Boston Childern's Hospital

Core Access Case Study

Boston Children's Hospital
Until every child is well™

Boston Children's Hospital chose Core Security to achieve sustained efficiencies, ensure HIPAA compliance, and improve business velocity. Key results include:

- Reduced password reset calls by 80% and help desk call volume by 25% per month
- Reduced IS staff involved in account administration from over 20 to one
- Saving~ $650,000 per year in equivalent labor cost
- Clinical staff given IT access appropriate to their responsibilities
- Consistent access revocation of terminated employees
- Increased password strength
- Immediate and appropriate end user access to critical applications
- Improved SLA from two weeks to two hours or less for all new hires

Background

One of the largest pediatric medical centers in the United States, Boston Children's Hospital treats approximately 300,000 patients each year.

The Challenges

Being a premier healthcare provider comes with unique challenges, including the simultaneous arrival and departure of 500 new interns twice a year, each of whom must be provided passwords and system accounts; a highly mobile work force that needs to access information from surgical units, inpatient floors and offices; high-ranking researchers and surgical chiefs who aren't employees of the hospital; numerous legacy systems and applications; departmental IT groups that run their own account management systems; and the need to comply with strict government regulations such as HIPAA. Providing immediate and appropriate access for users to corporate and healthcare information has been one of the organization's greatest challenges and is a critical component to ensuring Boston Children's Hospital maintains the highest level of patient care.

Twice a year, Boston Children's Hospital receives an influx of 500 pediatric doctors and specialists in training which constitutes a five percent staff turnover in just one week. Accounts need to be provisioned quickly for these users since the new staff will be working the day they arrive. The new workers also need to access information from surgical units, inpatient floors and offices. And of course, all account access needs to comply with HIPAA standards. Prior to implementing a solution, it would take up to three weeks for new doctors and nurses to get accounts set up, which became unruly with nearly 20 clinical applications that new employees need to access.

In addition to new workers, existing users often need changes made to their account access. It is imperative that IT ensures users have immediate access to critical applications in order to serve patients while at the same time limits their access to only those systems appropriate to their position to ensure HIPAA compliance and patient privacy.

"IT now has the ability to bring security management practices in line with regulations and to help hospital staff do their jobs more effectively... The faster physicians are able to access information, the better the care."

—Paul Scheib Chief Information Security Officer, Boston Children's Hospital

Under Boston Children's Hospital's old account creation process, users would send a fax requesting an addition or a change to an account, and a help desk staffer would then manually enter this request into the hospital's help desk system. Because account information was transcribed, the potential for errors was high.

The hospital also faced password management problems such as account sharing and passwords written on "Post-it" notes. The organization had many authentication systems in place, including those in PeopleSoft HRMS, Netscape e-mail, Oracle database, and several healthcare-specific and internally built applications. This led to numerous orphaned accounts. Because of the sensitivity of the information to which the staff sought access, an arcane system had been implemented in order to keep patient information from falling into the wrong hands. However, this system was

proving to be unreliable, costly and time consuming.

The improvised way in which the staff dealt with their various pass- words was anything but secure. Leary calls this the "3M Factor"; users kept track of their many passwords with "Post-its" affixed to their computers. Resetting these passwords was the most trouble- some concern of all. This was done entirely off-line, and required a tedious phone call to the help desk, in order to go through an elabo- rate, though necessary, identity authentication. The entire process could take several minutes. "I was very disillusioned," says Leary. "I wanted to give users complete control over their destinies, and I also wanted a way to synchronize passwords across multiple applications and platforms."

In addition to dealing with issues around productivity, compliance and security, the manual processes for managing user access and passwords were expensive, costing the organization upwards of $320,000 per year for password resets and $466,000 per year for account pro- visioning in labor costs alone.

With a three-fold mission to facilitate caregiver access to information technology resources, improve privacy and protect patient information, and reduce costs and reinvest in patient care, it had become painfully clear that Boston Children's Hospital needed a solution to automate the manual, costly processes of provisioning resources and managing passwords for its 9,000 users if it was to remain steadfast to its goals. The organization made the decision to look for an auto- mated system that would:

- Provide appropriate and streamlined access to vital patient information for clinicians, enabling doctors and nurses to focus on critical care by simplifying access to IT resources.
- Meet HIPAA guidelines by ensuring clinical staff only has access to appropriate applications and patient data.
- Automate account creation for the impending "baby doctor" influx to improve service levels from weeks to hours for all new hires, enable more secure password management practices, provide audit trails of use and disclosure of PHI and reduce security administration headcount and operating costs via automation.

The Approach

The IT staff evaluated several solutions. After an extensive search and careful consideration, Boston Children's Hospital chose Core Security's Access Assurance Suite.

Core Security's solution connects in real-time to the underlying data defining work communities and policies where they exist. Boston Children's Hospital needed to enable automated provisioning quickly and required a solution that could sustain and adapt to the change the organization constantly experiences at a business, IT and operations level. The solution provides agility to the provisioning infrastructure to quickly and effectively respond to and accommodate changes without the need to re-code or re-script when relationships, policies and infra- structure changes. Because the solution leverages data where it exists, in the authoritative data sources, any changes to role or access are picked up in real time with minimal or no effort versus other products that would require recoding or re-scripting for any and all changes.

Like many healthcare institutions, Boston Children's Hospital has numerous legacy and home grown solutions that it was unwilling and unable to replace. The provisioning solution it chose had to be able to integrate with those systems. Core Security's solution would enable Boston Children's Hospital to leverage its existing infrastructure through Core Security's Link Technology – a system of pointers that connect in real time to existing databases and directories.

Also appealing was that Core Security's solution could enable Boston Children's Hospital to immediately begin provisioning user access without role definition or data consolidation projects which meant it could meet its aggressive timeline for having a provisioning system up and running before the next influx of interns. With Core Security, Boston Children's Hospital would be able to quickly and successfully accomplish the provisioning of user accounts and passwords without defining roles, without a management hierarchy and without having to consolidate data into a centralized repository. This would enable it to accelerate the process and start seeing results immediately versus other solutions that would require extensive and time consuming upfront projects before any provisioning could be done.

An Incremental Approach to Provisioning

Boston Children's Hospital selected an incremental approach to alleviate end user pains and realize a return on investment. Its first goal was to gain control of password management. This would not only improve productivity by alleviating the number of calls coming into the help desk, but it would immediately meet various HIPAA standards and demonstrate a clear ROI to the organization.

Leading up to the initial implementation, the Boston Children's Hospital IT staff worked with power users and department heads to understand how to make the system work in a way that would be the least painful to users and would cause minimal disruption to routines.

After just two days of training with Core Security, it took only one day to install the initial implementation of CORE Password, Core Security's password management solution. Boston Children's Hospital established a web site that allows users to self-register themselves to perform their password resets. Passwords are automatically and simultaneously reset across approximately 20 target applications. All user and reset activity is captured through an interface to their Remedy ticketing system to enable reporting, troubleshooting and auditing. In addition to the Web site, the IT group leveraged CORE Password's desktop login access option to enable users to

reset their passwords before they even login to Windows. CORE Password can be accessed right from the Windows login prompt or from the Windows desktop tool tray.

To drive user adoption, the IT department leveraged Core Security's Self-Service Attainment Program to develop a full-scale awareness campaign, including presentations to department heads, training for power users, "desk tent" cards with instructions, posters in the lobby and organization-wide e-mails. The result has been a 90% adoption rate.

The second phase of the implementation was to streamline account provisioning with CORE Provisioning, Core Security's user provisioning solution. While the password reset features provide the most visible and obvious benefits to users, the Children's IT staff knew that the biggest payoff would come from implementing CORE Provisioning to improve account management. Their primary objectives were to introduce controls that would ensure that clinical staff only have access to appropriate applications and patient data and streamline the overall account provisioning process.

"One important lesson I have learned is that enterprise provisioning is more of a continuous journey than just a single project or technology. [Core Security] has truly partnered with us since day one to ensure our success, and we look forward to continuing our work together to ensure our organization is rapidly responding to the constant change and the evolving needs of our business, our the market, and most importantly our patients."

—Michael Ford, Information Security Manager, Boston Children's Hospital

The IT department wanted the rollout to be essentially invisible to users and managers. The upfront work the staff did in deploying CORE Password greatly reduced the time and effort required to deploy the provisioning piece.

The first step in the CORE Provisioning implementation focused on automating provisioning for the influx of interns that would be arriving and leaving in just a matter of months. Working on an extremely tight deadline, the IT group completed this step in the implementation in just four months.

Prior to this phase, Boston Children's Hospital did not have a management hierarchy in place. However, the organization was still able to automate the provisioning process without this defined structure.

Today, the organization has completed its management hierarchy and is working on the next phase of the implementation to enable self- service provisioning in order to distribute the ability to provision accounts out to the business managers.

The Results

Within a few months, Boston Children's Hospital was seeing dramatic benefits.

Sustained Efficiencies

Leveraging Core Security's Access Assurance Suite, Boston Children's Hospital reduced IT support costs and significantly increased productivity. Service levels have improved from two weeks to two hours or less for all new hires. The organization has reduced password reset calls by 80 percent, and calls to the help desk have decreased by 25 percent per month freeing those resources to focus on more strategic projects and urgent requests. Streamlining the process via automation has reduced the number of IS staff now involved in account administration from over 20 to one. And best of all, these labor costs are now saving Boston Children's Hospital approximately $650,000 per year which it is able to reinvest in patient care.

Transparent Compliance

The new system is helping the organization achieve HIPAA compliance and achieve tighter security. Boston Children's Hospital can now ensure the clinical staff is given IT access that is appropriate to their responsibilities, and system access is more consistently and immediately revoked when employees are terminated. The system has increased password strength and forced reset duration, and the organization has eliminated shared passwords or "Post-it" passwords on shared work stations. Boston Children's Hospital is also ensuring the privacy of user data by removing the help desk from the manual processes of assigning or resetting passwords and creating accounts.

"The improved efficiencies and return on investment were key benefits of moving password and account management to [Core Security]," said Scheib, "but these paled in comparison with the ability IT now has to bring security management practices in line with regulations and to help hospital staff do their jobs more effectively. The business impact was tertiary behind helping with HIPAA and providing a better user experience. The faster physicians are able to access information, the better the care."

Business Velocity

Today, users now have immediate and appropriate access to critical applications. New hires are now provisioned within two hours or less versus the previous two weeks. The yearly intern influx is no longer a painful event, as all users are now easily granted appropriate and necessary access on day one within a matter of hours or minutes. This means workers are more productive and patients are receiving better care.

Core Security has also enabled the organization to extend provisioning to include the seamless management of non-IT assets. Today, Boston Children's Hospital is able to provision for 1,000 wireless PDA users. These users have immediate and secure access to the information they need without being constrained by location.

Planning for the Future

Boston Children's Hospital has a number of provisioning enhancements they are either currently working on or have planned for the near future. One goal is to put in place a process that would require staff to accept, disable or change access to IT resources based on periodic access verification to ensure users have the minimum necessary access. The organization is also looking establish an automated link between application access and security training and account provisioning. By doing so users would only be granted automatic access to assets if they take and/or pass any required training or testing. Another goal is to develop automatic disablement of inactive accounts.

Boston Children's Hospital is planning to implement multi-factor authentication. They hope to set up shared workstations in clinical areas to allow clinical staff to access the network through two-factor authentication using a proximity card and biometric device. When clinicians walk away from a workstation, a secure screensaver will automatically come on. If they return, the workstation will recognize that they have returned via the proximity card. These devices will authenticate the clinicians' access through Active Directory and will integrate with Core Security's Access Assurance Suite.

The organization is currently deploying single sign-on to enable clinical staff to logon once and gain access to several clinical applications. Integration between the provisioning and single sign-on solutions will provide end users with a seamless access experience. Users will have all their accounts automatically provisioned and registered with the single sign-on solution. This process will not only improve and simplify the user's experience, but also improve productivity levels by get- ting users connected to their accounts quickly and with less effort required.

Another project the organization is planning is the implementation of Cerner. The flexibility of Core Security's Access Assurance Suite provisioning solutions will enable Boston Children's Hospital to quickly provision user access to the new Cerner system, enabling immediate access only to appropriate users.

ABOUT CORE SECURITY

Core Security provides companies with the security insight they need to know who, how, and what is vulnerable in their organization. The company's threat-aware, identity & access, network security, and vulnerability management solutions provide actionable insight and context needed to manage security risks across the enterprise. This shared insight gives customers a comprehensive view of their security posture to make better security remediation decisions. Better insight allows organizations to prioritize their efforts to protect critical assets, take action sooner to mitigate access risk, and react faster if a breach does occur.

Core Security is headquartered in the USA with offices and operations in South America, Europe, Middle East and Asia. To learn more, contact Core Security at (678) 304-4500 or info@coresecurity.com

CORE SECURITY