Clipper Notes™
VENDOR-AGNOSTIC EXPLANATIONS AND ADVICE
FOR THE INFORMATION TECHNOLOGY BUYER

Navigating Information Technology Horizons℠

New in 2007 Report #TCG2007050 April 5, 2007

The Challenge of Enterprise Security

Analyst: Mike Kahn

Management Summary

It's income tax preparation time for many of us. It should be a simple enough chore. For many, it is very straightforward. You gather up your W-2s[1] and maybe some 1099s for interest and dividends received. By hand or with the aid of tax preparation software, determining your taxes due and whether you owe more or have a refund coming is easy. While you may fret over it, you know that this is an achievable task. Doing your state income tax return may be a further chore, but if you are lucky, it too should be straightforward. Why? Because you live a simple life. **Managing a simple life is easier – easier to live, easier to mitigate (simpler) risks, etc.**

However, many readers may find that their financial lives are anything but simple. Add a spouse, children, maybe a former spouse, mortgages, tax-deferrable income (i.e., 401Ks and IRAs), capital gains/losses from sale of a house or securities, earnings from multiple employers, possibly in different states, pension income, Social Security income, taxes paid to multiple districts, etc. You can see the complexity in all of this, even before you begin to wrestle with whether to file as a couple or individually, whether the Alternative Minimum Tax will apply, etc. No wonder the majority of U.S. taxpayers use either software or a professional to file their returns.

What is the reason? It's just too complicated to imagine doing it all in your head (even with the help of paper and spreadsheets). **Increased complexity compounds the situation very quickly.** It is easy to get to a point of being overwhelmed. As intelligent beings, we don't like to put ourselves in that situation, so we try to limit the complexity of what we do. If you can achieve more simplicity, that is great, but **most of us cannot give up what we do for the sake of making our lives simpler and thus more manageable.** It would be nice if our business environment was simple. For most, this is a fantasy, because our enterprises have many divisions, many lines of products and services, a complicated nest of reseller and customer relationships, geographic presence around the world, many different tax and legislative rules to follow, etc. Sure, it would be nice to be simple, but there is no getting there from where you are. Of course, **that doesn't mean you won't try to make IT in your enterprise simpler and more manageable. Nonetheless, security requirements build from the complexity of the enterprise and its lines of business.**

Those of us who have been around IT for the last couple of decades, or more have seen many schemes for "simplifying IT". One worth mentioning is running each application on a separate server. It sounds simple until you end up with more than a thousand servers, each running at far less than full capacity yet consuming a full share of power and cooling. That has led to server consolidation, which makes a lot of sense, but violates the goal of simplicity.

None of this is, by itself, a new challenge. We have been here before. However, the world in which we have to operate has changed. IT now works around the clock, around the world, with many more objects[2], and people involved (users of all sorts), more scrutiny and demands from governments, partners, and customers, and, most important to this bulletin, with many more threats to consider, anticipate, and repel. **The bottom line is that *managing* and *protecting* applications, data, and users in today's enterprise environment are each complex tasks. Since each goes hand in hand with the others, the overall challenge is formidable.** Read on to understand the challenges of *serving* and *protecting*, how they usually compound one another, and what you really need to do to be secure.

IN THIS ISSUE

[1] For those of you not from the United States, this is the annual report of wages received, taxes withheld, etc., from your employer.

[2] Such as data (from many sources) and applications (both interlinked with one another and those less intertwined).

The Clipper Group, Inc. - Technology Acquisition Consultants ♦ Strategic Advisors
888 Worcester Street ♦ Suite 140 ♦ Wellesley, Massachusetts 02482 ♦ U.S.A. ♦ 781-235-0085 ♦ 781-235-5454 FAX
Visit Clipper at *www.clipper.com* ♦ Send comments to ***editor@clipper.com***

Beyond Comprehension

Few of us have a perch so high that we can see all of an enterprise's applications in a single frame. There are just too many of them. To make matters worse, there are many relationships among them, rendering a two-dimensional visualization to a dense collection of spaghetti connecting a large tray of meatballs. Seeing this in 3D might improve the visualization, but not by much. This is the reason that many enterprise IT organizations divide their application realm into much simpler collections or application domains. While it might be simplifying to segregate the manufacturing department from sales or finance, i.e., to presume that there are no relations between them, we all know that this is an artificial and potentially inefficient segregation. You might ask, can't we subdivide the world or applications somehow, say between separate divisions? While the answer might be yes, this might not always be true. Increasingly, there is no such thing as independent, standalone work, especially in an era of Service Oriented Architectures[3], enterprise retention policies, and more. **Everything is related, or might be at some time. Presuming the problem away (into segregated silos) just doesn't cut it anymore.** (See Exhibit 1, at top of next column.)

The Heart of the Security Problem

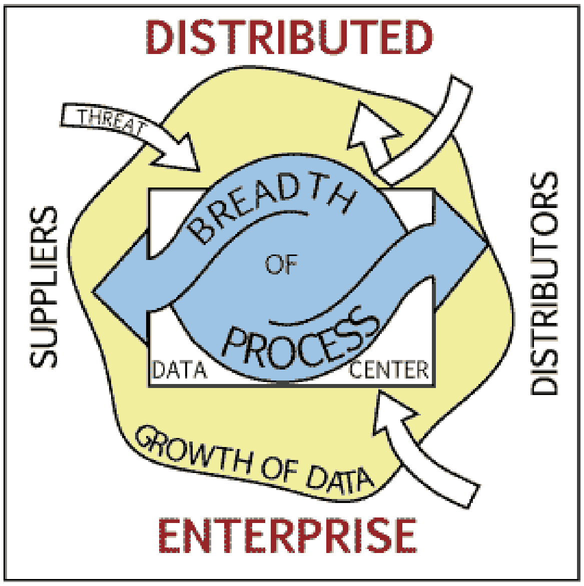
This presents a curious set of problems to the IT organizations that are hosting enterprise applications and enterprise databases. *How do I manage the hundreds or thousands of applications that clamor for server resources?* That's a tough question, but not the one that is at the heart of this bulletin – *How do I manage security in this complex, interrelated environment consisting of all of these applications, all of the folks who use them in any way, and all of the data and transactions involved?* OK, you're right; the two questions of management and security are closely related. **Unless all things are treated equally (e.g., all applications, data, and users are all treated the same), it is necessary to manage (i.e., deliver) the IT resources to applications and users in order to address how they are going to be secured.**

Controlling the View

Nonetheless, we need to abstract away the resource (e.g., server assets) part of this problem, in order to focus on the security issues. Consider the blue-shaded area in Exhibit 2, on page 3. We can assume that most "IT activity" can be classified as a work element: a task, or some kind of project, depending on the number and types of users, objects, and applications/programs/services that are involved. These are bound together intrinsically. While users may come and go, and data may change, and application components may be re-amalgamated over time, sometime on the fly across all three, **the relationships tend to be enduring according to task or work at hand.** This is a convenient truth for us. While we may want to specify security requirements for groups of users, classes of data, and applied uses (applications) individually, **it is the interrelationship among all three for which security needs to be implemented, in an auditable manner.**[4] While we may care what resources are to be deployed to deliver the qualities of services required, it is best if we think of these as virtual "containerized resources" that consist of the underlying resources needed to get the job done, effectively and securely, as shown in the yellow-shaded area of Exhibit 2, on the next page.

If we assume that the containerized IT resources operate in partitionable and extensible environments in which the work/projects/tasks can be related to one another and that the underlying resources can be enabled, protected, managed, optimized, and accounted in an auditable fashion (i.e., "served up" in some virtual sense), it makes our discussion of enterprise security much simpler. So let's do that. Let's assume away the collections of equipment and

Exhibit 1 –The Nature of the Problem



[3] **In a Service-Oriented Architecture, the focus is on what is being delivered and/or done as opposed to where the data is, who owns it, and who controls it.** The SOA approach has revolutionized the development and evolution of both the massive applications that drive the enterprise and the capabilities of the applications that feed off their data. The component-style approach requires a more atomic approach to IT security.

[4] **Auditing, i.e., the audit function, is a key component of enterprise security**, just as it is a fundamental part of the enterprise accounting function. You can't be secure without looking for deviations from enterprise policy.

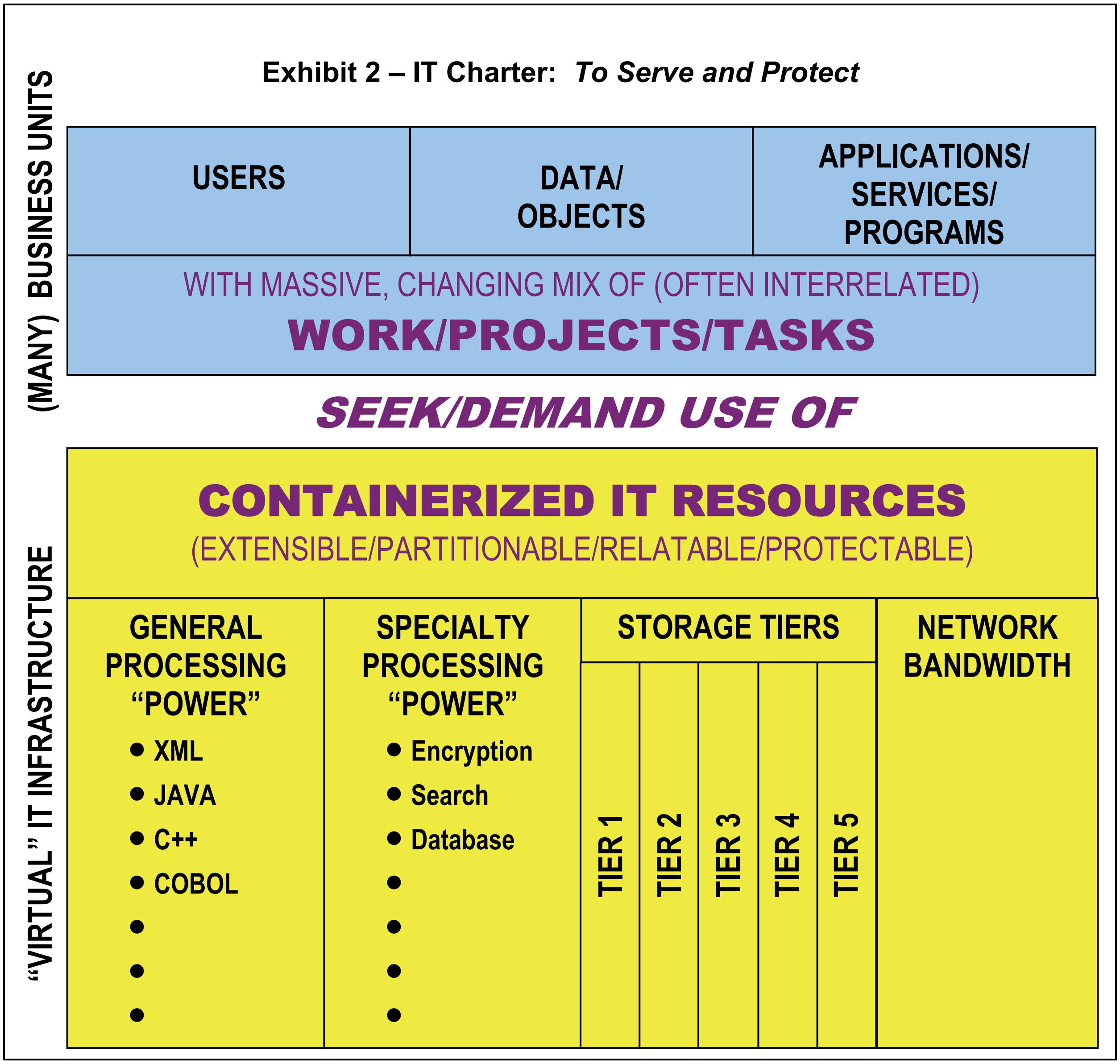


Exhibit 2 – IT Charter: *To Serve and Protect*

(MANY) BUSINESS UNITS

USERS

DATA/ OBJECTS

APPLICATIONS/ SERVICES/ PROGRAMS

WITH MASSIVE, CHANGING MIX OF (OFTEN INTERRELATED)

WORK/PROJECTS/TASKS

SEEK/DEMAND USE OF

"VIRTUAL" IT INFRASTRUCTURE

CONTAINERIZED IT RESOURCES

(EXTENSIBLE/PARTITIONABLE/RELATABLE/PROTECTABLE)

GENERAL PROCESSING "POWER"
- XML
- JAVA
- C++
- COBOL
-
-
-

SPECIALTY PROCESSING "POWER"
- Encryption
- Search
- Database
-
-
-
-

STORAGE TIERS

TIER 1

TIER 2

TIER 3

TIER 4

TIER 5

NETWORK BANDWIDTH

data that underlie how this might be done in a variety of environments. This still leaves us with a large task of protecting what we serve up and process.

Earlier, I dismissed the idea that "security by isolation" was an acceptable solution for the typical large enterprise. Of course, that would make life in IT a lot easier, but it just doesn't fit today's enterprise needs. Therefore, let's begin by assuming that this kind of "top secret" segregation is not the answer. *So, what are the enterprise requirements for security in our virtualized, containerized IT environment?*

An *integrating mechanism* (i.e., security pro. gram) is needed, one that allows us to state the policies of segregation and use and an executable environment that is capable of taking these policies and uses and providing protection accordingly. **IT resources must be *allocatable* and *manageable* to permit this.**

1. **Each component needs to be certifiably isolatable from other components, when required.** For example, the payroll application needs to be separated from the sales application, except when sales commissions are translated into compensation. Financial reporting data needs to be segregated from manufacturing data, except when manufacturing data is used in financial reports. Users need to be separable and isolatable by class (say, by whether a customer, a partner, or an employee) and by use. (See *Virtual Partitions or Containers*, below.)
2. **We need to allocate and manage in a reliable and auditable way.** This amounts to a big challenge, especially if you have not been doing this across your varied IT infrastructure. If you have a hodge-podge of applications running on a

heterogeneous set of servers and environments, then you have a great challenge to sort this out, which must be done before you can secure the environment.

Again, let's make the problem a little simpler by making another assumption, just for now – that all applications are running on a single operating environment, say *Linux*. This makes it easier to discuss because Linux applications can be run in many hardware environments and architectures. If we can assume that these underlying physical assets (i.e., the servers) are interchangeable, then we can imagine more easily that there can be a single point of management and control. This simplifies a lot, which is OK for this discussion. So, **what we now require is an IT environment where we can secure work in isolation and in relation to other work and systems processes, in an auditable manner.** What does that imply?

Virtual Partitions or Containers

First, we need to make sure that our "virtual partitions" or "containers" that hold and run our applications are truly isolatable. The same is true for virtual memory and storage resources. Second, we need to define what it means to be isolated. Is it good enough to have a password authenticate the application's or user's right to access and modify data? What about a server-to-server request? Can you really tell who is making the request, by paying attention only to who made the last request in a chain of requests? Does your audit trail extend from the final requesting object all the way back to the original requestor, or does the trail end at the last requesting server (thus, requiring you to attempt to trace manually back through all of the intermediary service logs to attain a useful picture)?

To do this right (i.e., in a proper (auditable and enforceable) way, requires that we know what we are tracking, be it administrator, user, application object or data object. To do this in the larger enterprise requires clear policies and IT vehicles to enforce and report on them.

Transparency

Second, **transparency is needed for your IT operations.** Just what does this mean? This can be boiled down to a "need to know" basis, which might be better termed "permitted to know".

- Who can see what applications are running in which containers?
- Who can change the containers or applications?
- Who is allowed to see what data; who can change, remove, or supplement it?
- Who is allowed to copy IT or application information (data, transactions, logs, reports, etc.) to a client device or attach it to an email?
- Who can print any of this or copy it to a USB drive?

A reasonable degree of paranoia can make the task of securing IT more feasible than assuming a *trusted environment*[5].

Recordkeeping, Prevention and Mitigation

Beyond the need to know is the auditing requirement to track all of this, i.e., who has accessed/ printed/distributed what, when, where, how and to whom? Beyond even this is the need to be able to prevent any of the above from happening, when prevention is needed. This raises a lot of questions, especially about the nature of the inherent problems.

- *Are we trying to keep the "bad guys" from accessing private data?*
- *Are we trying to keep disgruntled employees from doing damage or stealing?*
- *Are we trying to keep users from going or doing what they are not allowed to see or do?*
- *Are we trying to keep administrators from going and doing what is outside of their domain? Who should be allowed to see which metadata and which real data?*
- *Are we trying to track all of the attempts to do the above and to follow the outcomes, for better or worse?*
- *If it happened anyway, i.e., you found out after-the-fact, do you want to be prepared to mitigate that risk or damage?*

For almost all larger enterprises, and many smaller, the answer is "yes" – to them all and more. For many, this is a lot more than they have been doing, except within isolated silos. Whether driven by government mandate, new threats to business operations, integration of operations (either by mergers and acquisitions or to meet the increasing desire to serve customers better across many product and/or service lines, etc.), **the challenge is, for now, how to do all of this.** Sticking your head in the sand is no longer an acceptable alternative. It might cost your business millions or billions and you might go to jail.

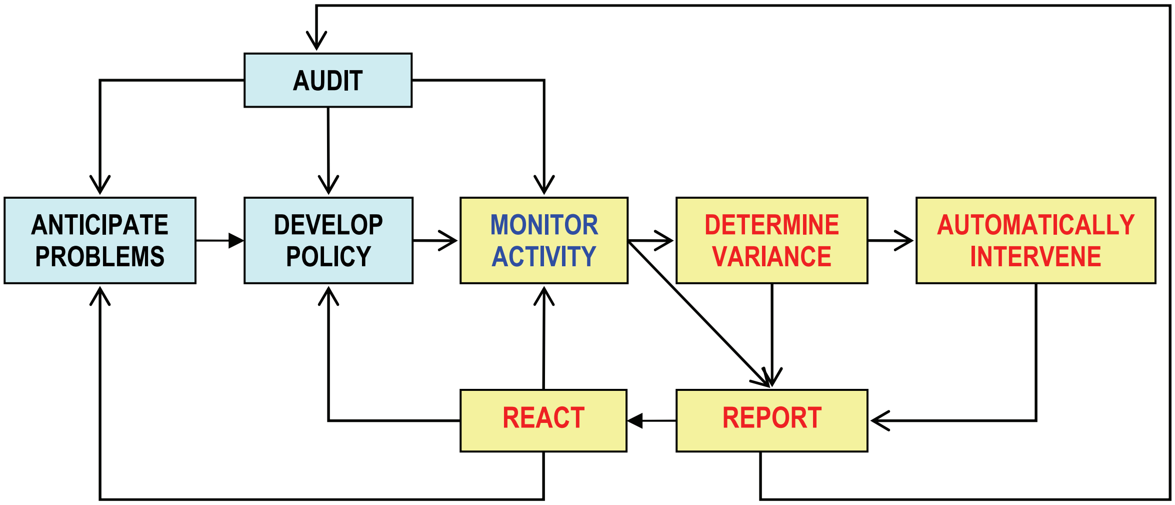
The Big Picture

If you haven't gotten the big picture, you have missed the most important point. This is about the *big picture* and not the individual items within the picture. If you have been focused on archiving email, preventing hackers from access over your networks, stopping SPAM, virus-laden attachments, and spyware from entering or incubating within your enterprise, this is all well and good. However, it ignores several most important facts.

Your greatest threats are inside of your enterprise. You should hope that you are this far along in protecting your enterprise. While a moat

[5] Where everyone assumes that everyone else is trustworthy.

Exhibit 3 – A Simple Model for Managing Security and Auditing Requirements



may keep the bad guys on the far side of your perimeter of defense, you have done nothing to address administrator or user error, their own unsavory intentions, or the imperfections that you have used as inner perimeters of defense.

You may be changing your business models and underlying IT requirements in many significant ways. What worked before may not work in an era of greater data interdependence and analysis, much greater interdependence of applications and processes (accelerated by the use of recyclable components through SOA and other approaches).

The scope of the IT management challenge is so big that meeting the challenge cannot be done by unstructured and ad hoc means. Putting policies in a manual just doesn't cut it any more. (Ask your auditors!)

If you thought that the growth of your data was a big problem, from provisioning, to management, to cost, you better prepare yourself for something even bigger! Securing, in an auditable manner, your administrators, users, applications, and data are a much bigger challenge!

Thinking about the Larger Security Challenges

By this point, you should recognize that securing and auditing is a lot more than password-based user authentication. Yes, you need to authenticate and keep out those that are not authenticated or, at least, constrain how they interact with your enterprise, i.e., align the risk with the potential reward. What is needed is a way to look at security and auditing as a continuous, real-time process. Consider the following flow diagram, in Exhibit 3, above. The goal is to do the following.

1. *Anticipate* problems
2. *Prepare* for them
3. *Monitor* activities
4. See if there is a *variance* from established policies
5. *Automatically intervene* (if the situation mandates, say, before the data leaves the enterprise)
6. *Report* on deviations and interventions
7. *React* on such reports by enhancing the problem/risk assessments
8. *Change the policies* to incorporate the new risks, etc.
9. *All while satisfying the needs of auditors*, who may further identify problems and/or suggest changes to your policies.

All of this seems logical, maybe even straightforward, but it cannot be achieved unless your infrastructure is properly aligned (i.e., containerized) and in support of your policies.

If your systems cannot secure the applications and data adequately (to a level of enough detail to achieve your objectives) then your hoped-for success ends here. If you cannot manage all of your resources (and ultimately the applications and user experiences) to predefined service levels, through Service Level Agreements (SLAs) or other means, then you may be secure but not getting the job done. Once you the concept of big picture of security requirements, you must append these to your operational business requirements. **To have security but not meet needed**

levels of service or to meet the needed levels of services without adequate security and auditability just isn't good enough. You've got to do them both and do them well, i.e., *serve* applications and data and *protect* them, the users, and your infrastructure.

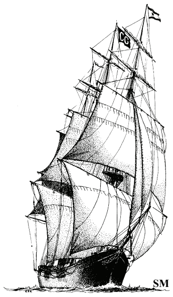
Some Guidelines to Begin Your Journey

1. **Do you really care about *security?*** Then you must have clear business policies and be able to enforce them throughout your IT environment.
2. **Do you care about *high availability of applications?*** Then you must **secure the container**. Failure to secure the container ultimately will result in application failure, either because of application error or because of spillover from another container's problems.
3. **Do you want *secure container-to-container communication in a high-performance environment*?** Then you need to co-locate related processes. You must consider the performance implications of introducing latency into your most frequent mission-critical application-to-application and application-to-data processes.
4. **Do you care about *controlling, knowing, or logging who is accessing data or an application?*** Then you must be able to log the transaction from originating client or server to the data or application, i.e., end-to-end awareness. It won't do you any good to find out that a process on another server corrupted your data. You need to know who initiated the process, regardless of how many intervening procedures and servers were involved.
5. **Do you care about *securing data in transit?*** Then you must encrypt data in flight. This must be done efficiently, else you will slow all of the involved applications.
6. **Do you care about *secure and manageable key management?*** Then you must consolidate your key management. Having multiple key management solutions ultimately will limit the effectiveness of your controls.
7. **Do you care about *governance at the object level*?** Then you must categorize all objects and metadata and control them accordingly. While categorizing only some of your objects and metadata may be a transitional goal, you can't declare a governance victory by only governing selected objects.
8. **Do you want to *control and audit access to data of many types?*** Then you need digital rights management and/or a well-secured repository to track data use.
9. **Do you want to r*epulse intruders' attempts to go where they are not permitted?*** Then you need real-time intrusion detection. Otherwise, you are just able to report about it after the breach.
10. **Do you want to have the *right level of protection for differing levels of risk?*** Then you first must assess and prioritize your risks and your tolerance for differing levels of risk. It is as important to look at the rewards that greater openness (risk) might bring and the penalties to business of reducing risk by eliminating availability.
11. **Do you want to *control the costs associated with securing, monitoring, and auditing your IT infrastructure?*** Then consolidate, as much as possible, your security infrastructure under a single point of control.
12. **Do you really want to do *cost accounting and chargeback?*** Then you must have secure access and activity tracking. Otherwise, who will believe your accounting data?

Conclusion

You have reached the first milestone in facing the challenge of enterprise security – you have a sense of its scope and importance. What makes this different (than you might have presumed before journeying this far) is that you now understand that simplified, siloed solutions just won't get you where you really want to be.

Fear is a good motivator. Enterprise security is about managing risks that scare you. Hiding from the risks is not the answer, as your business potential will suffer. **Spending on enterprise security needs to be positioned as adjusting for or mitigating the risks for less than one or more occurrences likely will cost you. The key to achieving success is to rely on policy-driven automation.** Whether you choose to do this yourself, get some help, or outsource the responsibility to someone else, now is the time to take the next step.



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

Mike Kahn **is Managing Director and a cofounder of The Clipper Group.** Mr. Kahn is a veteran of the computer industry, having spent more than three decades working on information technology, spending the last third at Clipper. For the vendor community, Mr. Kahn specializes on strategic marketing issues, especially for new and costly technologies and services, competitive analysis, and sales support. For the end-user community, he focuses on mission-critical information management decisions. Prior positions held by Mr. Kahn include: at International Data Corporation - Director of the Competitive Resource Center, Director of Consulting for the Software Research Group, and Director of the Systems Integration Program; President of Power Factor Corporation, a Boston-based electronics firm; at Honeywell Bull - Director of International Marketing and Support; at Honeywell Information Systems - Director of Marketing and Director of Strategy, Technology and Research; with Arthur D. Little, Inc. - a consultant specializing in database management systems and information resource management; and, for Intel Corporation, Mr. Kahn served in a variety of field and home office marketing management positions. Earlier, he founded and managed PRISM Associates of Ann Arbor, Michigan, a systems consulting firm specializing in data management products and applications. Mr. Kahn also managed a relational DBMS development group at The University of Michigan where he earned B.S.E. and M.S.E. degrees in industrial engineering.

- ***Reach Mike Kahn via e-mail at MikeKahn@clipper.com or via phone at (781) 235-0085 Ext. 121. (Please dial "121" 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***, 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.