

Protecting sensitive information in transit

Encrypted USB devices from MXI Security

Chris Mellor December 14, 2007

For the City of London Police, information leakage isn't just business critical, it is a matter of life or death. Loss of life could be the ultimate price to pay should sensitive data being transported by police officers be mislaid. That's why the City of London Police has taken industry-leading steps to make sure that an electronic data breach remains unlikely.

The City of London Police is also involved in implementing the Home Office IMPACT program, designed to improve the ability of the UK police service to manage and share information between police forces to prevent crime and provide safer communities.

Protecting its electronic borders

Defining best practice in this field has also required the City of London Police to develop a model IT governance policy in order to protect information within and from outside its own network. Over the last five years, the force has taken sweeping measures to protect its electronic borders and defend the integrity of its information. In addition to a comprehensive and rigorous IT security policy, all potential points for electronic data leakage have been systematically identified and secured.

As well as safeguards against unauthorized electronic transmission of data, the City of London Police has taken steps to prevent "thumbsucking" – the unauthorized copying of data on to portable storage devices. To achieve this it has locked down USB computer ports on all computers – and not with superglue.

However, the force also recognized that a complete system lockdown would be counterproductive, as officers and administrative staff still need to physically move data around during investigations and operations, and when interchanging intelligence with other forces, such as the neighbouring Metropolitan Police. Therefore, the City of London Police has established and implemented secure procedures for anyone who wants to bring in or take out digital information – issuing secure, personal portable storage devices to authorised officers and civilians.

USB ports

The threat of electronic data leakage came to the forefront when the City of London Police upgraded to a Windows 2000 Professional-based network in 2005. Beforehand, the unauthorized copying of data was less of an issue since USB ports were simply not recognized by the earlier Windows NT 4.0 operating system, and all USB devices were disabled at system BIOS level. However, in planning the upgrade, Gary Brailsford-Hart, the City of London Police Head of Information Management, was well aware of the new challenges he would face.

After evaluating various options, Brailsford-Hart chose to secure all USB ports with DeviceLock, a sophisticated solution that not only controls device-level access but also logs information copied to and from permitted USB devices and drives.

Secured USB ports required secured USB devices

To harden the security policy, City of London Police regulations state that officers and civilians may only be issued with portable media devices once they have successfully submitted a written risk assessment – with the policy applying to all portable storage media, from a humble 1.44MB floppy disk drive through to portable hard-drives with capacities running into hundreds of GB.

This comprehensive set of measures ensures watertight control of portable storage devices within the police network, but it Brailsford-Hart looking for the missing link in the puzzle: control of portable storage and the possible consequences should sensitive, unprotected data be lost or stolen while outside the force's four walls.

He said: "Information leakage represents the greatest risk to our integrity. There is a risk to life if information from our systems is released publicly."

To solve this, the City of London Police bought a number of password-protected or biometric USB devices and put them to the test. "In general, we found that most of the devices were not up to our needs," explained Brailsford-Hart. "Most devices were physically not very robust, and user-activated software places too much reliance on the user to encrypt. We wanted something more."

Uncrackable Stealth MXP

Clear winner of the rigorous testing procedure was the Stealth MXP device from MXI Security. "Our first impression of the Stealth MXP product was that it was immediately attractive, thanks to the physical security controls being protected by a robust case with a retractable USB port – because we'd had a number of other devices that were physically broken during the pilot and returned in various states of disrepair."

The City of London Police then decided to run a pilot programme for Stealth MXP and issued 10 devices to a test team. "We took the approach of granting least-effective rights, which meant we took the smallest memory size. From an information management perspective, I want to limit the amount of information that people can carry on these devices. The bottom line is that these devices are ideal as a transit medium, for carrying around a number of documents and images, but users are discouraged from using them as a storage medium," said Brailsford-Hart.

"We gave a Stealth MXP device to our internal high-tech crime unit and asked them to break into it. They were unable to do so and therefore gave us the thumbs up," he recalls.

Stealth MXP was confirmed by the City of London Police as its default device for carrying sensitive electronic data and devices are available to any officer, on request.

Deployment

Currently, more than 100 units are in the field, used by plain-clothes and uniformed officers of all ranks, and civilian administrators, including members of the senior management team.

Within the City of London Police, so far, no devices have been lost in the field, and the casing has provided protection against wear-and-tear. All devices are tracked by the force's Crypto-Custodian, whose duties involve issuing Stealth MXP devices and auditing the materials that users store on them.

"Users are duty-bound to report loss, and we also want to see what material people are putting on the devices, so that if necessary we can make sure they are aware of procedure," said Brailsford-Hart. "We make sure that devices are used for the transportation of data, not for general storage."

In the field, Police Officers gathering information from external sources – such as other police forces and court services – use Stealth MXP devices for secure transportation of this information to the three City of London Police main police stations, where intelligence data is consolidated.

The force also has hard-drive based Outbacker MXP units from MXI Security – offering the same strong biometric authentication benefits but larger data storage capacities. These units are reserved for Special Operations, says Brailsford-Hart, including a now-completed "multi-agency anti-terrorism exercise".

"The deployment of Stealth MXP has given us an additional level of accessibility to transfer data that we did not have before," says Brailsford-Hart, who himself uses a device for transporting all files relating to the City of London Police's IT security strategy. "Whatever is on there is safe should the device get into the public domain. I have the confidence to trust that this information would be secure, regardless of the circumstances in which it was lost."

As Chair for Information Management of the Police Service, Brailsford-Hart has also underlined the intrinsic value of using Stealth MXP to other police forces, both at home and abroad.

With MXI Security devices in daily use in the field, Brailsford-Hart confirms that the availability of secure, portable storage devices is something he would not want to do without. Not only do the Stealth MXP devices provide convenience but they are also the force's insurance policy against the unplanned or accidental loss of highly-sensitive data.

Brailsford-Hart acknowledges the huge implications of one officer losing just one unsecure USB stick holding confidential data. "Our data is of significant importance to the public in the UK," he says. "If an officer stored information on an insecure device then left it on a train, it could cost us millions, or even lead to loss of life. For me, avoiding that is the best return on investment."

This article was printed from **Techworld** : www.techworld.com The UK's infrastructure & network knowledge centre © 2006 : All rights reserved
[Click here to close this window and return to the website](#)