Obscure Email Issues

Rebecca Herold, CIPP, CISSP, CISA, CISM, FLMI

Final Draft for May 2007 CSI Alert

There are increasing reports of email misuse, malicious use, mistaken use, and just plain bad implementations of email systems that allow the many outside threats and desperado insiders to exploit vulnerabilities. It is most common for information assurance pros to be fairly diligent in trying to keep malware out of the enterprise network through scanning and filtering emails, and it is good to see that it is also becoming a growing trend to try and prevent sensitive data from leaving the enterprise by using scanning and encryption. However, there are many other obscure mishaps and business damage that can occur through the use, or misuse, of email and email monitoring that can have negative business impact and legal implications.

The dangers of phishing, viruses, and clear text data are discussed often within email security and privacy publications and reports. However, there have been a rash of email incidents that I have read about and discussed with information assurance professionals in the past few months that I have not read much about. However, these are issues that organizations need to think about and address appropriately. A few of these topics include:

- Employee use of the company email system
- Email surveillance
- Reusing email addresses
- Non-business emails for business use

Employee use of the company email system

How much personal use does your organization allow through your email system? Have you clearly defined what constitutes acceptable personal use?

The question of whether employees have the right to use their organization's email system to communicate with each other about union matters and terms and conditions of employment ignited some pointedly different views from attorneys in a March 27 oral argument before the National Labor Relations Board (N.L.R.B., No. 36-CA-8743-1, oral argument 3/27/07).

As a brief overview, the Register-Guard, a daily newspaper in Eugene, Oregon, disciplined a copy editor/union officer for sending emails to her co-workers about union matters. The NLRB argued that allowing employees to communicate with each other in the workplace via email was in the employers' best business interests, and that a broad policy that prohibits all non-business email use should be illegal, except in special circumstances. The Register-Guard legal counsel argued that the email system is the company's equipment and private property, and that the company has the right to regulate and restrict its use for business purposes. Ultimately the judge ruled that not allowing labor union communications was discriminatory and that such communications on the company's email system must be allowed.

Most organizations I speak with, with the few exceptions of perhaps some of the most restrictive government agencies and some military units, allow for "reasonable" personal use.

When I ask these organizations what "reasonable" personal use actually means, and what the thresholds are for what goes beyond reasonable, none I have spoken to have a specific answer. It is a very subjective determination. This subjectivity related directly to an important part of the NLRB argument.

If the amount of personal use allowed is not specifically described, but indicated simply as being "reasonable," that creates a foundation for a very wide range of interpretation if an incident similar to this one goes to court.

Has your organization clearly defined what type of personal use is allowed or disallowed through your company's email system? Do you describe it with specific examples? Do you put any metrics around what constitutes disallowed personal use, such as message size, time of use, types of communications, entities with whom the emails can and cannot be shared, and so on?

Email surveillance

I have seen organizations where management and staff members were so fixated on protecting the company that they ended up doing completely inappropriate actions that involved infringing on privacy, not following their own policies, and breaking laws.

Have you ever watched The Office? I've known, and worked with, people just like every character on that show. The Dwight Shrute character demonstrates his zealousness for the company with complete disregard for the people around him, and often their privacy. He is always asking his coworkers for personal information he has no right to ask for, and he has often spied on them, often with the approval of Michael, his manager. Fiction is mirroring real life.

Recently a Wal-Mart employee was fired for snooping on email, text messages and taping phone calls. The employee was reportedly doing the surveillance at his management's approval and request. As a result of an internal investigation of the activities, Wal-Mart also fired his supervisor and demoted a vice president.

This situation points out that the insider threat is not only a conscious malicious action against the company, or a mistake, but that it can also come from a conscious decision based upon an overzealous effort to, in fact, try to protect the company in ways that not only infringe upon privacy, but also that break not only corporate information security policies, but also may be violating data protection laws.

Monitoring is an important part of information security and compliance, but it must be appropriate and legal and not at the discretion of a manager's whim or overzealousness.

Reusing email addresses

Does your organization ever reuse email addresses whenever someone leaves the company? Do you know that some of your customers' and personnel's email service providers reuse email addresses when their subscribers leave?

A friend of mine recently told me about receiving some very interesting messages containing a large amount of confidential information to a new email account he had

created. He created a fairly nondescript email address, let's say something like C.SMITH@PopularISP.com. He started receiving email to his new address from an ecommerce organization. The messages included a woman's full name, full address, phone number, credit card number, account number, and purchase history. He called the woman to let her know this sensitive information was being sent to him. She said the she HAD used that email address, but that she had cancelled it a few months earlier. Apparently she did not notify the organizations with whom she communicated with through that address. It was a good thing my friend, also a CISO, was a good guy and not some crook that would have used the information fraudulently.

This incident points provides several lessons for information assurance professionals, just a few of which include:

- Do not send confidential and personally identifiable information (PII) in clear text email messages; it is very possible it could be received by someone else.
- Do not rely upon email communications to send important information to your customers; they may no longer be using that address, and in fact someone else may be using it.
- Periodically validate your customer email addresses; make sure your customers are still actually using them.
- Do not rely upon email as your primary means of breach notification; some of your customers may no longer be using the email address you have on file for them.

Non-business emails for business use

During the first few months of 2007 the White House was accused of trying to hide emails about government business, that are subject to the Presidential Records Act, by using unofficial email accounts. The Presidential Records Act requires that all communications about and from the president must be retained.

Those emails contained information about many interesting things, such as Republican re-election campaigns and the December 2006 firings of federal prosecutors in eight cities. These emails were discovered on the Republican National Committee email domain, gwb43.com, which is not part of the official White House communications system that is configured to retain communications in compliance with the Act. Emails with information reportedly subject to the act had been used from this domain since February 2003. Apparently at least one of the emails had been forwarded to the White House email system, which led to this discovery, giving the impression to many folks that the administration was trying to "skirt the law governing preservation of presidential records." (http://www.cnn.com/2007/POLITICS/04/09/white.house.emails/index.html)

Do any of your personnel use their personal email accounts for business communications? Do they use them to communicate with your customers? I know of at least two large organizations that discovered some of their employees had forwarded all their business email to their personal email addresses so that they could answer them while they were on extended leave or vacation and not have to go through the "hoops" to get set up for the organizations' remote access solutions. This creates significant problems.

- Others may be able to access business email that contains PII.
- The personal email system may not be secure, leading to such things as having customer and personnel emails being harvested for spam, DoS or malware attacks.

- Answering customer communications from personal email accounts does not only look unprofessional to the customer, it puts your customer communications out of the control of your organization, leaving you without the ability to monitor or log such communications.
- Customers may start communicating with the personal email accounts instead of with your business accounts.
- Personnel may mistakenly send personal, and possibly inflammatory, communications to customer accounts.
- Allowing such communications to be sent outside the corporate-controlled communications system could be viewed as not following a standard of due care to protect customer information, making your organization vulnerable to noncompliance with applicable laws and regulations and potentially subject to civil actions from upset customers if bad things happen to their information as a result.

Rebecca Herold, CIPP, CISSP, CISM, CISA, FLMI is an information security, privacy and compliance consultant, writer and Norwich University MSIA adjunct professor. Her latest publications are Say What You Do (Shaser-Vartan) and The Privacy Management Toolkit (Information Shield). She can be reached at rebeccaherold@rebeccaherold.com or http://www.privacyguidance.com.