RANDOM THOUGHTS
Communications With A Purpose

William Blinn
COMMUNICATIONS
179 Caren Avenue
Worthington, Ohio 43085
614-785-9359
Fax 877-870-4892
www.Blinn.com

December 2005

Public relations: Saving or killing the company

I don't consider myself to be a public relations professional, but I do know enough about the discipline to be able to tell good PR from bad PR. Sony BMG Music damaged itself in November with astonishingly poor response to an equally poor decision.

If you're one who believes that the public relations department is responsible only for "spinning" bad news, I must start by telling you that you're wrong. Public relations professionals have several duties — chief among them is communicating the company's point of view to its various "publics". Those publics range from employees to government agencies to clients and customers.

Another duty that is largely unknown outside the PR profession is that of representing those various publics to the company's managers — to look at company plans, procedures, and policies from those publics' points of view.

In late 1982, Johnson & Johnson's public relations department worked overtime to handle a crisis that occurred when 7 people in Chicago died after consuming Extra-Strength Tylenol capsules laced with cyanide. Johnson & Johnson knew that the tampering happened outside its plant and could have said that and done nothing more.

Instead, the PR department recommended, and the company accepted, a plan that involved recalling every container of Extra-Strength Tylenol (31 million bottles with a retail value of more than $100 million 1982 dollars) and then keeping the product off the market until packaging that would reveal tampering could be developed. When the new package was ready, the company launched a huge advertising campaign and called on 2000 employees to make presentations to medical professionals — the PR component of the recovery phase.

Tylenol is still around today because the company's PR professionals demanded that the company put its customers' interests first.

When PR goes wrong: The Sony fiasco

Sony BMG's troubles could have been avoided if anyone in the PR, legal, or research and development departments had carefully examined a proposal to install copy protection software on CDs so that those CDs would install a "rootkit" on Windows PCs (but not on Macs or Linux machines.) Sony's goal was to stop piracy, of course, but no copy protection software will ever deter professional pirates. All it does is inconvenience the company's ethical customers, the ones who buy the CDs. And the Sony BMG scheme inconvenienced the company's customers spectacularly.

A rootkit is hidden from Windows, has no Registry entry, and is difficult to find or remove. Worse still, some of those who did find it and tried to remove it discovered that they then had to reinstall their operating system because their machines would no longer boot!

The anti-virus community is livid. F-Secure says Sony is "playing with rootkits and other blackhat techniques" that virus writers use to hide malware.

Sony's initial response was to defend its actions, but within 3 days at least 2 rootkit-based Trojan horse applications were in circulation. Both installed malware that took advantage of Sony's copy protection.

The first was an e-mail that pretended to be from a British business magazine. "Your photograph was forwarded to us as part of an article we are publishing for our December edition of Total Business Monthly," the message said. "Can you check over the format and get back to us with your approval or any changes? If the picture is not to your liking then please send a preferred one. We have attached the photo with the article here."

The attachment wasn't a photograph, of course. Instead it was an application that created a file called sysdrv.exe. Sony's rootkit immediately intercepts files with "sys" in their name and cloaks them so that the user can't see them and neither can antivirus applications.

A week later, Sony finally released an application to remove the rootkit-based protection software and announced that it is recalling all such CDs that are in stores.

Sony's research and development teams are staffed with intelligent people, but apparently nobody considered this lunatic scheme to be hazardous for either customers or the company. Sony must have some intelligent employees on its legal team and I have to wonder if anyone there approved the plan. And the public relations department certainly failed to fulfil its responsibilities, both before and after the fact.

Finally, the PR department said the company "shares the concerns of consumers" over the discs. Those "concerns" should have surfaced long ago.

An even later follow-up from Sony BMG promised that the company will no longer use the rootkit method of copy-protecting its CDs and that it will stop shipping all of the existing CDs with the rootkit, remove an estimated 3 million

Random Thoughts (ISSN 1543-1525 [print] – ISSN 1543-1533 [electronic]) is a publication for clients and friends of William Blinn Communications, 179 Caren Avenue, Worthington, Ohio 43085.

discs on store shelves, and recall 2 million CDs that have been sold (paying the postage both ways.) At last, they're starting to get it right, but only after a lot of people made a lot of noise.

Public relations professionals are supposed to help the company do things the right way the first time so that the company can avoid the embarrassment of having a lot of people say bad things about the company. Sony is now "committed to making this situation right." As they should have been in the beginning.

What else can go wrong?

Would you be surprised to learn that people are lining up to sue Sony BMG? The State of Texas and the Electronic Frontier Foundation have already filed suits against Sony. Both allege that Sony BMG's copy protection violates laws against spyware and make computers vulnerable to attack.

In Texas, Attorney General Greg Abbott said Sony BMG installed files on consumers' computers without their owners' knowledge. That may not be entirely accurate because Sony provided a (long, complex) legal explanation with information about "proprietary software" near the end. Texas is seeking $100,000 for each violation of the law, attorneys' fees, and investigative costs. Sony will probably defend itself vigorously because several thousand violations at $100,000 per violation would put a big hole where the profits were supposed to be.

The Electronic Frontier Foundation's suit include claims similar to those made by the Texas AG, but the EFF also says the Sony BMG end user licensing agreement (EULA) is "unconscionable" because it establishes conditions each consumer must agree to before the CD can be played in a computer but that the copy-protection software is installed even if the buyer of the CD refuses the agreement.

The bottom line is this: If you have a public relations department, the director should report directly to the president and should be made aware of the company's plans. Let the PR people do their jobs. If you're a small company without a PR department, then just keep the clients' interests in mind. It's hard to go wrong if you do that. ß

No FBI query by e-mail

I'm writing this issue of the newsletter in the days following Thanksgiving. In the past week, Trojan-infected messages have accounted for more than 15% of all e-mail traffic. A lot of them say that they're from an FBI (or sometimes a CIA) address.

The message is usually along these lines: "We have logged your IP-address on more than 30 illegal Websites. Important: Please answer our questions! The list of questions are attached."

There are several clues that this is not a valid message. First, the FBI doesn't conduct investigations by e-mail. Second, there's that pesky grammatical error in the final sentence ("the list are attached.") A message from the FBI would not be likely to contain such an error.

According to the FBI, "The FBI does not conduct business this way." If you open the attachment, your computer will be infected with yet another variant of the W32.Sober virus.

According to the Computer Emergency Readiness Team, this version of Sober will do the following:

- Modify the system registry to prevent Windows XP's built-in firewall from starting.
- Attempt to harvest e-mail addresses from a configurable list of file extensions.
- Utilize its own SMTP engine to send itself to the harvested e-mail addresses.
- Modify the HOSTS file to prevent the computer from accessing certain security and commercial web sites.
- Attempt to terminate a number of running processes, some of which are security related.
- Open a backdoor on the system that allows the attacker to communicate remotely with the system via IRC. This may allow the attacker to upload and execute arbitrary code on the infected machine.

Why do people open these messages?

Many of the mailing lists I participate in have had warning messages about this virus, but why? A west coast high-tech company I'm familiar with even had to remind all employees "There are emails coming in that have .ZIP files attached (example: question_list.zip). If you are not expecting a zip file, DO NOT OPEN. If you have opened any attachment that you were not expecting, disconnect from the network (unplug the blue, green, white Ethernet cable from the back of your machine) and call x---- for further assistance."

No high-tech company should ever have to tell its employees something this basic. I'll go further: No company should have to send out a message like this.

If people would simply be sufficiently attentive and intelligent not to open any unexpected attachment without first confirming with the sender that it was sent intentionally, no virus would ever spread beyond the office of the crook who wrote it.

But even a cursory examination of most virus-laden messages should raise alarms: If the message's to field doesn't contain your address, the message should be suspect. Any misspelling or poor grammar should raise warning flags. If the message that claims to be from your best friend doesn't sound like your best friend wrote it, take a few moments to confirm that the message is really from your best friend.

In other words, it's not rocket science. Skepticism is good and if more people were skeptical about messages that land in their e-mail in-boxes, companies would have a lot less trouble with viruses. ß

CORNER on the market by A.J. Stinnett

"If you would motivate workers, it requires that you first care for them."