CAS Severn

Intelligent Answers.

CASE STUDY: IDENTITY MANAGEMENT SOLUTION RESULTS IN SECURITY COMPLIANCE FOR INSURANCE CO.

Commercial Business

THE SITUATION

A large, growing New York-based insurance company employs more than 1,100 employees, either full-time employees, contractors or consultants. And the company was continuing to hire more people to keep up with business demands. The company used a manual process for onboarding, which included new hire paperwork and the IT security access process. Based on their job function, employees, contractors, and consultants all needed access to a myriad of different applications. The human resources department contacted the IT department each time a new employee was hired. The IT department then manually issued access to the appropriate applications.

> "Our collaborative approach to the complex project resulted in a strategic success for our customer. We have a lot of experience with complex projects and we have served as a trusted advisor to this customer for many years. As a result, they were confident that we could meet their objectives and we did."
>
> *– Steve Drew, CAS Severn President*

THE CHALLENGE

The company onboarding process was inefficient and cumbersome. In addition to the inefficiency of adding employees, there was no follow-up or accurate means to validate the removal of people from applications when they no longer needed them or left the company. This was a significant problem in terms of meeting industry regulatory requirements and the ability to pass audits. In an audit, the company could not prove that all the identities on the individual systems were for people that still needed access to those particular systems. Contractors were especially problematic because they start and leave frequently and were often not taken off their accounts.

CLIENT

A large New York-based insurance company

INDUSTRY

Insurance

CHALLENGES

- Inefficient onboarding process for new hires
- Manual process used to grant access to IT applications
- No process in place to remove access rights for terminated employees
- Unable to pass regulatory audit

SOLUTION

- IBM Security Identity Manager

RESULTS

- Streamlined hiring process
- Access to IT systems controlled
- Achieved compliance with industry regulations

CAS Severn

HEADQUARTERS

6201 Chevy Chase Drive
Laurel, Maryland 20707
800.252.4715
cassevern.com

WITH OFFICES IN

Forest Hill, Maryland
Richmond, Virginia
Denver, Colorado
Kansas City, Missouri
Albuquerque, New Mexico
Raleigh, North Carolina
Charlottesville, Virginia

Premier Business Partner IBM

This exposed the insurance company to a grave risk of a security breach.

A solution was needed to streamline the onboarding and exiting process, to help the company comply with industry regulatory requirements with regard to security, and to ensure they could effectively pass audits. The insurance company asked CAS Severn for recommendations to solve these issues.

THE SOLUTION

Based on vast experience with identity management and in-depth understanding of the customer's needs, CAS Severn selected IBM Security Identity Manager as the solution.

When the customer described the audit requirements, it was clear they needed a way to automate their onboarding procedure. IBM Security Identity Manager automatically provisions user IDs and security access based upon an authoritative source, such as the HR system. The CAS Severn proposed solution includes an intuitive user interface. As soon as the insurance company's human resource department adds a person to its database and selects the applications the person will need, it automatically triggers and tracks the appropriate access for the employee. The reverse is also true. When a person leaves the company their access is immediately revoked and an audit trail is established of these actions.

IBM Security Identity Manager:

- Empowers line of business managers to automate and define users' access across the enterprise.
- Reduces complexity of enterprise identity management with centralized policy, integrated identity lifecycle management and support for third-party environments.
- Improves user assurance with strong authentication integration, audit reporting and closed-loop user activity monitoring.
- Provides effective and actionable compliance with centralized identity and access management across the enterprise.

THE RESULTS

As a result of this deployment by CAS Severn, the insurance company has an efficient and productive onboarding process, which now takes minutes instead of days. With the identity management solution, the company is less at risk for a security breach due to inappropriate access to systems. The company is able to pass audits and meet industry regulations. Lastly, the project enhanced the company's own corporate compliance.