The merger of United Air Lines and Continental Airlines in October 2010 resulted in an airline with the most comprehensive route network in the world, serving 376 destinations on six continents through 10 hub locations. Integrating systems and processes of both airlines into the “New United” is not an easy feat—and not one that will take place overnight. The first major milestone was the issuance of a single operating certificate on November 30, 2011. The second was the merger of the two airlines’ passenger service systems, including frequent-flyer programs and websites, on March 3, 2012. And much more is to come.

Technology has always been important to both United and Continental Airlines, but it took on new meaning because of the merger. “Our CEO, Jeff Smisek, characterizes the ‘New United’ as a technology company with wings,” says John Van Hoogstraten, managing director of IT Security and Risk Management at United. “IT is central to everything that we’re doing as a company. This includes security and compliance. It must permeate everything we do.”

The IT organization took the merger as an opportunity to completely reassess its IT toolsets and infrastructure. “We are taking the best of both worlds,” Van Hoogstraten says. This includes the security and compliance programs. “When you look at the IT infrastructures of both companies, they are very much organic,” he continues. “They work, but they are pushing the boundaries of maintainability and flexibility—and this was before the merger. As we launch the new United brand and the underlying systems and services that go with it, this is a perfect time to reassess our overall IT strategy and approach to security and risk management.”

Saying no to the “no” culture
“Historically, security has been a culture of ‘no’ in many IT organizations,” Van Hoogstraten says. “As
IT has become the business—and this is certainly the case at United—and consumerization of IT and the cloud emerge as driving factors, this simply won’t fly any longer. We must work with the business so that security is part of the solution.

At the same time, security and compliance functions aren’t any easier to manage. “Just a few years ago it was easy to identify the edges of the perimeter,” Van Hoogstraten observes. “But with the introduction of more and more mobile devices and adoption of shared services, a blurring of the edges has occurred.”

The “new security”
So what is Van Hoogstraten’s proposed solution? Tighter integration with the business. He’s structured his team so that different members are assigned as virtual team members of not only broader segments of the business but specific project teams. Take the airline’s move toward mobility as an example. “Recognizing the emergence of trends such as consumerization of IT and the rapid adoption of mobile devices, we have a team developing a series of corporate mobile apps for employees, partners, and customers,” Van Hoogstraten says. “The first app to be rolled out is called the ‘Electronic Flight Bag’ and is part of our larger strategy to equip our 11,000 pilots with iPads.”

Using the Electronic Flight Bag app, pilots will be able to discard their conventional flight bags containing everything from operating manuals and reference handbooks to navigation charts and flight check lists. “The cost savings and environmental impact is huge,” Van Hoogstraten points out. “The reduction in weight equates to 326,000 gallons of jet fuel savings each year, or a 3,200 metric ton reduction in greenhouse gases.” In addition, pilots will consume a sum total of 16 million sheets of paper less each year, or the equivalent of 1,900 trees.

When it comes to security, Van Hoogstraten has a member of his team assigned to the mobility app development team who works with them to design the solutions from the ground up with security standards in mind.

“We’ve taken the same approach with application development in general,” Van Hoogstraten says. “We get involved at the forefront and make sure that security standards and compliance protocols are involved during the design stages. This ensures that our applications are, number one, secure; and number two, security friendly.”

There are a number of benefits as a result of this approach. Van Hoogstraten elaborates: “Because our team is involved throughout the development lifecycle, we can deploy applications more quickly and minimize last-minute hold ups due to security testing and remediation. Building secure and security-aware applications means that we can also significantly reduce the need for complex and costly compensating controls while still taking a layered (defense in-depth) approach to securing United’s IT environment.”

Strategic security and IT risk management
Making security and IT risk management more strategic is offset by a reduced focus on operational aspects. Van Hoogstraten explains: “We are trying to get day-to-day functions from my team to the operational teams so that we can focus on a more strategic approach. An example would be our network firewalls. I don’t want to own their day-to-day troubleshooting and management.”

Another instance where Van Hoogstraten wants to offload the responsibility is monitoring and managing the threat landscape. “I don’t want to be in the security

Flying Data Center
Planes are becoming “flying data centers,” according to United’s John Van Hoogstraten, managing director, IT Security and Risk Management. “We’re talking about real-time telemetry, computer systems that directly interface with the aircraft,” he says. “We can even troubleshoot mechanical problems while planes are in the air. Aircraft begin a data download before they even reach the gate, including cabin inventory and maintenance information. This allows us to service and turnaround flights more quickly and minimizes maintenance downtime.

A great example of how technology has become an overarching issue is in the engineering and shipment of the next-generation Airbus and Boeing aircraft that United will be adding to its fleet—the 787 later this year and the A350 in 2015. “I have members of my staff at Airbus and Boeing facilities working alongside their engineering and manufacturing teams to ensure that security standards and the corresponding IT infrastructure are embedded in those aircraft—both control systems and customer service systems—when they ship.”

symantec.com/ciodigest 37
operations center business,” Van Hoogstraten relates. “I see low value in managing an in-house security operations center. Our internal resources can be better utilized on initiatives that deliver more tangible business value.”

Seeing the cloud through the star
Because of the breadth and complexity of its operations, United sees immense advantages through cloud services. The IT department has focused on private clouds—Platform as a Service (PaaS), Software as a Service (SaaS), and Infrastructure as a Service (IaaS). “Security and compliance standards must be built into all of the applications that we deliver through the cloud,” Van Hoogstraten says. United has several objectives as it extends its current cloud services and builds additional ones. “Cost is obviously one,” Van Hoogstraten notes. “Flexibility is another. Our internal customers require rapid configuration and deployment of services; our private clouds provide this capability. We also have what we call ‘elasticity on demand,’ the ability to quickly scale up and back down again based on computing-demand fluctuations. At the same time, this model is something that has indirect cost advantages for us.”

Further evolution of the private cloud is on the horizon for United. A next-generation data center will go online in the near future that will be predominately dedicated to private cloud services. “The cloud delivers lower costs and greater agility,” Van Hoogstraten explains. “My team is already working with the data center team to ensure that security and compliance standards are part of the architectural design.”

Compliance uplift
Compliance is a critical requirement for United. “We’ve been heavily focused on PCI (Payment Card Industry Data Security Standard) because of credit card transactions,” Van Hoogstraten says. “For the passenger service system deployment, as the entire e-commerce environment is tied into it, getting the right compliance frameworks and reporting structures was vital. PCI has certainly been a focal point for us and the passenger service system rollout.”
United and Continental had disparate compliance toolsets, and Van Hoogstraten and his team conducted a thorough evaluation and are in the process of deploying a standard compliance solution based on an integrated set of tools. “Symantec Control Compliance Suite is one of them,” he says. “We did not have an integrated solution at United but rather a number of point solutions. Continental had been using Control Compliance Suite for a number of years and had achieved tangible results with it.” With Control Compliance Suite, Van Hoogstraten’s team will be able to automate a number of different compliance processes that were previously manual, allowing them to work on other initiatives that drive business value.

Security management and data loss prevention flight path

For security management, Continental had relied on Symantec Security Information Manager. United used big logging engines to cull the data, which was then aggregated and fed to a third party. Before the merger, Van Hoogstraten had an abortive attempt at deploying a competitive toolset to Symantec and discovered that it wasn’t a suitable fit for his requirements.

“Very quickly, it became apparent that we would need four full-time headcount just to manage the solution,” he says. “Continental had a positive experience with Security Information Manager and it met our needs, providing a comprehensive view of and reporting across our environment—all with minimal fuss.” Though not scheduled for full deployment until later this summer, the solution will reduce the cost and time required to manage security.

Another area of focus for Van Hoogstraten and his team is data loss prevention. “While protecting the infrastructure remains critical for us, particularly because of the nature of our business, protecting our information is just as important,” Van Hoogstraten comments. “Continental had a very successful implementation of Symantec Data Loss Prevention that we plan to extend across our entire environment later this summer.”

Working with the different business owners, Van Hoogstraten’s team will reverify the policies for endpoints, storage, and eventually the network. They also plan to use Data Loss Prevention for Tablets to monitor, manage, and enforce data loss prevention.

Building the World’s Largest Airline

The first flight linked to United occurred on April 5, 1926, when Varney Air Lines—based in Boise, Idaho—flew the first contract Air Mail flight. The flight was the first scheduled airline service in the United States. William Boeing founded his own airline, Boeing Air Transport in 1927, and began buying other airmail carriers, including Varney Air Lines.

In 1929, Boeing merged the company with Pratt & Whitney to form United Aircraft and Transport Corporation. The company launched passenger services in 1933 with the operation of the Boeing 247, enabling travel across the U.S. without an overnight stop or changing planes. With the passage of the Air Mail Act in 1934, the company broke into three entities—United Aircraft (eventually becoming United Technologies), the Boeing Airplane Company, and United Air Lines. With the end of World War II, consumer demand for air travel boomed, with revenues jumping fivefold during the 1950s.

United displaced American Airlines as the world’s second largest airline when it acquired Capital Airlines in 1961. The airline’s history is full of first and industry-leading initiatives. The company purchased Pan Am’s entire Pacific Division in 1985 and the airline’s routes to London Heathrow Airport in 1991. It was the first carrier to operate the Boeing 767 in 1982 and Boeing 777 in 1997. United is a co-founding member of the Star Alliance, and with its merger with Continental Airlines in 2011 (single operating certificate received on November 30, 2011), United became the world’s largest airline. Its coverage includes 376 destinations in 61 countries and more than 5,600 daily departures.
Using VMware vSphere and several Microsoft Windows servers over the past couple years. Several thousand endpoints, and we can already see improvements there.”

Endpoint security tailwind
Symantec Endpoint Protection has been a mainstay for endpoint security at United and Continental for many years. Endpoints are much broader in scope for United than simply desktops, laptops, and the data center. As a starting point, United has several thousand servers and storage systems in its data centers. “It is a very heterogeneous environment,” Van Hoogstraten says. United also has approximately 40,000 clients, primarily consisting of desktops and laptops. “We also have all of the airport information display systems, call center terminals, airport terminals, and check-in kiosks,” Van Hoogstraten adds. “We must secure all of these different endpoints, and this does not include the rapidly growing number of mobile devices.”

The United team is currently in the process of upgrading to Endpoint Protection 12, a project Van Hoogstraten expects to complete this summer. “New features such as Insight technology and the scan engine will provide us with enhanced security and better system performance,” he notes. “We’ve rolled it out to some of our endpoints as well as virtual machines in the data center, and we can already see improvements there.”

United has moved rapidly in the direction of virtualization over the past couple years. Several thousand Microsoft Windows Server operating systems are virtualized using VMware vSphere and several hundred Oracle servers are virtualized using Solaris Containers. This presents a number of security and compliance challenges. The standardization initiatives Van Hoogstraten and his team are spearheading certainly improve the organization’s IT risk posture and drive efficiencies. But this is a stepping stone, according to Van Hoogstraten.

“Eventually, I would like to get to the point where I can tag a ‘container’ as PCI-sensitive or containing highly confidential information,” Van Hoogstraten comments. “Then, wherever that ‘container’ goes, regardless of where it resides in the data center, it automatically takes the same security posture with it. This obviously will require further work with our various technology providers—VMware, Symantec, Oracle, HP, Microsoft, and the like—but it is a desired state that we hope to achieve in another couple years.”

What’s emerging
The recent advertisement touting the newly merged United depicts aircraft undergoing a complete retrofit to the airline’s new brand—logo and colors. The commercial closes with the tagline: “Who’s merging is not nearly as exciting as what’s emerging.”

This is quite true: the results of the merger are really what matters. What’s really exciting are the new services that will be available—from expanded network route coverage, to a fully integrated passenger service system, to a new fleet described as “flying data centers.” And IT—including security and risk management—is at the heart of all of these efforts. Indeed, without IT, like

From Gliders to IT

John Van Hoogstraten’s roots are in the airline industry. His father-in-law was an airline pilot for more than 35 years. Van Hoogstraten started flying gliders in the mid-1980s and became a commercial pilot in 1990. In 1995, he took a position with a dot-com startup that was doing pioneering work in two-factor authentication and secure communications (bank-to-bank) over the still nascent Internet. This is when Van Hoogstraten first became interested in information security. “The career move was supposed to be temporary,” he says. “But it eventually evolved to the point where I found IT to be more challenging and interesting than being a commercial pilot.”

A couple years before the dot-com bubble burst, Van Hoogstraten took a position with Southeast Toyota. There, he served in a number of different roles over a 10-year period, including overseeing the information security function during his final five years. Early on in his career, Van Hoogstraten had an opportunity to gain a wide range of experience in different IT areas—including IT infrastructure, enterprise architecture, project management, disaster recovery, and business continuity. This experience serves as a valuable backdrop for him in his current role. “I have a broader understanding of the business because of the breadth of IT roles that I’ve held,” he notes.

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.