



Market Perspective Whitepaper  
March 2007

## Control Your E-mail, or It Will Control You

> [orchestriawhitepaper](#)

**Business has a health problem**

Almost every corporation today is faced with a condition that can destroy them and disgrace (perhaps even imprison) their leaders. Yet, most choose to ignore it, allowing it to worsen. This represents a potentially fatal inaction on the part of the business community.

The ailment we refer to here is uncontrolled electronic communication. Not the technology itself, mind you, but the lack of control. But, if it's such a threat, why ignore it?

Unfortunately, we seem predisposed to just this sort of inaction. Illness is unpleasant, so we have the temptation to ignore it. It can be expensive and difficult to treat, so we have an incentive to let it slide. It's also frightening, so we want to pretend it isn't there. Ignored and left untreated, any illness can grow and worsen, subjecting the victim to an array of symptoms, pain, and debilitating effects.

The wise course, even though it may be difficult, painful, and expensive, is to treat the malady for what it is. Attack it with medications and other treatments as may be needed to subdue it, including changing one's behavior and habits permanently.

Since we're talking about electronic communication, wouldn't the most expedient and effective solution be to simply cut it off? Hardly. In reality, we can no more do without electronic communication in business than our bodies can do without vital organs.

So, we are left with a search for treatment, perhaps even a cure. Before we find it, though, we need to know what we are dealing with.

**What is electronic communication?**

Principally, when we speak of electronic communication we mean e-mail. But, there are really two basic varieties. The first and still the most common is the message, which is transmitted via enterprise e-mail systems like MS Exchange, mobile devices like Blackberries, and

*The ease-of-use has created a casual and impulsive e-mail culture. People give little thought to what they write in an e-mail, even in a business environment. Compounding this dilemma is the lack of control over electronic messages, since they can be printed, saved, and forwarded at will.*

Web mail services like Hotmail and Yahoo. The other basic variety is the conversation, which is typified by Instant Message services like AOL IM, and MS Instant Messenger.

From here on, whenever we use the word “message” we refer exclusively to those individual missives transmitted via any one of a variety of electronic communication technologies. And, we will use the term “messaging” to include those technologies, especially e-mail and IM.

All forms of electronic communication have a few common characteristics:

- They’re easy. After all, that’s the point of the technology: all you need to do is type and press “Send.”
- They’re impulsive. That is, messages typically are created and sent without a great deal of planning or forethought.
- They’re indelible. Messages leave a virtually permanent trail of electrons and pieces of data in the computers, servers, and networks used to create and transmit them.
- They’re uncontrolled. That’s the point here. Messaging is uncontrolled because the threat is not well understood and largely unrecognized.
- They’re outside the law. Although this characteristic is a matter of perception, the effects are very real.

The ease of use and ubiquity of messaging has given rise to an informal, even casual, communication culture in which anything goes. People will do things via the Internet and say (i.e., write) things in e-mail and IM that they might never consider committing to a physical document—including illegal things. And, therein lays the root cause of the critical business problems we discuss here.

#### **When silence is not golden**

Interestingly, the characteristics of messaging have also produced one of the more curious and potentially damaging quirks of our modern electronic culture: the lost capacity for conversation. In offices everywhere, workers and managers are choosing not to speak

to colleagues in the next office or even in the next cubicle, communicating instead by e-mail or, increasingly, IM. This practice extends well beyond the office cooler to include our business, personal, and professional relationships. We are becoming a devocalized society.

In a devocalized society, there is a presumed privacy, even anonymity to messaging. But this could not be further from the truth. While a personal conversation or a telephone call may be transient events, a message has permanence. That presumption of privacy and the ubiquity of messaging combine, in the devocalized society, to dissolve the caution and judgment that we formerly applied to all our communication.

When that happens, all control has been lost.

#### **Control is not a new idea**

Every business has its own set of mission-critical software applications. They keep track of finances and inventory; control manufacturing, supply, and purchasing processes; and manage relationships with employees and customers, just to name a few. All of these types of electronic systems contain data that is critical to the success of any company in the form of intellectual property and highly confidential information. Just think how near and dear your financial records and contracts are. The information they hold has a value that far exceeds that of the products and services they may represent.

All enterprise-level software applications have tight controls to limit access, control usage, and protect corporate assets. That is, all but one: messaging. Without control of the messages flowing into, out of, and within your corporation, you really have no effective control over anything else.

#### **Truth and consequences**

The threat is real and immediate. Research done in 2004 by the AMA and the ePolicy Institute showed that more than one in five companies had their e-mail records subpoenaed and more than one

*In a devocalized society, there is a presumed privacy, even anonymity to messaging. But this could not be further from the truth. While a personal conversation or a telephone call may be transient events, a message has permanence.*

in eight fought lawsuits that were triggered by employee e-mail. Yet only one in three had e-mail retention policies and only about one in twenty retained Instant Message (IM) conversations.

The array of abuses that can be committed via electronic communication is almost limitless. In fact, for nearly every use that electronic communication can be put to, there is at least one abuse that can be committed by the same action. With the simple click of the send button, a message can:

- Be the vehicle for the deliberate theft or inadvertent loss of intellectual property and sensitive information, including trade secrets and confidential customer or consumer information;
- Send inappropriate content, as in the Zubulake discrimination case;
- Breach your industry rules and regulations and;
- Bind you to contracts without due authority;

The truth is that every message sent from your company bears, at the very least, the apparent authority of the corporation. In addition to the actual authority that may be explicitly granted in a message, or the implied authority that the recipient of a message might reasonably expect the sender to possess, any message sent from your company can be seen as speaking for your company. Remember, every message leaving your company carries your company's name (or at least a recognizable part of it) within the domain name in the message header. So without control, anyone can speak for your company.

Also, the threats of internal abuse are as great as those of external abuse. That is, messages that never leave your firm can still do great harm. This is why perimeter-based solutions are inadequate. They ignore the internal threats and abuses.

All messaging abuses can cause material harm, whether the intention to do so exists or not. Ultimately, they can destroy brand and damage shareholder value.

*The truth is that every message sent from your company bears, at the very least, the apparent authority of the corporation.*

*Just because your company doesn't keep an archive doesn't mean the messages they might otherwise store don't exist. Quite to the contrary, they do exist, and they exist outside of your control.*

### **Out of sight, out of mind?**

Importantly, the lack of a centralized message archive offers no protection. In fact, without an archive, the danger is worse. Just because your company doesn't keep an archive doesn't mean the messages they might otherwise store don't exist. Quite to the contrary, they do exist, and they exist outside of your control. Just because you don't archive, don't assume others don't. Those messages still exist in the private archives within the PCs of every sender and recipient, as well as within recipients' corporate archives.

And, you should have no doubt that individual employees are storing their own messages, both sent and received. This is especially true for employees contemplating resignation. In fact, a key indicator of the intent to resign is the sudden personal archiving or downloading of company data by an employee. This is exactly the situation in which uncontrolled messages can be the most dangerous.

### **Corporate responsibility**

The question of accountability is central to this debate. Who, in fact, is accountable? Employees? Managers? Shareholders? The fact is all are accountable and responsible.

Employees must act responsibly, ethically, and legally when messaging. They must learn to communicate under the assumption that every word is viewable and traceable.

Management teams have a duty to care—for their own actions, their employees' welfare, and shareholders' expectations. Finally, shareholders have a duty to ensure that no measure to control messaging is ignored.

Moreover, all employees have the right to a safe workplace. But their safety is threatened by uncontrolled messages. Employers are liable for all incidents of harassment and abuse among employees. In many cases, both the act of abuse and its evidence exist in the form of a message.

*There's much more to curing this ailment than telling people what not to do. What's needed is detailed and real-time visibility into each of the numerous actions and behaviors that can pose a threat.*

### **At last: a cure**

The Radicati Group estimates that by 2008, more than 40 billion IM conversations will take place every day. Yet, despite the looming threat, there is a pervasive belief that control is simply a matter of informing employees (and executives) about restrictions on the use of corporate messaging and warning them about privacy limitations.

However, there's much more to curing this ailment than telling people what not to do. What's needed is detailed and real-time visibility into each of the numerous actions and behaviors that can pose a threat. And beyond visibility, corporations today need the ability to act—appropriately and in real-time—on every message that bears on good governance.

Happily, there is an answer: the ability to apply intelligent, accurate policies and uphold corporate standards in every press of the Send button. That's the ability that comes with the Electronic Communication Control (ECC) approach. ECC works with your employees in real-time, analyzing every single message as it is created and amends each one before it is sent to be certain it is working for you and not against you.

ECC can be applied to all communication channels, from e-mail to Instant Messages to Web transactions to mobile messaging. This ensures that uncontrolled, unethical, and potentially dangerous messages won't go undetected—or uncorrected.

Policies are at the heart of ECC. Highly accurate and effective policies enable APM to detect and deter in real time. But, they go far beyond the capabilities of typical keyword lists. They take the rules and sound practices determined by law, regulation, ethics, and good common sense and apply them to messages. A good policy determines who can send what—and say what—to whom, and what happens when there is a violation.

### **The final word**

At the beginning of this discussion, we made a comparison between uncontrolled messaging and ill health. That comparison is neither

unjustified nor exaggerated. And, with a cure at hand, the only question is, why not take it?

In case you still think you avoid the contagion, you can't. Just like any illness, uncontrolled messaging is an equal-opportunity threat. Remember, people discriminate; messages do not.