Global Information Assurance Certification Paper

DOCUMENTATION SECURITY:

An Ignored Computer Security Vulnerability

Michael Cassidy (casspc87@hotmail.com)
September 11, 2000

OVERVIEW:

Many organizations pay little attention to securing their sensitive computer documentation. Numerous documents are generated that contain key corporate information, yet little, if any access controls or audit trails are instituted to keep these documents out of hackers and/or competitors hands. In the past, "dumpster diving" was vogue for many hackers, but this required physically digging through trash to find information. Nowadays with the advent of the Internet, proliferation of e-mail, "virtual worksites", and weak overall security practices by organizations, the risk exposure of having sensitive documentation intercepted virtually, without ever getting dirty, has greatly increased.

"Dumpster diving" is still an art practiced today. Case in point, the recent alleged Oracle effort to obtain information from the Association for Competitive Technology (ACT), a pro-Microsoft trade group, was foiled due to an honest cleaning staff. {3} In this case, an individual attempted to bribe the cleaning staff twice, upping the monetary offer each time to the tune of $1200 for three members of the cleaning crew. {3} Matter of fact, one of the "biggest hacks in history", dubbed the Phonemasters, used "dumpster diving" to obtain technical documentation, phone directories and other files allegedly penetrating AT&T, MCI, WorldCom, Spring, Equifax, TRW. {7}

While physical destruction of sensitive computer documentation is still necessary as the previous example shows, the larger risk to organizations is the control of numerous electronic copies that are floating around both inside and outside of an organization. Many organizations do not understand or just plain ignore the fact that documentation, such as Contingency/Disaster Recover Plans, Detailed Network Design documents, etc, contains key information that would make any hacker's attempts to penetrate the network quite easy. In addition to worrying about hackers, organizations, especially 'knowledge centric' companies that provide services, have to worry about corporate espionage and theft of their proprietary tools and methodologies.

Although the focus in the previous paragraphs centered on an organization's physical company site, companies need to pay particular attention to documentation being utilized by tele-commuters who work at home and/or off-site staff that reside at client sites for short or long-term engagements.

An overwhelming majority of tele-commuters lack the security tools, i.e.

firewalls, encryption, etc, for the home computer that may contain sensitive documentation. In addition to lacking the software and hardware based security protection at home, many users do not follow proper procedures for securing their computer files. With the advent of cable modems and Digital Subscriber Lines (DSL), organizations will need to address in their security policy how to properly handle and secure documentation outside the organizational site. {4}

One high profile case in particular stands out. The case of John Deutch, former CIA Director, was found guilty of creating and storing classified data on a non-classified system at his home. {2} When you have the head of a top secret agency, whose business is security and securing documentation, committing these type of security policy violations one can only imagine what goes on elsewhere.

One risk that really stands out in my mind is the outsourcing model that many organizations follow when producing computer security documentation. When organizations outsource the development of computer security documentation, ultimate control of the information is outside the purview of the company. This makes it difficult to track those who have access to the documentation, placing a lot of trust with another organization that may not always have the best security procedures in place. With the rise of Application Service Providers (ASPs) this issue will become more prevalent in the near future.

MITGATION STRATEGIES:

Although the picture "painted" above seems bleak, there are many controls and processes that can be instituted in organizations to mitigate and minimize the risk exposure to un-secure computer documentation. While some of the approaches may be impractical from a cost and/or personnel perspective, each organization must analyze and rate their risk level and probability for this to occur. Based on the probability and risk level, organizations can better determine which recommendation, if any, they should pursue.

High-risk organizations generally are larger more geographically dispersed, with numerous physical sites and tele-commuting staff. Moreover, the larger organizations generally have more consultants and contractors in and out of their sites regularly. Low-risk organizations generally are small companies with fewer physical locations. In addition, the smaller companies tend to shy away from consultants and contractors due to cost considerations. The key to remember is these are generalizations and do not apply across the board, all organizations need to take a look at this often ignored issue.

Based on past experience and research for this paper, my recommendations can be boiled down into five actions organization can execute to better protect their sensitive computer documentation:

- *Buy a Shredder:* As discussed earlier dumpster diving is alive and well. The Supreme Court ruled that garbage left at a curb for pick-up is public domain and subject to inspection and seizure by anyone. "Anyone" being hackers and corporate competitors. {1} Every organization should have a shredder, no matter how large or small, along with a policy dictating how sensitive computer documentation will be disposed.

- *Diskless Workstations:* Although not foolproof, by eliminating disk media (Floppy, ZIP, CD-RW, etc) at the workstation level organizations can reduce the probability that users will steal or borrow sensitive documentation. {6} Organizations may especially want to consider this policy for outside consultants and vendors where there is high turnover.

- *Incorporate Security Procedures into Contracts:* Ensure all consultants and contractors that work within an organization have a clear understanding of security procedures. Specify in contracts with service vendors that documentation deliverables will become sole property of the organization once work has been completed, with all relevant information turned back in. Develop a method to track what documents leave an organization to service vendors when work is being done.

- *Install Auditing and Monitoring Software:* Organizations that install auditing and monitoring software will need to achieve a balance between monitoring organizational assets and being labeled "big brother". An upfront policy stating what will be monitored in the security policy seems to be a good practice from a legal and public relations perspective.

  (NOTE: Always obtain legal counsel before attempting to institute this type of policy.)

- *Embed Hyperlinks into Documentation:* Microsoft Word allows users to embed a "web bug" with a uniform resource locator (URL) pointing to a graphic on a web server. Whenever someone opens the document, his or her computer will send an HTTP request to the server asking for the graphic to display it. This request can log the computer name and IP address without the user's knowledge. {5}

  (NOTE: Again, check with legal counsel before implementing this measure.)

CONCLUSION:

Hopefully this paper opens organization's eyes to an often ignored or misunderstood threat to their network security. Many other strategies can be implemented to mitigate this risk, but that would take much more space that allocated in this venue. The proper security tools and policies coupled with solid security training for tele-commuters and off-site personnel will reduce an organization's overall risk exposure to this threat.

References:

1}. Anonymous “Protect Against “Dumpster Diving” With Shredder”. Date Unknown.
URL: http://www.b4-u-buy.com/09c4700.htm

2}. Friel, Brian “CIA suspends former director’s security clearances” August 24, 1999. Government Executive Magazine (On-line)
URL: http://govexec.com/dailyfed/0899/082499b1.htm

3}. McClure, Stuart and Scambray, Joel “Forget the firewall; guard your garbage against ‘Dumpster Diving’ hackers” June 30, 2000. InfoWorld.
URL: http://www.infoworld.com/articles/op/xml/00/07/03/000703opswatch.xml

4}. McClure, Stuart and Scambray, Joel “Internet privacy shows troubling prospects; constant erosion leads to lots of exposed data” June 18, 2000. InfoWorld.
URL: http://www.infoworld.com/articles/op/xml/00/06/19/000619opswatch.xml

5}. Sayer, Peter “Word documents can be tracked on Web” August 31, 2000.
URL: http://www.infoworld.com/articles/hn/xml/00/08/31/000831hnwebbug.xml

6}. Schwartau, Winn “Anatomy of a friendly hack How to assess your enterprise security, correct vulnerabilities and thwart attacks” February 2, 1998.
URL: http://www.nwfusion.com/netresources/0202hack.html

7}. Simons, John “Unplugged! The biggest hack in history” October 3, 1998.
URL: http://www.zdnet.com/zdnn/stories/news/0,4586,2345639-1,00.html