10 Top Tips for Data Protection in the New Workplace

shaping tomorrow with you

Balancing Workplace Security with Workforce Productivity

One of the key things that keeps CIOs awake at night, is worrying about the loss or leakage of sensitive information from user devices.

In the past, desktop computers remained in the office until the IT department had them professionally replaced. Today, increased connectivity and mobility aren't just creating new working styles; they're creating new security headaches. The rise of BYOD culture – initiated by an influx of Generation Y employees and accelerated by the rush to enable mobile working and collaboration between global teams – has changed the game for information security professionals.

IT organizations must manage these rapid technological changes against a background of increased regulatory pressure, as companies grapple with meeting new compliance requirements such as Sarbanes-Oxley and Basel II.

As organizations look for ways to manage devices, applications, and data within the network and beyond the firewall, it's important to find the right balance between information security and employee productivity. Clamp down too hard, and you risk damaging efficiency and employee satisfaction. Become too lax, and the risk of data breaches and non-compliance grows.

Managing Rising Risk in the New Workplace

For IT professionals, the challenge is to protect corporate networks, data, and services while enabling ready access to information and faster, more efficient communication to drive productivity. And all this must be done in the context of a constantly changing threat landscape and increased incidence of data breaches.

The penalties for failing to provide adequate data protection can be severe; from loss of revenue and intellectual property, to legal costs and punitive fines, as well as irreparable damage to brand reputations.

It's no wonder that security is the top concern for all CIOs, but unfortunately there's no 'magic bullet' that will make the risks disappear. Every organization must assess its own security posture against the current and future threat environment to identify where additional controls are needed, always keeping in mind the need to balance security with access.

Here we look at the importance of identifying the right balance for your organization, and the practical steps you can take at each of the four layers of workplace information security: system protection, access management, data security, and audit-proof protection.

Control access to data and services

1 Use smarter passwords

If thieves do get hold of a device – either digitally or physically – you need robust identity and access management, which starts with users **choosing strong passwords**. It's also essential to have a different password for each important account, and to change passwords regularly.

2 Or use biometrics – even smarter than passwords

But if you really want to prevent unauthorized access, there are much more secure methods than passwords, which can be forgotten, lost, hacked, or stolen. **Fingerprint sensors** built into notebooks offer a more secure alternative, and improve the user experience by replacing multiple passwords with single sign-on capabilities.

For the ultimate in access control, you could use more advanced **biometrics technologies like FUJITSU PalmSecure™**. This system authenticates user identities by recognizing patterns of veins within the palm, which are unique to individuals and incredibly difficult to forge.

Simplify compliance and make your data protection audit-proof

3 Back up your data and eradicate data on used drives

Fujitsu storage solutions, such as CELVIN NAS servers and ETERNUS storage, provided all the flexibility, scalability, and ease of use you need to back up data efficiently and cost-effectively.

To ensure your data protection is completely audit-proof, it's vital to have proper disk sanitization in place. One of the key information security vulnerabilities for many organizations is that data stored on old hard drives isn't properly deleted, or isn't deleted at all. **Fujitsu's EraseDisk technology** overwrites – and thereby irretrievably deletes – all sensitive data on a hard disk before a system is retired, repurposed or sold. An audit-proof record of the deletion can be copied to an external USB drive to demonstrate compliance.

4 Stop thieves getting hold of your data

That's great for retiring devices, but what if one of your devices is stolen? With severe consequences for data breaches, it's essential to use anti-theft technology on all client devices. **Fujitsu's Advanced Theft Protection** solutions track devices and issue tamper alerts; automatically or remotely erase sensitive data; disable the notebook completely, rendering it useless until recovered; and help local police to recover the stolen property.

Protect your systems – digitally and physically

5 Stay up to date and keep on patching

Any connected device can be susceptible to malicious attacks, so it's vital that **malware and virus protection software** is constantly updated. Ideally, all client devices should be set up for automatic updates to the operating system, software, drivers and BIOS to eliminate known security vulnerabilities.

6 Lock devices up

It's a good idea to make devices more difficult to steal. A **Kensington security lock** on notebooks offers a practical way to prevent theft from the workplace or on the move. Another simple but effective theft deterrent is to **customize devices with a corporate logo**, making them less attractive to thieves.

Use encryption to keep your data safe

7 Protect encryption keys

Your next line of defense is to encrypt valuable files and sensitive information. But if the encryption key is stored within the device, it can be hacked and used to decrypt your data. **SmartCard technology** is ideal for generating and storing encryption keys, as they enable keys to be used without exposing them to the riskier environment of the device itself. In combination with PIN or fingerprint sensor technology, SmartCards can also be used for access protection.

8 Encrypt the whole drive

For maximum security and minimal performance overhead, **full disk encryption** is the answer. This needs to be performed within the BIOS rather than the operating system to prevent encryption keys being found in the hard drive itself.

Take the next steps to balance user access with corporate control

9 Manage security on user-owned devices

As more user-owned, non-Windows based devices access corporate data and services, new security holes open up. To keep these holes closed, a robust **mobile device management system** is needed. An alternative is to implement a **Virtual Desktop Infrastructure** solution, so that sensitive data is stored on a secure server instead of on client devices.

10 Identify vulnerabilities and create your action plan

First you need to assess your current information security to establish where protection can be strengthened, as well as where cost savings can be made. Working with an **external security review partner** like Fujitsu helps you create a compelling business case for change, and provide independent measurement of improvements after changes have been made.

Once you know where the gaps are, you need to clearly define what needs to be done to achieve best practice information security. It's important at this stage to establish equilibrium between the tighter security you're aiming for and the seamless user experience that employees need to collaborate and stay productive.

Simple steps to minimize risk

At Fujitsu, we know there's no such thing as total security. But there are plenty of simple ways to minimize the risk of data loss in the new anytime-anywhere workplace. By using some of the techniques and technologies we've looked at, you can eliminate many of the most common risks while enabling users to find the information they need to work and collaborate – wherever they are.

Get in touch today to learn more about our workplace security solutions and see how you can reduce the time, cost, and effort of protecting sensitive information.

Contact us:
http://workplace.global.fujitsu.com/contact-us
For more information visit:
http://workplace.global.fujitsu.com

Fujitsu Technology Solutions GmbH

Mies-van-der-Rohe-Strasse 8,
80807 Munich, Germany.

Contact: fujitsu.com/fts/contact

www.fujitsu.com/fts