

Durable defence against data loss

Joseph Souren, VP and GM EMEA of **Wave Systems**, examines data privacy legislation and presents a compelling case for how current security – built on proprietary layers of software – is proving inadequate, and why a new approach that leverages industry-standard hardware-embedded security is needed.



Banking institutions house a large amount of confidential information. With the global proliferation of data privacy regulations, protecting the customer data contained within endpoint devices is a top priority if banks are to preserve brand integrity and ensure goodwill.

Throughout Europe, there is strong impetus to produce tougher data breach reporting regulations. Most countries have formal Data Protection Authorities that monitor and actively audit company compliance and reporting procedures; in many countries, including Germany, Luxembourg, Belgium and France, failure to comply can result in substantial fines and/or imprisonment. The topic of data loss is attracting increased attention at an international level, most recently at the global conference chaired by William Hague, the UK's First Secretary of State and Secretary of State for Foreign and Commonwealth Affairs.

A key issue is the need for companies to provide proof of compliance and data protection reporting procedures – tasks that are becoming increasingly complex and difficult, while also placing C-level executives, who may be held responsible for inadequate security, in the regulatory firing line.

“Wave Systems’ secure, robust, and trusted solutions allow financial institutions to take control and re-establish security as a firm policy rather than as a reactive strategy.”

In the UK, enforcement of data protection legislation resides with the Information Commissioners Office (ICO) and the Financial Services Authority (FSA), which can levy fines and issue directives. The FSA requires financial services companies to inform the regulators of any breaches, and last year the association fined Zurich Insurance £2.27 million for losing the personal details (including bank account and credit card information) of 46,000 customers. The fine – the highest ever imposed upon a UK company for a data protection failing – was levied after a South African outsourcing company, employed by Zurich, lost an unencrypted back-up data tape. To many organisations the cost of the fine is insignificant compared with the damage caused to their reputation.

Ever-tightening data protection laws

In the EU, the security compliance and reporting landscape continues to evolve as the scope of breaches expands. Authorities understand the global character of investigations and cooperation is on the rise.

In the US, the Securities and Exchange Commission has issued strong data breach reporting guidelines while simultaneously admitting a defence breach of its own network; California has led the way in terms of data protection compliance and reporting for some years, and Massachusetts and Nevada now also require companies to report data breaches.

The number and breadth of investigations that companies now face, and the scale and severity of the sanctions, heighten the need for a measured and cooperative regulatory approach, according to The Lawyer.com. In fact, lawyers predict social media, privacy, data protection and storage will come to dominate the future legal landscape.

In June, vice-president of the European Commission Viviane Reding announced a crackdown that would make it mandatory for businesses – financial institutions included – to report all security breaches. Commissioner Reding is aware of banks' concerns about the extra work that could be created, but believes that an obligation to notify all serious data security breaches would enhance consumer confidence in data security and oversight mechanisms.

The EU regulations will be enforced very shortly and the UK Government is working closely with the EU to produce similar regulations, with discussions focusing on the extent and nature of what needs to be reported. The ICO is fully supportive of this process.

Banks must review their security, compliance and reporting procedures now to avoid the danger of being caught out by these new, stronger regulations.

20th-century software defences: not up to the job

The fact that mandatory data breach reporting is now a given across the EU (and further afield) should be a compelling reason for the financial sector to conduct a full security strategy review. The problem is that the current security software defences, built in ever more complex layers, are broadly the same technologies that have been in use for the past 20 years.

In order to tackle the new threat landscape head on, banks would be well advised to consider implementing hardware-embedded security based on the standards set by the Trusted Computing Group, an international industry group focused on developing a safer computing environment.

This framework provides companies with the superior defence and assurances needed to address compliance issues, deliver the very best reporting and protect themselves in the more robust regulatory environment over the coming years.

Wave Systems' security framework centrally manages the open industry-standard technology installed in endpoint devices. The Trusted Platform Module (TPM) ensures that only known devices access a company's network, while the use of back-up data tape is being superseded by more secure archive storage services such as Self-Encrypting Drives (SEDs). These secure, robust, proven and trusted solutions allow financial institutions to take control and re-establish security as a firm policy rather than as a reactive strategy.

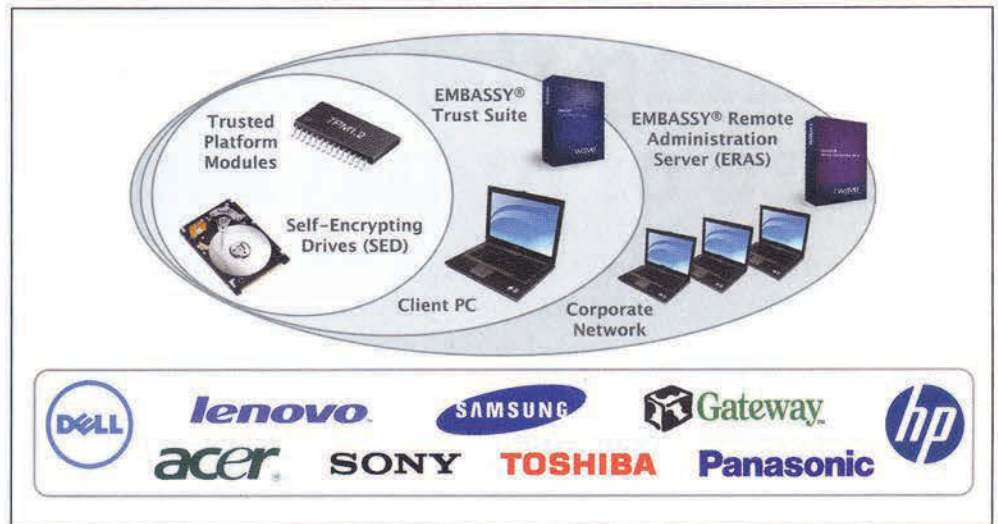
Recent security breaches in the financial sector amplify the need to develop stronger endpoint defences. In the US, Sovereign Bank and Pentagon Federal Credit Union discovered hacked laptops on their networks that could have led to customer data being accessed. Furthermore, back in May more than 360,000 credit card accounts in Citigroup's North America region were affected as a result of its card account management website being compromised.

The financial sector is also familiar with the penalties for failing to adequately protect customer information. Following the theft of a laptop from an employee's home, the UK's Nationwide Building Society was fined £980,000 by the FSA for its ineffective information security control systems.

In South Africa, the Protection of Personal Information (PPI) Bill is shortly to become law. All companies will then be responsible for what happens to their customers' data. If a business device containing customer information is lost or stolen, the company will be responsible. This new law means that robust hard drive encryption is just as essential as defending the device with best-in-class access security.

Security by design

In every other industry, 'security by design' is embedded. For example, in the automotive sector every vehicle comes equipped with a wide range of essential safety devices (airbags, brakes, shatter-proof windscreen, secure locking, alarm, etc.). At the IT security level, however, crucial defence elements are an add-on – security by design should be a key part of the data defence culture. The TPM and SED, which



The SED and TPM are essential components in Wave's hardware-embedded endpoint data security system.

are built into the endpoint device, provide security by design that is easier to manage and more cost-effective over the life of a device than such add-ons.

Trusted Computing offers a more secure way forward and the foundation of Trusted Computing's offering is the facilitatory TPM hardware chip.

The TPM is already installed in half a billion devices and gives any size of organisation – from ten people to hundreds of thousands – secure network access. Activating the TPM in an endpoint device ensures that security keys, which are used for authentication of network devices, cannot be accessed via rogue software processes.

The SED, which stores security access and encryption keys within the device, offers even more robust data storage protection. SEDs boast a circuit built into a disk drive controller chip that automatically encrypts and decrypts all data to and from the magnetic media. This process renders data almost impenetrable to unauthorised access even if a laptop is lost or stolen.

SEDs are also considerably cheaper to manage over the device's lifetime. For example, it will cost about 70% less to protect 1,000 PCs for three years using a managed SED solution than doing so through traditional managed software encryption.

The security that every company in the financial sector needs is designed to open industry standards. Centrally administered through Wave Systems' comprehensive management framework solution, it controls TPMs and SEDs installed within client endpoint devices.

This affords banks and other financial organisations more cost-effective and future-proof data protection and compliance. ■

Further information

Wave Systems
www.wave.com
 Email: sweekes@wavesys.com
 +44 1235 520 956

