

Securing the Pipeline

Norwegian powerhouse, Hydro, strengthens ties between IT and business leaders

The Norwegians have been seeking their fortunes in the North Sea for about 1,300 years. But it's been less than half a century—since 1963—that they found them. It was then that the country's scientists, economists, and government agencies agreed that the black pitch seeping from the coal beds on either side of the sea—the same goo their Viking ancestors used to seal the planks of their ships—would change the fortunes of the nation and along with it, one of its oldest commercial enterprises, Norsk Hydro (Hydro). “We are a true Norwegian company,” Torstein Gimnes Are says wryly. “We all have to agree on everything before we implement a solution.”

By Lynn Tryba

To Gimnes Are, Hydro's director of corporate information services security since 2004, that meant getting consensus on a policy to protect the data of a company that long outgrew its roots as a fertilizer manufacturer and is today a NOK200 billion (about US\$30 billion) per year enterprise, a leading offshore producer of oil and gas, and the world's third-largest aluminum supplier.

Simplifying solutions

To keep the information handled by Hydro's 33,000 employees in 40 countries safe, Gimnes Are focused on improving security reporting from technology solutions and simplifying data protection standards for Hydro's business leaders. “Better reporting gives us

better documentation to take to management when we need money to improve things,” Gimnes Are explains. “All the security processes we put into place for information risk management must be easy to understand and deploy. That improves our ability to

get best practices implemented in the business areas.”

The Hydro oil and energy business area is mainly centralized in Norway, while its aluminum metals and products business area operates factories and

offices worldwide. The information security standard is a complex 10-page document based on ISO 17799, an internationally recognized set of controls. Gimnes Are is currently simplifying the best practice documentation by communicating the relevant requirement to the right target group or role in the business areas. “I provide the corporate requirements as to how people can handle information electronically. But it is each business area's responsibility to abide by those requirements,” Gimnes Are says. “The IS organization strives to get the business side to take responsibility for information security.”

To that end, Gimnes Are has been working for the past year to anchor IS concerns into Hydro's enterprise risk management process.

“We began thinking this should be a bottom-up process. We would do a risk analysis for every system and then aggregate a risk picture for the information services systems. It is a demanding process and the CIOs from each business area wouldn't accept it,” says Gimnes Are. “Instead, they wanted a top-down approach, so we built the requirements into the enterprise risk management process. Now, when information systems pose an enterprise-level risk, we dig into a more detailed risk analysis of that system. Linking the process of information risk management to enterprise risk management has been an important task for us.”

Safeguarding systems

Having a strong security strategy is critical for Norsk Hydro, which, like other energy companies, uses Supervisory Control and Data Acquisition (SCADA) systems technology to monitor and regulate the flow of oil and gas through its pipelines. While SCADA makes data readily available to company engineers and contractors, it creates more risk because the system can be remotely accessed.

To better safeguard Hydro's computer systems, Gimnes Are needed a more comprehensive view on the company's security challenges, specifically patch management and the handling of viruses and malicious code.

Under Gimnes Are's leadership, Hydro expanded its use of Symantec antivirus and client security products, which provide antivirus, firewall, intrusion prevention, and antispyware capabilities. Symantec AntiVirus

» Inside the Pipeline

Backup Exec System Recovery Server
Symantec AntiVirus for Network
Attached Storage 4.3
Symantec AntiVirus Enterprise Edition
Symantec Client Security
Symantec AntiVirus for Mac
Backup Exec
NetBackup
Storage Foundation HA for Solaris

Enterprise Edition provides reporting, as well as centralized distribution of virus updates for enterprise-wide management. Symantec products also handle viruses from email attachments and spam emails. “On the technical side, we have achieved a great deal,” Gimnes Are says. “We now have monthly reports on patch and antimalware from all of Hydro’s business areas.”

Gimnes Are also described Hydro’s identity management processes. “We have procedures to ensure an employee operating a computer in a particular location is, in fact, the right person,” he says. “We have different levels of authentication depending on how critical the system is or what kind of information is stored there. Critical systems have stronger authentication requirements based on a digital certificate or two-factor authentication. The business areas define what is critical information and how it should be safeguarded.”

Business areas are required to run a risk analysis using a common harm reference table to assess risk. “If one of the business areas wants to provide a new application for e-business over the Internet, we require that they run the risk analysis to put the right security requirements in place for that application,” Gimnes Are says.

Internal support

Finding funding for information security projects can be challenging—at least on the aluminum side of the business. The oil and energy business area can support advanced IT systems, including remote oil production and e-operations, and also works continuously with user awareness. “In aluminum, it is more challenging. We have a lot of factories and offices globally,” Gimnes Are explains. “It’s difficult for those units



“Linking the process of information risk management to enterprise risk management has been an important task for us.”

—Torstein Gimnes Are, Director,
Corporate Information System Security, Norsk Hydro

to work methodically with information security because it’s a very distributed organization. I give the business areas our standards and procedures and follow up with internal audits to see if they implemented corporate requirements.”

When necessary, Gimnes Are funnels money to problem areas through Corporate IS Services. These services are intended to handle business-critical issues as well as the company’s common infrastructure. Each business area pays a monthly fee to Corporate IS based on the number of computers it uses. When Gimnes Are becomes aware of a threat, he approaches management with possible Corporate IS Services solutions. “If the business areas find it reasonable, we take money from Corporate IS Services to address threats,” he says.

In 2007, Gimnes Are intends to double the money spent on internal audits. “That’s the best measurement I have to check the effectiveness of information security work,” he says.

“Among other focus areas, we will continue to develop our use of the Symantec products. We’ll address both sides: technical solutions and an awareness campaign to make end users aware of their behavior. I think it’s important to put awareness on the agenda, but it is more effective to address security problems with technical solutions.” ■

Lynn Tryba is the managing editor of CIO Digest: Strategies and Analysis from Symantec.

Read Online:
www.symantec.com/ciodigest/emea/hydro