

Gone in sixty seconds

The Executive Guide to internal data theft



CENTENNIAL
software

Executive Summary

Another month, another fad. That's how IT security can often appear to the business manager. There's always some 'crisis of the day', whether it's a new malicious computer virus, security vulnerability in Windows or spate of internal data leakages.

But through all of this, there is an inescapable trend that needs urgent attention from the board – the increasing threat of confidential data being removed from the network *inside* the organization through the use of removable media devices such as USB flash drives, 'plug and play' hard disks, PDAs and MP3 players.

But what can possibly be dangerous about the latest iPod? Good question. With 60GB of storage space, they're great for any music fan that wants to carry their entire collection with them on the move. But what if that iPod isn't used to carry songs, but instead has 60GB of your customer databases, financial records and HR files on it? After all, an MP3 player is just a big hard disk.

Now consider that one of these devices can be connected to any PC on your network and used to copy hundreds, if not thousands, of sensitive files in a single minute without anyone noticing.

It might sound like James Bond fiction, but the risk is all too real.

With your internet and email gateways largely secured against the threats of external hackers, up to 70% of security breaches are now occurring *within* your network. After all, why go to the trouble of hacking through several layers of external security measures when you can just walk into an office, download files without raising an eyebrow, then walk straight back out again?

But why should the board be worried and why should the issue of removable media device use be placed above the many other IT and governance initiatives vying for priority?

The simplest way to answer that question is to ask what value you place on your organizations' data, your customers and your reputation? They might not have their own place on your balance sheet, but combined these assets are worth millions, if not billions, to your business. After all, where would you be if suddenly your nearest competitor had all your latest technical blueprints, or if your customers all cancelled their accounts due to a data leak?

Research published in July 2006 suggests that the average publicly-traded company sees a \$10 million loss on stocks within two days of a privacy breach being made public. And that doesn't include indirect costs such as legal fees, fines, loss or reputation etc.

Even if you're not yet convinced about the risks of data loss and identity theft, be in no doubt that your customers already are. The fear of identity theft and data security breaches are leading many consumers and businesses to re-evaluate who they do business with and who they trust to hold their personal data.

And who can blame them? It is estimated by the Privacy Rights Clearinghouse in the USA that some 88 million Americans have been put at risk of identity theft between February 2005 and June 2006, all because of a raft of high-profile security breaches where customer data has been leaked or stolen.

Thankfully, there is some good news. Armed with the right technology and mindset, dramatically reducing the risks presented by portable device usage is not difficult.

DeviceWall from Centennial Software allows organizations to monitor and manage the use of all types of removable media devices and wireless connections – allowing authorized staff to go about their legitimate business, while automatically blocking any unwanted connection attempts. DeviceWall stops opportunists and criminals from copying information to or from the network – significantly reducing the likelihood of data leakage, identity theft and the spread of malware or spyware.

There's also a strong financial case for acting now. With many firms losing as much as \$1,500,00 / £875,000 per year due to internal security breaches, the ROI for taking charge of portable device use is compelling to say the least.

With 66% of the European working population now owning some form of portable storage device – your organization cannot afford to ignore this security gap any longer.

Contents

Introduction	1
Understanding the dangers	3
Accidental data leakage	3
Identity theft	3
Industrial Espionage	3
Productivity and Legal risks	3
The usual suspects	4
Accident-prone	4
Opportunist	4
Disgruntled	4
Criminal	4
Social Engineering – the USB way	5
Addressing the risks	6
Scenario 1 – “DeviceWall stopped me copying confidential files”	7
Scenario 2 - “I nearly introduced a virus onto my PC by accident”	7
Scenario 3 - “I was offsite and needed urgent access to my CD drive”	7
Scenario 4 – “My lost USB stick nearly cost us millions”	7
Scenario 5 - “I haven't noticed any difference!”	7
Calculating the ROI for DeviceWall	8
Cost of security breaches (prices in UK£ and US\$)	8
DeviceWall ROI example	8
Conclusion	9
Next Steps	10
Glossary	11
Sources	12

Introduction

The proliferation of small 'lifestyle IT' accessories is nothing short of overwhelming. In just three years, Apple has sold over 50 million units of its now infamous iPod. And while two years ago, a 128MB USB flash drive was an expensive "nerd's toy" which few could afford, today a 1GB flash drive can be yours for around \$30 / £17.

Mobile phones have always been something of a status symbol. In 2004, the craze was for color screens. Today, if your phone doesn't have an external memory card and enough internal storage to hold many hundreds of files, it's just not worth having.

The dramatic reduction in the cost of portable storage devices – whether explicitly designed to hold business documents or more lifestyle oriented – means that more and more of them are being brought into the office every day.

The risk posed by the invasion of these types of device onto the corporate network is threefold:

- **Unauthorized removal of content from the network**
Computer users can freely copy sensitive files from the network to a portable storage device, effectively bypassing existing security measures
- **Transfer of malicious and unwanted content from the device to a company PC**
Even well-intentioned employees can bring viruses, spyware and legal risks onto the network from their personal devices
- **Exposure of sensitive data carried outside the organization**
Data carried legitimately off-site can be lost or stolen and subsequently compromised by unauthorized third parties

Research conducted by Centennial Software at Infosecurity 2006 in London found that 70 percent of respondents connected some form of removable media device to their company PC on a daily basis. This same research found that 64 percent of companies either have no measures in place to manage the use of these devices or rely solely on the discretion of line managers.

Which isn't to say that all companies are turning a blind eye to the threat of portable storage devices in the workplace. At the other end of the spectrum, 12 percent of respondents said their organization operated a complete blanket ban on the likes of USB sticks, iPods, PDAs and other plug and play devices.

However, given the ease with which someone can conceal such a device, walk into an office and copy huge amounts of files without anybody noticing, none of the above approaches can possibly work.

And while pondering whether 'to ban or not to ban', it's important to understand that there will be a small number of occasions when it is deemed acceptable for trusted staff to carry sensitive files on a device such as a USB flash drive. In these scenarios, the threat changes from the illicit removal of data from the network to the exposure of the data to unauthorized third parties. The key here is to secure the data already carried on the device – to ensure that it does not fall into the wrong hands.

On the one hand, not having the means to control these devices is tantamount to inviting unauthorized parties to help themselves to your (and your customers') data; while on the other hand restricting all users from using these devices will inevitably hurt business productivity (not to mention being completely unenforceable).

The only way organizations can be sure that unauthorized devices are not being used to remove sensitive files from the network is to electronically intercept those devices as they are connected to work PCs, automatically verifying the security rights of the user and instantly allowing or blocking the attempted data transfer accordingly, finally creating a permanent record of the connection.

When is a lifestyle gadget dangerous?

When it can be connected to a PC and has sufficient storage capacity to hold even a single business file. It's as simple as that. As such, the list of potentially-dangerous devices comprises:

- USB flash drives, U3 devices and other external hard disks
- PDAs and Blackberry-style email clients
- iPods and other MP3 players
- Mobile and 'smart' phones
- Digital cameras (not for the photos, but for their large memory cards)
- CDs and DVDs
- Floppy disks – yes even the humble floppy can steal 1.44MB worth of confidential files...

So why are these devices considered dangerous? Largely it's because organizations' existing security strategies are focused primarily at the perimeter – stopping the bad guys hacking your network, or employees emailing offensive content etc – rather than the individual PCs on the network. This means that there's nothing watching the desktop, keeping a look-out for unauthorized data transfers.

Before the introduction of CD writers, USB, Firewire, Bluetooth and Wi-Fi ports on desktop and laptops PCs, there was only a limited number of ways in which computer users could transfer data to and from the network. But in the last 18 months, these types of fast local and wireless data transfer mechanisms have become standard on most office PCs.

The popularity of these ports, combined with Windows' increasing 'plug and play' (where no additional product-specific software is required) support for portable storage devices means that it is now easier than ever for computer users to connect a device to a PC and copy files backwards and forwards in a matter of seconds.

Understanding the dangers

Having understood that any device with storage capacity that can be directly connected to a work PC poses a theoretical risk to the organization, the next obvious question is to address in what ways that 'risk' can manifest itself.

For the sake of simplification, portable storage devices pose four major threats to the integrity of the organization's systems and data:

Accidental data leakage

Just like analysts agree that around 70 percent of all security breaches occur inside the network, research confirms that 60 percent of security incidents are caused primarily by human error.

Whether it's a foolish employee leaving a USB disk in the back of a hire car (as happened with the Dutch air force), an auditor leaving an unencrypted CD on an airplane (ask Deloitte) or unauthorized staff taking IT kit home (Veterans' Association), the fact is that humans are uniquely skilled at making mistakes when it comes to securing sensitive information.

Research by Centennial Software confirmed this when it discovered that two-thirds of USB sticks are lost by their owners and that 20 percent of mislaid disks have sensitive information on them. Where, as in the examples above, the lost data is unprotected (whether by password or encryption) it is all too easy for anyone 'finding' the lost data to read it and cause huge amounts of cost, disruption and embarrassment.

Identity theft

According to the FBI, identity theft is now one of the fastest-growing areas of crime. In the UK, the Financial Services Authority (FSA) has repeatedly warned finance companies to be on guard for individuals gaining employment within their businesses specifically to access and feed personal data out to organized criminal gangs, who are making great gains from credit fraud etc.

But identity theft doesn't just affect the consumer. Many organizations in the last year have suffered significant financial losses through compensating disgruntled customers, paying for years of credit checks and watching consumers turn their backs in favor of other suppliers.

To highlight how easy it is to defeat an organization's existing security measures, a British tabloid newspaper recently purchased thousands of UK customer financial records from an Indian call center worker.

Industrial Espionage

Stealing company secrets to sell to a competitor may conjure up images of long trenchcoats and darkened alleys, but in truth it's much easier to walk brazenly in through the front door and help yourself to a company's data through one of its PCs.

While a company's email and internet systems may be configured to stop the unauthorized transmission of confidential data files, the huge majority of organizations have no such measures in place to stop an employee, contractor or even an unknown computer user simply copying these files from a PC to a portable storage device.

Productivity and Legal risks

Attitudes on employee productivity vary from company to company. Some say that the cost of letting employees do a limited amount of personal computing at work pays for itself in morale. But few can argue that allowing computer users to bring in malicious applications and offensive content into the office can be a good thing.

Indeed, most companies already have policies and security measures in place to stop employees downloading such content from the internet. But again, there is nothing to stop users putting the organization at risk by accidentally or deliberately bringing unwanted content onto the network through local connections on the PC.

Whether it's lost productivity caused by games and other types of unwanted software, systems downtime caused by Trojans and other malware or the legal risks associated with inappropriate content being stored inside the network, the cost of failing to manage devices being connected to company PCs could cost the organization millions in direct and indirect costs.

The usual suspects

If all potential data thieves wore striped shirts and carried a bag marked 'swag' it would be easy to spot them. Unfortunately, we all know that in real life things are not quite so simple – and that not all data leaks are actually thefts.

However, for the sake of simplicity, there are four identifiable character types that pose a risk to your networks and confidential data:

Accident-prone

Having established that 60 percent of all breaches are the result of human error, it should come as no surprise that the average computer user is potentially the number one risk to data integrity. In fact, 96% of IT directors in financial services companies fear misuse of computer systems by staff (source: Deloitte & Touche).

It's not that these employees are malicious or deliberately negligent – it's primarily the organization's fault for not putting measures in place to prevent mistakes being made.

Whether it's a well-intentioned employee taking data home to work over the weekend or an ambitious new joiner bringing in files from his home PC, there is massive potential for sensitive files to be lost or disruption to be caused by malicious code being transferred onto the network.

Opportunist

It's a commonly-held view that the majority of thefts are not masterminded by criminal geniuses, but are the result of an opportunist – whether an employee, contractor or visitor to the office – taking advantage of the moment.

Recent research estimated that around 70 percent of employees have helped themselves to employer's data, with 72% saying they rated it alongside lying on an insurance claim.

Leaving PCs unprotected will be viewed by some individuals as an invitation to help themselves to your data. And special new software programs designed to automatically run from USB flash drives and U3 devices (Check out Abe Usher's "slurp.exe" on the web – it perfectly illustrates just how easy and potentially dangerous this is) make it easy for the opportunist thief to harvest hundreds of files in less than a minute.

Disgruntled

For a variety of reasons, staff can fall out of love with their employer – perhaps due to disciplinary action, impending redundancies or a missed pay rise. When this happens, there is often a temptation for individuals to help themselves to company data, whether because they believe it will help them in the next job, either to cause disruption to a soon-to-be-former employer or because they think they can gain financially by making the data available outside the organization.

A pertinent example of this is the ongoing trial of a former UBS systems administrator, accused of loading a 'logic bomb' virus onto his employer's network which cost the firm \$3.1 million to repair.

Criminal

With the Financial Services Authority (FSA) explicitly warning companies that organized criminal gangs are infiltrating call centers and branches in order to gain access to highly-confidential customer account information, no-one can underestimate the dangers of the determined criminal.

While hacking into systems from the outside might still be seen as the more likely threat, the truth is that more and more data theft and disruption of systems is happening from the inside.

No matter how and why the threat originates, the result can be just as costly and disruptive. Thankfully it's not as difficult as you might expect to combat the majority of the risks. Simply deciding and enforcing who can and cannot use different types of portable storage devices on the network is a major step towards minimizing the risk of data leakage.

Social Engineering – the USB way

To help highlight the dangers associated with portable storage devices, a US security consultant recently conducted an experiment into “USB social engineering” to test whether a client’s existing security policies and technologies were up to the job.

Steve Stasiukonis, founder of Secure Network Technologies, left a number of unmarked USB sticks lying around outside a client’s offices early one morning, and was unsurprised to observe that it did not take long for employees to start picking the devices up.

Within three days of starting the experiment, 15 of the 20 USB devices littered around the building had been picked up by employees and connected to a company PC inside the office – despite the employees having absolutely no idea what was contained on the memory sticks!

It could have been a virus

What the employees certainly didn’t know was that an associate of Stasiukonis had written a dummy “virus” for the memory sticks – which as soon as the device was connected to a PC, sent a message to a remote server. In this instance, the message was entirely innocent, but it would have been extremely easy for the malicious application to have collected data from the PC and either sent it off-site through an internet connection, or simply collated the information onto the flash disk for later retrieval.

Needless to say, the client was shocked by the results. The experiment has exposed a critical flaw that highlighted failures in policy, training and security technologies. Worse still, the act of dropping these devices around the office carried no risk whatsoever for the perpetrator – compared with physically stealing assets or hacking into the computer system, on this occasion it was the employees (not the hacker) who bore legal responsibility for causing the security breaches.

Freely-available USB hacking tools

While a very eloquent way of drawing attention to the issue, these sorts of actions are not the preserve of highly-skilled security consultants. A number of potentially-harmful tools are already freely available to download from the internet.

Here is just a brief sample:

- **Nmap** – can be used to scan large networks quickly to discover what security technologies are present
- **Ethereal** – intended to be used for network troubleshooting, this tool can be used to sniff all traffic on the network
- **Nemisis** – designed to allow security consultants to test intrusion detection systems, it can help internal hackers figure out how to bypass existing security measures
- **Netpass** – loaded onto a USB stick, this password-cracking application could potentially allow unauthorized parties to log-in to locked PCs

Try it yourself

So if you’re still not sure if uncontrolled portable devices are a problem for your organization, why not take a leaf out of Stasiukonis and leave a couple of devices lying around your office? You might be surprised at how quickly they find their way onto the network.

To read Stasiukonis’ first-hand account of the experiment, visit:

http://www.darkreading.com/document.asp?doc_id=95556&WT.svl=column1_1

Addressing the risks

Having established the risks associated with portable storage devices, now is the time for your organization to consider whether it should:

- Limit the use of portable data storage media and devices except with specific authority
- Automatically record the attempted connection of any and all devices to the corporate network
- Prevent MP3 players, digital cameras and mobile phones being connected to PCs
- Automatically encrypt all data carried outside the network on portable devices
- Amend definitions of 'misconduct' within appropriate HR policies to reflect the new issues facing organizations as a result of these lifestyle devices

If all of the points above sound sensible in principle, but difficult to execute against, the good news is that the vast majority can be done automatically through the use of an endpoint security solution like DeviceWall from Centennial Software.

Put simply, DeviceWall allows the organization to quickly define who in the organization should be able to use what kinds of devices (it hooks seamlessly into Active Directory), automatically allow or block connections depending on the user's privileges (a small client agent manages local security both on and off the network), audit all device connections (it provides graphical and log-style reports), secure data copied legitimately to USB sticks (it uses 256-bit AES and Blowfish encryption ciphers) and react flexibly to one-time usage needs (it features a unique temporary access tool).

Putting the business first

The technical jargon is in brackets deliberately – because while it may be important to your colleagues in IT, they're not the reason that organizations use DeviceWall to manage their endpoint security. Instead, it is DeviceWall's intuitive approach to managing the issue of device usage that makes it the default business choice.

The founding principle behind DeviceWall is that it should support the way the management team wants the business to operate, ensuring that security becomes a commerce enabler not a productivity inhibitor. Likewise, DeviceWall is not a job creation scheme for IT security professionals – it is designed to be managed by your existing staff with no re-skilling or support overheads.

For the wider organization, DeviceWall can be transparent or highly visible, depending on your business culture. If you want to simply enforce your security policies with no exceptions and no excuses, run it silent mode and the users won't even know it's there. Or if you want to ensure that all staff understand why the security policies have been enforced and what part they have to play in maintaining the integrity of the company's network, then take advantage of the many customizable communications dialogs.

To cater for those exceptional occasions where an employee will have a legitimate request to be temporarily exempt from a policy (e.g. a sales representative on-site with a customer needs to take information from a USB drive), DeviceWall supports authorized temporary policy over-rides for both online and offline users.

Any effective security solution must include a thorough and accurate audit log which records all policy changes over time. DeviceWall offers both an immediate snapshot of the current policy deployment status as well as a full log of all incremental changes, including the issue of temporary access permissions. What's more, the security application is self-healing, so PCs will automatically update themselves with the latest policies without user intervention.

DeviceWall from Centennial Software is the only solution to address the need to manage portable devices and data in an intuitive and comprehensive fashion – providing access to all key administrative features through a single control interface and automatically integrating with Active Directory.

Examples of DeviceWall in use

To help you understand why DeviceWall is critical to managing the risk of data leakage, identity theft and legal liability within your organization, the following real-life examples explain how Centennial Software's endpoint security solution has already saved companies like yours millions in averted risk:

Scenario 1 – "DeviceWall stopped me copying confidential files"

Contractor Jonathan doesn't mind how he makes his money, either from the companies he works for or the people who would pay for the information he has access to. But his attempts to copy customer account information from an unmanned PC were thwarted by DeviceWall, which blocked access to his PDA.

Without DeviceWall in place: Jonathan could have easily copied more than 1GB worth of customer databases or records to his PDA without anyone being any the wiser. He could have sold the records on for \$3-5 each, while the company could have faced millions worth of compensation and credit-checking claims had the ID theft been successful.

Scenario 2 - "I nearly introduced a virus onto my PC by accident"

Catherine borrowed a USB stick from a friend which she believed had holiday photos on. What she didn't know was that the device was also carrying a virus which could have caused havoc on the network. DeviceWall blocked access to the USB drive, preventing costly damage to files.

Without DeviceWall in place: The virus could have been copied with the document to network, subsequently infecting every other PC used to open a copy of the document. This could have resulted in large amounts of downtime and lost productivity which would have cost the organization hundreds of thousands, if not millions, in lost revenue and remediation costs.

Scenario 3 - "I was offsite and needed urgent access to my CD drive"

At a meeting with an important client, Joe needed to copy files to a CD. While Joe did not normally have privileges to write CDs, his manager agreed that this was a special case and an administrator was able to allow Joe temporary access to write the CD, keeping the client happy.

Without DeviceWall in place: Permanently locking USB drives and other communication ports can be bad for business. Without DeviceWall's ability to unlock the required device remotely, Joe would not have been able to copy the files, potentially losing a major deal for his employer.

Scenario 4 – "My lost USB stick nearly cost us millions"

As a senior manager, it is accepted that Phil needs to sometimes carry sensitive information around with him on the road. But thanks to DeviceWall's ability to automatically encrypt all data copied to his USB flash drive, when he inadvertently left the device in the back of a New York cab, he knew that while the device was lost, at least no-one could read the financial forecasts contained on it.

Without DeviceWall in place: Phil would probably be looking for a new job and his employer could be facing millions in lost revenues or compensation claims. Without strong encryption in place on devices such as USB sticks, they are highly vulnerable to data theft and misuse if they are mislaid. Anyone finding an unprotected USB stick can easily access highly-confidential information that is at best embarrassing for the owner and at worst financial disastrous.

Scenario 5 - "I haven't noticed any difference!"

Marketing manager Sally often uses a digital camera to take product shots for use on the company website. DeviceWall's granular access rights allow her read from her Digital Camera's CompactFlash card but not write to it, ensuring she can continue to perform her duties without putting the organization at risk.

Without DeviceWall in place: The organization would have no insurance policy in place to guard against Sally making an uncharacteristic mistake and exposing sensitive information to unauthorized parties by copying files to an unprotected CD or USB disk.

Calculating the ROI for DeviceWall

While security projects might have once preyed on the nervousness of senior managers to escape the need to justify themselves, current IT spending strategies demand a clear and compelling business case for any proposed initiatives.

To help illustrate the cost and risk mitigation case for DeviceWall, the first set of figures below were taken from the "Information Security Breaches Survey" to help understand the direct financial impact (the indirect cost is harder to calculate, but needless to say adds to the figures published below considerably) of internal security breaches.

Cost of security breaches (prices in UK£ and US\$)

Disruption to business	£50 - £150k <i>1 - 3 days</i>	\$90 - \$273k
Time spent responding	£3 - £6k <i>10-20 days</i>	\$5 - \$11k
Direct cash spend responding	£5 - £10k	\$9 - \$18k
Direct financial loss	£2 - £4k	\$4 - \$7k
Damage to reputation	£5 - £20k	\$9 - \$36k
Total cost directly attributable	£65k - £190k	\$118 - \$346k

Working on the assumption (as supported by a number of analyst firms) that 70% of security breaches are internal – that suggests that the average sizeable organization faces nearly £900,000 / \$1,600,000 of risk due to security incidents behind the firewall.

On this basis, the cost justification for DeviceWall is compelling:

DeviceWall ROI example

Average cost of breach	£125,000	\$228,000
Average number of breaches per year	10 (up to 52)	10
Sub-total Internal Risk (70% of Total risk*)	£875,000	\$1,594,000
DeviceWall (1,000 seats) License	£10,500	\$18,900
Support & Implementation	£18,000	\$33,000
Sub-total cost of DeviceWall	£28,500	\$51,900
POTENTIAL ROI	£846,000	\$1,542,100

Even if your organization is lucky enough to face just one security incident involving portable storage devices in a year, avoiding this risk through the deployment of DeviceWall will save the firm over £90,000 / \$180,000. More realistically, the savings against multiple breaches can be more like £800,000 / \$1,500,000.

With analysts predicting even higher rates of security breaches for 2006/7, can your organization afford not to address the issue of endpoint security?

Conclusion

Although the risk of data theft from the network would appear to be an “IT problem” – the responsibility for leading any project to address this issue must lie squarely with the senior business managers. The risk is simply too great to view the threats posed by portable devices as an IT issue alone.

And while technology like DeviceWall is key to addressing the majority of the dangers, it's not actually the technology itself that is important. The success of any initiative will hang on the businesses ability to continue 'business as normal' without either losing productivity due to over-strict policies or unmanageable technology, or leaving gaping holes in the internal network's security.

As such, Centennial Software recommends a five-step approach to managing the risk of portable storage devices:

- 1. Understand the endpoint security risks**
How many employees use USB sticks, iPods and other portable media devices at work? How often do they connect those devices to the network? Are certain departments more prolific users than others?
- 2. Review the business requirements**
For a minority of employees, using a PDA to keep track of appointments and contacts is an efficient ways to conduct business. However, connecting an iPod to the network and downloading music almost certainly is not. The key is to determine what constitutes a legitimate business need by a department or individual employee – whatever activity is not entirely necessary is an operational risk that needs to be addressed.
- 3. Create a removable device policy**
Existing 'acceptable use policies' (AUPs) may provide some direction on how employees use portable media devices, but are unlikely to provide detailed or enforceable guidelines on device usage. What's more, employees must be aware of the policy through effective internal communication. An example of an effective AUP that addresses the need for USB lock down can be found at www.devicewall.com
- 4. Enforce the policy – intelligent USB lock down**
If there is no electronic enforcement of these written policies, human nature means that breaches will occur. While complete PC lock down is a common method for protecting against USB security breaches, companies must be aware that blanket restrictions of users' access rights will dramatically impact productivity.

However, any tool providing USB lock down must not impede staff from carrying out their daily responsibilities. DeviceWall ensures that individual users have access to the devices they need to use, while automatically blocking all unauthorized connections by default.
- 5. Educate, review and repeat**
Don't leave staff in the dark. Communicate that security software has been deployed to help enforce the acceptable use policy that has been established. DeviceWall can help you achieve this by delivering configurable messages to users at deployment, logon and when they attempt an unauthorized connection.

Once deployed, it is important to continue monitoring device connections to spot trends and ensure that the policy is consistent with the current perceived level of threat. Again, DeviceWall's 'Connection Auditor' ensures that managers have full visibility of the devices being connected to company PCs and that a full audit trail is maintained for future reference.

To date, some organizations have been lucky to escape internal data theft, some have faced very public and costly breaches, while many more are losing data every day without even knowing it. What is certain is that more and more breaches are being reported in the international media and that consumers are becoming wiser to the risks and less tolerant of lax security practices.

Those companies that continue to ignore the threats posed by employee-facing network access points not only risk the loss of intellectual property, but more importantly, the company's reputation and financial position.

Next Steps

To find out more about how DeviceWall can help your organization manage the threats associated with uncontrolled portable storage devices, either visit our website or contact one of our security specialists today:

www.devicewall.com

UK & International	+44 (0)1793 836200
USA	1 503-238-7455
Asia Pacific	+61 2 9025 3966

Further reading

A selection of guides and white papers are available from Centennial Software, including:

- Taking control of devices
- Effective IT policies – building the perfect AUP
- The threats of lifestyle computing

Each of these papers can be downloaded free of charge from www.devicewall.com

About Centennial Software

With more than four million licenses sold to blue-chip organisations around the world, Centennial Software is a leading developer of IT asset discovery and security management solutions. Available through a global network of resellers and market-leading OEM vendors, Centennial Software's solutions are designed to help organisations better manage their IT infrastructure, maintain compliance and reduce operational risks.

The company operates offices in the USA, UK, Germany, South Africa and Australia. For more information about Centennial Software, visit www.centennial-software.com.

STOP PRESS!

DeviceWall has been named Techworld's "Security Software Product of the Year" for 2006.



© 2006 Centennial Software

Glossary

- AUP –** An Acceptable Use Policy (AUP) is used by many organizations to inform employees how they are expected to behave on the corporate network. However, many AUPs fail to address the risks of portable storage devices and the majority of AUPs are poorly communicated and monitored, which makes them impossible to enforce.
- Data Leakage –** This broad term covers all unauthorized exposure of company information to unauthorized parties. As such, this can include the theft of data, the loss of data in transit or the accidental exposure of data through human error.
- Endpoint Security –** All PCs on the network can be considered ‘endpoints’ as, thanks to developments such as CD burners and USB ports, they are often the last link in the chain between the corporate network and the outside world. As such, “endpoint security” is a broad term that covers any measures taken to protect the endpoint from creating a risk to the wider organization.
- Smart Phone –** A mobile phone with the capability to carry additional information types such as business documents, emails etc. Smart phones can typically be connected directly to a PC through a local or wireless communication.
- USB Flash Drive -** Often referred to as a ‘memory stick’, ‘thumb drive’ or ‘USB stick’, these small storage devices can hold up to 64GB of data and can connect directly to any PC with an unprotected USB port.

Sources

Understanding the dangers

1. "Breaches attributed to error", NetworkWorld, 18 April 2006

Despite all the attention organizations are devoting to security, mistakes still happen. A recent survey from the CompTIA shows that human error was responsible for nearly 60% of IT security breaches in the past year.

<http://www.networkworld.com/newsletters/itlead/2006/0417itlead1.html>

2. "Officer lost memory stick with details of Afghan mission", Expatica.com, 2 Feb 2006

The Dutch military is red-faced following the revelation it has let confidential information slip through its fingers - twice.

The military recently had to own up to losing a USB memory stick with sensitive information. Then the news division of broadcaster RTL reported on Wednesday it had come into possession of top-secret information from a second misplaced memory stick.

http://www.expatica.com/source/site_article.asp?subchannel_id=1&story_id=27303&name=Officer+lost+USB+stick+with+details+of+Afghan+mission

3. "Auditor loses McAfee employee data", ZDnet.com, 23 Feb 2006

The disc contained personal details on all current U.S. and Canadian McAfee workers hired prior to April 2005 and on about 6,000 former employees in the same region, MacDermott said. (The security company currently has approximately 3,290 employees worldwide.) The information wasn't encrypted and potentially includes names, Social Security numbers and stock holdings in McAfee.

Deloitte & Touche confirmed the incident. "A Deloitte & Touche employee left an unlabelled backup CD in an airline seat pocket," a representative for the professional services firm said.

http://news.zdnet.com/2100-1009_22-6042544.html

4. "All veterans at risk of ID theft after data heist", MSNBC, 22 May 2006

America's veterans were sent scrambling for their credit reports Monday, as the Veteran's administration announced nearly all of them — and some of their family members — were at heightened risk for identity theft.

A long-time analyst at the massive federal agency was blamed for the theft of 26.5 million Social Security numbers after he took home sensitive data and his home was burglarized, the agency said. Now the VA is sending letters to every living veteran and some of their spouses with the bad news.

<http://www.msnbc.msn.com/id/12916803/>

5. "Banks face prosecution over Indian call centre leak", silicon.com, 23 June 2005

The security leak was discovered following an investigation by a newspaper reporter from The Sun, who was able to buy bank account, credit card, passport and driving licence details of UK bank customers for just £4.25 each.

The call centre worker in New Delhi also told the reporter he could supply confidential data from 200,000 accounts per month. The newspaper handed a dossier with all the details to the City of London police.

http://www.silicon.com/research/specialreports/offshoring/0_3800003026_39131387_00.htm

The usual suspects

1. "Trial exposes the internal threat", *Computin (UK)*, 22 June 2006

The court trial of Roger Duronio, the systems administrator who allegedly crippled investment banking giant UBS's computer network, is a timely reminder of the security threats that businesses face from their own employees.

www.computing.co.uk/2154068