BCC PREVENTS E-MAIL NUISANCES

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

The consensus in our profession – despite the dreadful lack of hard statistics – is that something like 2/3 of all the damage caused to our information systems is from insiders who are poorly trained, careless or malicious (for a detailed discussion of security statistics see http://tinyurl.com/b6zzh or http://tinyurl.com/96u2n). For example, a study published in late 2005 reported that “Sixty-nine percent of 110 senior executives at Fortune 1,000 companies say they are 'very concerned' about insider network attacks or data theft, according to a study by Caymas Systems, a network security technology firm based in San Jose, Calif. And 25 percent say they are so concerned they can't sleep at night, Sanjay Uppal, a vice president at Caymas Systems, told eSecurityPlanet.” <http://tinyurl.com/mmnuw>

A McAfee-sponsored survey in Europe showed that (in the words of the Department of Homeland Security Daily Open Source Infrastructure Report <http://www.dhs.gov/iaipdailyreport>), “Workers across Europe are continuing to place their own companies at risk from information security attacks. This "threat from within" is undermining the investments organizations make to defend against security threats, according to a study by security firm McAfee. The survey, conducted by ICM Research, produced evidence of both ignorance and negligence over the use of company IT resources. One in five workers let family and friends use company laptops and PCs to access the Internet. More than half connect their own devices or gadgets to their work PC and a quarter of these do so every day. Around 60 percent admit to storing personal content on their work PC. One in ten confessed to downloading content at work they shouldn’t. Most errant workers put their firms at risk through either complacency or ignorance, but a small minority are believed to be actively seeking to damage the company from within. Five percent of those questioned say they have accessed areas of their IT system they shouldn’t have while a very small number admitted to stealing information from company servers.” <http://tinyurl.com/8rjz5>

In my last column, I presented an example of careless or ignorance that can bypass technical security. I pointed out that combining the unthinking use of REPLY ALL with visible distribution lists from a CC field can lead to violations of privacy even inside an organization. In this column, I want to finish my discussion with a few more points about the dangers of using visible distribution lists.

The problems caused by CC are worse when the recipients do not know each other. I have often received messages from technically unsophisticated correspondents who put dozens of e-mail addresses in the CC field even though many of the recipients are total strangers to each other. Such exposure of e-mail addresses always makes me nervous; who knows whether everyone on the list is trustworthy? Even if the list is not misused for outright spam, people often REPLY ALL with what I consider useless information, effectively adding me to a discussion list that I never wanted to be on.

One particularly annoying habit is to REPLY ALL with a joke stemming from some initial message. People then generate a series of increasingly long messages including copies of all the previous copies of the ostensibly clever repartee, driving me to generate an addition to my junk
In one embarrassing case I was personally involved in, I added a new course developer to my MSIA faculty list and put the list name in the CC field by mistake in an all-points-bulletin. To my horror, the course developer cheerfully added my faculty members to a newsletter without permission. You can imagine the repercussions; there were two red faces that day and apologies to everyone.

The habit of using REPLY ALL is annoying enough when a reply does not in fact have to go to everyone on the original distribution list. However, REPLY ALL is a positive menace if it is coupled with the abhorrent practice of using an existing e-mail message as a shortcut to creating a new one with a completely different topic. Not only do many lazy users fail to modify the original message subject -- thus running the risk of having their new message ignored or filtered or misfiled -- but they may easily send sensitive information to the wrong people. This sloppy use of e-mail can result in gross violations of confidentiality.

In conclusion, you may want to put a note in your corporate security newsletter about the proper use of CC and BCC fields the next time you’re casting about for a topic.

* * *


M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance <http://www.msia.norwich.edu> 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 © 2006 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.