

Disclosure

Why companies need automated, always-on security to protect their endpoints & data – and avoid the watchdog's bite.

Executive Summary

The UK and European data watchdogs are now getting teeth, and the bite they will be able to inflict on organisations that lose personal data is set to be both painful and costly.

With data breaches becoming an everyday occurrence, the powers of the Information Commissioner's Office (ICO) are to be extended from April 2010. This will enable it to fine companies that recklessly or maliciously breach the Data Protection Act.

What's more, in October 2009 the EU passed its data breach notification rules, to be introduced in member states in 2011. Although these currently apply only to telecoms service providers, the EU has committed to extending the regime to all organisations that process personal data, such as online retailers and banks. Draft legislation will be presented as soon as 2011.

These rules will mean stiff sanctions for organisations that do not comply with the rules, as well as significant costs for notifying affected individuals.

So how do companies ensure that they protect sensitive data on business laptops, USB memory sticks, DVDs and removable storage – and avoid the watchdog's bite?

This document looks at emerging data breach legislation, what it means to businesses, and at how they can manage and protect data on vulnerable endpoints to avoid losses.



Data breach legislation – how did we get here?

It's now over two years since the largest ever UK data loss, when HMRC misplaced two unencrypted CDs with data on all 26 million child benefit claimants. Since that breach in November 2007, reports of laptop thefts, lost USB flash drives and other data breaches have become a mainstay of media headlines.

In 2008 and 2009, the UK ICO reported breaches from over 720 businesses, government bodies and charities – or around one data loss event per day. With media and public concern growing over how organisations handle individuals' data, the ICO has moved to extend its powers beyond enforcement notices and warnings to actual penalties, in line with similar developments in Europe and the US.

This move has been driven by ongoing data breaches, and by the slow uptake and deployment of endpoint security solutions that would help to prevent breaches happening.

In December 2009, Check Point surveyed UK companies in both the public and private sector on their use of data encryption. Less than 50% used any encryption on company laptops and mobile devices. This figure is almost identical to the results of a survey Check Point conducted in November 2007, using a similar survey sample. In fact, in two years, encryption uptake grew by just 1%

This pattern of low encryption uptake is also found internationally. A recent Ernst & Young survey on 1,900 companies in 60 countries found that just 41% of respondents encrypted data on their business laptops, with only 17% planning to do so in the next 12 months.

This is significant for several reasons. The overwhelming majority of breaches have occurred because laptops or removable storage media were lost or stolen, and the data stored on them was not encrypted.

In 2007, only 48% of UK organisations had encryption deployed. In 2008, this had increased by just 1% - and remained the same in 2009

Source: Check Point / eMedia survey

Yet encryption technology is mature, readily available, and easy and relatively affordable to implement. The impact to users during deployment and everyday use is also low. In other words, there are few serious barriers to deploying encryption.

With this in mind, it's no surprise that international regulatory bodies feel it necessary to introduce tougher legislative measures against organisations that handle data in a careless or reckless way.

When the UK deputy information commissioner welcomed the ICO's new powers, he also made the intentions behind them crystal clear. The ICO statement read:

“We are keen to encourage organisations to achieve better data protection compliance, and we expect that the prospect of a significant fine for reckless or deliberate data breaches will focus minds at board level.”

So the intention is push responsibility for data breaches and losses up and out of the IT department, and into the boardroom. Let's take a closer look at what emerging data breach regulations will mean to businesses – and the likely penalties and costs of non-compliance.



New legislation gives regulators teeth

In late 2009, there were two significant moves toward the introduction of data breach legislation with real, enforceable penalties, at both UK national and at EU-wide level.

Breaches of the UK Data Protection Act (ICO)

From April 2010, the ICO, the UK's privacy watchdog will be able to fine companies that breach the Data Protection Act (DPA) through either 'reckless or malicious' practice.

Previously, the ICO's strongest sanction was to serve enforcement notices to organisations that had caused breaches, requiring them to improve data security or face legal action. The UK Ministry of Justice is consulting on the maximum fine that can be levied on a company, with the current proposal set at £500,000.

Also, penalties are not limited only to companies responsible for data breaches. Under its new powers, the ICO could also fine organisations that have:

- Stored or processed personal data in a country outside of Europe that does not have adequate data protection legislation
- Obtained personal data unlawfully
- Accidentally deleted that data

These measures are intended to draw a line in the sand and set clear, basic standards for handling, storing and processing personal data.

European union data breach notification

In October 2009, the EU agreed on the introduction of rules on the reporting of data security breaches. The current requirements only apply to providers of electronic communications services (telecoms service providers, ISPs etc), and member states will be required to introduce the rules by 2011.

But the EU has also committed to extending the breach notification regime to all organisations, which process personal data, such as online retailers and banks. Draft legislation on this extension will be presented in the next 12 months.

The key elements of the new provisions are a:

- Duty to notify the relevant national regulator "without undue delay"
- Duty to also notify the affected subscriber or individual if the breach is "likely to adversely affect" that individual's privacy" except where the provider can demonstrate it has applied "appropriate technological protection measures" which render the data unintelligible to unauthorised users (in simple terms, if a company has encrypted the data using a recognised, strong encryption process, it can avoid notification)
- Power for national regulators to audit providers' compliance and to impose appropriate sanctions for non-compliance



Disclosure

The new legislation also boosts existing provisions in the Privacy & Electronic Communications (PEC) Directive, which already mandate “appropriate” technical and organisational security measures, with the following minimum standards:

- Ensuring that personal data can only be accessed by authorised personnel
- Protecting personal data against unlawful or accidental destruction, loss, alteration, storage, processing, access or disclosure
- Ensuring the implementation of a security policy

However, fines for data breaches are not the only penalties facing organisations that breach data handling regulations. There’s also the issue of the costs of notifying the parties affected by the breach.

Notification costs

The main precedent for data breach disclosure laws, and the index for the costs of notification following a breach is California SB 1386. Following its introduction in that state in 2002, over 30 other US states have introduced very similar legislation.

California SB 1386 requires organisations to notify affected individuals if there is a possibility that personal information may have been exposed by a data security breach. This means organisations have to spend hundreds of thousands – even millions – of dollars following data breaches that involve individuals’ personal information.

In many cases, meeting the notification demands of the law has a greater financial impact than fixing the data breach itself. Since the introduction of California SB 1386, analyst Gartner estimates that organisations spend on average at least \$90 per personal record, for each data breach. Research body, The Ponemon Institute states the cost is still higher, at up to \$140 per personal record.

Notification costs include:

- Communication with affected individuals
- Customer service costs (call centres, credit protection and so on)
- Identity theft monitoring services
- Professional fees and legal expenses
- Clean-up costs and security improvements

The result of this emerging legislation is that organisations will face a very strong financial impact if it is proven they handled data recklessly, or carelessly.



Avoiding the watchdog's bite

The previous sections paint a somewhat gloomy picture. However, while the data breach legislations mentioned here vary in content, they all have one key point in common.

That is a 'safe harbour' provision, if the organisation can prove it took reasonable steps to protect data prior to the breach. Let's look again at the wording of the EU Data Breach Notification provision mentioned earlier:

"... except where the provider can demonstrate it has applied "appropriate technological protection measures" which render the data unintelligible to unauthorised users."

By implementing data encryption to secure information on laptops, removable storage media (such as DVDs, flash drives, removable hard disks and so on), together with appropriate security policies, organisations can demonstrate they applied due care and appropriate measures to protect data, and avoid penalties and disclosure costs in the event of data loss or theft.

Of course, the benefits are not just financial. There's also the reduction in overall risk; increased goodwill from stakeholders; an improved image and reputation for the organisation.

Deploying effective data security at endpoints

When correctly deployed, an effective data encryption solution will help you to:

- Avoid the costs of notification and remedial action following the loss or theft of a laptop or storage device
- Cut the risk of loss of sensitive or legally protected data
- Eliminate legal liabilities of data breach disclosure
- Prove that information, although lost, cannot be accessed or exploited by unauthorised parties

A closer look at endpoint data security

Although the data breaches we see in media headlines are usually caused by the loss or theft of a laptop computer or a USB memory stick, it's important to note that all computers within an organisation – both desktops and laptops – are endpoints, with access to sensitive data. So all computers should have data security controls installed.

These controls should include:

- Full-disk encryption with pre-boot authentication
- Port/device control software
- Removable media encryption



Encryption is the process of making data unreadable to anyone except authorised users, usually requiring a key or password to decrypt the data and render it readable again. 'Full-disk' encryption simply means that all data on the computer is encrypted, all the time.

In other words, the user does not have to remember to apply encryption, nor do they have to choose what data or files need encrypting: it's all done automatically, without the user being able to affect the process. This is a key point that we will return to shortly.

Support for multi-factor authentication options, such as smart cards and tokens, can provide an additional level of security. In the past, encryption has been cumbersome to execute on endpoints and has impacted system performance. However, newer encryption solutions and improvements in computers' processing power have solved these issues.

Port / device control allows enterprises to centrally manage the use of individual ports on an endpoint. One practical benefit is the ability to block unauthorised transfers of protected data from an endpoint to a removable media storage device such as a USB flash drive. Additionally, some solutions allow enforced encryption of any data transferred to an authorised removable storage device.

For these security solutions, it's important for administrators to have central visibility and control over endpoints to ensure compliance with the organisation's security policies. For example, that means having the ability to update computers in the event of user or policy changes, see reports of what data has been copied to removable media, schedule security updates, and view resulting reports.

From policy to practice – taking human error out of the loop

The ability to centrally enforce security policies with IT solutions is critical in data security. Over the past two years, many of the data breaches that hit the headlines were blamed on individuals who ignored security policies.

This way of thinking masks the real problem. The vast majority of breaches happen not because of malicious behaviour, but because a well-meaning person was just trying to save a little time, or get their task done faster.

In most cases, the person is aware of the organisation's data security policy – but they thought it would be OK not to follow policy, just this one time. It's human nature.

So shouldn't we look beyond finger-pointing blame games, and instead address the issue? One CSO reported recently that he felt his job was primarily "to protect users from themselves."

The solution is to automate the process so that security is applied automatically to the data in any circumstance – whether on shutting down a laptop, or copying data to a memory stick or CD. The security also needs to conform to policies determined by the IT department.



"My job is to protect users from themselves".

The CSO of a leading UK plc

This is why data security controls should be on every computer in the organisation, and centrally managed by the IT team to ensure that policies are always enforced, and that users cannot tamper with, or work around, the data security solutions.

The solution should also only interrupt end-users' work when absolutely necessary, such as for security warnings, and remain transparent otherwise. The less the user is aware of the solution – and latest generation products are highly transparent – the better the resulting security.

The 'Holy Grail' of endpoint security is to give the IT team central management of all security functionality and endpoints - including configuration, deployment, client and policy updates, password recovery, reporting and deactivation.

The combination of always-on, transparent security and easy, central management helps to eliminate a significant source of risk while minimising exposure to data breach disclosure laws.

A case in point: Michael Page International

Michael Page International was founded in 1976, and is one of the world's leading professional recruitment agencies. Employing more than 5,000 people in 166 offices across 28 countries worldwide, Michael Page sources permanent, contract temp and interim employees for clients ranging from global multi-nationals to small and medium enterprises (SMEs).

The company wanted to secure its confidential data on both office-based PCs and its fleet of 50 laptops used by directors, senior management and IT staff.

Head of IT Security, Graham Taylor said: "Confidentiality is absolutely essential in our business – our clients and applicants depend on it. As part of an ongoing drive to improve data security, we identified the need to better protect desktop and laptop computers against the risk of data loss or theft. With around 300 PCs in 65 offices across the UK, we needed a solution that was easy to deploy and control across a distributed network."

Following an evaluation of possible solutions, Michael Page chose the Check Point Full Disk Encryption and Media Encryption products.

Automated, transparent security

Check Point Full Disk Encryption provides automatic real-time encryption of a PC's entire hard drive, which can be configured to meet the customer's needs. Pre-boot authentication increases security by requiring username and password before the operating system loads.

Check Point Media Encryption was chosen for its full control over USB ports, devices and media drives, its centralised management, and ability to provide complete audits of device usage.



The solution prevents unauthorised copying of sensitive data by combining port and device management, content filtering and centralised auditing with robust media encryption. This plugs potential leakage points and logs data movement to and from any plug and play devices, providing comprehensive control of security policies.

The products give businesses automated, industry-proven solutions that deploy quickly and easily to protect all sensitive data. They are also scalable to meet the needs of any sized company. The Check Point solutions were deployed on desktop PCs in Michael Page's 65 UK offices, and on its laptop fleet.

Auditing and managing usage

A key benefit is the ability to audit and control data being copied to removable drives and storage media from office-based PCs. The Media Encryption solution gives centralised, granular management over these functions.

The Full Disk Encryption solution protects sensitive data on the laptops used by Michael Page's directors, senior management and IT personnel. Graham Taylor said: "It means the user doesn't have to make any decisions about what data needs protecting – unlike file-based encryption solutions. With the Check Point product, the security is always on and data encrypted on the fly, keeping confidential records safe and removing the responsibility from users. What's more, users report little or no difference in computer performance.

"Both Check Point solutions have been 'fit and forget' after initial set-up. We now have complete control over these endpoints, and any changes we need to make, such as giving a member of staff permission to use a USB device, are quickly done."

Learn more about protecting your organisation's endpoints and reputation

Check Point is the global leader in network security, endpoint security, and security management. The company offers the industry's most comprehensive endpoint security solutions, which deliver unified security controls on every endpoint, while simplifying management of endpoint security across the organisation.

For more information about Check Point Endpoint Security and other solutions, visit http://www.checkpoint.com/products/endpoint_security



About Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. (www.checkpoint.com), the worldwide leader in securing the Internet, is the only vendor to deliver Total Security for networks, data and endpoints, unified under a single management framework. Check Point provides customers' uncompromised protection against all types of threats, reduces security complexity and lowers total cost of ownership. Check Point first pioneered the industry with FireWall-1 and its patented stateful inspection technology. Today, Check Point continues to innovate with the development of the Software Blade architecture. The dynamic Software Blade architecture delivers secure, flexible and simple solutions that can be fully customised to meet the exact security needs of any organisation or environment. Check Point customers include tens of thousands of businesses and organisations of all sizes including all Fortune 100 companies. Check Point's award-winning ZoneAlarm solutions protect millions of consumers from hackers, spyware and identity theft.

CHECK POINT OFFICES

Worldwide Headquarters

5 Ha'solelim Street
Tel Aviv 67897, Israel
Tel: + 972-3-753 4555
Fax: + 972-3-624-1100
email: info@checkpoint.com

U.S. Headquarters

800 Bridge Parkway
Redwood City, CA 94065
Tel: +1 800-429-4391 ; 650-628-2000
Fax: +1 650-654-4233
URL: <http://www.checkpoint.com>

©2010 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check Point Endpoint Security, Check Point Endpoint Security On Demand, Check Point Express, Check Point Express CI, the Check Point logo, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoreXL, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Full Disk Encryption, Hacker ID, Hybrid Detection Engine, IMsecure, INSPECT, INSPECT XL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpect, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management, Power-1, Provider-1, PureAdvantage, PURE Security, the puresecurity logo, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Security Management Portal, Sentivist, SiteManager-1, Smart-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartProvisioning, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartView Tracker, SMP, SMP On-Demand, SofaWare, SSL Network Extender, Stateful Clustering, Total Security, the totalsecurity logo, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, UTM-1, UTM-1 Edge, UTM-1 Edge Industrial, UTM-1 Total Security, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power Multi-core, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VSX, VSX-1, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm ForceField, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone Labs, and the Zone Labs logo are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. ZoneAlarm is a Check Point Software Technologies, Inc. Company. All other product names mentioned herein are trademarks or registered trademarks of their respective owners. The products described in this document are protected by U.S. Patent No. 5,606,668, 5,835,726, 5,987,611, 6,496,935, 6,873,988, 6,850,943, and 7,165,076 and may be protected by other U.S. Patents, foreign patents, or pending applications.