

Honeywell Security & Data Collection



For additional information,
please visit www.honeywell.com/security/uk

Honeywell Security & Data Collection

Honeywell Systems Group
Aston Fields Road
Whitehouse Industrial Estate
Runcorn
Cheshire
WA7 3DL
Tel: 08448 000 235
Fax: 01928 701 063
www.honeywell.com

HSG-CONV-01-EN(1108)WP-COE
November 2008
© 2008 Honeywell International Inc.

Industry View: Checklist for Converged Access Control

Honeywell

Honeywell

Introduction

In the past few years, perhaps no security industry buzzword has been defined in articles and promotional materials as many times as 'convergence.'

These definitions have most commonly referred to the integration of physical security and IT systems, with occasional elements of building control. These definitions, while helpful to end users, beg the ultimate question: 'How do I make it work?'

Convergence uses data generated by both physical security and IT systems to drive both business process efficiency and security, and its framework defines a migration path for organisational growth. Here are some basic elements required to ensure a solution is truly converged.

Common Security Policy Management and Control

The IT infrastructure is the backbone of a converged solution, sharing knowledge of key business data across systems. The physical security system does not inherently know critical business data such as employee status, staffer security clearances and training certifications. A computerised HR system, though, often has this knowledge. IP-enabled security systems therefore allow users to take advantage of fixed investments and improve return on investment (ROI).

Developing common protocols for managing access to company assets and data enables more efficient provisioning and management. An organisation develops role-based policies that can manage badge issuance, enrollment and revocation processes by leveraging XML/SOAP interfaces for integration with identity management solutions. The key benefit is that building security personnel continue to use tools best suited to their jobs and HR personnel continue using HR tools.

Organisations should identify:

1. Authoritative sources (the system that has the ultimate say) for each person who has a building badge or an IT account.
2. Sources (IT systems or people) of key data used to determine whether a person has permissions to use a resource or access an area.
3. Compliance or audit needs where the data exists on multiple systems.
4. Any business or security concerns that are unique or are especially important to an organisation.
5. Key business processes (onboarding, offboarding, change of position) and determine the responsibilities of different systems.
6. A policy platform that supports customisable workflow creation tools to easily model processes and approvals.

Common User Provisioning

Convergence drives the business to contemplate the inter-relationship of physical security on IT security and vice versa.

How many organisations can definitely claim that terminated employees or contractors are immediately removed from their building access control systems? How many are confident that a former employee who tailgates into the building does not have active IT accounts? How many are confident current employees would recognise former employees and know the person has been terminated?

Provision dynamics are evolving and driving user permissions in non-IT and external IT systems.

Organisations must:

1. Determine how many terminated employees or contractors still have active building badges and IT accounts.
2. Determine how many contractors who have not been on site for the last three months still have active building badges.
3. Perform studies to see if anyone questions tailgaters.
4. Benchmark how long it takes for someone to be provisioned or de-provisioned.
5. Educate employees on security risks.

Single Access Credential

Building security starts with a badge, often a prox card. IT security, meanwhile, starts with a user name and password.

When organisations want to add more security to a card, they can add a PIN or a biometric. As IT systems look to increase security, however, the choices are not equivalent. Organisations can add:

- An RSA token or biometric that authenticates the correct person.
- A contact smart chip - embedded either in a card or in a USB dongle - that authenticates the correct person, and is also used for non-reputable digital signatures. Digital signatures are important in regulated environments to verify a person did approve or take action.

A single-card solution that includes a contact smart chip for IT and proximity technologies (contactless smart or 125 kHz prox) enables the organisation to manage one resource for each employee, thereby minimising both material and administrative costs. An optimised card issuance process allows building security to continue issuing badges and the badge issuance process will be connected to IT systems for provisioning as a single process.

Steps to take:

1. Building security teams should discuss access credentials with their IT counterparts to identify opportunities to leverage cards across the organisation.
2. IT departments should review authentication and PKI requirements/needs.

Correlation of Events

By connecting systems, organisations can correlate seemingly disparate physical and IT security events. For example, it may not seem suspicious for an employee to download large amounts of data. However, system correlation might show the employee only downloads the data when he is in the room by himself.

Organisations must identify:

1. Thresholds of normal employee behaviour by job classification. It may be necessary to audit current behaviours.
2. Business events that may cause security breaches (receipt of a resignation notice, termination for cause, unexpected change in work hours).
3. IT resources and/or locations with sensitive information (intellectual property, identity data) and develop a plan to lock down for normal security levels and for a heightened security level. Organisations must determine the return on risk for each sensitive item and develop security response plans accordingly.
4. Normal usage for each sensitive resource and what would be considered abnormal (downloading all customer data or customer credit cards).

In Summary

Convergence is the first step for any organisation to connect its critical systems to provide a comprehensive and coherent security policy. By integrating systems to share information, an organisation can see vulnerabilities in real-time and link IT security events with physical security responses. These abilities all drive real-time security policy management.

The next step will be proactive threat management, which enables correlation of real-time information with historical information. The system will 'learn' how to manage the current environment and react in a real-time manner, increasing system value and improving ROI. The system, for instance, can classify behaviour such as a certain employee trying to access random doors every few days or unusual behaviour by a subset of employees who all had security clearances processed by a specific adjudicator.

Using a converged system can reap substantial benefits and will provide additional benefits in the future as convergence continues to evolve. How organisations choose to implement these new toolkits is up to them and their individual security and compliance requirements.

