**The Death of the Perimeter**
**by Brad Dinerman**
**August, 2012**

"Behold the gallant knight, who returneth now to the castle. Let down the drawbridge, so that he may enter and not be stuck across yonder moat." Security in the year 1100 AD was fairly straight forward. You had a castle, fortified with stone and protected by soldiers with iron helmets, bows and arrows. Emptying cauldrons of hot tar on the advancing enemy was always a nice intrusion prevention system as well. If you wanted to enter the castle, you secured permission from the front sentry who let down the drawbridge, and you easily entered.

Fast forward 100 or so years and the story now reads like this: "Behold the gallant knight, who returneth to the castle. Let down the drawbridge, so that he may enter and not be stuck across yonder moat. Let also his partners-in-cavalry enter through castle back doors, and behold the 2011th Catapult Division which sails without any ropes into the court yard from above. Let us not forget his squires, who tunnel through the castle wall and who bring with them all manners of treasure, though we hope that none drag a captured, wooden horse from the strange lands that they have visited."

Although this example is presented with humor, the point that it makes provides an analogy to demonstrate how information security has changed over the past years. A workforce that has grown increasingly mobile and that now demands always-available access to corporate data has forced management and IT to change not only the systems that they support to provide functionality, but also those that they use to protect the corporate and personal data.

**What Is "The Perimeter?"**

Until fairly recently, the "perimeter," for the majority of organizations, was the delimiter between the corporate workspace and the wild, wild Internet. Systems inside were "trusted;" anything outside was "untrusted" and therefore a risk from which the organization must protect itself. To protect the corporate network, a firewall was typically implemented at the perimeter which would permit or deny access based upon a specified set of rules.

This concept held well, especially for those organizations that had standard workdays and employees that only worked at the office. A vacation was actually a vacation and most users neither needed nor wanted to be connected to the office.

However, the perimeter as we know it has died, or perhaps just evolved.

**A Holy Perimeter**

Technology changes. That's been the case even since our example of the returning knight. The rate of change might have been slower in the twelfth century - catapults weren't released with integrated mead purifiers until 1175 - but it was still necessary for users to adapt. Now, however, we must adapt at an alarming speed. Failure to do so may compromise the integrity of our business and the financial well-being of our customers.

So what's changed? Employees and management now work from home and cyber cafes using virtual private networks (VPNs) or other remote access solutions. People check email using their iPhone/Andrdoid/Blackberry smartphone from their high-rate-of-speed vehicle, and finish the marketing presentation while on a chaise lounge at the beach. Applications that once resided on a server in the office have been moved to a data center or flown up to the "cloud." This all adds up to one thing for IT and security professionals: lots of new holes ("exposures") and a headache.

**What Can We Do?**

It's still necessary to have a firewall at the company's Internet connection. After all, firewalls provide network address translation (NAT) to mask internal addresses, stateful packet inspection (SPI) to make sure that a packet really is what it says it is, antivirus, antispyware, content filtering and more, all under the label of "Unified Threat Management." But the addition of multiple, remote access techniques and movement of applications and data to new locations introduce a huge number of exposures through which attackers can have a go at your corporate data and network. Additionally, employees can access data from and copy it to locations where it just shouldn't be stored, typically for regulatory/legal reasons but also for protection of proprietary information.

To enhance security at your organization, here are three basic areas that you need to address:

1. ***Obtain buy-in from management.*** The first step that any IT organization must take is to obtain buy-in from management that something needs to be done and will be allowed to be completed as needed. It's of no use if management agrees that a solution is needed but won't provide a budget for it or wants exceptions made for itself. Therefore, IT needs to plan and present its case.

2. ***Identify and document exposures.*** Assuming that management has given the go-ahead to implement a security solution, the next step is to identify the exposures, or make a map of the "new perimeter." This means that it must identify what types of remote access methods are being used (such as VPN, RDP or LogMeIn) and from where, what types of handhelds employees are carrying, what applications the handhelds are running (email, Web or other apps) and what type of data is being accessed. Additionally, identification of where all data resides and what protection mechanisms are already in place around it need to be clearly understood.

The importance of that final point – the identification of where all data resides – cannot be stressed enough. Data has become extremely scattered (decentralized) over the years, and many organizations have lost track not only of where it resides, but also of what it contains. In this era of identity theft, a company's very existence can depend on the knowledge of where the data is and what is protecting it. As mentioned previously, data can exist on in-house servers, in data centers, in the "cloud," on handheld devices, or on personal laptops and home computers. (Raise your hand if you've ever sent a sensitive document to yourself by email so you could work on it later.)

For one good model of how to identify your exposures as a first step toward reducing them, consider Massachusetts regulation 201 CMR 17.00 ("Standards for the Protection of Personal Information of Residents of the Commonwealth"), which took effect in March, 2010. This regulation states that any

organization that maintains the personally identifiable information (PII) of a resident of Massachusetts must go through the process of identifying where PII resides and what is being done to protect it, and then create a **written policy** detailing this effort. For the full text of this regulation, see http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf.

The "cloud," whether you see this as a new concept in IT or as an old one that has resurfaced under a different name, also presents a whole new set of security challenges. How can you identify the exposures for your data in the cloud? As an example, consider hosted backups. You should know how the data is being protected, who has access to the tapes or disks on which it is stored, and where the data is physically located. You should also be aware of whether your data is isolated from that of other customers of the service provider. Although the service provider might provide you with a written statement ("Yeah, we protect it."), that's not the same as having it in your own hands, and you must therefore have a very high level of trust in that provider. The same set of issues can apply to other cloud-based services, such as hosted email or spam filtering.

3. ***Standardize on solutions, and preferably secure ones.*** Walk into any consumer electronics store and the first area you'll walk into is the one for mobile telephones. The assortment is spectacular. Whether you are a fan of Apple iPhone, BlackBerry, Android, Windows Phone or Fred's Homemade Smartphone, there will be a selection for you.

So how can IT handle this assortment of devices, most of which cannot be centrally managed? There are four general responses, varying in complexity or severity:

1) Ban any remote access technique, whether by handheld or by VPN. This might be the most secure response from the perspective of data protection, but it will most certainly result in reduced business productivity and angry management and staff. Obviously, for a significant number of organizations, this is not a realistic solution any more.

2) Create and enforce a corporate standard. Configure IT-supplied devices for maximum security and then provide them to the end-users. Risk upsetting end-users who prefer the latest, consumer-focused device with all the bells and whistles over the encrypted, password-protected one that you've provided.

3) Let users select their preferred bells-and-whistles devices and set their own level of security (if any), and hope that nothing bad happens. Regrettably, too many organizations opt for this solution, as management wants to keep its end-users happy and productive. Security concerns have once again been ignored and our first point from the previous section (management buy-in) has fallen by the wayside. The perimeter has become much more tenuous.

   The same can be said for remote access solutions. There are many ways to access data from outside the organization. PPTP VPNs are common and easy to implement, but a single, weak endpoint (i.e. a remote user's computer) can thwart all security as it opens a direct tunnel to the corporate network. SSL VPNs are also fairly common, though a bit more involved to implement.

4) For an intermediate level of protection, enforce a basic level of security on devices if your applications support it. For example, many companies use Microsoft Exchange Server for email and collaboration. Recent versions of Exchange Server can force a password for any device that attempts to connect to it directly (ActiveSync). Similarly, Network Access Protection is a service that checks for the health of a system that attempts a remote connection. If the system fails any of its tests, it will be denied access until corrections are made.

Ultimately, the responsibility for identifying the new perimeter and securing the organization falls to the IT department but must be supported by management. Whether it has chosen to standardize on remote access methods or consolidate all applications in-house instead of being hosted in data centers or in the cloud, it must understand where all the data resides and who requires access to it, and then thoroughly integrate protection around that. Even though the perimeter now extends well beyond where it used to be, it's still possible to provide a strong level of protection for your organization, keeping your end-users happy and productive, and your systems and data secure.

This article appeared in CSO Online at http://bit.ly/pclhAk

**About the Author:**

Brad combines a rare blend of security, high-end systems architecture and application development skills with a unique sense of humor. On top of these, he adds a strong scientific background that he draws upon to analyze and troubleshoot complex IT problems. Brad is the founder and president of Fieldbrook Solutions LLC, an IT, MIS and security consulting firm based in Ashland, MA. Prior to that he was the vice president of information technology for a similar firm in Newton, MA, and he has also been the manager of MIS for a major Boston-area data center. He has taught classes in Active Server Pages, JavaScript, HTML and the Theory of Relativity.

He is a Certified Information Systems Security Professional (CISSP), a Microsoft MVP in Enterprise Security as well as a Microsoft Certified Systems Engineer (MCSE), a Certified SonicWall Security Administrator and an Acronis Certified Engineer. He also earned a Ph.D. in physics from Boston College to help him calculate how long it would take to launch his frozen computer across the local highway.

Brad is a frequent contributor to various online TechTips sites and gives user group/conference presentations on topics ranging from spam and security solutions to Internet development techniques. He also published numerous articles in international physics journals in his earlier, scientific career.

Brad is the founder and president of the National Information Security Group (NAISG), the former chair of the Boston Area Exchange Server User Group, a member of the FBI's Infragard Boston Members Alliance, and a member of the Microsoft IT Advisory Council.