Keep your business information assets safe

Part III: Addressing your Technical Security

This is part three of a four-part series that identifies business information assets, helps business owners understand the value of their information and then explains how best to protect information as a valuable business asset.

In the 13th century, a strong empire required protecting the riches of the kingdom, similar to protecting the assets of your business. Comparing kingdoms of past to our own businesses, the principals are similar but the tools have changed in our modern world. Instead of swords and catapults, the battle to protect business assets must be fought with sound organizational structure, physical logistics and secure technology.

In two previous articles, we discussed how to identify the true value of a business's information and how management needs to establish and enforce policies and procedures to ensure staff is following good security practices. The next piece of comprehensive asset security is technical security – what it is and how it should be approached. When we address the technical aspects of asset security, we are looking at hardware and software.

There are two approaches that I call the "onion" approach and the "perimeter" approach. The perimeter approach is based upon the idea of protecting your castle (business) by only using a moat or high walls (or firewalls in technical terms) to protect the castle's riches. With castles of old, if the enemy was able to get past the moat and castle wall, the kingdom was plundered and destroyed. The problem with the perimeter approach is it doesn't address attacks that are unwittingly permitted from within, such as from employees. This would be similar to a castle with a deep moat and walls made of solid stone, but one of the knights likes to open the door at night for fresh air – or even worse, there's an imposter in the army! Instead of the perimeter approach, I encourage the "onion" approach.

The onion approach builds layers of defense, starting at the perimeter and work inward with your critical asset – your information – at the center. The first layer is the firewall, which is designed to keep unwanted or unauthorized intrusions out. The drawback of the firewall – which may be the single defense mechanism for a business using the perimeter mentality – is it isn't designed to keep things in, only out. It is similar to a guard on the castle wall watching for intruders but not paying attention to people or things leaving the castle. A firewall still allows all company transactions – messages, traffic, critical information, etc. – to be sent to the outside world. This brings us to the next layer of defense.

Intrusion Detection System (IDS) is similar to having a second guard standing at the gate who checks everything going in and out of the castle. IDS looks for patterns of behavior that would be considered hazardous to the well being of the company. Patterns to keep an eye on might be an excessive number of messages to a repeated address or location (IP) or activity within the network that is unusual or inappropriate. If unusual activity is detected, the IDS system notifies the systems administrator or designated person of the activity, allowing them to react and take action.

The next defense layer of the onion approach is the network operating system (NOS). The NOS is like the captain of the guard. The captain of the guard moves throughout the castle ensuring that the guards are in the proper places and doing their jobs. The NOS checks to make sure the right people have access to the right places and unauthorized people are kept out of protected areas. The network determines whether every user is identified and authorized, and once a user is authenticated, it determines where they can go.

Medieval guards were also posted at key points throughout the castle to control access to different areas of the castle. This is similar to routers and switches used in today’s networks. Routers and switches act as transfer points and are the next layer of the onion. They have the ability to monitor and restrict traffic based upon parameters determined by the systems administrator.

The reason for defense is to protect the castle’s crown jewels (your company’s data). This is directly protected by your knights (employees). Then, it becomes essential that your knights have the proper defense tools – an employee’s desktop operating system that has anti-virus and other security programs to directly protect the information.

Using the castle’s entire security program – from the moat to the king’s personal knights – is necessary to ensure the castle’s treasure is protected. Your information is your treasure. In your kingdom, it is essential to have all security measures in place – firewall, Intrusion Detection System, Network Operating System, routers and each employee’s operating system. Each security layer builds on the next layer and adds further protection. As stated in my last article, we must begin with an understanding from the top down. Management – the castle lord – must establish the attitude and policies to promote security and protection of the assets.

Regardless of the size of your system, there is a minimum standard all business environments should follow, including using a desktop anti-virus software that is kept current, automatic update feature with daily updates, desktop software firewall to control access from the outside (even if you are behind a corporate firewall), and corporate firewall that is properly installed, updated and monitored.

Protect your business’s assets properly, and you’ll protect the entire kingdom.