



From: [www.csoonline.com](http://www.csoonline.com)

## Case Study: Security Convergence

What does it take to make security convergence happen? One secret is to sneak up on it, the way Constellation Energy did, by seeming to be doing something else entirely.

by Sarah D. Scalet, CSO

**April 15, 2005**

At first glance, the security operations center for Constellation Energy Group is exactly what you'd expect from a high-tech Fortune 500 energy company. At the front of a windowless room twenty-some miles from the company's Baltimore headquarters, video monitors display office hallways, a trading floor, electrical substations and entrances to power plants. One screen is permanently tuned to CNN, which seems to be corporate America's ubiquitous intelligence source. Another shows a map of the world. Security operators are busy tracking and responding to events at facilities around the world. A smoke alarm goes off here, a door is held open too long there. The usual.



But that's not all that's being monitored.

The director of enterprise security checks his BlackBerry and then speaks in a low voice to the supervisor of the "information protection" unit, previously known as information technology security. The former is a onetime Marine, with closely cropped hair and a dark suit and tie, whose background is in corporate security and executive protection. The latter sports a well-groomed mass of curly locks, a soul patch beneath his lower lip, no necktie, and a handkerchief jutting out his jacket pocket. Until recently, he reported to the IT department rather than corporate security. Only a few feet from where security operators are monitoring gates and guards, these two very different men are assessing the security announcements from Microsoft on this "patch Tuesday." The particular workstation they stand in front of displays not a video feed but a security-incident management system that draws together information about the company's firewalls, intrusion-detection systems and other network operations.

Welcome to a converged security operations centera work in progress.

"We haven't made a full determination yet on how this is going to be integrated," says John Petruzzi, the former Marine who is director of enterprise security, as he surveys the room. Right now, two workstations are used to monitor physical systems, and a separate workstation is used to monitor logical or information systems. But Petruzzi thinks that may change within the year.

"We're leaning to the fact that we can get it to a point where the console operator will be integrated," he says. "I think we're almost there." That would mean that each security operator would monitor all kinds of security

incidents, both physical and virtual.

Call it integration; call it convergence; call it holistic security. Whatever its name, it is budding in this room and others like it across the country. In 2006, according to Forrester Research, North American companies will spend \$1.7 billion on projects that combine traditional physical security and IT security more than five times as much as they spent in 2004. And Constellation has undertaken the most ambitious type of convergence project of all: the wholesale integration of the two departments.

Along the way, those involved with the project are facing political, logistical and cultural challenges, with little to guide them. "I have not seen a repeatable organizational model for a completely converged, centrally managed security operation [that includes] physical and IT security," Forrester analyst Steve Hunt warns. (After this story was reported, Hunt resigned from Forrester to launch 4AInternational, a security consultancy that will focus on convergence strategies.) But he's delighted that companies such as Constellation are trying. "With good management, anything is possible. There's a chance they could succeed and save a lot of money and be much better than they ever were before at mapping security to actual business value."

What's more, if Constellation has its way, it could even be mapping out how the next generation of security will look. The New Guard At Constellation, the dramatic transformation to bring together information security and physical security can be traced straight to the top to Mayo Shattuck III, who took over as chief executive just weeks after the terrorist attacks of Sept. 11, 2001.

Shattuck could hardly have chosen a more tumultuous time to leave his post as president of Alex Brown, a Baltimore-based unit of Deutsche Bank, to take the reins at Constellation, then a \$3.9 billion energy generator and distributor. The energy industry had already been battered by the California energy crisis and concerns about terrorist attacks on the power grid. It was about to absorb another blow, with the collapse of Enron. And Constellation itself was in turmoil. On the heels of a failed attempt to merge with Potomac Electric Power, Constellation had just scrapped a plan to split into two companies: a regulated power distribution business and a nonregulated production and trading business. The company paid \$355 million to Goldman Sachs, its investment partner, to get out of the deal.

It was time for a regime change. It was time to focus on risk.

"Coming from the banking world, I was struck by the lack of centralized risk management on day one," Shattuck says. "It was probably the afternoon of day one that I decided that immediately I needed to mirror the way in which a universal bank [approaches] risk."

As Shattuck remade his senior management team, one of the most prominent new players to emerge was John Collins, a longtime finance employee who became the company's first chief risk officer (CRO).

"Originally we looked primarily at the financial risks—the risks around our marketing and trading operations, the risks around our loan-servicing business, commodity price movements," Collins says. "At the same time, my vision was always to also incorporate operational risk. Both security and business continuity planning seemed to be in places in the organization where they weren't really getting enough high-profile attention."

In late 2002, Collins officially expanded his purview. He took control of the company's business continuity and corporate security operations, which had been part of the general services department. But information security wasn't ready to make the move just yet.

That's because Beth Perlman, the company's first-ever CIO, was still trying to get a handle on the piecemeal systems that had grown out of decades of the business lines operating independently. "When I came here, you could not tell that all the divisions were part of the same company," says Perlman, who was hired in April 2002. "If I wanted to access our HR system, I had to go through firewalls. We did not have one IT security department; we had many IT security departments. The first step of convergence was formulating one IT security group. The last thing I wanted to do was just dump something that didn't work."

By this point, though, the players were all in place. Brandon Dunlap, supervisor of the information protection unit under the risk-management organization, had been hired to manage IT security. And Shattuck himself had

brought aboard Petruzzi, who had worked in executive protection at Alex Brown. Shattuck trusted Petruzzi, who had accompanied him on trips to South America to coordinate his protection, and thought that Constellation would be a good spot for Petruzzi to build and broaden his career.

As it turned out, Petruzzi, now just 34, would broaden a lot more than his own career. Not Just Another Project "We started [at Constellation] within, what, two weeks of each other, and started meeting almost regularly right after that," Dunlap says to Petruzzi, as Petruzzi settles into a chair in a conference room next door to the security operations center. Petruzzi has asked his three direct reports to gather here on this January afternoon to talk about how the convergence process is playing out.

There's Dunlap, with his cultivated eccentricity and deep technical know-how. (He's on the faculty of the Institute for Applied Network Security.) There's Frank Woods, a 25-year Constellation veteran who used to be supervisor of the security operations center but is now supervisor of a new access- management unit, which will handle all requests for logical and physical access companywide. Finally, there's Dave Feeney, the newly promoted supervisor of the security operations center, whose emphasis has been on making sure the operators hired to work in the center have plenty of tech savvy.

(Petruzzi's direct manager, Jack Ryan, declined to be interviewed for this story. Ryan, a 21-year Constellation employee who is head of corporate security, indicated through corporate communications that "all bases have been covered" by this story's other sources.)

There's an easy banter between the three men and their new manager, and a vitality that feels more like an Internet startup than a century-plus-old energy company. Petruzzi's crew had already dug into lunch by the time he arrived from headquarters with a reporter in tow. Dunlap makes a crack about Petruzzi still not letting him carry a gun. The conversation moves fluidly from network sensors to smart cards to concealed duress buttons that trigger alarms. Wasn't it always this way?

The convergence process didn't start as a big explicit project and this is key. "We didn't have a name for it," Dunlap says. "We didn't call it 'convergence.' We just thought, wouldn't it be great if we could work together more closely for efficiency."

As at many companies that have brought together physical and information security, the evolution began with the investigations group. Because investigations were conducted by corporate security but often involved data stored on computers or passed through e-mail, there were frequent handoffs between corporate security and IT. At the same time, the IT department was growing its monitoring capabilities. Dunlap's staff might notice inappropriate behavior on the network and report it to investigations.

"There was never this, 'We're shoving this down your throat,'" Dunlap recalls. "It was more like, 'Hey, if you're doing that, you really should get these guys involved.'"

Meanwhile, there was increasing recognition that information security belonged under risk management not technology. This was driven partially by the risk-management approach that Collins was spearheading and partially by regulatory concerns.

"When you look at corporate security," Collins explains, "the evolution of it has to be with information technology security, because you won't address the whole security environment unless you're looking at it together. We also think that it's the right thing to do, because otherwise you have the IT department watching the IT security, and is that really good internal control?"

There were financial incentives too. Collins believed that combining physical and IT security would simply be more efficient and effective. For instance, he thought the company could save labor costs by merging network and physical access monitoring. Simply put, Constellation wouldn't need as many guards.

By summer 2004, executives started mapping out the split. IT systems maintenance would stay within the IT department, but IT security would keep track of any maintenance required from a security perspective. IT security renamed "information protection" to distinguish it from IT would operate as a consultant to IT. "Gartner lite," Dunlap calls it, referring to the IT consultancy.

Here's how things would play out. If a change needed to be made to a firewall, the information protection group would make a request, and the IT infrastructure department would carry it out. If there was unusual activity on a port, information protection wouldn't disable it; they would call the network technicians. If a system needed to be patched, information protection would do the research and testing and then put the word out.

Complicated? Yes. But it made sense.

"We said, 'OK, this is a segregation of duties,'" says Perlman, the CIO. "You [security] are a consumer of the tools. We [IT] deploy the tools. Checks and balances."

Gradually, as the IT security function came together and started to operate more smoothly, its staff began working more closely with security, writ large. On Oct. 1, 2004, IT security employees officially started working for corporate security. The switch was thrown. Power Shift As CIO, Perlman stood to lose the most. After all, she was giving up employees and budget, and therefore power. But if this bothers her, she doesn't let on during a meeting with a reporter in her office on the top floor of Constellation's headquarters. Her lament instead? Now that IT isn't directly involved with investigations, she says with a laugh, "I don't get the dirt anymore. That's what I miss."

In truth, Perlman didn't lose much more than a few headaches. Only 12 IT employees and a handful of contractors made the move to corporate security, hardly denting her staff of 550 full-time employees and 150 contractors. The only part of her budget that has been moved, at least so far, is for security salaries and consultants. IT still controls the budget for everything from antivirus software contracts to smart cards, charging back costs to the business units. And not knowing "the dirt" anymore means that Perlman doesn't have to drop everything to deal with an investigation.

It also helps that she trusts Petruzzi. "If you don't trust the person you're giving the group to, forget it; it will never work," Perlman says. "While we were cleaning up our own shop, we were working on building trust with each other's groups."

Not that everything is perfect. Perlman and Petruzzi are still finessing the line between operations and security. They're also talking about moving more of the budget over to security for the next fiscal year. And the two don't always agree. Far from it. For instance, they're still trying to work out the best way for traveling employees to sign onto e-mail. Right now, employees use SecurID tokens from RSA, in addition to passwords. Perlman feels that the tokens are an expensive bother (one that her department must pay for and support) and would like to phase them out. Petruzzi's team thinks otherwise.

"The question is, is the cost of that infrastructure worth it, or are there other measures we could take?" Perlman says. "That's where we're having an argument. [Petruzzi] thinks the other options that we're offering are not as secure, so we're trying to say, what's the risk?"

"We just don't see that your cost-avoidance by doing away with the RSA tokens is worth the risk," answers Petruzzi, whose information protection group put together a page-and-a-half-long report outlining arguments against the change. Gartner lite.

For the time being, the two have tabled the issue until they address a new identity access and management plan next quarter. In other words, they have agreed to disagree. Their relationship is solid enough that when Perlman's assistant can't find her, she looks in Petruzzi's office. The RSA tokens are still in use, and Perlman isn't unhappy, because no one has said "no" to her without offering options.

"If it gets to the point where somebody says, 'You can't do that,' and doesn't offer me options," that's when the new structure isn't working, Perlman says. "You have to be good collaborators. You have to understand this is a business problem we're trying to solve." The Future of Security For Petruzzi, who has a degree in criminal justice, it's all part of the crash course he's been taking since joining Constellation. He's taken SANS Institute courses. He does outside reading. He peppers Dunlap with technical questions about solutions they are considering, making sure he has a sufficient understanding of the risks involved. And he's encouraging his staff members to do the same. In fact, he has told them that their performance will be evaluated, in part, on whether they make themselves into what he calls "the new breed of security specialists."

Training doesn't have to be complicated. It might consist of a few symposiums or on-the-job training with someone who has a different kind of security background. "It doesn't mean you have to be an expert," he says. "It means you need to be able to stand in court or in front of executives and state things clearly."

Those who have remained at Constellation through the turmoil of the past three years say they have embraced this new strategy largely because both IT and physical security staffs saw their positions as being elevated.

Woods, who runs the new integrated access management unit, remembers "the days when corporate security existed in a basement under the general services division. It was like the cleaning personnel and then security below them. We didn't have much authority." Now, corporate security has a clear line to the CEO.

Dunlap, too, saw convergence as an opportunity. "Before, we were kind of...I don't want to say sequestered, but to some degree we were just another guy at the table," he says. "We saw coming out and working for the risk management group as a kind of independence. It's not that we necessarily swing a bigger stick, but we have a very clear escalation path that doesn't go to the CIO anymore. It's not a server maintenance problem. It's a vulnerability management problem."

As for Petruzzi, he's getting savvier about navigating that escalation path. Collins, the CRO, has led him to approach things from a financial risk management perspective. It's been an education. It took Petruzzi three tries to get his first business plan right.

"The first-year approach was kind of going to be, let's just let things run how they are and build a better plan instead trying to come out of the gate with this plan to consolidate, reduce costs and make a more oversight-oriented business function," Petruzzi recalls. "That didn't fly. It was kind of like, 'That's not going to work. I'm a finance person. I want you to show me where you have places you can save costs by consolidation.'"

Three months later, Petruzzi finally got the plan approved and along the way became conversant with the finer points between, say, cost reduction and cost avoidance. Because Collins is chief risk officer and not chief financial officer, Petruzzi says, the focus on cost savings doesn't happen at the expense of good security. "At the same time that [Collins] is making us be financially responsible, he also is saying we're only going to go to a certain level of risk," Petruzzi says. He speaks like a person who has transformed from someone who merely secures assets into someone who analyzes and balances risks. Could it be that at the CSO level, the "new breed of security specialist" will not be a security specialist at all?

As for Constellation, it's still too early to say whether the project truly will lead to the increased efficiency and effectiveness that the company is expecting. Hunt, the analyst, doesn't mince words about the odds Constellation is up against.

"I think that most converged departments lead to a loss of efficiency, of effectiveness, or [to] utter failure. I wish it weren't that way." Hunt is convinced that companies will just not be able to reconcile the cultural differences between the two departments. He also suspects that in the long run, the most effective "convergence" may lie not in the integration of the two departments, but in targeted, specific projects done jointly—say, the installation of a new access management system.

Nevertheless, it's hard to argue with what Shattuck has done as CEO. Under his risk-focused leadership, the company has tripled in size. On the 2004 Fortune 500 list, it jumped from position 352 to 203. Revenues for 2004 topped \$12.5 billion, increasing from \$3.9 billion in 2001. And Shattuck is bullish that the new structure is already working.

Every Monday he begins his week by meeting with his risk management committee. Not only does he get a window into the company's current financial risks, but he finds out about security vulnerabilities. He doesn't care if they are physical or virtual, only whether they could hurt the company.

"This is really a top-down perspective," Shattuck says, "but for me [the converged approach is] the most convenient way of dealing with risks."

© CXO Media Inc.



**Eliminate network threats and downtime.  
The switch is on to comprehensive network security.**

