



CRAFTS THE POLICIES

that protect the systems and intellectual property of one of the country's largest defense contractors; manages a staff of 41 and a \$16M annual budget.



BALANCES NEED FOR SECURITY AND OPENNESS

required by one of the largest research universities in North America; a staunch advocate of defending against cyber-fraud and harassment.

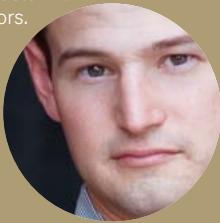


MONITORS AND AUDITS

access to patient records through data mined from hundreds of applications; safeguards privacy

of thousands and maintains the open nature mandated in a teaching hospital.

ADDRESSES SECURITY SHORTCOMINGS in critical infrastructure systems by establishing a program to develop language that owners can insert in procurement contracts with vendors.



AGENT FOR CHANGE within

his company and in the security community, delivering security as a managed service within the corporate walls, and identity exchange programs industry-wide.



BUILDS A STATE-OF-THE-ART

security operations center with a small staff and institutes successful two-factor authentication in 30 locations.



ENSURES THE SECURE DELIVERY of

real-time market pricing information, news and trading services to 330,000 financial services professionals, via a program that promotes service management within the security organization.



1234567

SECURITY

Seven Winners, One Mission

In recognizing seven individuals working in different markets, you might think their experiences and abilities would be quite diverse. And while it's true that all of this year's Security 7 Award winners possess their own traits and talent, all are unified by a single mission: align information security with the business. Across the board, the seven winners have succeeded in guiding large security operations toward this unification while keeping some of the world's largest and most sensitive networks safe from harm. The following profiles shed light on their accomplishments and provide insight into what drives some of the brightest practitioners in the industry.

Greater Good

BY MICHAEL S. MIMOSO

1

MICHAEL ASSANTE

Infrastructure protection strategist, Idaho National Lab
Industry Critical infrastructure
Location Idaho Falls, Idaho

Kudos

- Helped establish SCADA Security Summit
- Instrumental in creation of Cyber Security Procurement Language for Control Systems
- Former CSO American Electric Power
- Put together information sharing/training workshop uniting control systems security managers from five countries
- Done extensive vulnerability research into the interdependencies of control systems

OPPORTUNITY KNOCKS; SOMETIMES UNCERTAINTY ANSWERS.

Michael Assante spent the greater part of his early career securing the assets, people and facilities of a major Midwest utility. But all the while, he kept a watchful eye on the disturbing news and trends surrounding critical infrastructure and the SCADA control systems that support it.

“There were marked improvements in frontline IT systems and their protection profiles, but back-end systems were struggling,” Assante says. “Systems grew that weren’t intended to be connected, but became connected. I started worrying about these systems.”

Enter opportunity in the form of an opening with Idaho National Laboratory, a facility in Idaho Falls dedicated to nuclear energy research and focused on partnerships with the U.S. Department of Energy and Homeland Security.

Enter uncertainty in the form of relocation. The prospect of moving to Idaho and working and living near Yellowstone National Park and in the shadow of the Grand Teton mountains was a daunting contrast to the life Assante and his family knew in metropolitan Columbus, Ohio.

“It’s quite beautiful here,” Assante says. “I was immediately impressed with the lab and the amount of industry experience here, the guidance they provide to industry. I realized they weren’t in business just to do work for the U.S. government, but to bring value to the end user.”

Opportunity won out, and Assante, INL’s infrastructure protection strategist, joined the lab two years ago. He was immediately struck by the lack of emphasis put on security by control systems vendors, who countered pleas for improvements with the claim that customers just weren’t asking for security. Instead, customers were bearing the expense of tacking it on. “They weren’t really resourced or prepared to ask for [security from vendors],” Assante says.

Assante set out to provide control system managers with language to insert into procurement contracts to ensure vendors address security concerns. He sought help from Alan Paller at the SANS Institute and Will Pelgrin, director of the New York State Office of Cyber Security and Critical Infrastructure Coordination, to establish a SCADA Security Summit. The event in March 2006 brought together more than 400 SCADA experts and vendors, and kick-started the SCADA Procurement Project. Recently, version 1.6 of the Cyber Security Procurement Language for Control Systems was posted on the Multi-State ISAC site, msisac.org.

“Vendors were forced to make changes they knew they had to make,” Assante says.

Jerry Freese, director of IT security engineering at Assante’s former employer, American Electric Power, praises Assante as a man of vision and one who is driven to execute that vision.

“He’s a strategic thinker, very focused on the global security threat and astute at distilling that focus into relevant business and critical infrastructure protection planning,” Freese says.

SCADA systems were plagued by some common vulnerabilities, regardless of the provider, Assante says. For example, extraneous services were turned on by default, risky configurations needed to be addressed, as did some patch management, authentication, and weak policy management issues. The group edited the procurement language for months, and both sides made necessary compromises.

“It’s an incredible resource for asset owners,” Assante says, “who can cut-and-paste the language into procurements with vendors to get more secure systems.”

“He’s a strategic thinker, very focused on the global security threat and astute at distilling that focus into relevant business and critical infrastructure protection planning.”

—JERRY FREESE, DIRECTOR OF IT SECURITY ENGINEERING, AMERICAN ELECTRIC POWER ON MICHAEL ASSANTE

OUTREACH

Idaho National Lab takes part in several outreach programs with the Departments of Energy and Homeland Security to develop a risk management program for control systems. The lab has brought together ally nations like the U.K. and Australia for information sharing workshops, and has established training environments for critical infrastructure asset owners to demonstrate attacks against these systems, and optimize security technology to combat them.

“We have done a lot of work in vulnerability testing and discovery, looking especially at interdependencies between infrastructures,” says Michael Assante. “We’re looking at where these crossovers are, the vulnerabilities associated, and what could cause high consequences.”

—MICHAEL S. MIMOSO



LISTEN TO THE MUSIC

Favorite iPod sounds: “Take it Back,” Pink Floyd; “Speed of Sound,” Coldplay; “Hide and Seek,” Imogen Heap



REALITY TV BECKONS

“Project Greenlight” is the ticket; “It would allow me to incorporate my life and work experiences into a creative and exciting form of entertainment”

CONTRADICTION

Favorite sports franchise: New York Jets
 Favorite band: Boston



EXOTIC GETAWAYS

Phuket, Thailand
 Bali, Indonesia



UNWINDING IN IDAHO

Take the family—dogs included—camping, ATV riding and hiking.



Trend Spotter

BY BILL BRENNER

2

KIRK BAILEY

Chief information security officer,
University of Washington
Industry Education
Location Seattle
Certifications CISSP, CISM

- Kudos**
- UW's first CISO
 - Built sophisticated risk analysis of UW security posture
 - Secures perimeterless network used by 37,000 students
 - Founder of Agora, an information sharing group uniting security and law enforcement officials
 - Founder of the Pacific CISO Forum, a Pacific Northwest information security and knowledge exchange

LONG BEFORE ONLINE FRAUD and harassment were a mainstream concern, Kirk Bailey was passionate about them. In 1999, for example, he challenged computer security researchers to take a couple months to scour cyberspace for as much of his personal information as they could find. To the surprise of Bailey and others, the researchers amassed a pile of data in short order, proving that the Internet was a trove of information for good and bad.

Eight years later, Bailey, chief information security officer at the University of Washington and former City of Seattle CISO, is being praised by peers as an industry leader and someone who can spot security trends before others. He spreads the word as the driving force behind Agora, an expansive group of IT security professionals who come together to chew on the latest security challenges. And he is an expert on cyberstalking and risk analysis.

"Kirk has been on the leading edge of such issues as data privacy, critical infrastructure protection and active defense," says Port of Seattle CISO Ernie Hayden, a longtime friend and collaborator.

"He is often raising information security issues and concerns before the general community even recognizes the problem," Hayden says.

As one example, Hayden notes how four years ago Bailey was building the concept of active defense—ways to fight back against a cyberaggressor—at a time when few were paying much attention.

"Kirk's probing questions and concerns were hard to swallow by the mainstream information security community, but he was right in his perception of the issues, and today active defense is part of the general infosecurity dialogue and there are even conferences on the subject."

During his tenure with the City of Seattle, Bailey ran an innovative risk analysis exercise against the city's IT infrastructure called ALKI. The exercise produced innovative defense strategies, and Hayden says that without Bailey's leadership, such an exercise would never have happened.

Bailey says his passion for the job is driven by the fact that the public's appetite for new technology far outpaces the ability to secure it.

"Not enough attention is paid to the potential consequences of all this technology," he says. "Places like MySpace create an enormous opportunity for problems."

"The big unintended outcome of all this technology has been the loss of privacy," Bailey says. "More than 160 million letters have gone out to people telling them their privacy has been invaded, and that's just not right."

Bailey's mission is to take what he learns and share it with colleagues, peers and anyone else who will listen. He has learned to rethink the concept of security as data breaches escalate.

"Instead of worrying about perimeter security and perfect scores for zero compromises, we now have to operate under the premise that all systems can be compromised at any time, and act accordingly," Bailey says

To that end, he says the building blocks of a good defense are strong forensics and incident response plans, public education, partnerships and continued public debate about the legal issues surrounding information security.

"I worry the public doesn't understand the true risks, so my mission is to educate them," he says. •

MAKING A DIFFERENCE

One of University of Washington CISO Kirk Bailey's missions in life is to raise awareness of cyberstalking and help pass laws to protect people and privacy.

Bailey was instrumental in getting a cyberstalking law on the books after he and his peers helped bring to justice a stalker harassing a fellow City of Seattle employee online. The Working to Halt Online Abuse site says the Washington law declares a person guilty of cyberstalking if they use electronic communication to intimidate, torment or embarrass another. Cyberstalking is considered a felony in multiple offenses against the same person. •

—BILL BRENNER

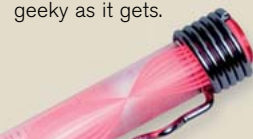
"He is often raising information security issues and concerns before the general community even recognizes the problem."

—ERNIE HAYDEN, CISO, PORT OF SEATTLE ON
KIRK BAILEY



OLD SCHOOL GADGET

Ballpoint pen that lights up is as geeky as it gets.



MY CALLING

If I weren't a security professional, I'd be a professional artist.



SAD STATE OF PRO SPORTS

Minor league baseball rules: "I'm quickly losing interest in major league sports."



KEEPING AN EYE ON...

The public's appetite for convenience, addiction to slick-marketed technology toys and lack of knowledge of the associated problems.

READING MATERIAL

Against the Gods: The Remarkable Story of Risk, by Peter Bernstein; *Blink*, by Malcolm Gladwell

Best Defense

BY BARBARA DARROW

3

MICHAEL K. DALY

Director enterprise security services, Raytheon

Industry Manufacturing

Location Billerica, Mass.

Certifications CISSP, Qualified Raytheon Six Sigma specialist

Kudos

- Chairs Raytheon's Information Security Council, a group of 18 security experts accountable to him for performance goals
- Leads Raytheon's incident response team, made up of 100 people organization-wide
- Runs Raytheon's Information Security Administrator certification program
- Participated in the president's National Security Telecommunications Advisory Committee
- Helped launch CertiPath, the first commercial PKI bridge

INFORMATION SECURITY IS A big deal for enterprises, but for a major defense contractor, the task takes on a whole other layer of urgency.

Michael K. Daly, director of enterprise security services for Raytheon Company in Massachusetts, knows that in his bones. When your company designs and manufactures missiles, and intelligence and defense systems, the potential downside to a breach can be disastrous.

Daly, whose team of 41 security professionals works under a \$16 million annual budget and supports 73,000 employees, 15,000 contractors and 5,000 partners, sees two major trends.

The first is "data exfiltration," which he says is a fancy way of saying the loss of intellectual property, including private information and corporate data. Previously, security pros spent the bulk of their time fighting off external hackers, he says. "We continue to fight that fight, but now there's also the issue of Trojan horses and viruses and worms that grab data off machines."

The second trend is the whole wide world of mobility. It's one thing to protect data that primarily stays under lock and key in a climate-controlled glass room. It's quite another to do the same with a mobile workforce, and where virtually every enterprise's supply chain includes outside partners—each with its own LAN.

"The architecture of our environments has changed," Daly says. "Companies used to build their own LANs, but now services are outsourced, you have different suppliers out on the Internet. Users are not necessarily sitting at workstations on your floor; they're on laptops connecting over T-Mobile, so we have to move the security control from the LAN out into the world."

A couple of Daly's projects reflect that reality. He and other industry leaders in the Transglobal Secure Collaboration Program launched CertiPath, the world's first commercial PKI bridge. That infrastructure enables qualified member companies to cross-certify and authenticate, and is itself cross-certified with the U.S. Federal Bridge, which connects the major U.S. defense agencies.

Jeff Nigriny, president and COO of CertiPath, has known Daly for years and says his efforts are invaluable to CertiPath and Raytheon. "We worked with Raytheon for more than a year [to get the company certified] and Michael rode his team pretty hard. The process is fairly onerous and it's fairly easy to get distracted, but he got it done," Nigriny says.

Inside Raytheon, Daly's group deployed new Internet and teaming gateways to Europe this year. Those gateways help ease Web access, remote access, Web hosting, email with spam and virus filtering, single sign-on to the various Raytheon groups in Europe and the Middle East and consolidate several smaller centers that were used in the past.

Daly, the son of not one but two Raytheon engineers, is a busy guy. Jeff Brown, chief information security officer for Raytheon, cites Daly's technical breadth, which he combines with an eagerness to keep learning.

"If you ask him a question on Friday and he doesn't know the answer, by Monday he'll be an expert," Brown says.

Raytheon CIO Rebecca Rhoads agrees. "He attacks everything. He's a voracious reader with great technology abilities and capacity, and he can do a lot of things at once."

Barbara Darrow is a Boston-area freelance writer.



"If you ask him a question on Friday and he doesn't know the answer, by Monday he'll be an expert."

—JEFF BROWN, CHIEF INFORMATION SECURITY OFFICER, RAYTHEON ON

MICHAEL K. DALY

TEXAS, BRITAIN, GREECE

iPod top three: "Got Me Under Pressure," ZZ Top; "Shut Your Eyes," Snow Patrol; "Olympia '06" album, Gregory Lemarchal

MUSCLE

Worked as a bodyguard 20 years ago for several famous—and unnamed—folks.

GADGETS & GAMING

Xbox 360; Playstation 3; Tivo; iPod; Zune



WHERE HAVE I BEEN?

Manaus, Brazil; Atyrau, Kazakhstan; and Bolivia. But nothing beats London.



ADMIRATION SOCIETY

Security heroes: Drs. Whitfield Diffie and Ed Amoroso. Both have holistic views of information security and have had an impact on security on a global scale.

Travel Guide BY NEIL ROITER

4

SASAN HAMIDI

Chief information security officer, Interval International
Industry Retail
Location Miami

Kudos

- Built state-of-the-art security operation center
- Instituted two-factor authentication in 30 global locations
- Leads program to introduce middle school and high school students to information security via handbooks, guest speaking engagements
- Served on PCI and FTC standards boards
- Former director of infrastructure and security at General Electric Power Systems
- Former senior network security analyst and project manager at IBM Global Network Security and AT&T Global Network Security

WITH A TYPICALLY SMALL staff and tight budget, Sasan Hamidi knows he has to sell security to enlist the help of his IT and business colleagues.

“Security is always looked at like we’re cops. We walk through the hallways and people try to hide,” says Hamidi, CISO at vacation exchange company Interval International. “My job is to bring people together, convince them security is important and could affect the bottom line.”

By all accounts, Hamidi does that quite well.

“He’s always aware of different skill sets of certain people in each division, and leverages those skill sets,” says Robby Fussell, senior information security engineer at AT&T Government Solutions and Hamidi’s former colleague at IBM and AT&T. “He’s proactive; most managers I’ve dealt with are reactive, plugging holes when there’s a crisis.”

The proof is in the results. With only two direct-report security staffers Hamidi, in his six years as CISO, has built a state-of-the-art security operations center, instituted two-factor authentication, secured mobile devices, assured compliance with regulations, and accomplished many other projects.

“He really does try to work with business, IT and other departments. He’s dogged at making sure they are aware of a risk and assume responsibility,” says Interval CIO Marie Lee, to whom Hamidi reports. “He always talks with the business managers and puts the need in a business context. And, he’s willing to explain and to compromise.”

“My mother says I should be a politician,” says Hamidi.

He’s much more than that. His knowledge of security policy, processes and technology is broad, deep and current. Hamidi built that knowledge base working at General Electric Power Systems, IBM Global Network Security and AT&T Global Network Security.

“What makes him extremely effective is not only wide knowledge of security across domains, but a vast array of products,” says Fussell.

“He’s the only person I know who has such wide knowledge,” Fussell says.

Hamidi believes strongly in adding the personal touch as well. Years ago he was impressed when a security executive said he spent 10 minutes at his company’s quarterly IT meeting telling people about his personal life—his career background, his military service, his wife and kids.

“I tried it and got a slew of email and calls,” Hamidi recalls. “It makes you more human.”

Hamidi’s zeal extends into the community, where he’s developing an initiative to introduce the basic concepts of information security to Orange County, Fla., middle and high school students.

“I’d just developed a comprehensive information security training and awareness program for my own organization,” says Hamidi.

“Being the father of an 11-year-old daughter who spends a considerable amount of time in front of a computer connected to the Internet, I thought it would be appropriate to put something similar in place for our kids,” Hamidi says.

And, though he’s making his mark in corporate America, there may come a day when a simpler life beckons. That’s why he found time to earn a Ph.D. despite a demanding career.

“I figured that some day, when the hustle and bustle of the corporate world gets to me, I can always teach and do research, my first loves.”

“He always talks with the business managers, and puts the need in a business context.”

—MARIE LEE, CIO, INTERVAL INTERNATIONAL ON

SASAN HAMIDI



MORNING, NIGHT & BRUCE

iPod tunes to live by: “Morning Dance,” Spyro Gyra; “Caspian Nights,” Strunz & Farrah; “Born to Run,” Bruce Springsteen



NEW ENGLAND CALLING

Most recent vacation spots: Boston, New Hampshire, Vermont; but none are as exotic as Rio.



THE CISO SHOW

Hopes to greenlight: “A Day in the Life of an Information Security Officer,” a reality show highlighting the torture endured by security managers spreading the good word of infosecurity.

THERE'S NOTHING LIKE...

A bike ride with my 11-year-old daughter.



MY FRIEND THE THEORIST...

Formed a friendship with Mathematica creator Stephen Wolfram.

$$e=mc^2$$

Risk Reward

BY ROBERT WESTERVELT

5

TIMOTHY S. MCKNIGHT

Vice president, chief information security officer, Northrop Grumman Corp.

Industry Public sector

Location Linthicum, Md.

Certifications CISSP, NSA certified in information security assessment methodology, Cisco Certified Network Associate

Kudos

- Founder, first president, Delaware Valley High Tech Crimes Investigation Association
- Former FBI special agent
- Member of U.S. Computer Emergency Readiness Team Portal
- CISO for the DHS' Critical Warning Information Network
- Member of IT sector Information Sharing and Analysis Center/National Coordinating Center in partnership with DHS
- Manages staff of 100
- Leader in promoting secure collaboration for the aerospace industry
- Fostered creation, adoption of federated identity management for aerospace industry
- Taught forensics at Georgetown University; teaching information security at Drexel University

TIMOTHY S. MCKNIGHT IS ON the front line against cybercriminals tied to organizations with anti-American interests. He's not that far removed from his previous life at the FBI, where, as a special agent he investigated bank robberies and corporate corruption. Now, as vice president and chief information security officer at government contractor Northrop Grumman, McKnight's perpetrators are less tangible, but just as crooked.

"That's what's exciting about security—it's constantly changing," McKnight says. "It's not like we're doing the same job every day—those days are gone. Today we need to get way ahead of threats, anticipate the business needs and reduce the risks to the company."

To reduce those risks, McKnight developed an extensive security metrics program that measures the effectiveness of the enterprise's security initiatives.

Each organization within Northrop Grumman reports on policy compliance, progress on security projects, critical patch response and implementation times, and mitigation of issues found during vulnerability scanning and penetration testing. As many as 50 metrics are rolled into a dashboard viewable by management.

The program helped the company become more efficient, improving patch-management and antivirus capabilities for all servers and desktops, says Keith Glennan, Northrop Grumman's chief technology officer. Not long ago, it took 45 days to deploy patches to 150,000 company devices. Today it takes about 48 hours, Glennan says.

"The threat tempo has obviously picked up, but the foundation Tim helped us put into place is directly attributable to our successes today," says Glennan. "Tim has helped to really frame security as a risk need as opposed to just a cost of doing business."

McKnight oversaw the deployment of disk encryption for Northrop Grumman-owned laptops to mitigate consequences of lost or stolen laptops.

To minimize the probability of virus and worm infections, he removed computers that were not Northrop Grumman-owned or supported from its internal network, and he reduced the risk of sending company-sensitive information to non-employees by removing those email addresses from the company's global address list.

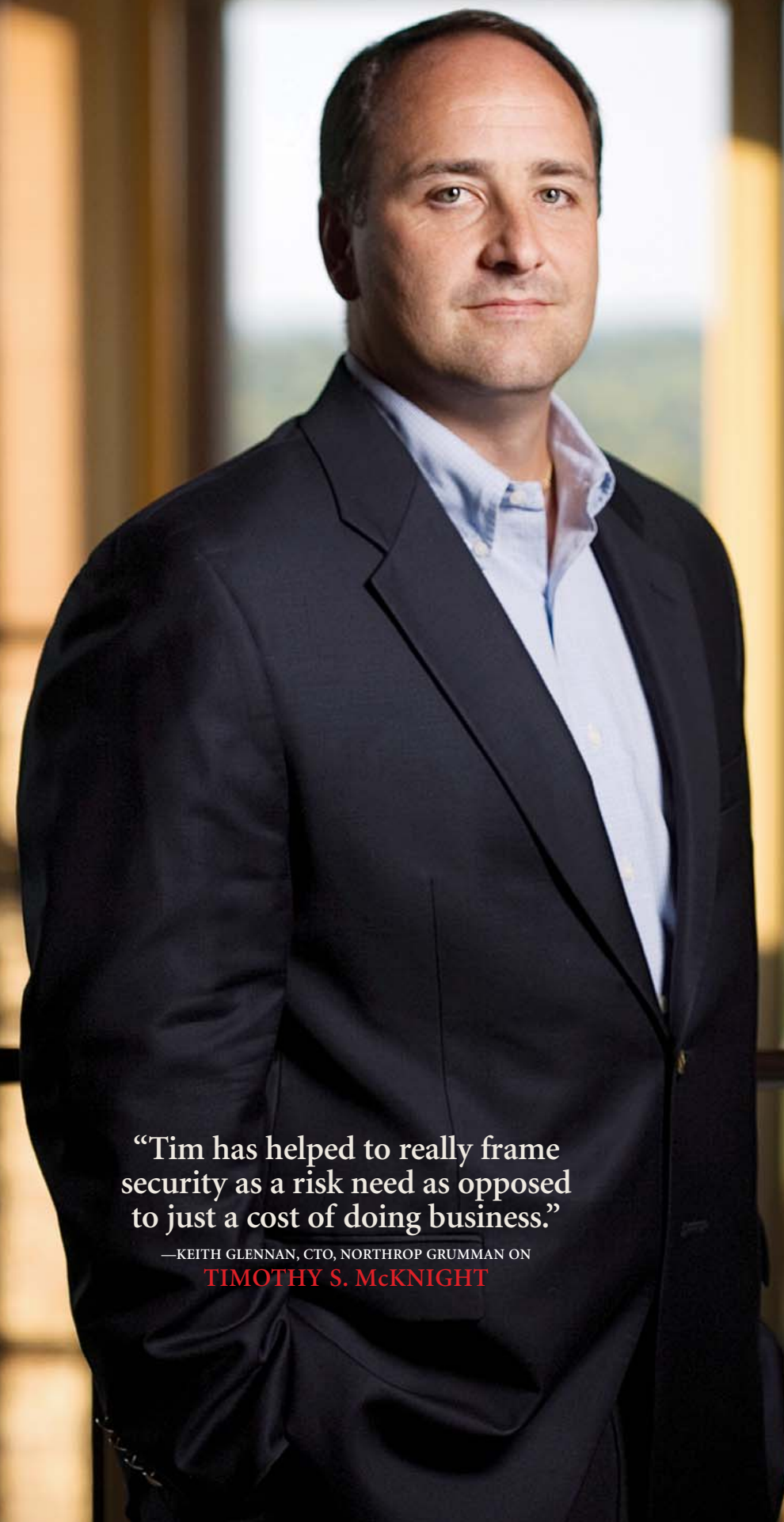
McKnight also helped form the Cyber Threat Analysis and Intelligence group within Northrop Grumman. Comprising former intelligence community experts, military personnel and analysts, the group helps assess threats and is focused on competitive intelligence.

Its work has led to an intellectual property protection and counterintelligence program at Northrop Grumman.

Outside Northrop Grumman, McKnight helped create and served four years as a board member of the TransAtlantic Secure Collaboration Program, which developed the CertiPath PKI Bridge, a third-party identity broker that links commercial contractors in the aerospace and defense industries with government agencies.

McKnight says today's CISO helps shape a company's overall strategic planning.

"The CISO [was] embedded in network organizations a decade ago and now we're getting seats at the table," McKnight says. "The role is becoming less technical and more about leadership and talking the business language in terms of risk."



"Tim has helped to really frame security as a risk need as opposed to just a cost of doing business."

—KEITH GLENNAN, CTO, NORTHROP GRUMMAN ON
TIMOTHY S. MCKNIGHT

ALTERNATIVE SOUNDS

Favorite iPod selections: "Wake Me Up When September Ends," Green Day; "Peace, Love and Understanding," Elvis Costello; "Cool for Cats," Squeeze

TRUMP CARD

Met Donald Trump several times; former Trump Plaza and Trump Taj Mahal employee; never fired.



LEAVING SECURITY FOR...

Dream job: scouting for his beloved New York Yankees.



CAPT. JACK MCKNIGHT

Tivo is always tuned to "Pirate Master," a reality series that puts contestants on a pirate ship searching for treasure.

HEROES

FBI special agent and top terrorism expert John O'Neill, responsible for security of the World Trade Center on September 11. O'Neill perished when the buildings fell.

Audit Doctor

BY MARCIA SAVAGE

6

MARK OLSON

Manager of information systems security and disaster recovery, Beth Israel Deaconess Medical Center
Industry Health care
Location Boston

Kudos

- Created Web-based system to train employees on the handling of patient records
- Involved security and business units in design and testing of security systems
- Secures activities of 10,000 users, 300 servers and 200 clinical applications
- Developed system for automatically auditing access to patient information
- Consulted in New York and Pentagon post-Sept. 11
- Worked for NCR, Digital and EDS
- Originally planned on being a dentist

WITH MORE THAN 11,000 employees using 250 clinical applications, auditing access to medical records of hundreds of thousands of patients at Beth Israel Deaconess Medical Center seemed a daunting if not impossible task.

But Mark Olson, manager of IS security and disaster recovery, tackled the problem head on. Working with other IT groups and the business conduct office at Beth Israel, a teaching hospital of Harvard Medical School in Boston, he and his security team devised a program that ensures compliance with privacy regulations by quickly catching employees who peek at patient records they have no business looking at. And there is a lot of temptation: Beth Israel is the official hospital of the Boston Red Sox.

The innovative program ties data mined from a cross section of clinical applications, security devices and databases with the geographic location of an IP address to quickly catch inappropriate access. It looks for atypical patterns like a physician accessing an extraordinarily large number of records in one day, or a clinician looking up data from an unusual location, and issues an alert.

Olson says the program is modeled on the credit card industry's system of monitoring spending patterns to detect abnormal behavior. He's getting the word out about Beth Israel's program through presentations at national and local conferences to help IT professionals understand that some basic data mining and ingenuity can go a long way in building an effective auditing program.

"People shy away from it because they look at the problem as too large of one to solve," he says.

John Powers, Beth Israel's chief administrative information officer, says Olson's creativity and thoroughness have been invaluable.

"The bottom line is that we think that the safety of our patient database is markedly improved compared to other hospitals as a result of this security umbrella we put over it using Mark's concept," he says.

The program is a novel turn on the usual reactive, complaint-driven approach to compliance with privacy standards, and allows the hospital to be proactive, says Tim Hogan, Beth Israel's director of corporate counsel.

Olson's team has also added auditing to a Web-based training system that meets HIPAA required training for handling patient records.

"He's just done tremendous work in bringing about a transformation of the technical security, but also in providing leadership across the various technology groups to get everybody aware of the need for security when making changes or introducing technologies," Powers says.

"We've buttoned down our environment mightily since Mark has been at the helm of our security," Powers says.

Today, Olson extols the benefits of auditing. In the health care industry, records are shifting from paper to electronic, which promises significant benefits but also presents challenges in guaranteeing that information is kept private and secure.

Being proactive is essential, Olson says, and doing more in the area of auditing would help the security industry become less reactive.

"Security isn't looked at as an auditing job and in my view it is," he says. "We need to do more auditing to discover trend analysis and find out [when] something is about to happen." •



"We've buttoned down our environment mightily since Mark has been at the helm of our security."

—JOHN POWERS, CHIEF ADMINISTRATIVE INFORMATION OFFICER, BETH ISRAEL DEACONESS MEDICAL CENTER ON

MARK OLSON

GUESS MY FAVORITE ARTIST

iPod must-listen songs: "Give it One," Maynard Ferguson; "The Fly," Maynard Ferguson; "It's My Pleasure," Billy Preston



CASABLANCA, ANYONE?

Morocco beckoned for an exotic getaway.



BLOG LOG

At work: Bugtraq
 At home: Lifehacker



STEEL CURTAIN

Lifelong Pittsburgh Steelers fan



WHAT'S GOT ME WORRIED

Our security posture is too reactive. I don't believe it's possible to be 100 percent proactive, but we need to be closer to that side of the pendulum.

Real-Time Security

BY MICHAEL S. MIMOSO

7

SIMON RIGGS

Global head of IT security,
Reuters Operations
Industry Financial services
Location London

Kudos

- Secures complex real-time data-feed infrastructure (30,000 switches and routers and more than 1,300 firewalls) and large historical databases
- Advocate of IT security service management
- Integrating security as a discipline into ITIL best practices
- Working toward unifying operations and security

REUTERS' BUSINESS IS PROVIDING the financial industry with real-time pricing information, market news and trading services. More than 300,000 professionals in the equities, commodities, foreign exchange and other markets count on the availability and reliability of the information Reuters delivers. It's a prime example where security services mustn't get in the way of business.

Simon Riggs, the global head of IT security, has an internal audit and consulting background guiding his insistence on bringing security in line with Reuters' established service management philosophy. At the core, Riggs wants his security teams to be proactive about finding weak spots in IT systems and business processes, using cutting-edge modeling to determine the risks imposed by not only security events, but changes to the network.

"I'm a great believer that we shouldn't be doing security for the sake of doing security. We should be doing security because we're running a business," Riggs says.

Service management is a Reuters-wide mandate, one spawned three years ago as a regimen of strict best practices based on the popular U.K. ITIL standard. Riggs is also working to integrate IT security as a global discipline into ITIL best practices.

"As a company we've been banging the drum about customer service, and we're pushing hard to ensure things are done in a systematic, disciplined way to make the customer experience even better," Riggs says.

Reuters' customers measure performance in hundredths or thousandths of seconds; latency is not tolerated. Thus it is dogged work tracking a complex environment of real-time data feeds, historical databases and an infrastructure of 30,000 switches, routers and more than 1,300 firewalls.

A standardized service management approach is the only logical means of keeping such complexity reined in, Riggs says. In addition, the company has unified operations and security around incident, problem, configuration, change and release management processes. For example, Reuters' security analysts examine every security incident—whether it caused a disruption or not—to understand a root cause of the management behavior that failed and why a service was not resilient. Finding the root cause allows Riggs' team to apply that information elsewhere and mitigate future events. Modeling exercises, meanwhile, allow them to anticipate problems in the event of future incidents or scheduled network changes, which can number hundreds per week.

"You always expect your infrastructure to come under attack. But if it fails, you have to understand the real underlying root cause. Was it a network design problem, a third-party quality failure, capacity overrun or did it fail because of a configuration problem?" Riggs says. "We want to pinpoint this as well as any aggravating factors and triggers...and then see where we may be exposed elsewhere and fix it before it causes customer pain."

Riggs has tried to instill that uniformity up and down Reuters' supply chain as well.

"I treat them as a virtual extension of my team, and expect them to behave in a certain way," Riggs says. "That's what I expect of the products they deliver."

Stephen Bonner, head of information risk management at Barclays, says Riggs' focus on service management has won over his share of supporters. "He brings a refreshing approach to security based around meeting business needs rather than slavish application of historic approaches," Bonner says. "He focuses on execution and delivery."

"He brings a refreshing approach to security based around meeting business needs rather than slavish application of historic approaches."

—STEPHEN BONNER, HEAD OF INFORMATION RISK MANAGEMENT, BARCLAYS ON
SIMON RIGGS



A FOUR-STEP PLAN

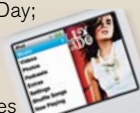
Simon Riggs espouses a four-step approach to unify operations and security in order to apply new modeling and analysis techniques and be proactive about security and risk assessments.

- 1 CATALOG infrastructure and device assets to establish attributes, locations, functions and management of those assets.
- 2 BE PROACTIVE in problem management; detail root causes of security incidents and shape a remediation strategy that can be applied uniformly across the enterprise. Sophisticated modeling proactively identifies problem areas as well.
- 3 CONTROL change management; model networks to verify the impact of changes to the network and risk controls before they are deployed.
- 4 INTEGRATE ITIL best practices; align security with Reuters' processes for incident, problem, configuration, change and release management.

—MICHAEL S. MIMOSO

FEELING GREEN (DAY)

On my iPod: "Are We the Waiting," Green Day; "In the Morning," Norah Jones; "One Week," Barenaked Ladies



CHARITABLE

He was part of a team from Reuters helping to rebuild homes in Sri Lanka after the 2004 tsunami.

TV'S GREAT ESCAPE

Wouldn't mind being picked for a stint on "Survivor" just to get away from his BlackBerry for a while.



CAMPY FUN

Spent his last vacation as a Scout leader on camp celebrating 100 years of Scouting. "I came back absolutely dead beat, and it took days to scrub the grime off. Fantastic."

ON THE BOOKSHELF

Life is Short, Wear Your Party Pants, by Loretta LaRoche. "Reminds us not to take ourselves too seriously."

CATCHING UP WITH CHRISTOFER HOFF

After winning the 2005 Security 7 Award in financial services, Chris Hoff has become a prolific blogger, willing to share his opinions on the security market and new technologies, in particular the need for security in virtual environments.

ON HIS NEW JOB WITH UNISYS I spent two years with Crossbeam and it was a fantastic experience. I gained exposure to the Fortune 500, carriers, mobile service providers and other spaces. [Crossbeam] is in a growth pattern and they're focused on applying strategy, not crafting it. I looked at the position with Unisys (chief security architect, security innovation) as an opportunity to expand my horizons.

They're in the middle of a business transformation, and it's a very interesting intersection.

I work for the office of business innovation, and one of the pillars of Unisys' business strategy focuses on security. That means more than information security; it means protecting borders of countries, working with the Department of Defense, container security, port security; it expands my horizons on the convergence of the physical and IT elements of security. It's been quite interesting.



ON SECURING VIRTUAL ENVIRONMENTS This technology is 30-40 years old; think about IBM and ALPARS (affinity logical partitions). People are looking for less footprint and more computing power. On the business side, CIOs are looking at cost savings, then think about security. One side of the market is centralizing with thin, dumb clients, and using hosted software as a service and Ajax applications, dispersing processing power to the edge. The two intersections are never secured.

Virtualization is fantastic: it does great things for cost, horrible things for security. But I think we're making progress on this portion of the uphill slant. Look at the classes of problems we have; we haven't eliminated any, we're creating more.

Ajax is an example, and we're at odds of how business and technology are approaching these problem sets. We've put all this power in users' hands and we yank it back because we never engineered proper security in the first place. It's not right.

ON ACQUISITIONS If there are 800 security companies in the dating pool, some of them were born to be commoditized, others were born to be snapped up. Data leak prevention, for example, is a feature without a market. And it's normal, and I welcome it.

You get these nascent products and the features either take hold or run out their lifecycles and get integrated into end-to-end suites. If you look back over time, this is natural and normal. Every time we carry over to another intersection of technology, economics and business problems, we end up having new niche companies. It will be a sad day if we don't have innovation.

ON BLOGGING I owe my blog (<http://rationalsecurity.typepad.com/blog/>) to one of the biggest agitators around, Alan Shimel [chief strategy officer, StillSecure]. He came out for a visit and told me, to blog and make a difference, it's something you have to do every day so that it becomes part of your life. It becomes addictive, like checking email. You gotta do it. And when people interact with you, it's quite amazing. I never expected it would open avenues of discussion, networking and more. ▶

—MICHAEL S. MIMOSO

honor roll

Information Security's list of past Security 7 Award winners:

- STEPHEN BONNER (Financial services)
- LARRY BROCK (Manufacturing)
- DOROTHY DENNING (Education)
- ROBERT GARIGUE (Telecommunications)
- ANDRE GOLD (Retail)
- PHILIP HENEGHAN (Government)
- CRAIG SHUMARD (Health care)
- EDWARD AMOROSO (Telecommunications)
- HANS-OTTMAR BECKMANN (Manufacturing)
- DAVE DITTRICH (Education)
- PATRICK HEIM (Health care)
- CHRISTOFER HOFF (Financial services)
- RICHARD JACKSON (Energy/utilities)
- CHARLES MCGANN (Government)

CATCHING UP WITH ANDRE GOLD

Last year's retail award winner has moved on to a new position in a new vertical market as head of technology risk management with ING.

ON HIS NEW JOB At Continental, I had responsibilities over policy, strategy and execution. Here, it's just strategies and execution; policies come from the group level. At Continental, the organization was 50 years old and never really

focused on information risk management; here in financial services, it's all about risk management. The first day I walked in, there were posters on the wall about Compliance Week and security awareness training. At the fundamental level, information risk management is germane across industries. It's just that a number of external statutes caused companies to lose track of the fundamental blocking and tackling of information risk management. At ING, that's what we focus on.

ON SWITCHING INDUSTRIES It was absolute culture shock. I have one of those posters in my office now, and I'm thinking of having some fun and making a PDF copy for some of my friends. 'See: this is what we were striving for!' It's a lot easier to get the business engaged; everyone has a notion of risk. The executive team is cognizant of the role information risk management plays in the delivery of products and services.

ON THE SECURITY MARKET Buying habits were a lot different 18 months ago than they are today. Big companies today are a lot more focused on providing synergies between product portfolios. Now, you're not looking just at best-of-breed, now it's about vendors telling their portfolio story, how they leverage XYZ products. What companies are doing is looking at who is going to be a technology security partner for them, making a bet on that company and leveraging their technology exclusively with one or two that they'll primarily buy from. On the other hand, there are still markets where you can a la cart some technology if you're trying to meet a particular need. It's about making the right choices.

ON THE PURSUIT OF HIS MBA I took the summer off with the new job, but grad school just started up again and I'm back riding the bull. I would have graduated this spring otherwise. ▶

—MICHAEL S. MIMOSO



Remembering a Model CISO



I met Robert Garigue a year ago at a luncheon in Chicago for the Security 7 Award winners. Robert was at my table, as were fellow honorees Stephen Bonner and Andre Gold. It didn't take long to ascertain who would carry the conversation at our table, and not because he craved the attention. No, it just gravitated to Robert because his opinions were so informed, his dialogue so pointed. It was readily apparent this man should be heard because his words weren't like what was being spoken at the time by other security professionals. That, and he was genuinely a nice man, one who asked if we'd be so kind as to send him a glossy print of his cover image so that he could present it to his mother for her home.

His death in January was a shock because he made such an immediate impression on all of us in the brief time we knew him. But to his colleagues, the grief was profound. Notes and email from many of them proved that he touched many lives, and a year later, it's appropriate to remember him in these pages with a sample of his work.

Doing some digging on our Web site, I came across a presentation he did for our 2004 Information Security Decisions conference on the evolving role of the CISO. It truly could stand as a thesis on the role of the corporate security officer. But one slide stands out best.

In it, Robert suggests the Emperor Charlemagne stand as a model CISOs should emulate. Charlemagne, Robert wrote, reunited Europe after the Dark Ages, established schools that were open to nobles and peasants. He brought scholars from all corners to encourage development of a standard script. He established money standards, urged new farming methods and spread education to all classes. He relied on others to build an infrastructure on which others could thrive.

There are lessons here, and it's fair to say, Robert followed them in his work and his studies. Perhaps Robert Garigue is a model more CISOs should emulate. ▶

—MICHAEL S. MIMOSO

BY THE NUMBERS
We quantify some leisure-time facts about this year's Security 7 Award winners.

Social networking use:

- 0 MySpace
- 1 Facebook
- 4 LinkedIn

iPhone:

- 1 owns an iPhone

Party Lines

- 1 Republican
- 5 Don't vote along party lines

Average Travel Days/Month:

7.3

connect to...

Many of our Security 7 winners have crossed paths in the past. Here are a few examples:

