



The Security Division of EMC

Survey Report

**The Confessions Survey:
Office Workers Reveal Everyday
Behavior That Places Sensitive
Information at Risk**



Introduction

In November 2007, RSA, The Security Division of EMC, conducted a person-on-the-street survey of government and corporate office workers in Boston and Washington, D.C. to gather anonymous self-reports of work-related security behaviors and attitudes. The results provide a snapshot of the everyday actions of trusted insiders who have access to sensitive data such as customer information, Social Security numbers, credit card data, company financials and intellectual property.

The findings of the survey underscore that the threat posed to data by well-meaning insiders – employees, contractors, suppliers, partners, visitors and consultants who have physical and/or logical access to organizational assets – greatly broadens that posed by malicious insiders who deliberately leak sensitive data for personal financial gain or

other criminal purposes. These "innocent" insiders can unwittingly initiate data exposures of extraordinary scope and cost through their ordinary, everyday behavior, whether through carelessness, working around security measures or following inadequate security policies.

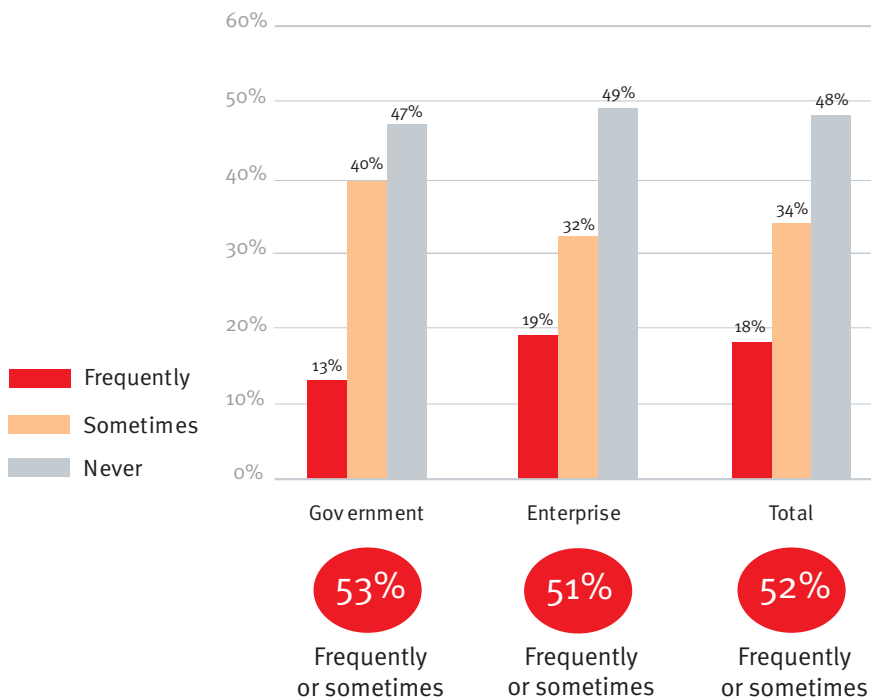
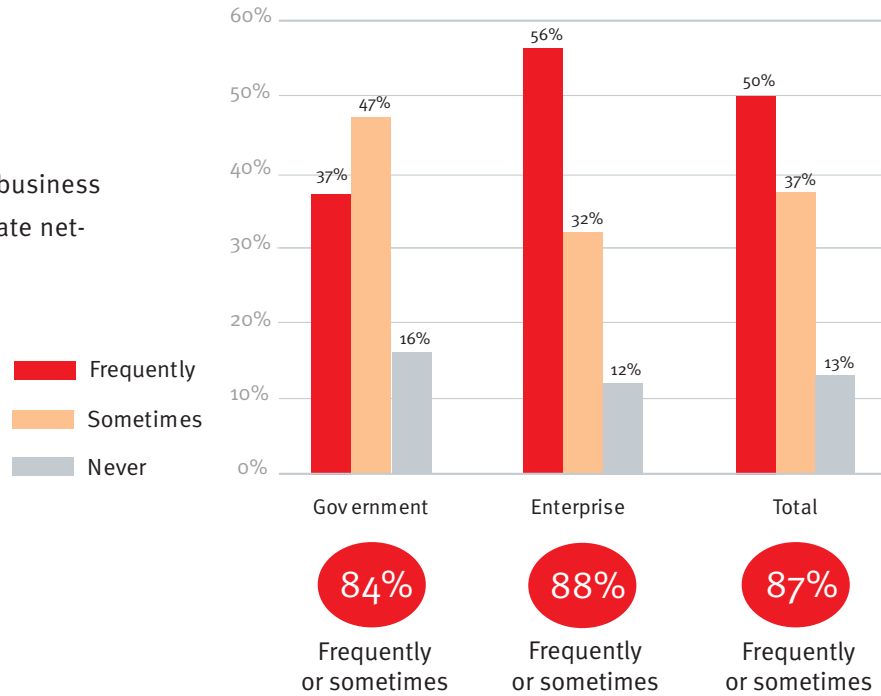
Organizations must understand the types of information their employees and other insiders need to access, determine the sensitivity of that information and then protect it with security measures commensurate with the associated risk. Well-protected information is an asset that gives individual workers and organizations the confidence to achieve more. Read on for the full survey findings and recommended measures for reducing information risk.

Media and Analyst Inquiries

If you would like to speak with an RSA executive about the survey findings and recommendations, please contact Jessica Hawks at jessica.hawks@rsa.com or +1 781 515 6067 to arrange a conversation.



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

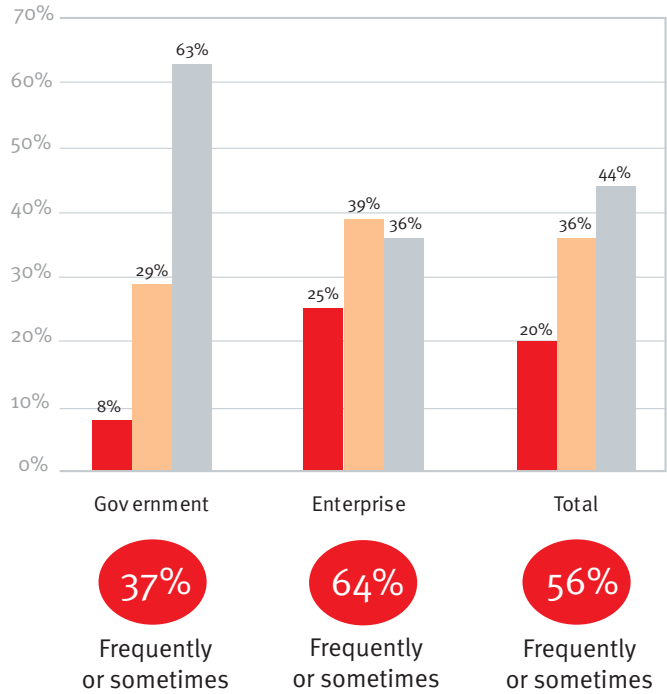


How often do you access your work e-mail via a public computer (i.e., a computer at an Internet café, airport kiosk, hotel, etc.)?

Q

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

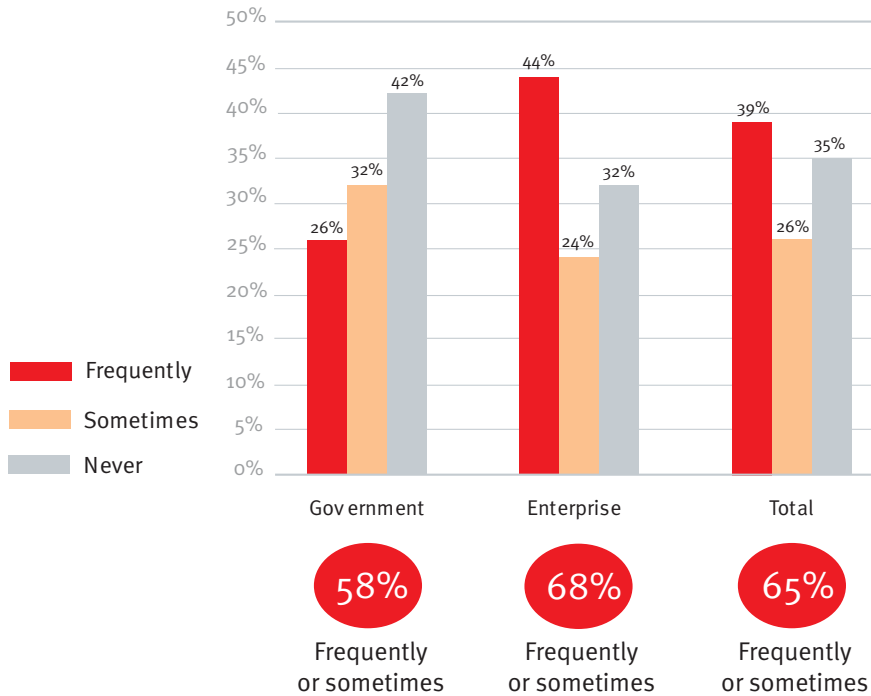
█ Frequently
█ Sometimes
█ Never



Q

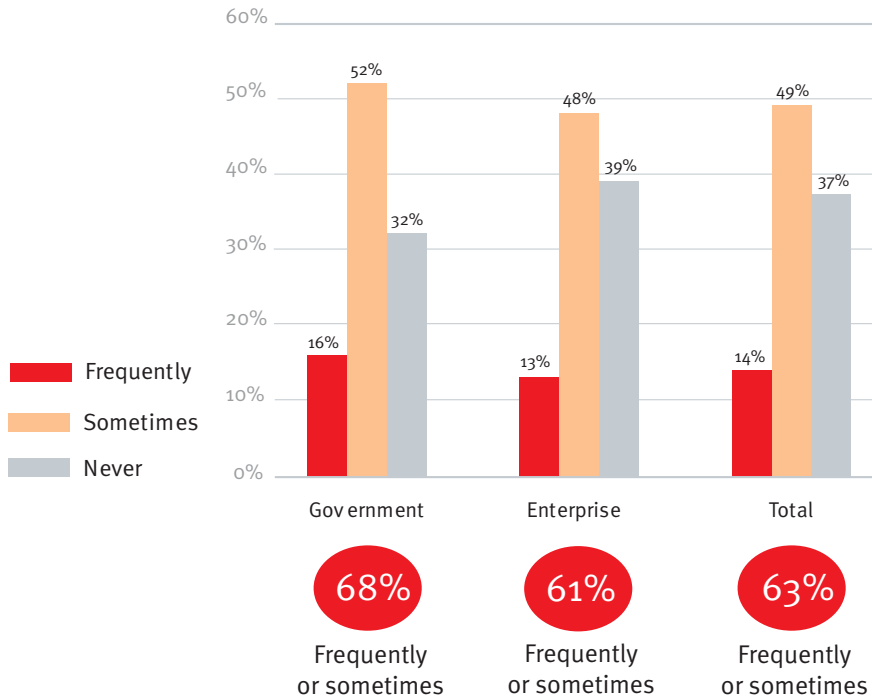
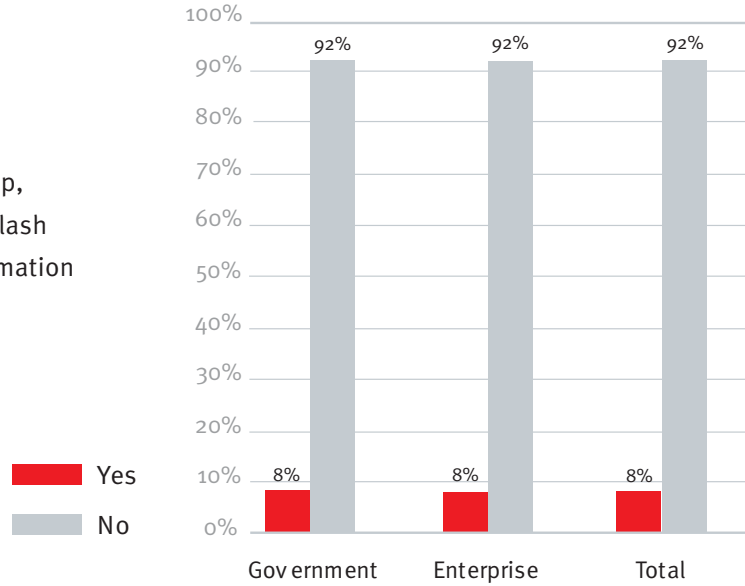
How often do you leave your work place carrying a mobile device such as a laptop, smartphone and/or USB flash drive which holds sensitive information related to your job?*

*i.e., customer data, personally identifiable information such as Social Security numbers, company financials, credit card data, or 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?

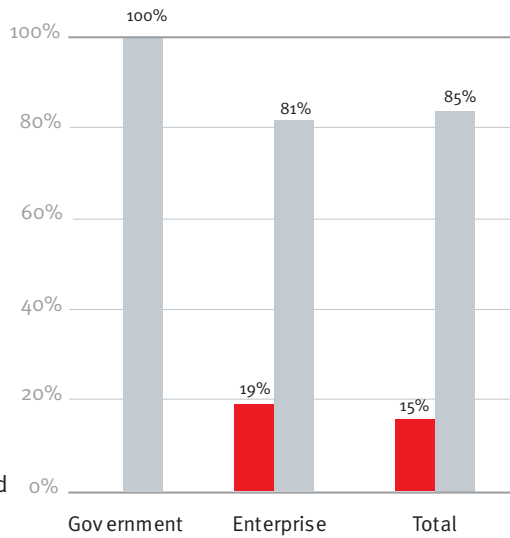
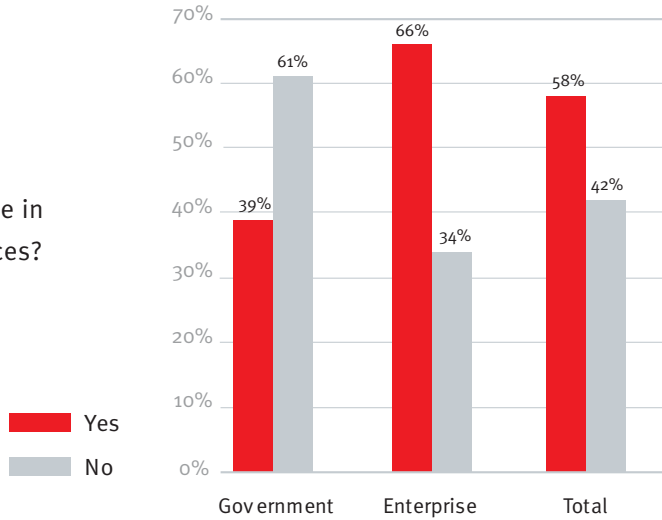


Q

How often do you send work documents to your personal e-mail address so that you can access them from home?



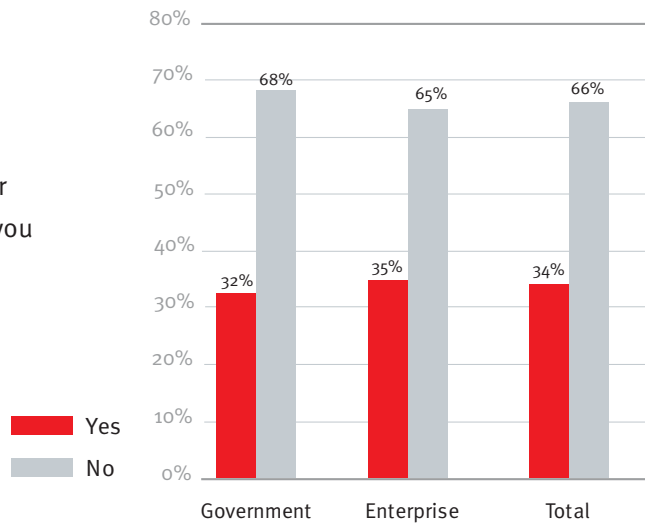
Does your company provide a wireless network internally for use in conference rooms and guest offices?



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

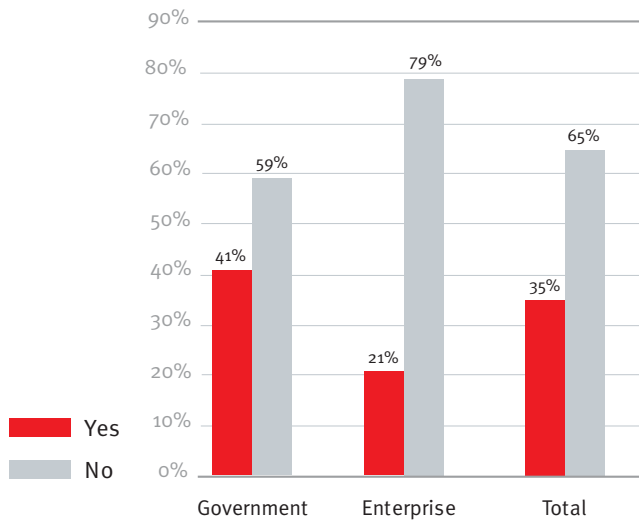
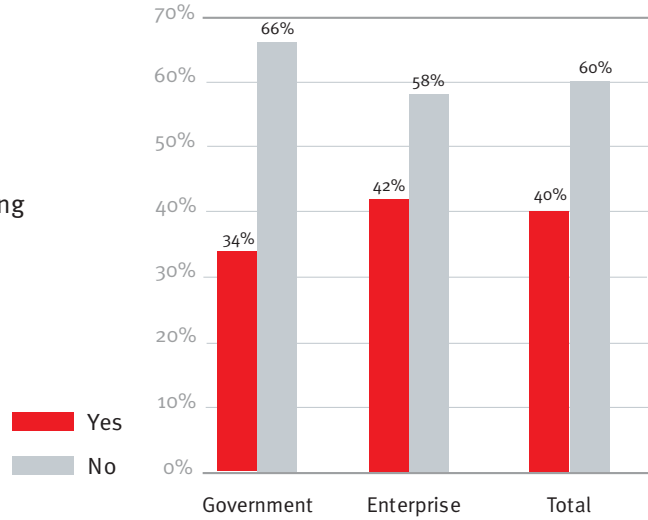


Have you ever held a secured door open for someone at work whom you didn't recognize?



Q

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

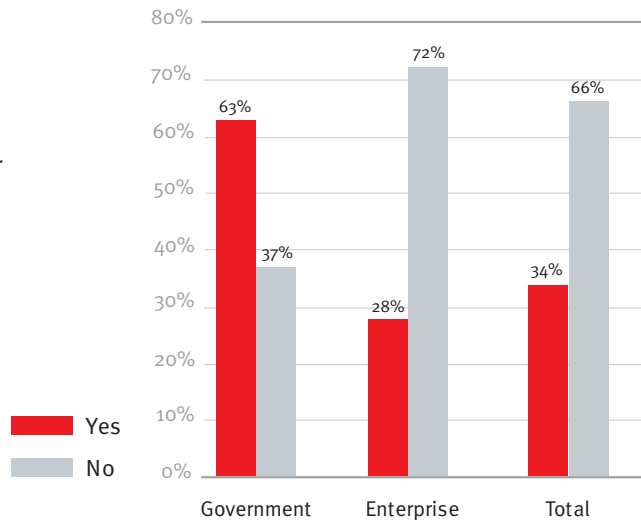


Q

Have you ever noticed an unfamiliar person working in an empty office in your area of the building?

Q

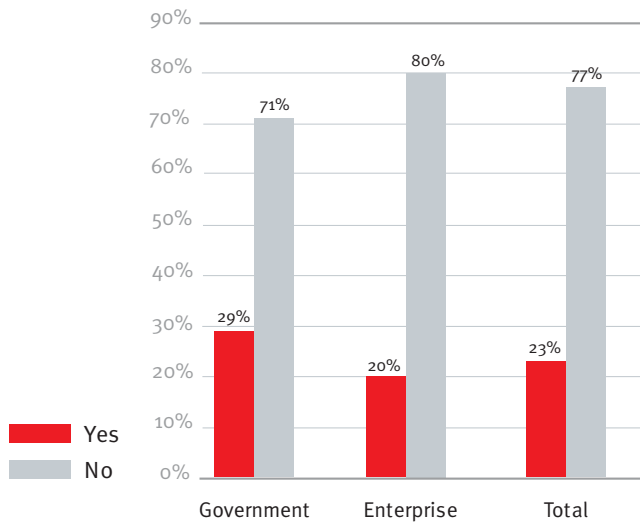
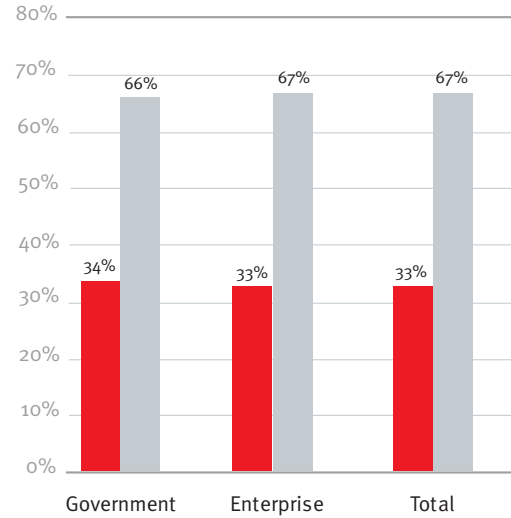
If yes, did you ask for identification or otherwise report the "stranger"?



Q

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

Yes
No



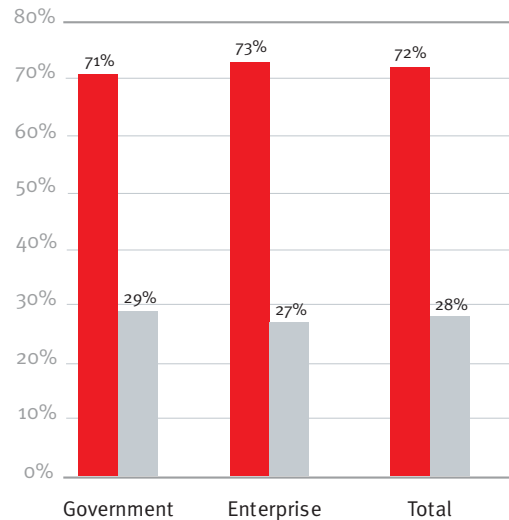
Q

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

Q

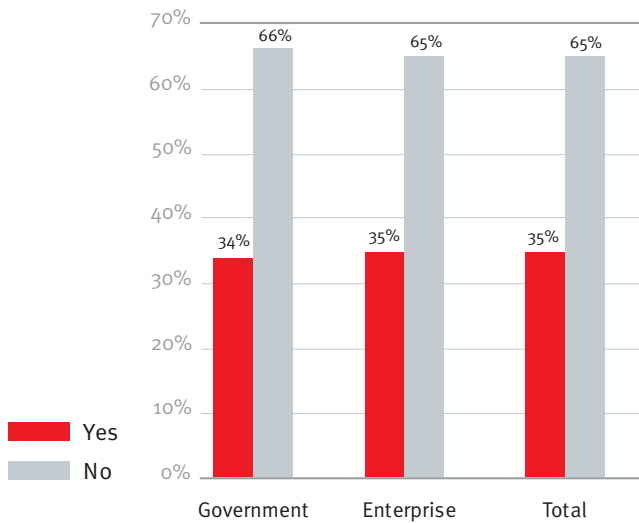
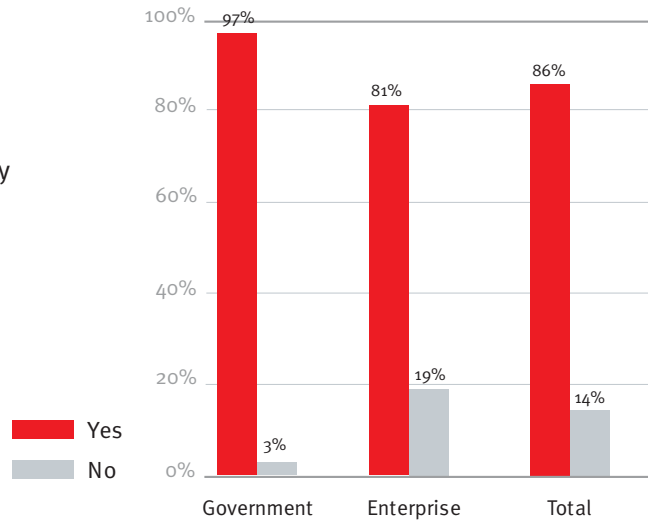
Does your company employ temporary workers and/or contractors who require access to company information and systems?

Yes
No



Q

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

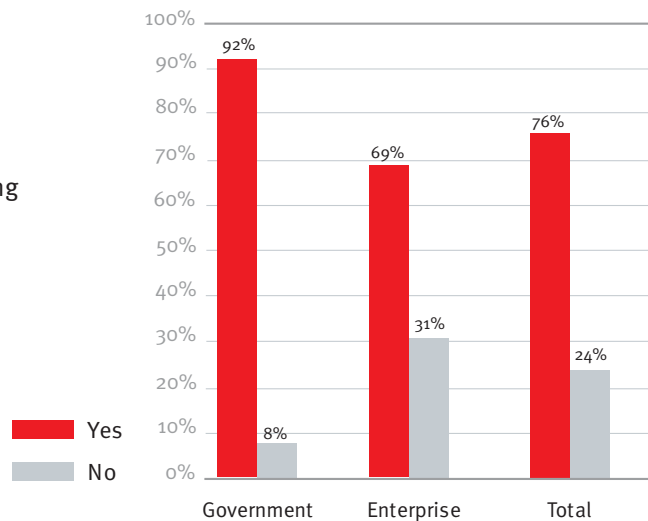


Q

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

Q

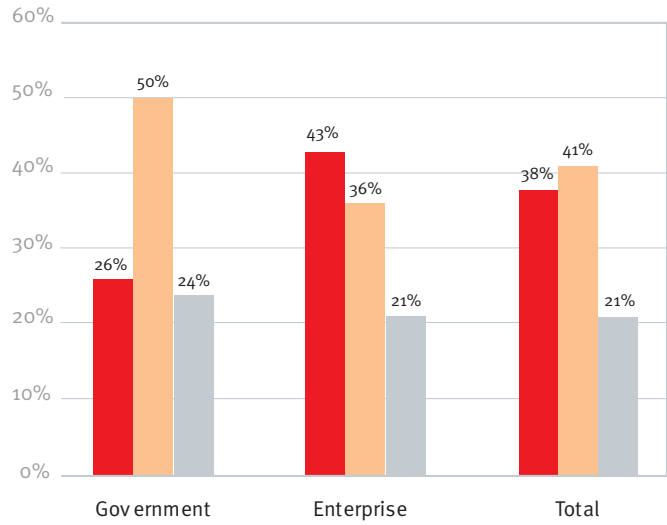
Does your company provide training about the importance of following security best practices?



Q

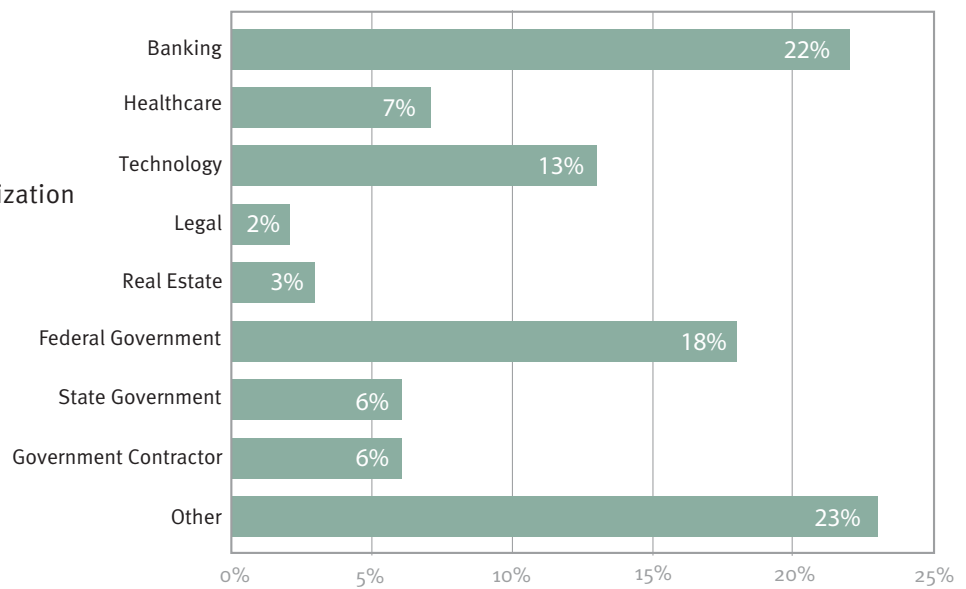
Do you believe security is an IT department issue or an employee issue?

IT
Employee
Both

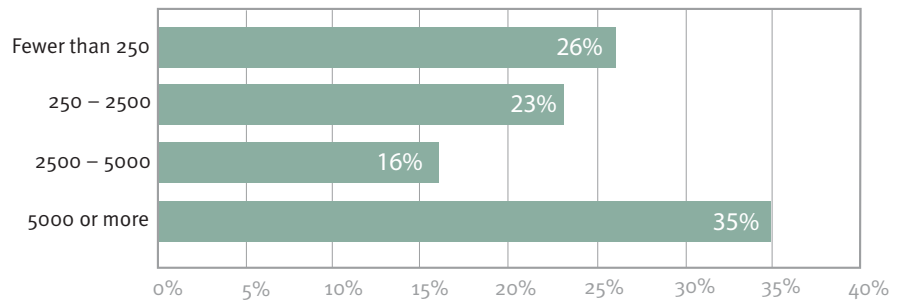


The Respondents

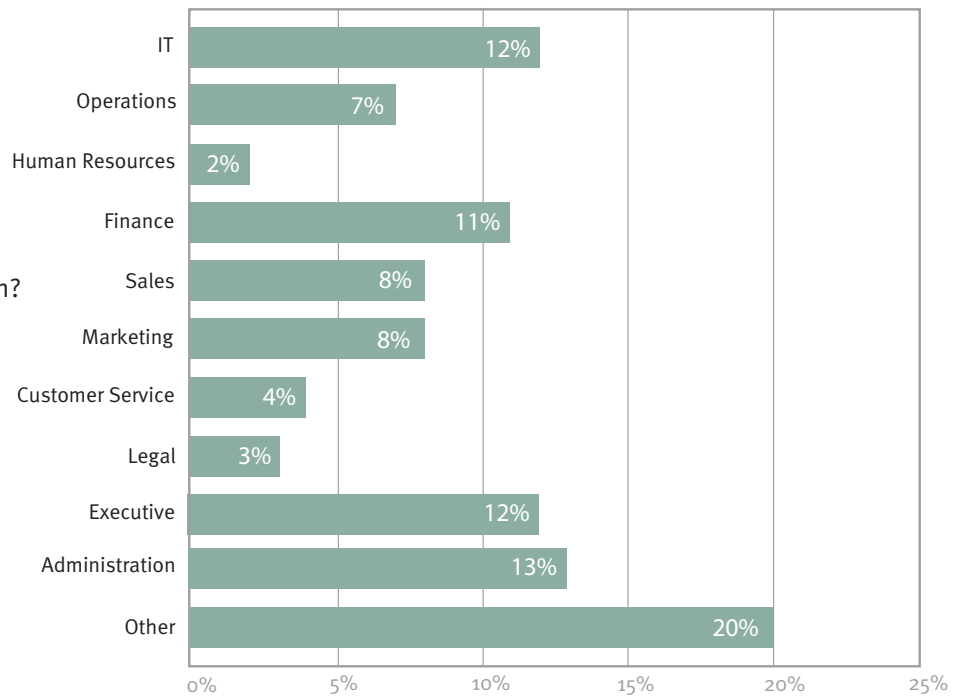
What type of organization do you work for? (total respondents)



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



What is your job function? (total respondents)



Recommendations for Managing Information Risk

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.

Insiders need technology and security policies that match their business needs

When trusted insiders work around security policies, usually no harm is meant. Regardless of intent, sensitive data can be exposed, subjecting the organization – and possibly consumers – to unnecessary risk. Organizations can mitigate this risk by developing information-centric policies that acknowledge and align with the needs and realities of the business. Once such policies are in place, companies should constantly measure actual user behavior against established policy and use what they learn to inform smart policy changes that minimize risk and maximize business productivity. When security is as convenient as possible for end users, they are less likely to work around security policy.

Insiders rely on remote access to sensitive information

Remote access to sensitive data calls for stronger authentication than a user name and password – which can be easily and quickly defeated. Organizations can maintain the flexibility of remote access while protecting sensitive data by requiring two-factor authentication to VPNs and webmail. Additionally, companies can create, monitor, and enforce information-centric policies to mitigate the risk of data loss in mobile environments.

For insiders to leverage information, that information has to be free to move

While mobility is essential to business agility, unprotected information – whether at-rest, in-motion, or in-use – increases risk. Organizations can minimize the risk by reducing the use of sensitive and personally identifiable information wherever possible and protecting sensitive information wherever it is: in-use at personal endpoints, at-rest on corporate file systems and databases, and in-flight across corporate and non-corporate networks. Organizations can establish automatic control and enforcement actions – to allow, audit, discard, quarantine or encrypt transmission – based on the sensitivity of the data.

Insiders trust one another

Physical access policies are not always adequate to guarantee that only authorized insiders are in the building. And even when physical access controls are working properly, not all people with legitimate access to the building should necessarily have access to an organization's information. To minimize risk, physical security controls should be coupled with logical access controls. Organizations can protect access to sensitive data by implementing two-factor authentication to internal wireless networks, desktops, domains, ports and applications, and enforcing appropriate access controls.

Insiders change roles often

Access to highly sensitive or personally identifiable information should be granted on a need-to-know basis. As such, organizations can implement role-based access to critical information to minimize the risk of exposure. Companies should make certain that role changes – including those of contractors and consultants – are promptly reflected in access privileges. Finally, organizations can mitigate information risk by centrally and tightly managing insider credentials, including user names/ passwords, one-time passwords and digital certificates, and developing watch lists to track and alert on unauthorized access attempts.

RSA and RSA Security are registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. EMC is a registered trademark of EMC Corporation. All other products or services mentioned are trademarks of their respective owners. ©2007 RSA Security Inc. All rights reserved.

CSURV WP 1207



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, 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.