Readers of this column and others in the Network World Fusion series have no doubt received announcements of a wide variety of recorded lectures available on demand for different topics. However, many of us ignore such invitations, so I thought it would be helpful to read a review of this resource.

I recently listened with great interest to the first seminar in the series called the “LANDesk Webcast Series” available free from the page at


The four seminars in the series are

* Security Within the Management Space (available now);
* Streamlining Patch Testing and Deployment (due in January 2005);
* Spyware and End-node Security (due in February 2005); and
* Mobile Security and Real-time Management (due in March 2005).

After a brief registration process, you are brought directly into a slide-show with narration streamed to your browser (it worked fine with MS Internet Explorer v6.0 but did not work with Opera v7.54 – there were no control buttons visible in the latter browser). However, try not to interrupt the stream: I found that the system often locked up if I paused for longer than a few seconds and I’d have to start over and then move the slider back to the right position to resume from where the stream had stopped or click on a link in the agenda pop-up.

The first seminar, “Security Within the Management Space,” begins with an excellent overview by Mark Nicolett, Research VP at Gartner Group. Some of Mr Nicolett’s key points:

* In surveys of top-ten business concerns in 2002, 2003 and 2004, security breaches and business disruptions climbed from off-the-map in 2002 to #2 in 2003 and #1 in 2004 (probably because of malware outbreaks).

* Data protection and privacy concerns in these surveys fluctuated from #4 in 2002 down to #10 in 2003 and back up to #3 in 2004 (probably because of the increasingly strict regulatory environment).

* The time from discovery or disclosure of a vulnerability to appearance of an exploit has been
shrinking towards zero over the last few years. Patching is therefore still necessary, but it can no longer be considered a sufficient protective mechanism.

* Sarbanes-Oxley (SOX), Gramm-Leach-Bliley (GLB) and Health Insurance Portability and Accountability Act (HIPAA) have serious implications for IT security; all of them lead auditors to look for clear, defined policies on privacy protection and methods for identifying and tracking breaches of these policies.

* Prime vulnerabilities remain in employee awareness and training for acceptable and safe use of IT resources; HTML and active content coding for Web servers and Web sites; user administration errors on client systems; and missing patches for all layers of the stack.

* The ongoing cycle of security management requires

> a discovery phase to establish the current status, identify vulnerabilities and define a goal for the more secure state;

> prioritizing actions based on risk assessment and risk management principles;

> shielding the system and reducing potential damage, especially by eliminating root causes for vulnerabilities; and

> monitoring compliance and evolving threats to keep our systems up to date.

Mr Nicolett continues with an overview of the threat life cycle; methods for shielding, scanning, blocking and containment; configuration management; defining and maintaining a structured environment; and mitigation and maintenance from an organizational process perspective.

Mr Nicolett speaks clearly and engagingly; one really gets the message that he knows his stuff.

* * *

The next section of the seminar is entitled “Today’s IT Security Challenges Need a Proactive Patch Management Solution” and is presented by Barbara Crane, VP of IT for Aramark Corporation. She speaks from an industry perspective from a company with 200,000 employees in 18 countries for 6,000 client sites and $6.5B in sales. At their HQ, they have 1,500 end users with another 500 users in regional offices who are connected in a wide-area network (WAN). Remote offices communicate their weekly data through broadband links. They have a long lifetime for their PC hardware, causing a complex situation for patching. She discusses why their firm chose LANDesk as their method for managing patches in this heterogeneous environment.

* * *

LANDesk Software’s Director of Product Management, Steve Workman, reviews his company’s perspective on the market for security management solutions to meet the growing demands for device discovery, audit and compliance, network access controls, patch management, spyware controls, and monitoring and denial tools.
I recommend his overview to anyone, but it will be especially useful in internal training as an interesting module to bring newcomers into the network and system security management team. I will certainly be referring my students to this valuable resource.

[Disclaimer: I have no financial involvement whatever with the companies named in this article, am not involved in the webinar series in any way and do not benefit from its success.]

A Master’s degree in the management of information assurance in 18 months of online study from Norwich University – see <http://www3.norwich.edu/msia> for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2004 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.