



# 2010 Corporate End User Study

## Small Business Findings

# Methodology

- 1,600 surveys in total, 400 corporate computer end-users were surveyed online per country in four countries: U.S., Japan, Germany and U.K, during March 2010.
- Qualification Criteria:
  - Full-time employed, with e-mail and Internet access at work
  - Use computers over 5 hours per week at work
- Quotas were set by size and type of computer as follows:
  - 25% (n=100) large company, use desktop or workstation most often
  - 25% (n=100) large company, use a laptop or notebook most often
  - 25% (n=100) smaller company, use desktop or workstation most often
  - 25% (n=100) smaller company, use a laptop or notebook most often
- In the US, UK and Germany, the split between large and smaller company was made at 500 employees. In Japan, the split was made at 250 employees.

# Seriousness of Computer Security Threats

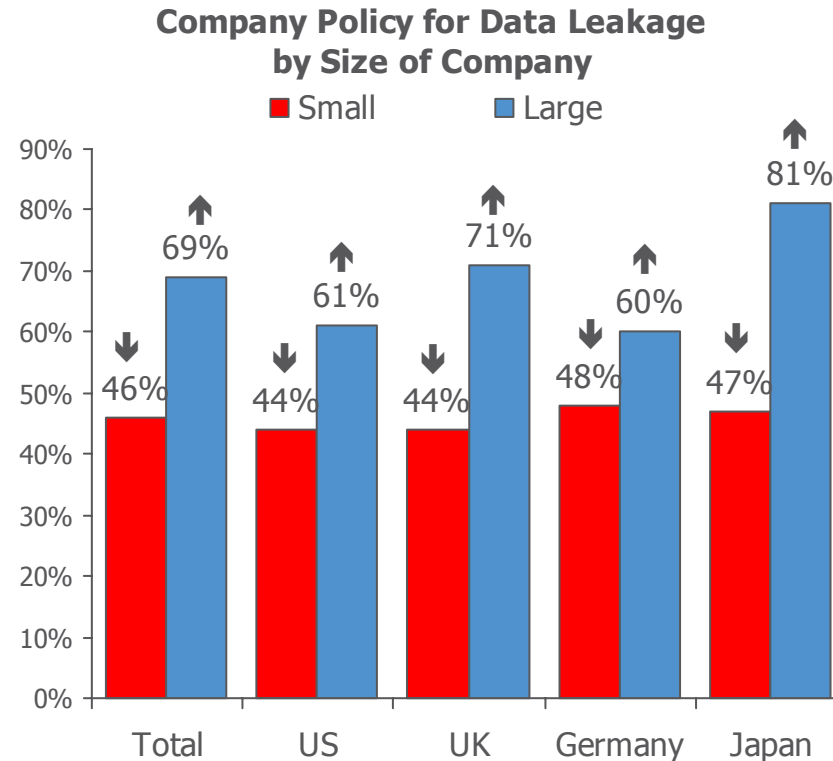
- Viruses, Trojans and data stealing malware are considered the most serious security threats among corporate workers in small businesses.

Country	Total
Sample size, n=	Varies by Threat
Viruses	63%
Trojans	60%
Data Stealing Malware	59%
Data Leakage	56%
Spyware	55%
Fake Antivirus or Rogue Antivirus	52%
Phishing	48%
Spam	40%

Q: How serious of a threat do you think each of the following are to you at work? A: Top 2 Box on 5 point scale (5= "very serious") Base: Users aware of each type of threat.

# Company Policies to Prevent Data Leakage

- In all countries, large organizations are significantly more likely to have preventative policies in place than small companies.

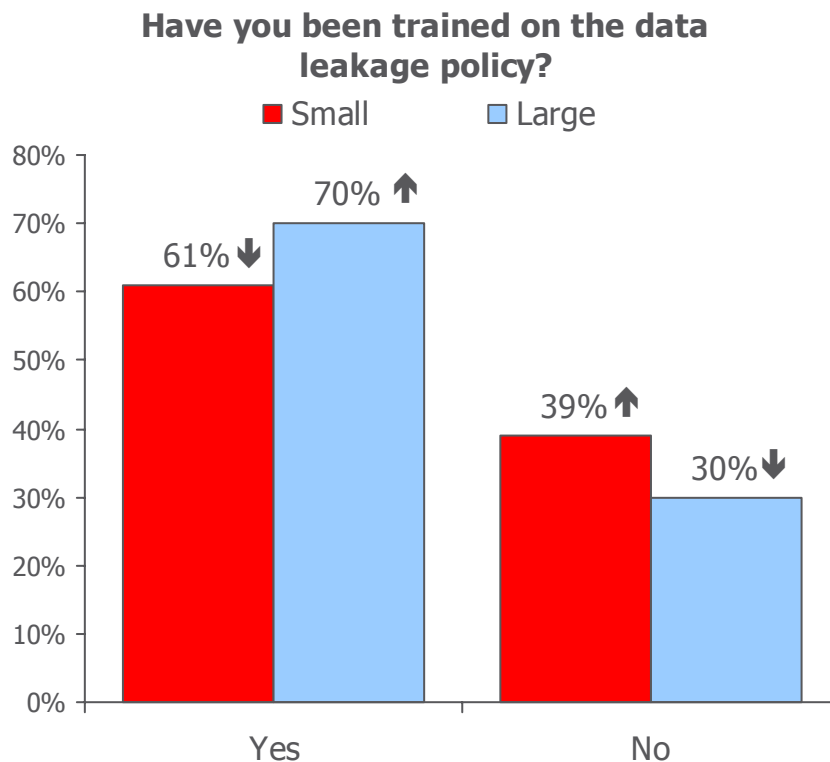


Q: Does your company currently have a policy for preventing data leakage?

↑↓ indicate significantly significant differences between countries or between small and large companies within countries. (z-test/t-test at 95% confidence interval).

# Training to Prevent Data Leakage

- For those small businesses that have preventive data leak policies in place, employees in large companies are also significantly more likely to have received training on data leak prevention than those in small companies.

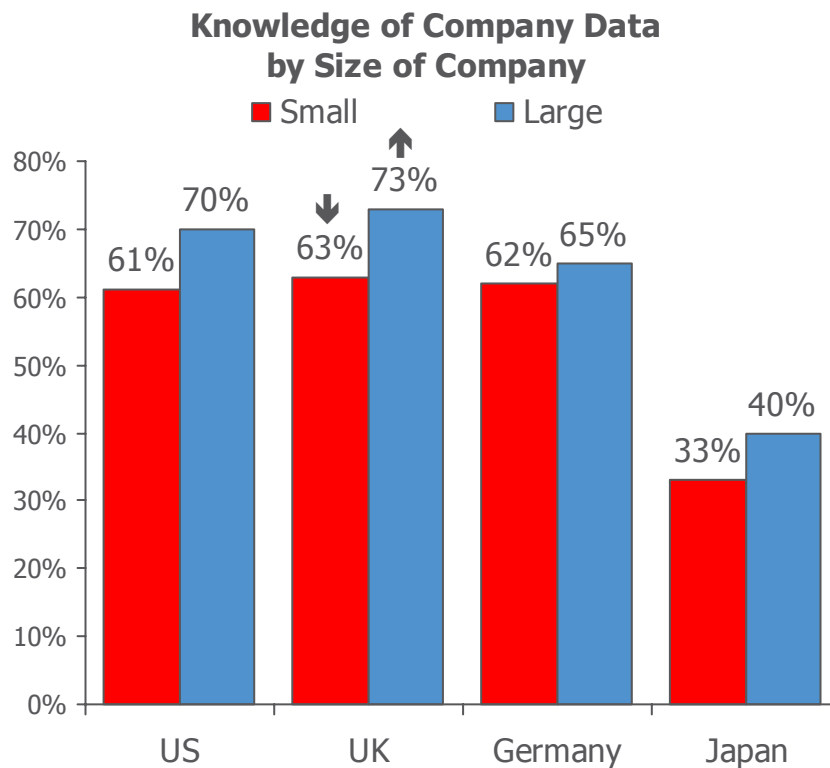


Q: Have you been trained on the policy for data leakage prevention? Base: End users in companies with a data leakage policy.

↑↓ indicate significantly significant differences between countries or between small and large companies within countries. (z-test/t-test at 95% confidence interval).

# Knowledge of Company Data

- In the UK, end users in large companies are significantly more likely to indicate knowledge of confidential information than those in smaller companies.

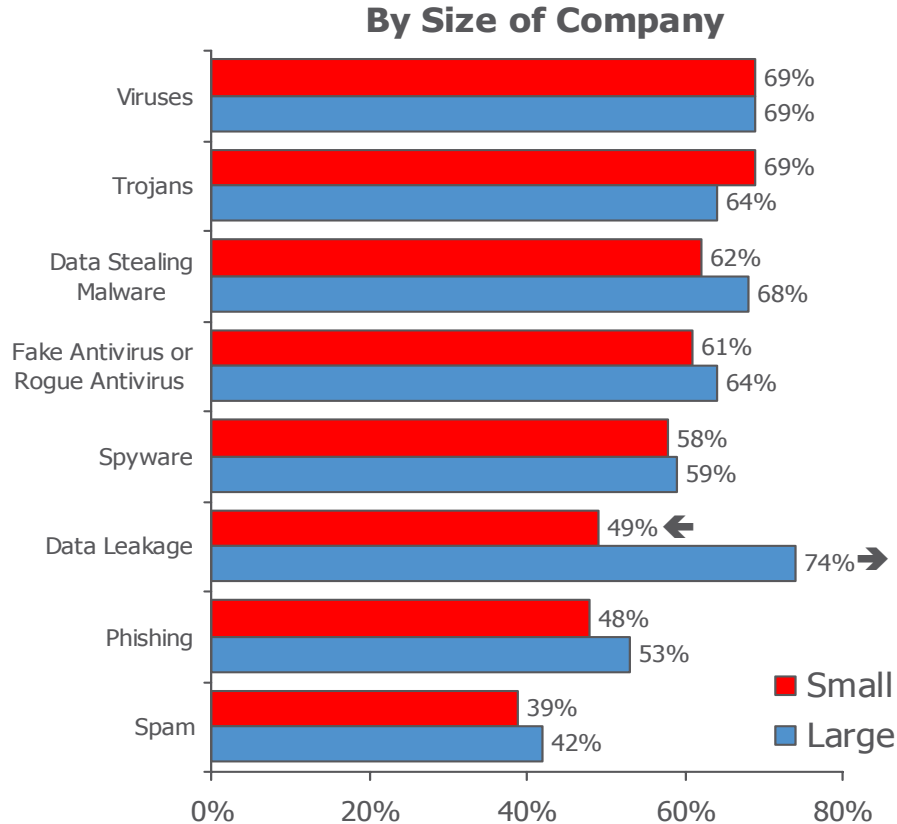


Q: Do you know what type of company data is confidential and proprietary?

↑↓ indicate significantly significant differences between size brackets or between desktop and laptop users within countries. (z-test/t-test at 95% confidence interval).

# Seriousness of Computer Security Threats: US

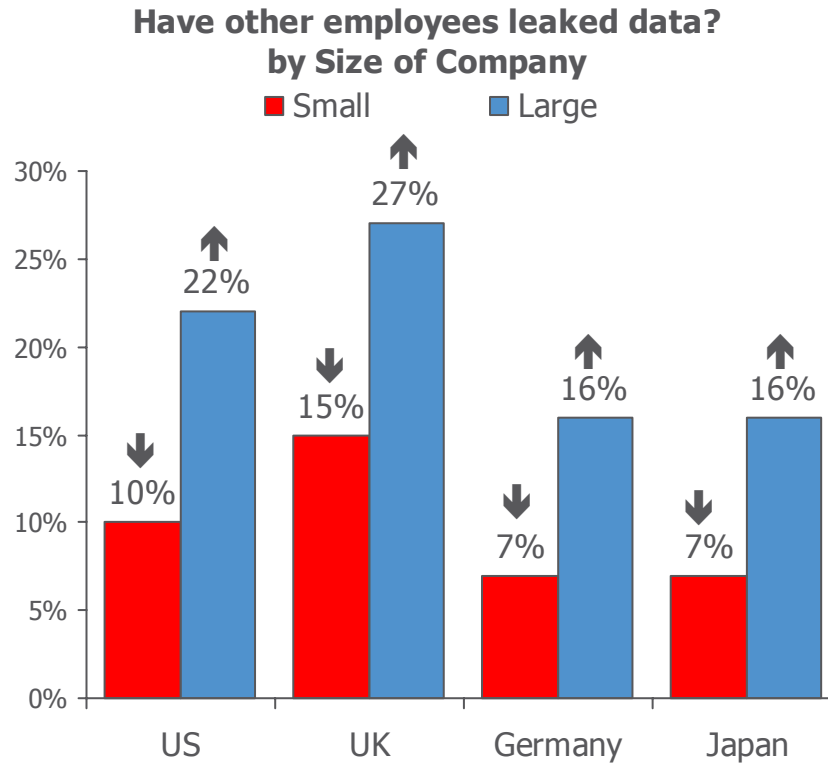
- End users in the large US companies are significantly more likely to indicate data leakage as a serious threat than those in smaller companies.



Q: How serious of a threat do you think each of the following are to you at work? A: Top 2 Box on 5 point scale (5= "very serious") Base: Users aware of each type of threat.  
↑↓ indicate significantly significant differences between size brackets or between desktop and laptop users within countries. (z-test/t-test at 95% confidence interval).

# Leakage of Company Confidential Data – Other Employees

- Data leakage by other employees is more widely believed in large organizations in all countries.



Q: Do you believe other employee have leaked company confidential or proprietary information outside of company?

↑↓ indicate significantly significant differences between countries on left chart or between small and large companies within countries. (z-test/t-test at 95% confidence interval).

# Small Business IT Departments: Data Stealing Malware

- The most prevalent form of IT protection from data stealing malware is installing security software, followed by restricting Internet access and issuing security policies.
- Japanese small company end users are more likely to indicate their IT department can do a better job protecting them from Data Stealing malware than those in the U.K.
- Overall more than one third of the small company employees indicated their IT department can do a better job educating them about Data Stealing Malware. In the U.K. and Japan, this percentage rises to almost 40%.

Country	US	UK	Germany	Japan	Total
Sample size, n=	101	141	148	58	448
<b>What does your IT dept do to ensure protection?</b>					
Install security software	47%	62%	61%	59%	58%
Restrict Internet access	29%	36%	29%	34%	32%
Issue security policies/Internet usage guidelines	30%	32%	34%	28%	32%
Provide troubleshooting help	26%	28%	37%↑	14%↓	29%
Offer education and guidance	28%	26%	15%	17%	21%
IT Department can do a better job <b>protecting</b> me	21%	14%↓	21%	38%↑	21%
IT Department can do a better job <b>educating</b> me	30%	39%	34%	41%	35%

Q: What does your IT department do to ensure that you are protected from the threats or dangers of each? Data Stealing Malware  
 Q: For which of the following threats do you believe your IT department can do a better job of protecting you/educating you?  
 ↑↓ indicate statistically significant differences between countries. (z-test/t-test at 95% confidence interval).