Editorial Preface

E-Commerce Security: An Organizational Perspective

Associate Editor: Mahesh S. Raisinghani, PhD
University of Dallas, Graduate School of Management

The worldwide market for information security services will nearly triple to $21 billion by 2005, up from about $6.7 billion in 2000, according to International Data Corporation’s research (Costello, 2001). The boom in the market will be driven by corporate desires for wireless access, extranets, and remote networks because new and greater security services will be needed to secure those technologies. Today’s world is a more dangerous place to conduct electronic business than it was in the 1990s. In the late 1980s and early 1990s, business crimes existed, some of which involved elaborate copying, manipulations and/or diversions of computer-based assets. With the leveraging of the World Wide Web as a business tool and as a semi-seamless information/transaction backbone, corporations have entered into an environment that is, on the one hand, a ubiquitous global presence and, on the other hand, a dangerous invitation to those who have the ability to conduct malicious attacks on their personal or corporate confidentiality, integrity, and assets.


In the 1990s, we saw a proliferation of malicious activity from a number of sources. Information gathered in the annual Computer Security Institute - Federal Bureau of Investigation Computer Crime and Security Survey (CSI/FBI) and all of the anti-virus vendors illustrates that this malicious activity is accelerating. While part of this activity may be the result of individuals or groups of individuals with some perceived goal, there is a certain amount of activity that is being conducted by individuals, companies and nation states with the ultimate purpose of compromising the resources of their targets. These attacks are the 21st century weapons of the domestic and international espionage and terrorist operations that skillfully bury their activities in the noise level created by the more media-friendly virus outbreaks.

Two factors complicate the detection and reaction to computer crimes: the speed at which these crimes occur, and the naïveté of those being targeted. If one reflects back upon two recent outbreaks of malicious code, Melissa and Love Bug, one can see the exponential increase in deployment speed that differentiates the two attacks. Whereas Melissa took approximately four days to reach what might be considered a critical mass in its impact of global resources, Love Letter reached an equivalent status in approximately five hours. Further emphasizing the impact of the malicious code are the estimates of the financial damage. Whereas Melissa may have caused between $93m and $385m in the course of its active lifetime, Love Bug is estimated to have impacted between $700m to $6.7b in its active state (Kessler, 2000).

Naïveté with respect to malicious activity takes several forms. There is the classic form—“it won’t happen to me.” The relevance here is that the targeted site does not prepare itself for the eventuality that something malicious might, in fact, impact them. A worse case of this scenario is the site that anticipates the problem, but does not dedicate adequate resources to protect their resources.

Figure 1 highlights that in 2002, 12% of the respondents to the CSI/FBI survey did not know
if their computer systems had unauthorized use. Though this percentage has decreased somewhat over the past six years, this could signal a gap in understanding the importance of being diligent to these issues. More disturbing is the decrease in the number of ‘Yes’ responses and a corresponding increase in the ‘No’ answers. This clearly illustrates a gap that demands the attention of a trained security professional.

The origins of attacks on these resources must be understood to provide an adequate defense. The respondents to the CSI/FBI survey illustrated in Figure 2 highlight several important concerns for a corporation. The Internet provides access to virtually every resource that is connected to it. Some of these resources are protected by authentication techniques and, perhaps, by an encrypted pathway, but the fact that these resources touch the Internet means that they can be “seen” by someone who is not authorized.

Figure 2 also illustrates the Internet is not the only medium for attacking corporate resources. Use of a corporation’s internal systems and remote access capabilities are also used to compromise the resources of the firm. An illustration of the compromise of the internal systems is rather prominent in today’s environment. A wireless network can be established in a corporation essentially without the corporation knowing that the network has been established. If misconfigured, such a network could provide direct access to corporate resources to anyone who is within the broadcast range of the wireless access point and who has installed a wireless NIC card in a laptop equipped with one of several open source wireless sniffing applications. A recent survey by the authors found one such network while traveling down the interstate at 60 mph. These unprotected networks could be compromised in a matter of minutes with a laptop, a $100 wireless NIC card and freely available software from the Internet (even if the WEP security feature is enabled).

But what are the perpetrators of these attacks attempting to compromise? Once again, the CSI/FBI survey addresses this question with startling results. The survey reported the malicious activity shown in Table 1 (reflected as a percentage of respondents) (Powers, 2002):

The final statistic that reflects the reality of computer crime is the number of incidents reported to the Computer Emergency Response Team (CERT) at Carnegie Mellon (Figure 3). Even with a cursory glance at the chart, one can see the exponential growth of malicious activity reported to CERT. It appears that the reported activity in 2002 will be at least double that which was reported in 2001, which in turn was double the activity reported in 2000. Assuming the current...
rate of growth, 2003 will be an interesting year with respect to combating malicious activities.

Future Trends in E-Commerce/Information Security in Organizations

The worldwide market for information security services will nearly triple to $21 billion by 2005, up from about $6.7 billion in 2000, according to International Data Corporation’s research (Costello, 2001). Many opportunities abound for the use of public and private transport media to conduct transactions between parties. From the perspective of business, electronic commerce has the capability of connecting suppliers and customers on a timely basis. In 2001, the online sales within one ISP alone topped $33 billion (White & Wingfield, 2002). The potential increased profits and decreased costs are driving businesses towards use of electronic commerce. The boom in the market will be driven by corporate desires for wireless access, extranets and remote networks because new and greater security services will be needed to secure those technologies.

CONCLUSION

The media has focused on the activities of crackers who have exploited the vulnerabilities of a particular site (an example is CNN’s recent article on a 20-year old who gained access to WorldCom Inc.’s corporate web sites) (Weiss, 2001). However, the real work of the professional information security specialist is establishing and enforcing a security policy and understanding what information resources need protection. Though these latter two ideas may seem somewhat “simple”, a failure in either can compromise the integrity of corporate resources and intellectual property. Noting how quickly the Love Bug worm was able to compromise the corporate resources, it is imperative that the corporate information security professional be trained in the art of establishing an effective resource protection program. That program must be in effect before an event like the Love Bug worm happens. There is not enough time to react otherwise.

In the longer term, we can expect more stringent Internet security efforts, including greater law enforcement and intelligence community demands for Internet surveillance in every country. There will also likely be stringent export controls on strong encryption technologies. All good security plans begin with a threat assessment that details the perceived threats to an entity’s information assets and networks. Based upon this assessment, a plan may be developed to map appropriate defensive tools to the threats. At this point, proposed solutions should be tempered with a cost/benefit analysis of perceived threats relative to protection costs. This editorial preface should be considered a call for more focused research in e-commerce/information security. The value of a balanced coverage
of theory and practice in the e-commerce/information security field cannot be overemphasized.

REFERENCES


---

**Table 1: CSI/FBI survey results of malicious activity (reflected as a percentage of respondents)**

<table>
<thead>
<tr>
<th>Malicious Activity</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial fraud</td>
<td>12%</td>
</tr>
<tr>
<td>Sabotage of data and/or networks</td>
<td>8</td>
</tr>
<tr>
<td>Theft of proprietary information</td>
<td>20</td>
</tr>
<tr>
<td>System penetration by an external source</td>
<td>40</td>
</tr>
<tr>
<td>Denial of Service attacks (DoS)</td>
<td>40</td>
</tr>
<tr>
<td>Unauthorized access by insiders</td>
<td>38</td>
</tr>
<tr>
<td>Employee abuse of Internet access privileges</td>
<td>78</td>
</tr>
<tr>
<td>Viruses</td>
<td>85</td>
</tr>
</tbody>
</table>


**Figure 3: Malicious Activity Reported to CERT (2002 estimated based on Q1 reports)**