PAINTING AN IT LEGACY

Jirawan Chiasakul,
CIO and VP, IT Services Department
Thai Airways International

Safety on the Go  Pg 26
Five Ways to Be Socially Cool  Pg 32
There are no limits when NEC takes care of the clouds

You may not be able to see our cloud but its positive effect on your business will be clearly visible. It optimizes reliability, grows revenue, lowers costs and creates new value chains. In our challenging and ever changing business environment these benefits will soon become clear. Today, more revenue streams are open to our partners and customers because NEC uniquely enables the creation of their new businesses by integrating both data-centre technology and telecom networks. Thanks to our invisible cloud, the sky and your business future are bright. www.nec.com/cloud
[ COVER STORY ]

Painting an IT Legacy
Over her 33-year career at THAI, CIO and VP Jirawan Chiasakul has seen IT go from a single application to a cluster of turbines propelling the company down the runway.
By Patrick E. Spencer

3  [ FROM THE CEO ]

Anatomy of a Data Breach
Stopping the drumbeat of data breaches.
By Enrique Salem

8  [ THINK TANK ]

Do CIOs Really Care About Security?
Where you spend your time reflects your business priorities.
By Gary Beach

10  Sustainable IT
As the dust settles, business value appears as principal driver.
By Patrick E. Spencer

[ MOBILITY FEATURE ]

Safety on the Go
Developing and implementing a mobile security strategy becomes increasingly more important as mobile devices proliferate.
By Mark Mullins

[ SOCIAL MEDIA FEATURE ]

5 Ways to Be Socially Cool
Organizations must implement the right social media strategies to minimize security and compliance risks.
By Courtenay Troxel

BEST PRACTICES

[ AMERICAS ]

Matriculating IT
Virtualization and cloud services are helping Northeastern Illinois University deliver value-added services to its students while optimizing IT assets.
By Patrick E. Spencer

Cover Photo by Michael Brunetto
“Due to our recent cost reductions, the company decided to use empty server racks to keep our cafeteria food warm.”
This year, there has been a steady drumbeat of data breaches in the news. It might seem reasonable to regard data breaches as an inevitable by-product of our connected world—a cost of doing business that we must simply learn to live with. It’s easy to reach this conclusion when we look at the connection between targeted attacks and data breaches.

As reported by the Ponemon Institute, malicious or criminal attacks are the most expensive cause of data breaches, and they are on the rise. In 2010, more than 31 percent of data breach cases involved malicious targeted attacks. To combat a data breach, the following three important truths must be recognized by organizations.

First, breaches are preventable. The three primary root causes behind them involve well-meaning insiders, malicious insiders, and targeted attacks. In each of these scenarios, there are key points within a targeted attack where countermeasures can be implemented to stop a data breach. The latter include incursion into the company’s network, discovery of data, capture of the exposed data, and exfiltration of the confidential data.

Second, the strategies with the best chance of success are both risk-based and content-aware. Preventing data breaches is all about risk reduction. To reduce risk, you must know where your data is stored, where it is going, and how it is used. Only then will you be able to clearly identify and address problematic practices.

Finally, preventing data breaches requires multiple solutions that work together to solve the problem. This means that the solutions an organization deploys must be integrated to create a centralized and actionable view of information security.

This issue contains some great content, starting with an exclusive interview with Jirawan Chiasakul, the CIO of Thai Airways International, who discusses her 33-year career at the airline and some of the key initiatives she and her team are driving today. Readers will also want to check out the two features. The first one maps out five ways organizations can minimize security and compliance risks. The other feature delineates some of the different strategies that IT organizations are employing to secure and protect information and identities as mobile devices and applications proliferate. Finally, don’t miss our case histories on thought leaders such as Northeastern Illinois University and Trusted Source and learn how they are relying on various Symantec solutions to enable their organizations to rise to new heights.

Regards,

Enrique Salem
President and CEO, Symantec Corporation

Adjusting to the New Normal
IT plays critical role to grow business

A new report from the Hackertt Group’s Key Issues study reveals that while IT continues to adjust to the “new normal,” doing more with the same or slightly more resources than last year, IT must continue to align initiatives to meet business requirements.

The top five issues shaping the executive agenda in 2011 include:

> Grow revenue, especially in global markets
> Improve competitiveness through increased productivity
> Counter market uncertainty through improved analysis and decision making
> Move from multinational to global strategies and operations
> Manage talent in asymmetrical markets

The combination of an uncertain business outlook and mandates for growth results in two critical requirements for IT to address:

> Develop new (or streamline existing) capabilities that can support enterprise efforts to grow revenue and support innovative business models
> Increase globalization of IT operations to raise business-function productivity while maintaining costs

This year’s IT priorities have a greater focus on business alignment and system agility. To learn more about what business needs from IT organizations, visit go.symantec.com/hackertt-it2011.

>> Internet Matters
Net plays important role in GDP

New McKinsey research found that the Internet now accounts for a significant and growing portion of global GDP. With millions of daily online transactions and communications, as well as downloads of all types of entertainment, the Net has become an explosion of economic growth.

Key findings from the McKinsey Global Institute (MGI) include:

> The Internet accounts for 3.4 percent of overall GDP in the 13 nations studied. More than half of that impact arises from private consumption, primarily online purchases and advertising.
> The Internet is a critical element of economic progress, accounting for 10 percent of GDP over the 15-year period from 1995 to 2009, and its influence is expanding.
> Most of the economic value the Internet creates falls outside of the technology sector: companies in more traditional industries capture 75 percent of the benefits.

These findings suggest that corporate leaders will need to sharpen their focus on the opportunities the Internet offers for new products and expanded customer reach. For more information, visit go.symantec.com/mckinsey-net.

<table>
<thead>
<tr>
<th>SYMANTEC CHRONICLES</th>
</tr>
</thead>
<tbody>
<tr>
<td>How To Lead</td>
</tr>
</tbody>
</table>
Symantec president and CEO Enrique Salem shares his thoughts on leadership and culture in a recent New York Times Q&A feature in the Corner Office. In the article, Salem highlights lessons learned from Shakespeare, Tennyson, and Colin Powell—about taking chances, learning from others, and staying positive. In addition, Salem highlights how his leadership style has evolved to be more direct to deliver a tough message. Although Symantec is a $6.5 billion company, Salem promotes a start-up culture where people are multidisciplined, take risks, and want to win. To learn more about Salem’s leadership, visit go.symantec.com/enrique-qa.
| Symantec Scores High in Dow Jones Indexes |
Symantec has been recognized as a corporate sustainability leader in the Dow Jones Sustainability Indexes (DJSI) for 2011. Symantec received the highest score in three areas: Software as a Service, Talent Attraction & Retention, and Corporate Citizenship and Philanthropy. The DJSI follows a best-in-class approach, including numerous sustainability metrics. For more information, visit go.symantec.com/djsi.
Social Media Protection
Safeguard against brand damage

More and more enterprises are embracing social media as a way to better share information, build stronger relationships with employees, partners, and customers, and generate increased revenue. But along with the benefits social media has to offer, there are potential risks if not properly prepared.

In Symantec’s recent Social Media Protection Flash Poll, it was found that enterprises risk increased litigation costs, damage to company reputation, and lost revenue due to social media incidents involving:

- Employees sharing too much information in public forums (46 percent)
- The loss or exposure of confidential information (41 percent)
- Malware (37 percent)
- Violating regulations (36 percent)

In fact, 94 percent of the organizations surveyed experienced the above incidents, resulting in increased exposure to litigation (37 percent), damaged brands (28 percent), and lost revenue (25 percent), costing a typical company $4 million over a 12-month period.

Companies are aware they must protect and retain all business communications and other unstructured data, and the same goes for social media content. As social media becomes pervasive in the enterprise, controls must be put in place to capture social media communications to comply with open records requests and industry regulations.

The survey also found that 82 percent of enterprises are discussing implementing archiving solutions to collect, preserve, and discover sensitive business information transmitted through social media, along with establishing social media usage policies and employee training. These findings are in line with the top three IT concerns: regulatory compliance (45 percent), information retention policy compliance (45 percent), and management of eDiscovery (37 percent).

For more information on what steps to take to safeguard against the potential risks of social media, visit go.symantec.com/sm-flash.

Symantec Intelligence Report
Pump-and-Dump Spam Campaign

Turbocharged financial markets trigger “pump-and-dump” stock scams, according to Symantec’s Intelligence Report released in August. In a pump-and-dump campaign, spammers promote certain stocks to artificially “pump” up the value and then “dump” them before their valuation crashes back to reality for a profit.

In addition, the report also revealed that there were as many new malware boot time (MBT) threats in the first seven months of 2011 as there were in the previous three years. An MBT is an area of the hard disk used by a computer to perform start-up operations. MBT infections can take control of computers, which make them attractive targets to malware creators.

The report also highlights that phishing activity increased, with many attacks coming from major brand names such as Apple’s iDisk service and a variety of Brazilian companies, including social networking and financial brands. Symantec identified an average of 3,441 websites each day harboring malware and other potentially unwanted programs such as spyware and adware; a decrease of 49.4 percent since July 2011. For more information, visit go.symantec.com/aug-intell.
The Evolving Role of CSOs

Focus on managing risk, not just security

The 2011 State of the CSO survey conducted by CSO Magazine highlights how the role of the CSO is evolving in today’s business climate. The findings show large organizations view a security leader’s role as strategic and essential to the business, with established security policies in place. With smaller organizations however, security awareness is still a work in progress.

The survey also revealed that organizations are placing increased value on risk management, with more time spent on regulatory compliance. In addition, over 50 percent of respondents use a formal enterprise risk management process or methodology. This includes multiple types of risks, such as disaster recovery, which influence behavior and justify security budgets.

The top technology trends that will have significant impact on the role of security professionals and risk to the business include:

- Ubiquitous data, 24/7
- IT on demand (e.g., cloud computing)
- Next-gen workforce with different values and work ethics
- Social media
- Consumerization of desktops and devices

As the security role becomes more aligned to the business, so do the responsibilities in strategically managing the ever-increasing operational risks to the business. To learn more, visit go.symantec.com/cso-2011.

>> Cybersecurity Challenge

Report highlights new cybersecurity model

The latest McKinsey research, “Meeting the Cybersecurity Challenge,” details how protecting business from cyber threats continues to be a critical management issue. While enterprises have dramatically strengthened their security capabilities, the survey found that there is still a growing concern over cybersecurity. The findings reveal five common trends that make corporate environments harder to protect:

1. Customer data creates a bigger incentive for cybercriminals as more information migrates online.
2. New devices such as tablets and smartphones are being used to access the corporate network, presenting new types of security threats.
3. Supply chains are increasingly interconnected, making it impossible to separate out a company’s technology environment.
4. Cybercrime is becoming more sophisticated and outpacing the skills and resources of corporate security teams.
5. Social networking sites are increasingly being used to design highly targeted “phishing” attacks, capitalizing on human vulnerabilities to spread spyware.

Because of these issues, a new business-driven cybersecurity model is starting to emerge. To learn more about what steps to take to ensure that cybersecurity is sufficiently addressed, visit go.symantec.com/mckinsey-cybersecurity.

>> data loss prevention technology to analyze Microsoft Exchange email content and metadata. Email content and metadata are automatically classified and assigned the appropriate archiving and retention policy and can even be flagged to be reviewed for compliance reasons. Another new feature of Enterprise Vault 10 is the ability to archive all social media interactions for compliance and eDiscovery purposes. For more information, visit go.symantec.com/ev10-dlp.

[ Symantec: a Leader in Gartner Magic Quadrants ]
Symantec continues to innovate and deliver multiple layers of protection to address today’s rapidly mutating threats. As evidence of its proven security technologies, Symantec was named a leader in the 2011 Gartner Magic Quadrants for data loss prevention, email gateway, and security information and event management. For more information, visit go.symantec.com/security-gmq.

[ Symantec Supports Women in Tech ]
In its continued effort at building a long-term pipeline of women interested in technology, Symantec is participating in the TechWomen program. TechWomen was developed to implement President Barack Obama’s vision of greater collaboration between the United States and the Muslim population. Secretary of State Hillary Clinton led the initiative in partnership with the Institute of International Education and the Anita Borg Institute for Women and Technology. For more information, visit go.symantec.com/tech-women.
ISBN: 978-1-4221-3870-0
Price: $29.95

Over the past 10 years we’ve seen companies that endured for over a century taken down by quickly changing market forces. In fact, more than two-thirds of the market leaders in the late 1990s no longer hold that title today. The question becomes what qualities does a 21st-century CEO need to possess in order to navigate today’s turbulent environment and lead their organization to success?

Based on Justin Menkes’ assessments of more than 200 executive candidates and 60 in-depth interviews with leading CEOs, *Better Under Pressure* defines three necessary attributes: realistic optimism, subservience to purpose, and the ability to make order out of chaos. These attributes are not innately inherent; instead, they are developed and honed by experience and continual self-improvement. More importantly, mastering these qualities helps executives realize not only their potential, but the potential of those around them.

Each chapter contains real-life examples that provide insight into the failures and successes that shaped different industry icons. It becomes apparent that the most success-

ISBN: 978-1-4221-6637-6
Price: $29.95

The result of detailed research jointly conducted by Gartner and Korn Ferry International, *The CIO Edge* presents seven leadership skills essential to a CIO’s success. Based on Gartner’s research into IT trends and over 1.4 million data points from Korn Ferry’s extensive empirical data on executive leadership capabilities, the authors elucidate skills that on the surface seem obvious, but sadly many IT leaders lack. These skills include:

1. Committing to being a leader first and delivering results through people;
2. Thinking analytically while acting collaboratively;
3. Connecting deeply with people by cultivating their softer side;
4. Forging winning relationships—up, down, and especially sideways;
5. Mastering communication so that messages not only are understood but also compel needed action;
6. Inspiring others to follow them;
7. And developing others’ capabilities and capacity to deliver results.

As the authors drill into each of these skills, they not only present theory and supporting data, but also liberally sprinkle interview comments from dozens of effective IT leaders from the likes of FedEx, Proctor & Gamble, American University, and Ford. These real-world comments are a valuable contribution and help to drive the authors’ key points home; for example, the authors point out that while technological knowledge is vital, nearly every leader interviewed could cite a specific point in their careers where they needed to lead differently and spend more time developing people skills and acting collaboratively.

Consider the leadership of Duffy Mees, CIO of Independence Air, who stressed how important it was to get his team together: “I really wanted them to feel I cared, and I was in this with them as much as they were. Sometimes I think I had more people in my office problem solving than we had on the floor....”

As I think about the most effective IT leaders who I have worked with during my career, it is uncanny how several of those leaders (CIO and director of telecommunications) possessed these skills; it is equally uncanny how ineffective leaders lacked nearly all of them.

I would recommend *The CIO Edge* to any current or aspiring IT leader, or for that matter nearly anyone seeking to lead; the book will prompt them to really think about these seven leadership skills.

Mark L. Olsen is a senior regional product manager in Symantec’s Endpoint and Mobility Group and has over 15 years managing and marketing high-tech products.
Where you spend your time as a chief information officer should reflect your business priorities. However, recent findings show that if that’s the case, business is in trouble.

Earlier this year, I spoke at an event sponsored by Symantec at NASDAQ OMX at Times Square in New York City. The focus of the presentation was on the just completed 2011 State of the CIO survey that CIO Magazine produces each year. In addition to survey overview slides, I developed a special slide called “CIOs Future Priority Index.” In it, I shared thoughts on areas where CIOs currently spend their time, and more importantly, where they want to spend more time in the future.

The adjacent table contains findings from that slide. Some of the data is quite sobering—and possibly alarming. Specifically, over the next three years, CIOs wanting to spend time in security management will shrink from 22 percent to 15 percent.

CIOs clearly don’t care much for the day-to-day operations of security. With other issues on their plate, such as growing top-line revenue, driving innovation, and redesigning business processes, there seems to be no meaningful interest in allocating more time to security. However, this can create huge regulatory, legal, financial, and reputation/brand risks.

But in a world that is producing 1.2 zettabytes (that’s with 21 zeros) of data a year, shifting to smartphone and tablet input devices, dealing with next-generation workforce demands, and trying to figure out what to do with social media, I just don’t understand why CIOs are not planning to spend more time with security matters.

Ah, that’s what the chief security officer, or chief information security officer, should be doing, right? Worrying about a firm’s physical and digital security as well as business continuity planning, data loss prevention (and the impact that can have on brand reputation), fraud prevention, risk mitigation, fraud prevention, and data privacy?

And as a growing group of professionals, CSOs and CISOs are doing just that. But there aren’t enough of them! Research from IDG Enterprise, the company I work for, which produces CIO Magazine and CSO Magazine, estimates there are 26,609 CIOs/CTOs and 5,989 CSOs/CISOs and security-related executives (for example, head of compliance, privacy, risk management, etc.) in North America.

This is a dramatic discrepancy and gives rise to the question: why are there 77 percent fewer security executives in North America than CIOs/CTOs? That’s dangerous, particularly when you consider the amount of time CIOs/CTOs currently spend—and moreover plan to—on security management.

What’s your take? Who handles security management at your firm? And to whom do they report? Drop me a note at twitter.com/gbeach or gbeach@cio.com. I plan to address the reporting structure of CSOs and CISOs in my next column and welcome your input.

Gary Beach is the publisher emeritus at CIO Magazine and former publisher for Network World, Computer World, and CIO Magazine. Follow Gary at twitter.com/gbeach.
As a leader in the ICT industry, ECS does more than react to market trends. We anticipate and capitalize upon them. ECS wants to lead the industry to embrace emerging technologies. The fact is, ECS isn’t just prepared for the future of technology distribution. We want to help redefine it.

With the wide market coverage of over 23,000 resellers and partners in the region, ECS has an extremely comprehensive presence in Asia, forging excellent partnerships with the ICT sectors in Singapore, China, Thailand, Malaysia, Indonesia and the Philippines.

Working with our partners in the way that best suits them, we are committed to long term relationships. We put importance in delivering our promises to every stakeholder. For us, we are not doing business with any stranger, but with trusted friends. Afterall, our guiding philosophy, “Technology is a Tool, People Make the Difference.” is what drives us.
Rapid development of prairies into farmland and lack of sustainable farming practices set the stage for disaster in the American Great Plains in the 1930s, when severe drought brought on the Dust Bowl. In response, farmers instituted a number of sustainability practices, not so much to comply with governmental regulations but for economic value. The same scenario is playing out in the arena of green IT today.

Introduction of the Internet changed the computing landscape and transformed how individuals and businesses interact. At the time of this transformation in the early 1990s, few likely realized the extent of the repercussions on global energy consumption. However, by the early 2000s, rapid growth in computing power consumption had become a tangible concern—and a business problem. Today, more than three percent of the world’s energy grid goes to power computer-related devices, and projections show this percentage will rapidly grow in the coming years unless changes are instituted.

The good news is that efforts around IT sustainability are beginning to change the pace of growth. Like the sustainable farming practices of the 1930s, sustainable—or green—IT practices are starting to bring about a change in IT energy consumption. For example, a recent study by the McKinsey Global Institute and The Climate Group found that green IT is a C-suite topic for many enterprises. IT has more than a seat at the corporate table when it comes to plotting their green strategies; it is often in the lead role.

Sustainable IT gained significant momentum heading into the 2008-09 financial crisis. And while nearly all segments of IT spending were cut—substantially in many instances—overall spending for those with green agendas either remained unaffected or accelerated in the vast majority of cases. Capital and operating expenditures surpassed corporate responsibility in terms of priorities, as green IT initiatives would have ended up on the chopping block for many enterprises.

Business value is both interconnected with sustainable IT programs such as lower energy costs and operating expenditures, and indirectly linked via areas such as capital expenditures and improved IT staff productivity. However, regardless of whether an IT program can be attributed directly to a green IT business benefit or not, the resulting business value provides justification for IT sustainability.

The growing adoption of cloud, smart grid, and other disruptive technologies provides IT organizations with additional toolsets that engender sustainable IT benefits, both in terms of sustainability measurements such as lower Power Usage Efficiency (PUE) and Carbon Usage Efficiency (CUE) and reduced capital and operating expenditures.

So where should you start with green IT as an IT leader? Mapping out the areas where business value is the greatest is a good starting point. In my next column, I will explore the primary areas and provide suggestions on how to calculate and measure value.

Patrick E. Spencer (Ph.D.) is editor in chief and publisher for CIO Digest. He is a co-author of a forthcoming book from Wiley (2012) on sustainable IT.
INSIGHT HAS POSITIONED ITSELF AS ONE OF THE WORLD’S LARGEST SOFTWARE PARTNERS

» Providing all Symantec industry leading technologies, fully supported by our Storage and Security solution teams

» Insight operate on a global scale - co-ordinating, supporting and supplying global clients with solutions from Symantec

» Over 1000 Technical and Sales Accredited Symantec Specialists situated across EMEA

» Offering unparalleled expertise and services at local, regional, and international levels

» Locations in 24 countries, support sales in 170 countries, 17 languages and 13 currencies

As a Trusted Advisor to our clients and our investment in Symantec’s technologies, Insight can assist with your requirements:

AU.INSIGHT.COM ▼ 1800 189 888
Symantec Chief Strategy Officer and SVP Angela Tucci has a passion for competing and playing team sports. “I played competitive sports in high school and college,” she says. A two-time Ivy League Player of the Year in softball, regional All-American in field hockey and softball, and inductee into the Connecticut Softball Hall of Fame, competing and winning for Tucci started a long time before she began her professional career.

After finishing a degree in physics at Princeton University, she continued to play competitive sports. “I took up cycling a number of years ago,” she says. “It provides me with an opportunity to compete against myself, as well as participate as a member of a team when cycling with others. It also correlates with my professional life. Competition and winning as a member of a team has always inspired me to push myself to higher levels of excellence.”

Tucci’s interest in gaining deeper insight into how businesses compete and win led her to return to university to work on a master’s in business administration at Stanford University. Indeed, over the course of her career, Tucci has found that orienting the business—from engineering, to marketing, to sales, to finance, to mergers and acquisitions—to what she describes as the “North Star” is extremely important. “Getting everyone focused on the ‘North Star’ and working in concert with each other unleashes immense potential,” she notes.

Owning your space—both as individuals and as a company—is also critical to achieving success, she continues. “I liken this to owning your lane when cycling or riding a motorcycle,” she says. “You never ride on the side of the lane but rather in the middle or on the side where you’re being challenged. Declare your lane and own it.”

Tucci’s current role and responsibilities encompass mergers and acquisitions, corporate venture investing, strategic partnerships, corporate strategy, integration management, and customer experience insights and advocacy. She has held a number of executive management positions in high technology over the past 15-plus years—experience that ranges from startups to large enterprises. In the following interview, Tucci discusses five IT megatrends, the lens from which Symantec approaches strategic investment, along with her background in venture capital and entrepreneurial startups.

PATRICK: You’ve been here a little more than a year now. What are some of the key initiatives that you and your team have driven?

ANGELA: Three things come immediately to mind. The first is the annual planning cycle—a process done in concert with the leadership team. The second involves augmenting our archiving and eDiscovery portfolio with the Clearwell Systems acquisition. The third is the small and midsize business segmentation that we announced at the beginning of the fiscal year. We completed a lot of research around this issue
for the various business constituents and helped conclude that we needed to have a dedicated group focused on the segment.

PATRICK: You mentioned the Clearwell acquisition. What does it add to Symantec’s existing portfolio?

ANGELA: We were encountering situations where customers needed more end-to-end eDiscovery features coupled with Symantec Enterprise Vault. Clearwell enables us to extend our capabilities in areas such as the ability to perform granular discovery for legal cases. We initially will offer it as a software form factor but have plans to extend it as part of our Symantec.cloud services.

PATRICK: The IT marketplace is focused today on delivering solutions that address several übertrends—virtualization, the cloud, mobility, the explosion in data, and the evolving threat landscape. Let’s start with virtualization. What are the different aspects and what role does Symantec play?

Angela Tucci at a Glance

Symantec Career Highlights: Named chief strategy officer and senior vice president at Symantec in January 2011. Her role and responsibilities encompass corporate strategy, mergers and acquisitions, corporate venture investing, customer experience insights and advocacy, and strategic partnerships.

Career Evolution: Before joining Symantec, she held the position of chief strategy officer at NEON Enterprise Software and was responsible for corporate strategy and market direction. Tucci joined NEON in early 2008. While at NEON, she held the post of chief executive officer at Compliance Spectrum, an IT governance, risk management, and compliance company. Her career includes a number of entrepreneurial ventures, including co-founding Terraspring, a pioneer in cloud computing, and Indicative Software, which specialized in performance management software solutions. The two startups were acquired by Sun Microsystems and CA/Nimsoft, respectively.

Tucci’s connections in the venture capital space extend from the relationships she developed at Stanford University and an assignment shortly thereafter at Clarify Software that had close ties to the venture capital community.

Education Highlights: Tucci holds a Master of Business Administration degree from Stanford University and a bachelor’s in physics from Princeton University. After completing her undergraduate work at Princeton, she went to work in the medical device industry, in ophthalmology and the use of lasers. She decided to attend business school at Stanford because she wanted to gain a deeper and broader understanding of the business and its direction.
ANGELA: Virtualization has been around forever. Storage pooling enables IT organizations to consolidate and get better efficiencies out of their storage infrastructure. Server virtualization is now entering a state of maturity. Most organizations have virtualized the lowest-hanging fruit such as Web and print servers and are now looking at business-critical applications. Then there is endpoint virtualization. It is being applied where you have a persistent desktop connection and the ability to stream applications, for instance in a hospital.

Symantec has an important role to play in all three areas. In the case of storage, sprawl is a real problem, an outgrowth of server virtualization, something that creates the need for more storage. The ability to reduce storage consumption and make it much more efficient to manage helps minimize the effects. Symantec offers a number of solutions in this area. A good example is our new Symantec FileStore appliance that serves as a “scale-out” mechanism. An IT organization simply needs to add more network connections to accommodate additional users and servers.

Server virtualization is enabled in a number of different ways by Symantec technology. Symantec Application HA provides a seamless, high availability VMware integration experience. On the security side of the equation, the latest release of Symantec Endpoint Protection delivers synchronous file scanning that helps ensure that system performance is not impacted.

In the case of endpoint virtualization, our Symantec Endpoint Virtualization Suite allows organizations to provision applications without having them reside on the endpoints via application streaming. This helps reduce security risks while creating an optimized software licensing model.

PATRICK: The cloud is taking the marketplace by storm. Its maturity level hasn’t reached that of virtualization in most instances; organizations are just beginning to tap into its fullest potential. What does Symantec have in this space?

ANGELA: The cloud is a business model and takes different forms. CIOs are now competing with the cloud providers and must begin creating business models that correspond with those offerings. In some instances it is simply more cost-effective to go to the cloud. In other cases it is better to implement on-premise services. And in some situations it is better to build your own private cloud, sometimes configured as a hybrid model that leverages the private and public cloud.

When it comes to the cloud, there are three basic plays for Symantec. First, we help cloud providers deliver secure environments and protect their customers’ information and identities. Second, through our Symantec.cloud offerings we are able to deliver to customers the ability to leverage various Symantec technologies as a cloud service. Finally, in instances where customers want to build their own private or hybrid clouds, Symantec data center technologies help enable this to happen.

PATRICK: Small and midsize businesses don’t want to own and manage IT assets. IT takes valuable time and resources away from their business. It would seem that cloud adoption will be faster in the SMB space, in general, than in the enterprise.

ANGELA: That is absolutely true and a trend we’ve seen with our Symantec.cloud services. The cloud is allowing small businesses to innovate faster, and they have fewer obstacles to clear than an enterprise.

PATRICK: Mobility is even less mature than the cloud, but it is quickly catching up. Where is the market headed and how can Symantec enable the momentum?

ANGELA: The phenomenon is that users are driving much of the innovation, and the introduction of tablet devices into the marketplace has accelerated adoption. This is good news and bad news. There is significant potential for productivity gains and innovative use cases. But it also introduces a number of compliance and security challenges—and IT needs to drive that portion. The risk is a balancing act. Users want access to information, but you cannot have it walk out the door. This is where technologies such as Symantec Data Loss Prevention come into play.
PATRICK: Exploding data growth—50 percent or more annually for most organizations—creates cost and operational challenges. What can be done to mitigate the effects?

ANGELA: The ways to generate unstructured data continues to proliferate; there are more and more applications and devices. As you note, storage requirements are growing at exponential rates. Storing data forever into one-size-fits-all storage architectures are no longer acceptable approaches. Beyond the capital and operational cost of storing and managing data indefinitely, there are risks—anything retained is a potential eDiscovery target in a legal case.

Organizations must design tiered storage architectures and implement archiving strategies based on storage policies, not to mention implementation of retention and expiration policies. The combination of Symantec Data Loss Prevention and Data Insight technologies is a great tool for helping IT organizations to catalog and index data based on ownership and type and then archive, retain, and expire it.

A second area where Symantec can help IT organizations address their storage challenges is deduplication—from the file system, to the host, to the device. Organizations can shrink their backup windows and data store by 50 percent or better in most instances.

A final area is thin provisioning. This pertains to the need to use and provision storage only as needed rather than acquiring blocks of storage that remain unused for lengthy periods of time. This also applies to the ability to scale up and down depending on fluctuations in storage requirements.

PATRICK: The threat landscape a few years ago was about securing the network and guarding against viruses and spam. It is much more complex today; virtualization, the cloud, mobility, social media, and the like have made the threat landscape much more complex. What are some of the implications?

ANGELA: Threats are now originating from organized crime and not just from rogue individuals looking to make a name for themselves. Further, they are going after information. Understanding what information exists, where it resides, and who has access to it is critical. The latter is particularly important and was one of the factors behind our acquisition of VeriSign’s identity and authentication business last year. With it, organizations can pinpoint who has permission to access different data types and from what device.

And one more thing—something that too few organizations realize—is that this is an important piece to have in place before moving to the cloud.

PATRICK: Your team is responsible for Symantec’s mergers and acquisitions strategy. What lens does your team employ when looking at possible acquisitions?

ANGELA: It must be in line with our vision—the ability to work and play freely in a connected world—or what I call our “North Star.” Securing and managing information and identities falls underneath that vision. The other aspect is to make sure that it is a good fit strategy and product-wise. The latter is particularly important because you don’t want to have an anti-body activity going on in the larger organization if it isn’t a good fit.

The megatrends we discussed earlier also play a role. The company has a double-down strategy in these areas and our acquisition approach will certainly focus on them.

PATRICK: Prior to coming to Symantec, you were the chief strategy officer at NEON Enterprise Software. What did your role encompass and what were some of the key initiatives that you drove?

ANGELA: The company had a number of different products, but not all of them were profitable. As a result, one of the first things that I had to perform was a portfolio rationalization. In instances where growth or the opportunity to make money was not possible, we shut down the product line.

The second thing was to take the company’s strengths in mainframe database, high-transaction environments and develop OEM relationships with database security software companies and other technology providers in this space.

The third area of focus was diversification beyond mainframes to other platforms—specifically Linux. To reach this decision, we formed strategy teams comprised of every-
“Getting everyone focused on the ‘North Star’ and working in concert with each other unleashes immense potential.”

– Angela Tucci, Chief Strategy Officer and SVP, Symantec

one in the company, and ultimately settled on Linux migration tools as our next big-growth opportunity. It was a very productive and positive experience. Everyone loved it.

PATRICK: You were only full time at NEON Enterprise Software during your last year with the company. Before this took place, you concurrently served as the chief executive officer at Compliance Spectrum, with the latter taking up about 75 percent of your time. What was the relationship between the two roles?

ANGELA: I was a member of a holding company that was managing six companies. One of them was Compliance Spectrum, a company that provided a hosted compliance solution. The company was burning through cash very quickly, and I was given charge to get the operational plan under control. Getting the company focused on where the solution worked best was a critical undertaking. Four years ago, the willingness to entrust services and data to the cloud was not what it is today. We had to recognize that a certain population of businesses would simply not be interested in the solution.

We put together a product roadmap and completed a market analysis. We started to win business and were being contacted by potential suitors. However, we ran into some IP challenges, discovering that the company didn’t have licenses to some of the IP in the product portfolio, and we had to shut the company down. It was the saddest day of my career, having to lay off an entire company that had executed exactly as directed.

PATRICK: You have an entrepreneurial background. It is much broader than the experiences at NEON Enterprise Software and Compliance Spectrum. Beyond the Stanford University MBA connection, what else contributed to your involvement with venture capitalists and startups?

ANGELA: I had the opportunity to work for a CRM company called Clarify in the mid-1990s. Members of the management team had roots in the venture capital community and moreover the company was highly successful on its exit, when Nortel Networks—now part of Amdocs—acquired them. One of my early-career mentors was my boss at Clarify, who provided me with a lot of insight and direction.

PATRICK: As you look down the road over the next year, what do you anticipate to be key focus areas?

ANGELA: There are several. The business units are largely focused on driving revenue from one quarter to the next. They are not focused on long-term strategy. But someone needs to look farther down the road and identify the obstacles and opportunities. This is where my organization needs to play.

The second is deciding what this long-term destination looks like and making acquisitions, partnering, and deploying resources wherever possible to shorten the journey. The final area is to find ways to rally the leadership team to coalesce around a set of strategic initiatives, thus leveraging the untapped potential of the entire team by getting them headed in the same direction—to the “North Star.”

Patrick E. Spencer (Ph.D.) is the editor in chief and publisher for CIO Digest and senior director of Symantec’s Customer Relationship and Publishing programs.
Digest Us Anytime and Anywhere!

Subscribe to quarterly alerts or download the app to your desktop and mobile devices.

Subscribe via Email or Desktop App
go.symantec.com/ciodigest-subscribe

Apple iTunes
go.symantec.com/ciodigest-itunes

Android Marketplace
go.symantec.com/ciodigest-android

Make sure to check out our NEW Adobe AIR-based desktop app at go.symantec.com/ciodigest-app. Read CIO Digest on your desktop or laptop at your leisure; content is updated in real time and can be read online and offline.
Legacy is something Thai Airways International Public Company Limited (THAI) knows all about. Founded in 1960, the airline has delivered 40 consecutive years of profitability and established a record of firsts such as the first Asia-Pacific airline to fly into London Heathrow and one of five founding members of Star Alliance in 1997. In the case of the latter, it revolutionized passenger services, as the group of airlines that came together offered something not seen before in the airline industry—integrated services to their passengers, regardless of which airline they were flying. The list of firsts and awards could continue for several pages.

Legacy is also something that Jirawan Chiasakul understands. CIO and vice president of THAI’s Information Technology Services Department, Chiasakul is entering her 33rd consecutive year with the company. After completing her master’s degree and spending a year as a research analyst at the university, she joined THAI in 1978 and has blazed a trail of innovation and execution. In particular, since taking charge of the IT Services Department in 2009, she led the team of nearly 300 professionals through the 2008-09 financial crisis, oversaw a complete reengineering of ERP and CRM systems, and mapped a future trajectory that places IT at the very center of the airline’s flight path.
Getting to know the business

When she joined THAI, Chiasakul’s initial assignment was as an application developer, and she was tasked with the development of the airline’s first online MVS-based application—an aircraft maintenance and engineering system. “It was a great time to enter IT,” she remembers. “After the aircraft maintenance and engineering system, I had a chance to work on a number of different systems—from crew management, to finance, to HR, to cargo management—that provided me with a broad view of the larger business.”

Fast forward about 15 years, to the mid-1990s. Chiasakul was given an opportunity to take the knowledge she had gained of the business and lead a newly formed IT Planning group. “Back then, not many IT organizations understood the dynamics of their relationship with the business,” she remembers. “We argued that IT should be understood as a service and not simply a set of capital assets with associated operating expenses. As a result, we began to map our IT strategy to our business strategy.”

It was during this time that THAI and Chiasakul had an opportunity to participate in the inaugural launch of Star Alliance, playing an important role in the development of its IT systems and processes. The initial focus was on creating an integrated customer view across all member systems. “This may not be a huge effort for most IT shops today, but it was 15 years ago,” Chiasakul quips. “What made it particularly exciting is the fact that it directly impacted customer experience and helped differentiate Star Alliance out of the gate.”

A long-awaited second international airport in Bangkok opened in 2006. The third busiest airport in Asia-Pacific, Suvarnabhumi Airport was an immense undertaking. Its IT systems were no exception, requiring support from various third parties, including the THAI IT Services Department. Chiasakul served on an IT committee tasked with overseeing the logistics and planning for the development of IT applications and infrastructure supporting the new airport. Their efforts included migrating IT systems and...
infrastructure from the previous international airport. “The opening of the Suvarnabhumi Airport was a big success, and I was very fortunate to have an opportunity to participate in it,” Chiasakul says.

Departing the gate

When Chiasakul assumed charge of the IT Services Department in 2009, she inherited a challenging situation. The airline industry was under immense financial pressures as a result of the 2008-09 financial crisis. “Our short-term objective was business sustainability—reducing cost while improving operational efficiencies,” Chiasakul recalls. “But at the same time we had to work on a long-term strategy. The airline industry had reached a point where transformational moves were required, and IT was needed to propel THAI to where we wanted to go.”

It was this latter objective that prompted THAI to initiate a corporate-wide program—THAI IT Transformation 2010—with the aim of leveraging IT services to drive innovation, lower cost, and operating efficiencies. “We have some aging infrastructure and applications and are looking to lower our cost and complexity while delivering enhanced services to our internal and external customers,” Chiasakul explains. THAI IT Transformation 2010 was designed as a joint initiative between the different business owners and the IT Services Department.

The ERP system was one of the first areas the THAI team decided to tackle. The previous infrastructure ran on proprietary platforms that were expensive and inefficient to manage. “We had 30 to 40 mainframe applications and migrated to a single-platform ERP solution based on hybrid Windows- and UNIX-based infrastructure,” Chiasakul says.

With this in mind, they completely revamped the underlying architecture and selected SAP as their next-generation ERP solution. The solution included the migration plan for nearly all mainframe applications to UNIX servers for databases and Windows servers for Web and application services. “We sought to reduce our footprint by migrating from mainframe systems and hundreds of other systems to fewer than 40 UNIX and Windows boxes,” Chiasakul sums up. The cost savings on the hardware and ongoing maintenance is substantial, into the millions of dollars, and this doesn’t even include savings for the energy required to power and cool the mainframe systems.

Virtualization was another area of rapid transformation. The team began with their UNIX environment, leveraging Solaris Containers to create virtual domains. For their Windows servers, they opted to deploy VMware vSphere. “We’ve been able to shrink our total server count in half, eliminating approximately 600 servers in total, 500 Windows and 100 UNIX servers respectively,” Chiasakul says. This translated into substantial reductions in cost—from energy consumption to capital assets. And

“It truly has been an exciting journey, one that I’m not done painting yet.”

– Jirawan Chiasakul, CIO and VP, IT Services Department, THAI

A 51-Year History

Headquarters: Bangkok, Thailand
Founded: 1960
Destinations: 37 countries and five continents
Employees: 25,000+
2010 Revenue: 184 billion THB ($6.1 billion USD)
2010 Passengers Served: 18.2 million
Website: www.thaiairways.com
the team continues to extend virtualization across their data center environment, with the objective to have the majority virtualized within the next year.

Another project Chiasakul spearheaded was a decision to move airline passenger services systems to a cloud services model, a customer-centric solution provided by Amadeus. Previously, THAI relied on an in-house solution that incurred capital and operating expenditures—from IT assets to ongoing maintenance. In addition to lower costs and reduced complexity, Chiasakul indicates the solution will provide THAI with better system integration and enhanced functionality. The team is in the initial phases of project rollout. “Our migration will not happen overnight,” Chiasakul states. “It will take two to three years to complete the entire move.”

**Standardization → virtualization → consolidation**

The groundwork for the THAI IT Transformation 2010 initiative was laid over several years preceding its actual launch. “How we manage our data center environment was a critical lynchpin in our preparation for the IT transformation we are spearheading,” Chiasakul explains. “Indeed, without the changes we’ve made in our data center, it would have been impossible to deliver many of the new services that we’re providing to our customers, employees, and partners.”

Standardization has been a focus for a number of years for the THAI team. And consolidation was overlaid as an objective with the launch of the THAI IT Transformation 2010 initiative, with virtualization as a critical part of this larger effort. “Our premise is that we can drive down costs and reduce complexity through standardization without impacting the quality of services,” Chiasakul states.

“We’re currently in the process of moving select applications and databases from big iron UNIX boxes to less-expensive servers running Linux.”

Consolidation and virtualization efforts feed directly into THAI’s larger set of corporate sustainability initiatives. “Green IT is a critical part of our corporate sustainability strategy,” Chiasakul states. “We believe that the company has a social responsibility and aspire to find ways to reduce our carbon emissions and thereby carbon footprint.” While still in the early phases, Chiasakul’s team is implementing processes to measure issues such as power usage effectiveness (PUE) and carbon usage effectiveness (CUE).

**Data center propulsion**

One of the first standardization projects for THAI involved the airline’s backup and restore infrastructure. In 2005, faced with IT staff inefficiencies, inconsistent backup rates, and growing backup windows, the team consolidated onto Symantec NetBackup. The ability to move from tape-based backups to disk-based backups and to leverage multi-dynamic pathing factored into their decision to move to NetBackup.

At the time, THAI relied on NetBackup for its Sun Solaris and IBM AIX platforms but used another solution for its Windows environment. By standardizing on NetBackup, the team is able to manage backup and restore with fewer staff, despite 30 percent annual data growth rates, at faster speeds, and with greater success. Total time spent managing backups was cut 90 percent, and IT staff productivity gains and cost avoidance over a six-year timeframe total more than $400,000 USD.

Shortly after the NetBackup standardization project, the THAI team implemented Veritas Cluster Server on select business-critical UNIX systems. They have added more UNIX and Windows clusters over time.

“The ability to avoid a fragmented clustered infrastructure enables us to manage our high availability systems with a small number of staff, managing maintenance and training on one tool set versus multiple ones,” explains Saroj Yuttatri, director, IT Operations and Services Department, whose team is responsible for data center infrastructure and operations.

**Fourfold Focus**

CIO and VP Jirawan Chiasakul explains that her team has been focused on four basic areas since she assumed charge of the IT Services Department in 2009. She elaborates on each.

1. **First**, the dynamics of IT are changing—from responsibility to management of the infrastructure to delivering services focused on business requirements; often with service level agreements and other associated business processes. **Second**, seeking to drive down cost and complexity.

2. **Third**, with the goal of always delivering better services to our customers, partners, and employees, we have been keen to implement best-in-class technologies as we evolve our IT infrastructure for the future. **Finally**, due to the rapidly changing threat landscape, we have been identifying and implementing security technologies and processes that will help protect our infrastructure and information.”

symantec.com/ciodigest
“IT should be understood as a service and not simply a set of capital assets with associated operating expenses.”

– Jirawan Chiasakul, CIO and VP, IT Services Department, THAI

“And as high availability is critical to our environment, avoidance of downtime—planned or unplanned—is very important, and Veritas Cluster Server has played a key role on this front.”

In early 2008, Yuttatri’s team added Veritas Storage Foundation for UNIX systems and some select Windows boxes. In 2010, they extended it across all of their server platforms. “The solution gives us the ability to seamlessly move data around our environment, including between different storage devices and systems,” says Yuttatri. “We have plans to extend it to our Linux environment once our migration begins in this area.” The solution has helped Yuttatri and his team to maintain an optimized storage environment; utilization rates have hovered around 60 percent since its deployment in 2008.

Last year, looking to leverage its enhanced virtualization support and deduplication capabilities, Yuttatri’s team upgraded to NetBackup 7. At the same time, they also instituted aggressive recovery time objectives. “The integration with VMware through the vStorage API provides us with the ability to maintain a single backup and restore panel across our environment—physical and virtual, UNIX and Windows,” says Yuttatri. “It has helped us avoid issues around sprawl that other organizations have experienced when moving to a virtualized infrastructure.”

With the NetBackup Deduplication Option, his team shrank daily backup volume by 90 percent and weekly backup volume by 50 percent. “Over time, this will greatly reduce our overall storage volume,” Yuttatri says.

Securing the cabin
The threat landscape is dramatically different than it was a few years ago. And consumerization of IT means that most organizations have employees, customers, and partners who want to use their own devices to access applications and the network. This creates a number of endpoint security challenges. The situation for THAI is no different. In 2006, seeking to better control malware intrusions and virus outbreaks, THAI opted to migrate from another endpoint security solution to Symantec.

Then, in early 2009, Chiasakul’s team elected to upgrade to Symantec Endpoint Protection. It currently is deployed across the data center environment as well as more than 9,000 desktops and laptops. “The integrated, consolidated console provides the IT staff with the ability to maintain transparent visibility across our IT environment,” Chiasakul says. “The intrusion prevention features provide us with the means to proactively identify threats. The firewall gives us the ability to enhance endpoint security for those clients that are mobile.” The team also uses ap-
To present themselves. Rather, they are not ones to recline and wait for challenges. Chiasakul and her team are not ones to spend almost 500 hours annually that can be spent on other initiatives. Adding flight paths of 40 hours of staff time each month for debugging systems; they now spend one or two hours. This equates to four or five days or weeks with the new Star Alliance Navigator app participating control in select instances to maintain closer control over the entire IT environment.

Currently, the team is in the initial phases of planning an upgrade to Symantec Endpoint Protection 12. “The one-two punch of Insight and SONAR technologies gives us the ability to approach endpoint security from two different directions,” Chiasakul says. “Blacklisting is no longer an adequate solution on its own; this is where Insight comes into play.”

Yuttatri continues: “As we’re rapidly moving to a virtualized environment, we’re also excited about the enhanced virtualization support, especially the performance on virtual machines.” He anticipates that the smaller footprint and revamped scanning engine will make it much easier to protect virtual machines.

At about the same time the THAI team upgraded to Endpoint Protection, they added Symantec Security Information Manager. “We did so because we wanted a centralized console that would provide a transparent view across our entire IT environment, including the ability to generate consolidated reports,” Chiasakul explains.

She goes on to point out that her team has been able to identify the root cause of virus and malware incidents much more quickly, thus reducing the breadth and magnitude of the intrusions. In addition to an enhanced risk posture, this translates into improved staff productivity. For example, before the deployment of Security Information Manager, Chiasakul’s team spent an average of 40 hours of staff time each month debugging systems; they now spend one or two hours. This equates to almost 500 hours annually that can be spent on other initiatives.

**Adding flight paths**

Chiasakul and her team are not ones to recline and wait for challenges to present themselves. Rather, they actively seek them out and have pinpointed several key areas of focus. They are interested in the next several years. Services through the cloud are a prime area of interest. “We maintain a five-year IT plan, one that we reevaluate every year in conjunction with our partners from the business,” Chiasakul notes. “The cloud is at the forefront of many of our planned efforts. These involve both leveraging services from the cloud and building out our own cloud services that we can offer not only to employees but even to partners and customers.”

One of Chiasakul’s directors is tasked with developing and managing the company’s cloud strategy. “Our transition to the cloud will not take place overnight,” Chiasakul says. “But it is coming. We believe that cloud computing has tangible business benefits—lower costs, reduced time to services, and enhanced efficiencies.” Ultimately, she believes embracing the cloud will help THAI to become more dynamic and customer focused.

The THAI team is thinking more broadly than just software as a service (SaaS); they are most interested in infrastructure as a service (IaaS), initially as a private cloud service. “It currently takes us three or four months to deploy a new service,” Chiasakul explains. “We can reduce this to a few days or weeks with infrastructure as a service. It also will allow us to plan our capital expenditures more carefully and lower our cost over time.”

The infrastructure tools THAI leverages from Symantec will underlie the different cloud initiatives. “We must continue to protect our data, efficiently manage our storage environment, and sustain high availability,” Chiasakul observes. “Symantec will undoubtedly be a critical piece of our cloud services infrastructure.” The ability to manage storage on premise and in the cloud with Storage Foundation is something she cites as one example. Another is the need for chargebacks to internal business units in a private cloud environment, a function Storage Foundation will enable.

Mobility is also something Chiasakul and her team have as part of their five-year IT plan. They recently participated in the development of the new Star Alliance Navigator app.
“The ability to avoid a fragmented clustered infrastructure enables us to manage our high availability systems with a small number of staff.”

– Saroj Yuttatri, Director, IT Operations and Services Department, THAI

that is available through the Apple iTunes store. Launched in July 2011, the new app delivers up-to-the-minute information about flights and enables passengers to make informed travel choices on everything from flight status and schedules to airport and city information.

“Mobility is where our customers, partners, and employees are headed,” Chiasakul says. “We implemented mail, calendaring, and scheduling on mobile devices about two years ago. It is the same experience employees have when they are on their desktops or laptops.”

But the team hasn’t stopped there. They are looking at a number of other mobility projects such as providing technicians with a mobile app that provides real-time access into maintenance records. “There are a number of different options,” Chiasakul observes. “It is a matter of building a business case and then mapping the technology solution to meet it.

“We can certainly look at offering apps through the iTunes store and Android Marketplace,” she continues. “For apps that are available only to employees, we can use the enterprise store on iTunes. But we are also looking at ways to build an application as a service (AaaS), whereby we can host and manage our own apps. We could even extend the service to other airlines.” These are just hypothetical ideas at this juncture, but they show that the THAI team is constantly innovating and thinking about their next set of strategic moves.

Painting a legacy
Chiasakul will be retiring and handing the IT controls at THAI over to Yuttatri and others. And despite all of her successes, legacy remains critically important to her, one that she plans to further evolve and transform before her departure. She equates it to the experience of painting, a pursuit she took up in the mid-1990s. “The planning and work that goes into a painting is analogous to the planning and work that must go into a successful IT strategy,” she explains.

Delivering optimal services to customers, employees, and partners is where the tires really meet the runway for Chiasakul and her team. “I’ve spent 33 wonderful years at THAI and recognize the importance of always-on IT systems and the critical need to protect the information entrusted to us,” she states. “I take my job very seriously and am proud of the legacy that we’ve built. IT has gone from a single application to a cluster of turbines propelling the company down the runway and up into the horizon. It truly has been an exciting journey, one that I’m not done painting yet.”

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.
Symantec Specialist partners have proven expertise in delivering innovative, market-leading solutions to help protect, secure and store your business critical information.

When you choose Imperium, the Symantec Specialist partner, you can be confident that you’re teaming with an expert who has the unique skills to deliver the very best results for your business.

Facing a rapidly evolving and increasingly sophisticated threat landscape, IT security has become a top-of-mind issue and businesses are looking for effective ways to secure their information and systems.

Achieving Symantec’s Specialisation further bolsters our confidence and ability in providing specialised consultation and value-added services along with industry-leading solutions, enhancing the win-win-win situation between Symantec, Imperium and our customers.

Tony Tan, Director, Imperium Solutions Pte Ltd.
When I was a small child in the late 1960s, I once accompanied my grandfather on his job as an oil field supervisor in rural West Texas. My most vivid memories of the experience center around a piece of equipment in his company car—a built-in telephone receiver that looked exactly like the one in my home. As he drove between drilling sites, he spoke with employees at other sites over his car phone. I had never seen such a thing and was utterly fascinated.

Motorola introduced the first car radio-telephone in 1946 to cater to what was then a small market niche—mobile workers like my grandfather. Twenty years later, the rotary-dial shoe phone worn by secret agent Maxwell Smart in the spoof TV series Get Smart still portrayed mobile communications as a novelty with few applications outside of international espionage.

Things have changed a lot since then. These days, mobile access to data is a business requirement for just about every company, and the trend is accelerating. “For several years we’ve said, ‘This is the year for enterprise mobility,’” says Steven Drake, program vice president for mobility and telecom research at IDC. “But right around the fourth quarter of 2010, we really saw the uptick in terms of adoption of mobile applications as
well as device management and security solutions. This coincided with a 75 percent increase in the use of smartphones during that calendar year.”

In addition to IDC’s Drake, CIO Digest spoke with executives at several organizations about mobility trends in their companies. While their approaches and emphases were as diverse as the companies themselves, all agreed on one thing: mobility is a phenomenon that is still in rapid flux, and best practices on issues such as security, identity verification, application management, and device management are not yet completely settled. In the words of Ralph Salomon, vice president of the IT Security and Risk Office at software giant SAP, “It’s one of the things that keeps my job interesting.”

**Enhancing the bottom line**

For corporations, the initial appeal of mobile devices was to enable workers to be more productive. Traditionally, the emphasis was on extending the availability of employees with pager access, and later with phone and email access. But opportunities for bottom-line improvements have grown exponentially as the devices have become more sophisticated.

“Mobile devices of different types have become indispensable in our business,” asserts SAP’s Salomon. “We support several devices and employees choose what they prefer personally, based on what apps are available. But we have to realize that since employees know what is easier for them, extending a choice helps maximize their productivity.” In the new world of mobile applications, a new level of productivity is possible. “For example, tablet devices initially were thought to have more of a consumer focus,” says IDC’s Drake. “But as it turns out there has been a huge adoption of these devices in corporations. “In particular, mobile apps can often enable sales professionals to do a better job of communicating with customers,” Drake continues. “A mobile app might simply make it easier for a sales professional to find traditional sales tools. But in other instances, a sales team might utilize an attractive user interface in a mobile app to give a compelling product demonstration. This can improve brand image and increase sales.”

**Optimizing the customer experience**

While forward-thinking companies are deploying mobile apps to boost internal productivity or increase sales, those whose ultimate end users are consumers often have no choice but to embrace mobile applications. One company that benefits from this trend is Q2ebanking, an Austin, Texas-based company that provides e-banking solutions for community-oriented banks and credit unions. “We help community institutions better compete with the big guys by offering a single platform for online, voice, and mobile banking,” explains Q2ebanking’s CTO Adam Anderson. “This enables them to match or exceed the services that the megabanks invested tens of millions of dollars to deploy. As more and more consumers and businesses conduct transactions on smartphones and tablets, this becomes critical to our clients.”

Another financial services company that was interviewed for this article, but asked not to be named, built a private cloud infrastructure to house its financial data. Partner financial advisors and employees can access the private cloud using a mobile app and provide on-the-fly valuations and investment reports to clients. “This is really where the market is headed over the long run,” notes Eric Meyer, president of Curious Minds Media, a digital media studio...
that works with clients to develop mobile apps. “The mobile app market is much broader than simply building consumer apps and selling them on iTunes or the Android Marketplace. The business-to-business possibilities are immense.”

**Getting the policy and strategy right**

But as any IT leader knows, deploying smartphones, tablets, and mobile apps is not as easy as flipping a switch. “I met with a number of CIOs last month,” recalls IDC’s Drake. “One of the things that always arises in this type of meeting is, ‘Do you have a mobile strategy?’” Most of them said, ‘Well, we’ve got policies, but we don’t have a strategy.’ That’s an important distinction.”

“From a security perspective, I think it is important that we begin seeing these devices as small PCs rather than telephones,” adds SAP’s Salomon. “We need to ensure that we have the full set of security requirements fulfilled based on the data they might contain. Since we still call these devices phones, that takes a bit of cultural adjustment.”

SAP has a standing security council, which includes members from each business unit. The council is responsible for establishing and maintaining all standards with regard to security. As a part of these security standards, requirements for the handling of intellectual property and other sensitive information are clearly outlined.

In 2005, SAP’s IT Security team recognized the proliferation of mobile devices connected to SAP’s email—mostly BlackBerrys at the time—and identified a potential security hole. “Based on the security concerns raised by the German Federal Office for Information Security (BSI) in 2005, we realized that we needed to establish protection of critical information in transmission to the devices,” Salomon observes. After evaluating several products, SAP deployed Symantec’s PGP Universal Gateway Email encryption solution partly due to its direct support for BlackBerry devices.

Today, SAP’s users are asking for a broad array of devices, and Salomon’s team is attempting to keep up. “We have to take a close look at each device, and each operating system, and check whether they can support our security requirements,” Salomon asserts. Currently, iPhones and BlackBerrys are certified for corporate use, and the team is in the process of analyzing several Android and Microsoft Windows 7 Mobile devices.

**A comprehensive approach to security**

“Security really is the foundation for everything that we do,” asserts Q2ebanking’s Anderson. “Community banks and credit unions want to differentiate themselves with security that is equal to or superior to what is available at the large megabanks. We wanted to offer a solution that went beyond the checkbox approach to security.”

“We recently launched a risk and fraud analytics product that does real-time decisioning on fraud detection and anomaly monitoring,” explains Ward Howell, Q2ebanking’s director of security solutions consulting. “It tracks the IP addresses users are logging in from, analyzes and monitors typical behavior for that user, and verifies identity through a multi-factor approach that includes VeriSign...”
Identity Protection. If a transaction cannot be verified as legitimate, our solution proactively suspends it in real time." VeriSign Identity Protection tokens are a key part of Q2ebanking’s security offerings to its clients, as well as the security strategy for its corporate network. VPN users within the company use VeriSign hard and soft tokens to access the corporate network remotely, and both types of tokens are also available to end users of Q2ebankings’s customers to protect transactions conducted online or from mobile devices. “When you think about community banks and credit unions, their biggest attribute is this whole idea of trust,” Howell notes. “Just as seeing the vault in a bank branch coveys a feeling of safety, and the VeriSign tokens bring that feeling of trust to Internet and mobile users.”

The future of mobility
The interviewees for this article all agree that the rapid evolution of enterprise mobility will continue unabated for the foreseeable future. “We expect that by 2014, 60 percent of all smartphones that are being used for business will be individually owned,” says IDC’s Drake. “This means that companies must learn how to control corporate data—and wipe it when necessary—without touching the personal data that’s on the same phone. And consumers will need to learn to keep their confidential information on the personal side of the device.”

“Businesses are beginning to wake up to the untapped potential of mobility solutions,” says Curious Minds’ Meyer. “Because accessing and archiving information is much more important for employee- and partner-facing solutions, protecting information and identities becomes critical.”

Mobile communications technology has transformed the work lives of many people, from my grandfather’s successors in the oil patch to Maxwell Smart’s descendants in the world of investigation and crime fighting. And it will likely revolutionize the way your company does business over the next several years. If you take the right steps to prepare, your company could reap many benefits. If you wait, your users may feel as if they’re using a 1969 car phone in an oil field."

Mark Mullins is a managing editor of CIO Digest and senior manager of Symantec’s SMB and Channel Publishing Programs team.

Symantec Solutions for a Mobile Workforce
VeriSign Identity Protection Authentication Service: Cloud-based authentication service that combines something you know (e.g., username and password) with something you have (e.g., token, mobile phone, etc.). Used to protect mobile apps that run on smartphones and tablets.

PGP Mobile Encryption: Delivers standards-based data protection via centralized policy management, accurate compliance-based reporting, and universal management.

Symantec Endpoint Protection Mobile Edition: Offers protection for Windows Mobile and Symbian smartphones against malicious threats; includes antivirus, firewall, and SMS AntiSpam features.

Symantec Mobile Management: Enables mobile email and application rollouts, safeguards mobile data and devices, and provides comprehensive visibility and control of the mobile environment.
<table>
<thead>
<tr>
<th>Symantec protects 100% of the Fortune 500®.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symantec scans 30% of the world’s email traffic.</td>
</tr>
<tr>
<td>Symantec tracks 1.5 billion security alerts daily.</td>
</tr>
<tr>
<td>Symantec monitors threat activity with 240,000 sensors.</td>
</tr>
<tr>
<td>Symantec backs up more than half of all the world’s business information.</td>
</tr>
<tr>
<td>Symantec protects more than 135 million consumers with Norton security products.</td>
</tr>
</tbody>
</table>
We protect and manage the world’s information 24x7

From the world’s largest data storage systems to the world’s smallest smartphones, from securing data and documents to securing devices and identities, Symantec can help you protect and manage the information that makes your business run. Visit us any hour of the day at symantec.com

Confidence in a connected world.
Social media is taking the world by storm. Social networking starlings such as LinkedIn, Zynga, and others have almost single-handedly revitalized the IPO market. Individuals are connecting with their favorite brands and entertainment, personal and professional networks, and even strangers.

Businesses recognize the new opportunity to connect with customers and partners, facilitate greater collaboration between employees, and grow revenue, so they are rapidly developing and implementing social media policies and systems. Participation in social networking is no longer an option—or even something that can be blocked; rather, most businesses understand the value and are embracing it.

Indeed, by tapping into social media, companies such as Dunkin’ Donuts and Ford Motor Company have revolutionized their go-to-market campaigns, extending their reach with customers, building and nurturing new and existing relationships, and growing revenue and margins. In a survey by the Altimeter Group, for instance, revenue for companies that had the greatest level of engagement in social media grew 18 percent, while revenue for those with the least level of engagement declined 6 percent.1

By Courtenay Troxel

5 Ways to Be Socially COOL

Enterprise strategies that minimize social media risk
Businesses are realizing that, as The Cluetrain Manifesto" said, the market owns the brand; ergo markets are conversations and you had better be in them," says James Governor, co-founder of analyst firm Redmonk. "And the ability to listen and respond to the market leads to all kinds of opportunities for the new social enterprise."

What’s at risk? $4 million
As more organizations empower their employees to engage in social media, the face of the company becomes everyone in it. This creates brand protection challenges, however. For example, social media has made it easy for employees to post sensitive company information, increasing risk for the company and individual employees.

In fact, Symantec’s latest 2011 Social Media Protection Flash Poll revealed social media incidents that trigger negative consequences cost enterprises an average of $4 million. This includes the cost of damaged brand reputation, litigation, threat mitigation, and lost revenue. Top incidents cited include malware attacks, regulatory violations, and inappropriate posting of information by employees that leads to exposure or loss of confidential data.

According to Governor, social media is another “forcing factor” to improve corporate security and data governance. Companies must identify what their trade secrets are rather than assuming that everything must be protected equally. They should make sure policies are in place so employees are comfortable using social media with customers and partners, then monitor the conversations that are going on. Finally and most importantly, they should listen and engage, responding to opportunities and issues that are going to help or hinder their business.

Need: tailored strategic response
Social media is not a uniform communications channel. Therefore, a one-size-fits-all policy or a stand-alone technology solution doesn’t address all of the different requirements. Also, consider that each of the social media channels have rapid permutations in functionality. Facebook, LinkedIn, and Twitter alone have seen nearly 600 functional changes over the past six months.

As a result, many organizations today are in the process of evolving their security infrastructure and processes. They must identify business-critical data, including who owns it and who is using it, institute corresponding data governance protocols, monitor, manage, and enforce social media conversations, and even archive and perform eDiscovery on social media exchanges. “Enterprises should enforce their social media policy with technology,” says Sarah Carter, vice president of marketing at Actiance, Inc., a firm that provides security, management and compliance solutions—both on premise and from the cloud—for instant messaging, unified communications, and social media. The technology that a company uses should map to its policies, Carter adds. “It should provide visibility into the conversations, establish specific boundaries on how people use the platforms, and ensure compliance,” she notes.

Conversations with analysts and key IT decision makers confirm these steps and reveal five top strategies that help companies minimize the risks associated with social media.

1. Identify and map risks
A key first step is to identify the risks associated with how an organization is using social media.
hires. In addition, protecting the brand is hugely important both in terms of Deloitte UK’s business operations and how it services clients. With this in mind, Deloitte UK is also a member of the Social Media Leadership Forum, which discusses issues around social media and the implications.

With many organizations looking to capitalize on social media, it has brought the intrinsic value of information into sharp view, whether its customer data or intellectual property. As a result, Deloitte UK has helped many of their clients deploy data loss solutions. “Symantec Data Loss Prevention is critical in that we recognize our clients are really struggling with understanding what information they have, where is it, and how it’s being used,” says Maddison. “We uncover this information, identify the potential risks, and more importantly, recommend the right level of controls and complete solution—not only from a technology standpoint but also business process and often cultural change.”

However, complex problems cannot be solved by any single technology. Deloitte UK recognizes that incidents often occur due to the staff not having the correct tools in place to do an effective job. As a result, Deloitte UK has also helped its clients deploy PGP encryption technologies from Symantec for protecting sensitive data from being inadvertently shared.

2. Establish social media policies

Once potential risks and sensitive information are identified, as well as industry regulations and IT compliance requirements, an organization needs to extend its corporate communications policies to include social media.

New regulations are shaping the way that social media can be used—especially in the financial services industry. In the United States, the Financial Industry Regulatory Authority (FINRA) requires every firm that intends to communicate through social media sites first ensure that it can retain

**Legal Tender**

According to FINRA, all communications via the Internet, including social networks, will be considered the same as in-person or written communications:

- **Publicly available websites** are considered advertisements.
- **An email or instant message** sent to 25 or more prospective customers is considered sales literature.
- **An email or instant message** is considered correspondence if it is sent to a single customer, an unlimited number of existing retail customers, and or less than 25 prospective retail customers (firm-wide) within a 30-day period.
- **Password-protected websites** (e.g., Facebook or LinkedIn) are considered sales literature.
- **Chat room discussions** (e.g., Facebook discussion, LinkedIn Q&A) are considered public appearances.

To download the FINRA Compliance Guide by Actiance visit, go.symantec.com/fina-guide.

“With Symantec Data Loss Prevention, we are able to monitor and even block unwanted activities.”

– Yuval Illuz, Head of Information Security, ECI Telecom, Inc.
records of those communications (Rules 17a-3).

A number of other organizations, including the U.S. Department of Defense, U.S. Federal Trade Commission, U.S. Securities and Exchange Commission with its Sweep Letter, IIROC for Canadian firms, the U.K.’s Financial Services Authority, and India’s Securities Board, have also released new rules and regulations regarding social media. Consider these judgments:

> In January 2011, after 32 tweets about AMD, founder of Titan Securities Jenny Quyen Ta was fined $10,000 and suspended from association with any FINRA member for a full year. FINRA determined that Ta’s tweets “were unbalanced, overwhelmingly positive, and frequently predicted an imminent price rise.”

> In a personal injury claim of Romano vs. Steelcase Inc. (N.Y. Supreme Court, Sept. 21, 2010), a former employee sued because of injuries allegedly sustained on the job. The plaintiff’s social media content was deemed relevant on the grounds that the plaintiff had placed certain information on social networking sites that was believed to be inconsistent with her claims concerning the extent and nature of her injuries.

Social networks are constantly changing and as a result, regulations and best practices will continue to evolve. Organizations will need to regularly refresh their social media strategies and policies to adapt to this fast-paced environment.

3. Train employees to minimize risks

Once social media policies are in place, employees must be trained in how to comply with them, and what actions to avoid.

ECI Telecom, a global telecom networking infrastructure provider, engages employees in social media because its channels are opportunities for conversation. “We use social media to get ideas and feedback from customers, as well as to increase brand awareness,” says Yuval Illuz, the head of information security at ECI Telecom. The company began using social media only after the right security protocols and processes were developed to prevent data loss.

ECI Telecom requires training for all employees who take part in social media on behalf of the company, and it uses Symantec Data Loss Prevention to enhance the training by monitoring and managing the content that gets shared through outside channels. A first step was to use the solution to automatically detect where sensitive information is within the company and where it is being used. Then Symantec Data Loss Prevention agents were deployed at endpoints to manage the

“As social media becomes the norm, demand for managing risk is now the challenge for IT.”

– Mike Maddison, Head of Security and Privacy Practice, Deloitte UK
information in motion and prevent it from being used inappropriately.

ECI Telecom recently worked with Symantec to extend Symantec Data Loss Prevention to monitor social media conversations. Now, it enables only authorized users to take part and blocks the sharing of inappropriate files and information over social networking channels.

According to Illuz, “Symantec Data Loss Prevention adds a flexible layer of protection that integrates easily into our current environment. With minimal interruption, it tracks confidential documents and key words to keep sensitive data from being uploaded or transferred to social media sites.” It also trains employees when they’re about to violate information sharing policies.

4. Archive social media to streamline eDiscovery
   Good controls and processes for social media don’t slow an organization down. They ultimately help it move faster. Consider Lotus Renault GP, an expert in speed. Its fans want to get as close as they can to the sensation of driving an F1 from 0 to 100 miles per hour in under three seconds, and social media enables them to get up close and personal, whether through a live viewing of the new car, raffling of driver memorabilia, or sharing of a driver’s story.

   But risk needs to be managed. “Today, the impact of social media has turned everyone into a journalist,” says Graeme Hackland, Lotus Renault GP’s director of IS/IT. “The minute you say anything, someone is tweeting—it’s just human nature to spread the news.” Case in point: the new design for the exhaust system of this year’s car was accidentally leaked to the public before the start of the 2011 season. This is the kind of leak Lotus Renault GP wants to avoid.

   Having better visibility is key—and knowing that a spike in tweets occurred 15 minutes after an internal announcement was made is very important for Lotus Renault GP to prevent data loss. The ability to do everything from monitor to enforce social media conversations is critical. As a result, Hackland and his team recently turned to Symantec partner Actiance and its cloud-based Socialite solution.

   Specifically, Lotus Renault GP is in the process of working with Actiance to add Socialite to manage social media access, identify and track social media users, and log social media conversations. Hackland and his team are also leveraging the integration between Actiance’s Socialite and Symantec Enterprise Vault to export social media conversations into an archive that allows them to be searched and retrieved as requirements arise.

   The solution captures the full context of the social media conversation as it archives. “With the ability to deliver a very extensive transcript, a compliance officer has an easy-to-read format within the Symantec Enterprise Vault interface, which businesses are already familiar with and trust,” notes Carter.

   To enforce data retention policies, the Data Classification Service feature of Enterprise Vault utilizes Symantec’s data loss prevention technology to automatically classify content and assign an appropriate archiving and retention policy. Classifications can also be used...
as filters, enabling legal teams to speed up the search and review process for eDiscovery.

“Actiance’s Socialite provides active compliance, as well as the ability to capture content and then seamlessly bring it into Symantec Enterprise Vault for archiving, records management, and eDiscovery,” Hackland states. “This comprehensive solution gives us a unified platform to comply with regulatory guidelines.”

Time to value was fast, observes Michael Taylor, IT manager at Lotus Renault GP. “Actiance’s Socialite has allowed us to achieve a rapid deployment while providing us with a secure, highly flexible solution,” he says.

5. Automate the enforcement of policies
To err is human. To catch and correct errors, ECI Telecom uses automation with Symantec Data Loss Prevention. The team is developing a custom pop-up tool that alerts users in real time when they are violating a social media policy, blocking their action and enabling them to make a more aware choice next time.

For example, should an employee receive a Facebook message from a friend and decide to click on a link to photos, the solution will be aware should the link lead to a page infected with Web-borne malware. At ECI Telecom, the tool will block the user from clicking on an infected link and indicate that a policy is being violated.

This type of threat occurs with increasing frequency. As the latest Symantec Internet Security Threat Report notes, social networking is a new megatrend in the threat landscape. Attackers are leveraging the news-feed capabilities on social networking sites to distribute links automatically from compromised accounts to the victim’s friends or associates, spreading malware to potentially hundreds or thousands of victims in a matter of minutes.5

“More than 90 percent of data loss is innocent,” Illuz states. “With Symantec Data Loss Prevention, we are able to monitor and even block unwanted activities on one hand, while fostering employees to use this important media on the other.”

Enforcement can be automated for IT policies as well as social media policies. Deloitte UK has deployed Symantec Control Compliance Suite at some of the world largest clients to automate internal and external IT compliance policy processes. “Compliance is in our DNA,” notes Maddison. “For our clients who are required to conduct compliance reporting, Symantec Control Compliance Suite is a much more efficient and cost-effective way to automate policy management and reporting of social media activities.”

With the right protections in place, social media presents an enormous opportunity. “Businesses must invest in a social media strategy, apply all the necessary risk management tools, and invest and trust in their employees to have a stronger dialogue,” says Governor. “In doing so, they can truly scale and maximize their efforts to deliver the business results social media has to offer.”

1The Altimeter Group, “ENGAGEMENTdb,” July 20, 2009
3Symantec, “2011 Social Media Protection Flash Poll,” September 2011
4Actiance FINRA Compliance Guide: Social Networks, Web 2.0, and Unified Communications
5Symantec Internet Security Threat Report, April 2011

Courtenay Troxel is a managing editor for CIO Digest and manager of online content and newsletters at Symantec.
Matriculating IT

*Results improve with each level of advancement at Northeastern Illinois University*

When Kim Tracy arrived at Northeastern Illinois University six and a half years ago and took the reins as executive director of University Technology Services, he inherited an IT environment that was highly fragmented. “There really wasn’t one IT head for a long period of time,” he recalls. “We had a bunch of different departments that were doing a number of different things.” This silo-based approach created significant cost and operational inefficiencies for the university.

A Senior Member of IEEE and the Association for Computing Machinery (ACM), Tracy drew upon ITIL best practices to consolidate IT infrastructure, processes, and services. “We created a strategy and planning group to drive an overarching vision, services delivery for day-to-day operations, and infrastructure and application functions,” he says.

**Next-gen ERP**

Much of the change and consolidation was driven by a large ERP implementation based on SunGard Banner that was overseen by Tracy and his team of approximately 80 IT professionals. As part of the architectural overhaul, they took an opportunity to refresh some of their aging hardware infrastructure. “We implemented a Fujitsu SAN solution that provides us with a tiered storage capability—from Fibre Channel to SATA—and upgraded the Sun Solaris servers powering the SunGard Banner system,” he says.

Since Northeastern Illinois University had substantially more storage than it needed at the time, the benefits of the tiered storage strategy have largely not been realized, though the milestone to do so is quickly approaching due to rapid storage growth. “What’s important is that we have the infrastructure in place to do so once this happens,” Tracy observes.

**Incremental virtualization**

Standardization and consolidation of IT systems was much broader in scope than the ERP solution; it simply served as the catalyst. “Identity management is crucial for an institution of higher education, particularly one as large as Northeastern Illinois University,” Tracy says. “As a result, we rolled out an identity management solution with role-based user provisioning and identity administration that is used across our different applications.”

Tracy and his team evaluated different virtualization technologies about five years ago and selected VMware. They currently have about 60 Microsoft Windows servers, with nearly 70 percent in a virtual state, a number Tracy indicates could easily be well in excess of 200 without virtualization.
The move to virtualization has been gradual, implemented in incremental phases over a period of several years. “Virtualization has allowed us to add new services and grow existing ones without acquiring more equipment,” Tracy says.

The Northeastern Illinois University IT team also leverages virtualization capabilities on many of the Sun Solaris servers using Solaris Containers. This was important when Tracy and his team implemented the next-generation ERP solution based on SunGard Banner. “We were able to use existing server capacity without purchasing additional Solaris boxes,” he states.

Another refresh of much of the Solaris environment is forthcoming, so Tracy is looking to migrate much of it to Red Hat Enterprise Linux—and he and his team plan to extend their VMware vSphere implementation, currently used for their Windows environment, to Linux. “We’ve achieved very good results with VMware on our Windows boxes, and we aim to replicate that same success with the Linux platform as we begin to move to it,” he predicts.

Making the “grade” with data protection
Symantec NetBackup was part of the backup and recovery infrastructure at Northeastern Illinois University when Tracy arrived. “But it was only used for our Solaris environment,” he explains. “We had a different solution for our Windows servers.” As a result, with standardization at the forefront of Tracy’s efforts to rationalize the university’s IT environment, he and his team opted to consolidate all backup and recovery to Symantec NetBackup.

They achieved some immediate results. “We previously had two team members managing backups, one for our Windows servers and one for our Solaris environment,” Tracy remembers. By standardizing everything onto NetBackup, he was able to reallocate the time one of the headcount spent managing backups to other IT tasks. And as NetBackup is more robust and stable than the Windows-based tool, Tracy’s team improved their backup success rates.

“We had a seamless transition to VMware and virtualization,” Tracy sums up. “No changes were needed to our backup and recovery infrastructure. It was important to have a unified view across virtual and physical environments; this is what NetBackup provides.”

Graduating to the cloud
“Our staff is overburdened with the challenge of managing existing IT services while addressing new educational and operational requirements,” Tracy says. “Anything that we can do to offload the complexity of the current IT environment is a big plus. This allows us to focus on improving our existing services and developing new ones that improve the efficiencies of our faculty and staff as well as enhance the educational experience of our students.” Though not the only reason, this is the primary factor Tracy is looking to move IT services into the cloud—and it started with messaging security.

Specifically, phishing and spear-phishing are onerous problems for Northeastern Illinois University. “Every time we had a compromised account, spam would start spewing from it,” Tracy explains. “The ISPs would then blacklist us, and our IT staff had to spend valuable time and energy working with them to clean up the situation and get us off the blacklist.” Though the attacks occur in spurts, Tracy estimates his team had to remediate three or four monthly. “It easily consumed 40 to 50 hours of staff time each month,” he reports.

When NEIU started having problems with phishing, they would crank up inbound filtering with the previous appliance-based solution. However, this inevitably increased the number of false positives. “We either spent time remediating blacklisting with the ISPs or helping our staff and students to retrieve legitimate emails that showed up as false positives,” Tracy explains. “It was a vicious circle.”

Network bandwidth was also an issue with the prior appliance-based messaging solution. With more than 16,000 mailboxes and 80 percent of mail as spam, this translated into significant traffic.
“Anything that we can do to offload the complexity of the current IT environment is a big plus.”

– Kim Tracy, Executive Director, University Technology Services

“Rather than having 200,000-plus spam pounding at my mail gateway every day, I wanted to make this someone else’s problem by moving to a cloud solution,” Tracy quips. “We would purchase more network bandwidth, and a few months later it had been ‘eaten up’ and we had to acquire more.”

But it was more than a bandwidth issue. Tracy reports that he had to add a third mail gateway last year to accommodate the load of incoming mail. This was an expenditure of about $15,000.

“And this doesn’t include the IT staff time required to manage it,” he adds. “Frankly, we probably could go down to one mail gateway, though we’ll retain two for redundancy.”

Operating expenditures also factored into Tracy’s decision to move to the cloud. “There are some things that simply make more sense if they are in the cloud,” he observes. “Messaging security is one of them.”

Tracy and his staff looked at several cloud-based messaging security solutions and ultimately selected Symantec MessageLabs Email Security.cloud. “Its multiple layers of scanning technologies were an important reason we chose it,” he says. “The service level agreement also gave us a level of comfort.”

The deployment of Symantec MessageLabs Email Security.cloud was seamless. “We had to spend a little time preparing our environment for the deployment,” he recalls. “But it took less than half a day to extend it across our entire environment.”

The Northeastern Illinois University team has outbound filtering, in addition to inbound, turned on. “The outbound filtering helps ensure that we don’t propagate spam and viruses inside and outside of our IT environment in case we do get infected or compromised,” Tracy says.

Upgrading is important

Before Tracy arrived, Northeastern Illinois University struggled with periodic security attacks. Since his team upgraded to Symantec Endpoint Protection 11 about two years ago, however, they haven’t had any malicious intrusions.

“The centralized security console provides us with a view across all of our endpoints, enabling us to take a more proactive approach to endpoint security,” he says.

Upgrading to Symantec Endpoint Protection 12 is now on the roadmap. “Endpoint security software can be a ‘pig’ on CPU resources,” he explains. This becomes even more dramatic for virtualized servers. With that in mind, the enhanced virtualization support in Symantec Endpoint Protection 12 is something...
Every day, your employees bring more and more iPads into your organizations, and onto your networks, where they are given access to sensitive corporate information. Fortunately, Symantec Data Loss Prevention for Tablets provides enterprise-strength data loss prevention, so you can allow employees the flexibility of working on iPads without compromising sensitive corporate data. Real-time alerts inform users when confidential data is being mishandled or a company policy is broken. It’s simple, unobtrusive, and most importantly, effective. Get the white paper “DLP for Tablets: An Intelligent Security Decision” at go.symantec.com/dlp

iPad® protection from the leader in DLP

Every day, your employees bring more and more iPads into your organizations, and onto your networks, where they are given access to sensitive corporate information. Fortunately, Symantec Data Loss Prevention for Tablets provides enterprise-strength data loss prevention, so you can allow employees the flexibility of working on iPads without compromising sensitive corporate data. Real-time alerts inform users when confidential data is being mishandled or a company policy is broken. It’s simple, unobtrusive, and most importantly, effective. Get the white paper “DLP for Tablets: An Intelligent Security Decision” at go.symantec.com/dlp

Confidence in a connected world.
he expects his team to begin leveraging later this year.

**Getting to the advanced curriculum**

When asked to cite some of the initiatives the team will be driving over the next couple years, Tracy culls a long list. The foremost priority is desktop virtualization.

Storage is also on the list of action items. “The deduplication option in NetBackup is certainly something that we plan to activate,” he says. “In addition to the storage cost savings and smaller backup windows, we will lay the groundwork for disaster recovery.”

Currently, Tracy’s team backs up data up to disk and then to tape after 30 days. The tapes are then shipped off site to a third party. “This is a complex and time-consuming process,” he states. “The cloud has become a viable alternative, and we’re looking at ways to begin moving in this direction.” With this in mind, he adds, “The smaller our backup volumes, the easier it will be to back up this storage into the cloud. Deduplication in NetBackup will enable this transition.”

Mobility is another area where Tracy sees substantial potential—from operational benefits to enhanced learning experiences for students. Evolving their identity management solution to provide unified access across all types of applications and all different types of devices, including handhelds and tablets, must happen first. “With the next-generation identity management solution in place, including seamless integration with our ERP system, we will be able to create a personalized view based on the identity of the user,” he says.

Indeed, Tracy believes the potential impact of mobile devices and apps within education is just beginning to be realized. “We still have a significant distance to go before mobility technologies mature and become the prevalent mode of interaction.” Yet this is inevitable, and preparing for that day is just as important as the actual occurrence itself, argues Tracy.

*“Matriculating the ball down the field”*

Successful IT matriculation is focused on both the present and the future; it is an interlacing of initiatives that forms a comprehensive whole focused on a long-term vision. This is something Tracy recognized six and a half years ago, and it still rings true today.

Originally hailing from the State of Missouri, Tracy knows the importance of carefully planned matriculation from an adage made famous by Hank Stram, the legendary American football coach of the Kansas City Chiefs: “Just keep matriculating the ball down the field, boys.”

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.
Leading-Edge TECHNOLOGIES CUSTOMISED to take your BUSINESS FURTHER

Datacentre Virtualisation
Increase the efficiency & availability of your resources and reduce your overall IT cost by 50%-70%!

Data & Storage Management
Enjoy faster & easier access to your data with the right storage management solution for your business.

Security & Network Infrastructure
Customised security systems for protecting and keeping your business safe, 24/7.

Technology Optimisation Software
Maximise your return on technology investments while achieving optimal results and productivity.

Pro-Datech Systems Pte Ltd
2, Alexandra Road, #06-02
Delta House, Singapore 159919

www.prodatech.com
Symantec™

Next-generation reputation-based technology

The fastest, most effective endpoint protection anywhere

Built for virtual environments

Symantec™ Endpoint Protection 12

It takes just seconds for today’s polymorphic malware to mutate into millions of threats, but now it has met its match. Introducing Symantec Endpoint Protection 12—simply the fastest, most effective reputation-based protection ever created. Improve the security of your information, devices, and employees. Download the trial version of Symantec Endpoint Protection at go.symantec.com/sep12

* Sources: PassMark Software, “Enterprise Endpoint Protection Performance Benchmarks,” February 2011. All-Test GmbH, “Remediation Testing Report” and “Real World Testing Report,” February 2011. Any forward-looking indication of plans for products is preliminary and all future release dates are tentative and are subject to change. Any future release of the product or planned modifications to product capability, functionality, or feature are subject to ongoing evaluation by Symantec, and may or may not be implemented and should not be considered firm commitments by Symantec and should not be relied upon in making purchasing decisions.

Copyright © 2011 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. VeriSign is a registered trademark of VeriSign, Inc.