Fast Break

Technology prescriptions and flawless planning and execution transform patient care and services at Hadassah University Hospital

S
treaking down the basketball court on a fast break requires a unique combination of skills, something that Barak Shrefler, the chief security officer at Hadassah University Hospital and a former professional basketball player, knows well. It is more than speed. It is more than strategic planning. It is more than coordinating with your teammates. It is more than raw talent. It is more than seamless execution.

Rather, it is an interweaving of all these aspects. "Failure to account for one area puts the end result at risk," Shrefler explains. "In a matter of a few seconds, five players must seamlessly plan and execute, all in perfect concert with each other."

The same model applies in the business world, though normally not at the same speed. "My experiences on the court serve as a valuable framework in my professional career," Shrefler says.

Standing at 6'4", Shrefler was a force in Israeli basketball, averaging 16 points, 9 rebounds, and 3 assists per game—including the ability to dunk. Unfortunately, his career was brought to an abrupt end by a knee injury. Before playing professional basketball, Shrefler completed a degree in accounting, and this was his expected career path. However, on a whim and the recommendation of a friend, he applied for an IT position at a company that provided IT services to the public sector. While boarding a plane for New York City, he received a call with a job offer; he accepted and thus began his IT career.

From back office to front court

Shrefler joined Hadassah University Hospital in 2003 as a systems administrator. "The circumstances when I arrived nine years ago were much different than those today," he reflects. "It was less intense. The lines of alignment between IT and the organization, including patient services, were nominal. IT was largely a back-office function."

This is no longer the case. Healthcare delivery and services are being transformed because of technology. "IT services are intricately intertwined within the larger organization," he reports. "Doctors and other healthcare providers expect to be able to access patient information, including digital images, from anywhere and on any number of devices."
In 2006, Shrefler assumed a new role at Hadassah University Hospital. Previously, the healthcare organization did not have a group dedicated to security. “The rapidly changing threat landscape necessitated that we create a team dedicated to security,” Shrefler remembers. As director of Information Security, he was given the charter to build and lead a team tasked to create and implement an organization-wide risk management program. “Security had evolved to encompass more than just systems and infrastructure,” he notes. “There were highly publicized incidents of data loss, and our executive management team wanted to ensure that we had the right technologies and processes in place to keep patient data safe.”

Security—it starts at the endpoint

Shrefler’s efforts began with the infrastructure. “We didn’t have a standard set of tools for protecting our various endpoints—from workstations to the data center,” he says. “The prior environment was insufficient and time-consuming to manage.”

One of the first steps was the selection of Symantec for endpoint security. “Endpoint security is much broader than simply antivirus and antispyware,” Shrefler notes. “It comes in what I call layers—firewall, intrusion prevention, gateways, messaging security.”

When Shrefler and his team upgraded to Symantec Endpoint Protection, they elected to migrate to Symantec Protection Suite. They added intrusion prevention and firewall for enhanced endpoint protection and on certain endpoints such as those supporting emergency room and surgical functions, they activated device control. For the latter, Shrefler explains that “it is absolutely critical that we protect those endpoints. We prohibit all device connections such as USB and flash drives and limit their application access. These systems must be completely clean and maintain 100 percent uptime.”

Messaging security was also a concern. “Nearly 90 percent of our incoming email is spam and this presents a perplexing problem,” Shrefler reports. Hadassah University Hospital’s earlier solution was inefficient and ineffective. Too much spam was making it through to users, a drag on productivity, and false positives were consuming valuable time—for both IT staff and users. As a result, Shrefler rolled out Symantec Messaging Gateway powered by Brightmail, part of Symantec Protection Suite. It is used to manage both incoming and outgoing messages. The Hadassah University Hospital team also deployed Symantec AntiVirus for Messaging to protect their Microsoft Exchange servers.

Centennial: Hadassah University Hospital

The roots of Hadassah University Hospital are found in the organization Hadassah, or the Women’s Zionist Organization of America. Established in New York City in 1912 with the objective to provide medical services and educational programs in Israel by American Jewish scholar and activist Henrietta Szold, Hadassah sent two nurses to Palestine in 1913. They set up a small public health station to provide maternity care and treat trachoma, a contagious eye disease eventually leading to blindness. Hadassah followed this initial endeavor with a mission named the American Zionist Medical Unit in 1918 composed of 45 healthcare professionals; they set up six hospitals that were turned over to municipal authorities.

Throughout the 1920s and 1930s, Hadassah continued to provide health-related services to the Jerusalem population. Its work included the opening of various hospitals—for treatment and teaching—in Jerusalem as well as other locations in Palestine. The cornerstone of the Mount Scopus hospital was laid in 1934, and the facility opened its doors in 1939. With over 350 beds and 30 departments and clinics, the Mount Scopus hospital serves all populations of Jerusalem without distinction to religion or race today.

In 1961, Hadassah opened a second hospital in Ein Karem in southwest Jerusalem that consists of 800 beds, 130 departments and clinics, and 28 buildings. The complex includes schools of medicine, dentistry, nursing, public health, and pharmacology from the Hebrew University of Jerusalem. The campus also lays claim to a famous synagogue with stained glass windows depicting the 12 tribes of Israel. A new inpatient facility was added in early 2012, the Sarah Wetsman Davidson Hospital Tower, a 19-story facility with an area of 90,000 square meters, 500 inpatient beds, and 20 operating rooms. Hadassah University Hospital touts many medical firsts and region-only capabilities. In 2005, both the Ein Karem and Mount Scopus campuses were nominated for the Nobel Peace Prize in recognition of their unwavering focus on maintaining equality of medical treatment, serving as exemplary models of cooperation and co-existence, and persevering to build bridges of peace through medical activities.
“This holistic approach gives us a more proactive messaging security posture,” Shrefler comments. Results were seen immediately. IT staff is saving at least one hour per week, time previously spent helping to resolve false positives. And users no longer need to deal with spam, an issue that consumed, on average, an estimated 15 to 30 minutes per week for each of the organization’s 6,500 employees.

In early 2012, Hadassah University Hospital upgraded to Symantec Endpoint Protection 12. “The reputation-based security approach is a substantial evolution for endpoint security,” Shrefler observes. “The new scan engine is a great addition, particularly for our virtualized servers. We’ve seen measurable performance improvements on those systems.”

Healthy regimen of endpoint management
The efforts Shrefler and his team have made around endpoint security align with their work on endpoint management. “We’re a long-time user of the Altiris endpoint management solution,” Shrefler notes. The original Altiris solution was pre-installed as part of a larger HP server blade acquisition. “Altiris Deployment Solution was bundled with the servers, and it proved to be effective,” Shrefler remembers. “It saves us a lot of time when deploying new servers or re-provisioning existing ones.”

The initial solution deployed on workstations and laptops was the remote control management feature in Altiris Client Management Suite from Symantec. With two campuses and numerous facilities on each, remediation of issues was a problem; valuable IT staff time was consumed walking between buildings and driving back and forth between the two campuses. Indeed, Shrefler estimates that the solution saves upwards of several hundred IT staff hours annually.

But the IT team was just scratching the surface of what was possible with Altiris Client Management Suite at the time. “We added the deployment capability about two years ago and patch management last year,” Shrefler says. The team saw substantial time savings with the deployment function. “We had a full-time headcount spending nearly 20 hours each week dealing with provisioning issues,” he recalls. “It is now only an hour a day.”

Patch management results were just as impressive. Shrefler comments: “Patch management is important, because we can use the solution to patch a number of devices and platforms—Adobe, Windows, Linux, among others.” Previously, patch management consumed 10 to 20 hours each week; with Altiris Client Management Suite, it is automated. “The earlier solution was a real headache,” he reports.

About two years ago, the Hadassah University Hospital team added several hundred biomedical devices to the network. They extended Symantec Endpoint Protection to each of them using the deployment component in Altiris Client Management Suite. Then, for patch management and remediation, they use Altiris Client Management Suite. “The complexity of protecting our endpoints has grown exponentially over the past several years,” Shrefler observes. “However, the combination of endpoint security and endpoint management from Symantec provides us with an extensive toolset.”

Authentication: tangible factoring
In 2011, Shrefler and his team sought to address a pain point that was an encumbrance on organizational productivity, along with a risk factor—
authentication. “Our previous authentication solution, though twofactor, was complex to manage and overly expensive,” Shrefl er recalls. “End users often were not able to connect, and they naturally turned to me and my staff. This happened at all hours of the day and night, so we needed a better solution.”

Shrefl er looked at different options and ultimately settled on Symantec Validation and ID Protection Service. “We have the option of hard or soft tokens,” he explains. “It also provides us with robust protection through its two-factor authentication. Plus, it is a cloud-based service. We don’t need to worry about hosting or managing it on premise; we can leave this task and worry to Symantec.”

Time savings from the Symantec solution are substantial. Shrefl er previously estimates that his team spent 15 hours per week remediating issues; this is time now spent on other initiatives. Cost savings are also tangible; each client is US$15 cheaper than the earlier solution—or US$80,000 if an aggregate tally is taken.

A cure for data loss
At about the same time that Shrefl er and his team implemented the next-generation authentication solution, the need for a data loss prevention solution became a pressing organizational requirement. Amnon Haursh, an IT manager and peer to Shrefl er, collaborated with Shrefl er in investigating different solution options. “A few years ago, you could talk about the world in terms of a global village,” Haursh quips. “Now it’s a building. Everything you do, everything you say, everything you write is on the Internet in a mere instance.” Haursh and Shrefl er ultimately concluded that Symantec Data Loss Prevention most closely met their business requirements.

The rollout of Data Loss Prevention was done in increments. The first step was to document data loss prevention policies by collaborating with different business owners—legal, HR, finance, marketing, and audit. The second step was to build out those policies using the universal modules—both out-of-the-box and custom—in Data Loss Prevention. “The policies cover everything from patient records to PCI compliance issues,” Shrefl er says. The third step was to begin extending Data Loss Prevention across the IT environment. “We started with the endpoints, then our storage environments, and finally the network,” Haursh continues. “We initially turned on the discovery and monitoring capabilities and will be adding management and enforcement for certain data types and endpoints later this year.”

The Hadassah University Hospital team also plans to implement Symantec Data Insight. “We want to know who created the data, who is ‘touching’ it, and where it is located,” Shrefl er says. “Once we have this insight, we will be able to define further our retention and expiration policies. At the same time, we will build this into our data loss prevention policies.”

Mobile: the next “security” frontier
In increasing numbers, doctors and other healthcare providers at Hadassah University Hospital began bringing their own devices and wanting to connect them to the corporate network. “The emergence of tablets creates a number of exciting opportunities in healthcare,” Shrefl er notes. “It also poses some perplexing security challenges.”

In 2011, Hadassah University Hospital embarked on a series of mobility efforts. Shrefl er and his team worked with different organizational owners to define a Bring-Your-Own-Device (BYOD) policy and institute network access controls and processes. The healthcare provider also initiated a mobile app development program. The first app is available on Apple iPad devices; it aggregates patient digital images and records and provides doctors, nurses, and other healthcare practitioners with a consolidated view. The app is scheduled for deployment in April via Hadassah University Hospital’s Corporate appstore.

“Protecting this rapidly growing mobile environment presents a number of challenges,” Shrefl er observes. Already using Symantec Validation and ID Protection Service for two-factor authentication, both hard and soft token, on laptops and workstations, he and his team didn’t need to look very far. They are in the process of increasing their mobile app development program. The first app is available on Apple iPad devices; it aggregates patient digital images and records and provides doctors, nurses, and other healthcare practitioners with a consolidated view. The app is scheduled for deployment in April via Hadassah University Hospital’s Corporate appstore.

Prescribing Online Trust
Hadassah University Hospital has relied on Symantec SSL for a number of years. “Our use of Symantec SSL actually predates my time at the hospital,” Shrefl er notes. “We use it as part of our authentication services. But we also use Symantec SSL, along with the Norton Secured Seal Powered by VeriSign, for our online donation services.”

Hadassah University Hospital plans to extend online payment services to patients later this year, and Symantec SSL and the Norton Secured Seal will be part of that e-commerce deployment. “The ability to leverage these services through the cloud makes it very easy for us to provision and manage them,” Shrefl er elaborates.
of installing Symantec Validation and ID Protection Service onto all mobile devices on which Hadassah University Hospital enterprise apps are provisioned. “The cloud-based approach is easy to use and cost-efficient,” Shrefl er states.

For management of mobile devices, Shrefl er is looking at the possibility of using Symantec Mobile Management. With it, Shrefl er’s team will be able to configure access to corporate services such as email, calendaring, applications, and content, secure the devices via password and access controls, and manage them all from a central server.

“Since we already have Altiris Client Management Suite in place, this is a natural migration for us,” Shrefl er explains.

As the applications and services available on the mobile devices provide access to confidential patient and organizational information, extending Data Loss Prevention for Tablets was also a critical requirement. “This spring and summer, we plan to activate Data Loss Prevention for Tablets on our iPad and Android tablets,” Shrefl er says. “As our endpoints evolve and mobile devices proliferate, it becomes more and more important to protect the information they access.”

Problem solver gets IT infrastructure
In January 2010, Shrefl er assumed additional responsibilities when IT infrastructure was added to his plate. They included supervision of servers and storage systems, the network, and all clients such as workstations. With a reputation of being able to quickly fix problems and drive operational efficiencies, Shrefl er was charged with several challenges when he was given this additional assignment.

The first was an ad hoc, problematic data protection infrastructure that ran different backup tools on different sets of servers and storage systems. “Our silo-based approach was very difficult and time-intensive to manage,” Shrefl er reports. “We had very long backup windows, and they were getting ready to push into business operations. Further, our backup success ratios were inadequate.”

In a matter of a few seconds, five players must seamlessly plan and execute, all in perfect concert with each other. — Barak Shrefl er, Chief Security Officer, Hadassah University Hospital

Hyper virtualization
The second infrastructure area on which Shrefl er and his team focused was acceleration of the hospital’s virtualization strategy. The IT team had embarked on a virtualization program in 2009 and Shrefl er sought to gain efficiencies—from cost to flexibility—by migrating the majority of the hospital’s 300 servers from a physical to virtual environment. To date, his team has virtualized about 100 servers that now run on Microsoft Hyper-V Server technology hosted on HP ProLiant server blades. Shrefl er’s team has started to move some applications over to Linux-based blade servers—both Red Hat Enterprise Linux and CentOS Linux. A handful of VMS boxes are also used for legacy application-specific functions. The team is currently running four virtual hosts for the 100 servers that have been virtualized. “We’ve been able to decommission about 50 boxes to date,” Shrefl er comments. “Later this year, we plan on shutting down another 35 servers.” From simply a hardware and maintenance standpoint, assuming an annual cost of approximately US$15,000 per box, the savings are substantial—in the range of US$1.2 million. “And this doesn’t account for the reduction in energy consumption, which feeds directly into our corporate sustainability initiatives,” he adds. “Green IT is an important part of our overall IT program.”

Shrefl er has established an ultimate goal of virtualizing upwards of 80 percent of the hospital’s server environment. “There are certain applications that are simply not compliant with virtualization and must remain in a physical configuration,” he says. “But the vast majority of our applications will be running on virtual servers within another year or two.”

Hadassah University Hospital plans to open a secondary, next-generation data center at its Mount Scopus site later this year, and the team is building it based on green IT standards, including virtualization. It will provide primary computing functions to the staff at the Mount Scopus campus, along with serving as a disaster recovery location. With virtualization, Shrefl er projects that his team will be able to cut server cost
in half for the new data center. “This adds up to measureable savings, money that can be spent on technologies and services that directly impact patient care,” he sums up.

Prescribing a data protection standard
With such a laser focus on virtualization, the team pinpointed virtualization support as a central requirement when evaluating different data protection solutions. “Symantec NetBackup quickly rose to the top,” Shrefl er says. “It has seamless integration with Hyper-V while providing one console and view across both our physical and virtual environments.”

Backup volume also remains a challenge for Shrefl er’s team. They currently back up 10 terabytes via daily incremental and differentials and then conduct full backups every week; however, this will grow to 40 terabytes later this year as Shrefl er’s team moves the entire data protection infrastructure over to NetBackup. “The deduplication capabilities, particularly at the source, are going to be critical for us—both in terms of our backup windows and our overall data store,” Shrefl er says. “Once we’re fully deployed, we anticipate that we will be able to reallocate in excess of 20 terabytes of storage. This is going to be a significant cost avoidance for us.” In addition, backup windows range in the vicinity of 12 hours, a timeframe Shrefl er hopes to cut in half once the solution is fully deployed.

With the release of NetBackup 7.5, Shrefl er’s team plans to upgrade their NetBackup environment later this spring. “We’re quite excited about the new functionality,” he says. “For example, while we’ve reduced our backup windows significantly by standardizing on NetBackup, we anticipate that we can do so further using NetBackup Accelerator. And the close integration between our NetApp storage environment and NetBackup, particularly Replication Director, will enable us to optimize recovery points and minimize our recovery times.”

Archiving speeds
A final infrastructure area that Shrefl er anticipates addressing later this year is archiving and retention. “We have a stringent quota for our end users,” he observes. “They spend a lot of time managing their mailboxes. And because PST files become critical data repositories, they quickly become quite large and often corrupt.” Rebuilding those PST files—when it is actually possible to do so—is a time-intensive process; time that Shrefl er’s team needs to spend on other projects tied to the business.

Hadassah University Hospital also has a rapidly growing—200 percent last year—Microsoft SharePoint Server data store. “We currently have in excess of a terabyte,” Shrefl er says. “We need a solution that will allow us to archive the data, retain and expire it based on policies, and then perform search and retrieval.”

Symantec Enterprise Vault is the natural migration path, according to Shrefl er. “We will use the PST Migrator option that is part of Enterprise Vault to import all of our PST files,” he says. “Having all of our Exchange and SharePoint data under one roof and searchable through eDiscovery will be critical.”

Culmination of the IT “fast break”
Just as a fast break involves different concomitant players and actions, the various efforts the Hadassah University Hospital team have led consist of intertwining initiatives. With the right strategic planning and collaboration and a comprehensive understanding of how everything fits together, including alignment with a larger set of organizational business owners, Shrefl er and others are showing how IT is not simply a service but critical business enabler.

“The aspects of teaming and competing in basketball provide me with a lens in my IT career,” Shrefl er explains. The same exhilaration that occurs at the end of the fast break with a slam dunk or an easy layup corresponds with the feelings derived from driving a strategic IT initiative to culmination.

Patrick E. Spencer (Ph.D.) is the editor in chief and publisher for CIO Digest and the author of a book and various articles and reviews published by Continuum Books and Sage Publications, among others.