
PRIVACY SELF-ASSESSMENT

Can you answer **yes** to any of these questions?

- Does anyone in your company use email?
- Does your company record anyone's personal credit information?
- Does your company have confidential financial information?
- Does your company have any staff turnover?
- Do your employees surf the Internet for purposes that are not work-related?
- Does your company hold or have access to medical information about anyone?
- Do people who work at your company carry a PDA, wireless device, or cell phone?
- Would employees, investors, customers, or donors be upset if their personal information was leaked from your company?
- Does anyone use remote access to log onto your company systems?
- Do suppliers, vendors, or maintenance personnel enter your company premises?
- Does your company have any personal information about employees, contractors, or customers?
- Do you ever use the Internet for research?

If you answered **yes** to any of these questions, you might be in very real danger — and you might not even realize it.

Can you answer **no** to any of these questions?

- Are you certain that your company's information systems have never been compromised?
- Do you know what indirect costs could result from an information breach?
- Does every remote user have up-to-date firewall protection on their laptop and home computer?
- Has a security clearance check been done for each person who has access to your company's information systems — including contractors, vendors, and janitorial staff?
- Are all of your company's critical applications documented?
- Do you have an ongoing privacy awareness program?
- Do your access controls limit access to data only to those who have a legitimate need to know?
- Do you have current and complete Information Privacy and Data Handling policies in place?
- Can you be sure that the virus protection on your remote workers' laptops and handheld devices is up-to-date?
- Are you certain that unauthorized off-site wireless devices cannot penetrate your systems?
- Are your company's access control lists kept current?

If you answered **No** to any of these questions, your company, investors, and stakeholders are probably at risk.

Do you know the answers to these questions?

- How can privacy planning increase profitability?
- Which international privacy or data protection laws affect your company?
- Could your company survive the indirect costs of even one breach — regardless whether the breach is real or rumor?
- Would your insurance cover losses arising from cyber risks?
- Would you or your company face liability if an employee was dismissed for downloading pornography?
- Can sending joke email result in a lawsuit?
- Do all users know what information privacy and data handling policies are in effect at your company?
- What would happen if investors or donors thought their personal information was leaked from your company?
- What would happen if your competitors gained access to confidential corporate data?
- Who's looking at the data in your data warehouse?
- Which employees really need to see sensitive data to do their jobs?
- What data in your organization is personal and sensitive in nature?

If you **Don't Know** the answer to any of these questions then your company, its employees and stakeholders are at risk.
