# No Hiding in the Cloud:

## THE TELLTALE SIGNATURE OF INEFFICIENT, NONSECURE PROCESSES

As organizations increasingly adopt cloud technology, the chief information security officer (CISO) role is taking on greater prominence as broker across corporate divisions in order to ensure proper due diligence is performed and strong data protections are in effect. As a result, many are turning a critical eye on one particular business process that continues to defy auditing, lacks anti-tampering controls and eschews digital authentication and authorization: the paper-based, "wet-ink" signature.

There's little doubt that cloud technology, or IT delivered as a service, is dramatically transforming traditional business processes. In CIO magazine's "2012 State of the CIO" survey, the cloud was the factor cited most often as influencing the role of the CIO in the next three to five years.

### ✔ SECURE BUSINESS ASSETS IN THE CLOUD

The cloud equation is indeed a strong one. Today, ROI discussions are often centered around what can be more cost-effectively deployed, transitioning previously automated functions "into the cloud" to take

DocuSign®

InfoWorld
Custom Solutions Group

## 2
# No Hiding in the Cloud

"With the increasing demand and expansion of the global role of security, the role of a modern CISO is evolving from simply being a technical officer to a leader in business strategy."

advantage of the cost benefits, flexibility and scalability derived from software-as-a-service (SaaS), infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS)—utilizing technology as a utility.

According to a report earlier this year surveying 554 IT professionals, six out of 10 U.S. companies already have at least one application in the cloud, and 71 percent expect to increase spending on cloud services in the next 12 months.[i] In addition to business continuity, the top business drivers for moving to cloud services are increasing speed of deployment, gaining the flexibility to react to market conditions, and improving customer support.

Yet that same survey indicates significant concerns that putting data in the cloud also carries risks, with 70 percent of the respondents citing security worries as the top barrier to their adoption of cloud computing. Whether implementing services via public cloud, private cloud or a hybrid of both, organizations are relying on some form of shared access beyond the walls of the data center, often intending to increase availability of those resources to mobile users within or outside of the organization.

Already concerned about compliance and security for more traditional IT resources, CIOs, CISOs and CEOs now have to worry about managing risk and building trust within a new computing paradigm that is evolving rapidly and along different lines of deployment. Of paramount importance to these executives advocating a cloud-based approach is the determination that the cloud provider offers the same—if not greater—level of information security as the organization itself. Beyond business efficiency qualifications, the very nature of a CISO's responsibilities is to ensure any selective adoption of cloud service providers meets stringent due diligence and compliance requirements to protect sensitive data and intellectual property.

The forces transforming the delivery of information technology via cloud and to an increasingly diverse array of mobile devices are also transforming the role of the CISO. As Forrester analyst Andrew Rose noted in a recent blog, "Security management now encompasses much more than technology; CISOs can build their reputation and enhance their personal career prospects by talking 'ROI' rather than 'IPS' and influencing their colleagues at the highest levels of the organization."[ii]

IDC senior market analyst Naveen Hegde, reviewing results of an IBM survey of CISOs, came to a similar conclusion: "With the increasing demand and expansion of the global role of security, the role of a modern CISO is evolving from simply being a technical officer to a leader in business strategy."[iii]

One of the key factors in this transformation of the CISO role is the growing requirement for sharing information securely outside of the walls of the enterprise. According to PriceWaterhouseCoopers, "Once seen only as the first step in asset protection, today's security plays a critical role in enabling the exchange of sensitive information with other organizations."[iv]

### ✔ PAPER, PEN AND INK: THE WEAK LINK IN THE SECURITY CHAIN

One of the most persistent forms of exchanging information with other organizations is the written signature. Used for myriad purposes, from legally binding contracts to proposals to finance applications and so on, the "wet-ink" signature is a fundamental business process that

**i** Lauren Brousell, "CIOs Plan to Increase Cloud Spending," March 28, 2012. CIO magazine.

**ii** Andrew Rose, "Go Beyond Technology To Build An Effective Security Practice," July 24, 2012. Forrester Research.

**iii** Naveen Hegde, "IBM Study: Changing Role of CISO, from Technical Officers to Business Strategy Leaders," July 2, 2012. IDC Insights.

**iv** "How to align security with your strategic business objectives," 2005, PriceWaterhouseCoopers LLC.

# 3
# No Hiding in the Cloud

"DocuSign's eSignature services not only allow for secure business transactions to be completed from almost anywhere, they make our sales process more efficient, customer-centric as well as credible."

many organizations are still struggling to automate.

Considering the time involved, and the effort and cost of printing, faxing, scanning and overnighting documents of all types for signature—not to mention the labor-intensive processes of keying and rekeying data—it is remarkable how many of today's highly automated businesses still remain tied to eminently manual methods. Many make significant investments in sales and marketing automation to accelerate the acquisition of new customers and revenue, only to leave the most crucial part of the process—actually gaining a binding customer agreement—completely manual, time-consuming and labor-intensive.

What is more striking, however, is that "wet-ink" signatures and paper-based documents are inherently unsecure. For the most part, both can be duplicated, used by unauthorized parties, and even stolen without anyone realizing it.

Marci McCarthy, president and CEO of T.E.N. and creator of the Information Security Executive® Programs recognizing the contributions of security professionals within organizations, is a proponent of adopting electronic signature for business efficiencies and transaction management within a secure platform service. "DocuSign's eSignature services not only allow for secure business transactions to be completed from almost anywhere, they make our sales process more efficient, customer-centric as well as credible," McCarthy says. "Furthermore, this type of product provides T.E.N. and our customers with a virtual repository that is accessible, auditable and accountable."

An organization's most valuable asset outside of its employees is the intellectual property around the data it transacts, yet transmission of paper documents lacks basic security protections that are routinely applied to electronic data, such as encryption and authentication. So, why has paper-based signing persisted when nearly every business process leading up to and following the signature has changed?

"Signatures remain small, but important, components of myriad business transactions," Gartner Inc. analyst Gregg Kreizman wrote in a 2012 report.[v] "Signature requirements can be found in internal and external interactions, but are most sought as formal components in transactions among parties in different organizations."

While other business processes succumbed to automation, adoption of electronic signatures, or e-signing, lagged behind, for many reasons. Initially, there were legal issues regarding acceptance of digital signatures on filings and contracts, but the European Community in 1999 and the United States in 2000 adopted legislation to ensure legal validity of electronic signatures and electronic documents.

Also, before the Web and cloud, organizations were only able to take advantage of on-premise server-based systems, which were complex and lacked standards for certification, limiting their appeal at many organizations that were already struggling to maintain disparate systems and facing interoperability issues with partners and customers.

## ✔ E-SIGNING COMES OF AGE

Consumer-facing businesses such as lending and insurance have adapted quickly to customers who are increasingly comfortable with and often expect to be able to transact all activity electronically from their desktops, laptops, mobile phones

**v** Gregg Kreizman, "The Electronic Signature Market Is Poised to Take Off," May 21, 2012. Gartner Inc

# 4
# No Hiding in the Cloud

As companies look for innovative ways to increase speed to results, reduce costs and enhance customer engagement, electronic signature has gone from a "nice to have" to a "must have" business imperative.

and tablets. That has dramatically transformed acceptance, adoption and use of e-signing.

Organizations reliant on customer relationship management (CRM) or sales force automation (SFA) systems have come to recognize that e-signing can accelerate the ROI from these systems by shaving days or even weeks of processing time off of orders and contracts that require signatures.

The cloud has dramatically lowered barriers of acceptance. In 2010, DocuSign introduced the Connect API to increase interoperability with key cloud platforms like Force.com, Ruby and PHP, allowing developers to easily and securely create and integrate native applications with the DocuSign electronic signature platform.

As companies look for innovative ways to increase speed to results, reduce costs and enhance customer engagement, electronic signature has gone from a "nice to have" to a "must have" business imperative. High-availability cloud-based service makes documents readily available wherever they need to be accessed from.

But, even when dealing with electronic signatures, it's not enough to proclaim trust, reliability and business efficiency. These factors need to be validated through extensive third-party audits and certification of cloud-based vendors.

To this end, DocuSign strives to ensure that it is the most continually audited and highest certified global eSignature service in order to provide optimum levels of security assurance. DocuSign is the only eSignature service to achieve global ISO/IEC 27001:2005 certification as an information security management system (ISMS). DocuSign is also continually SSAE 16 examined and tested, PCI DSS 2.0 compliant as both a merchant and level-one service provider, TRUSTe certified and a member of the U.S. Department of Commerce Safe Harbor.

## ✔ WHY E-SIGNING IS A BETTER SOLUTION

Whether it's sales teams closing more deals, banks and credit unions processing more loans, insurance providers and agents accelerating the speed to coverage for clients, or healthcare companies getting patients the care they need more quickly, e-signing is helping companies transform their processes, automate workflows and accelerate transactions to do business faster and better —all while delighting customers and reducing costs.[vi]

In an assessment of DocuSign's electronic signature platform, Nucleus Research identified key benefits of utilizing DocuSign, including accelerated sales, improved data quality, improved audit trail and reduced costs.

DocuSign can be utilized on a personal level, for a workgroup or across a global enterprise. Using DocuSign Ink, users can legally send and sign documents with mobile devices while enterprises can accelerate compliance and improve business continuity and disaster recovery by being able to access documents any time, from anywhere.

## ✔ BEST PRACTICES FOR ELECTRONIC DOCUMENT MANAGEMENT

Because it is so easy to implement cloud-based services, the role of the CISO in establishing adoption policies and monitoring best practices across business units has never been more important.

**vi** "Assessing the Benefits of Electronic Signatures: DocuSign," November 2010. Nucleus Research Inc.

# 5
# No Hiding in the Cloud

Some purported electronic signing applications simply "paste" an image into a PDF and call it good.

To validate the integrity of the document, to manage version control of the document, and to ensure oversight of the process by the document sender, documents should always be accessed securely during the signing process within their secure repository.

Private and confidential documents should be encrypted in storage so that no one can read them except those who are authorized. Documents stored with application-level encryption provide confidentiality and assurance.

Much like paper counterparts, electronically signed documents can become the subject of a dispute. The signature *process* must provide enough proof to uphold the transaction.

Some purported electronic signing applications simply "paste" an image into a PDF and call it good. This creates a document that has no real value because it does not produce a file that has any assurance that a particular person signed it. It is not linked to any "proof" to make the signature legally binding.

Following such best practices, DocuSign's comprehensive approach includes:

- A digital audit trail that logs associated activities and applies a time/date stamp on all signer actions.
- Secure encryption so the document can be read and signed by only designated users.
- Unique signatures created by each user, accessible only to that user, and stored securely online.
- Signature areas (Stick-eTabs) so signers can initial and sign in specific parts of the document.
- Selectable user authentication methods to be commensurate with the transaction's security requirements.

## ✔ CISOS STEPPING UP TO THE PLATE

Cloud technology has proven ruthless in exposing inefficiencies and inconsistent business processes. Nowhere is that more evident than with paper-based signatures, perhaps the last bastion of the pre-information systems age. As CISOs step up to the plate and take charge of encapsulating security at the forefront of changing business processes, signatures can no longer stand alone against the tide of efficient, secure and reliable management systems. E-signing enables departments and functions across the enterprise to integrate signatures into the systems and processes required for success in the digital age—but only when those signatures are trusted.

For more information, please visit **DocuSign** at http://esignature.docusign.com/learnmore.