

WHITE PAPER: SECURITY MANAGEMENT

IT Security Management as a Business Enabler

MARCH 2007

Sumner Blount

CA SECURITY MANAGEMENT

Table of Contents

Executive Summary	1
SECTION 1: CHALLENGE	2
Issues Surrounding Security Management	
SECTION 2: OPPORTUNITY	2
Requirements for Effective Security Management	
Business Opportunities from Security Management	
Operational Efficiency	
Risk Mitigation	
Enhanced Compliance and Auditing	
Security Management as a Business Enabler	
Customer Acquisition	
Improved Customer Relationships	
Enhanced Business Credibility and Customer Confidence	
New Partner Business Models and Opportunities	
Identity Federation in Use	
Increased Business Agility	
SECTION 3: BENEFITS	11
The Business Impact of Security Management	
SECTION 4: CONCLUSIONS	11
SECTION 5: REFERENCES	12
SECTION 6: ABOUT THE AUTHOR	12
ABOUT CA	Back Cover

Executive Summary

Challenge

IT security organizations must manage risk, meet regulatory compliance requirements and fulfill user needs, all the while working to constantly reduce costs. But IT security can do much more than “keep the bad guys out”; IT security can “securely let the good guys in,” thereby helping to enable critical business initiatives.

Opportunity

Effective IT security management is based on a comprehensive and integrated strategy that includes three major components: Identity and Access Management (IAM), Security Information Management (SIM) and Integrated Threat Management (ITM). Properly managing all three of these core requirements, in an interconnected way, can help you to more easily and effectively grow your business and strengthen relationships with customers and partners. Specific benefits can be achieved in the areas of Operational Efficiency, Risk Mitigation, Compliance and Auditing, and Business Enablement.

Benefits

Comprehensive and integrated IT security management can:

- Help speed the development and deployment of new applications
- Provide a consistent and positive online experience for users inside and outside the enterprise, improving overall satisfaction and loyalty
- Strengthen customer confidence that confidential information will be properly protected
- Expand and more tightly integrate your partner ecosystem and supply chain so you can greatly extend the services available to your online users and partners
- Create a more agile enterprise that can respond more rapidly to threats and opportunities

SECTION 1: CHALLENGE

Issues Surrounding Security Management

In today's business environment, with the amount and type of sensitive data managed by organizations, security stands out as one of the most pressing IT concerns. IT security groups must effectively manage their costs while reducing IT risk, meeting regulatory compliance requirements, and fulfilling the needs of all IT users — employees, customers and partners. They must accomplish this in the face of old, new and emerging threats, attempts at unauthorized access (intentional or otherwise), as well as a constantly changing and usually growing user population.

Many organizations are currently managing security in application “silos” — highly targeted security implementations that are not consistent or integrated across the enterprise. This approach often involves the use of “point security” for specific problems, but does not provide a holistic approach for centralized security management. It may provide short-term benefits to a particular department or business unit, but this is often at the expense of future IT efficiency and effectiveness at the enterprise level.

A holistic and integrated approach to security management enables organizations to understand their security environment in all its complexity. Raw security data can be turned into actionable information, and critical IT assets and services can be protected against improper access across the entire environment.

In this type of environment, IT security can make a measurable contribution to the business initiatives of the enterprise. But this is still an opportunity that is often underemphasized during IT security planning and resource allocation. This paper provides a point of view on how effective IT security management can help enable growth for your enterprise.

SECTION 2: OPPORTUNITY

Requirements for Effective Security Management

As an organization expands its assets and increases its exposure to a variety of users — including employees, partners and customers — a patchwork approach to security management controls is no longer adequate. Instead, organizations require a comprehensive solution that allows proactive management of their security environment.

An effective security management solution consists of three primary functional areas:

IDENTITY AND ACCESS MANAGEMENT (IAM) Create and manage user identities, their accounts and access entitlements, and enforce access policies across the environment.

SECURITY INFORMATION MANAGEMENT (SIM) Aggregate, filter and provide reports and analysis of all security-related events within the environment. An effective SIM solution also provides full auditing for provable compliance.

INTEGRATED THREAT MANAGEMENT (ITM) Identify and combat electronic threats such as viruses, spyware, spam, etc.

A complete security management solution must provide capabilities in each of these three critical areas, as illustrated in Figure A. As you can see, all of these areas of security management contribute to the creation of a strong security and compliance environment. However, many of these components, especially IAM, provide capabilities to help strengthen current business relationships and create new ones, thereby expanding growth opportunities. The next section explores the major benefits provided by integrated security management, followed by a broader discussion on enablement of business growth.

FIGURE A

An effective, enterprise-wide security management platform requires the integration of these three key areas of security management.

AREAS OF SECURITY MANAGEMENT



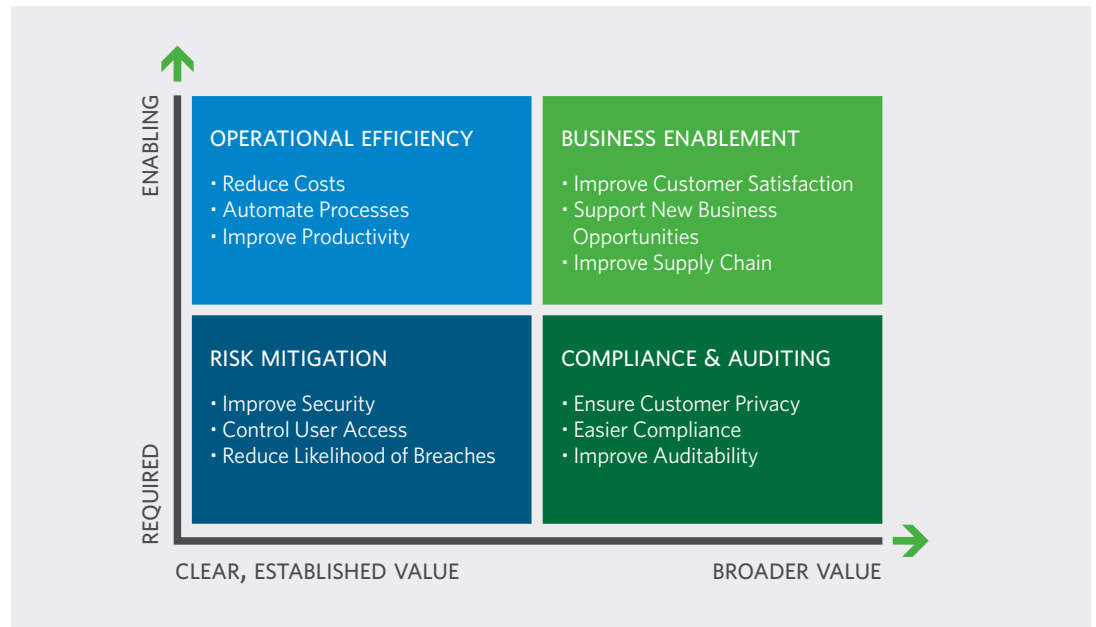
Business Opportunities from Security Management

A comprehensive and integrated security management platform can provide a number of important opportunities. The following graphic (Figure B) illustrates four of these, and places each one along a continuum of established vs. broader value (the horizontal axis), and required capability vs. enabling capability (the vertical axis). A “broader value” opportunity is one that has impact beyond its specific scope. For example, compliance activities can have significant benefits far beyond merely complying with the requirements of each regulation.

FIGURE B

Integrated security management platforms can pose opportunities in reduced risk and improved operational efficiency and compliance, but those benefits can also be leveraged to drive business enablement.

OPPORTUNITIES RELATED TO SECURITY MANAGEMENT



Let’s briefly review three of these core opportunities that an integrated security management solution can provide. We’ll then explore in more detail how such a solution can actually help to enable the fourth opportunity: the ability to help grow your business.

Operational Efficiency

IT security managers today must not only ensure a secure environment to protect the company’s assets and industry reputation, but they often are being asked to do it at a lower cost than in the past. The pressure on IT to “do more with less” is ever-present and unlikely to change.

The challenge for security managers is to reduce the total costs of their IT operations and infrastructure, and to improve the productivity of everyone who uses it, particularly security administrators. An integrated security platform, especially an IAM suite, can provide very compelling efficiency benefits by:

- Centralizing all user identity management, so that IDs and profiles don’t need to be created or managed on multiple systems.
- Centralizing all access management, so that security doesn’t have to be managed in each application or each operating system.
- Automating the provisioning (and de-provisioning) of all access rights and applications to each user. This eliminates the need for administrators to grant this access on each system manually.
- Automating all vulnerability management, so that systems can be updated with patches for the latest vulnerabilities more easily (this is also a very strong security capability).

A white paper called “Reducing the Costs of IT Security Management” is available at: <http://www3.ca.com/solutions/Collateral.aspx?CID=88840&ID=4348>

- Allowing users to create and manage some of their own profile information (such as passwords), so that it doesn't have to be done by administrators or the help desk.
- Allowing some users to be managed by the partners or business units that they belong to ("delegated administration"), so that a centralized administration team doesn't have to manage these users.
- Automating the collection filtering and analysis of security information management. This means that audit logs are aggregated and correlated so that important events are much more easily identified. This provides tremendous savings in time and effort for security administrators, as well as reducing the probability of overlooked security breaches.

Risk Mitigation

One of the most important opportunities related to comprehensive security management is mitigating a range of operational risks, such as hacker attacks, malware, unauthorized access to protected resources and systems, accounts for departed users that are not terminated quickly, abandoned accounts, and security threats that are unrecognized due to the amount of audit log data. Explicit mitigation plans are required to keep all of these risks at an acceptably low level. These threats not only impact the security of critical IT assets, but they also make regulatory compliance dramatically harder. An integrated and holistic approach to managing all of these security threats is essential for an effective risk-mitigation plan.

There are two major areas in which effective security management can provide significant risk mitigation:

ASSET PROTECTION How can you ensure that valuable corporate resources are kept secure and private, and are only available to properly authorized individuals for approved actions? A complete and integrated IAM platform, with comprehensive auditing and logging, can provide this asset protection.

SERVICE CONTINUITY How can you ensure that the services provided to employees, partners and customers are available as needed, with no degradation in quality or level of service? An integrated threat management solution can help to ensure continuity of critical IT services.

Enhanced Compliance and Auditing

Security management is at the heart of many industry and governmental regulations, especially those dealing with privacy requirements. Without a strong security infrastructure that protects systems, applications, data and processes from unauthorized use or access, compliance with these regulations is very difficult.

The key requirement for compliance with these regulations is a strong set of internal security controls. These controls must not only ensure the validity and effectiveness of critical ("material") internal processes and information, they must also be easily auditable in order to prove compliance to internal and external IT auditors.

A complete and integrated security management solution that addresses the three major needs — IAM, ITM and SIM — can help you create strong and effective internal security controls across the enterprise. The result is much easier, as well as much more cost-effective, compliance with all relevant mandates.

A white paper called "Managing IT Security Risks" is available at: <http://www3.ca.com/solutions/Collateral.aspx?CID=82802&ID=271>

A white paper called "The Role of Security Management in Regulatory Compliance" is available at: <http://www3.ca.com/solutions/Collateral.aspx?CID=70177&ID=271>

Security Management as a Business Enabler

So far, we've talked about security management largely in terms of "keeping the bad guys out." In the cases of viruses, hacker attacks and unauthorized access attempts, this is clearly the goal. However, one important (and often underappreciated) opportunity related to integrated security management is "securely letting the good guys in" — and the associated enablement of business initiatives. Effective security management provides the infrastructure upon which you can more easily grow your business. It also strengthens the relationship with existing customers and partners, thereby creating a sales opportunity for additional products and services.

Let's look in more detail at how an organization can use integrated security management to help grow and strengthen its overall business.

Customer Acquisition

Every organization wants to grow its business. You can do this by "selling more stuff" to your existing customers, and by expanding your business to new customers. To do this, any organization must be able to introduce new (and often online) products and services quickly and painlessly.

A key to doing this is a centralized IAM platform, coupled with automated SIM.

This type of solution speeds the development and deployment of new applications through:

CENTRALIZED SECURITY ENFORCEMENT When application authorization is handled within a centralized access management service, authorization code does not need to be developed within each application. This greatly reduces development costs, but also ensures greater consistency of access enforcement across the enterprise since enforcement is not handled in multiple places.

CENTRALIZED ENTITLEMENT MANAGEMENT Managing user entitlements across these newly deployed applications is much simpler when it can be done centrally. Entitlements can be role- or rule-based, and do not have to be created and managed in multiple locations. Applications can be deployed more quickly because creating entitlements is often just a matter of adding a new access policy to one or more already defined user roles.

CENTRALIZED SECURITY EVENT MONITORING Without an effective SIM solution, deployment of new applications can significantly increase the burden of security event monitoring and analysis. Automation of the collection, filtering and analysis of security events makes it much easier to bring new applications to full deployment.

Improved Customer Relationships

Customers today expect high levels of responsiveness and service from the organizations with which they do business. One important way to keep customers happy and loyal is to provide them with an excellent "experience" every time they interact with your company — for any reason. Their experience consists of the combination of all their interactions with your company, and their website experience is certainly one of the most important and high profile of these.

An integrated IAM platform can provide you with the ability to create an effective and improved overall experience for customers. It allows you to leverage the identity (and preference) information that you have for each customer, to provide them with the most targeted and appropriate information for their specific needs. It also makes it easier to navigate across websites in the partner ecosystem, to provide customers with a broader range of services, thereby solidifying their loyalty to your business.

An integrated IAM platform can provide the following capabilities in order to improve your customers' online experience:

A CONSISTENT IDENTITY ACROSS SITES By centralizing the management of user identities, and by using industry standards to communicate identity and entitlement information between partner sites, you can create a seamless experience for your customers. They do not have to re-authenticate or provide profile information as they move from one partner site to another.

PERSONALIZATION Content personalization is at the heart of successful targeted marketing and sales strategies. When you present each user with applications, options and information uniquely targeted to their identity, access rights and preferences, it becomes much easier to upsell additional products and services to them. In addition, when users see information closely suited to their needs, they are much more likely to conduct business or return later for further browsing. Options or applications for which the user does not have access rights can be eliminated, and only the most relevant content can be presented.

SINGLE SIGN-ON (SSO) Users often are frustrated by repeated logins to the applications and sites that they need to access. An IAM platform can provide SSO not only across your own applications, but across partner sites as well, thereby significantly improving the customer experience with those integrated sites.

SELF-SERVICE CAPABILITY Everyone knows the horrors of lost passwords — and how help desks are often flooded by forgotten password requests. IT administrators want to reduce these costs, and customers want to control their own information and get access to appropriate information and applications quickly. Full customer self-service capability allows them to do this, as well as to reduce the administrative expense required to support them. Self-service capabilities typically include self registration, password reset, and requests for access to new applications and services. A robust identity administration solution can provide this capability, which can help keep customers satisfied and “in the fold” during the entire customer life cycle.

INCREASED AVAILABILITY OF SERVICES Users don't return to sites that are not reliably up and running. Continuity of services and applications is therefore critical for ensuring repeat customer visits. When a site doesn't “work” for any reason, customer and partner relationships are threatened. An integrated threat management solution can help combat threats of all kinds (including new and complex blended threats) so that applications and services can be available when your customers need them.

Enhanced Business Credibility and Customer Confidence

In almost all kinds of business, the most important corporate asset is the corporate brand and reputation. Public knowledge of security breaches can have a catastrophic effect on the willingness of the public to do business with you.

An example from early 2006 illustrates this point. When Acxiom (a company that processes credit card information) lost a tape containing customer data, the effect was dramatic.

The direct costs to manage the situation were close to \$1 million, but the effect on the company's reputation was much worse. According to an Acxiom executive, "The cost to your reputation is huge. If customers can't maintain trust in a business like ours, we're out of business."¹

Assuring the privacy of customer confidential information (whether health-related, financial, or other) is critical not only for customer confidence but also for meeting the requirements of various governmental privacy mandates.

Some organizations have adopted widely used IT security frameworks, such as ISO 17799 or CobIT, to create an environment of accepted security best practices. This approach, when used consistently throughout the organization, can help strengthen customers' confidence in the privacy of their confidential information. One essential element of conformance to these security frameworks is a strong and integrated security management solution.

Such a solution can help organizations ensure privacy of customer information, avoid costly and dangerous security breaches, and prevent all types of unauthorized access to critical IT assets. Cutting-edge security practices can enhance customer confidence and protect brand equity.

New Partner Business Models and Opportunities

One of the biggest challenges to the creation and expansion of robust customer/partner ecosystems is the lack of strong, consistent security across these environments. Many organizations would like to tightly integrate suppliers, distributors, outsourcers and other marketing partners into a unified IT infrastructure that allows members of one organization to securely access the applications and information of another.

Identity Federation is a security management technology that enables this business dynamic. It provides the underlying services to allow external identities to be managed, so that information and applications can be shared across partner organizations. This important capability has been defined as "the agreements, standards, and technologies that make identity and entitlements portable across autonomous domains."² Federation is the enabling technology (used in conjunction with related industry standards) that allows creative and sophisticated partner ecosystems to be developed, which can help to drive significant new business opportunities.

There are two basic types of federation — browser-based and document-based. Browser-based federation supports business models where live users travel between websites to conduct business, often unaware of the organizational boundaries of the sites that they visit. Customer identity and entitlement information is passed between these sites transparently to the users, so that they are presented with a seamless and pleasant user experience while getting access to applications and data from multiple organizations.

For a more detailed description of these types of identity federation, please see the "Business Value of Identity Federation" white paper at: <http://www3.ca.com/solutions/Collateral.aspx?CID=66744&ID=4348>

Document-based federation is focused on the use of XML documents communicated between two security domains, both of which are using Web services standards to support this interaction. Documents are created and processed by cooperating Web services located on both ends of the transaction link. A typical example of this type of federation involves large supply chains, in which suppliers and distributors are linked into a common infrastructure in which each participant partner can securely access the other's business information (such as manufacturing production schedules).

Identity Federation in Use

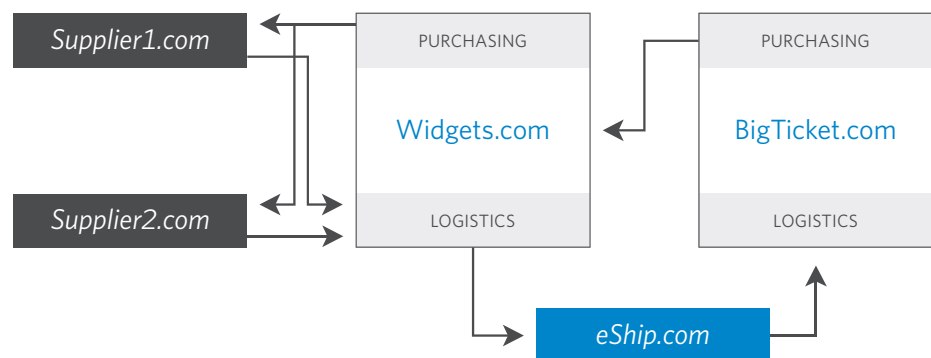
Let's look at a hypothetical use of identity federation to create new business opportunities. This common use of identity federation occurs in manufacturing partner ecosystems, when a company wants to integrate more tightly with their suppliers, distributors, and potentially even downstream customers. Consider the case of Widgets, Inc., a large manufacturer of widgets used in products produced by BigTicket, Inc. Widgets has a number of suppliers that need to be tightly integrated into Widgets's production schedule, as well as their component procurement applications. Likewise, Widgets is a supplier for BigTicket, and therefore needs to be linked into the procurement and manufacturing logistics applications of BigTicket. And, to make it more complex, eShip is a company that does contract shipping for Widgets, and must also be integrated into this efficient supply chain.

Figure C gives a simplified view of these interactions. The Purchasing and Logistics applications exchange identity and entitlement information with the partner websites. The result is that an employee's Supplier 2 identity will be verified and then granted authorized access to the logistics application at Widgets.

FIGURE C

Identity federation can streamline customer/partner interactions up and down the supply chain.

IDENTITY FEDERATION IN THE SUPPLY CHAIN



As we can see from this simple example, a comprehensive identity management solution that includes identity federation can provide very significant benefits in terms of expanding the partner ecosystem, providing new and more integrated services to customers and employees, and greatly improving the overall efficiency of manufacturing supply-chain environments.

Increased Business Agility

The area of security management that is most important in improving the ability to quickly react to industry events is a comprehensive, centralized IAM system. A fully deployed IAM platform allows an organization to more easily and quickly react to growing user populations, requirements for new applications, and changing business requirements or models. This provides greatly increased business agility, and will position the company strongly to react quickly to changing market conditions.

Let's look briefly at some of these elements of business agility:

EASIER MERGER AND ACQUISITION ACTIVITY An enterprise IAM environment supports a growing user population, such as in the case of a corporate merger or acquisition — much easier than if identities and access were managed within each application. As a simple example, if a company stores identities in, say, 40 different locations and the acquired company stores their identities in 30 different locations, the merged business now has identities stored in 70 different repositories. With a centralized IAM system deployed in both places, this integration of identity information can be done with a minimum of effort and complexity.

FASTER RESPONSE TO COMPETITIVE THREATS Your competitors would like nothing better than to catch you flat-footed, and outmaneuver you in the marketplace. One way to do this is to introduce new online products and services quickly, to gain a competitive edge. An IAM platform allows you not only to respond to these threats quickly, but even to introduce your own services more easily, to turn the tables on your competitors.

With an IAM platform, applications can be developed and deployed more easily, user access can be granted and enforced more easily, and the new applications can personalize the experience to the unique attributes of each user.

INCREASED SCALABILITY FOR FUTURE GROWTH An integrated IAM and SIM solution can dramatically increase the scalability of an IT environment, thereby enabling growth to include many more customers as well as new applications. It does this by automating many IT management and administrative processes, and centralizing IT security management external to the applications.

A comprehensive SIM solution is particularly important for scalability. As the number of online users increases dramatically, collection and analysis of all the security event information needs to be automated in order to avoid being swamped by event and auditing logs from all these users.

¹ IT Compliance Institute
² The Burton Group

SECTION 3: BENEFITS

The Business Impact of Security Management

Integrated IAM can help enable new business initiatives, as well as strengthen existing ones in the following ways:

- An integrated IAM platform allows you to speed up the development and deployment of new applications, and to simplify the process of managing the entitlements of users to these applications.
- It provides capabilities to provide a consistent and pleasant online experience for all users, thereby improving their overall satisfaction and loyalty.
- IAM helps to strengthen customer confidence that their confidential information will be adequately protected by your organization. The confidence that these customers have in the security of the entire environment will be a key factor in their decision to remain a customer.
- An IAM solution allows you to expand and more tightly integrate your partner ecosystem and supply chain, so that you can greatly expand the set of services available for your online users and partners. An identity federation environment can significantly help open up new and promising business opportunities for any organization.
- Finally, an integrated IAM platform can help make your company more agile in the ever-changing business world. You can respond to competitive threats more easily, as well as adopt new organizational structures (including M&A activity) more easily, compared to organizations in which there is no centralized way of managing identities.

SECTION 4:

Conclusions

Organizations today face many challenges related to “keeping the bad guys out.” As important as this is for ongoing business operations, it’s “securely letting the good guys in” that will help fuel business growth.

A comprehensive IT security platform is a key enabler for business, and can help grow it in a number of ways. Many highly successful organizations have learned the benefits of this approach to fuel their overall business expansion.

SECTION 5:

References

“Reducing the Costs of IT Security Management”:

<http://www3.ca.com/solutions/Collateral.aspx?CID=88840&ID=4348>

“Managing IT Security Risks”:

<http://www3.ca.com/solutions/Collateral.aspx?CID=82802&ID=271>

“The Role of Security Management in Regulatory Compliance”:

<http://www3.ca.com/solutions/Collateral.aspx?CID=70177&ID=271>

“Business Value of Identity Federation”:

<http://www3.ca.com/solutions/Collateral.aspx?CID=66744&ID=4348>

SECTION 6:

About the Author



Sumner Blount
CA Security Management

Sumner Blount has been associated with the development and marketing of software products for over 25 years. He has managed the large computer operating system development group at Digital Equipment and Prime Computer, and managed the Distributed Computing Product Management Group at Digital. More recently, he has held a number of Product Management positions, including Product Manager for the SiteMinder product family at Netegrity. He is currently the Director of Security Solutions at CA.

CA, one of the world's largest information technology (IT) management software companies, unifies and simplifies the management of enterprise-wide IT for greater business results. Our vision, tools and expertise help customers manage risk, improve service, manage costs and align their IT investments with their business needs.

WP05GMIAMSM0E MP308890307