



www.rsasecurity.com

RSA Security Password Management Survey Results Report

September 27, 2005

Demographic Data

TOTAL NUMBER OF RESPONDENTS: 1685 (all U.S.)

Title

Chief Security Officer/Chief Information Officer	8%
Other C-level	8%
IT Director/Security Director	11%
Other Director-level	6%
IT Manager/Security Manager	22%
Other Manager-level	17%
IT Administrator	27%
Help Desk Administrator	2%

Industry

Automotive	1%
Consumer/Retail	7%
E-Commerce	4%
Education	7%
Energy	2%
Finance	12%
Government	13%
Insurance	3%
Healthcare	8%
Legal	2%
Manufacturing	8%
Technology	32%
Transportation	2%

Organization Size

Less than 250 employees	43%
251 – 1000 employees	18%
1,001 – 2,500 employees	8%
2,501 – 10,000 employees	16%
More than 10,000 employees	15%

Survey Results Data

Number of passwords respondents that must be kept track of at work

1-3	15%
4-5	26%
6-12	30%
13-15	5%
15 or more	23%

Most common insecure methods for keeping track of passwords at work (multiple answers accepted)

Keep a record on my PDA or handheld device	22%
Spreadsheet or other document stored on PC	25%
Affixed to my PC with Post-It or other note paper	4%
Keep a paper record in my office/work space	15%



RSA Security Password Management Survey Results Report

www.rsasecurity.com

September 27, 2005

Level of frustration with the password management process at work:

Highly frustrating	17%
Frustrating	30%
Somewhat frustrating	41%
Not at all frustrating	12%

Average length of time it takes respondents' IT organizations to reset a forgotten or lost password:

Immediate – (automated, self-service functionality)	18%
2-5 minutes – (provided by IT help desk staff)	45%
6-15 minutes – (provided by IT help desk staff)	20%
16 minutes – 1 hour – (provided by IT help desk staff)	11%
More than one hour – (provided by IT help desk staff)	6%

If a "master password" was provided at work to gain access to all of the respondents' other passwords, the level of importance for using providing an added layer of protection for that "master password":

Very important	55%
Important	32%
Somewhat important	11%
Not at all important	2%

Current use of an enterprise single sign-on product at work (defined as technology that offers the ability to use one set of credentials, a username and password for example, to authenticate and access information across multiple Web sites and applications)

Yes	28%
No	72%

Importance of providing self-service capabilities if using a two-factor authentication device combined with enterprise single sign-on (in the event you lost or misplaced the device)

Very important	39%
Important	41%
Somewhat important	16%
Not at all important	4%