



## Spotlight: Trusted Communications

*An exclusive interview with Gartner's Avivah Litan, vice president and research director, with an introduction from Adobe president and chief operating officer, Shantanu Narayen*

### Delivering Trusted Communications

Welcome to Security Matters, the first in a series of online, quarterly analyst insights on document control and security. This series will examine important issues enterprises face today and offer potential solutions that provide safe and trusted communications.

Each day your employees, customers, and partners create, distribute, and receive information electronically and through paper-bound processes. Every minute, documents containing critical information and workflows – your competitive advantage – travel within and outside of your enterprise. How can you safeguard enterprise communications so they are not compromised, stolen, forged, or maliciously manipulated?

Trusted communication protects the authenticity of a document's origin, the integrity of its content, and the confidentiality of the communication. Most documents do not qualify as trusted communications because not all parties are confident of the document's point of origin or are certain that information provided online or offline is sent only to intended recipients. Without secure communications, your enterprise could miss business and revenue opportunities and experience loss of brand equity.

The Adobe legacy has been built around helping organizations deliver visually rich and secure communications. We have now become a leader in developing new security technology for today's enterprise communications – whether published stock reports, government hearing transcripts, loan applications, or case management forms. Adobe security solutions help protect intellectual property, safeguard the privacy of customer data, and meet corporate and government regulations.

Today's spotlight interview on trusted communications features commentary from Gartner Research director and vice president, Avivah Litan, an expert in security solutions for the business-to-consumer and business-to-business markets.

We hope this information proves useful in determining how your enterprise can take advantage of today's solutions to better secure and control your documents and paper-bound processes. We invite you to visit [www.adobe.com/security](http://www.adobe.com/security) to continue your research.

Thank you for your interest in Adobe's document control and security solutions, an important document service built on the Intelligent Document Platform.

*Source: Adobe*

### ISSUE 1

#### IN THIS ISSUE

- ▶ Spotlight: Trusted Communications
- ▶ Exclusive Interview with Gartner Analyst Avivah Litan
- ▶ In Closing

[www.adobe.com](http://www.adobe.com)

**Gartner**

## Exclusive Interview with Gartner Analyst Avivah Litan



*Avivah Litan is a vice president and research director in Gartner Research. Her area of expertise includes emerging payment applications and financial flows for the business-to-consumer and business-to-business markets.*

*Prior to joining Gartner, Ms. Litan worked as a director of financial systems at the World Bank, where she managed its multicurrency disbursement, financial, accounting, and Web-enabled global information systems for borrowers in more than eighty countries. Concurrently, she worked as a journalist and as a weekly computer columnist for the Washington Times.*

*Ms. Litan earned a master of science degree from the Massachusetts Institute of Technology. She also graduated from an executive education course at the Harvard Business School while working at the World Bank.*

### Why is the issue of secure communications important to enterprises? What has caused the change?

There is a rapidly escalating need to transmit sensitive customer communications in a more secure fashion than is commonly done today. For good reasons, consumers and other types of customers are becoming increasingly suspicious of emails that land in their in-box, especially those asking them to update or retrieve information by going to Web sites referenced through embedded URL links in the emails. Many such emails are actually phishing attacks or other types of cybercams that are intended to trick email recipients into divulging sensitive information that is later used for identity theft related fraud.

The rapid proliferation of cyberattacks through email threatens the online channel because consumers and other end-users are beginning to rightly lose confidence in the integrity of the channel.

It is, therefore, important for enterprises to secure electronic communications with their customers. By protecting online customer communications, enterprises can ensure that they can continue taking advantage of significant process improvements and cost reductions enabled through electronic communications. In some cases, they also need to make sure that documents they send customers maintain their authenticity and are not tampered with by any third party. This will prevent the proliferation of fraud committed through false or forged communications.

### Who is hurt or affected when communications trust is broken?

Many parties in the chain are hurt or affected when trust in electronic communications is broken. First, it hurts consumers because they lose confidence in email communications and their ability to conduct secure online commerce. In worse-case scenarios, consumers who fall victim to identity theft fraud as a result of responding to fraudulent emails can face the very difficult, lengthy, and daunting task of repairing damage done to their credit history and/or finances.

Consumers suffer numerous losses, first from loss of confidence, and second due to several types of identity theft fraud that may result from insecure communications. An equally big hit is incurred by enterprises servicing consumers, such as financial institutions who have to respond to consumer inquiries and undergo costly cybercrime investigations. Oftentimes, they must refund customers' money as a result of phishing attacks, or other cybercrimes committed through insecure communications.

Broken trust in electronic communications also hurts online consumer service providers like AOL, eBay, or Paypal because customers become wary of engaging in email or other online communications with them. Online providers are able to maximize revenues and lower customer interaction costs through the electronic medium. Broken confidence undermines their ability to achieve these goals, and also results in high customer service costs incurred as a result of customer calls and emails to the customer service desk.

For example, banks use email communications and electronic document delivery to reduce their volume of outbound paper statements, and are able to achieve significant cost savings by replacing hardcopy with electronic statements. They also leverage email as an online marketing tool by sending consumers highly targeted messages that can be quickly adjusted to meet market demands and responsiveness. This is a much easier task to accomplish through online communications than it is through processes that depend on paper mail, where it is much more costly and impractical to deliver agile and highly segmented marketing campaigns.

Banks and other service providers can launch online targeted promotional offers, and see how consumers respond to that marketing by monitoring who reads the email, who responds to the ad in the email, and who buys the products and services that are advertised. With electronic online processes, they can quickly adjust their marketing campaigns if they discover they are not achieving the results envisioned. This flexibility and ability to quickly fine-tune campaigns is not possible in the offline paper world. Broken trust in online communications hurts enterprises in many different aspects, both in their ability to reduce costs, and to gain new revenues through marketing campaigns and cross-sale activities.

### **How large is the problem of compromised communications, and how does it play a role in phishing identify theft and document forgery?**

The problem of compromised communications is large; consumers are becoming highly suspicious of their emails for good reason. According to a survey we did last spring, in the past year over 40 percent of online U.S. adults, or an estimated 57 million people, say they received an email phishing attack, or what looked like an email phishing attack. I am sure this number is even higher now.

In fact, 57 million affected adults, even at the time of the survey, is probably an understatement of the magnitude of the situation, because many consumers do not recognize phishing attack emails for what they are. I would venture to say that probably 80 to 90 percent of all email users have gotten one of these phishing attack emails because there just are not very many domains and users that are spared from them. So the problem of compromised communications is huge.

Most of these attacks happened in the last six months preceding the survey, and about 92 percent of the attacks occurred in the year before the survey. That means phishing attacks are a relatively new phenomenon, even though they have been around for a few years. It is only in the last year and a half

that we have seen the rapid proliferation across the Internet; hence, there is more urgency than ever to secure our online communications and the Internet channel.

According to the Gartner survey, about 80 percent of online consumers conduct some sort of financial transaction online. Of this transactor group, 58 percent are either “extremely concerned” or “very concerned” about the security of the financial and personal information that is stored online.

Consumers have good reason to be nervous. About 3 percent of those who think or were sure they received a phishing attack email actually recall giving sensitive information – such as bank account number, credit card number, user ID and password, etc., – away to a spoof site or imposter. It is likely that this number is even higher than 3 percent because many consumers who are duped into giving information away do not realize what they have done. And the 3 percent of the population who recalled giving sensitive information away were about three times more likely to have fraud committed against them in the year preceding the survey than did the average online user.

We are not just talking about perceptions. We are talking about actual losses taking place against consumers who have received these imposter emails. The problem is escalating, and is threatening the use of the online channel.

Electronic document forgery is also becoming a bigger problem. We have several examples out there of fake press releases having either falsely driven up or driven down the market value of company stock. Three cases in point were:

- PairGain – a forged press release caused the company stock to go up thirty-one percent.<sup>1</sup>
- Emulex – a fake press release caused the market value of the company to plunge by \$2.5 billion dollars.<sup>2</sup>
- Parmalat – probably most people recall this December, 2003 scandal that turned into a full blown crisis for Bank of America because of forged documents purporting to have billions of dollars worth of cash in a Bank of America account in the Cayman Islands.<sup>3</sup>

We have seen hard examples of forged press releases and documents that have rocked the financial status of companies, and we will likely witness more of these in the future.

---

<sup>1</sup>CNET.com, D. Goodwin, 15 April 1999.

<sup>2</sup>CNET.com, C. Grice and S. Arnd, 25 August 2000.

<sup>3</sup>The UK Guardian, M. Tran, 23 December 2003.

## **What are the hard and soft costs implications to organizations when trust in their communication is broken?**

There are many different types of costs to organizations when trust in online communications with their customers is broken. As stated previously, in the case of phishing attacks, victims are about three times

more likely to suffer from identity theft fraud than non-phishing attack victims. In the year ending May 2004, when our last survey was done, those victims had lost about \$1.2 billion in some type of identity theft fraud.

There is also an increase in customer service costs associated with increased call volume. For example, when phishing attacks are launched against a bank, the bank's customers and employees will phone in to the call center to ask about the disturbing emails. I have heard reports of bank call centers receiving hundreds of calls a day during a phishing attack. Depending on the nature of the customer interaction, each call can cost anywhere from \$4 up to \$10 to handle. Call center calls, where customers talk to a customer service representative, are expensive. Financial institutions and other large customer-facing companies like EBay and Paypal are seeing a substantial rise in customer service costs because consumers are getting nervous about what is landing in their email boxes or what they are experiencing on various Web sites they are directed to.

There is also the cost of not being able to do business on the Internet the way many enterprises planned for. For example, there are many banks and billers, including telecommunication, credit card, insurance, and utility companies who send statements and bills to customers electronically, in order to significantly reduce many of their operational costs. According to a Gartner survey of major U.S. consumer billing companies, a typical firm can save \$15 million a year if all their consumer bills are delivered over the Web. The average company in this case sends out about 1.92 million bills a month. Producing and sending a paper bill costs a typical company \$1.10, while the Internet version costs 44¢.

In addition, moving customer service phone calls to Web self-service results in very substantial cost savings. A typical consumer biller, for example, can save \$7.3 million a year if all their customers' service calls are moved to the Web self-service channel. The average enterprise surveyed by Gartner receives 1.7 million calls a year at its call center, and each call costs that company \$4.50, as opposed to 10¢ for each Internet self-service incident. Some companies, especially credit card issuers, receive 12 times more calls, and can, therefore, save 12 times as much.

More than one-third of the calls coming in to a call center concern invoices, and there are many opportunities for cost savings when those are sent out electronically and customers can answer their own invoice-related questions through the online channel.

It is also possible to automate invoice dispute functions as part of sending out paper electronic bills, as opposed to paper bills. There is a great deal of achievable savings in this category as well. The average large U.S. biller company surveyed by Gartner can save \$3.72 million by enabling the resolution of customer invoice disputes through email and online communications, as opposed to having to use paper-based or telephone communications.

Furthermore, consumers may lose trust in the brand they are dealing with as a result of compromised communications. Consumers who witness or hear of a lot of phishing attacks or other online scams involving their bank, for example, may start wondering if they should move their money to

another bank. False communications damage brand equity and hard-earned corporate identities and images.

## **What can recipients look for in an electronic document in order to trust the source?**

Recipients need to be trained and educated on what to look for in order to trust the source of an electronic document they receive. There are different methods enterprises can use to convey to users that a document can be trusted. One such method is making an email look a little different in an inbox; for example, putting a little lock on the email that tells the user it is a securely signed email. The email title can also have a different color code or another predetermined indicator that symbolizes a digitally signed document.

Different methods and protocols, like a gold lock at the bottom of a browser window, have evolved over the years to indicate to consumers that they are engaged in secure communications. Since the market still does not have that much volume of secure communications, the methods of conveying the security of communications and documents are still not standardized. Eventually the market will likely settle on a couple of seals that tell consumers, "You can trust this document." In the meantime, enterprises must communicate to their customers how they let them know if the documents and messages they send them are indeed secure.

## **What types of solutions exist today (protection and detection) so that organizations do not fall victim to cybercrime?**

Many types of solutions exist today to insure that organizations do not fall victim to cybercrimes, and security solutions exist at many different levels. Let's discuss two broad categories of security solutions; (1) those that apply at the network and enterprise level, and (2) solutions that apply at the document level.

First, an enterprise must adopt sound holistic security practices. For example, they should encrypt data where possible, keep intruders out of their network, manage access to enterprise data and files, encrypt transmission of sensitive data, and employ back-end fraud detection software that prevents account takeover. This latter measure is particularly important because in the end, if all else fails and the crooks get into customer accounts, the enterprise needs to make sure they are unable to steal funds or information out of them. Enterprises also require email and content filtering solutions so that they prevent "bad" or malicious content from getting to customers and/or employees. There are also Web site analysis solutions that watch for suspicious activity on enterprise Web sites.

There are all types of front-end customer authentication solutions that provide more security than simple passwords do, ranging from software based challenge/response systems to hard tokens. Enterprises need to apply layers of security appropriately. For example, a bank may require a

simple password to log into their Web site in order to check the status of a service request, and at the same time may require smart-card access to transfer more than \$1,000 out of a bank account.

There are different solutions that enterprises can distribute to their customers' desktops to ensure they are not running malicious spyware or viruses, at least while they are communicating with the enterprise. There are also enterprise brand protection solutions including services that scan the Web to monitor abuse of domain names. There are many different types of solutions to minimize online crime, and an enterprise has to put up as many walls as possible to keep out the crooks.

In addition to network and enterprise level security solutions, there are also solutions that provide security at the data and/or document level. As noted, enterprises must apply many security layers around an application, but it is also important to provide added protections at the most granular level for the most sensitive information. That is usually performed at the data or document level.

Protecting the physical perimeter of an enterprise is important to ensure employee safety and security, but with regard to information security, this perimeter is becoming less relevant due to the proliferation of mobile and remote workers. The network perimeter is porous and becoming a significant barrier to business processes as the need for collaboration with non-employees rapidly increases and the corporate firewall migrates to the user desktop. The application perimeter has become one of the last defensible outposts in the information security perimeter and the current focus of most attacks. The data/document perimeter is one of the final frontiers. Creating a secure container for electronic documents will help ensure information security that is as portable and persistent as the documents themselves.

### **How can customers and others outside the firewall trust communications such as press releases, financial filing, and email?**

It is imperative that enterprises refrain from forcing customers to buy new software, or doing anything out of the ordinary that deviates from what they would usually do. End-user security has to be made very intuitive and very simple to use. Consumers should not be expected to read a manual to figure out what to do. At the same time, enterprises have to be able to easily communicate to their customers that they are transmitting a secure document or form to them.

Some kind of easy-to-understand seal or icon must tell the customer, "If you see this seal, you can be sure that this is a secure document. It is coming from who you think it is coming from, and we also know you are who you say you are." This latter function is also known as two-way or mutual authentication, which is becoming increasingly important in light of the plethora of phishing attacks.

## When a customer submits a form online, how do they know the information is being captured correctly, and by the desired destination?

When customers submit forms online, or interact with a Web site, they must have some kind of sign saying, "This Web site is really the site you think it is." An enterprise must authenticate itself to its customers, as well as enable its customers to authenticate themselves in turn. As discussed above, some kind of indicator is required. There may be a picture, perhaps, that has been pre-selected by the customer so the enterprise can essentially say upon user log-in, "Here, you logged in, you gave us your user ID, and now we will show you this picture that only you know about. This tells you it is us." In this example, no one else besides the enterprise has access to that picture or symbol, which would have been pre-selected by the user when the user enrolled with the service provider or enterprise.

Enterprises can also use other prearranged indicators at the document level, such as a sign for a digitally signed document that is impossible to tamper with. In this manner, the recipient of the document knows that the document originated from the stated enterprise, and not from a fraudster who somehow intercepted the communications.

Enterprises must come up with some method of authenticating themselves and their documents to their customers, and that method preferably should be a visual graphic. Still other types of text-based systems can also be used; they are just harder for users to remember or work with. There are many different methods that can be used for service and customer authentication, and the overriding rule is to keep the customer's interface simple and intuitive.

It is also especially useful for a third party to provide validation of a sender (or the enterprise) for the customers. Likewise, it is useful for a third party to validate a user's identity and to financially back up the assertion of identity, so that if there is fraud committed, the identity validator is liable in most circumstances. These types of solutions will start to evolve, and secure document exchange is likely to be a key catalyst in this evolution.

*Source: Gartner*

## In Closing

Security matters. Enterprises cannot afford to gamble with the contents and privacy of their employee, customer, and partner communications. Documents and paper-bound processes with the appropriate security and controls enhance business opportunities and mitigate risks.

Adobe's document control and security solutions help organizations protect the authenticity of a document, the integrity of its content, and the confidentiality of the communication. Using these solutions, organizations can apply digital signatures to Adobe PDF files, publish certified documents, and add controls that expressly define who can open, view, print, copy, or modify a document.

We hope you enjoyed the first edition of *Security Matters*. We look forward to sharing future editions throughout the year, including spotlights on:

- Risk management and regulatory compliance
- Digital signatures
- Secure statement delivery

If you have suggestions or comments about *Security Matters*, please e-mail them to [securitymatters@adobe.com](mailto:securitymatters@adobe.com).

For more information about Adobe's document control and security solutions, please visit [www.adobe.com/security](http://www.adobe.com/security). For an up-to-date listing of local and international security-related events, please visit [www.adobe.com/securityevents](http://www.adobe.com/securityevents).

---

*Security Matters* is published by Adobe. Editorial supplied by Adobe is independent of Gartner analysis. All Gartner research is © 2005 by Gartner, Inc. and/or its Affiliates. All rights reserved. All Gartner materials are used with Gartner's permission and in no way does the use or publication of Gartner research indicate Gartner's endorsement of Adobe's products and/or strategies. Reproduction of this publication in any form without prior written permission is forbidden. The information contained herein has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Gartner shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.

© 2005, Adobe Systems Incorporated. All rights reserved. Adobe and the Adobe logo are either registered trademarks or trademarks of Adobe systems Incorporated in the United States and other countries.