Massachusetts
Institute of
Technology

Online Gated Communities

Architecting Secure Extended Enterprises

Daniel J. Greenwood, Esq.

Issues Overview White Paper of the MIT E-Commerce Architecture Program
http://ecitizen.mit.edu, Comments to dang@mit.edu

Communicator Inc

Made possible by the support of Communicator Inc

1. Introduction

There are, today, pressing fiscal reasons for corporations and government entities to work more closely with partners, contractors, suppliers, customers or citizens and others via the Internet. Successful enterprises must be able to instantly, securely and reliably connect the right people together with each other and with the right information and processes. This must be done, however, while protecting the organization's networks, data and online operations.

Through a dizzying patchwork of approaches, including pinpricks through firewalls, special virtual private networks, elaborate "DMZ" alleys for staging area applications and servers, and many other creative measures, companies have been struggling to open access. One of the common threads through all these attempts is that they are almost all tailored to a given group of people using specially designated systems and methods that have not scaled to a broader array of applications and users. The management of these varied short-term measures is itself becoming a security and cost center problem.

The market is demanding easier, more scalable, less costly and more comprehensive solutions. In response to this need, various consortia have developed suites of technology standards for security and transactions, and a myriad of hardware and network layer offerings. Perhaps the most relevant emerging standard is the Liberty Alliance specification, supported by American Express, GM, Nokia, Sony, Novell, Communicator Inc, Trustgenix and others. But the technology standards alone are merely tools without a blueprint to guide them. "Gated community" solutions can provide the framework and operational functions necessary to extend the enterprise while protecting the borders. This approach to extending the enterprise and bridging systems among different organizations provides a powerful and elegant balance of strategic and security needs.

2. Hardening the Walls Vs. Extending the Enterprise: Vantage Points on the Problem

This paper focuses on the problem of extending an enterprise by opening systems and operations up to remote employees, business partners, customers, suppliers and others — while at the same time maintaining or tightening security and risk management to protect the organization's assets. The online gated community is a way to address the dilemma of proliferating heterogeneous networked systems and user identity schemes. Existing information technologies and new types of network service providers enable gated communities and cross-boundary business integration as a solution. Such business opportunities provide avenues for direct cost reductions, greater productivity and new revenue sources.

Defending the Gates: Information Security and Assurance

Today, an organization can be defined by its information networks. The digital enterprise comprises the constituent users (employees, customers, partners, etc.), their communications and transactions. The boundary of the electronic environment is the boundary of the business.

Threats to the digital enterprise are tantamount to threats to the business or government unit itself. Strategic objectives require ever more porous boundaries in the network – opening holes and connections for all manner of external users and applications. Consequently, the job of protecting the enterprise becomes more urgently difficult.

From the perspective of information security and assurance, it is common knowledge that barriers to access are good. In selecting the most efficient and lowest risk methods to cross these barriers, it is useful to review the purposes they were erected to achieve. These barriers exist to assure valuable resources are accessible only to authorized users: intellectual property is tied to licensed users, trade secrets and sensitive communications are strictly limited to insiders, and transactions are conducted only with customers under contract, among other reasons. Of course, they also serve the purpose of maintaining walls and watch towers against wrongdoers of various ilk, from petty thieves and hackers to threats against national and economic security.

Extended Enterprise: Greater Revenue, Productivity and Cost Containment

Clearly, bringing systems and people together from different organizations inside or beyond a single business or government is a "must do", not a "nice to have", based upon the new requirements of the information economy. While business lines blur, hardening the critical information and network systems underlying these interactions becomes more important now than ever before. There needs to be a way to openly connect people to processes and devices across organizations, while avoiding additional exposure to attacks or creating other vulnerabilities.

As organizations attempt to strike a balance between conflicting security and business needs, both the public and private sector also have an economic imperative to apply solutions that will bring down costs, enhance productivity and enable greater revenue. Technologies that permit the right connections and information sharing between the right people at the right time can dramatically enhance productivity. More importantly, extending the enterprise to bring customers, buyers, suppliers and other economic partners in closer interoperation can speed recognition of and open new channels for revenue, and can also reduce transactional drag and other inefficiencies.

Wherever practicable, however, organizations need to extend the useful life of existing technology systems. The last several years have seen an unprecedented outlay of money, dedication of staff and other resources focused on acquisition of new technologies both in government and throughout the private sector. Plans that call for the tearing out of existing systems that are still operating well for their intended purpose have the effect of increasing costs. Sometimes this is necessary, but technical architectures that allow continued use of backend and other systems over a longer period, while still achieving strategic business goals, are preferred.

3. Online "Gated Community"

An Online Gated Community addresses the challenges and balances outlined above. Such a community is comprised of users who are members of different organizations – within or outside a given enterprise. These users are virtually connected with each other while securely and reliably excluding unauthorized users and other intrusions. A digitally networked gated community can be as large or larger than a nation-state, or as minute as a handful of small businesses or smaller, and may be home of many different types of people and activities. But the gates represent a boundary inside of which a common code exists. Common codes of conduct, commercial code, and computer code, when properly applied, blur together into community. The notion of a common code inside a bounded community allows for open, high velocity, and creative styles of interaction inside the gates.

The secure electronic boundaries, because they are manifested technologically, can cut across organizations, enterprises, and geography, bringing together exactly the right people, processes and information. But the technology only supports and reflects the real boundaries, which are expressions of business, policy and legal agreements to cooperate across organizations, tied directly to practical goals and objectives. This can be thought of as an "open but bounded" system, because clear, enforceable boundaries allow participants to form real-time, lower risk and faster transactional relationships with others on the inside.

The concept of a gated community is distinct from other methods of connecting users securely. For example, technology offerings called "virtual private networks" or "value added networks" focus upon securing particular parts of the connection between users, devices and networks. They focus upon encrypting and authenticating end-points over protocols like "IPsec" and "SSL" (common security technical specifications). While very useful, these approaches are very different from the online gated community solution. The gated community approach directly addresses the multi-faceted needs of users to work together in an extended enterprise. A gated community includes adequate technical security, but also supports other functions and components, resulting in a flexible, scalable and safe cross-organizational environment of users.

4. The Five Building Blocks

The basic building blocks of an online gated community include:

- **Identity Management, Authorization and Workflow:** The ability to easily designate users as "in" or "out" of the gated community, to synchronize user identities from across the community, and to maintain simple and community-wide management controls for identity creation, change and closure. The system rules and practices defining user authorization, task sequence and process paths are thereby enabled. This simplifies the log in experience for users spanning organizations inside the community. It also makes administration of individual user accounts and options manageable. This building block is discussed in more depth in the next section.

- **Messaging, Presence and Collaboration:** The ability for any users inside all the affiliated organizations to "see" each other, to communicate and to form small self-clustering groups of users to regularly or spontaneously collaborate together. This suite of closely related functions bridges the gap between individuals across the larger bounded community. The capacity to securely and instantly open a channel for talk, data sharing, collaboration and group discussion marks a key difference between the online gated community and ordinary corporate web sites. Typically, it is not possible for any given user even to be aware of how many or which other users might be at the same web site, much less to reach out and communicate with others. To assure efficient knowledge transfer and group work, these features are fundamental. This topic is also discussed in more depth later in this paper.

- **Content Aggregation:** Simple ways to deliver streams of content from heterogeneous sources inside the gated community to authorized users across the gated community. In an online gated community, content aggregation provides the users with context sensitive flows of information based upon their needs and their relationships to others in the community. By establishing a gated community, it is possible to maintain a balance between the safeguarding of proprietary information and its accessibility to those who require it. This balance is set by the rules governing the community and enforced by the technical and legal infrastructure. The architecture of such a community, enabled by the technologies that give it life, allows for information to flow from any part of any participating organization to any person under the tent, whenever and wherever they seek it.

- **Security, Compliance and Audit:** The capacity to administer and closely track activities, usage and access to all systems and applications within the bounded community. Those administering this building block assure high security, appropriate notifications, auditability, archiving and regulatory compliance. This includes appropriate use of encryption and authentication technologies, as well as intrusion detection and internal controls. Selection of appropriate technologies and standards is a key element, but is hardly sufficient to achieve security. The softer actions, such as assuring internal personnel controls to reduce the risk of insider attack are equally important. The agreements governing risk allocation, including insurance, and dispute resolution, are also key to understanding the overall threats and countermeasures of the community. At the highest and most abstract level, the cost, benefit and risk judgments driving security measures are a matter of executive decision-making at the governance level of the community.
- **Governance:** The organization and process by which the rules and executive decisions affecting the online gated community are made. Through policy, operating rules and other such instruments, the governing body sets the rights, responsibilities and roles of every user within the boundaries of the community. A representative body of stakeholders and decision-makers inside the gated community exercise this responsibility. In essence, the role is to govern the operations, set risk allocation, dispute resolution, other rules and determine strategic direction. This creates the "boundedness" members rely upon, enabling a predictable and enforceable framework supporting their activities and transactions. In determining which members will participate in governance, and to what extent, factors might include financial support of the community, liability exposure or whether they bring necessary information or users. The affiliated enterprises retain their own governance and autonomy.

Another important factor to consider is the need for an "Independent Service Provider". This is not a generic building block for all gated communities, because in some centralized communities, there may be an in-house and non-independent department that actually provisions and delivers the services. However, in an environment where there are multiple organizations with comparable negotiation power or authority, there will frequently be a need for an agreed upon trustworthy independent party, to administer and host the cross-organizational services. This third party is not like an authority or direct stakeholder with commensurate governance power, but rather is a highly reliable and trustworthy contracted service that communicates, implements, and enforces consistent rules by which the community operates. There are many examples of third party network application providers that handle very sensitive, high value and mission critical information and transactions for extended enterprises, including Salesforce.com (managing sales, marketing, and customer service and support operations), Communicator Inc (managing secure cross-enterprise identity management and communications), Recruitsoft (attracting, hiring, retaining and deploying employees), SAVVIS (managed hosting and IP VPN for mid-sized companies) and LextraNet (managed hosting and robust collaboration tools for multi-party large scale litigation support).

5. Identity Management

The first building block, Identity Management, deserves a deeper treatment. The proliferation of user accounts across networked systems is creating a security problem, because it invites users to keep their various passwords in handy locations. In addition, the current trends are quickly moving toward a ceiling in terms of available business channels and partnering opportunities. The overhead of administering too many systems becomes a hard stop to new business arrangements. Pressure to provide simple to use, yet secure ways for users to sign into the various systems behind the gates is significant.

This means better “Identity Management” solutions are needed. The concept of a “single sign-on” technology has been bandied about for many years as a proposed technical response to this need. However, the typical underlying assumed business model supporting single sign-on is a centralized, hierarchical organization. This approach is an especially poor fit for most organizations today. Hierarchical structures are even harder if applied to multiple networked enterprises that must cooperate with, rather than command, each other.

One way to cut the problem is to view “Identity Management” as a means of determining who is “inside” vs. “outside” the community of authorized users of a business system, and the ability to easily add new communities into the fold while making the intersections between affiliated communities transparent to end-users. In this way, it is possible to rapidly create new business combinations among partnered organizations, clusters of customers and suppliers. Identity management solutions also provide a way to keep up with the dynamically changing internal employee and contractor environments, ever subject to reorganization, mergers and other recombination.

Conceptual Approaches to Identity Systems Across Boundaries

Conceptually, there are three basic ways to achieve identity management:

1. Decentralized self-clustering of individual people (PGP “web of trust” model)
2. Centralized organizations of people (“command & control” model)
3. Decentralized federated organizations of people (“Liberty Alliance” model)

Bottom-Up Systems: The dream of totally decentralized systems of individuals who aggregate themselves in self-clustering webs of trust has not been demonstrated in a scalable, affordable and reliable manner. One could say that the “buddy lists” supported in public Internet Instant Messaging applications are examples of peer-to-peer bottom-up self-clustering groups. Similarly, the PGP digital signature and key chain system permitted the “web of trust” model, wherein individuals could compile a trusted address book, and share entries with other individuals. Other types of anarchic systems have also been tried. These systems are interesting in that they are completely citizen/consumer centered, but their scalability and applicability to sound business models remain to be proven.

Command and Control Systems: Within a single enterprise of clear hierarchical lines of control, it is possible and frequently advisable to simply require a single centralized system. However, large organizations in the private sector and in the government world are seldom structured that way. The organizations are large, pluralistic and complex. Despite the appearance of a single authoritative decision-maker at the top of an organizational chart, like a CEO or a Governor, it is difficult or impossible to force a single digital identity solution across the enterprise.

Inhibitors to forcing a single central digital identity system include entrenched but incompatible practices across lines of business, non-interoperable internal legacy systems and data models, and interdependencies with different external systems. For a variety of reasons, people develop settled cultures around particular ways of doing and naming things. Other challenges to centralized single systems include the additional security vulnerabilities associated with systems monoculture, core choke points and other points of failure, and stunted innovation.

However, this approach may be appropriate where the organizational lines of command can support a single, centralized system and where there is a business need to exact uniform lines of control and homogeneous back-end systems and business methods. In certain limited cases, the significant increase in costs necessary to force different organizations to fully adopt an identical approach is warranted.

Federated Systems: The federated approach can be thought of as a mosaic. It requires agreement across agencies, departments or enterprises about process and use of bridging technology to make identity management work. But there is no need for all parts of the federated extended enterprise to use the same back-end technology or practices. In a federated system, each part of the larger gated community can continue to do things its own way and use its own legacy systems, while the connecting technology and standards provide the bridges. In this way, the cost of scaling or re-combining different constituent organizations is kept low. No tearing up of legacy systems, business practices and cultures is necessary. But the benefits of open connections inside the new boundaries of the gated community are still available.

6. Bringing People Together: Presence, Communication and Collaboration

The second building block, "Messaging, Presence and Collaboration" also deserves deeper treatment. Creating gates and boundaries does not, in itself, create community. Shielding insiders from outsiders is necessary, but insufficient to yield the true benefits of a gated community. The ability for those inside the affiliated organizations to see each other, communicate, share access to resources, and form small working groups is critical. There is precedent for the creation of successful online communities of various degrees of functionality. Successful online communities all share several traits: they provide space for users to cluster based upon their own areas of interest, they provide some form of "presence" awareness so that users know when their associates are online, and they enable users with no prior relationship to meet and become acquainted inside the safety and context of the gated community.

There are "moments of value" in any transaction, such as when a contract is finalized, a decision is made, or important information is received. Strategic use of instant messaging and collaboration applications within a gated community can be a key method for enhancing that value. For example, through the process of a large business to business or government procurement, the ability to remain in close contact with the appropriate sales, management and technical staff at each organization can reduce the time to implement, more rapidly surface issues, and deepen knowledge transfer and requirements setting.

In the context of public sector domestic security, one can imagine personnel being far more efficient at guarding the homeland thanks to the real-time connections to the right people in affiliated public safety, law enforcement and intelligence communities. The ability to have access to the vast array of information known throughout government can make the difference for those in the field making quick decisions. To support these and other types of strategic uses of messaging and collaboration, organizations could designate certain employees as "on deck" to field certain types of interactions, as needed. With relatively little change in staffing, bringing the right people together in a secure and spontaneous fashion can dramatically increase mission success and revenue opportunities, as well as reduce costs and other delay.

The notion of "digital presence" is perhaps one of the most important and fundamental technical underpinnings of online community. Networked community architectures suggest that knowledge should flow when, where and to whom needed in the same way information fires across synapses in a brain. People with an interest in certain types of information gain easy access to it based upon the seemingly serendipitous connections with like-minded people. People are excellent conduits of information, and naturally convey whatever is relevant to their peers. Linking people with related interests together globally in an organized yet flexible online community allows, for the first time, knowledge to flow with nearly no friction from geography or social boundary.

7. Online Gated Communities in the Public Sector

There are many government initiatives today that could leverage “Community” solutions to great effect. Clearly, there are effective applications of this solution in the public sector ranging from coordinated provision of services to beneficiaries of several government programs, to ease of use for regulated companies dealing with an array of oversight agencies at all levels of government. But domestic security presents one of the most difficult and pressing needs for the benefits gated communities can yield. For example, imagine the following scenario:

A lone law enforcement officer (whether police, U. S. Coast Guard, or otherwise) happens across a suspicious looking situation at a port. A suspicious vessel or activity triggers an initial on-the-scene inquiry. Upon seeking the identity of one of the parties, the law enforcement officer will need a rapid and effective method of validating that identity, determining if that identity is on any known watch list or otherwise presents obvious issues for follow up. In addition, gaining some knowledge of the business or manifest of the vessel or the stated activities of the parties can trigger still other opportunities to verify the information and establish whether there is a potential urgent intervention needed, or other less pressing government intervention

Technically, the process might include establishing a real time link to relevant agents or other employees from different parts of government, each with access to parts of the information and analytical puzzle. This might include creating an ad hoc forum in which appropriate staff resources can congregate in support of a single emerging event in the field or among analysts. In the forum, users would already have a high degree of certainty that the other users are who they claim to be and that they are the appropriate people in their organizations. This is due to the inherent properties of identity management inside a gated community. In addition, the forum could house personnel from different organizations, who connect using very different systems in the back-end and via different networks. The forum can provide an easy way to get current telephone numbers, as needed, to talk directly, and can support inside the online channel a chat interface and sharing of data through direct links or otherwise.

Of course, other less dramatic but also critical components of homeland security will include bringing many relevant but heterogeneous organizations together, both inside and beyond the boundaries of the new Department of Homeland Security. This will include the ability to coordinate large installed user bases, leverage common network services, and open access to resources inside the larger organization to those both inside and outside the Department who need it when they need it. There are also opportunities to create economies of scale in a gated community inside the new homeland security “community of communities” without the need for ripping out legacy systems or unnecessarily forcing together practices and organizational cultures.

This is a good example of an environment where there may be opportunities for both centralized systems and also a keen need for federation. Federation will be especially useful as a technical and governance framework when federal and state homeland security communities begin to integrate their systems, interactions and communications more closely. Under the U.S. constitutional system, a single centralized system of command and control is not appropriate for systems spanning federal and state boundaries.

8. Online Gated Communities in the Financial Industry

In the private sector, the financial industry presents powerful opportunities for the use of online gated communities. The current state of affairs in this industry, resulting from competition, globalization, customer demands, regulatory requirements, and risk management needs are a good fit for the structure and benefits of online gated communities.

Taken as a whole, no other economic sector is further along the technology adoption curve than the financial industry, with information systems permeating nearly every aspect of the business. However, as is common across the economy, the systems are of different types, frequently require different methods of use, and are of limited interoperability. Another important aspect of the financial industry is that it is better understood as a series of industries, variously overlapping or disparate. From retail banking with individual consumers, to commercial transactions to institutional investing to bank-to-bank transfers and far beyond, the business models, practices, applicable regulations and market needs of the varied sub-sectors within the financial industry are broad indeed. As such, the financial industry is well suited for the online gated community architecture – allowing each well-defined community to cluster.

Despite the fact that the financial industry is actually a "community of communities", it is nonetheless useful to consider it as an industry with many commonalties, including:

Globalization and ever-larger conglomerations of financial services companies are creating a new market playing field, with new pressures to compete and to cooperate. The new market reality is that companies must be faster, leaner, better coordinated and more flexible. At the same time, they are getting bigger, more complex and juggling more lines of business. Online gated communities can be used to help members of widespread business units share information, leverage central services, and connect to common customers. The architecture of these extended enterprise solutions also fits well with the business models of partner organizations that may need to federate rather than merge in order to cooperate in a given environment while maintaining autonomy in other arenas.

Customers across the sector are getting more sophisticated and demanding higher quality and better-coordinated services. The commoditization of many types of financial services makes competition across the industry more pressing than ever. Meanwhile, customers are starting to balk at the proliferation of passwords and non-synched systems that comprise their workday. As other industries begin to provide more seamless, coordinated and high quality online services to customers, they start to expect the same state of the art offerings from every sector. This introduces yet another form of competition, across otherwise non-competing industries, to satisfy customer service expectations. The online gated community allows end-users to see a portfolio of their various accounts and relevant points of contact across an enterprise, much like a customized portal.

Regulatory requirements across the financial industry have long separated this sector from others, and have recently taken on a new relevancy and urgency in terms of information technology. Legal rules with specific impact on technology systems in financial services include a raft of new "Know Your Customer" and "Anti-Money Laundering" requirements emanating since the attacks of September 11, 2001, the Sarbanes-Oxley statutory and emerging regulatory requirements for new types of reporting and compliance related to financial statements and internal controls, and various consumer protection and privacy requirements addressed to special electronic consumer notices, disclosures and internal processes. The drive toward more corporate transparency and accountability in the wake of the Enron, MCI and other large-scale scandals has been a driver of new legal requirements. The auditing, archiving and security features of online gated communities are well attuned to the new regulatory requirements and risk management needs affecting the financial sector.

Envision the following scenario: After speaking to a large client, a trader seeks to quickly conduct three transactions at three different financial institutions. To take advantage of prevailing market conditions, it is necessary for this trader to act as quickly as possible. The lag time introduced by having to log in to three different systems, while acceptable in other circumstances, may be a severe obstacle in this situation, with measurable economic consequences. Traders have been known to keep the passwords to various trading systems in plain view, believing the savings in time and resulting ability to get a better deal is well worth the potentially increased risk. Security should always safeguard but not unduly hamper legitimate lines of business. The ability of this trader to securely and seamlessly gain access to all trading systems participating in a broader online gated community would be a win for every participant.

This sort of scenario has already taken hold with great success for other transactions within the financial industry. In 1999, Securities.Hub addressed the challenges confronting Wall Street with a federated Online gated community solution. The resulting community, SecuritiesHub, (owned by Citigroup, Credit Suisse First Boston, Goldman Sachs, JPMorgan Chase & Co., Lehman Brothers, Merrill Lynch, Morgan Stanley, UBS Warburg, and Communicator Inc) is a leading provider of financial information to the fixed income online community. SecuritiesHub co-mingles more than 800 analysts and trader's daily news and research, bond market prices and data from Wall Street's eight leading dealers. Over 24,000 institutional investors from more that 60 countries currently use these services, making SecuritiesHub an excellent example of successful online gated community.

Online Gated Communities can provide the tools and the models necessary to solve the emerging requirements facing the financial industry by enhancing speed and access to critical information and systems across increasingly competitive global markets. Allowing coopetition among a diverse group of participating organizations, while yielding the ability to create a "community of communities", makes this architecture a good fit for the financial sector.

9. Online Gated Communities in the Pharmaceutical Industry

The pharmaceutical industry, sprawling and diverse as it is, is essentially about the business of creating and selling chemicals. The search for "New Chemical Entities" (NCE) has intensified, as competition and change in the pharmaceutical industry has heightened. Much depends upon research and development, and the economics of this industry reflect this fact. The pharmaceutical industry has one of the highest ratios of research and development to sales of any economic sector – equaling as high as 1/5 total sales. The factors that determine success in R&D revolve around capacity for collaboration, communication and coordination among partnered research organizations.

Mergers and acquisitions are one of the major trends over the last several years in the Pharmaceutical Industry. The industry giants have become ever larger, while smaller niche players continue to be acquired. Meanwhile, even as the bulk of the large industry players increase, the commercial output of the newly aligned companies has actually been less than the combined number of products commercialized by the individual organizations prior to the mergers. Meanwhile, the race to find NCE's is hastening. Exacerbating the competitive challenges are the advent of more complex technologies, changing regulatory environments, and ever-smaller periods of exclusivity for new compounds which further fuels the need to reduce the time-to-market. Under these circumstances, the pressure to assure more efficient and effective work among employees and other affiliates is urgent.

Pharmaceutical companies rely upon tight working relationships among many partners and affiliates in the research, development, marketing and sales cycles. During R&D, Contract Research Organizations (CRO) and globally sprawled labs within the newly enlarged corporate structures all must work in close connection. CRO's are being used increasingly to off-load some of the labor and computationally intensive work of quickly moving new compounds through the pipeline, and more rapidly ruling out those that are unsuitable. The scale and complexity of the interlocking research initiatives across affiliated universities, private CRO's and numerous internal labs and research units in the pharmaceutical sector presents one of the most difficult management problems in today's economy.

The utility of an online gated community in this market is compelling. Among other benefits, the gated community structure provides:

- Collaboration that works well for small partnerships between labs at a large pharmaceutical company and a small university professor's lab as well as scalability to meet the needs of large global joint development agreements among several parties;
- Access to new and relevant content, with news feeds, competitive intelligence and research materials pushed to or pulled by the people who need it, when and where they are;
- Security and reliability to protect the trade secrets and other intellectual property of the participating organizations, while at the same time encouraging cooperation and sharing among all those who need to know it.

From the vantage point of larger players, online gated communities address the need to better manage and coordinate highly cooperative yet organizationally and geographically dispersed units. From the point of view of smaller organizations, the ability to reduce transactional friction and lag between their outpost and the rest of the community is an advantage. In addition, it provides simple ways for smaller players to manage affiliations with more than one pharmaceutical company alliance. Finally, the capacity to be in contact across functional units with the people and knowledge needed at clutch times in the invention process is one of the most important factors leading to successful research.

The adoption of online gated communities in the pharmaceutical sector would enhance the manageability of the existing alliances. In fact, the existing business model, relying upon many different organizations within a given pharmaceutical company and external enterprises as well, is a perfect fit for the architecture of online gated communities. And the resulting up-tick in communication, collaboration and coordination among these organizations would directly address the competitive pressures in R&D characterizing this industry.

10. Conclusion

Across the public and private sectors and throughout the emerging information society, the pressures to enable secure yet open access across organizations are growing. Organizations must balance the protection of sensitive, high value and mission critical information and systems against the imperative to open access to a growing and diverse set of people, processes and devices across enterprises. Online gated communities offer a reliable, efficient and scalable means of achieving this balance. In addition, when applied in a way tailored to the context of participating organizations, online gated communities can qualitatively enhance existing work channels by unleashing the genius of individuals and teams – free to collaborate, learn, transact and innovate.

About the Author:

Daniel Greenwood, Esq. has been a lecturer on eGovernment and eCommerce policy and information architecture since 1997 at the Massachusetts Institute of Technology (MIT) School of Architecture and Planning, most recently teaching in the MIT Media Lab. Since 1999 he has also served as the Director of the MIT eCommerce Architecture Program (http://ecitizen.mit.edu/).

For nearly 6 years, Mr. Greenwood served as Deputy General Counsel for three Chief Information Officers of the Commonwealth of Massachusetts, concluding his government tenure as Acting General Counsel. Daniel Greenwood has testified several times before the U.S. House and Senate on matters of electronic commerce, electronic signatures and public policy in a federalist system. Currently, in conjunction with his academic practice, Mr. Greenwood consults to government and private companies on authentication and electronic transaction systems, policy and law in association with the CIVICS.com consultancy, which included his appointment as a Special Deputy Attorney General for Electronic Authentication in the State of Idaho and various other engagements with Fortune 500 companies and public sector entities.

Mr. Greenwood also serves on the Boards of Directors of various eBusiness and eGovernment related trade and technical associations, chairs the eContracts Technical Committee of OASIS/LegalXML, and chairs various committees and task forces dealing with information security, business automation and public policy for Bar Associations at the state and national levels. Daniel Greenwood serves as an e-arbitrator under the Internet Corporation for Assigned Names and Numbers, where he arbitrates Internet domain name disputes. Mr. Greenwood has also developed legal processes for online mediation used by eBay and others. Mr. Greenwood is a frequent speaker appearing on national television, the Wall Street Journal and other media on policy, technology, and strategy related to eGovernment and eBusiness.

About MIT:

Massachusetts Institute of Technology — a coeducational, privately endowed research university — Is dedicated to advancing knowledge and educating students in science, technology, and other areas of scholarship that will best serve the nation and the world in the 21st century. The Institute has more than 900 faculty and nearly 10,000 undergraduate and graduate students, and is organized into five Schools — Architecture and Planning, Engineering, Humanities, Arts, and Social Sciences, Management, and Science — and the Whitaker College of Health Sciences and Technology.

The School's activities range widely across architecture, urban studies and planning, real estate, media arts and sciences, and the visual arts. The School values design excellence, technological inventiveness, and imaginative scholarship, and believes that design and policy interventions should be grounded in unwavering commitment to equity, social justice, and making a positive difference in the everyday lives of real people. The MIT E-Commerce Architecture Program (eCAP), at ecitizen.mit.edu, is an initiative to explore the legal, business, policy and technical inputs to information architecture of eGovernment and eBusiness.

Attributions:

A draft of this White Paper was presented for comment at the Kennedy School of Government thanks to the gracious support of Professor Jerry Mechling.

This work was made possible by the support of Communicator Inc

Communicator Inc

About Communicator Inc:

Communicator Inc (www.communicator.com) is pleased to sponsor the MIT White Paper, "Online Gated Communities: Architecting Secure Extended Enterprises." Communicator Inc provides **communication, community and content solutions** that address the business and technology challenges of the extended enterprise.

Companies and government organizations often have difficulty securing their communications and access to information across disparate systems, and managing identities of individuals, employees, customers and partners. In addition, multi-enterprise communities introduce security and compliance challenges that fundamentally cannot be managed internally by any one of the participating organizations. Communicator Inc, through its **technology and managed services** approach to federated identity management, content aggregation and real-time messaging, acts as a neutral third-party, connecting the right people to the right information in real-time.

Communicator's suite of technologies and services includes:

- **Hub ID**, a secure identity management service that consolidates administration and lowers the cost of managing personal identities, for applications including cross-enterprise sharing of employee and customer data, consolidation of directories and single sign-on.
- **Hub Content & Portals** is a secure, multi-enterprise information management service that excels at aggregating and rationalizing documents and data from numerous sources, delivering it through decision-making applications and web portals, and linking users back to the information providers.
- **Hub IM**, a secure instant messaging and collaboration service that accelerates decision-making by combining instant messaging, group discussion forums, an organization or industry contact directory, and instantaneous information and news delivery.

Communicator Inc solutions serve over 100,000 business professionals across thousands of organizations. For more information, call 914-872-2800, email info@communicator.com or visit www.communicator.com.