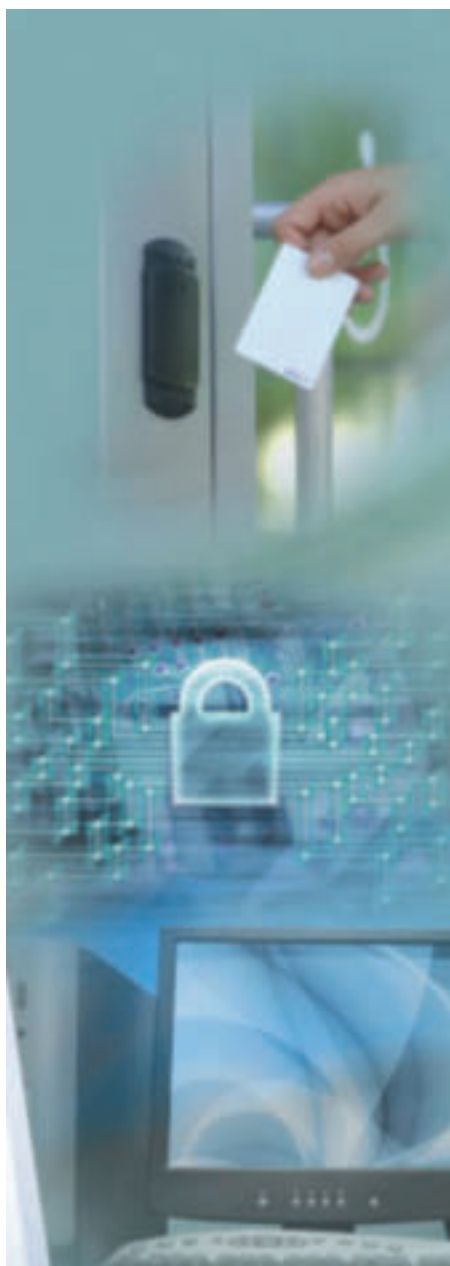


The burden of proof

The case for complying with corporate governance and compliance regulations.
By Geoff Hogan, Senior Vice President, Business Development and Product Management/Marketing, Imprivata



Security is an important part of any organisation's approach to IT. From firewalls and intrusion detection through to one-time password tokens for customers to prevent phishing attacks, the level of investment in new technologies continues to grow. This requirement for security extends inwardly as well, and ensuring that members of staff have access only to the data that they need is a major task. However, there is another consideration for the IT department beyond securing the organisation's buildings, networks and data. Being able to prove that users have followed security policies as well as relevant industry legislation is an ongoing overhead that the IT team has to face.

For example, the banking industry as a whole is covered by various pieces of national, regional and international legislation. A number of financial bodies exist that are responsible for ensuring that processes are in place and best practices are adhered to, such as the Sarbanes-Oxley Act and the Gramm Leach Bliley Act (GLBA). Retailers and other organisations that process payments have the Payment Card Industry Data Security Standard (PCI DSS), which includes rules to follow ensuring that there are controls in place and used by all employees that have access to payment data. Additionally, workers at public sector organisations require access controls to sensitive information on citizens.

Whilst all these areas of legislation cover very different territories and industries, they are all concerned with access to

information and control of data; each of these standards has a specific focus for keeping access secure. The common theme is that organisations have to be audited to prove that they are compliant.

This proof of compliance can be a bigger overall headache than any initial installation as it represents an ongoing requirement. There is also the possibility that the legislation an organisation is supposed to be compliant with can be changed or amended over time. This can also be extended to the organisation's physical security: access to sensitive areas within buildings, or to locations where electronic data is physically stored is also an area that has to be considered. Making sure that unauthorised individuals cannot access data either physically or through the network is a major undertaking, and one that will be subject to the security audit procedure.

Any audit, either internal or external, can lead to a large amount of work for the IT team, as records of which employee has had access to what applications and when have to be pulled together, sometimes from multiple sources. It is not enough to have security technology in place; being able to prove that security policies were followed and sensitive, or confidential data was only accessed by those employees that were authorised to view it, is also critical.

Compiling this list of records across one application or one group of users requires a significant level of resources, and impinges on the ability to support other, more high value activities. For smaller organisations, this represents a



very serious issue that has the potential to affect how IT can support the business going forward.

To combat this, identity management and access control have a strong role to play in reducing the burden that IT teams have to shoulder in proving compliance with corporate governance or relevant legislation. By monitoring all access to applications, all the data on access and user activity can be stored centrally. This can then be automatically put into reports to significantly reduce the amount of time that the IT team spends on this task.

There are two areas of technology that can be integrated to track user interaction while also increasing security. Firstly, strong authentication involves having a second "factor" present for access to data and networks, so that only approved individuals can see sensitive information. The second factor is presented whenever a user has to authenticate themselves, in order to increase security. A good example of this from the consumer world is the Chip and PIN card, where something you have and something you know are combined for greater security. Examples of factors that can be used alongside passwords include one-time passwords, finger biometrics and smart cards.

Secondly, single sign-on (or SSO) is the act of using one strong password or strong authentication modality to grant access to all the applications that an employee is authorised to use, based on their policy; instead of multiple passwords, this one credential can automatically be entered to allow access.

By linking this to each user's network identity, workers will have all the relevant application credentials entered for them whenever they open up an application. All application access requests can be stored centrally and used to generate reports on access activity.

Because all application access requests are tied to the user's network log-in, any sharing of password information between users will show up automatically. As the credentials are captured and stored, employee activity can be tracked.

By linking SSO to strong authentication, the organisation can automatically demonstrate that employees only have access to the data that they are authorised to view, while using a second factor for strong authentication ensures that overall security is enhanced. This combination of technologies can also ensure that the correct security policy is enforced at all times. An example of this is customer record data: if only specific members of staff with their own passwords and smart cards can access the data, this can be shown through the central log of user activity and a report generated over any access request that is made.

The physical security of the organisation will lead to another set of policies that employees will have to follow. Ensuring that these are enforced is now also becoming another task for the IT team to consider, due to the portability of data and the number of staff with USB drives or iPods that could be used to take sensitive information away. Locking down USB ports and installing physical security

systems can deliver some protection, but unless the building security is combined into the overall IT security framework, there is a possibility that these measures can be circumvented.

Linking a door access system to the user's network access can make certain that employees are following the physical security policy. If a user does not present their physical access token when they enter the building, they won't be registered as being present; when they attempt to log-in, the IT security system can query the building access records and if the user is not marked as having badged in, they can be denied access. This approach is designed to automatically enforce compliance with the organisation's rules over security.

Being able to prove that a strong authentication factor was used when required will be an easy way to show that the investment in technology is meeting the demands of the business as well as compliance legislation. There are stiff financial penalties in place for any regulated organisation that has a breach of its IT security system, while such an event can have serious implications for an organisation's reputation. Having proof that the investment in security has been made and doing the job it is intended to do can help the organisation in the event of any crisis taking place as well as mitigating any potential risks.

Being able to demonstrate compliance automatically is a big potential cost saving and ensures that the organisation can show it met the demands associated with its activities. **CS**