



EContent™

This article is reprinted with permission from *EContent magazine*, June 2009. © Online, a division of Information Today, Inc.

Marji McClure

Creating Safe, Collaborative Cultures in a Web 2.0 World

Social networking sites and online collaboration tools make it easier for employees to collaborate and share their knowledge. Add email and instant messaging (IM) to the mix and the result is a knowledge-sharing system that can bolster communication and productivity throughout an enterprise.

“You now have a variety of available technologies that allow you to create applications and content,” says Joseph Feiman, VP and Gartner Fellow at research firm Gartner, Inc. “For the first time, individuals are able to create their own applications, even if they’re not application developers. They create their own content, their own websites, and they can express themselves.”

While this is good news for employees, it can mean bad news for companies. While employees are creating this content and expressing themselves in a variety of social media and messaging applications, the truth is that they are also sharing this company-centric content with entities that aren’t on the payroll; entities that can be dangerous enough to lead to an organization’s downfall.

“What’s happened is that the tools that companies use today to be productive, to collaborate, and to communicate are not just within a corporate firewall, they are often out there on the web,” says Ed Brice, SVP of worldwide marketing for security software solution provider Lumension. “They are browser-based types of applications. We also have this emergence of social communities where people are sharing information, collaborating with each other, and this is also outside of the corporate firewall. As such, they’ve become a very ripe environment for cyber criminals to exploit.”

It usually starts innocently enough. Mark Thompson, VP of product management of Verdasys, a data risk management solution provider, recalls how a client employed an individual who wanted to use Google Calendar. “They were just going to use it for this one group and they were just going to post group activities and no proprietary data was going to get posted into it,” says Thompson. “They actually thought about it before they started it, but within 2 weeks after they started using it, the security guys looked through it and what did they find? Attachments added to those calendar entries that had proprietary data that shouldn’t have been there.”

Through a combination of social networking sites, instant messaging, and even email, companies and their employees can easily leak valuable proprietary content to external



sources—and not even realize it. “People are using calendars that are available to everyone. It’s pretty dangerous,” says Feiman. “People believe that if it’s their information, it belongs to them. Wrong. On the web, whatever you’ve posted, it doesn’t belong to you anymore.”

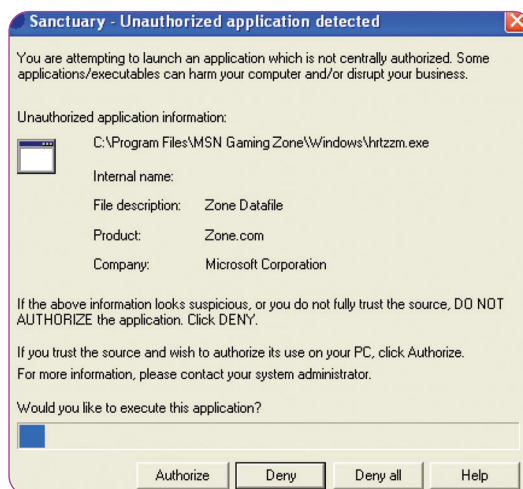
Right or not, information can be taken and used by anyone who can find it, including computer hackers who seek to cause harm to organizations. Feiman explains how hackers can take bits of information from these sources and wreak havoc. “They get a piece of information by intercepting some IM that your enterprise is planning to have a board of directors meeting. Then by intercepting an email, they understand that your enterprise is working on some innovative product. Then you’ve published through Google Calendar where that board of directors meeting takes place. Putting all of this together, they’re coming to a pretty correct conclusion that you’re about to announce your new innovative product on such and such date. Then they buy your stock at a lower price.”

This may seem like an extreme scenario, but it illustrates the seriousness of breaches that can be caused by today’s online collaborative work environments.

INTERNAL AND EXTERNAL THREATS

Most security solutions available in the market today focus on two main objectives: preventing security breaches with an organization’s invaluable content and educating employees in the process. These solutions monitor and block compromising activity from external and internal sources and educate individuals on proper behavior regarding transmitting content across Web 2.0 channels.

While hackers remain a prominent threat and require companies to track exactly where their data is going, it seems that lately almost as much attention is being paid to who is sending the information out. With today’s struggling economy leading to massive layoffs, organizations are becoming more aware



Lumension clients can help prevent employees from launching a potentially harmful application by presenting them with a visual warning that their behavior may cause harm.

their applications, notes Feiman. “Whoever you are, you should be applying these security procedures and technologies,” he says. “These technologies allow you to analyze your code when you program it and detect potential security vulnerabilities.”

There are also technologies that can monitor, control, and prevent leaks to prevent employees from revealing vital company information through email and instant messaging, adds Feiman. “You can set up those technologies in such a way that they can listen and monitor all IPs and see if there is sensitive information there and they can block certain information,” he says. “Preventing, monitoring, termination—that’s what is being used. You can analyze source code to prevent potential vulnerabilities. You can monitor activities that are going on today. You can harden your code to make it more secure. You can harden your content to make it more secure.”

Essentially, these technology solutions help bring the control of content back to the enterprise. Lumension offers a solution that begins with vulnerability assessment. “We scan your entire network environment and identify where you don’t have the latest application patches and help you take inventory of what’s on your network, and as software developers release patches, we take those patches and we automate the delivery into the parts of your network that are not patched,” says Brice.

Lumension also offers endpoint security protection—which allows organizations to identify what they want to run on their networks and halt what they don’t—and data protection. Lumension can automatically encrypt files and prevent malware from being added to a client’s operating system.

With its data leakage prevention solutions that comprise its Fidelis XPS

of the threat of content security breaches posed by disgruntled soon-to-be ex-employees. “It’s of tremendous concern to companies,” says Chris Bradley, VP of marketing and business development at MessageGate, Inc., an email governance software and services provider. “There are a lot of emotions and hurt feelings and people trying to take care of themselves, understandably, and it can lead to tremendous risk and exposure by the organization.”

However, Bradley and other content security solution providers agree that most employee offenses related to content security are done without malicious intent. Often an employee is just performing assigned job duties and is unaware that his or her behavior is putting company data at risk. Thompson tells the story of a client’s employee who was uploading source code to his Gmail account at 2 a.m. “He was a software developer working late, and he shipped the source code to himself at home so he could continue working,” says Thompson. “He just wasn’t thinking about the fact that it was a huge risk.”

KNOWLEDGE IS POWER

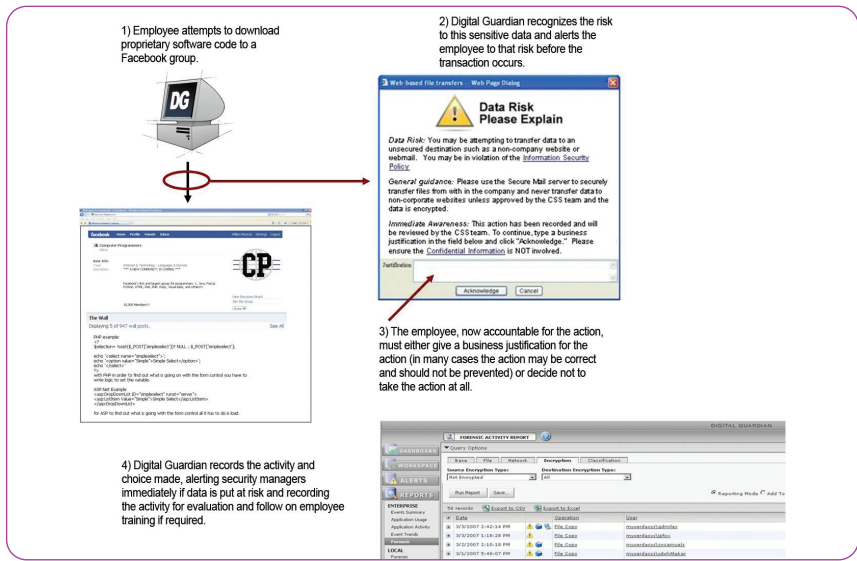
Regardless of where a threat originates, be it inside or outside of an organization, and from which particular channel it comes (anything from social networking applications to email), there are many technological offerings available to help organizations secure

Verdasys reports, which are available through the Digital Guardian product, enable clients to gain a clear view of who within their organization is accessing what data.

product, Fidelis Security Systems, Inc. is able to look at content and its context and determine appropriate use, explains David Etue, VP of product management for Fidelis Security Systems. “Data loss prevention gives you the controls of making sure your information doesn’t get shared improperly,” says Etue. “Ultimately, it comes down to understanding your information and how it should and shouldn’t be shared and providing people with the right tools to make that happen.”

Verdasys offers data risk management solutions through its Digital Guardian suite of products that monitor and track data use. The software can track who within an organization is accessing data and how the data is being used. Thompson explains that the software agent resides on the desktop or laptop and reports to a central administration server that reports and monitors the health of the agent. “It monitors everything on that machine—network traffic, email traffic—and it can look for data,” says Thompson. “We provide an audit trail of who’s handled that data so you can show that people who were restricted from it didn’t get to it.”

DataMotion, Inc., a provider of hosted governance services for data integration and collaboration, provides its clients with a platform that tracks data that is transferred via email and adds governance to the process, according to Patty Dock, DataMotion’s COO. “We add security and tracking and the visibility to where those files go,” she explains. “We set it up with them so when someone needs to send those files, we have tracking of where they email those files, visibility to who opens any of those files, and the tracking and monitoring of anybody who ever opens the file, looks at it, reads it.



“The people who are using it are getting a single view of where the information is going,” adds Dock. “It’s the difference between sending your package from the post office or FedEx. It’s the ability to track the information.”

AN EDUCATIONAL TOOL

Along with systems that enable clients to more easily track and monitor their data as it moves through social networking channels and email, content security vendors also offer features that are designed to prevent breaches going forward. This involves the component that informs employees about proper data sharing in the Web 2.0 environment.

“It’s about educating the employee at the time [of the action],” says Thompson. He provides an example: If an employee’s browser is on one of the social networking sites and he or she is about to copy company information onto the page, the Verdasys system will generate a pop-up box written by the client company that tells the employee why such an action isn’t appropriate and suggests the data be sent through another channel. “Many of our customers use those prompts in a soft mode, so it’s just informing the employee. But they get 80% to 90% compliance,” says Thompson. “Most people want to do the right thing. Intervening at the moment when they were going to do it, you’re giving them the perfect education. Without interfering with the business at all, you can get rid of 80% to 90% of the risks that you can identify of data moving in inappropriate ways out of the company.”

MessageGate’s solution enables companies to create policies that can evaluate an email flow in real time. “The policies look at both

Employees of Verdasys clients are notified via a pop-up box when they attempt to transfer company data to an unsecure location. They are provided with suggestions of how to utilize the data in a secure manner.



MessageGate's solution enables clients to create policies around their data to ensure its security.

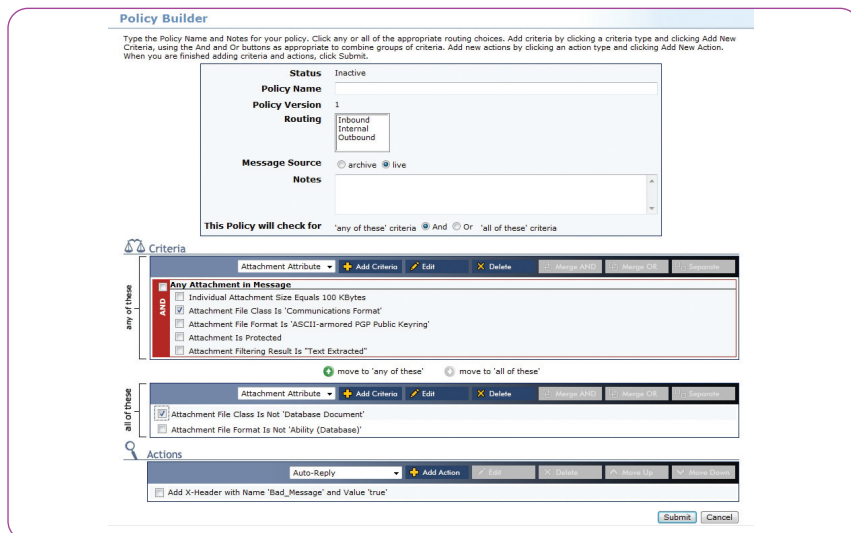
content in the metadata around the email—in the body itself or in the attachment—in context, who is sending to whom and who belongs to what privileged groups or communications,” explains Bradley. The technology “can make decisions based on those policies as to whether or not the email should be blocked, whether or not it should be sent back to the sender, or sent to a third party for review.”

MessageGate offers a feature called “sender confirm.” When there is a violation, such as a social security number being sent from one professional to another to help complete a business transaction, the system can halt the message. “It goes back to the sender and says, ‘This is the policy that this communication violated. Are you really sure you want to send it?’ It can not only be self-corrected, but it’s an educational opportunity,” says Bradley.

According to Bradley, the product comes with predefined policies, but it is designed for companies to create their own policies. “What we find is most of the time, canned policies don’t address what companies are looking to do,” he says. “They want it tailored to their environment and their own use case.”

CREATING A SAFER ENVIRONMENT

There’s no question that the issue of content security is at the top of minds throughout the enterprise, not just the IT department. Security vendors say that in addition to meeting with IT professionals at their client companies (mainly because of IT’s involvement in technological



implementations), they are also working with senior-level leadership in other segments of the business. MessageGate’s Bradley notes that it is a cross-functional sell and that sometimes MessageGate will begin a client engagement with an organization’s corporate compliance officer or HR professional.

Dock says that DataMotion used to communicate with the IT professionals, but “it’s moving from IT people to business people. Today we’ve found it’s the business person with a very specific problem,” she says. “They have a driving need to solve a specific business problem. We used to have to go out and explain that governance is needed. People now know they need the governance and the visibility.”

Still, Verdasys’ Thompson says that the list of problems potential customers come to the company for is different from what problems are actually solved. But regardless of what brings customers to content security solution providers, they seem increasingly dedicated to provide financial resources for such initiatives. “In the past couple of years, companies have changed their security budgets to where DLP and encryption are actual line items,” says Etue. Whereas 3 or 4 years ago, it was a “nice to have” feature, it is becoming a requirement.

“Policy is not just a matter of creating these filters. It has to be tied to a coherent policy about proper usage of corporate resources, particularly email,” says Bradley. “If it’s not in place already, we encourage companies to make sure there is a coherent published policy that employees can understand. It’s an expression of culture. That’s an easy tie to this idea of a culture of compliance. You want your employees to be productive and creative, but they need to comply with corporate policies, outside regulations, and good legal practices.”

Companies will most likely have to continue to adapt their policies as new applications are created; something technology providers are ready for. “One of the things we do self-consciously with Digital Guardian is we try to future-proof it,” says Thompson. “You can never be perfect at that. But whatever next year’s risk is and whatever the new Twitter is ... we try to design against that so that the worst case for our customers is they need to take an upgrade to be able to secure that.”

MARJI MCCLURE (MARJIMCCLURE@SBCGLOBAL.NET) IS A FREELANCE WRITER BASED IN CONNECTICUT. **COMMENTS?** EMAIL LETTERS TO THE EDITOR TO ECLETTERS@INFOTODAY.COM.

Companies Featured in This Article

- | | |
|---|--|
| DataMotion, Inc.
www.datamotion.com | Lumension
www.lumension.com |
| Fidelis Security Systems, Inc.
www.fidelissecurity.com | MessageGate, Inc.
www.messagegate.com |
| Gartner, Inc.
www.gartner.com | Verdasys
www.verdasys.com |