

INTEGRATING THE TWO WORLDS OF PHYSICAL AND LOGICAL SECURITY

A White Paper

Author: Guy Huntington, President, Huntington Ventures Ltd.

Date: February 20, 2009

Table of Contents

Integrating the Two Worlds of Physical and Logical Security	1
Integrating the Two Worlds of Physical and Logical Security	3
Why Integrate Physical and Logical Security?.....	3
Two Worlds	4
Key Solution Components	5
Integrated Management Structure	6
Identity Type Definition and Identity Business Processes	6
Enterprise Directory.....	6
Identity Management System	7
Physical Security Vendors Interface	7
Asset Management System Tied to the Identity Management System.....	7
Delegated Security Badge Approval	8
Segregation of Duties and Regulatory Reporting.....	8
Unified Security Ops Command Console.....	9
Enterprise Risk Management.....	9
This is all nice, but do I need all of this to start?	10
About the Author:	10

INTEGRATING THE TWO WORLDS OF PHYSICAL AND LOGICAL SECURITY

There is a growing trend to integrate physical and logical security systems together. However, doing so isn't always easy. There are usually enterprise political challenges in doing so, lack of understanding by both IT and Facilities on each other's needs, identity business process challenges for new identity types not in the IT systems, etc. Based on the author's past experiences in doing these integrations, this white paper addresses these challenges and makes recommendations on how to proceed.

WHY INTEGRATE PHYSICAL AND LOGICAL SECURITY?

Many militaries around the world have or are currently integrating physical and logical security systems together to mitigate the risk of cyber and physical attacks. This same trend is slowly seeping into the commercial, medical and industrial space.

Many enterprises have experienced attacks from insiders who's security badge and logical access rights wasn't revoked when they the identity was terminated resulting in insider attacks. Further, many critical infrastructure industries are trying to fortify themselves to mitigate the risk of terrorist or organized crime attacks on their enterprises. As a result, there is a growing number of regulations such as Sarbanes-Oxley (SOX), GLBA, SAS 70, Basel II, Government mandated FIPS 201, NERC CIP's and numerous International and EU Privacy laws that enforce strict governance in financial reporting and security controls (both physical and IT) to create "trusted" corporate governance paradigms.

There are a number of benefits to enterprises who achieve this:

- Same day provisioning, role change and termination of an identity's physical and logical access rights as well as asset issuance and recovery
- Lower operating costs for the physical security system
- Application of enterprise security policies based on risk across the enterprise both for physical and logical access control
- Low cost, quick, easy to do regulatory compliance reporting
- Unified central security ops command console displaying physical and logical security
- Senior management displays illustrating the enterprise risk based on combined physical and logical security
- Segregation of duty policy enforcement for both physical and logical security access

While all this reads well, achieving this has some challenges that are often more political than technical.

TWO WORLDS

The main challenge I have found in my past experiences is that the physical security people and the IT people operate in what I call “two worlds”. IT people have little idea of the complexity of physical security systems. They don’t understand most of the following:

- Access times – In an IT world if the user’s access is denied they can call the help desk, use on line password resets, etc. If the network is down, then the user has to wait until it comes up to get access. This won’t work in many of the physical security world where people need to get in the door ALWAYS.
- Physical area security zones – In most enterprises, when you’ve successfully authenticated to the network, then you’re able to access most applications. In the physical world however, there are often numerous different security zones with time of day access rights and unique exceptions that are required.
- Many different identity types – The IT world has several different identity types that access their networks and applications (employee, contractors, temps, third parties and customers). What IT usually doesn’t understand is the complexity of the identity types who access facilities. These range from all the aforementioned ones IT deals with to cleaners, lawn mowers, air conditioning, delivery personnel, locksmiths, window washers, etc. Some of these are regular repeating visitors while others are one time visits.
- Segregation of duties – IT people are becoming familiar with segregation of duty challenges when it comes to financial and privacy systems. However, they know little or nothing about physical security segregation.
- IT people normally work on the order of C.I.A. (Confidentiality, Integrity and Availability). Physical security people, especially in process environments work on A.I.C. (Availability, Integrity and Confidentiality).
- Org Chart – The IT folks work for people like the VP IT, CIO and possibly a CSO. The physical security people usually work for Facilities and sometimes a CSO.
- Budgeting system – Many physical security systems are run out of operating budgets dealing with individual buildings covering everything from toilet paper to the badging systems. Since these are localized, what IT people don’t understand is that this results in having numerous different physical badging systems often reporting to the local security guard at the front desk.

What the physical security folks don’t know about IT is:

- Identity management – they are usually at the end of the email chain letting them know an identity is arriving or is to be terminated. Often there is poor communication on a role change requiring security badge access. This usually results in security badge role creep.
- The Facility people are not usually on the IT folks’ radar screen when designing the identity management system.
- Poor communication – Often, especially for contractors, there is no end date sent to the Facilities people to assign to an incoming contractor. As a result, I have often seen where the security badge folks assign a date of one year for the contractor.
- Master Building Keys – I have found that there is often paper based tracking systems for master building keys in facilities. In one enterprise, I found that 30% of master building keys were either lost or never returned. Worse, I found no plan to address this and rekey the buildings.

- Facilities often runs the security badge system off its own networks – this is becoming a problem as many enterprise adopt wide usage of digital surveillance video cameras and want to put them on the IT network. Many physical security people don't understand IT networks.

All of this results in “turf wars”. People in both IT and Facilities want to protect their empires. As the technology converges, it places them in adversarial political positions. Often the CIO doesn't want to take on physical security nor does Facilities want to let go of physical security.

As a result of all the above the following occurs:

- Users often get frustrated at having to use different badges at different facilities, or they arrive at the security desk to find that no one let security know they were coming
- Attack vectors are created. An attacker can usually get themselves in a physical facility and then quickly explore ways to begin an internal cyber security attack.
- Poor processes mean people who are terminated still have logical and physical access

KEY SOLUTION COMPONENTS

How does an enterprise successfully integrate physical and logical security? There are several key components:

- Integrated management structure
- Identity types identified for all identities accessing both physical and logical systems
- Enterprise wide identity business processes agreed upon
- Enterprise directory
- Identity management system
- Physical security vendors interface
- Asset management for physical keys tied to the identity management system
- Delegated security badge approval
- Segregation of duties and regulatory reporting
- Unified security ops command console
- Enterprise risk management

Integrated Management Structure

While much can be done by having Facilities and IT work together, I have found that in the end enterprises need to have a central security senior manager. In many enterprises this is the Chief Security Officer (CSO). This person needs to:

- Oversee risk assessments for physical and logical access
- Have management authority for security budgets for both physical and logical security
- Have direct reports who operationally administer physical and logical security
- Oversees operational monitoring and reporting of logical and physical security systems

Identity Type Definition and Identity Business Processes

There are many different identity types that interact with the enterprise physically and logically. For many of these identity types, neither IT nor Facilities “owns” the identities. For example, contractors are often administered by Purchasing; employees are managed by HR, and customers by Marketing. What this means is that an enterprise identity management committee needs to be formed.

This is often the hardest part of a project. Getting HR, Purchasing, Marketing, Facilities and IT to jointly agree to map out the identity business processes is hard politically and time consuming to achieve. The business processes need to be mapped for identity creation, modification, role changes and termination. Thought must be given to what physical security privileges, network, application and asset privileges are required for each identity type including all types who access enterprise facilities physically. It requires senior management commitment to provide the leadership.

As part of this process, authoritative sources need to be identified for each identity type. This could be an ERP (Enterprise Resource Planning), HRMS (Human Resource Management System), CRM (Customer Relationship Marketing), individual databases, etc.

Once this is done, all sorts of wonderful things can happen!

Enterprise Directory

These identity types can all be fed from the authoritative source to an enterprise directory or directories. What is this? These are identity touchstones for the enterprise. It forms a central point for the identity management infrastructure for both access control and provisioning activities.

Directories use a technology called LDAP (Lightweight Directory Access Protocol) that is able to do very fast reads and is easily partitionable. The ability to partition it is very important in designing highly available systems since the directory can be physically located geographically close to the user.

Enterprises should consider the use of something called virtual directories to assist them in quickly connecting their different authoritative databases to the enterprise directory.

Identity Management System

Most large enterprises already have some form of an identity management system and enterprise directory in place. A typical identity management system has the following components:

- Access Control system – usually web single sign on (WSSO) and enterprise single sign on (ESSO)
- Provisioning and role based provisioning system
- Web services security
- Identity management – able to view and change certain identity features, display org charts, etc.

The provisioning system is able to do workflows for identity approvals, security badge approvals, and role changes, voluntary and involuntary terminations. It can either automatically or semi-automatically provision networks and applications. However, when physical security systems are involved there are some challenges.

Physical Security Vendors Interface

The challenge in integrating physical access control systems to identity management systems is that almost all the vendors use their own unique APIs (Application Programming Interfaces), their own databases and their own reporting methods. Five years ago, when I did my first physical and logical security integration, it meant that integrating was very difficult. Today however, there is much good news.

[Quantum Secure](#) has solutions that mean integrating identity management systems with physical security vendors can be done very quickly. They have developed a number of products that allow an enterprise to easily integrate their physical security products from numerous physical security vendors to identity management such as [Oracle](#), [Sun](#) and [IBM](#). As well, their products assist the enterprise in doing regulatory reporting, providing consistent on and off-boarding of identities, providing physical event reporting and managing segregation of physical access duties.

Asset Management System Tied to the Identity Management System

Tracking building keys and especially building master keys is critical to mitigate the risk to enterprises. All key management should be done using the identity management system to oversee who should receive master keys. The actual key issuance can be done close to the identity.

For example, often many enterprises use IT systems like Remedy to control IT business processes. It is easy to have keys placed in the Remedy asset system and to have a user interface for building administrators given to them. They then add a new key for a user when the Remedy system approves it.

When an identity's role changes or they are being terminated, the identity management system would automatically give the identity's current manager a list of all enterprise assets the identity currently uses, including keys. The manager and/or HR would then recover the key.

The identity management and Remedy systems would jointly track key recovery times or the fact that the key hasn't been recovered. This can be escalated to senior management. Further, it is optional that final payment to the identity might be held back until the assets are returned.

Delegated Security Badge Approval

In some enterprises, there is often much out-sourcing of certain functions. This means that third parties or suppliers are often the ones providing many of the identities who are going to need security badges. There are some options for enterprises to consider improving the issuance as well as the termination processes for these situations.

The identity management system has the ability to do "delegated administration". This allows the enterprise to delegate identity administration to whatever level within their enterprise that is closest to the identity OR, to outside parties. Let me give you an example to illustrate this.

Acme Co is a preferred supplier or contractors for a large project at your enterprise. You negotiate the contract with Acme such that the contract states that Acme will use your enterprise's identity management external web interface. There they will add, modify and terminate identities within a pre-determined amount of time.

The Acme Co administrator logs on to the interface and says that Jane Doe will be the new identity and selects what role Jane will play as well as determining the end date (all of this is preset by your enterprise in advance only using the roles and options that you feel is required and appropriate). The identity management provisioning system will then decide based on the role and time Jane is going to be there, what access rights she requires. The provisioning workflow might direct the request to your enterprise's managers for approvals or, if you decide, automatically approve the request. Jane would then be granted a security badge, which is waiting at the front desk, when she arrives. When Jane is terminated, Acme must terminate her within 24 hours or else severe financial penalties will occur.

Segregation of Duties and Regulatory Reporting

Often in enterprises there is application and physical access rights that neither the enterprise nor its auditors want the identity to have access. The identity management system can do routine checks on segregation of duties through apps and, with the physical security vendor interface, on physical access rights.

Additionally, the identity management system is the best tool to use for regulatory reporting. It can easily generate attestation reports to line managers. These are electronic reports on all the identities that report to them and what access rights, physical and logical that they have. It only takes a few minutes or less for the line manager to do an approval or note changes to access rights.

This is then combined in automatic regulatory reports. The reports deliver all the information that regulators and auditors are asking. Further, the identity management system, combined with the physical security interface and the actual physical security vendor's access database, can quickly provide drill down detail for forensic analysis.

Unified Security Ops Command Console

The physical security vendors' interface allows for combining the physical security monitoring from many different locations and/or different security systems with enterprise IT and logical defence perimeters. This provides the enterprise with the ability to create a unified security ops command console. While this can take time to create, it gives the enterprise a complete picture of what is happening at their physical locations and by network, application and database access. This is a critical component in helping mitigate enterprise risk IF the security ops command centre has good security trigger points, escalation pathways and knowledgeable personnel administering it.

Enterprise Risk Management

By integrating physical and logical security together, it also allows for enterprise risk management to be uniformly enforced throughout the enterprise. Physical access rights can be more uniformly enforced from the enterprise level, than by having numerous localized physical access systems, each with their own way of assigning privileges. Stronger forms of authentication for certain medium or high risk physical areas can be assigned and enforced.

THIS IS ALL NICE, BUT DO I NEED ALL OF THIS TO START?

Every enterprise has different politics, infrastructure, budgets and priorities. The integration of physical and logical security is usually phased out over a number of years across a large enterprise. However, my advice is to “look before you leap”.

Like any other major project, doing integration requires careful planning and much thought given before you rush out and buy products and hire consultants. Good questions to ask before you begin include:

- Do we have an identity management system?
- What physical access areas are you going to consider?
- What identity types use these physical areas?
- What’s involved in getting these identity types into the identity management system?
- Will other business units support this?
- What kinds of regulatory reporting are you doing or should be doing?
- What kind of operating costs are you currently experiencing for physical security and for regulatory reporting?
- What is the business case I can make for this project or program?
- What kind of resources will I require?
- What hardware will I require?
- How can I lower my operating costs for physical security?
- What is the master building key return rate?
- Do we have any physical separation of duties challenges we should be addressing?
- What kind of centralized security ops centre and/or console should we be aiming at?
- Do we have an enterprise risk management for all physical areas integrated with logical access?

When you have answered all these questions, then you’re good to go, find money and create projects. It may be that you will start off small, or if you uncover some serious challenges, then you will move quickly into integrating physical and logical security.

ABOUT THE AUTHOR:

Guy Huntington, President of Huntington Ventures Ltd, has lead, rescued and architected many large Fortune 500 identity projects including Boeing, Capital One and Kaiser Permanente. He has done several physical and logical security integrations including Capital One and Toronto Hydro. Guy’s expertise is in helping senior management understand the benefits, avoid the pitfalls and successfully procure and implement. He is able to work with different consulting firms for the actual implementation, different physical security vendors and different identity management products.

Guy can be reached at:

604-861-6804 (cell)

Guy.huntington@hvl.net

www.authenticationworld.com