



Top 10 Technology Risks

It's only human. People make mistakes, learn from them, and move on to the next challenge — usually without dire consequences. But in business, particularly in information technology, mistakes can be costly. From information theft to lost worker productivity to missed sales opportunities, technology errors can put your business at risk. That's why Intel has compiled this list of the Top 10 Technology Risks your business faces and how you can avoid them. And if like many businesses you've already made a few of these mistakes, don't worry. You *can* fix them — and we'll tell you how.



10. Sharing work e-mail addresses and other sensitive information on the Internet.

The Problem:

When employees share their e-mail addresses on Internet sites or in public chat rooms, those addresses can be easily picked up by SPAM companies, who can then flood work in-boxes with junk e-mail. They can also be picked up by individuals or entities with more malicious intents.

The Consequences:

When employees share their e-mail addresses or other private information over the Internet, they risk your company's:

Productivity — SPAM-clogged in-boxes can impair workforce productivity, robbing employees of valuable time that would be better spent working on core business tasks.

Security — SPAM can compromise the security of your computing environment. Access to an employee's e-mail can help someone with malicious intent gain information about an employee and then pose as that employee to acquire sensitive information about the company. SPAM e-mails are also ideal hosts for spreading viruses.

TCO — Collectively, managing anti-SPAM processes can be costly. If the problem escalates, it may require additional IT support and specialized tools to prevent critical IT resources from being overwhelmed.

The Solution:

Create a company policy requiring employees to use generic or free e-mail accounts when they share their information on the Internet. Develop clear guidelines around when, where, and how employees can share their work information with outside parties.



9. Modifying or replacing internal PC hardware components to achieve better performance or keep legacy systems running.

The Problem:

To satisfy specific end-user needs, companies may need to upgrade some internal components, like video cards. But to achieve better performance or to keep legacy systems working, some company employees — and even some IT departments — may turn to practices like overclocking or component swapping. These methods can make the PCs faster or keep them working past their useful life expectancy. But they're usually Band-Aids* that expose a bigger problem: the need for more powerful PCs for end-users.

The Consequences:

When employees or IT personnel engage in these unsafe practices, they risk your company's:

Productivity — Employees who spend work time swapping out parts or tweaking system performance lose valuable work time that should be spent performing core tasks to reach business goals.

Profitability — The more hardware and software variations in your PC install base, the more it costs your IT support personnel to troubleshoot and repair problems.

PC Quality — Techniques like overclocking and component-swapping can compromise PC quality and reliability.

IT ROI — The parts and labor costs to modify a PC and get it running aren't significantly cheaper than purchasing a new one.

The Solution:

To efficiently meet the demands of multitasking users and multiple power-hungry applications, consider equipping your end-users with PCs with Intel® Pentium® 4 processors with Hyper-Threading Technology. HT Technology empowers the PC client to perform two tasks or threads simultaneously, which gives your users the power to do more at once. So they spend less time waiting and more time working.



8. Operating and maintaining multiple servers without considering consolidation

The Problem:

Frequently, companies fail to examine their server infrastructure and assess opportunities for various levels of consolidation, like application consolidation, server reduction and virtualization, data consolidation, and location centralization. An audit of existing servers can pinpoint major inefficiencies and help companies implement consolidation projects that deliver the greatest ROI while improving IT efficiency. In the long run, only a comprehensive and well-conceived consolidation strategy can deliver lasting business value.

The Consequences:

Failure to seize opportunities for server consolidation can risk your company's:

TCO — Inefficient, multiple servers running the same applications in multiple geographies require local IT management and support, raising the overall TCO.

Computing Infrastructure — Redundant geographically distributed servers, identical application servers, and multiple “small-scale” legacy servers increase the overall complexity of the computing infrastructure, making it more difficult and costly to maintain.

Efficiency — As the complexity of the server environment and the physical number of servers increases, it becomes more difficult to implement sound IT practices, policies, and processes that improve overall operational efficiency.

The Solution:

Determine which computing resources can be consolidated. Plan your consolidation projects to address the inefficiencies that drive up your company's operating costs and impede your business agility. Focus on consolidation projects that deliver maximum value for every dollar spent, and you'll be able to lower your costs, simplify your environment, and create a more agile infrastructure for meeting future business challenges.



7. Using illegal, unauthorized, pirated, or shared software.

The Problem:

When employees require software that's not available internally, they may find other ways to get it, like loading a pirated version from outside the company or borrowing a coworker's CD. Worse still, they may attempt to install a legal but unauthorized program onto their system, potentially causing compatibility issues with the IT-approved software load. Companies may potentially face a host of serious consequences when they neglect to carefully monitor their employees' machines for illegal or unauthorized software, or overlook employees' critical software needs.

The Consequences:

When you leave software licensing unchecked or take it for granted, you risk your company's:

Profitability — Software copyright infringement may cause serious financial damage to a company. The fines are severe, and litigation is even more costly.

Software Stability — Unauthorized software can cause problems with the software load installed on the employees' systems. When an employee uses non-compliant software, it can break the image, escalating IT support costs, and rendering the machine unusable until it is repaired.

Integrity — Software copyright infringement can lead to very public disclosures about a company's non-compliance. Even if you have no knowledge of your employees' actions, illegal software puts the company at risk for criminal fines or other judicial actions.

The Solution:

Enforce a comprehensive software management program and communicate your software policies to employees. Your program should include: 1) accurate record-keeping and documentation, 2) random audits of employee machines, 3) a company software repository where employees can get the authorized software they need easily and quickly, 4) an expeditious process for employees to get approval for non-standard software, and 5) adequate departmental funding to make the software purchases you need for business-critical tasks.



6. Maintaining multiple images in the client PC base.

The Problem

Every IT manager wants to limit software images and qualify their PC platforms using a standardized image. But when it's time to deploy new PCs, it's never easy. When a vendor makes a hardware change, it can affect a previously qualified PC platform, and then the software image has to be updated for the changed PC. After a few such changes on multiple system components, the cost benefits of PC platform standardization begin to unravel.

The Risks:

When you maintain a complex PC infrastructure with an unmanageable amount of PC hardware configurations, you risk your company's:

Profitability — More PC platform configurations mean more time and money is required to test the compatibility of new software, updates, bug fixes, and security patches within the installed base.

Efficiency — More PC hardware configurations increase the scope of IT and help desk support requirements, resulting in more training, documentation, and unique process requirements.

Security — IT's ability to respond to necessary new software security patches, updates, and bug fixes can be significantly increased by PC infrastructure complexity. Therefore, the increased time it takes to qualify and deploy the latest security patch to your PC installed base increases your vulnerability to a potential security threat from an opportunistic hacker.

The Solution

Deploy stable image platforms by choosing products that have been designed around the Intel® Stable Image Platform Program. Implementing the Intel Stable Image Platform Program helps IT managers control costs and assists in PC transition planning, as it enables corporations to qualify PC platforms on an annual schedule and then deploy new PCs based on this platform for the next year.



5. Giving employees the wrong machines for their jobs.

The Problem

In an effort to simplify and standardize PCs — or simply to save money — many companies give their employees PCs that may not be appropriate for their job function. Employees who travel, or those who frequently work away from their desk, may benefit significantly from using a notebook PC instead of a desktop PC. Perhaps there are employees using PCs that are either more powerful than what they need, or worse, not powerful enough. In either case, new PCs must be chosen carefully and matched to user groups to ensure optimal business value and maximum ROI.

The Consequences

When you don't adequately match clients to user groups, you risk your company's:

Productivity — If an employee can benefit from mobility but is equipped with a desktop PC, then meeting and travel time equal downtime. If multitasking users don't have rich, powerful clients, it takes them longer to perform tasks. In both cases, productivity drops significantly.

ROI — If you don't analyze your users and understand their needs, you can't choose machines for them that provide maximum ROI over time.

Employee Satisfaction — Your employees want to know that your department is working to meet their needs. This improves goodwill toward not just the IT department, but your company in general.

The Solution

Analyze and segment your users based on their job functions. Then, give each user group the right machine for its tasks and work style. Be flexible, and have qualified notebook and desktop PCs readily available when employee job functions and roles change as business goals and conditions change. Consider notebook PCs based on Intel® Centrino™ mobile technology for employees who can benefit from a more flexible computing model.



4. Using outdated or manual data storage methods as your primary data backup solution.

The Problem:

Many companies, especially small- and medium-sized businesses, don't have a comprehensive and reliable data backup solution for their information assets. Many still use manual methods, like burning CDs, or other backup solutions like portable storage peripherals. In some cases — like backing up data on a single machine — these methods may be useful. But as the primary backup solution, these practices are risky and may cost your company time, money, and, in the case of complete failure or disaster, the permanent loss of vital company data.

The Consequences:

When you use antiquated or manual backup solutions, you risk your company's:

Profitability — It costs more to backup manually or with outdated technology than it does to use a new, robust server solution. Manual backup requires manpower, media, and storage costs. Antiquated technology requires more IT support and maintenance.

Information Assets — Without a comprehensive and reliable data backup solution, your company's critical business information is at risk. In the event of a disaster — like fire or flood — or malicious employee misconduct, important information may be lost forever. And without secure storage, electronic files containing sensitive business information can fall into the wrong hands.

The Solution:

There are many server-based storage solutions available, but choosing the right one for your business may entail some initial research and investigation. In general, companies can benefit substantially from a robust, scalable storage solution. A storage area network (SAN), for example, can provide a flexible, networked storage infrastructure that decouples storage devices from their respective servers, preventing permanent data loss and securing your information assets in the event of a disaster. Learn more about Intel® storage solutions.



3. Installing unauthorized wireless access points in a company building.

The Problem

When employees want wireless LAN access inside a company building and the service is not available, they may be inclined to take matters into their own hands. IT managers who don't carefully monitor their computing environments could end up with "rogue" wireless access points, installed by employees, throughout the building. This opens the company's WLAN to a host of security problems.

The Consequences

When employees install unauthorized wireless access points in your building, they risk your company's:

Information Assets — Rogue wireless access points expose your computing environment to intruders, who can gain access to confidential documents.

Network Security — Unauthorized wireless access points can make your network more vulnerable to virus attacks.

WLAN Service — Unauthorized wireless access points can interfere with the wireless access points your IT department has installed, thus degrading the quality of your WLAN service.

The Solution

Know the locations of all your IT-installed wireless access points and be alert for any access points that are installed elsewhere. Communicate your security policy with your employees, explain the risks of installing unauthorized wireless access points, and outline the consequences of security non-compliance. Implement a plan to audit and monitor company buildings for both authorized and rogue wireless access points.



2. Using a desktop PC as a server.

The Problem:

In an attempt to save money, companies large and small occasionally use business desktop PCs as “servers” by loading server software and adding more powerful internal components like larger or additional hard drives and more memory. A desktop PC is designed to serve a single user and cannot provide the expandability, performance, or dependability that a server offers.

The Consequences:

When you use a desktop PC as a server, you risk your company's:

Information Assets — A PC is less secure than a server, which means your sensitive documents and e-mails could more easily fall into the wrong hands.

Productivity — PCs don't offer the same reliability as a real server. If the PC is modified with excessive hardware and software loads, it may be more likely to crash, which could lead to lost files, e-mails, and other important records.

Revenue —If the PC “server” crashes, business operations can be interrupted, potentially costing your company valuable transaction revenue, not to mention downtime for business operations as well as increased IT support costs.

The Solution:

Use the right tool for the job. At price points your business can afford, consider moving to a real server based on the Intel® Xeon™ processor. The server you choose should be a robust, dual-processor, expandable system designed to serve multiple users and run shared applications. Ensure that it uses high-reliability technologies, like ECC memory, that keep your data secure.



1. Delaying your regular refresh cycle for desktop and notebook PCs in an effort to save money.

The Problem:

When budgets are tight, companies may delay their PC replacement programs in an effort to save money. But the longer those aging PCs remain in a company's infrastructure, the more hidden costs escalate — losses such as lost end-user productivity and downtime. When you factor in security risks, high maintenance costs, and reduced productivity, refreshing your client base could actually save your company time and money — important business goals in any economic climate.

The Consequences:

When you allow aging PCs to remain in your company's infrastructure, you risk your company's:

Security — Older PCs can't run continuous virus scanning and encryption in the background, making them the weak link in your total enterprise security solution. And if they're running an old OS, security patches may no longer be available.

Productivity — Employees take longer to finish a job on an older PC. Older machines don't have the power or technology to support today's multitasking business environment, so employees spend more time waiting and less time working.

Profitability — After three years for desktop PCs and two years for notebooks, hidden costs escalate, such as IT support costs, loss of end-user productivity and system downtime.

The Solution:

Convince your management team that a regular PC refresh cycle is one of the most cost-effective ways to deliver large-scale benefits to the organization. Learn how replacing those aging systems can enhance security and increase end-user productivity. Make your case to senior management by telling the financial story with tools like a PC ROI Analyst*, and present data such as return on investment, net present value, and internal rate of return. And once you've got the go-ahead, understand the risks, pitfalls, key issues, and best practices for implementing your PC refresh in the PC Lifecycle Resource Center.