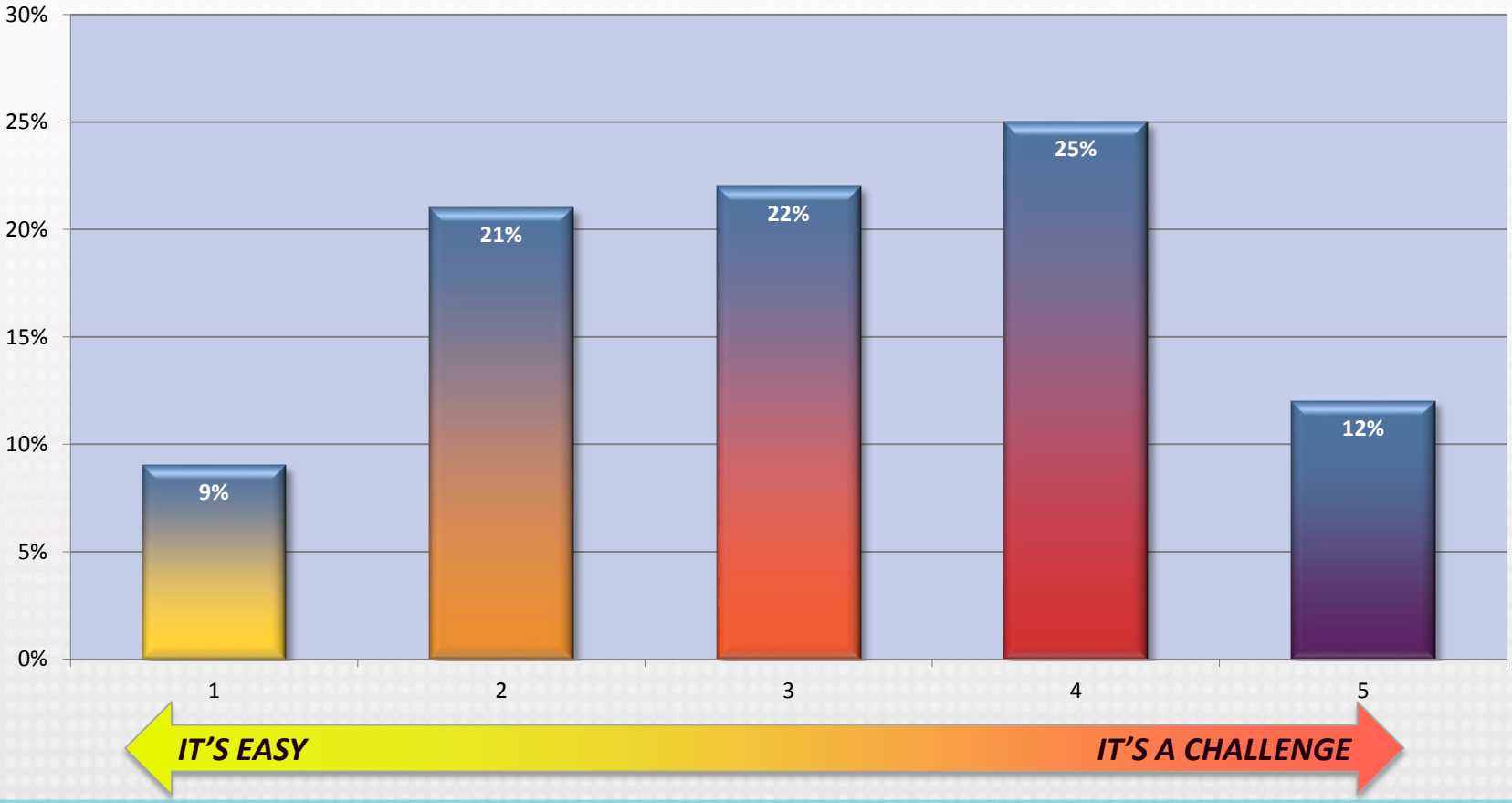
- ***Detecting fraud/suspicious activity isn't easy.*** 38% of respondents consider it a major challenge to detect suspicious activity in their web applications. Asked to evaluate the difficulty of detecting fraud in mobile applications, 37% of respondents characterize the task as "challenging."
- ***Finding the source of fraud takes too long.*** Only 30% of respondents report they can isolate the origin of fraudulent activity within hours.
- ***Loss of data, money, and service are the most worrisome security threats.*** By a wide margin, respondents cited loss of customer data as the most detrimental security threat (75%), followed by fraudulent money activity (52%) and DDoS attacks (44%). ***For most, actual losses due to cybercrime are not trivial.*** Just 36% of responders characterize their ecommerce cybercrime/fraud losses last year as "insignificant."
- ***Security technology: not one solution, but many.*** Asked to list technologies employed to protect their customer-facing applications, respondents reported using numerous strategies and solutions.
- ***Web behavior analytics is new territory.*** Only 13% of respondents report being familiar with using web behavior analytics to detect/investigate cyber attacks.
- ***Fraud investigation: a big job often done by a small team***. 61% of those surveyed report that their organization has assigned just 1-5 people to online fraud investigation.
- ***Will more security slow down our site?*** 66% of responders express concern that more security will affect site performance. Other concerns include "alert fatigue" (46%) and transaction abandonment (38%).
- ***Goals: reduce cost, improve customer experience, stop fraud.*** Predictably, top business goals responders cite over the next year include reducing operational costs (65%) and improving customer experience (58%). But increasing the efficiency of fraud teams also ranked high (38%).

How well is your organization able to detect fraud or suspicious activity occurring in your Web applications?



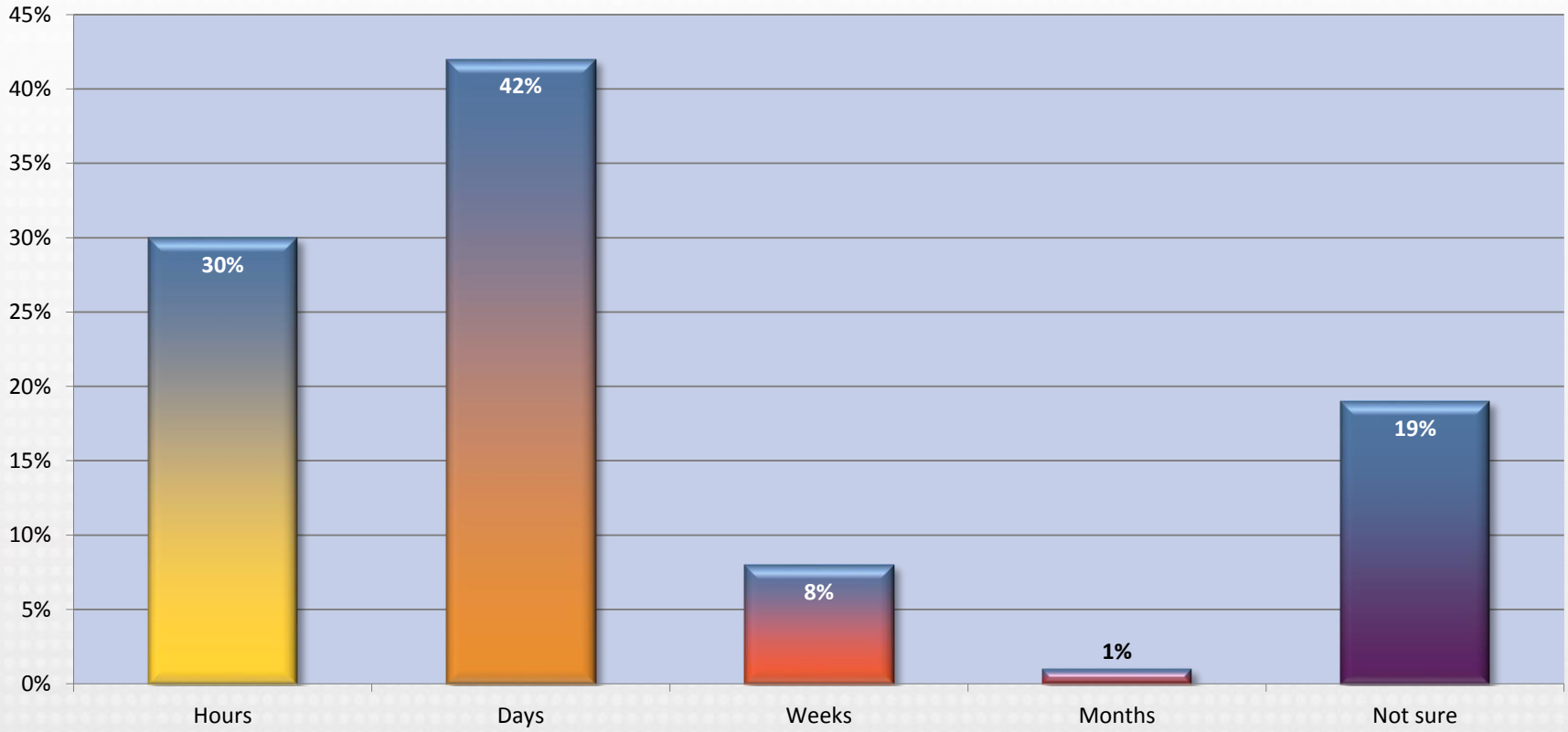
Detecting fraud/suspicious activity isn't easy. *38% of respondents consider it a considerable challenge to detect suspicious activity in their web applications.*

How well is your organization able to detect fraud or suspicious activity occurring in mobile applications?



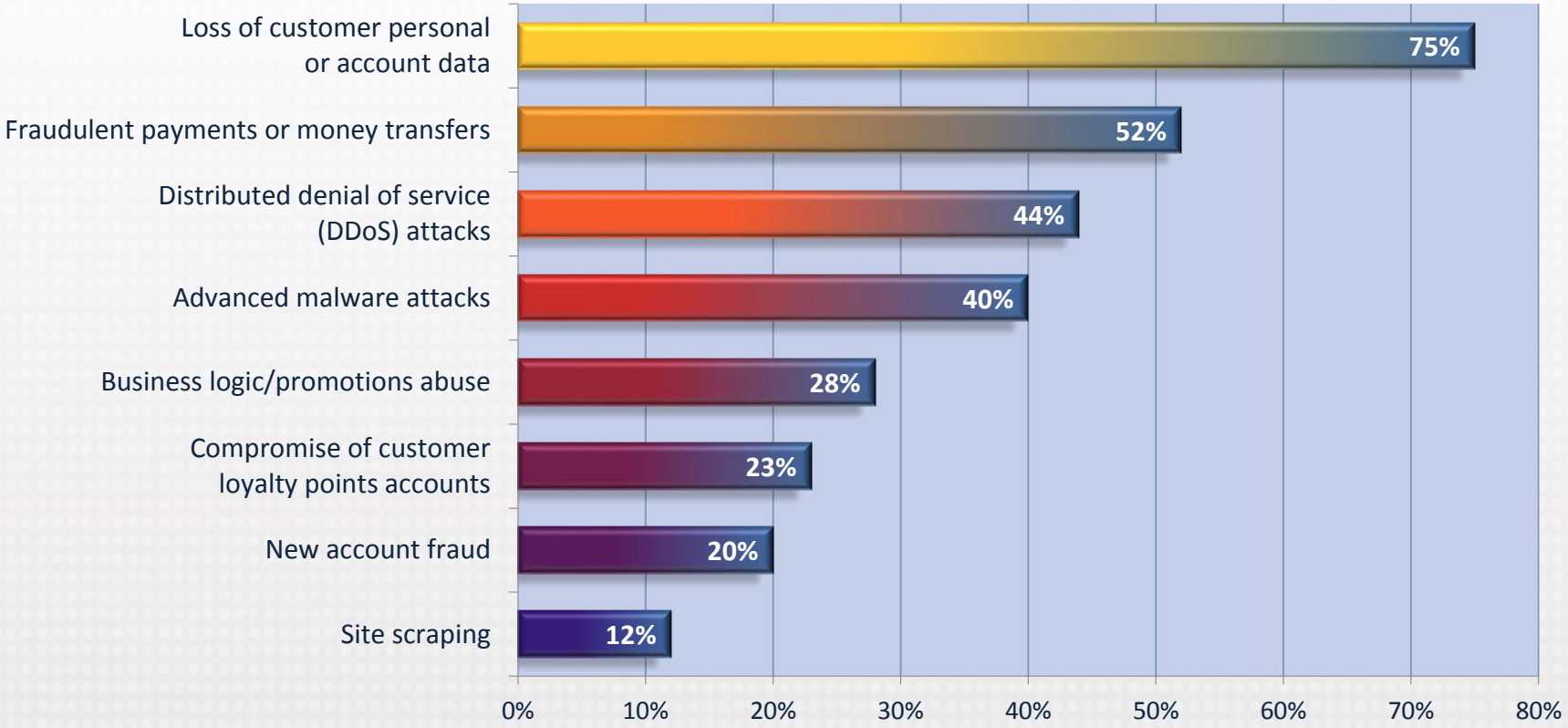
Discovering suspicious or criminal activity in mobile applications is difficult as well. *Asked how easy it is to detect fraud in mobile applications, 37% of respondents consider it challenging.*

How long does it typically take to investigate and determine the origin of fraudulent activity?



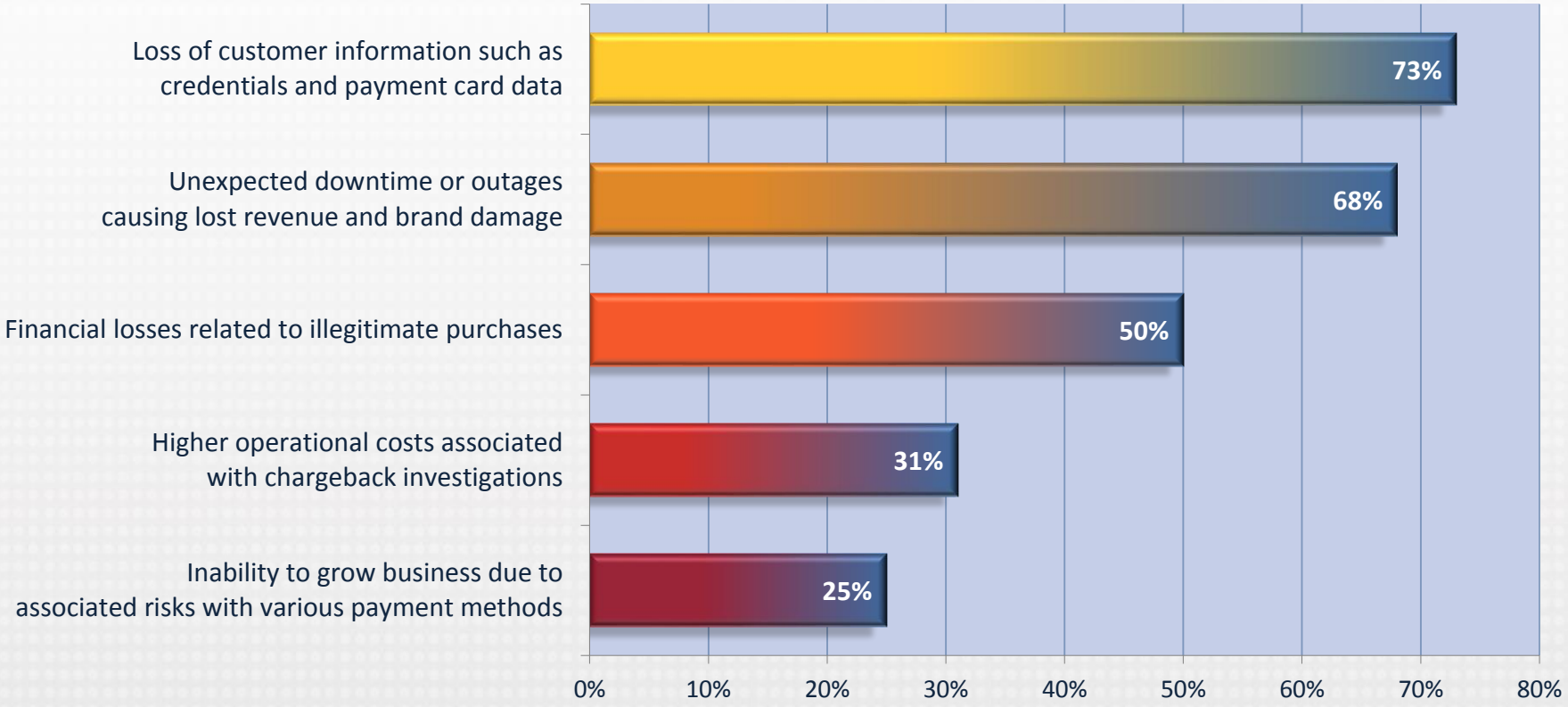
***Finding the source of a fraud takes too long**. Only 30% of respondents report they can isolate the origin of fraudulent activity within hours.*

What kinds of security threats are most detrimental to your ecommerce business?



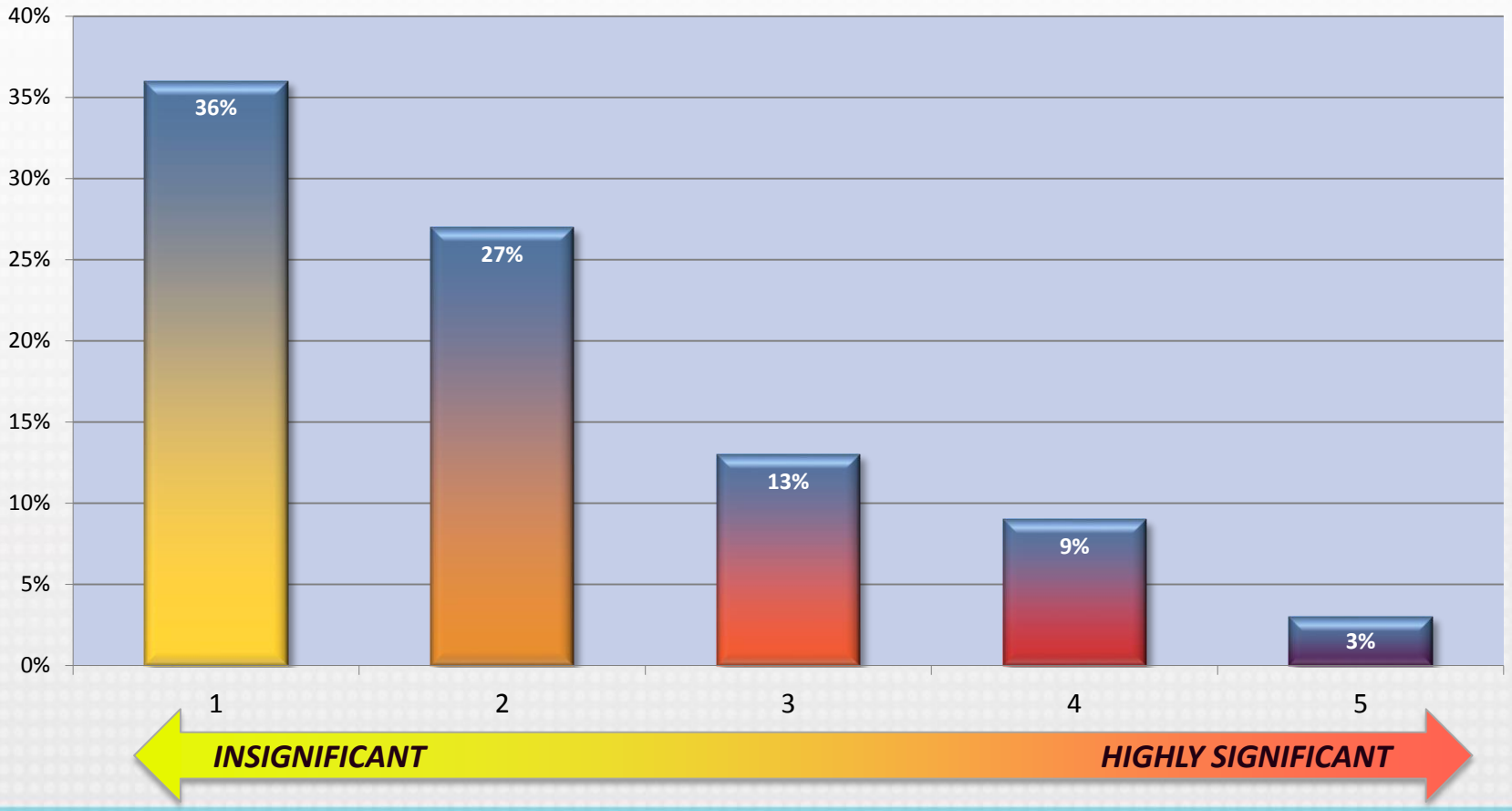
Loss of data, money, and service are the most worrisome security threats. *By a wide margin, respondents cite loss of customer data as the most detrimental security threat (75%), followed by fraudulent money activity (52%) and DDoS attacks (44%).*

What potential consequences of cyber attacks would concern you the most?



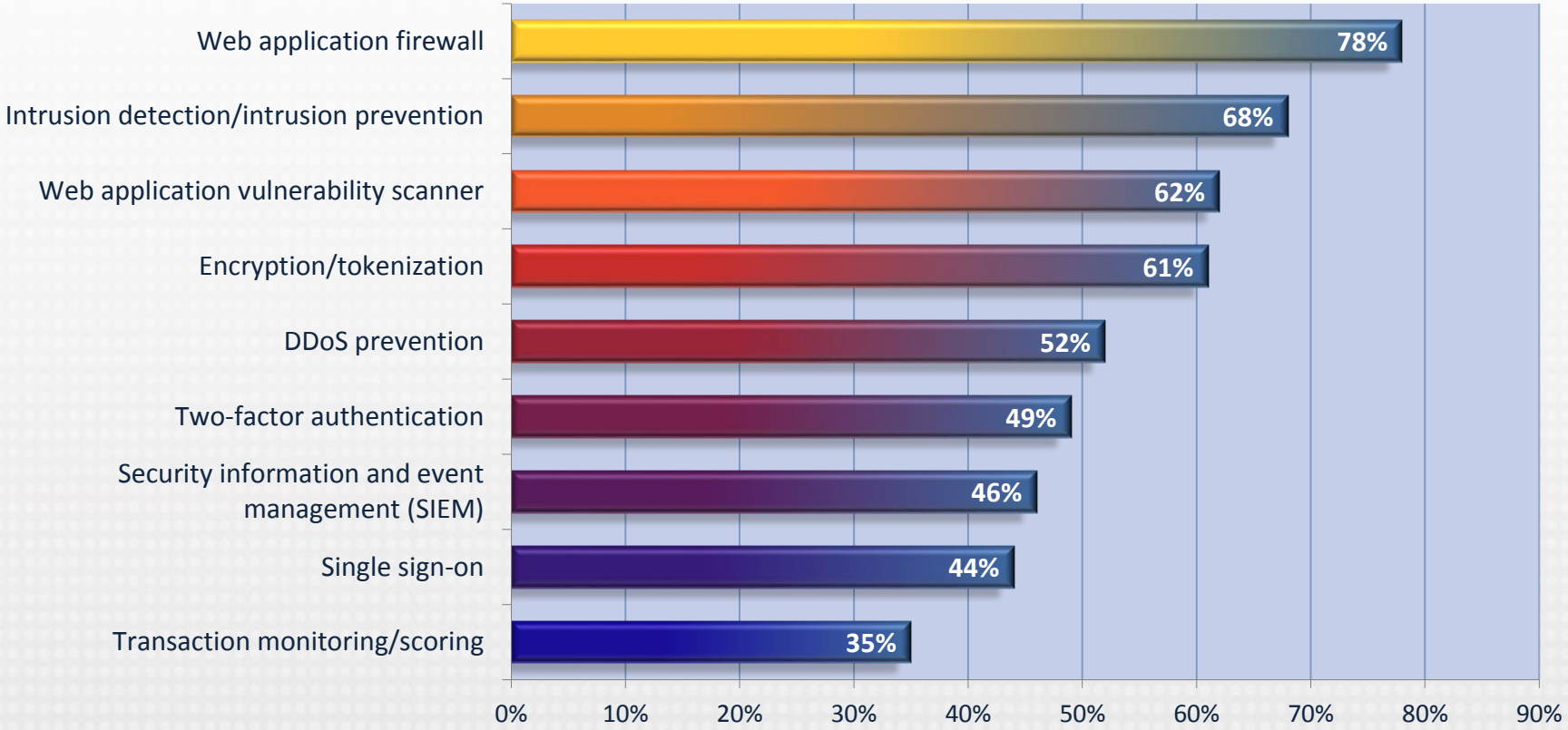
The most distressing impacts of a cyber attack: data loss, downtime. *Responders rate customer data theft the most distressing potential consequence of cyber attack (73%), followed by damage resulting from downtime or outages (68%).*

What was the overall impact of cybercrime and fraud losses on your ecommerce business last year?



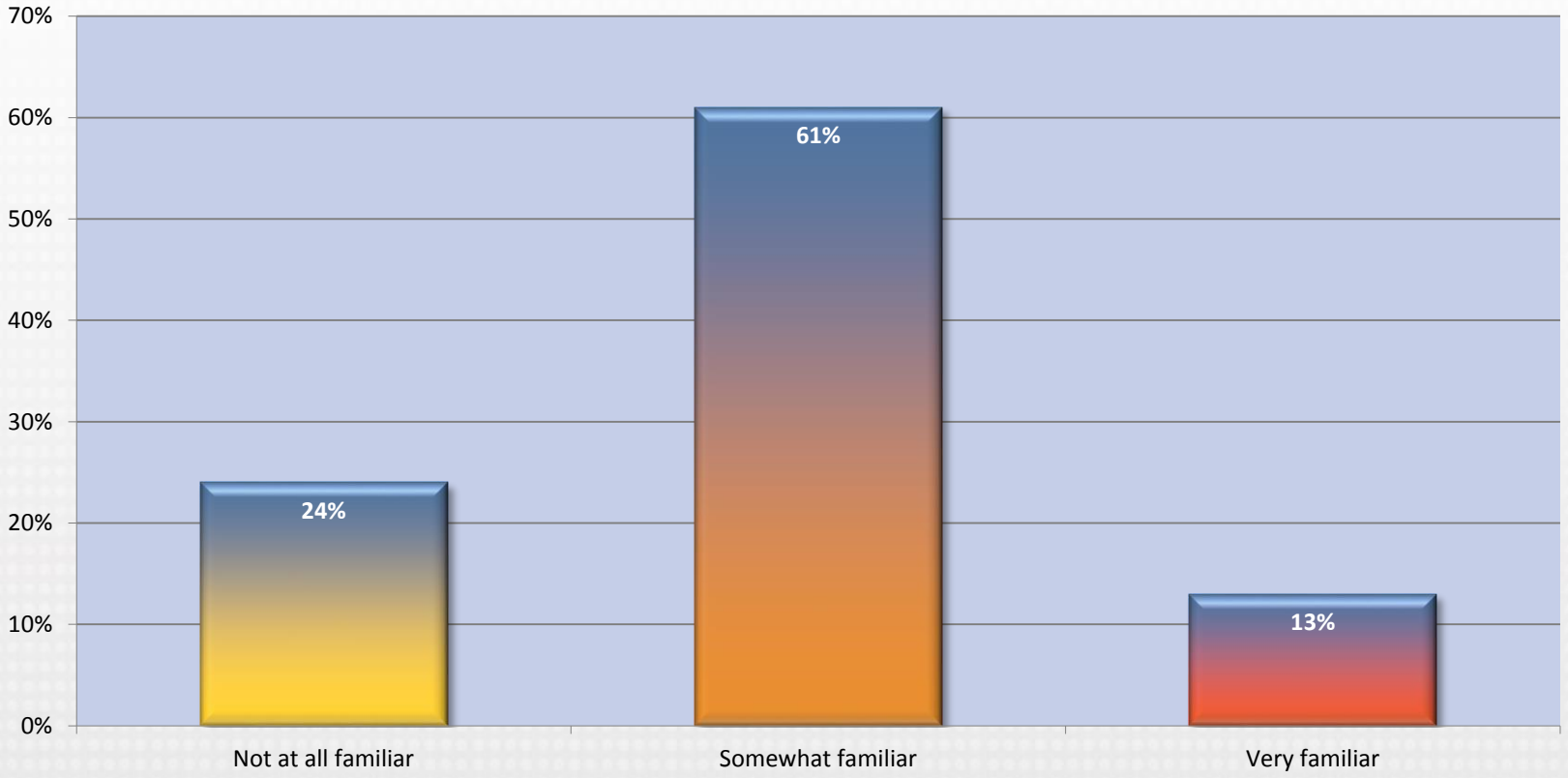
***For most, actual losses due to cybercrime are not trivial**. Just 36% of responders characterize their ecommerce cybercrime/fraud losses last year as "insignificant."*

What type of security technologies are you currently using to protect your customerfacing applications?



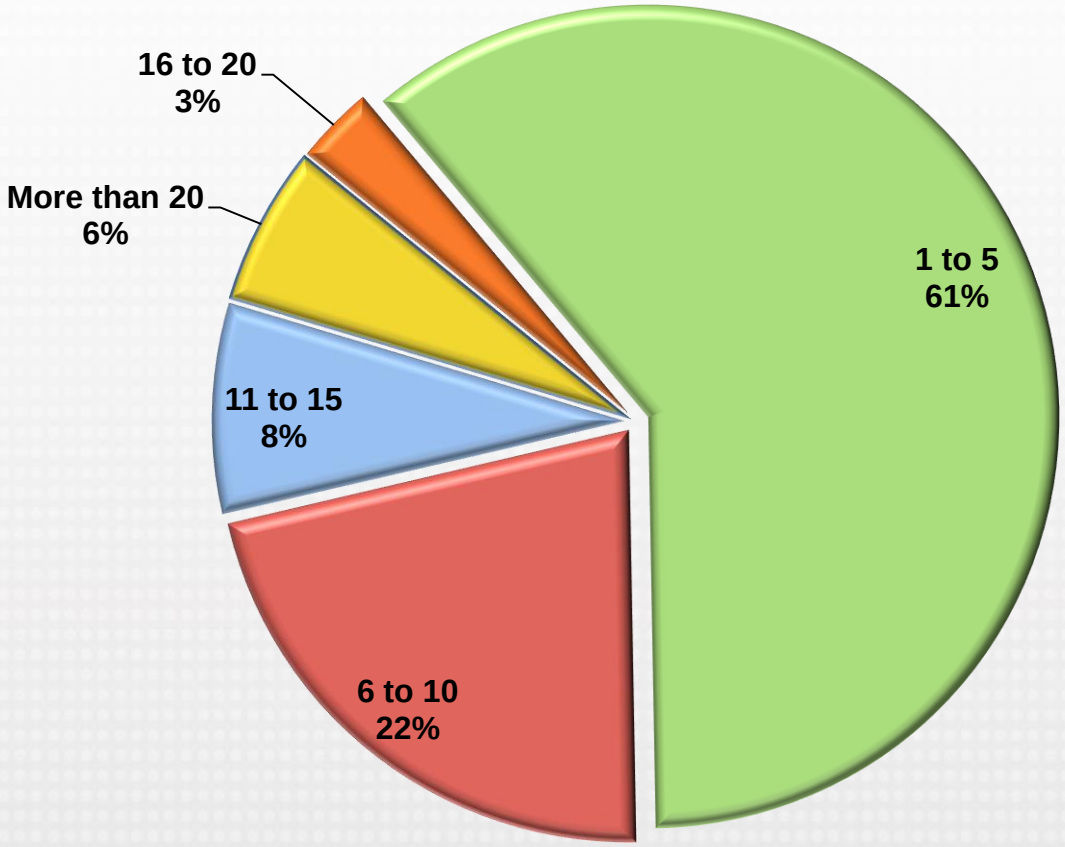
Security technology: not one solution, but many. *Asked to list technologies protecting their customer-facing applications, respondents reported using numerous and diverse strategies and solutions.*

How familiar are you with the use of web behavior analytics for detecting and investigating cyber fraud attacks?



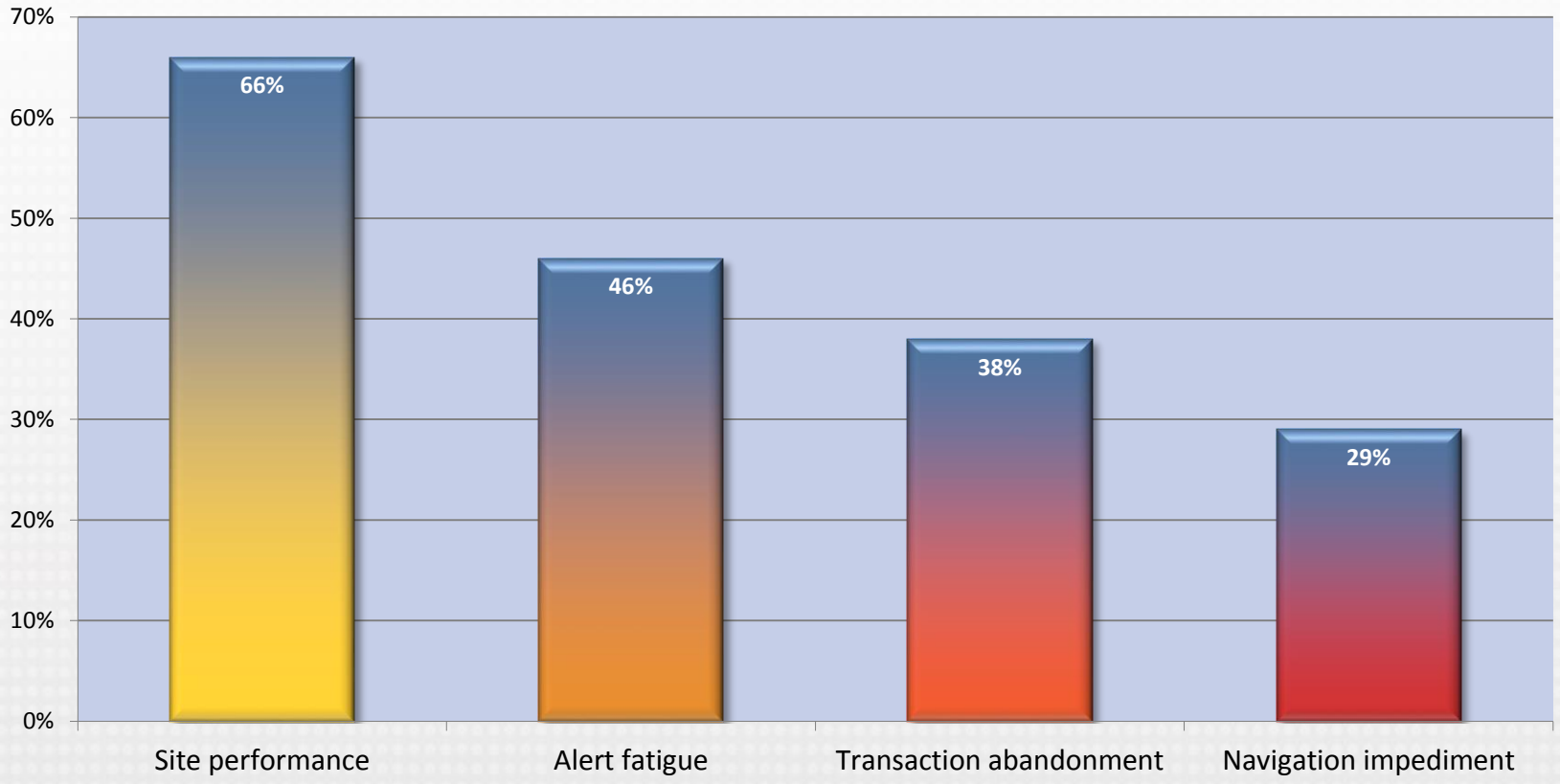
Web behavior analytics is new territory. *Only 13% of respondents report being familiar with using web behavior analytics to detect/investigate cyber attacks.*

How many people comprise your online fraud investigation team?



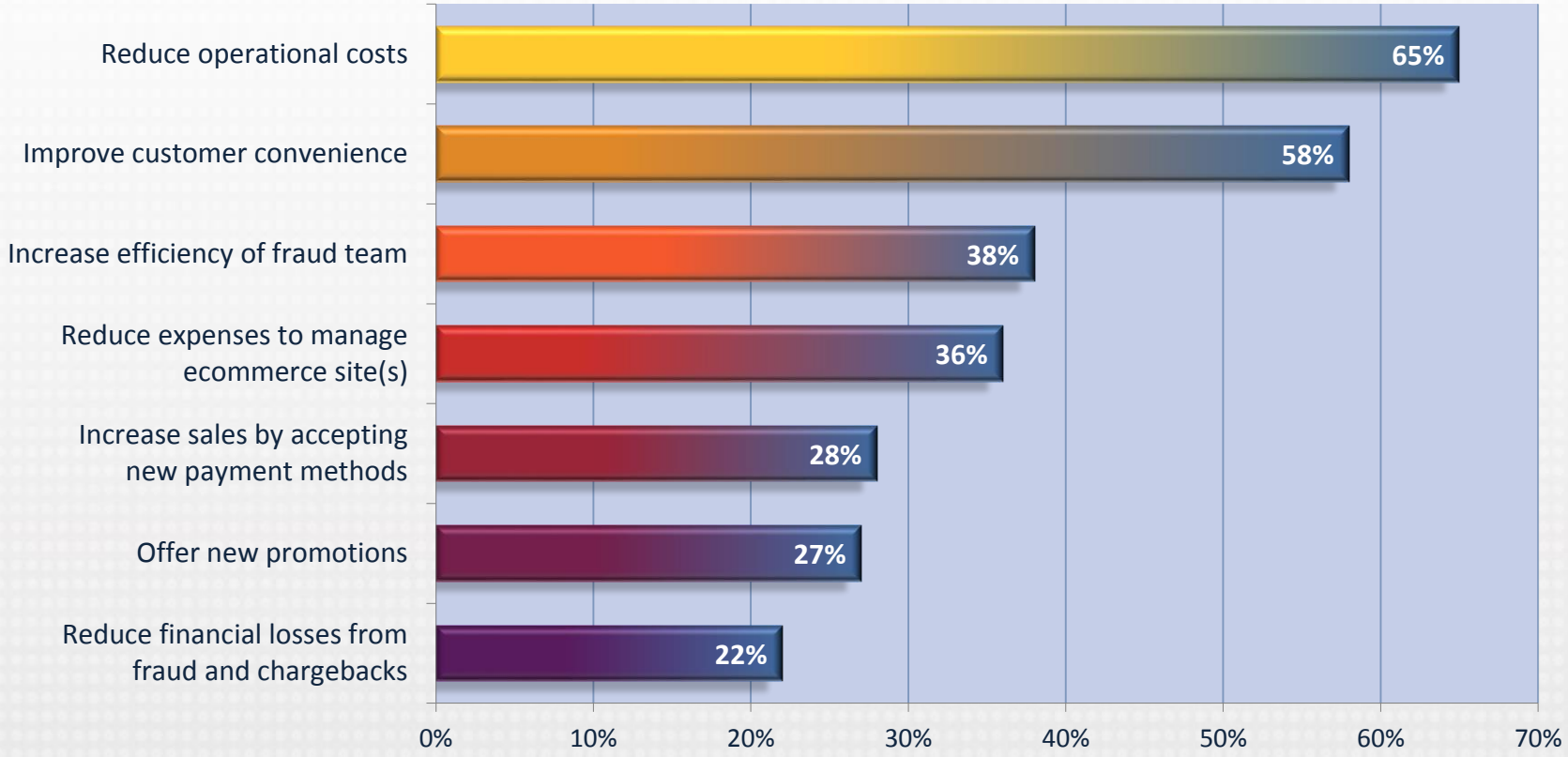
Fraud investigation: a big job often done by a small team. *61% of those surveyed report that their organization has assigned just 1-5 people to online fraud investigation.*

What concerns do you have about adding more layers of security?



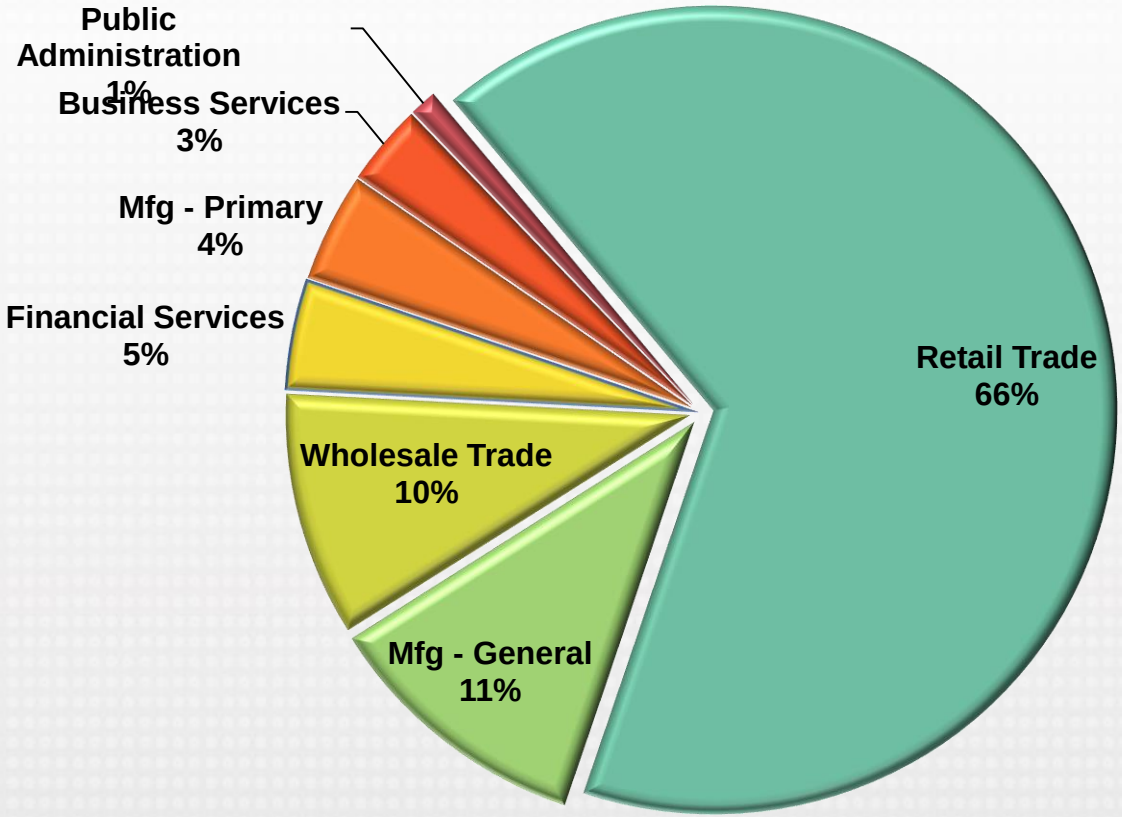
Will more security slow down our site? *66% of responders express concern that more security will affect site performance. Other concerns include "alert fatigue" (46%) and transaction abandonment (38%).*

What are your business goals in the next 12 months?



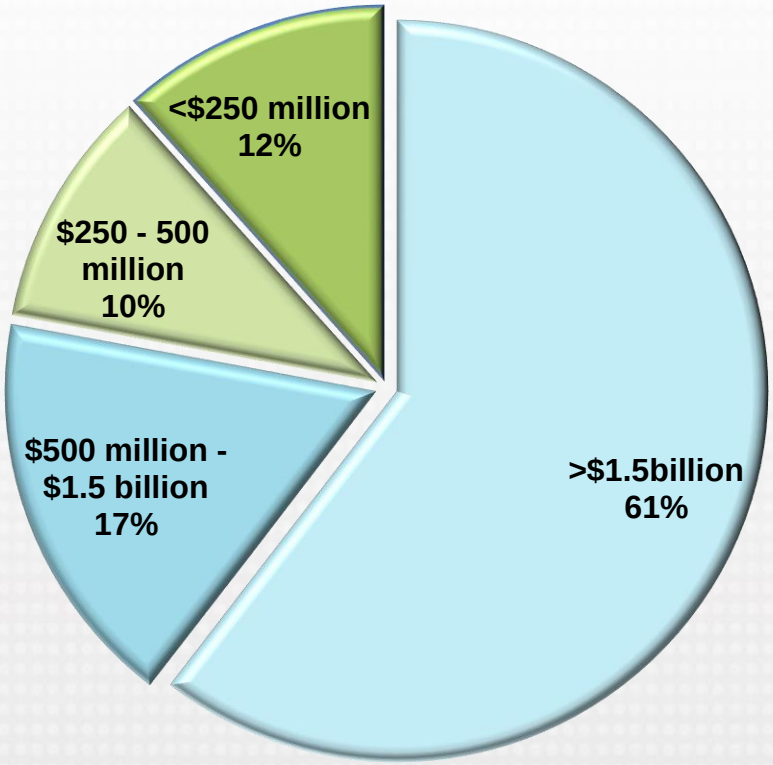
Goals: reduce cost, improve customer experience. *Predictably, top business goals responders cite over the next year include reducing operational costs (65%) and improving customer experience (58%). But increasing the efficiency of fraud teams also ranked high (38%).*

Profile of Responders: Industry Sectors



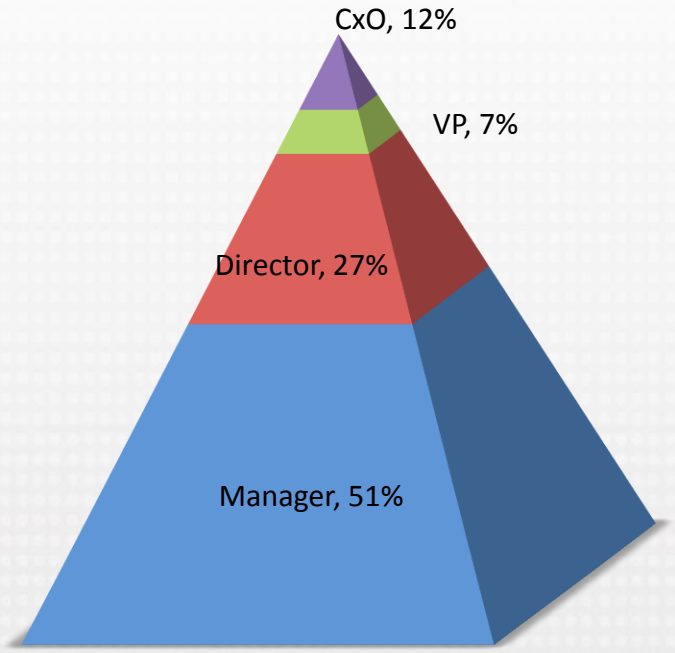
Two thirds of survey responders work in the retail trade industry.

Profile of Responders: Revenue



60% of responders work for Fortune 1000 companies with annual revenues over $1.5 billion.

Profile of Responders: Job Level



Almost half the survey responders hold executive level positions at their organizations.

RSA helps you leverage web behavior analytics to improve fraud detection and investigation in your ecommerce business.

For more information, go to www.RSA.com

Additional Resources:

Web Session Intelligence for Dummies

2016 Cybercriminal Shopping List

Request a Demo