7

Email Security Policies

WE ARE QUICK TO EMBRACE NEW TECHNOLOGIES when they improve the ability to communicate. The explosion of email is the most recent testament to that. But email is not the panacea everyone believes. Aside from its ability to improve communications, email can be used to transmit proprietary information, harass other users, engage in illegal activities, and be used as evidence against the company in legal actions.

Over the last few years, there have been quite a few lawsuits that relied on evidence gathered from email archives. Recently, in the antitrust trial *United States versus Microsoft*, the government's attorneys used archived email from Microsoft executives as evidence against Microsoft. This focused the attention on many organizations' policies regarding how email is used and treated once transmitted.

Email is the electronic equivalent of a postcard. Because of this, it requires special policy considerations. From archiving to content guidelines, organizations have much to consider when writing email policies.

Rules for Using Email

Email has been around since the birth of the Internet. Messages are sent in near real-time and are not that obtrusive. The recipient does not have to read the message immediately, so it is not as an intrusion like a telephone call. It also gives the writer a chance to word the message carefully.

But this time-honored transmission comes with some responsibilities, which should not be lost on policy writers. In fact, when creating email policy, I recommend that the general rules and guidelines that users need to abide by should appear first in the email policy document. One client decided that in order to grab the attention of the users, he would include a "Ten Commandments of Email." Using email policy statements such as this is a creative way of expressing policy that gets noticed. Although they are edited to protect my client's confidentiality, here are those commandments[1]:

1. *Thou shalt demonstrate the same respect thy gives to verbal communications.*
2. *Thou shalt check thy spelling, thy grammar, and read thine own message thrice before thou send it.*
3. *Thou shalt not forward any chain letter.*
4. *Thou shalt not transmit unsolicited mass email (spam) unto anyone.*
5. *Thou shalt not send messages that are hateful, harassing, or threatening unto fellow users.*
6. *Thou shalt not send any message that supports illegal or unethical activities.*
7. *Thou shalt remember thine email is the electronic equivalent of a post card and shalt not be used to transmit sensitive information.*
8. *Thou shalt not use thine email broadcasting facilities except for making appropriate announcements.*
9. *Thou shalt keep thy personal email use to a minimum.*
10. *Thou shalt keep thy policies and procedures sacred and help administrators protect them from abusers.*

Administration of Email

What your organization does with its handling of email is just as important as your users' usage of the system. The policies and procedures that are put into place can become subjects of lawsuits, grievances, or other procedures that could embarrass the organization or the users.

The ramifications that come from email, whether it is content or how it is handled, do not appear to be taken seriously. This is a real concern because of the high-profile cases and security problems with email. Email policies should promote appropriate due diligence for both the user and administrator.

As you might have noticed, this section assumes that your organization manages its own email services. If your organization outsources its email services, you can check the contract to ensure that the service provider can manage the service to comply with the policies. However, if your organization uses an online service provider, such as AOL, your policy will concentrate on usage and have little to say on administration.

[1] These commandments are loosely based on "The Ten Commandments of E-mail Etiquette" attributed to Patricia McIntosh (`fyrewede@concentric.net`), which was sent to many mailing lists (date unknown).

Establish the Right to Monitor Email

The Internet's most ubiquitous application also can be its most dangerous. Email can be used to transmit sensitive data, harassment, and security problems. All these can be mitigated if your organization monitors email for traffic and content as well as archive messages so that problems can be investigated. If you are worried, you should consult an attorney to see what is legal in your area. Otherwise, the right to monitor is setting policies for the overall handling of the email, archiving user messages; and scanning can be the basis for these policies.

Handling of Email

A client was worried about its email policy following a lawsuit filed by a former employee. It was a small company, less than 70 users, and it was concerned about adding architecture information in its policy. After questioning this request, I was handed a copy of a deposition that was taken of its System Administrator. The plaintiff's attorney questioned how the system handled the routing of email and if that was part of the security policy.

I reviewed the deposition and other supporting documentation. I became concerned that even best-practice architectures could be used as evidence against an organization. The challenge I faced was to write a policy statement that would allow the organization to architect a system yet protect themselves from being prosecuted for those technical decisions. Following is what I came up with:

> *Network and Security Administrators shall architect the email system in a way that will allow the proper delivery of messages both within the organization and to the Internet. This system shall be allowed to use, but not be limited to use, proxy, forwarding, gateway, and manual services to operate this service.*

Although this is a very broad statement that could be used for any architectural policies, it satisfied the organization's attorneys.

Archiving Email

Do not take the storage and retention of archived email lightly, because if Microsoft had followed its policy, the messages that were used by the government would not have existed. This is not to say that I support using email for allegedly illegal activities; but if your organization is going to have a policy, it should be realistic and should be followed.

Archiving and retention policies have two components. The first is to say that email will be archived. The other is to define some parameters for the length of time that email could be archived. As with other policies, it might be best to defer the storage types and some of the retention lengths to the implementation documents. However, you should include some guidance in the policy document:

> *The organization shall retain and archive all email messages that pass through its servers. The archive shall be retained on an online storage medium. Administrators shall archive messages to an offline storage medium every six months and purge those messages from the online stores.*
>
> *The organization shall retain that offline storage medium for at least two years but may retain it for longer periods at the discretion of management. The offline medium shall be erased or destroyed in a manner commensurate with its technology.*

Some larger organizations, especially government contractors, could have problems with creating a single policy for archiving and retention. They might be contractually required to implement a policy that is different form the one you are writing. If this is the case, the organization can include the following in its policy statement:

> *The organization shall alter its policy to comply with contractual obligations on an as-needed basis and without policy review. These changes shall only affect those users who perform work for that contract, and the organization shall notify those users of the changes prior to their implementation.*

Scanning Email

Over the last few years, email has been used to spread computer viruses around the Internet. To combat this problem, many administrators have installed virus-scanning capabilities to their networks. This can be good, but is there a policy to do this? In this litigious world, you would probably not be allowed to do anything with information gathered without a policy.

Content-scanning policies allow the organization to look at the content of the messages. For whatever reason, some organizations feel they need to monitor email content to prevent embarrassment or proprietary information from being disseminated. The problem is that content-scanning policies are just not nice. They read like the organization is looking over the shoulder of its users because they are not trusted. For some organizations that project a "family" atmosphere, I can see how the culture might frown upon this practice. For others, it could be a necessary evil.

The concept is to write a policy statement that will allow your organization to scan all email in a manner consistent with the organization's business goals. If your organization is scanning for viruses and other problems, the policy should say this. If your organization will be doing content scanning, then the policy should say it. Regardless of the policy, if your organization chooses to scan email, there should be something, such as a publicly accessible document, that explains what is being scanned.

For virus scanning, you can have a policy that reads

> *The organization shall scan every email message that passes through its server to check for computer viruses, worms, or other executable items that could pose a threat to the security of the network. Infected email shall not be delivered to the user.*
>
> *Administrators shall have procedures in place for handling infected email messages.*

When content scanning, one policy I helped write read

> *The organization shall be allowed to scan the content of every email message that passes through its servers based on a predetermined criterion. If the message does not pass the criteria, the message shall not be delivered to the user.*
>
> *Administrators shall have procedures in place for handling rejected messages.*
>
> *Management shall have procedures for enforcing these policies, including, but not limited to, disciplinary procedures for users or involving law enforcement for non-users.*

Finally, either section may add the following:

> *The organization shall make available the list of items being scanned at the server.*

Limiting the Size of Email

Email clients have made it easy for users to create fancy messages and transmit large amounts of data by attaching files stored on the system or the network. With each new file format, the amount of data filling network bandwidth increases. One well-known university estimated that over half of the email messages sent through its servers contained attachments of a newly popular audio file format.

The problem is not limited to universities. Some organizations are finding that users have been sending documents to colleagues via email rather than using network file servers as a single storage location. To manage resources used for email, some organizations have updated their policies to include a limit on the size of the file transmitted.

Email size restriction policies can be as simple as everyone being limited to a particular size message. However, there could be cases where exceptions need to be made. In one organization I worked for, a person acting as a librarian was required to send and receive large messages from customers. They wanted a policy that was more flexible than limiting everyone to one size. Their solution was to create a policy with a statement that said there could be an exception if reviewed by a manager. That policy read

> *Email messages sent to and from users shall not exceed 40 kilobytes in total size. Exceptions shall be made for users with requirements that cannot be meet within those limits. The user's manager shall review these exceptions individually.*

Use of Email for Confidential Communication

I cannot stress enough that email is the electronic equivalent of a postcard. Information that is transmitted over the Internet passes as readable bytes available to anyone who can read them. As the traffic passes from one network to another, the probability of your email message being read increases. Additionally, if your message ends up in the wrong mailbox, you can unintentionally reveal information that should not be released.

After the message leaves your system, you have no control over who can read the message or that it even reaches its proper destination. Because of this, some organizations create policies that do not allow confidential or proprietary information to be included in email. Others might have policies in place to allow users to send confidential information among themselves but not to users outside the organization.

Encrypting Email for Confidentiality

The third option is to have a policy that requires confidential and proprietary information to be encrypted before it is transmitted. By encrypting the message, it should be able to be read only by the intended recipient. However, the use and handling of encryption is not to be taken lightly. There are many issues, such as key management, key recovery, and export restrictions, that are beyond the scope of an email policy. Although encryption policies are discussed later (see Chapter 9, "Encryption"), you can include a provision in your email policy for its use. For example:

> *Proprietary information sent to users outside of the organization shall be encrypted prior to its transmission. The use of encryption shall be consistent with the organization's encryption policies.*

Digitally Signing Email

Another concern with email is that a message can be created to disguise the real sender. This is called "*spoofing*." Although it is used by those who send unsolicited bulk messages (spam), it also can be used as a tool in corporate espionage. In this scenario, messages sent to the organization's users look like they came from familiar sources in an attempt to convince them to return proprietary information.

Users can contact the suspected requester to verify that they sent the request. But the culture of email is so trusting that this is rarely done. The only way to ensure that the message is a valid request is if it was digitally signed. Digital signatures are part of an encryption system that uses the cryptographic algorithms to create a numeric value unique to your message. Like encryption, policies governing digital signatures are best left to the encryption policy statements (see Chapter 9). Again, you can include a provision in your policy such as

> *Any request for proprietary information shall be digitally signed and that signature verifiable.*
>
> *Users transmitting proprietary or sensitive information shall digitally sign the message to demonstrate validity and traceability to the recipient.*
>
> *The use of digital signature shall be performed in accordance with the organization's encryption policy.*

Summary

Email is the electronic equivalent of a postcard. Because of this, it requires special policy considerations. From archiving to content guidelines, organizations have a lot to consider when writing email policies.

1. Rules for using email:
    - Policies should be written to promote the responsible use of email that supports the organization's goals and business requirements.
    - Some of the items that should be included in the policy concern courtesy, content, general usage, and compliance with the policy.
2. Administration of email:
    - Policies describing the administration of email discuss the actions the organization will follow in the management of the email system.
    - Administrative policies should establish the right to scan messages passing through the email system. This scanning can be for viruses or content. Regardless of the scanning type, there should be a policy in place that says the organization is doing this.
    - Email policies might include mechanisms to limit the size of messages to prevent the overloading of servers and network bandwidth.
    - To mitigate other problems, the organization might want to include a policy that allows them to use proxies, gateways, and other means to aid in the transmission of messages. These policies should not imply that messages are being filtered or retained.
    - If email messages are archived, there should be a policy that outlines the basics for how this will work. This policy also should define retention periods and potential exceptions to the policy.
3. Use of email for confidential communication:
    - Policies for sending confidential communication include provision for encrypting the data before transmission and signing them with digital signatures.
    - Encryption policies are really not the scope of email policies. Thus the policy statements should refer the user to the organization's encryption policy for that information.