

Secure Time Management in the Financial Industry:

A White Paper

CRA Reports

*This report was prepared by
the Washington Bureau of
CRA Reports, an independent
editorial firm based in
Washington, DC.*

Copyright © 2002
All rights reserved

Secure Time Management in the Financial Industry

An Executive Briefing

Part 1. Introduction	3
Part 2. Dealing with “Time-Integrity” in the Financial Industry.....	5
Part 3. A Technological Overview	9
Part 4. Operational Imperatives for Secure Time Management.....	12
Part 5. Conclusion	15
Part 6. About the Sponsor: Datum, Inc.....	16

Editorial Director
Lane F. Cooper

Research Associate
Mike Wiebner

PART 1:

Introduction

This White Paper addresses the subject of Secure Time Management (STM) within the financial industry. Problems caused by ineffective secure time management can cripple a financial organization's ability to serve its customer as a result of lost data, operational failures, failed processes, legal exposure and compromised security. The report explores the policies, processes, and technologies that organizations in this industry can use to ensure the integrity of electronic transactions within and between organizations.

The Internet has had a dramatic effect on all sectors of the financial industry—from retail and commercial banks, to insurance and securities firms. In a few short years it has prompted a rapid shift to electronic processing for virtually all categories of financial transactions. To wit:

- A study presented this summer by the Federal Reserve reports that approximately 29.5 billion electronic payments were originated in the United States by consumers, businesses and government agencies in the year 2000, the most recent year for which this analysis could be undertaken. The total value of these electronic transactions reached a value of \$7.3 trillion.
- Officials at the Wall Street Technology Association point out that its members—brokerages and securities trading firms—are under continuous and increasing pressure to support and sustain e-commerce infrastructures and applications on a 7x24 basis as they are called on to provide customer service and support to external customers who may be located anywhere in the world in any time zone.

While the entire industry has made remarkable strides in building the enabling infrastructure that has supported the shift to online transaction processing from paper-based systems, there are still areas of concern about how to ensure the integrity of electronic transactions—and, on a larger scale, confidence in electronic trading systems.

Industry experts interviewed for this White Paper readily concede that there has been great improvement in enterprise-wide business automation software over the last few years. However they all point to a major vulnerability that the financial industry must address: ***a broad absence of Secure Time Management procedures and infrastructures.***

Secure Time Management is the management of the clocks and time-sensitive operations within the digital business environment. At a granular level, STM strategies ensure the “time-integrity” of devices and applications that create, process or transmit records related to transactions—including email systems, database applications, spreadsheets, securities sales report applications, and user logs.

For the purposes of this report, STM is divided into two discrete segments:

- **Networked Time Synchronization** – which makes sure all mission critical system clocks in the enterprise are synchronized; and

- **Networked Time Signing (or Stamping)** – which uses objective time reference points, such as Coordinated Universal Time (UTC), administered in the United States by the National Institute of Standards and Technology (NIST), and its military counterpart, the U. S. Naval Observatory (USNO), to establish with an extremely high degree of certainty that an event (such as a transaction) occurred when the system clocks said they occurred.

This White Paper takes the position that time records of transactions processed by most financial organizations today are simply too easy to change. Even novice users can alter the clocks of most computers within seconds. Multiply this vulnerability across tens, hundreds or even thousands of computers and the opportunity for confusion and fraud becomes great. Many of the established measures to protect the integrity of transactions were put in place to protect paper/manual processes, and are either ineffective or non-applicable in the new digital environment.

This White Paper concludes that STM must play a critical role as the industry completes its transition to a real-time digital processing environment.

PART 2:

Dealing with “Time-Integrity” in the Financial Industry

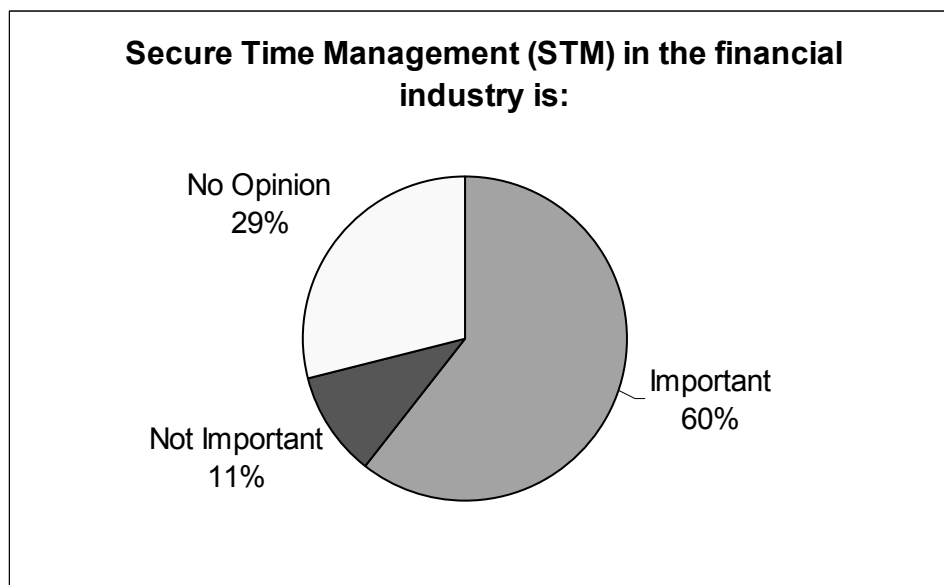
“Time is all traders and clients talk about. But the firm is also under the gun to keep the IT budget manageable, which means that our leadership frowns on new enterprise-wide initiatives. It is an up-hill battle to get them to see issues like this [time-integrity] as a worthwhile investment.” – IT Executive in Brokerage Firm.

The shift from paper-based to purely digital transactions has accelerated a great deal in the past several years. What had for years been mostly trade-show hyperbole has become a business requirement for financial organizations that have elected to take the paperless transaction-processing route.

To execute transactions electronically many financial organizations have expended significant effort to build secure infrastructures that deny access to unauthorized users, and ensure the performance and reliability of these systems. But in the process the role of “time-integrity” in transaction processing has been given short shrift.

The industry has done an excellent job of determining with certainty “who did what.” However, the question of “when” actions took place in a digital environment is much more difficult to answer for most financial organizations.

While Secure Time Management (STM) is recognized in the financial industry as an important factor in preserving the integrity of transactions and enhancing confidence in digital trading systems, few institutions are taking active steps to address the issue of “time-integrity.”



In a **CRA Report** Financial Industry Survey of IT executives at 47 institutions representing a cross section of banks, insurance companies and securities firms in the financial industry, a full 60 percent of respondents reported that STM is important in ensuring the integrity of events and transactions in the industry, but only one third

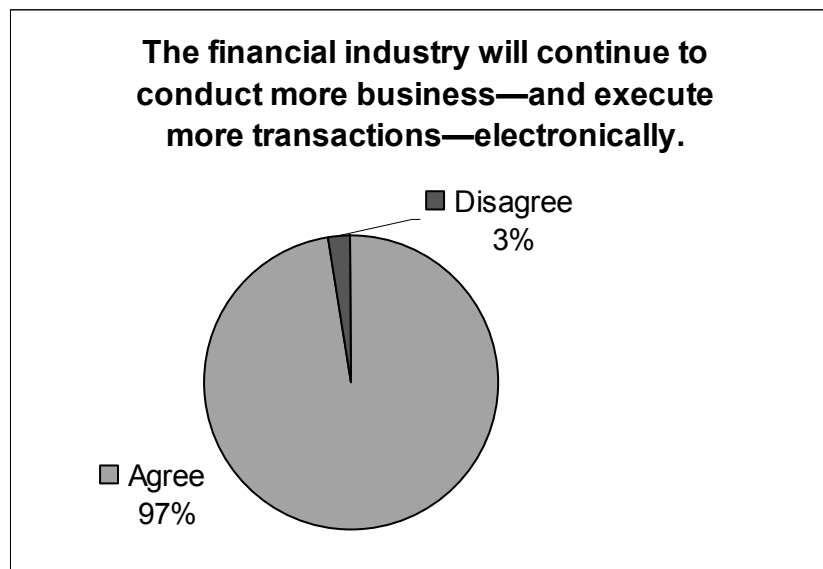
reported having specific concrete initiatives in place to address time-related security issues.

...Preserving the Integrity of “Digital Time”

Over the years, all sectors of the financial industry developed conventions and procedures designed to ensure the integrity of paper-based transactions. Time stamped paper documents played—and continue to play—a central role in the system of checks and balances that prevent malicious fraud or benign mistakes. Physical time-stamping provides auditors with an accurate time reference, allowing them to put together the sequence of events that took place in the correct order.

A similar level of certainty over time-related factors in a digital environment has not been attained. There are few industry-wide conventions governing “time-integrity” and consequently there is a major gap between the effectiveness of paper vs. electronic audit trails.

The challenge of preserving “time-integrity” is further exacerbated by the fact that movement toward the digital marketplace has exponentially increased the number of transactions executed in any given period.



The reason is simple: the Internet has broken down traditional limitations to transaction processing by introducing a 24x7 service availability paradigm that can serve clients in any time zone at any hour of the day or night. This has created an immense opportunity for financial organizations to capture additional market-share and tap new revenue streams. But the sheer increase in transaction volumes has also exponentially raised the level of risk associated with mishandled or fraudulent transactions.

If an organization’s time basis is not accurate or if there’s no tamper-proof way of assuring the time integrity of every single transaction, the potential problems for an organization are enormous.

The growth in the volume of transactions in the digital environment has made it imperative that organizations be able to track and independently verify when each transaction occurred. Authentication ties people or devices to data, but digital records require one other element if they are to be trustworthy—a secure, accurate and auditable time stamp.

The consequences of not implementing STM strategies can range from seeing a drop in electronic transactions processed because of lost customer confidence, to going out of business altogether. Specific risks include:

- Operational failure of automated events such as data backups or order processing. This can happen because time-triggered actions are initiated at incorrect times or because tasks that are supposed to be carried out on different computers in a coordinated fashion fail to be synchronized to ensure the proper sequence of events;
- Widening of security holes because information assurance operations designed to be tightly coordinated within and between organizations fall apart due to poor synchronization and the failure to use industry-standard protocols (such as network time protocol or NTP). This can create a wave of problems: firewalls can temporarily and inadvertently leave themselves open to penetration by hackers; and after attacks are detected, the absence of STM can make it difficult to hinder, mitigate or prosecute the perpetrators of damaging attacks;
- Legal liability can occur in commercial disputes because there is no way to prove that transactions took place as stated by computer logs. Even the authenticity of digital signatures on contracts can be effectively challenged because of poor STM; and
- Data loss because system software erroneously saves out-of-date files.

With effective STM strategies and infrastructures in place, financial institutions can mitigate these risks and, by being early and vocal adopters, differentiate themselves from competitors to enhance credibility, customer confidence and loyalty.

While financial organizations are still in the early stages of forming an industry-wide consensus on how to integrate STM into their security paradigms, there are some basic principles that have already emerged that can guide executives. Among them:

- **Use good time and frequency sources.** Three sources of timing and frequency information are generally used in telecommunications and commercial applications: cesium standards, rubidium oscillators and quartz oscillators. In addition, GPS and CDMA receivers capture and process timing information generated by satellite-based cesium and rubidium timing devices. (See Technology Impact Analysis)
- **Bind the time stamp cryptographically** to the data record of the digital signature or transaction. This makes it nearly impossible to tamper with the “time-integrity” of a digital signature without being clearly noticed.

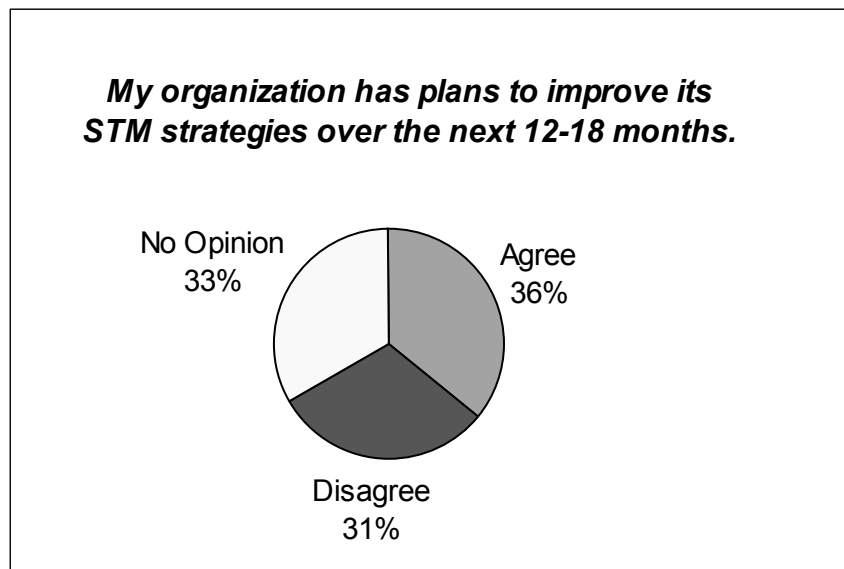
- **Embed a self-auditing routine** within the time stamp to substantiate the validity of the time stamp or signature.

STM technologies and packaged solutions are now available to players in the financial industry interested in buttressing the “time-integrity” of their systems on a point solution basis. They include:

- Synchronized Time Servers;
- Time Stamp/Signature Servers;
- Time-Secured Communications Devices; and
- Test, Measurement, and Validation Equipment.

...Looking Ahead

In coming months, this White Paper predicts that next-generation enterprise applications—such as e-mail servers and database applications—demanded by leading financial organizations will require that strong STM capabilities be embedded in packaged and/or deployed offerings.



Indeed, a plurality of respondents (36 percent) to the **CRA Report** Financial Industry Survey reported plans to improve STM strategies over the next year and a half.

In the meantime, there will be strong interest in—and demand for—the relatively few experts in strategic STM deployments that are active in the market today. Leading players in the financial industry are moving now to assess time-related vulnerabilities and take immediate actions to use available point-solutions to enhance their STM posture.

“Protecting the integrity of time must be done at the transactional level and at the process level by synchronizing time devices across the enterprise and by establishing a body of connected system clocks that are certified, coordinated and monitored.”—John Bernardi, President, Datum Trusted Time Division.

PART 3:

A Technological Overview

*"I have found that there is very little understanding of the technological issues associated with managing time in a large, dispersed IT shop. Most of the team is focused on keeping up-to-date on the technical issues that are considered mission critical...like item or check processing. So, yes, there is a technical knowledge gap when it comes to this [secure time management]." – **Commercial Banking Operations Executive.***

Simply depending on individually installed and calibrated computer-system clocks can lead to great peril because a number of factors can cause time kept by these devices to be inaccurate—even over relatively short periods of time. Among them:

- **Offset** – the initial setting of the clock can be improperly performed creating an immediate phase, or offset error. Page: 9 [0]
- **Aging** – the systematic change in frequency with time due to internal changes in the oscillator. (Page: 9 [0]) This is sometimes confused with drift)
- **Temperature stability** – frequency changes can occur due to shifts in temperature.
- **Accumulated time error** – over time, a combination of the above factors can contribute to the accuracy of a clock.
- **Short term stability** – a sudden change of frequency over 1-100 seconds can occur. (This is sometimes called flicker or jitter.)
- **Long term stability** – a change of frequency can occur over hours or days. (This is sometimes confused with aging.)

In developing a strategy that addresses the major threats to “time-integrity,” network administrators in the financial industry must first understand exactly what comprises a good STM infrastructure.

Networked Time Synchronization makes sure all mission critical system clocks in the enterprise are on the same page. This is achieved by installing network servers called timeservers. Typically costing less than \$5,000, these timeservers can support a network of thousands of computers and devices and require little in the way of administration. The best timeservers are based on the Network Time Protocol (NTP), which is very important for financial organizations that need to introduce time synchronization into heterogeneous corporate computing environments.

- NTP is an international standard for computer synchronization via a local area network (LAN) or a wide-area network (WAN). It provides a roadmap for setting individual computer clocks, and achieving synchronization accuracy. How often

computers and devices are synchronized with NTP timeservers is dependent upon the network system, and the tolerance the applications have for time discrepancies. According to industry experts, computer clock drift across an enterprise network is typically several seconds a day.

Time synchronization solutions tend to be first on most companies' STM wish lists. They are less expensive and easier to deploy than solutions that integrate time stamping capabilities. They also require very little implementation or integration support since most enterprise applications already are designed to look for time sources—though usually the source they seek keeps inaccurate time.

By using a networked approach to time synchronization, IT administrators can overcome the geographical dispersal and the diverse technical environments that characterize the infrastructures of financial companies to synchronize the different platforms through a master timeserver.

Networked Time Signing (or Stamping) uses objective time reference points, such as Coordinated Universal Time (UTC) administered in the United States by the National Institute of Standards and Technology (NIST), and its military counterpart, the U. S. Naval Observatory (USNO), to establish with an extremely high degree of certainty that an event (such as a transaction) occurred when the system clocks said they occurred.

- UTC is the internationally recognized time standard replacing Greenwich Mean Time (GMT). The STM infrastructure should be redundant so that the timeserver can switch to multiple sources should the need arise.

Implementing time stamping requires a close look at the existing technology topology. The time stamping solution must not only fit into the legacy systems of heterogeneous financial industry networks, but also fulfill time stamp requests from throughout the wide-area network (WAN) and deliver a unique, tamper proof identifier with the time and other pertinent transaction data.

For instance, a time stamp will take a record of a stock trade and generate a time stamp token that includes a hash (algorithms for computing a 'condensed representation' of a message or a data file), the time, the identity of the clock. A "package" is then signed and returned to the application which generated the time stamp request to further validate and secure the "time-integrity" of the logged event.

...Time Sources

Three sources of timing and frequency information are generally used in commercial applications: cesium standards, rubidium oscillators and quartz oscillators. In addition, GPS and CDMA receivers capture and process timing information generated by satellite-based cesium and rubidium timing devices.

The most stable and accurate timing devices in widespread use are based on the resonance of cesium atoms. Cesium standards operate by energizing a reserve of cesium atoms with microwave energy at a precise frequency. Because they are accurate to within a fraction of a second over 100,000 years, cesium clocks are used as international primary reference standards. Rubidium oscillators combine sophisticated

glassware, light detection devices, and electronics packages to generate a highly stable frequency output for cellular and PCS telecommunications base stations. Rubidium oscillators provide atomic oscillator stability at a lower cost and in smaller packages than cesium standards.

Quartz oscillators utilize the unique physical properties of quartz piezoelectricity and provide a cost-effective option for the synchronization of voice and data traffic over analog cellular transport systems. Applying a voltage potential across a properly prepared quartz crystal causes the crystal to vibrate and generate an electric signal with a relatively stable frequency. Quartz oscillators provide a less stable frequency than rubidium oscillators, but are available at a substantially lower cost.

GPS receivers, which capture timing information from cesium standards or rubidium oscillators aboard GPS satellites, provide another option for stable and accurate timing and frequency information. GPS receivers are typically used in systems integrated with quartz or rubidium oscillators that provide consistent timing output in the event the receiver loses the external satellite-based signal.

“An appliance approach to secure time management means that a dedicated device can be plugged in to deliver a very specific function – at a low cost without software conflicts, or administrative headaches.”—Gary Hawks, Chief Operating Officer, Datum Trusted Time Division

PART 4:

Operational Imperatives for Secure Time Management

*“An audit trail is basically a report on the order of events that took place: what happened, who did it, when did it happen. If an audit trail can be tampered with, then it can be used to perpetrate or obfuscate fraud. But there are other challenges as well. Often, when corporate customers complain about audit trails, banks simply give up defending themselves because it’s too hard to prove when things actually happened. But what about if the SEC starts asking questions?”—
Peter DiToro, Vice President, Datum, Inc.*

Operating on Internet time is more than just a catch phrase. The consequences of failing to maintain correct time within a company’s network are growing more serious while at the same time the potential problems (i.e., transactions) are multiplying at an exponential rate. While network administrators are increasingly aware of these challenges and potential liabilities, some in upper management are operating on what this White Paper contends is an incorrect belief: **that secure time management is strictly an operations issue, not a bigger, strategic-level issue worthy of C-level executive attention.**

Executive inattention can create problems for network administrators who must try to overcome the political problems inherent in persuading their counterparts throughout the organization—who are often responsible for different technological components and/or are located in different cities, states or even countries—to agree to cede some of their oversight, specifically of “time,” to a centralized source. C-Level influence can smooth the choppy waters and help make this a reality.

However, making the overall case for taking operational action on STM issues is not difficult. Mitigating risk has never been more important or challenging, given the current state of affairs facing the financial industry. The daily headlines are chockfull of reports on hacker attacks, employee fraud, securities malfeasance and accounting improprieties. They all point to just some of the challenges faced by commercial banks, securities firms and others in the financial arena.

An individual with access to a company’s system clocks, for instance, can create havoc – and abscond with large sums of money – simply by changing the times associated with various actions they’ve taken. In digital terms, they alter the system clocks to cover their footprints. This route has been taken by hackers and dishonest employees alike.

Hackers, once they’ve penetrated a company’s firewall, tend to troll from computer to computer, until they come across the information they’re after. When an organization’s clocks are not synchronized and transactions are not time stamped, most attempts to identify the criminal behavior, much less catch the perpetrators, are doomed to failure because network administrators cannot rely upon the unsynchronized times of multiple system log files to help them track the illegal activity.

...Managing the Threat Within and Between Institutions

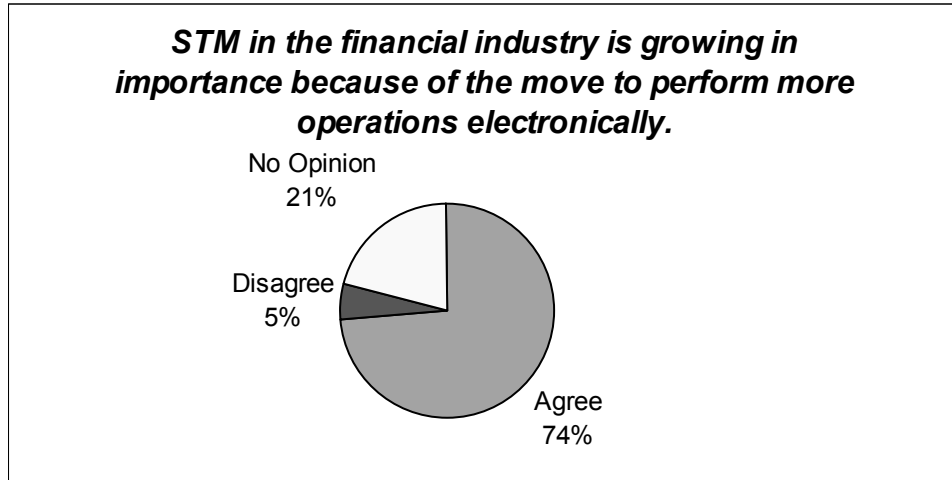
Dishonest employees have also been caught manipulating digital time to commit financial crimes as well. Take the case of a bank employee who had been withdrawing money from inactive accounts for more than a year before one victim tried to make a withdrawal and found her account was nearly tapped out. A nursing home resident, the victim had been recovering from an accident only to find she'd been robbed. The employee had simply altered the system clocks to remove all indications of his illegal withdrawals.

In addition to stamping out fraud, Secure Time Management plays a critical role for financial institutions that are pursuing B2B E-Commerce opportunities via the Internet. Their enterprise software systems, while robust and secure, are quite expensive to operate and maintain. Doing business via the Internet can lower transaction processing costs, improve ease of use and provide greater network resource availability.

Advances in virtual private networking (VPN) technology have made it possible for organizations to send sensitive transactional information (such as purchase orders, invoices, payment authorizations, etc.) by using public key infrastructure (PKI) to prevent unauthorized access to the data until the transmission reaches its destination. But if the time-clocks on the two sides of the interaction are not synchronized for time-sensitive transaction—such as an advanced ship notice (ASN) or electronic funds transfer (EFT) authorization for a just-in-time (JIT) manufacturing operation—then operations that are supposed to be tightly coordinated can be severely disrupted at a high operational cost, not to mention exposing all parties (buyers, sellers *and* participating financial institutions) to considerable legal liability.

A very similar dynamic is at play in the securities industries, as brokerages, trading houses and regulatory agencies work together to develop straight-through processing (STP) conventions that are specifically designed to reduce the steps and the time elapsed between a placed “buy” or “sell” order and its ultimate execution.

With time always in play in financial transactions, nearly every operation, device and process has a time component—and a corresponding need to ensure correct, synchronized time across the enterprise in an independently verifiable/irrefutable manner. This explains why 74 percent of respondents to the **CRA Report** Financial Industry Survey consider STM strategies that integrate both time synchronization and time signing/stamping as growing in importance.



The real question is: How can STM strategies be deployed in an efficient and cost effective manner?

This is a particularly salient issue for financial institutions, which tend to be geographically dispersed and—as a result of mergers & acquisitions that have characterized this industry’s development—have given rise to highly complex, heterogeneous technological topologies. Any given institution can have legacy mainframes, a full spectrum of Netware, UNIX and Windows NT platforms, and a broad array of desk-top client devices as well as dumb terminals. Each technological environment within an organization has its own set of discrete administrators accustomed to running their own respective shows.

It is a task that seems daunting. However, by using automation principles—which means tapping the hubs of activity or gateways through which the bulk of transactional traffic runs—it is possible to quickly and cost-effectively deploy an enterprise-wide STM strategy.

High level commitment and leadership combined with an educational approach that focuses on standards-based STM implementations can help overcome potential political squabbles. This means:

- Making a commitment to the network time protocol (NTP) for timeservers which synchronize the time for all the devices across an organization’s network; and
- Using open standards for time stamping, specifically RFC 3161 the time stamp protocol published by the Internet Engineering Task Force, the leading Internet standards body.

PART 5:

Conclusion

“Secure time management is a critical part of the transition to real-time processing in financial services. Companies are just starting the transition to this environment. Messages related to payment and securities trading are especially important and are getting most of the early attention.”—Susan Cournoyer, Analyst, Gartner.

Making any business decision requires an understanding of both the dollars and the sense. While defending against future liabilities, hackers and lost business cannot generally be assigned a specific monetary value, the possible results of failing to act can be described in harrowing detail.

Hackers, dishonest business partners and/or disgruntled employees are aware that time is a vulnerable element in most company's computer networks. This growing awareness, coupled with how easy it actually is to manipulate standard computer clocks, has contributed to an increase in corporate fraud, hack attacks and other malfeasance. The joint annual report from the Computer Security Institute (CSI) and Federal Bureau of Investigation (FBI) indicates that a growing percentage of computer fraud is perpetrated from within the affected companies. And in the case of fraud, time-manipulation of computer systems is often at the heart of the crime.

Consequently, various regulatory bodies have stepped up their efforts to create rules that protect the “time-integrity” of transactions and other mission critical events. This is leading to an increasingly demanding—and sometimes confusing—compliance environment for players in the financial industry.

In the securities arena, for example, the SEC rule 17a-4 requires exchange members, brokers and dealers to maintain records with different levels of accessibility based on the age of the records and to prove the integrity of the messages. NASD member firms must comply with Order Audit Trail Systems (OATS) regulations, which require financial institutions to carefully track and record customer orders, calls and other transactional activities.

Failure to keep all computers within three seconds of UTC time as presented by NIST can prompt an audit finding that can lead to censure, fines, and bad publicity.

Add to this the large volume of transactions that are executed simultaneously across different servers using different systems, and one can begin to appreciate the nature and scope of the risks to which financial institutions are exposed.

In the highly conservative financial industry, a number of STM pilots are now underway, mostly dealing with time synchronization. The use of time stamping has been more limited, but the rise in the lawsuits and widely-reported acts of corporate fraud highlight the importance of security, protecting against internal fraud and developing tamper-proof, independently verifiable audit trails for all key business processes.

Part 6:

About the Sponsor:

Datum, Inc.

Datum, Inc., founded in 1969 and headquartered in Irvine, California, manufactures and markets a wide variety of high-performance time and frequency products used to synchronize the flow of information in today's telecommunications networks. Datum's timing products are capable of accuracy to within a fraction of one second over 32 million years.

The company is a leading supplier of precise timing solutions for computing networks, satellite systems, electronic commerce, and test and measurement applications. Datum invented the rubidium oscillator in 1971 and now supplies the majority of the high-precision rubidium atomic clocks used in cellular and PCS network base stations. The company also produces extremely precise hydrogen maser and cesium standards, GPS/CDMA receivers, and recovery clocks that generate or capture timing and frequency information for use in wireline telecommunications infrastructures. Datum's Trusted Time Division provides secure and auditable time stamping technology for electronic transactions, time references for computer networks, and encryption engines for distribution and reception of confidential information.

Datum Inc.
9975 Toledo Way
Irvine, California 92618-1819
Phone: 949-598-7500
E-mail: Corporate@Datum.com
Web: www.datum.com