**“How to Spend a Dollar on Security”**

www.computerworld.com, 11/9/00

By Patrick McBride, EVP, METASeS

A shy, spiky-haired 24-year-old reputedly unleashes a global computer virus causing an estimated $10 billion in damages, paralyzing computers from the Pentagon to the Parliament. Hackers spend six weeks peering at Microsoft's network programming code for a new generation of Microsoft products. Legendary cracker Kevin Mitnick violates national security by entering a military computer.

If hackers can break into these digital Fort Knoxes, is anyone safe?

Well, that depends.

It depends on how well you secure your network but also on how you plan against attacks, how well you educate system users and many other factors -- most of which are reflected in your IT budget.

Businesses know money must be spent to secure their infrastructure. But how do organizations budget for security?

In order to help companies determine the best use of their resources, here's how to carve up a single dollar in a first-year security budget. This is a method that will work whether you're a Fortune 500 firm or a mom-and-pop e-commerce shop.

15 cents: Policy

Spend 15 cents on nailing down the organization's overall security policy. Ultimately, an effective security program may involve firewalls, perimeter security, vulnerability reduction, operating system hardening and other technical components. But these elements will remain fragmented without an overall, unifying strategy. A top-level security policy documents and explains security goals for everyone in the organization. As a clear management articulation of security strategy, it helps prevent communication breakdowns among corporate divisions.

40 cents: Awareness

Education and support generate the single biggest return on security investments. Even with perfect technology, employees can be talked into unwittingly helping a hacker.

Hackers view data as transparent when it travels via the Internet. But they're often more shrewd than they are technical geniuses. One digital sleuth described Kevin Mitnick as "technically dull." Yet he could hack into almost any system. Many Mitnick conquests, the sleuth pointed out, resulted from social engineering, imitating lineman's jargon, impersonating superiors and talking employees out of field manuals.

Twenty cents of this category should be used to advertise the security program to general users, who must modify their behavior. For example, they need to stop jotting passwords on yellow stickies and posting them on computer monitors in plain sight of cleaning crews.

Use the other 20 cents to educate IT professionals responsible for building a more secure system. They must keep abreast of new policies, standards and procedures, and they must be trained in building a secure infrastructure. Professionals require a steady flow of information, advice and resources, from both internal and external sources.

10 cents: Risk Assessment

A secure organization must understand what assets to protect, the internal and external threats to those assets and where the organization is most vulnerable.

Ongoing risk assessments help organizations locate their greatest vulnerabilities. This portion of the budget should encompass every risk assessment tool, from ethical hacking and penetration testing to social engineering.

But beware: Many security consultants advise organizations to spend more than 10 percent on risk assessment. Penetration tests, however, aren't needed throughout the network. Tests in a statistically relevant sample of the organization area can allow you to understand systemic issues and make appropriate recommendations.

20 cents: Technology

Here's where geeks have their fun. They love firewalls, virtual private networks, vulnerability scanning tools, intrusion detection systems, access control tools -- you name it.

The geeks have got it right, at least in part. Organizations must keep up with the latest technology. A single system with outdated or poorly configured software can seriously compromise network security.

But before spending huge sums on additional "techy toys," organizations should fortify their foundation by hardening existing systems. Mounting good technology onto an old, crackable system exposes the expensive, new technology to easy intrusion.

15 cents: Process, Process, Process

Security depends both on management process and technological wizardry. Ongoing, life-cycle development -- creating new processes and modifying old ones -- can keep networks humming smoothly for years. Security is a continuous initiative involving everyone in an organization, from top to bottom.

Security should be viewed as a state of mind that must be engineered into a physical system. Automobiles didn't really get safer until safety was made a goal and engineered into them. Before that, seat belts merely restrained passengers, holding them in place in what were otherwise not-so-safe vehicles.

The same holds true for networks. Until security is engineered into them, as a management goal and process, they'll be prone to intrusion.