Vulnerability Management:
Effective Use Policies and Secure
System Architectures for Email and Instant Messaging

Final Term Paper

Megan Casey
Senior in MIS
BADM 395
Abstract:

Businesses are becoming more and more connected through online communication systems. Two components of these systems are email and instant messaging. Both of these functions provide similar benefits of easier and more efficient communication, but they also come with inherent security risks that can threaten any organization. Threats such as viruses, malware, spam, identity theft, stolen confidential information, and privacy issues plague the benefits that come with these systems. There are multiple ways to protect against these though, and all businesses can take steps to protect against any vulnerability that threatens them through email and instant messaging systems.

Introduction:

Many corporations have been depending more and more on internet communication and collaboration tools to get their businesses moving faster. Email and instant messaging provide more flexibility and convenience in communication that has not been available before. But with this convenience come new types of security and vulnerability concerns that are inherent with instant messaging (IM) and email systems. Many email systems have been tailored to manage the growing number of security problems, but new problems have arisen with the use of IM. A business needs to recognize these problems and vulnerabilities and take steps to remedy them through a certain best practices framework. They can do this by not only physically securing their network from viruses, spam, and intrusions through a tailored enterprise instant messaging system, but also by writing an effective use policy for email, instant messaging, and other internet
communication software use. These measures will provide the security protection that is needed now and will be needed even more with the increasing use of instant messaging in the workplace.

**Email Security:**

When using email in an organization, there are a number of security issues that come into play. These concerns include viruses, worms, spam, phishing, and the loss of confidential or sensitive information. (Licari 46) Viruses and worms can cause large losses of company information at times when unknowing employees open an infected email and bring this virus in to spread throughout the corporate network. These viruses are actually now evolving and being combined with spam to find new ways of entering a network. Spam messages that employees receive can install a virus or worm onto the network or even trick the employees to give away confidential information through “phishing”. Employees are given a false link to a website that they trust and enter information like user names and passwords that are directly sent to the criminals running the impostor websites. (Licari 46) This information can be used to access company files, networks, or emails, and sensitive information such as customer identifying information, employee information, or financial information from these directories can be stolen and used against the organization.

There have been many countermeasures created to combat these email security concerns, such as tighter multiple-level virus protection, spam filters, and phishing recognition.
software. Most organizations have learned that web-based email providers are not secure enough for their corporate environments and have created their own proprietary email systems or use an enterprise email system provided by a software company. (Holman) These systems are much more secure than free web-based systems in that they use encryption and secure local authentication and servers. (Holman) IT administrators can create controls over these email systems that are not possible with consumer email systems. The internet and email policies are also integral to a secure network and protect against any legal response to a security breach. These policies outline what is expected of employees when it comes to using a computer on the company network, and they protect the employees’ rights and the rights of the organization. Specifically, there are use policies for communication software such as email and instant messaging.

**Use Policies Best Practices:**

There are best practices when it comes to writing an organization’s policy for communication software use. Basically these best practices rely on three key issues: the privacy rights of the employees, the need of the employer to protect system security and manage company resources, and rights of third parties to obtain access to company files. (Peltier 35)

In the case of the privacy rights of the employees, there is a need to protect the company from security breaches, but there is also a need to protect the employee from too much monitoring done on the part of the organization. The aim of the policy should be to
create a balance between these two factors. (Peltier 35) When it comes to employee privacy rights, it is important for the employee to know that their every single move is not being watched when they send email so that they feel free to use email to communicate efficiently and effectively. The employer then needs to perform a risk audit to determine if they need to monitor any parts of email transmission, since the organization needs to protect their security and their company resources. Based on the risk that they find, the policy the organization writes may have to include their positions on issues such as sexual harassment by email, discrimination by email, libel and slander by email, using email for insider trading, leaking trade secrets or competitive advantage information through email, and the rights of third parties to get access to certain company files using email. (Peltier 36-37) Since online communication is not face-to-face, there is more of a risk for employees to feel freer to sexually harass, discriminate, or give away confidential information since they feel partly anonymous over the internet. An email policy is therefore needed to address these issues.

The email and internet communication policy should primarily address three key issues: “purposes for which email can be used”, “what third party access to email is allowed”, and the “consequences for a breach of the email policy.” (Peltier 40) Also included should be the statement that the employees’ privacy will be kept, and then the organization will list what monitoring measures they will take, if any. The employee should be trained in the email system to protect privacy and security, and the organization should fully disclose this email policy to the employees. (Peltier 38-39) Some organizations might even include a policy on the creation of passwords for email. With
each of these provisions, employees feel more relaxed that their privacy is being
protected, and the organization keeps their rights to protect the security of the company
network and the privacy of the company.

**Email Use Policy Example:**

An example of an email use policy is that of the University’s, as was described by Mike
Corn, the director of security and privacy services. The University’s acceptable use
policy is made up of underlying principles for the use of the University network,
UIUCnet. These underlying principles give academic freedom to electronic
communications, but also state that proper etiquette, behavior, and legality will be
enforced. If any violations occur, the user could lose their privileges to network access or
be reported to authorities if needed. (“Policy on Appropriate Use of Computers and
Network Systems”) The policy then goes on to define who are the authorized users of the
network and the responsibilities of those users to keep their password private and protect
their user identity. It goes on to talk about what process the University goes through
when monitoring electronic messages and disclosing them to the authorities, if this is
warranted. Mike Corn also talked about this in his presentation and shared how the
University has had to follow this policy in the past when authorities take advantage of the
network administrator’s access to electronic transmissions. The policy then goes on to
state who has responsibility in maintaining, securing, and designing the network, and any
bandwidth limitations that are put in place on the network users. (“Policy on Appropriate
Use of Computers and Network Systems”) The University acceptable use policy is just
one example of how organizations protect their networks from privacy invasions and security breaches.

**Instant Messaging Security:**

Many of the security threats are the same for instant messaging as for email, but because of the real-time nature of IM, many aspects of these systems that are unlike those of email systems are creating new security problems for many businesses. The constant demand for information is driving the need for real-time communication systems in a majority of organizations today. The speed with which information is accessed with these systems creates valuable business efficiencies for those organizations that use them; these organizations gain an advantage that businesses without instant messaging systems cannot obtain through only email or telephone. Along with these domestic efficiencies, comes the opportunity for efficient and effective global communication within worldwide organizations. (Gilliland 16)

With these faster real-time communications systems, there is a threat of information and network security intrusions. These threats are increased if the system is mismanaged, or not managed at all, by an organization’s information technology department. Some companies do have policies regarding the authorized use of instant messaging systems, but most of the time, these companies lack the basic security and management controls needed for safe use of these systems.
Instant messaging systems are becoming more and more widely used in many corporations, increasing the threat of attacks with each unmanaged user. By 2008, the estimated IM user base will be 592 million, with 85% of enterprises using some sort of an instant messaging system at this time. (Gilliland 16) The reason that the use of these systems is spreading so rapidly is because of the benefits that come from using real-time internet communications, but also because the common IM clients are free and easy to install and use. Clients such as AOL instant messenger (AIM), Yahoo! Messenger, and MSN Messenger are readily available and installable even in networks with active, locked-down firewalls. Increased numbers of users mean even more value for an organization; more people can be easily contacted in real-time if more people are using an IM system, making efficiencies even greater. (Gilliland 16)

More widespread use has meant more opportunities for hackers to use IM systems to their advantage. A new way of gaining access to a network or information has been created with the use of IM clients. Some hackers prefer this since instant messaging is an unprotected and widely used channel. They can use IM to start instantaneous threats to a network. In some cases, up to 500,000 machines can be infected in a network within 30 seconds. (Gilliland 17) IM systems are also an easy target because users can easily transfer file-based content and are in use on a number of mobile devices and personal computers. (Gilliland 17) Viruses and malware are most easily spread in IM systems through links in instant messages or personal user profiles. A user is led to believe they are receiving an image or website link from one of their fellow trusted users, when in actuality the other user has become infected and the virus is being spread through their
IM client. This is one of the ways viruses and malware threats are rampantly spread throughout a network. Other security concerns of instant messaging are eavesdropping and identity theft and impersonation. (Park 18-19) With eavesdropping, individuals look at what is sent over the public internet with a sniffer. This means that anyone with this technical knowledge can see exactly what an employee is saying to another person on their free IM client software. This can be damaging to the organization if the employee regularly talks about sensitive company information while instant messaging. Along these same lines is the threat of identity theft. Sensitive company information can also be stolen when an employee’s user name and password is hacked into and they are impersonated online. The impersonator can then ask for information from another employee and it will be given to them because they are seen as the trusted employee. (Park 19)

The first reaction an organization may have to the use of instant messaging in their network is to totally block all IM clients on their computers. This proves more costly and difficult than one would think because of the way that IM systems were designed to find their way out of a corporate environment. Common IM systems are designed using a simple architecture, composed of a specialized client and a scalable service. When users log in, they communicate only over that connection and the service never actually connects with the user. The user establishes all connections with the service, and this is initiated from the “inside out”. (Gilliland 18) After the client logs in, they are redirected to additional dispatch servers. The client will cache the IP address of this server and connect directly to it each time they log in. Because of this, IT administrators cannot
possibly block all the IP addresses of these dispatch servers because new clients log in all the time and new servers are constantly being added. (Gilliland 17-18) Another problem is that in an enterprise environment, IM systems will find ways to connect to the server using HTTP. When they do this it makes is harder for the client to be blocked. (Gilliland 19)

Another problem with totally blocking IM systems is the lost productivity or efficiency that the organization gains from using instant messaging. People in the organization would not be happy about administration blocking this convenience from them. Taking the approach of totally blocking instant messaging systems can impede an employee’s productivity and hinder business activities that depend on instant messaging for communication. (Gilliland 19) Rather than blocking IM usage, a better strategy would be to leverage IM use for the benefit of the organization. This would include administrators controlling and managing IM use and providing real-time message filtering and virus protection. Since current virus protection is not sufficient enough for IM systems, some changes will have to be made. This is because desktop protection does not provide the multiple-layer protection that is needed to secure the IMs and since frequent updates are required for desktop protection, it may not be able to detect a new virus that has been spread at the speed that IM systems allow. Therefore there is a need for immediate virus protection even before the updated virus directories are updated to each machine. Also, since IM users are more likely to trust other known users and fall victim to becoming infected from their infected friends, desktop virus protection can sometimes not prevent these deliberate actions. (Gilliland 20)
**IM Security Best Practices:**

In order to proactively manage and secure the use of instant messaging, organizations should develop a corporate policy for the use of instant messaging within the enterprise. This should include flexible management and security solutions that can ensure that all policies are being followed. Also, administrators should deploy a means to allow the IM client to connect to the service, but then the connection should be managed and controlled by an application or an IT administrator. Malicious content should be filtered and scanned and user access to file sharing within the IM client should be controlled, along with users’ IM usage. (Gilliland 20) Organizations should continually educate employees on security risks and enable proactive spam and spy ware protection (Licari 48) If IT administrators take these steps, they can still allow common IM clients in their enterprises and not be worried about the inherent security concerns that come with these programs. Businesses will be able to embrace IM systems and reap the productivity and financial benefits that a communication system like this can provide.

An instant messaging corporate use policy would be similar to those of email use, but with more of a focus on real-time communication and the security issues that come with it. According to the Multi-State Information Sharing and Analysis Center (MS-ISAC), there is a certain format or template many organizations can use that will fit their needs. The main parts of this template include the purpose of the policy, the specific policy, the rules that must be followed, term and acronym definitions, the rationale or source of the
policy, any cross-references to any other corporate policies, reviews or revisions to the policy, and the governance of the policy. The purpose includes aims such as to “outline the limitations of the use of the technology”, “protect company information”, “describe the expectation of privacy when using the company provided system”, and “outline the rules applied when using the company provided system.” (“Instant Messaging Use Policy”) After the purpose, the policy itself is stated. This usually states that the employee must use the instant messaging service provided to them in a manner that is not personal and they must not use it to communicate sensitive information that may hurt the company, usually the two largest issues in instant message use policies. The rules are then stated after the policy. These rules give specifically what is and what is not allowed when using the instant messaging service, and also what the privacy rights of the employee are. For example, the policy may state that IM cannot be used for personal use, it may not contain profanity, obscene jokes, confidential information, or any illegal content, and it will state that the company will be monitoring the instant messages and saving conversations for a particular period of time. The rules are followed by the term and acronym definitions for any unfamiliar terms that are used in the policy, and then by the rationale the company used to create the policy. Cross-references with any other use policy are then stated and the governance - what responsibilities there are to adopt or implement the policy - is listed last. A well-thought out and organized plan like the one outlined by the MS-ISAC can make it clear what expectations a company has about their employees’ use of instant messaging and can protect them from any misuse that may occur. (“Instant Messaging Use Policy”)
Enterprise Instant Messaging Systems:

Another approach to embracing instant messaging and using it for communication in an organization is using an enterprise instant messaging or EIM system. These systems are built with different architectures that make them more secure and also easier to control. (Park 31) If organizations take the time to analyze their environment and these four EIM architectures, they can choose which one is sufficient for them and best for their network.

The first of these architectures is gateway policy enforcement with a consumer instant messaging (CIM) system. This is the simplest architecture since it still uses a free client instant messaging system. In this system there is a local centralized control function to make it easier for administrators to monitor and enforce IM traffic. This is done by installing software just behind the corporate firewall so the administrators can monitor all network traffic and ensure that the instant messaging traffic is routed through the gateway. This software can also enforce any restrictions put in place by the administrator or by a use policy, including IM blocking, user blocking, conversation logging, content inspection, and auditing. The gateway policy enforcement architecture does not replace or change the basic functions of the consumer instant messaging system, but it transfers administrative control for these systems from the individual user to a centralized function. (Park 31-32) This architecture is pictured graphically in the diagram below from an article in Information Systems Security by Joon Park and Tito Sierra.
Another architecture for instant messaging systems is the dedicated EIM architecture. Free consumer IM (CIM) systems are not used with this architecture, but an entirely different and secure dedicated system is utilized. The functionalities of the free client IM systems are mimicked, but the system is much more secure since all the functions are handled behind the company firewall. This architecture supports only EIM sessions and not CIM sessions. (Park 32) The diagram of this architecture from the same journal article follows.
The next architecture, the hybrid solution, is a combination between the gateway policy enforcement architecture and the dedicated EIM architecture. This architecture supports both EIM and CIM messaging sessions, with EIM messages being routed and encrypted locally and CIM messages being routed through the previously mentioned gateway software. (Park 33) An illustration of this architecture from *Information Systems Security* is pictured below.
The fourth and final EIM architecture is centralized IM control. With this architecture, a centralized hub model is used to support both EIM and CIM sessions. An example of one of these centralized hubs is Yahoo! Business Messenger, which routes the messages from the Yahoo! Servers. The functions of presence and message routing are handled on servers outside of the company firewall and the functions of authentication and security management are handled within the company firewall with this architecture. (Park 33) An overview of this system is outlined in the following diagram from *Information Systems Security*.
When analyzing and comparing these different architectures, the chief differentiation factor between regulated EIM systems and unregulated CIM systems is the addition of local administrative control. (Park 34) EIM systems shift control from the employees to
an administrator within the company that can control the IM traffic and enforce any use policies that are put in place. This access control is the major selling point for all EIM systems. Different access configurations can be set up, such as restrictions on access to IM clients on the enterprise or employee level, or even on the group level. These restrictions would be needed if some employees have not followed the use policies for instant messaging, or if IM is not needed with some groups of employees. It also allows for the control of who can share messages with whom on the network, and whether file sharing and transferring will be allowed within the organization. All of the architectures mentioned except gateway policy enforcement authenticate users locally behind the firewall, which provides even more control and protects against the possibility of an attacker intercepting transmitted messages which may contain sensitive information. (Park 34-35)

There are six other functions that differ among the four EIM architectures: the messaging sessions supported, the message routing, the client software used, encryption, interoperability with an existing CIM system, and finally performance. The gateway policy enforcement architecture supports only CIM clients while dedicated EIM supports only EIM clients; hybrid and centralized IM control support both types. Being able to send and receive messages with the much larger CIM user base would be attractive to some companies, but the increased security with only utilizing EIM messaging is also an asset for companies that use the architectures that support them. (Park 36) As for message routing, it is more secure for messages to be routed internally through an EIM session (like it is with dedicated EIM, hybrid, and centralized IM control) than through a
CIM session since these messages are encrypted and can be more closely monitored. (Park 36) The only architecture that does not require the installation of a new IM client is gateway policy enforcement. The others require an application to be installed on each desktop, which may cause some disruption with users. This is a key selling point for gateway policy enforcement solutions. (Park 37) Since CIM clients have not originally supported encryption for message sessions, the gateway enforcement architecture is the only one that does not give encryption as an option; encryption can reduce the threat of eavesdropping on IM conversations. (Park 37) All of the architectures except for dedicated EIM offer interoperability with a CIM client; this interoperability is required for the gateway enforcement policy architecture. The hybrid and centralized control architectures have interoperability with a CIM client as an option that can be controlled by an administrator. Having interoperability with a CIM client offers a lower level of security because of the unregulated manner of the client. (Park 37) Finally, from a performance standpoint, those architectures that are routed locally – dedicated EIM, partly hybrid, and centralized IM - are expected to have improved performance since they are not routed externally over the internet like with CIM sessions. (Park 37)

The differences between the functions discussed are illustrated in the table below, taken from the journal article by Joon Park and Tito Sierra. Based on these differences, the best architectures from a security standpoint are dedicated EIM, the hybrid solution, and centralized IM control, since access control, authentication, message routing, and encryption are done on a local level within these architectures. The only drawbacks to these designs are the fact that a new EIM client must be installed for each user of the
system, and also that the user base of instant messaging is greatly reduced from the millions of users that use consumer IM systems. (Park 38) An organization can assess the company’s and employees’ needs and determine firstly whether a CIM or EIM system is right for them and secondly, if an EIM system is most sufficient, which architecture would best fit those needs. For those organizations solely concerned about efficiencies and saving costs, and have no resources for an enterprise instant messaging system, using a consumer IM system with gateway enforcement would be the best choice for them. On the other hand, a larger corporation with plenty of resources may want to take full advantage of an EIM system and gain the benefits of both the heightened security and additional functionalities. It is necessary for any organization to audit their systems, determine which system would fit in best with their existing infrastructure, and figure out which aspect (security, functionality, low-costs, or ease of utilization) is most important for them.

<table>
<thead>
<tr>
<th>Table 2</th>
<th>Comparative Matrix of the Four EIM Architecture Types</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Gateway Policy Enforcement with CIM</strong></td>
<td><strong>Dedicated EIM</strong></td>
</tr>
<tr>
<td>Access control</td>
<td>Local</td>
</tr>
<tr>
<td>Authentication</td>
<td>Remote</td>
</tr>
<tr>
<td>Messaging sessions supported</td>
<td>CIM only</td>
</tr>
<tr>
<td>Message routing</td>
<td>Centralized CIM</td>
</tr>
<tr>
<td>Encryption</td>
<td>Depends on vendor</td>
</tr>
<tr>
<td>Client software</td>
<td>Existing CIM</td>
</tr>
<tr>
<td>Interoperability with CIM</td>
<td>All major CIM services</td>
</tr>
<tr>
<td>Performance</td>
<td>Low</td>
</tr>
</tbody>
</table>

(Park 36)
EIM Example:

Besides offering different configurations and security features, EIM systems can add new functionalities that not available with CIM systems but are beneficial to employees. An example of one of the EIM systems that is available for all organizations to use is the Sun Microsystems Enterprise Messaging system. This is a packaged system that can be easily installed into a corporate environment and can be integrated with other Java applications. Being a dedicated EIM architecture, the administrator has control over access, authentication, encryption, and other system functions. The instant messaging system is part of the larger Enterprise Communications Suite, which includes enterprise solutions for calendars, email, and real-time collaboration. For each employee, this suite costs $50 and includes all support needed for the switch to the new software as well as troubleshooting. (“Sun Java System Instant Messaging”) The real-time communication tool adds a lot more useful functions than free consumer IM client offers, such as a Java applet-based messenger for either one-on-one or group messaging, group chatting, polling, file transferring, a conference room-like environment for online meetings, news channels, message archiving, calendar reminders, and message forwarding to a wireless device if desired. All of these functions can be configured both by the user and by the corporate administrators, with the administrators controlling access and user functionalities, using logging and message audits to control content in messaging, and controlling spam and viruses with message filtering. Development features within the system also allow different organizations to augment the system and tailor it to their own
needs by adding functionalities or changing configurations. (“Sun Java System Instant Messaging”) This system also ties in directly with any IM security policies that are established. The features and access controls directly reflect what the organization has established as a standard. Overall, the security that this EIM system offers gives an organization peace of mind that their sensitive information is secure, they are protected from viruses, and that their employees are collaborating more easily and gaining productivity and satisfaction. (DeMaria)

**Conclusion:**

With the information provided earlier, it is evident that organizations must take both technical and administrative measures to ensure that corporate information is safe, corporate networks cannot be infiltrated, and both employee and customer information remains private. With instant messaging systems, companies must realize that while great efficiencies and conveniences are created, there are also real and dangerous security risks associated with these systems. By first auditing their needs, capabilities, and risks, companies can create efficient email and IM use policies and protect against privacy and security threats. The controls they create in these policies can then be directly implemented through the management of their email and instant messaging system. Users can be restricted, file sharing can be blocked, and administrators can filter messages to ensure the policies are being followed. With these controls, organizations can leverage IM use for the benefit of the company, rather than blocking it entirely and losing efficiency. By taking the time to analyze their systems and risks, organizations
can be sure to recognize risks to security, write the correct use policies, install the correct online communication systems, and understand their environments so they can be ready for the next innovation in communication systems and the security threats that come with it.

References:


