By Ray Coulombe

The Cure for Security Inconsistency

Genzyme, a Sanofi company, may specialize in rare diseases, but its security team has made integrating disparate systems their specialty

While a great deal of the focus when it comes to healthcare security is on patients, HIPAA, workplace violence, emergency rooms and pharmacies, the reach of the "healthcare market" actually stretches much further. Take Genzyme, a Cambridge-based biotechnology company, as an example. Genzyme's goal is finding and developing treatments for Multiple Sclerosis, thyroid cancer and rare genetic diseases known as lysosomal storage disorders (LSDs); thus, while you likely won't find them on a hospital campus, security for such an organization is vital to protect its facilities, staff, information and products.

Genzyme was founded in 1981 as a tiny start-up researching rare genetic-related diseases. The small company did not really consider security as a major issue until a problem was discovered with missing lab notebooks. "The senior leadership of the company understood the importance and advantage of a security program with a unified approach to physical and information security," says Dave Kent, Vice President and Head of North American Security.

The company's security department and procedures evolved from the notebook incident to become a model for holistic security and risk management in a multi-national, multi-cultural company. When French global healthcare giant Sanofi acquired Genzyme in 2011, it got more than it bargained for. While it added an important new source of bio-technology research and products, little did company officials realize that they were also acquiring a world-class security capability.

An Integrated Security Program

In the mid-1990s, two key managers, Kent (now Sanofi Vice President and Head of North American Security) and Bhavesh Patel (Senior Director, Security Services and Technology) joined Genzyme to begin the process of constructing a comprehensive security operation and program. By 1998, they had implemented "convergence" — long before the term had become a buzzword in security industry circles — by tying HR strongly into the access control system.

By 2000, security was fully integrated into the company's real estate process, where no property went online until all security issues had been properly addressed. This, and subsequent alignment with Finance and IT, set the environment for breaking down silos and creating a pervasive atmosphere of security awareness. Security was defined in a broad sense, encompassing enterprise risk, supply chain, insurance and competitive technical information. Physical security, IT security and product security were all placed under Kent, a single "Head of Security."

This path to integration did not occur without challenges. Due to a number of acquisitions, an estimated 30-40 different access control systems were put into the Genzyme mix. "We didn't want to take a cookie-cutter approach or drive a corporate mandate," Patel explains. "We established a cross-functional team and built a new standard based on the business culture and risk."

The two-way dialog resulted in agreement that a fully integrated company-wide approach would not only provide better security and functionality, but also immediate day-to-day benefits. These included savings in both time and money, resulting from centralized Tier 1 and 2 support, system troubleshooting and badge provisioning.

The Management System

Badges are extremely important — those new to the company by acquisition or hire must be provisioned with a credential that would be recognized in any company facility worldwide, thus facilitating both access and also company unity and morale.

These efforts led to the deployment of enterprise-level access control across 110 locations in 46 countries with personnel data from 23 different systems, using a single security management system, Pro-Watch by Honeywell.

"The Pro-Watch suite of software was developed from the onset to support multiple access

Kent and his security team were tasked with integrating nearly 10,000 card readers and more than 5,000 video cameras in North America onto a unified platform.

control hardware platforms in addition to our own line of products," explains Dave Karsch, Honeywell's Global Account Manager for Pharma/Healthcare. "Hardware-agnostic by design, (the system) is an open, scalable platform that enables end-users to grow their security system as their needs change."

Patel, in fact, was an initial member of the supplier's "End-Users Group."

The more difficult challenges, though, were not technical, but rather geo-political. Since security went global before HR did, it encountered numerous privacy issues at international locations. Regulations such as when video could be recorded and the length of time transactional data could be kept were negotiated with each entity (nearly 50 in all) on an individual basis. To be sure, the intangibles of trust, fear of corporate oversight, and individual personalities complicated these negotiations, but collaboration and good sense won out.

Acquisition Complications

Fast forward to 2011, the year of Sanofi's acquisition — by then, Genzyme's processes, procedures and measurement had been so well-tuned that the Global Risk Group operated like a separate business unit. It kept its own financial data encompassing costs and positive contributions; in fact, security considerations had become one of the baseline criteria for many business decisions.

"Prior to the acquisition, we knew Sanofi and its integration history well, and were concerned that the value of our program might be overlooked," Kent says.

Life usually changes dramatically for a company when it is acquired, but Sanofi Senior management in Paris and North America immediately saw the value of Genzyme's integrated security platform, seeing the potential value of a combined program. Sanofi's global head count, at more than 100,000, is ten times the size of Genzyme's, and Sanofi's additional acquisitions of animal healthcare company Merial (2009) and consumer products company Chattem (2010) had created a situation where 15 different access control systems and a like number of video management systems were operating across North America, encompassing nearly 10,000 card readers and more than 5,000 video cameras.

Kent was named Sanofi Head of North American Security and his group was empowered to be the catalyst for change. Fortunately, each entity already had a professional security staff, setting the stage for meaningful and collaborative integration post-acquisitions. A significant piece of the Sanofi integration was tying together these previously independent programs into a cohesive North American security team, which included Marvin Washington, Director of North American Security Operations, and his Security Operations team.

"Sanofi's portfolio of companies in North America, with more than 20,000 employees and 135 locations, faces a diverse set of current and emerging security risks," says Head of North American Security Dave Kent. "Our challenge is to align our programs, services and systems in a way that enables the business to operate securely."

Using Kent's template for successful integration, a primary task was to whittle down 15 access control systems to three; however, it was not just about access control — the challenge was multi-faceted. "Sanofi's portfolio of companies in North America — with more than 20,000 employees and 135 locations — faces a diverse set of current and emerging security risks," Kent says. "Our challenge is to align our programs, services and systems in a way that enables the business to operate securely."

First In on PSIM

Even before being acquired, Kent and his team at Genzyme had begun to think about its multiple security challenges, and in response had developed and deployed the Genzyme Event Manager (GEM), a system that today would be termed a "Physical Security Information Management" (PSIM) system. It handles an array of inputs and to provide security operators guidance on procedures to follow to resolve the alarm or event.

These inputs could be internal alarm-generated, or external, such as that from third-party situational awareness software or traveler software; however Sanofi is a pharmaceutical company, not a software company, and Kent says it was hesitant to develop and enhance a software product like GEM unless there was no alternative to meet its needs.

The alternative presented itself in SureView Systems, which, with its roots in alarm monitoring software, had recently broadened its product line to extend alarm management into security information management. Its Immix software platform, unlike GEM, is a .NET web-based system, requiring no client software to be installed on operator or supervisor PCs. The system consolidates all monitoring activities from any source including video surveillance, access control intrusion, two-way audio and GPS alarms.

"The technologies in the marketplace today are limitless, but without process around the technology, it's just a fancy gadget," Patel explains. "Technology must be integrated into business processes to bring measurable and sustainable value to the enterprise."

Fortunately, SureView was able to leverage its existing relationship with Honeywell to develop the Pro-Watch integration. The net result is a system that provides operators with immediate notification of exception-based alarms from the Pro-Watch access control system, and then ties these events this into Sanofi's other security systems, giving operators a complete situational awareness when responding to remote events.

Another security system is provided by NC4, an enterprise-grade application that provides situational awareness alerts, with potential impact on the business security of the organization. Prior to the Immix integration, NC4 alerts were simply received into individual email accounts, providing no alarm management, enforceable Standard Operating Procedures (SOPs) or consistent event response. Now, the alarms incorporate information about the location, GPS coordinates and nature of the event. Ultimately, the alerts make more responsive the operators and the organization in general.

(continues on page 37)

Bhavesh Patel, Senior Director, Security Services and Technology; and Dave Kent, Head of North American Security, have teamed to construct a comprehensive security operation.

ADVERTISER'S INDEX

Advertiser	Page #	Website URL
Assa Abloy Inc	3	www.securityinfowatch.com/10212899
Avigilon	5	www.securityinfowatch.com/10215735
Axis Communications	2	www.securityinfowatch.com/10212966
Detex	9	www.securityinfowatch.com/10213445
DSX Access Control Systems	39	www.securityinfowatch.com/10214208
HID Global Corporation	40	www.securityinfowatch.com/10213866
Honeywell Security Group	21	www.securityinfowatch.com/10213896
IFPO	37	www.securityinfowatch.com/10214049
Inovonics	23	www.securityinfowatch.com/10213994
Linear Corp.	7	www.securityinfowatch.com/10215766
Secured Cities	17	www.securityinfowatch.com/10752984
Security Specifiers	25	www.securityinfowatch.com/10300750

This directory is provided as a service. Publisher assumes no liability for errors and/or omissions.

CLASSIFIED

Security Inconsistency

(continued from page 20)

"Having exception-based system alerts enables our operations team across the region to focus limited resources on critical and other priority events," Washington explains.

Other enhancements include automatically rolling over alarms to alternative operators, escalating alarms on operator demand, customized operator screen layouts, hyperlinks to pages with Sanofi's own operator response scripts, reaction to email-generated alerts, and enterprise multi-site capability. The Immix system is being rolled out by Sanofi this year as part of a larger implementation of Pro-Watch 4.0 and its Integration Kit, Honeywell's platform to integrate diverse devices and systems. Additional systems, such as Lenel's OnGuard legacy access control system, will be tied in as well.

More on the Horizon

What's next on the agenda for the Sanofi security team? First, there is the completion of the North American access control integration; then, there is the matter of working towards a truly globally integrated system — a road that Genzyme has already traveled successfully. Patel has been named to chair the company's Center of Excellence for (Global) Security Technology, bringing past experiences and lessons learned to the table. There's also the challenge of globally integrating the corporation's diverse systems: "Today we are inventorying our global systems and looking for opportunities to replicate the success we've seen here," Patel says.

The effort is well worth it — Sanofi's system provides the basis for true collaboration, delivering a platform to manage and protect the assets of a major global commercial enterprise quickly, cost-effectively and without the need to replace or reengineer systems and processes already in place.

At the end of the day, for Genzyme and Sanofi, it is all about curing disease — and that means providing effective business security. "We have the ability to take a fully integrated approach to organizational security risk," Kent says. "We were doing this at Genzyme and are now on the same path at Sanofi." ▮

Ray Coulombe is Founder and Managing Director of SecuritySpecifiers.com and Principal Consultant for Gilwell Technology Services. He can be reached at ray@SecuritySpecifiers.com, through LinkedIn, or on Twitter @RayCoulombe.

RESOURCES

Request more info on the companies in this article

Honeywell: *www.securityinfowatch.com/10213896*
Lenel: *www.securityinfowatch.com/10214226*
NC4: *www.securityinfowatch.com/10855607*
SureView Systems: *www.securityinfowatch.com/10486857*

Bandwidth

(continued from page 8)

3. Test and document video network traffic. Many IT departments use Wireshark or similar free network monitoring software to capture and examine five minutes of video network traffic from a newly deployed security video system. They examine the traffic log to verify and document the acceptable state of the new system. Video-savvy IT departments or security integrators repeat this exercise annually, from a good sampling of locations where video viewing is desired. This is information to be shared and evaluated by Security and IT.

4. Document and register the video high-availability requirement with IT Security. Maintaining the integrity of security video traffic should be a standard part of network security, whose job it is to maintain the confidentiality, integrity and availability of critical systems. ▮

Write to Ray about this column at ConvergenceQA@go-rbcs.com. Ray Bernard, PSP, CHS-III is the principal consultant for Ray Bernard Consulting Services (RBCS), a firm that provides security consulting services for public and private facilities. For more information about Ray Bernard and RBCS go to www.go-rbcs.com or call 949-831-6788. Mr. Bernard is also a member of the Content Expert Faculty of the Security Executive Council (www.SecurityExecutiveCouncil.com). Follow Ray on Twitter: @RayBernardRBCS