



The Security Division of EMC

Survey Report

The 2008 Insider Threat Survey:

Workers Admit to Everyday Behavior That Puts Sensitive Business Information at Risk



Introduction

In the spring and summer of 2008, RSA, The Security Division of EMC, conducted an Insider Threat Survey among attendees at industry events in North America and Latin America. The survey polled 417 individuals – including delegates at the RSA Conference – on their work-related security behaviors and attitudes. The survey respondents were employees, contractors, partners, visitors and consultants who have physical and/or logical access to organizational assets.

These individuals worked across a range of industries, with a heavy concentration within the financial and technology sectors. Almost half of the respondents' job functions were within information technology. During an era of well-publicized data breaches, the results indicated that perhaps even those who should know better are not exempt from the everyday behaviors that can trigger significant risk to sensitive business information.

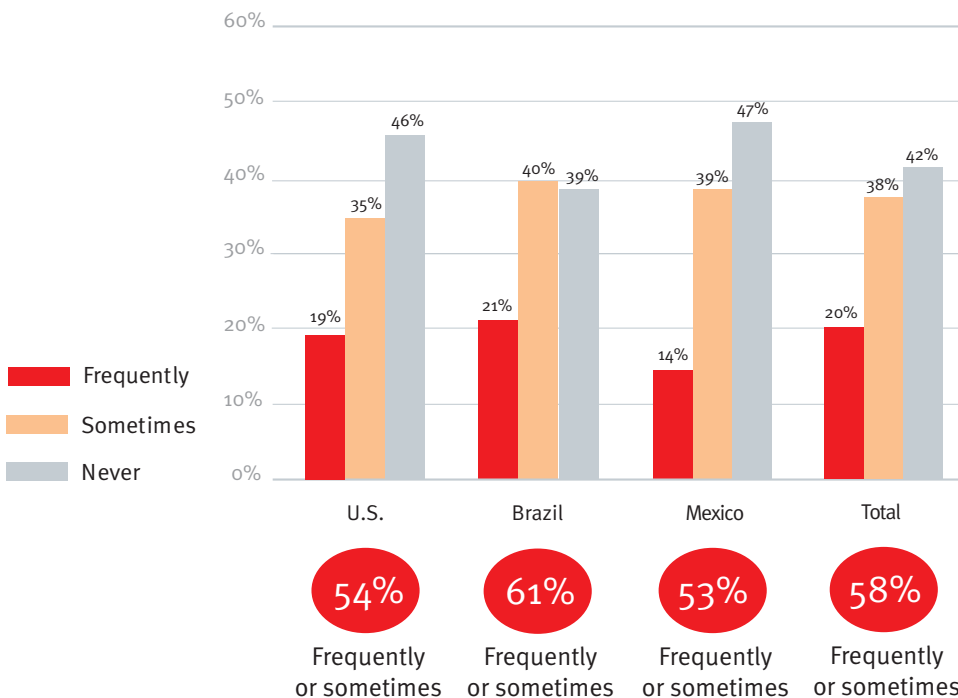
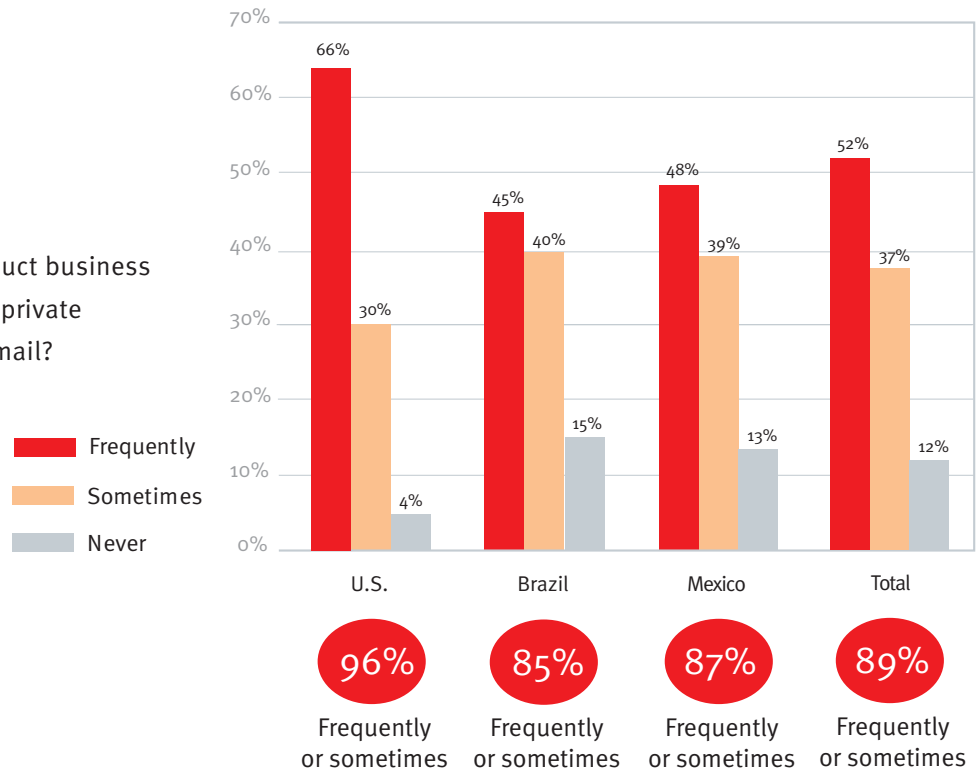
The survey also revealed that it is as important for businesses to diligently enforce information security controls and policies focused on protecting the everyday actions of well-meaning insiders as it is to enforce those designed to defend against those with malicious intent. Corporate assets held at risk through unwitting workers' habits include customer information, financial reports and intellectual property, in addition to personally-identifiable information such as Social Security numbers and credit card data.

The 2008 Insider Threat Survey was taken by 417 attendees at three industry events in three countries within North America and Latin America:

- RSA Conference U.S. (April 7-11, 2008; 134 respondents)
- Demystifying the Payment Card Industry Standard: Routes to PCI Compliance, Mexico City (May 28, 2008; 44 respondents)
- CIAB 2008 Brazil (June 11-13, 2008; 239 respondents)

Q

How often do you conduct business remotely over a virtual private network (VPN) or web mail?

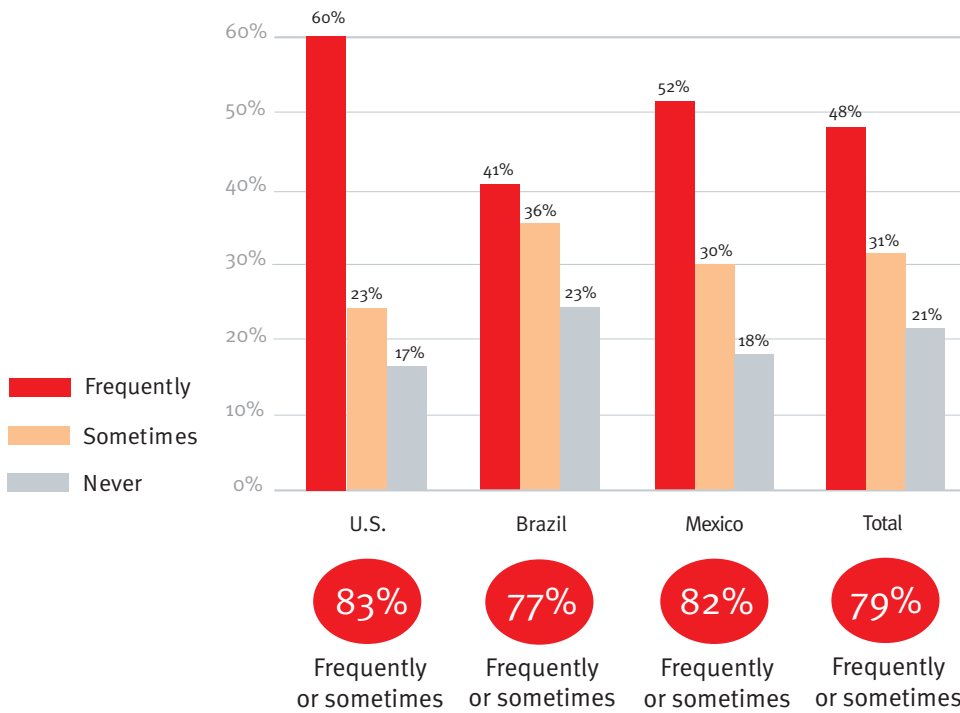
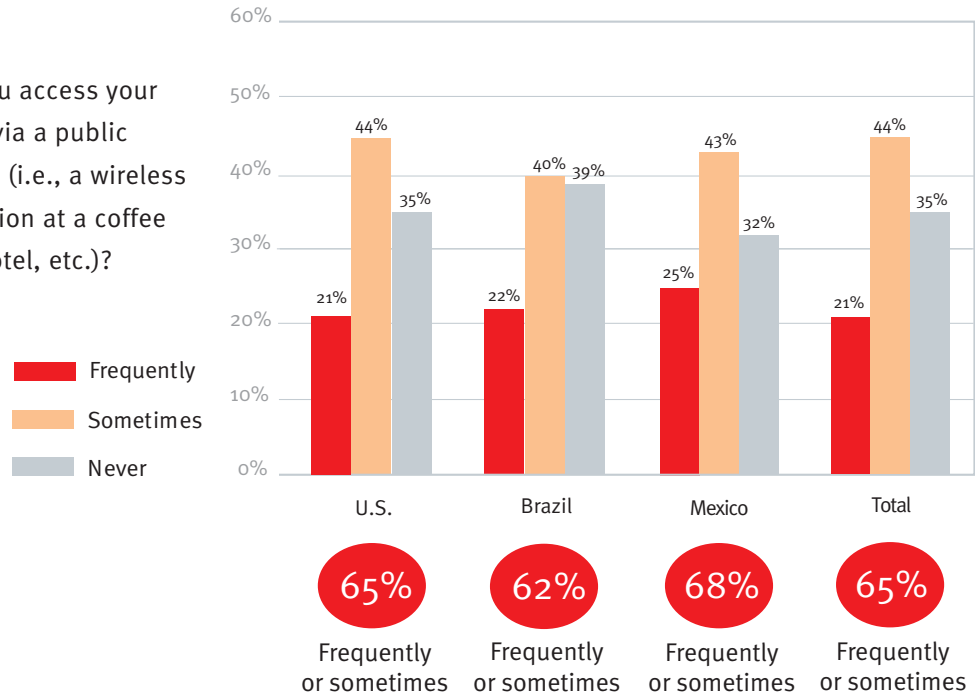


Q

How often do you access your business email via a public computer (i.e., a computer at an Internet café, airport kiosk, hotel, etc.)?

Q

How often do you access your business email via a public wireless hotspot (i.e., a wireless Internet connection at a coffee shop, airport, hotel, etc.)?



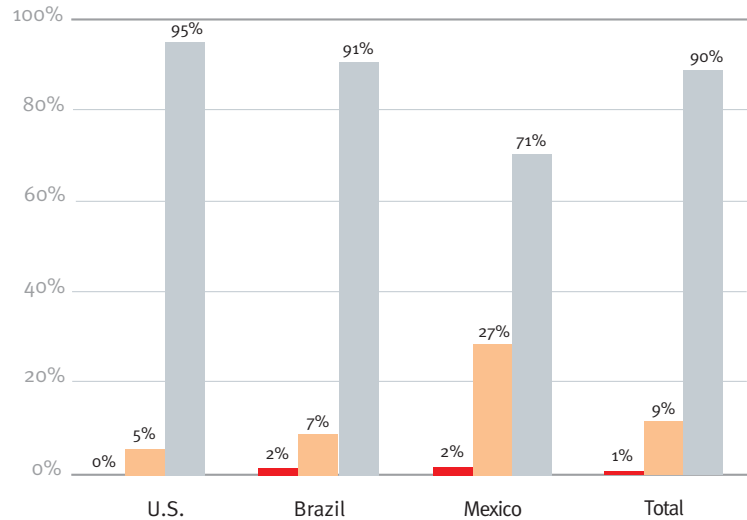
Q

How often do you leave your business carrying a mobile device such as a laptop, smartphone and/or USB flash drive which holds sensitive information related to your job (i.e., customer data, personally identifiable information, company financial, credit card data, competitively sensitive information such as product plans?)

Q

Have you ever lost a laptop, smartphone and/or USB flash drive with corporate information on it?

Frequently
Sometimes
Never

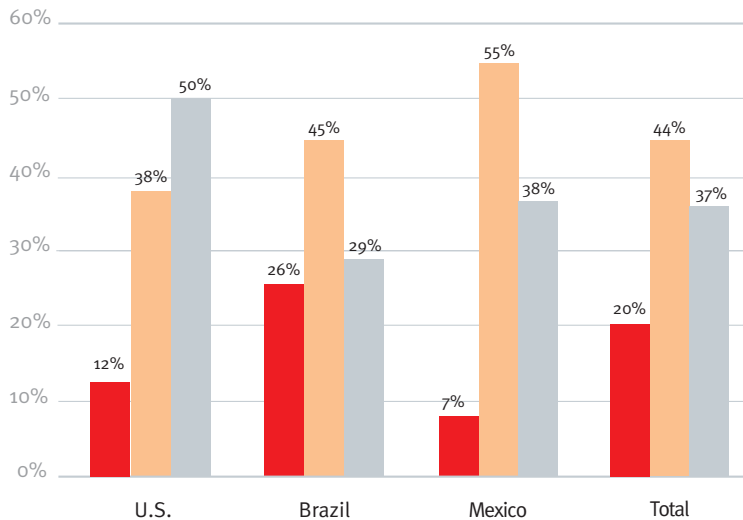


5%
Frequently or sometimes

9%
Frequently or sometimes

29%
Frequently or sometimes

10%
Frequently or sometimes



Frequently
Sometimes
Never

50%
Frequently or sometimes

71%
Frequently or sometimes

62%
Frequently or sometimes

64%
Frequently or sometimes

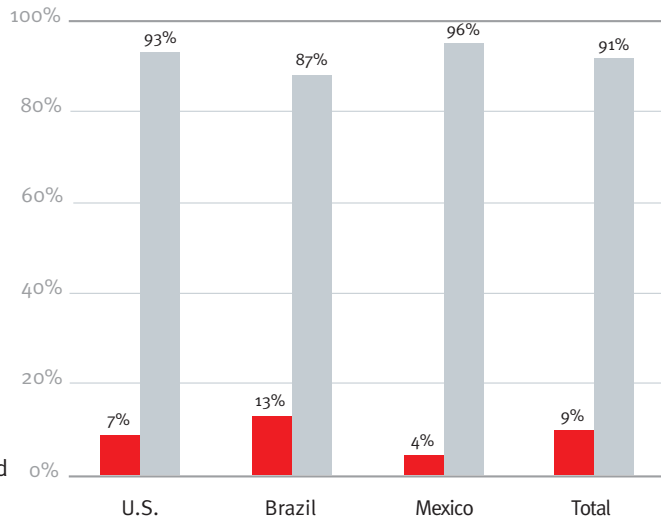
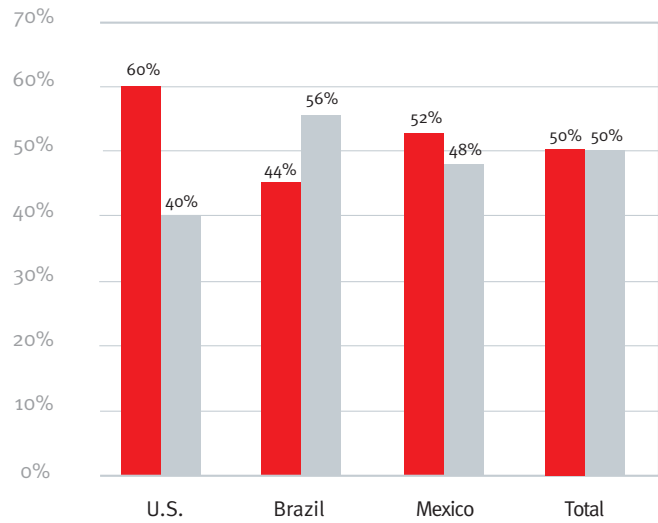
Q

How often do you send business documents to your personal email address so that you can access them from home?

Q

Does your company provide a wireless network internally for use in conference rooms and guest offices?

Yes
No



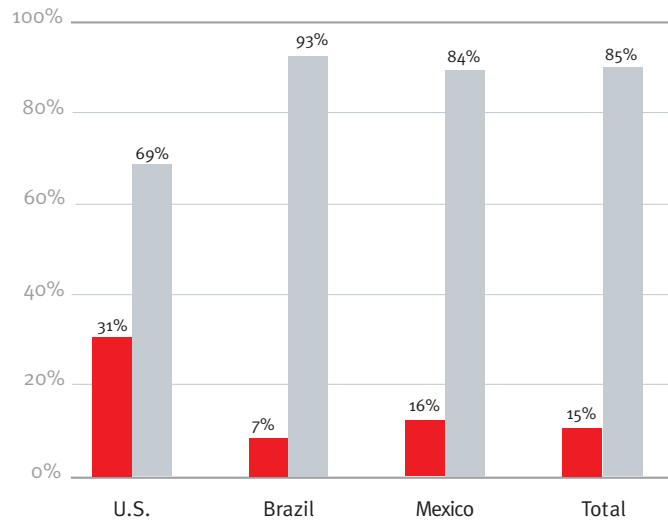
Q

If yes, does the wireless network require a login, or is it open?

Q

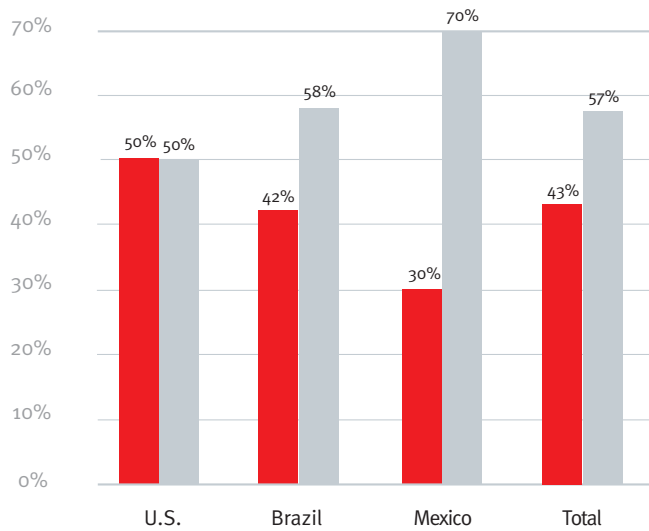
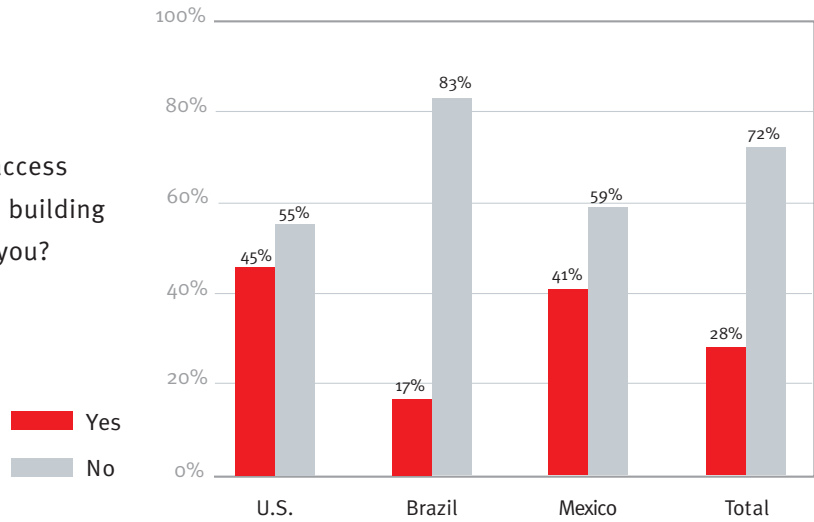
Have you ever held a secured door open for someone at work who you didn't recognize?

Yes
No



Q

Have you ever forgotten your access card/key and been let into the building by someone who didn't know you?



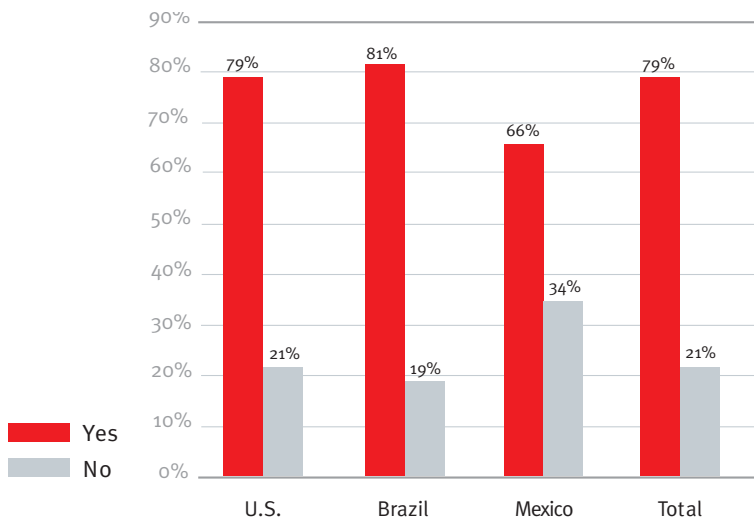
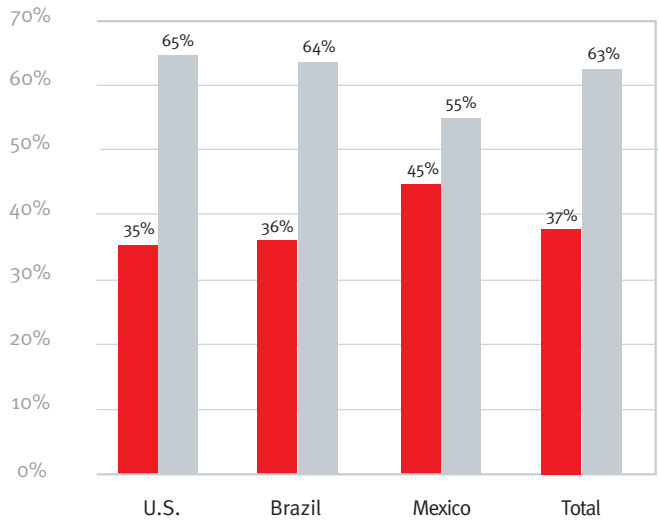
Q

Have you switched jobs internally and still had access to accounts/resources which you no longer need?

Q

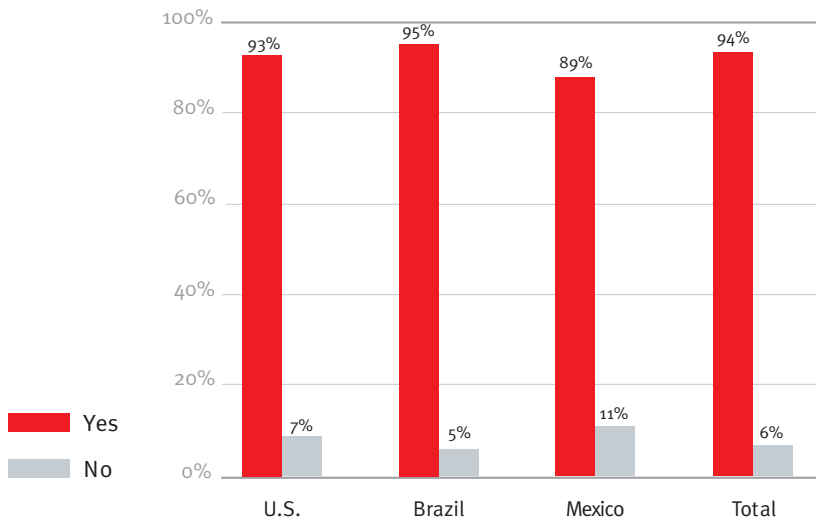
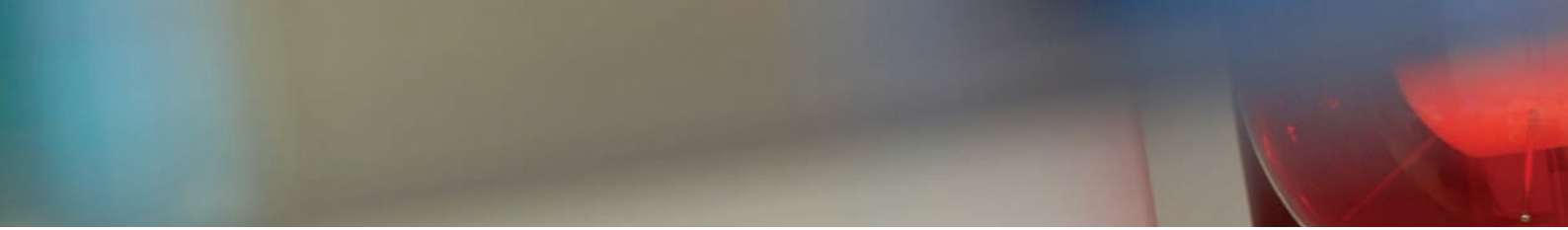
Have you ever stumbled into an area of your corporate network to which you believe you should not have had access?

Yes
No



Q

Does your company employ temporary workers and/or contractors who require access to company information and systems?



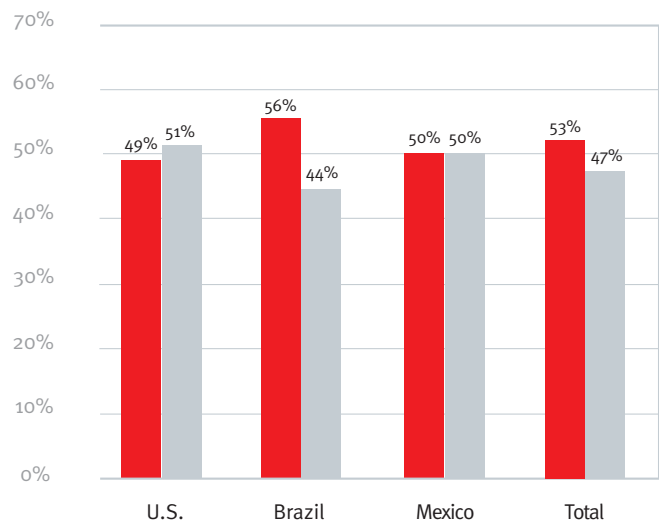
Q

Are you familiar with the IT security policies of your company?

Q

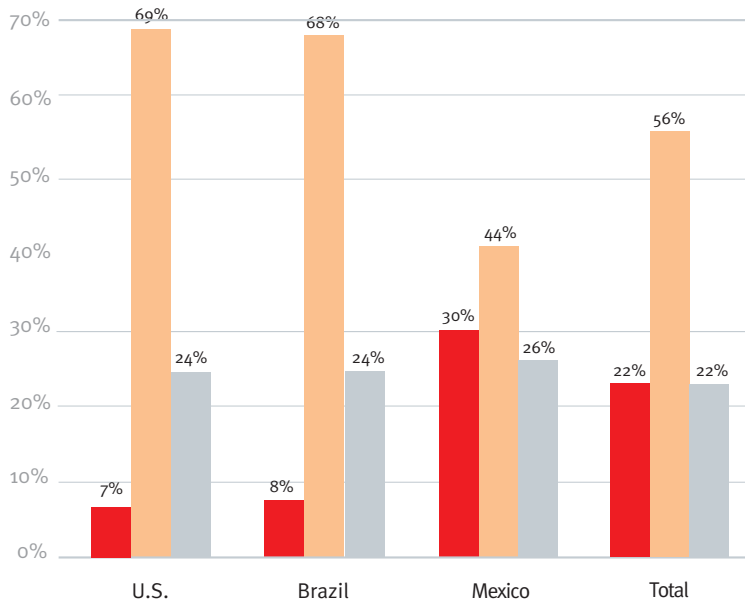
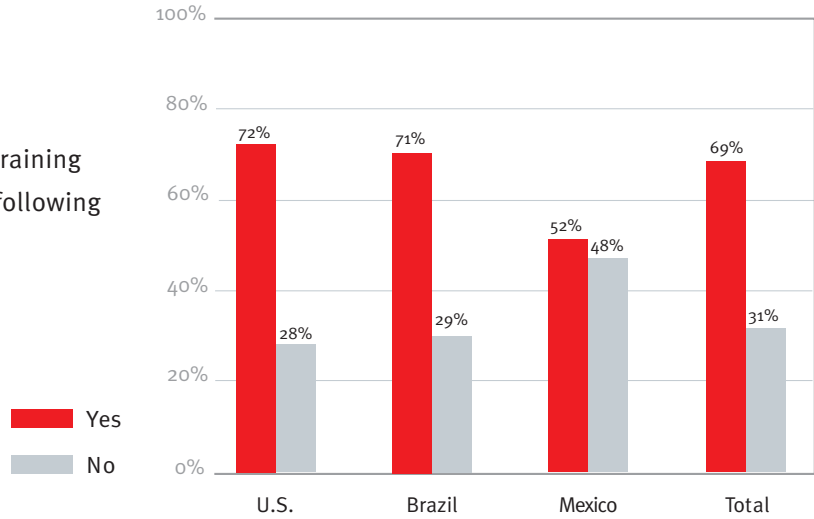
Do you ever feel you need to work around your company's established security policies and procedures just to get your job done?

Yes
No

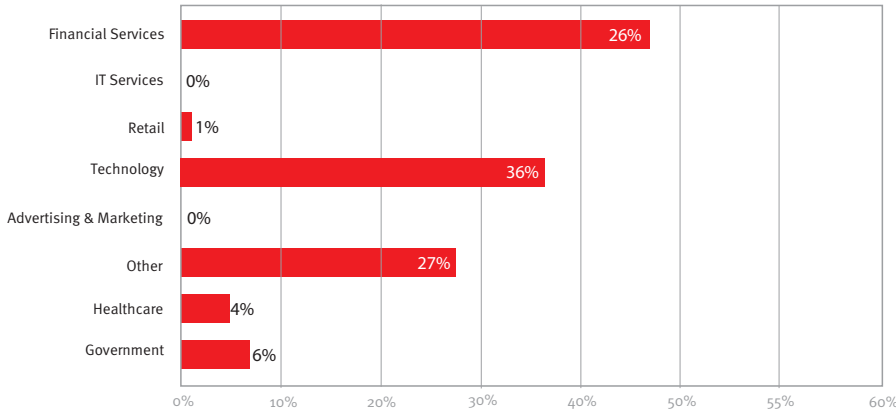




Does your company provide training about the importance of the following security best practices?



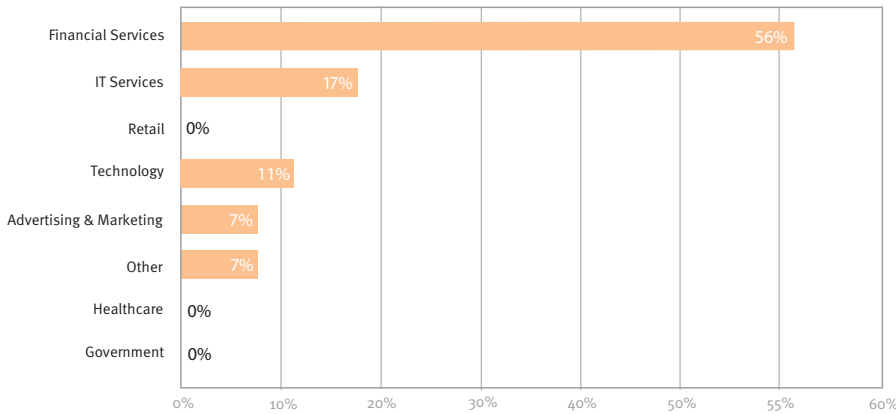
Do you believe security is an IT department issue or an employee issue?



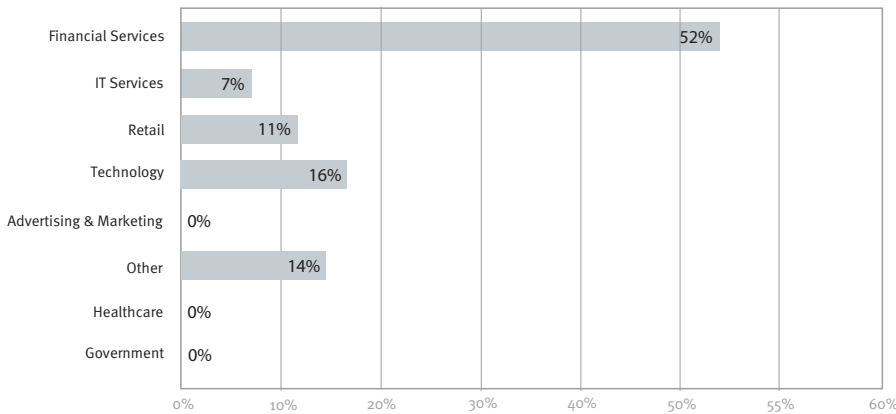
The Respondents

Key:

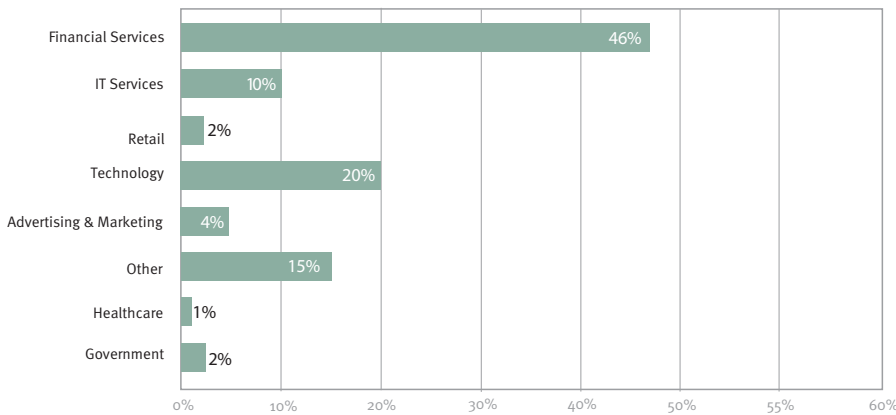
- US = RSA Conference US
- Mexico = Demystifying the Payment Card Industry Standard: Routes to PCI Compliance, Mexico City
- Brazil = CIAB 2008 Brazil



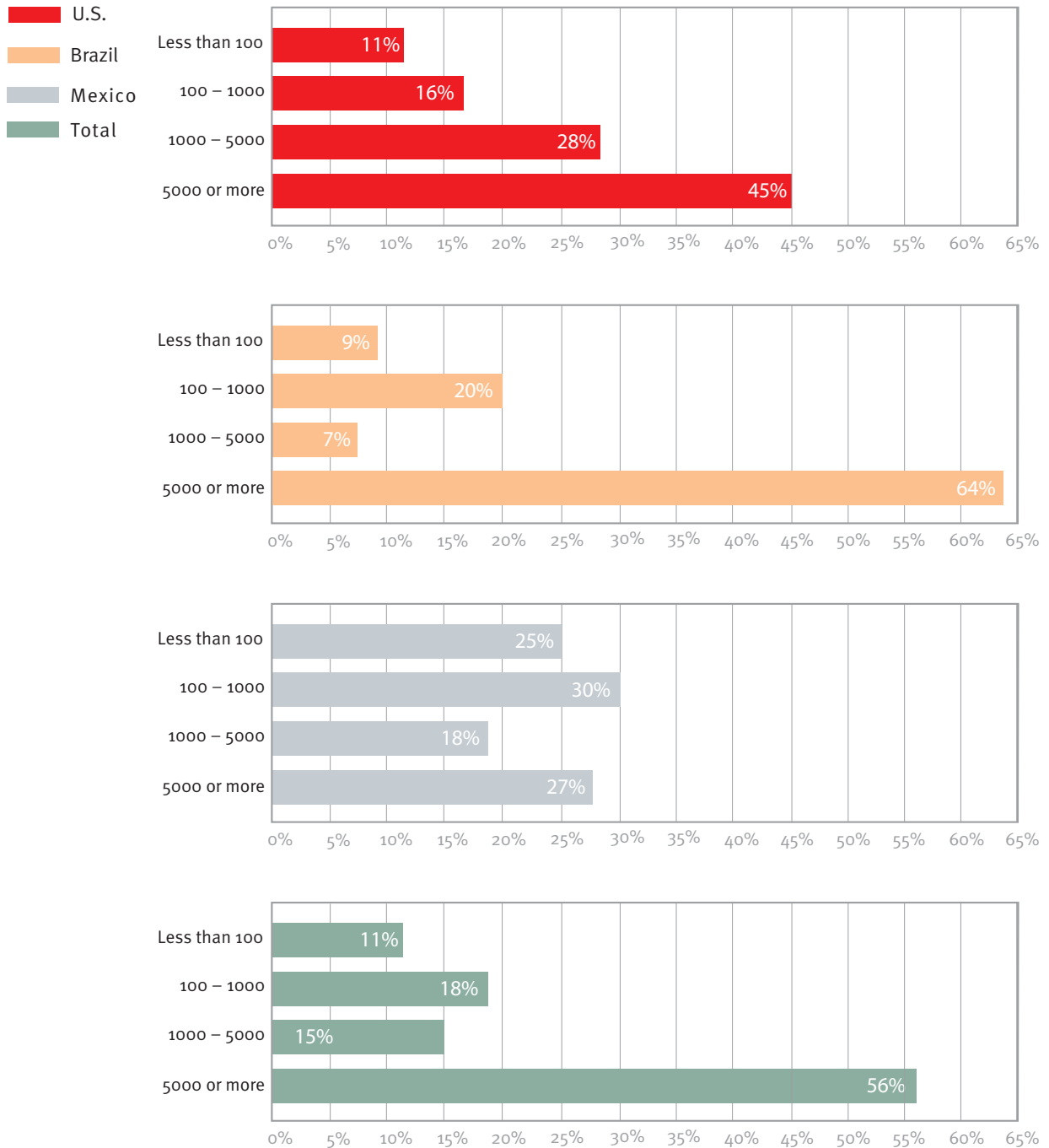
What type of company/ organization do you work for? (total respondents)

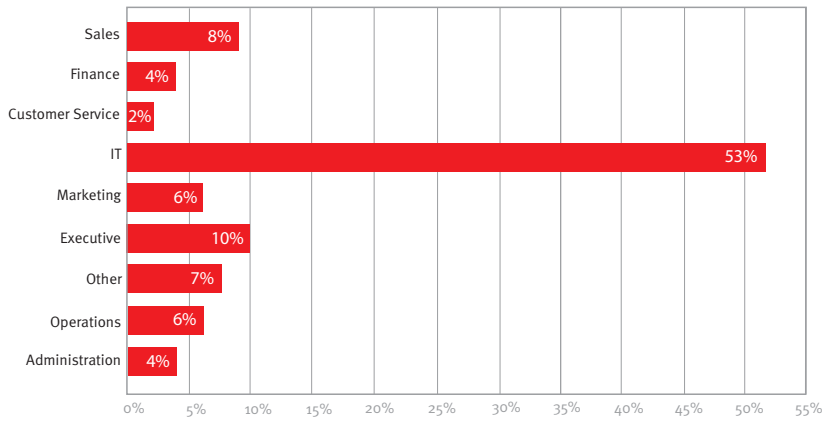


- U.S.
- Brazil
- Mexico
- Total

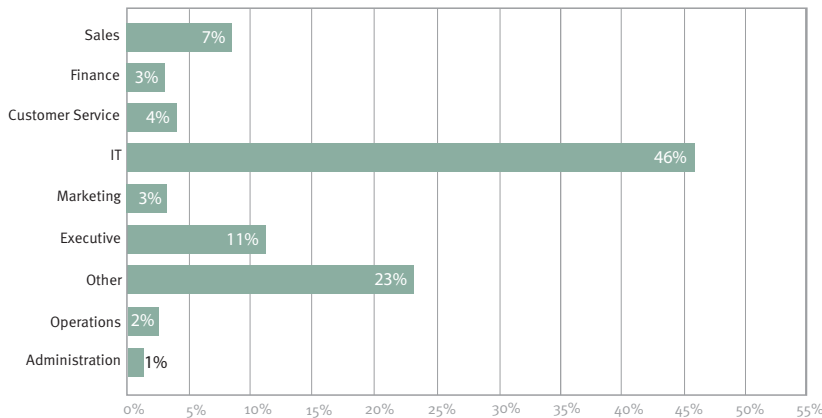
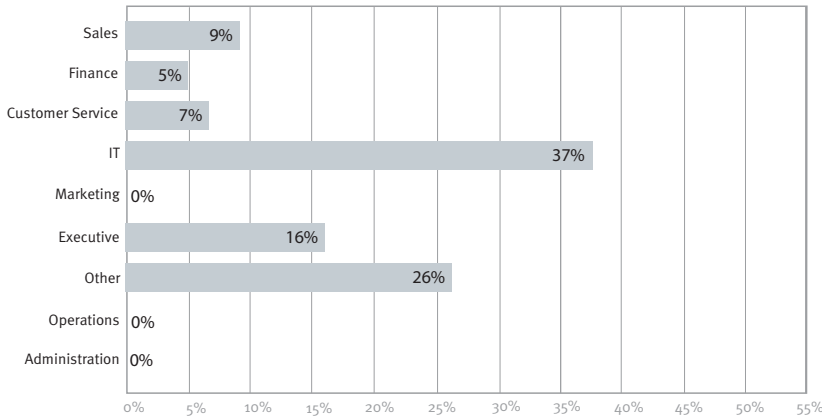
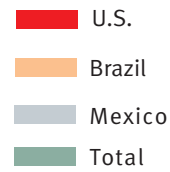
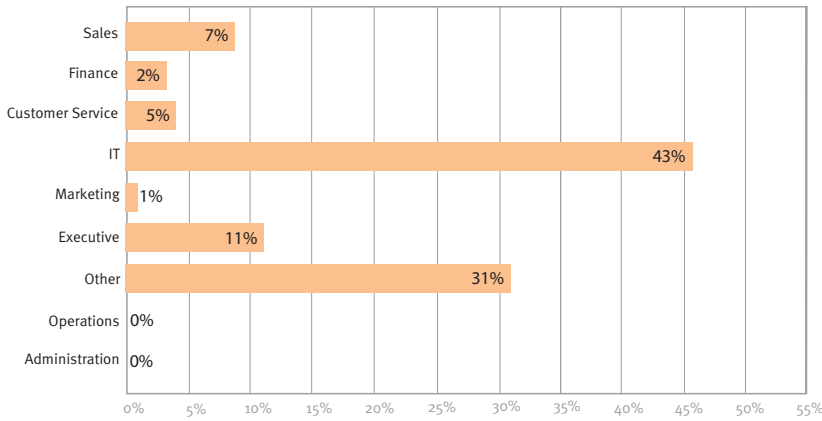


What size company/ organization do you work for? (total respondents)





What is your job function?
(total respondents)



Recommendations for Mitigating Insider Risk

The survey reveals that it is as important for businesses to diligently enforce information security controls and policies focused on protecting the everyday actions of well-meaning, innocent insiders – as it is to enforce those designed to defend against those with malicious intent. A holistic, information-centric security strategy takes people, process and technology into account and has a feedback mechanism. It is not enough to establish policy; actual insider behavior must be measured and tracked against established policy in order to keep security aligned with the business and in turn, to minimize information risk and maximize reward.

RSA advises that businesses to take a layered approach to security to help mitigate the insider threat and keep data safe. As such, it is important for any organization to know:

- Where sensitive information lives, how to measure its level of risk, and apply data security controls to protect it
- Who has access to sensitive information and how to control access to it through policy, based on entitlements and roles
- Monitor for suspicious activity to verify user identities
- Transform real-time event data into actionable compliance and security intelligence

People do as they will, regardless of awareness of best security practices

The results of the survey show that employees are well aware of the restrictions placed upon them by their corporate IT departments, yet many often work around these controls in order to get their jobs done in a convenient and timely manner. When trusted insiders work around security policies, sensitive data can be exposed that places businesses and their customers – often consumers – at unnecessary risk. Organizations can greatly mitigate this risk by developing information-centric security policies that acknowledge and align with the needs and realities of the business. This can help guard the integrity and confidentiality of information throughout its lifecycle—no matter where it moves, who accesses it or how it is used. In tandem, organizations should build-in more convenient, invisible, and layered security technologies that can reduce the factors that cause employees to break the rules and defeat their own company’s security policies.

Remote access to sensitive information: random and unprotected

In a mobile world, the survey affirms that employees depend on remote access to corporate information when outside the office, whether at home or in public places. Remote access to sensitive data requires stronger forms of authentication than a simple, static and vulnerable combination of a username and password. To help solve this problem, organizations can maintain the flexibility and convenience of remote access to VPNs and webmail by providing one-time passwords via a hardware token, or a software token that is easily accessible on mobile devices such as BlackBerry® smartphones.

Information can be a moving target – and portable data is regularly mishandled

The survey findings show that, in order for employees to be most productive, information has to be free to move. However, employee mobility increases the collective responsibility of protecting the information that is carried outside of the organization. While mobility is essential to business agility, unprotected information – wherever it is kept or stored – increases risk. A policy-based approach to securing data helps to enable organizations to classify their sensitive data, discover that data across the enterprise, enforce controls, and report and audit to ensure compliance with policy.

Making sure the right users have access to the right information

Organizations are dynamic and individuals’ roles often change within the organization – be it an employee’s internal move to a different job function or an outside consultant who moves on after the completion of an engagement. However, the governance of the corporate network does not always stay in lockstep with these moves. Access to highly sensitive data should be granted only to those who need it, and in some job functions access to only very specific areas within the information infrastructure are necessary. Organizations can manage large numbers of users while enforcing a centralized role-based security policy that ensures compliance, protects enterprise resources from unauthorized access and makes it easier for legitimate users to do their jobs.

RSA is a registered trademark or trademark of RSA Security, Inc. in the U.S. and/or other countries. EMC is a registered trademark of EMC Corporation. The BlackBerry and RIM families of related marks, images and symbols are the exclusive properties and trademarks of Research In Motion Limited.

CSURV2 WP 1008



The Security Division of EMC

RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

About RSA

RSA, The Security Division of EMC, is the premier provider of security solutions for business acceleration, helping the world's leading organizations succeed by solving their most complex and sensitive security challenges. RSA's information-centric approach to security guards the integrity and confidentiality of information throughout its lifecycle – no matter where it moves, who accesses it or how it is used.

RSA offers industry-leading solutions in identity assurance & access control, data loss prevention, encryption & key management, compliance & security information management and fraud protection. These solutions bring trust to millions of user identities, the transactions that they perform, and the data that is generated. For more information, please visit www.RSA.com and www.EMC.com.