

Time to Rethink Corporate Security

Mobile Workers have made Data More Vulnerable

When you left the house this morning, you locked the front door and quite possibly put the alarm system on. You put a security perimeter in place that would stop criminals from gaining access. For years, your company has probably had the same type of protection; security guards at the front desk, locked doors with pass keys, and a firewall that stops Internet intruders from hacking into your network. Now, an increasing number of experts want you to rethink the basics of corporate security.

One problem is that as companies with distributed offices use data communications to increase efficiencies, those regional and branch offices also become more vulnerable to online attack.

Laptop computers, BlackBerrys, high-speed mobile networks and broadband Internet access allow executives to be more mobile. With many executives accessing company computers from the road, the edges of the organization have become more amorphous.

Firewalls (devices designed to block unauthorized access to networks) have protected networks from intruders, but what happens when an employee who has been surfing the Internet at home on a company laptop infects the whole company network?

Security Levels Key to Protecting the Castle

"Malicious software doesn't care if it sits on a consumer PC, or regular ISP, or on corporate network [*sic*] behind a firewall," says Dave Marcus, security research and communications manager with McAfee's Avert Labs. "That has to be taken into account because when you talk about spam, it's sent out in an undirected way."

Focusing less on the perimeter of the organization and more on the the protection of internal systems is the way forward for IT security, argues Michael Legary, founder of Winnipeg-based IT security consultancy Seccuris.

"Deperimeterization isn't necessarily taking down the firewall, but it's creating a more open, effective business environment by integrating security throughout your technology," he explains.

"We've survived for a long time on the idea of protecting the castle, but it's not appropriate today. We need segmentation, so instead of keeping the bad guys out and the good guys in, we're ensuring that people with different sensitivity levels can only get access to what they want at the appropriate time."

Doing that doesn't necessarily mean taking down the the firewall altogether (you'd be unlikely to ever do away entirely with a castle drawbridge, after all). However, it does mean assessing the vulnerability of your corporate computing assets from a business perspective, building an understanding of how a successful cyber-attack on each of them might impact your ability to run the company effectively.

This risk analysis is one of the first steps towards deperimeterization, says Rob Sadowski, senior manager of technology at security hardware and software vendor RSA. RSA supports an information-centric view of security,



Michael Legary, founder of Seccuris: "Deperimeterization isn't necessarily taking down the firewall, it's creating a more open, effective business environment"

where data is king. "If you agree with that notion that information is data in the hands of a person, you need a process to control that data for all the groups that need access to it," he says.

Understanding how vulnerable that information is to attack involves auditing your computing systems to find out where the risks to them are, says MR. Sadowski, who then breaks down the protection process into three steps: securing the data, securing access and ongoing audit capabilities.

Securing the data involves steps such as encrypting access so that if stolen, thieves won't be able to use scrambled information. Securing access involves steps such as user authentication and access control, but this is more complicated than it sounds. Identity management is a critical component of user access control, Mr. Legary says.

"The actual costs are coming from the technology component—there's a lot of preparation and understanding of identity, and what roles need access to what information. That's where we find the up front costs come from," he says. The technology part—such as the use of single sign-on technology to give an executive access to all the information they're authorized for with a single password—is relatively mature, he adds.

Even identifying the levels of security needed by particular assets can also be a long process, warns Mr. Legary, adding it is partly why he advocates a long-term approach to investment in deperimeterization. "Even though there are a number of up-front challenges that need to be overcome, it typically takes 12 to 24 months for a solution to really get off the ground," he says.

Board-level executives, already hit with significant costs thanks to increased corporate compliance requirements, are unlikely to want to swallow that cost. Mr. Sadowski advises them to look at it as a business enabler, rather than investing out of fear.

"It's not that I put in place protection for my online banking application—it's that when I deploy an online banking application, I need to deploy some security technologies, but in doing so, it raises my revenues and lowers my costs," he says.

Turning the argument around that way is neat sales trick but won't stop executives from seeing investments in deperimeterization as an unwelcome cost of doing business securely. The alternatives, however, are dire. Companies could ignore the need for deperimeterization, assuming criminals won't get past the firewall and discover the soft, vulnerable underbelly of their IT infrastructure. Retail giant TJX Group may have thought that, but the company recently filed a report with the U.S. Securities and Exchange Commission admitting that details on more than 45 million customer's credit cards were stolen over years, using software placed by cybercriminals on its servers.

When critical assets are so easily compromised, you know it's time to take a fresh look at security.

Bradbury, Danny. "Time to Rethink Corporate Security." [National Post](#) 29 May 2007: SR1