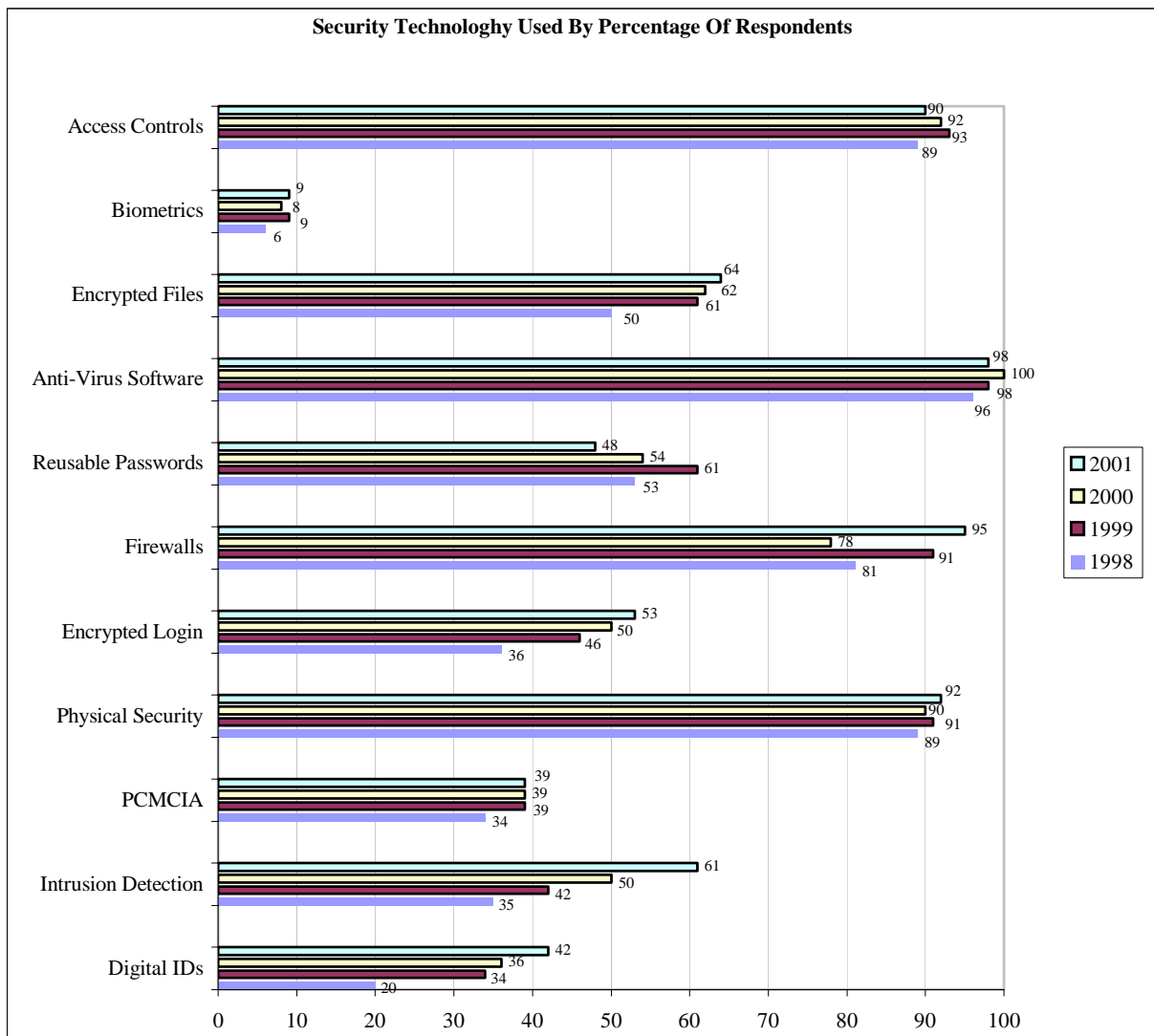


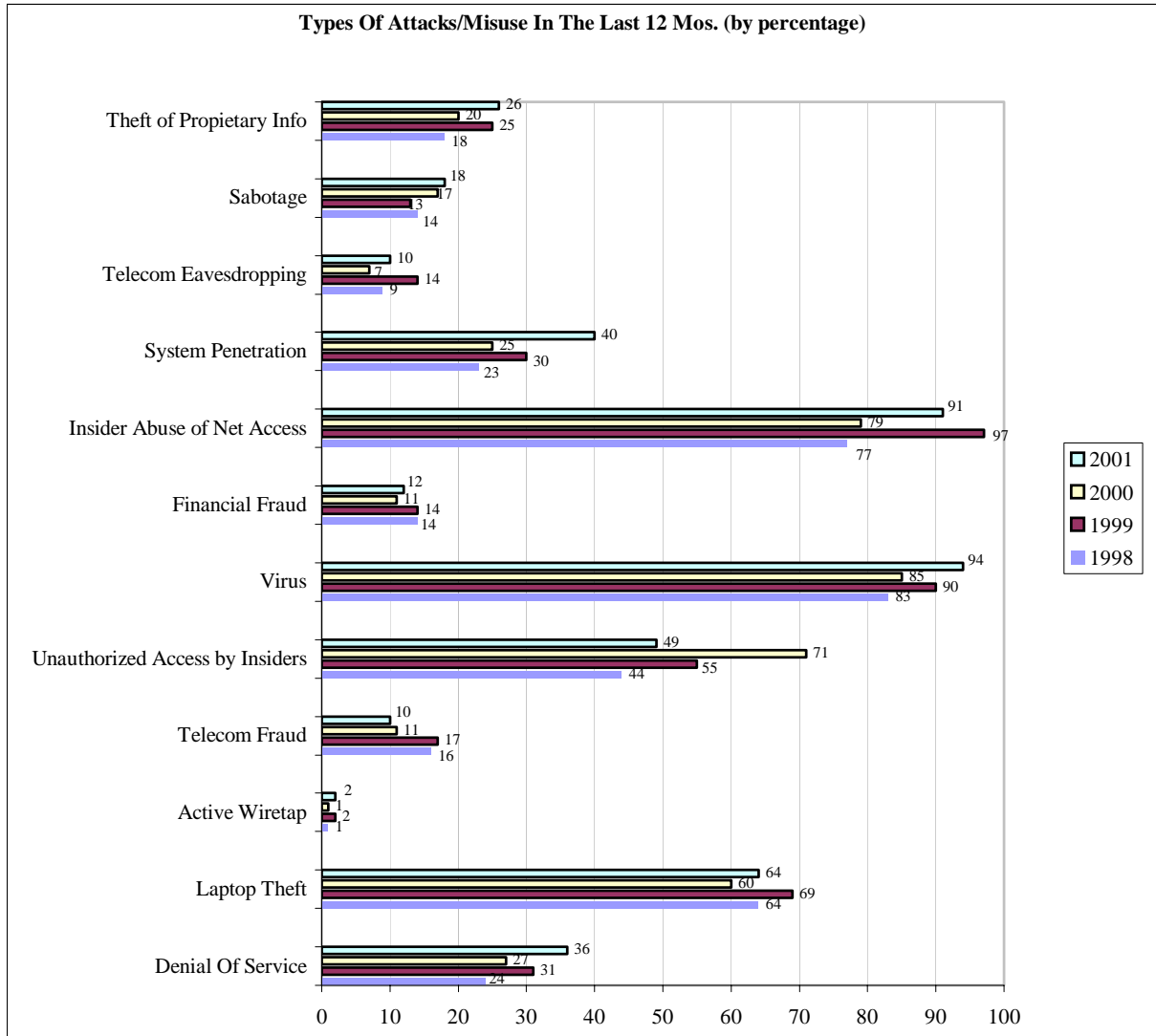
Information Security: The Curious Paradox

The last article in this series, “Information Security: What You Don’t Know Can Hurt Your Business,” helped you get a feel for the information security issues that threaten your business as well as gave you some questions that need to be addressed to help assess your organization’s current security policies. Another area dealt with heavily in the last article was the importance of firewall technology. While the necessity of firewall technology in information security cannot be emphasized enough, one’s efforts cannot stop there. There are many additional security measures that should be considered and possibly implemented depending on the level of security your organization requires. But don’t be fooled, simply implementing these solutions may not be enough. Therein lies the paradox. Companies are employing varied security solutions in an effort to protect their information assets, as they should. Yet these same organizations are still sustaining damage from a hacker’s exploits. To help emphasize this point, consider the following two graphs. The first, Graph I, highlights the various security measures taken over the last four years by more than 500 companies. The second, Graph II, shows several types of attacks that these companies suffered over the same four-year period. These numbers were taken from the **2001 Computer Crime and Security Survey** prepared by the Computer Security Institute, in conjunction with the FBI.



Graph I

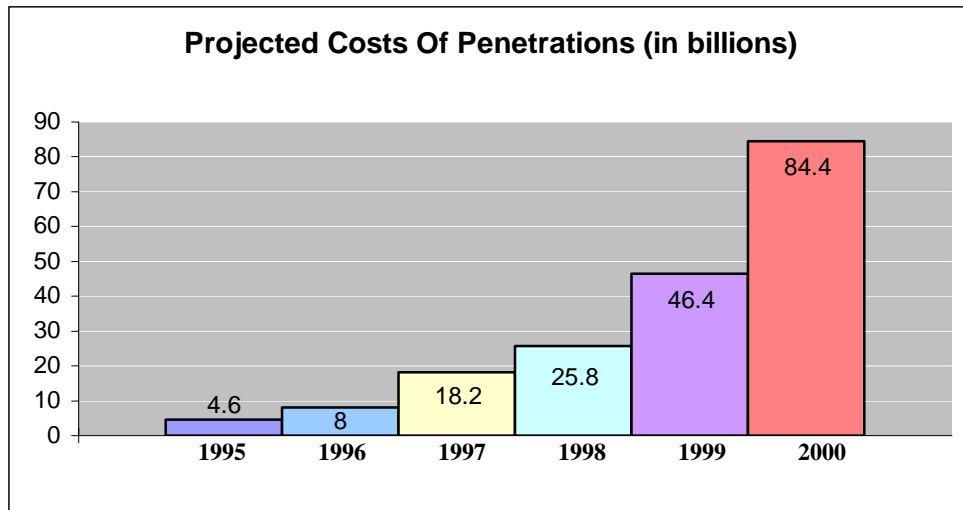
2001 CSI/FBI Computer Crime and Security Survey



Graph II

2001 CSI/FBI Computer Crime and Security Survey

Considering this information, one must ask: “*What went wrong? Why did these security measures fail?*” Well, it is obvious that the problem is not a lack of effort. A majority of the respondents had several security measures in place when these attacks were sustained, the most detrimental of which are the denial of service attacks, viruses, system penetration, and unauthorized access by insiders. These are the attacks that can bring a company’s operations to its figurative knees. The next graphic, Graph III, helps illustrate the financial losses that can be suffered if network security is not properly addressed and maintained. Taken in aggregate, the implication is that despite the security technology in place there is a disturbing trend of more frequent and serious attacks over the designated six-year period.



Graph III

Once properly illustrated it is easy to see that damage can be inflicted on any unsuspecting company despite the implementation of various security measures. So what's going on here? Well, now that we have your attention it is time to talk seriously about why some of these measures failed and what can be done stop this from happening again. For many of these companies, the short answer is vigilance.

One cannot implement various hardware and software security measures and just walk away assuming that they have done all they can. It is, unfortunately, not that simple. Securing your companies information assets is an ongoing, ever evolving, process. Hackers and attackers of all sorts are continuously getting "better" at what they do. The only alternative for companies is to become better as well. To drive this point home the Short Sermon has been boiled down into a few well thought out sentences. If you take nothing else from this article, please take the Short Sermon to heart, it could save your ASSets someday (information assets, that is).

THE SHORT SERMON

While a properly configured firewall can be the centerpiece of security architecture, it is a grave mistake to rely on it totally. An effective security architecture includes a frequently monitored intrusion detection system, virus software, a properly configured e-mail system, complete and updated OS and software patches, secure routers, good passwords, and people who keep current on the latest hacks, exploits, viruses, tools and security practices.

This is not meant to imply that it is solely the IT department's responsibility to stay on top of current and future network threats. As pointed out in the last article, it is the responsibility of any and every individual in an organization to keep abreast of not only the current network situation but also the inevitable threats to security from both outside and inside the organization. One invaluable resource for such information is the Computer Security Institute (CSI). Information much like what is displayed in graphs one and two is made available on the CSI website along with pertinent findings from various surveys and studies in

downloadable pdf form. If nothing else, it is highly suggested that you at least review the information in the **2001 CSI/FBI Computer Crime and Security Survey** found at <http://www.gocsi.com/pdfs/fbi/FBISurvey.pdf>. This document will provide information that is essential in making reasonable decisions about your own companies network security and policies. Remember, when it comes to information security:

“It’s always better to invest a little more than you planned rather than less than you should have”

- Zig Ziglar