



nuBridges Secures Sensitive Data across the Business Ecosystem

Analyst: Anne MacFarland

Management Summary

In today's highly partnered world, perimeters must be made to be crossed, not just defended. The efficiency of supply chains can spell the difference between efficient service to loyal customers and an eroding customer base. If we are serious about curbing our use of fossil fuels, optimizing supply chain operations for energy use as well as customer satisfaction will require more sharing of information between partners – not less. When businesses were more self-contained, strong fences made good neighbors. With the Internet, extensions beyond the organization proliferated – but many companies retained a sense of central control. Today, the habit of growth by acquisition and “strategic” partnering, a customer predilection for not only self-service but more push-back and control, and an acknowledgement of insider threats have pushed security strategies into a more pragmatic, component-based, inside *and* outside approach. It is not just the systems that must be defended, but also the information they hold – much of it sensitive corporate and customer information. It is not just access to the data, but the data itself that must be secured.

The risks of holding sensitive information have grown. The fulfillment and cross-sell/up-sell ramifications of eCommerce have expanded both the relevance and the use of customer information. The intolerance of current business models for bulky inventories and development cost overruns produce a need for more precise and real-time knowledge of customer requirements. More instrumentation of edge devices (such as grocery loyalty card scanners) allows more detailed data to be collected. Some of this information may seem trivial, but it all falls under the aegis of privacy regulations. Search and indexing make information more findable. Collaboration tools make it sharable. Indices of information become a new point of risk, and a new kind of information that must be secured. If, like many businesses, you have used key customer information – names, account numbers or, even worse, governmental identifiers like Social Security numbers – you increase your data security challenges in many dimensions. And, finally, the more data you have about your customers, the more worthwhile it is to steal.

Such a world calls for a data security strategy that fits the mode of business like a glove – providing both comprehensive coverage and flexibility. A company called nuBridges, based in Atlanta, GA, with roots in B2B integration for retail and manufacturing sectors, has focused on what might be called *gregarious businesses* – those with extended value systems, for whom bridging information between organizations is a way of life. nuBridges started in the B2B gateway and Electronic Data Interchange (EDI) space, and expanded into managed file transfer, data protection, and PCI-DSS compliance markets. Their pragmatic, data- and information-focused approach to security addresses the burgeoning risk of data security and, in the process, makes addressing other challenges of security, such as users (people and applications) and infrastructure (facilities, the physicality of IT, and logical/virtual) less complex. For more details about nuBridges' approach, please read on.

IN THIS ISSUE

➤ Securing Sensitive Data.....	2
➤ nuBridges Solution Strategy	2
➤ Conclusion	3

Securing Sensitive Data

Risky sensitive data in IT systems goes far beyond that associated with purchase transactions. Customer data is used in many other ways in IT systems – Customer Relationship Management, order-to-cash systems – and in pre-deployment testing of any applications that touch the customer. Corporate data used in partner relationships and negotiations is equally high-risk.

Data and information security in a gregarious business must be granular. The information that you share with one partner but not another is very specific – a single table or a single column in a database. Industries such as retail, that thrive by cultivating multiple sourcing and second sourcing relationships, must be able to manage a lean inventory of constantly changing products in a simple way. This need drives information and data focused security with the following design parameters.

Topography

Topography addresses the extent of a business' *value net*.¹ Most organizational value nets are distributed but not entirely. When business operations cross boundaries, the data transferred must be secured. With the growing awareness of internal threats, data transfers within an organization often need similar security. The most effective way to secure data is to do so directly where the data originates or is stored, not just by reinforcing and monitoring the pipes. This is achieved with encryption and key management. For sensitive data, even higher security is provided by the use of tokens. To be organizationally effective, data security must extend across the entire value net, including partners who may not have always-on connectivity. With this kind of data security in place, intrusion detection has more time to react effectively, and attackers can steal nothing that is immediately useful.

Risk Profile

Every business or organization should be aware of its *Risk Profile*² – something that is both specific to the business and changeable

¹ A value net includes a business and its suppliers and distributors – all the participants that transform raw materials into a delivered product or targeted service. A useful conceptual domain in a complex world, it is also used to calculate environmental impact via carbon credits.

² This is different from an organization's information profile (what data and information sources exist, and where they are stored), which has relevance far beyond data security.

over time.

When it comes to customer or corporate information, the penalties for data exposure dictate that pro-active security strategies must be used. Destroying data that is neither regulated nor useful to the business reduces the scope of the challenge. Often the next step is to analyze operations and focus security on the areas of highest risk – such as credit card transactions in insecure locations or Websites. However, **in the long run, a more comprehensive approach, specifically focused at data security, can go a long way to proving that exposure has not occurred.**

Management paradigm

In a world of always-on operations and 24x7 commerce, a single administrator is a systemic weakness. That single person cannot be always available, and can be a large risk if not honest. In larger organizations, the tasks of creating distributing, and managing tokens and keys are done by different people. With the availability of on-line secure workspaces, some companies today are turning, for day-to-day policy administration, to a committee approach with a quorum (n of m) approach to support a persistent workforce that can set and revoke policies and privileges. It also gives built-in operational oversight that strengthens operational integrity.

Data security management must also ensure auditable logging, and support it in a way that allows the heritage of access to particular data to be quickly assembled. Logs should be compliant with syslog standards.

nuBridges Solution Strategy

Encryption and Tokens

There are certain basic practices that underlie to data security.

- Encryption of sensitive data is best done sooner (when the data or information is generated or captured) rather than later.
- Standard forms of encryption should be used, and updated as needed.
- Decryption should be done as infrequently as possible.
- Logging of events touching sensitive information and auditability of those logs is required.

Beyond the disciplines of data encryption outlined above, one way to minimize the occasion of risk of exposure of sensitive data

further is by using tokens. Here is how it works. Encrypt the original, segregate it in a safe place (repository), and then assign a unique, format-preserving token. Unlike with hashing or simply encrypting, the token can be the same data type and data length as the original, which lets it be used in application testing, and in shared databases without having to make changes to the application.

This token cannot be broken, for it is a substitution rather than a transformation. Therefore, the token can be sent within the organization and between organizations without risk. When the exact components or values of sensitive data are needed (which is surprisingly seldom), the token is very securely submitted to the secure repository, and the precise information needed very securely sent. This additional security can be added by using more rapid key rotation.

Key Management

Keys and key rotation are an inherent part of data security. Key rotation is like dynamic routing. It reduces risk by changing keys – like changing passwords – more frequently. This rotation must be disciplined, but can be implemented during lulls in activity. nuBridges' key management is a separate and separately-secured subsystem.

The nuBridges keys themselves have “rotate by” metadata (like the sell date on milk cartons) so the decryption process can link to the proper profiles and keys. The other alternative, some annual schedule – is onerous, predictable (another source of risk), and insufficiently flexible. Some highly sensitive information may benefit from more frequent key rotation.

The nuBridges Key Manager is an out-bound server that supports all sorts of platforms, including z/OS – and, now, z/VM Linux applications on mainframe processors. The key management can be part of a purely distributed or a hub-and-spoke model. The distributed model can work with a local, secure data vault, or a central server that assigns a token that is valid anywhere. It all depends on your organizational and risk topography, and on your data flows and business processes.

nuBridges' solution handles any type of data. The solution extends to any platform. Key strategy is to encrypt data at its source, and move the data to where it can persist without decrypting and re-encrypting.

Conclusion

Securing sensitive data in a way that does not constrain either business ambitions or agility is, these days, key to business survival. If you have been dismayed by the complexities and security challenges posed by the participation age, nuBridges' data and information perspective may be just what is needed to turn your data security challenges into opportunities.



About The Clipper Group, Inc.

The Clipper Group, Inc., is an independent consulting firm specializing in acquisition decisions and strategic advice regarding complex, enterprise-class information technologies. Our team of industry professionals averages more than 25 years of real-world experience. A team of staff consultants augments our capabilities, with significant experience across a broad spectrum of applications and environments.

- ***The Clipper Group can be reached at 781-235-0085 and found on the web at www.clipper.com.***

About the Author

Anne MacFarland is Director of Data Strategies and Information Solutions for The Clipper Group. Ms. MacFarland specializes in strategic business solutions offered by enterprise systems, software, and storage vendors, in trends in enterprise systems and networks, and in explaining these trends and the underlying technologies in simple business terms. She joined The Clipper Group after a long career in library systems, business archives, consulting, research, and freelance writing. Ms. MacFarland earned a Bachelor of Arts degree from Cornell University, where she was a College Scholar, and a Masters of Library Science from Southern Connecticut State University.

- ***Reach Anne MacFarland via e-mail at Anne.MacFarland@clipper.com or at 781-235-0085 Ext. 128. (Please dial “128” when you hear the automated attendant.)***

Regarding Trademarks and Service Marks

The Clipper Group Navigator, The Clipper Group Explorer, The Clipper Group Observer, The Clipper Group Captain's Log, The Clipper Group Voyager, Clipper Notes, and “*clipper.com*” are trademarks of The Clipper Group, Inc., and the clipper ship drawings, “*Navigating Information Technology Horizons*”, and “*teraproductivity*” are service marks of The Clipper Group, Inc. The Clipper Group, Inc., reserves all rights regarding its trademarks and service marks. All other trademarks, etc., belong to their respective owners.

Disclosure

Officers and/or employees of The Clipper Group may own as individuals, directly or indirectly, shares in one or more companies discussed in this bulletin. Company policy prohibits any officer or employee from holding more than one percent of the outstanding shares of any company covered by The Clipper Group. The Clipper Group, Inc., has no such equity holdings.

Regarding the Information in this Issue

The Clipper Group believes the information included in this report to be accurate. Data has been received from a variety of sources, which we believe to be reliable, including manufacturers, distributors, or users of the products discussed herein. The Clipper Group, Inc., cannot be held responsible for any consequential damages resulting from the application of information or opinions contained in this report.