



Recruiting *Entrepreneur*

ADDRESSING THE UNIQUE NEEDS OF SENIOR LEVEL EXECUTIVE
RECRUITERS AND EXECUTIVE SEARCH FIRM OPERATIONS

special security issue

INSTANT MESSAGING AMONG EMPLOYEES

When installing AOL Instant Messaging (AIM) the terms of service agreement gives AOL the right to "reproduce, display, perform, distribute, adapt and promote" all content distributed across the chat network by users. "You waive any right to privacy. You waive any right to inspect or approve uses of the content or to be compensated for any such uses," according to the AIM terms-of-service. Although the user will retain ownership of the content passed through the AIM network, the terms give AOL ownership of "all right, title and interest in any compilation, collective work or other derivative work created by AOL using or incorporating this [user] content. "In addition, by posting content on an AIM Product, you grant AOL, its parent, affiliates, subsidiaries, assigns, agents and licensees the irrevocable, perpetual, worldwide right to reproduce, display, perform, distribute, adapt and promote this content in any medium," it added.

"They're encouraging businesses to use AIM to discuss details of their business correspondence, even to sync their Outlook contact and calendar files, which, according to their TOS, AOL then has the right to publish in any way they see fit, including, among other things, providing that information to business competitors. I'd be pretty damn leery of using AIM@Work for any kind of business," said Ben Stanfield, executive editor and founder of MacSlash, Inc.

Greater than 90 percent of IM usage is still occurring over consumer services like AOL, MSN and Yahoo. This grassroots adoption has created a pipe between the corporate network and the outside world. IM is downloaded by consumers, so it is difficult for IT administrators, compliance officers, or anyone else who is worried about data leakage or

confidential information leaving an organization to monitor. There are a lot of lessons to be learned from e-mail with regard to setting policies.

For small firms, using an affordable consolidated hosting solution for email, WAN, and a private IM will help by allowing you to monitor and capture communications instead of AOL AIM and others. Educate employees on the approved use of IM in the workplace and let them know IM usage, like e-mail usage, is monitored. The message is clear: Even though you installed a rogue consumer IM product you are still using corporate assets, and corporate policies apply.

When crafting policy in and around IM, organizations should start by recognizing the gravity of the topic, said Ed Moyle, a manager with CTG's Information Security Practice. IM should be approached with the understanding that it's a full-fledged communications tool. Just like any communications tool, IM technology can be dangerous if used inappropriately. Moyle points to the public embarrassment of eFront in relation to its CEO's ICQ logs that revealed the struggles of coping with a corporate shakeout in 2001. The logs were stolen from a PC used by eFront CEO Sam Jain. The public display of his explosive discussions about business partners, employees and others were a nightmare for Jain and the company. "IM technology used in an inappropriate way can have a direct and negative impact to the firm. And it goes without saying that IM can also be a vector for the same threats as other communication channels: loss of intellectual property, inappropriate discourse, malware and loss of employee efficiency," Moyle said. Some enterprises have chosen to extend corporate "acceptable use of electronic communications" policy to cover IM as well as e-mail. Others have elected to prohibit IM

technology altogether. Still others have elected to create new IM-centric policies.

IM is a somewhat different animal from e-mail. Sure, it's all digital communications, but those digital communications don't travel through cyberspace the same way. E-mail goes through the corporate server. Consumer IM applications do not. Regardless of the specific approach selected, analysts said it is important to realize that technical enforcement of that policy can be difficult to implement.

One approach Moyle is seeing more often is the use of an officially sanctioned internal IM infrastructure that allows IM communications while retaining some measure of control over how the technology is used. "By hosting the entire infrastructure within the firm, they can archive, filter and monitor the traffic as fits the needs of their business," he said. For search firms, a hosted solution such as Prospect City's combination of email, Jabber and even VoIP phones can create a private environment where all communications are filtered and controlled by the search firm, who can then create and enforce a corporate policy for all communications. "The IM Manager allows companies to scan IM traffic for certain keywords, keep records of conversations and also put disclaimers in the conversation that pop up to notify the user that the messages are being monitored," Sakoda said. "This works with the policy and puts IM usage on the corporate radar screen. Employees can no longer communicate below the radar."

With the Radicati Group predicting corporate IM usage will grow in the coming years -- worldwide IM revenue is expected to grow from \$142 million in 2005 to \$365 million by 2009 -- analysts said the time to implement IM policies and technologies to monitor enforcement is now.

Email: Legal and Confidentiality Disclaimers

Many email exchanges in the executive search industry include tagline disclaimers warning users of the confidential nature of the email, the rights, ownership and a requirement to destroy misdirected emails. Do they actually have any teeth?

If you're like me, you routinely ignore the email disclaimers that many messages seem to have attached to them. I'd more or less accepted that some used them, while others didn't – but paid little mind to the question – do email disclaimers matter? Turns out they can be used for a whole list of things – but in the search industry, the most common are those that guarantee the privacy and confidentiality of documents. They usually look something like this:

This email and any files transmitted with it are intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.

With the prevalence of e-mail communication, statements like these have become more and more ubiquitous among private and public companies – many are automatically generated whenever a user sends out any information regardless of the content of the message.

If you are concerned about the privacy and confidentiality of your

email, we offer some ideas.

People and Policies

One of the best methods for protecting information is to establish and effectively communicate expectations for proper use of email (if you need some help learning how to communicate policies more effectively – pick up the phone and call someone).

Every organization should put in place a company policy with regards to sending confidential information through e-mail. This could range from a “no forwarding” policy to restrictions on what information can and cannot be sent. Clear guidelines within an organization can provide directions for individuals to understand the proper use of e-mail and decrease disclosure of sensitive information.

Location, Location, Location

If you're convinced that you need to continue to use a disclaimer, then you might consider where you place it. Arguments have been posed that by placing the disclaimer at the bottom of the e-mail, the user is undermining the enforceability of the disclaimer.

Think about it - how can you comply with a disclaimer after

having read the content of the e-mail? As a result, there are some who advocate (albeit annoying for those who rely on email) that the disclaimer appear at the top of the e-mail. This option is known as the “envelope within an envelope” approach. The confidential information is sent as an attachment and the text of the e-mail only contains the actual language of the disclaimer. While this does not guarantee that the recipient will not open the attachment, it could provide some greater standing in litigation if disclosure does occur. Such evidence would be relevant into providing proof that the sender took reasonable measures to ensure the confidentiality of documents.

Currently, there is little case law or statutory interpretation that discusses the legal rights of senders vis-à-vis e-mail disclaimers. With the prevalence of internet use, it is understandable that individuals would attempt to ensure some level of privacy when sending e-mails. Unfortunately, the law today does not provide protection for the misuse of confidential information sent over the internet regardless of a written disclaimer. Companies and individuals need to determine, on their own, the risk of disclosure and how to best protect their privacy.

Database Security

In executive search, your database often extends outside your primary company database to include MS Outlook (contacts, email, calendar, etc.) or Exchange Server, your computer (documents, software, etc.) and your mobile device (replicated contacts, calendar, email, phone directory, etc.). This is a lot of data to be concerned about. A single, automated backup program can manage backing up your computer on a regular basis – even the simple software that comes with MS Windows will handle it. However, for those with servers holding MS Exchange, Cluen's Encore or Dillistone's File Finder, who's backing up – how often – and where?

For small businesses such as boutique search firms, remember: most data loss is the result of theft, not hacking. So what if a thief stole your equipment or it was lost in a fire? If you don't have a simple easy answer, you need to create a disaster recovery plan. The plan should not only cover what's being done to protect and replicate your data, it should also include what to do when equipment is stolen, lost or fails. Keep the plan in a safe location accessible by all employees. If you don't have an externally hosted database, talk to your vendor about how you can best safeguard your system.

Security Tips

RESEARCH



Regularly change the passwords for your online research resources. It may seem harmless if someone else gains access to your OneSource account, but consider that any user who logs in is assuming your identity. The systems assume it's you and allow you access to important account information that may include your credit card number, for example. In addition, these users may have the ability to add new users or change the status of your account.

TECHNOLOGY



The most common security breach in small business is not a hacked network or a compromised password. It's equipment theft. While in the office, take a look around your area and inventory the items, which if stolen, would hurt you and your business. PDAs/Blackberries/Mobile phones, memory sticks (cameras, for example), computers, external drives, CDs, etc. should be on your list. Back it up frequently, but first, learn to store it out of plain site.

ACCOUNTING



As a search firm owner, accounting information is usually on the top of your priority list for security. Backups are important and in many cases somewhat automated by the accounting program – in the form of reminders, for example. However, users often default to backing up in another location on their computer or drive. The best option for backing up any data is to get it off site. Having data stored or replicated in multiple locations is an ideal protection for small businesses. Many online solutions exist, including XDrive, etc.



Recruiting Entrepreneur
Questions or comments?
rcruz@recruitingentrepreneur.com