

## Pay Now or Pay Later: Obtaining ROI from Security Solutions

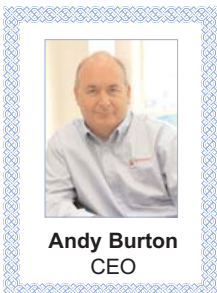
Information security is a top concern for credit unions today and most senior managers are aware of the issues at some level. IT departments are expected to provide a secure network and endpoints along with all the other high-priority projects they have. Unfortunately, most boards are not aware of the range of threats organizations face today. In general, if the company has antivirus software, they think they are covered.

To secure proper funding and prioritization for security projects, there are three primary messages the credit union IT professional must convey to management. First and foremost is to demonstrate that security is not just a technology, but rather how it is an integrated component of effective and efficient business processes. Without effective IT security, the business operates in an environment of unnecessary redundancy in an effort to implement some level of human-based controls. The threat of course, is that manual controls are easily circumvented or not enforced, leaving the credit union vulnerable to data theft, network attacks and compliance failures.

The second message is to educate the board on the range of threats they face today. Most companies have antivirus software and firewall protection and have created a fortress that appears impenetrable. But most are not yet protecting a much more pervasive point of vulnerability – the desktop. iPods, MP3 players, USB flash drives, PDAs and other personal devices can all be used to remove data from the network or introduce viruses or malware. Antivirus and firewall software will do virtually nothing to protect against these threats.

The third and final message that must be conveyed is that of the cost of failing to properly secure the network and endpoints. A security investment is an insurance policy that you hope never gets exercised. However, the example ROI for a project to secure computer endpoints should include specific costs that would arise from just one incident of member data theft:

1. Cost of fines imposed by state and federal regulators
2. Loss of deposits from member defection
3. Loss of deposits from loss of potential members
4. Loss of revenue from loans serviced elsewhere
5. Cost of investigating the data theft incident
6. Cost and disruption from a rush-implementation of security software
7. Loss of goodwill from negative PR



With the appropriate background for educating boards and senior management as well as tools to implement effective solutions, IT departments will be able to implement levels of information security that keep their credit union ahead of the threat curve.

DeviceWall® from Centennial Software is a leading endpoint security solution that helps organizations protect their networks against the threat from the explosion in the use of personal devices such as MP3 players, PDAs and flash drives inside the workplace. DeviceWall supports the way IT Security managers and organizations want to work by taking a process-oriented approach to endpoint security education, enforcement, exception handling and providing evidence of protection.



**Andy Burton** is Chief Executive Officer of Centennial Software, a network discovery and device security solutions provider. Andy is responsible for overseeing the day-to-day operations at Centennial as well as driving the company's strategy to grow its global reseller and customer base. A highly experienced and successful senior manager within the IT security industry, Andy has already played a key role in shaping Centennial's future product roadmap and re-defining the company's go-to-market strategy. Founded in 1997, Centennial Software is a multi-national software company with over 4 million licenses of its solutions sold to blue-chip organizations around the world.