Financial services security

Getting in line to keep data safe

ebook

An SC Magazine publication

Sponsored by

Getting in line to keep data safe

With high fines and punishments, many companies do not have a choice whether or not to become compliant. There are tools, services and strategies to help, reports Jeffrey Ober.

Financial services organizations have more than their fair share of regulatory mandates with which to comply. Really, no matter the company, no matter the technology, there are going to be a mass of government regulations, citing information security requirements, that need to be stringently followed. But as CSOs and their bosses scramble to ensure their companies have a handle on these, it is difficult to determine just which mandates are the most important.

So, just how are companies deciding their compliance priorities and avoiding duplication of their efforts when complying with frequently similar security requirements noted in many government and industry mandates? What are they doing to find ways to comply with these ever-changing mandates? Which ones do companies truly need to comply with and which do they not?

And, asks Richard Mackey, VP of consulting for SystemExperts, an IT and security consultancy, why comply? The answer, he says, is because business partners and clients are going to ask. "It is becoming self-policing these days. There is talk about financial penalties, but these really only apply if there is a breach."

Every company that has customers will have to come up with answers to these and other related questions if they want to survive in business today. And information security leaders need to have the answers ready for any audit at any time.

Mandates impacting the financial sector

Perhaps the superstar of regulations that affect financial and other types of companies is the *Sarbanes-Oxley Act (SOX)* passed in 2002. It is an over-arching law with numerous regulations tied to accounting checks and balances, and was one of the first to require massive changes in accounting and other inter-company processes for businesses. Today, compliance with *SOX* is built into almost every business process.

"Any company that doesn't already have *SOX* compliance as part of the way they are doing business today is a company that's really behind the times in today's world," says Bhavesh Bhagat, president and CEO of EnCrisp, a solution lifecycle management and compliance company.

Prior to *SOX*, the *Gramm-Leach-Bliley Act*, also called the *Financial Services Modernization Act of 1999*, added a few new compliance issues in the areas of financial privacy, safeguards and pre-texting. However, it was primarily designed to allow various types of corporations to merge – commercial banks, insurance companies and securities trading firms could now be combined into one corporate entity which had been previously prohibited by law. But the law has its weaknesses, Mackey says.

"*Gramm-Leach-Bliley* is more of a concept. It requires the company to abide by intent, and people tend to interpret that intent differently," he explains.

Other guidelines have been on the books for decades. In 1979, the Federal Financial Institutions Examination Council (FFIEC) was established to determine uniform principles, standards and reporting formats for financial institutions in the United States. This agency requires institutions to comply in a number of areas, such as with the *Home Mortgage Disclosure Act (HMDA) of 1975* and the *Community Reinvestment Act (CRA) of 1977*. More recently, the FFIEC has issued guidelines and requirements for electronic and internet transactions.

Another that can affect companies in the financial services market depending on their specialties or partnerships, and which cer-

56%

of information security budgets have increased

– Deloitte, June 2010

tainly hits many others, is the *Health Insurance Portability and Accountability Act*, or *HIPAA*. Passed in 1996 to much controversy due to the unknown amount of personnel power and resources that were going to be required for companies to come into compliance with it, organizations are still struggling with *HIPAA*, especially given new developments made by the Obama administration.

The main portion of *HIPAA* provided that consumers could carry their health insurance from one job to another. But the second portion, Title II, created a set of standards for the use, retention and administration of all individual health care data for companies and health providers. The regulation created a set of data, called protected health information (PHI), and set out rules to determine how that data should be protected from accidental or intentional disclosure without permission from the individual. This set of rules is referred to as the "privacy rules" of *HIPAA*.

HIPAA also set up standards for reporting data electronically, including sets of data and

Financial firms: Security budgets stable, increasing

Despite a lingering recession, information security budgets at financial institutions generally are staying stable, or in many instances, even have increased, according to a study conducted by accounting and consulting firm Deloitte.

The seventh annual survey of security spending and priorities at financial institutions worldwide, released in June 2010, found that 56 percent of information security budgets have increased. Additionally, the survey found there was a 20 percent drop this year in the percentage of respondents who said a lack of sufficient budget is a major barrier to information security.

When it comes to priorities, the largest percentage of respondents cited identity and access management (IAM), followed by data protection, regulatory and legislative compliance and compliance remediation.

Regulatory pressure is driving much of the security activity within the financial sector. "The regulators of most large financial institutions have been much more aggressive over the last 18 to 24 months in general, translating to much more pressure in existing regulations," Ed Powers, leader of Deloitte's security and privacy practice for the financial services industry, told said.

This year was the first time since the survey began that information security compliance came out as one of the top five security initiatives. Thirty-four percent of respondents said regulatory and legislative compliance is a top priority, while 33 percent said compliance remediation is of most concern. Financial firms are hiring more internal auditors to resolve the findings of internal and external compliance audits, the survey found.

This heightened regulatory pressure has resulted in increased visibility at the board level for security and risk, especially with regard to customer data protection and sustained or increased budgets, Powers said.

Also, financial institutions of all sizes, but especially larger organizations, reported excessive access rights as a top security problem, the survey states. As a result, IAM has become a main priority for 44 percent of those surveyed.

Financial organizations also recognize that external threats are becoming more targeted, organized and sophisticated, Powers said. Organized criminals are targeting these institutions for financial gain, but there also is growing concern about the potential impact of cyberattacks on an organization's infrastructure. Consequently, the survey found that security infrastructure improvement is a main priority for 36 percent of respondents. – *Angela Moscaritolo*

25k

patient records at risk of exposure after computers stolen from offices of Fort Worth Allergy and Asthma Associates in Aug. 2010

codes for various types and statuses of different health conditions and health care provided. In 2003, another rule related to *HIPAA* was implemented called the "security rule." This set out a specific set of security standards for all related health data and PHI data.

HIPAA is one of the best understood of the various government regulations because, according to Mackey, "*HIPAA* has addressable controls. A company has to do a risk assessment to determine which of the addressable controls to use to ensure compliance."

> "Compliance is an extremely high priority."
> – Leon Thomas, president and CEO, Jelecos

In 2009, a further set of rules related to *HIPAA* was created, including privacy act requirements covered in the *American Recovery and Reinvestment Act of 2009*, otherwise known as the stimulus act, which President Obama signed into law and subsequently penned the *Health Information Technology for Economic and Clinical Health Act*, or *HITECH Act*, into existence last February. *HITECH* introduces a number of changes to *HIPAA* requirements and enforcement that do indeed punch up privacy and security regulation for the industry – especially when considered in light of increased EMR use, health care experts widely agree.

Among the changes: Health care organizations suffering a security breach affecting 500 or more individuals now must not only notify individuals of unauthorized disclosures of their unsecured PHI, but also report said incidents to the U.S. Department of Health and Human Services (HHS) for public notice. As of mid-April, the HHS has posted breach notices from 59 organizations, including several just over that 500 mark and a couple with multiple hundreds of thousands of individuals affected.

Meanwhile,The Payment Card Industry Data Security Standards (PCI DSS) apply to information security data. These standards were created and defined by the Payment Card Industry Security Standards Council in order to create a level of security associated with payment processing information for use with Visa, MasterCard, American Express and Discover credit cards. The latest version of PCI DSS is version 1.2.1, released in August 2009. These standards are defined in six groups. Vendors processing these cards are required to build and maintain a secure network. They are also required to protect cardholder data and maintain a vulnerability management program. Any vendor using or accessing customer data from these credit card brands also must implement strong access control measures, regularly monitor and test networks, and maintain an information security policy.

Today, many companies realize the level of complexity involved with these vast government compliance issues. Many will go outside to private companies that are experienced and specialize in government compliance to ensure they are fulfilling their mandated obligations.

"PCI DSS compliance is the most common [type of compliance] that we have to help our clients with," says David Johnson, vice president of The Fulcrum Group, an IT consulting firm.

Privacy compliance

One of the primary areas associated with regulatory compliance and information technology is privacy. Various regulations require PII be retained under certain circumstances and be protected against breaches. These laws and regulations vary between federal and state laws, with some states requiring more protection than do the federal laws.

"Privacy compliance has a lot of unknowns," says EnCrisp's Bhagat. This is owing to the fact that state and federal governments are continuing to add and change requirements leaving corporations in limbo regarding compliance.

"Companies are revising their policies, using more encryption and trying to secure all

$41m

T.J. Maxx agreed to pay in its settlement with Visa

customer data in any way possible," he says. "Enterprises aren't doing anything dramatically new or earth-shattering, just using technology that has been around for some time to ensure increased privacy."

Bhagat adds that most organizations are very responsive and take privacy concerns very seriously. For some, it is one of their top priorities, he says, and not just because of the very large fines for failure to secure private data. In most cases, the fines are per transaction and per record – so a seemingly small lapse in privacy can quickly result in a fine of millions of dollars.

"But companies are even more worried about the potential loss of good will in any case of privacy lapses," he says, noting that retailer TJ Maxx is still reeling from its loss of credit card data years ago.

"Companies are increasing privacy protections today," adds Mackey.

Many corporations, particularly several in the financial vertical, are searching for common solutions to the various compliance

ATM FLAW: Researcher forces ATMs to spit out cash

A security researcher in late July forced two ATMs to spit out bundles of cash thanks to security weaknesses in the machines.

Barnaby Jack, director of security researcher at IOActive Labs, completed the feat while on stage at the Black Hat conference in Sin City. Jack demonstrated a physical and remote attack on two cash machines that he had purchased on the internet. The attacks allowed him to force the machines to spew cash, seemingly at an unlimited rate.

"Every ATM I've looked at I've found the game-over vulnerability that lets me get cash out of the machine," Jack said in a press conference after his talk.

In one of his demonstrations, Jack used a master key that he purchased online for about $10 to open the door to the ATM, which allowed him to install modified software in the form of a USB key to the motherboard, thereby overwriting the machine's firmware. The maker, Mississippi-based Triton, which has some 150,000 machines worldwide, has since issued an update that prohibits software from running that hasn't been digitally signed by the company, Triton engineers said at the press conference.

Jack awed the crowd when he opened up the machine, applied the modified software and, not long after, the ATM began spilling cash, bill after bill. He even forced it to play music resembling the sound a slot machine makes when a player hits the jackpot.

In the other case, Jack used an attack tool he named "Dillinger," after the infamous 1930s bank robber, to exploit a vulnerability in the remote monitoring authentication process, which is turned on by default in most machines made by the manufacturer Tranax, based in Hayward, Calif. This allowed him to remotely install a rootkit he named "Scrooge," which hides itself on the machine from things like the process list and file system.

He called the exploit "100 percent reliable." However, Tranax now is offering a workaround – disabling remote access by default, Jack said.

Jack said his work underscores the security problems around embedded systems, such as electronic voting machines and parking meters. As a response, vendors must upgrade their firmware, roll out machines that require unique physical keys and conduct proper code review, including penetration tests.

Jack said he is confident bank ATMs are just as easy to penetrate and take control of, mostly because they are based on even more vulnerable operating systems than Windows CE. However, he has not had an opportunity to study them because they are not sold over the internet.

– Dan Kaplan

$204

per compromised customer record in 2009 was the cost of a data breach

–Ponemon Institute

requirements and are often creating higher levels of compliance just to ensure the vital data is protected.

"For example, if a company has to protect data for the residents of Massachusetts in a certain way to meet state requirements, the company isn't going to go through the trouble of separating state residents from other residents," Mackey says. "Instead the company will end up protecting all [clients'] required data per the state requirements."

> "Companies are recognizing that regulations are there for a reason."
> *– Doug Landoll, director of risk and compliance management, Accuvant*

Another thing that he says companies are doing is simply eliminating data. "If the company reduces the amount of data they store, they reduce the amount of data they have to protect," Mackey points out. "Some companies are retaining data only long enough to complete an order, but then delete all privacy data that needs protection. Other companies are taking the data they receive and are encoding it using one-way hashes to encrypt the data so personally identifiable data has been removed. Then, if there is a compromise, there is no danger of exposure of personal, private data."

For example, a company may collect private data about a customer, but then convert the Social Security number into a hashed number so if the data is stolen, it is useless as identifiable data, he says.

Doug Landoll, director of risk and compliance management for Accuvant, a national security consulting organization, refers to these as the "more mature regulations." Because they have been around for so long, he says, most of his clients have moved beyond the first stage of gap assessment and remediation. Instead, he's seeing clients working more on efficiency and integration related to *SOX* and *Gramm-Leach-Bliley*.

"The controls that are required by the regulations are now being well integrated into overall operational processes and companies are looking for efficiency through process improvement and automation," Landoll says.

Other companies offer consulting services to ensure that their clients submit themselves to various outside audits and checks. Leon Thomas, president and CEO of Jelecos, an IT consulting and services firm that specializes in helping companies become compliant, uses various methods to ensure compliance.

"As a service provider, compliance is an extremely high priority. Not only are we contractually bound to provide proof of compliance, it provides a competitive advantage in the marketplace,"he says.

To keep up with the changing demands of government compliance, many companies also have added C-level executives, such as chief compliance officers (CCOs) or chief risk officers (CROs), in addition to chief security/information security officers (CSOs/CISOs), who are responsible for ensuring that their companies are in line with mandates.

"Compliance responsibilities are migrating from the CIO to the CFO because of the personal risk and responsibilities placed on the executives in the compliance laws and regulations," Bhagat says.

The Fulcrum Group's Johnson agrees: "We typically try to engage with our clients at both the executive/management and IT levels, and try to ensure that there is executive buy-in regarding the importance of compliance."

Compliance priorities

While much of the news related to non-compliance surrounds the financial penalties, Mackey says those threats are not really the reason that most companies constantly work on getting in line with mandates.

"It is unlikely that a company will be audited for a compliance check out of the blue," he says. "There are too many companies and not enough inspectors. Instead, companies are normally audited only after a breach."

$6.7m
average total cost of a data breach in 2009

–Ponemon Institute

Further, many C-level officers at financial services companies, as well as with organizations from other sectors, are focusing their efforts on common requirements for different compliance areas. The top priorities are finding three to five areas of risk that are common across various different compliance categories and working to ensure compliance in those areas. Older areas of compliance, such as *SOX*, are nearly automatic, but many companies are having trouble with new and current compliance areas that are rapidly changing due to government changes and to the varied and sometimes conflicting requirements between state and federal governments.

"*SOX* is not as applicable today," says Mackey. "At first, companies were scrambling to determine how to comply with *SOX*, but companies are not having troubles today as *SOX* is just a part of doing business today."

To come into compliance, a company first has to find the information and data the company has, he adds. "Who has it, where is it and what regulations apply?" By applying the most restrictive limits to all data, the company will reduce its exposure and the possibility of compromise.

"In addition, companies today have to deal with various electronic partners," says Mackey. "In order to remain compliant, the company must not only protect all private data they receive from partners, they also need to protect all data they send to other partners. There is no official compliance standard today, so companies need to rely on their partners claiming their own compliance. Some will use ISO standards, deciding that if a company is ISO compliant, it will also be compliant with the various specific government regulations."

Accuvant's Landoll says one way companies are working more efficiently with various government compliance regulations is to "build compliance requirements into a more holistic security program so that it becomes part of the program that is enacted and monitored day after day."

Storage risk: Citi urges iPhone app update

Citigroup released an update to its iPhone mobile banking application after it was discovered that the previous version, unbeknownst to users, saved confidential account information in a hidden file on their devices. The prior version of the Citi Mobile application also may have saved the same data onto users' computers if they synced their iPhone to their computer using iTunes.

"This update deletes any Citi Mobile information that may have been saved to their iPhone or computer, and it eliminates the possibility that this will occur in the future," said a Citigroup statement.

Neil MacDonald, a VP and fellow at research firm Gartner, said users should expect to see similar incidents in the future due to poor developer design and a lack of security vetting by owners of application stores, such as Apple.

"I think because of that implied responsibility, Apple needs to step up the testing it performs," he said. "I'd say the same of Google [maker of the Android] and Microsoft [maker of Windows Phone 7]."

Meanwhile, developers such as Citigroup must implement similar guidelines and conduct threat modeling, a process that will help determine things such as where sensitive data is being stored, how might a hacker might be able to access such data and whether the user properly is being notified appropriately of any data being stored, MacDonald said.

He said that many times developers make mistakes in a rush to distribute a product.

"You cannot overlook security in the development process, even if it is agile development," MacDonald said.

An Apple spokesperson did not respond to a request for comment. – *Dan Kaplan*

79k

retirees, current and former employees who participated in a pension plan at AMR Corp. may have had their personal information stolen by the theft of a hard drive containing microfilm files.

– Privacy Rights Clearinghouse

Too many companies, he says, spend their efforts and budgets on checking off compliance boxes and implementing point solutions. "Companies should be taking a risk-based approach," he says. "This will enable them to spend less money, reduce the amount of time lost reacting to emergency situations, deliver effective protection of carefully researched and identified sensitive data, and still comply with the various requirements and standards."

High-value compliance

When it comes to compliance and avoiding penalties, each company – whether or not in the financial vertical – has to decide which areas are the most important and which areas should be brought into compliance first.

Bhagat says one area affecting the financial sector involves the U.S. government increasing prosecution in export compliance. "In the last two years, the government has ramped up prosecution in the area of export compliance," he says. "They are doing much more aggressive prosecution in the areas of defense and finance to get money for government. The government is looking for violations in areas of money laundering and export encryption. Many of these areas of compliance also include gray areas and are not as black and white as other areas."

Mackey says the area that is the most difficult to bring into compliance is the area of PCI data because it is a contract, not a law or regulation. However, he says the state of Nevada requires that merchants must comply with PCI rules, making it a law and a contract.

While the PCI rules are detailed, they still are often difficult to follow. "Some companies will follow a checklist for PCI and believe they are in compliance because they have a small number of transactions," says Mackey. "However, that is just the suggested process for a company with a small number of transactions – and the company is not actually in compliance until they have met all the requirements listed. It is very difficult for any company to have 100 percent compliance with PCI."

In fact, Mackey isn't sure he's ever seen any company 100 percent compliant in this area.

"Companies are paying most attention to regulations with big hammers (deadlines and penalties), and focusing on the checklist of required controls to avoid fines and reputational stigmas," says Accuvant's Landoll. He agrees with Mackey that PCI is causing companies lots of trouble. He says it is driving companies to spend entire annual IT budgets on point solutions to address specific elements of the Data Security Standard. Because of these tremendous costs and focus, other areas of security are getting pushed aside and neglected – this is possibly setting up to more risk of exposure other company data not related to customer security and regulation.

> "HIPAA has addressable controls."
> *– Richard Mackey, VP of consulting, SystemExperts*

"*HIPAA* protects medical privacy information around patient care," he says. It does not, however, list any requirements related to vulnerability management or any risk-based decision-making. "*Sarbanes-Oxley* section 404 assesses the effectiveness of internal controls around financial information, but beyond this scope, the security environment is largely ignored," says Landoll. This process is causing a lot of companies to spend a great deal of time and money checking off boxes, but ignoring real processes or potential security problems.

"Mandates such as *SOX* and *HIPAA* often present the largest challenges simply because they are generally not very well understood and there are sections of these mandates that are left up to interpretation," adds Jelecos's Thomas. These different areas of interpretation make it difficult for a company to know if it is truly in compliance. And if government regulators interpret the rules differently than the company, the company may find itself out of compliance.

1.2m

customers of Lincoln National Corp. were put at risk of ID theft after a security vulnerability in the company's portfolio information system could have compromised account data

– Privacy Rights Clearinghouse

New technologies

Many of the technologies currently used for compliance simply did not exist even five years ago. While basic privacy protection does not require any new technologies, many strategies and tools are being introduced to help support compliance issues. In many cases, financial services companies, as well as organizations in other sectors, had different technologies in different areas of the company, and they need to actually locate and combine the technologies for compliance issues. These organizations are also spending a good deal of time identifying the needs they have for compliance based on the technologies they currently have in place.

Software automation is one way that companies are changing dramatically to meet various government regulations. "Health care and *HIPPA* regulations are causing IT to expand," says Mackey. "The wave of new laws and regulations are causing companies to find their own data and determine how to protect that data. Previous laws dealt primarily with notifications, but new laws are more specific and are prescribing how to protect private data."

Cloud computing is a new, rapidly expanding technology that EnCrisp's Bhagat says has huge potential for companies in the area of compliance. "This technology opens all sorts of new opportunities and challenges in managing data."

This technology, he says, will soon allow financial and other companies to manage data in the data lifecycle like inventories in the supply chain management system – which most companies are already intimately familiar with.

Landoll adds that data leakage prevention, encryption, GRC tools and access and security logging tools are the most commonly used new technologies companies are using to safeguard critical data.

For his part, Thomas uses extensive encryption in any custom application his company builds to safeguard data combined with standardized equipment hardening procedures and physical and logical security configurations and procedures.

Regulations are there for a reason

Bhagat says that financial services companies, along with organizations from other sectors, are spending millions of dollars in often erroneous ways because they are failing to identify their needs and problems related to compliance from the outset. As a result, many discover that even after the spending spree, they may have plenty of solutions in house, but none that are really helping them to comply with required mandates.

He expects more consolidation in the provider space over the next five to 10 years, especially in the areas of IT, as vendors develop more products that are designed to help with the various governmental compliance rules.

"Companies are recognizing that regulations are there for a reason," says Landoll. "However, they need to realize that there are best practices and there are implementations. Proper implementation of security controls – rather than just meeting regulatory requirements – will bring about efficiencies."

And, in order to improve corporate security policies and the safety of critical information overall, as well as remain a viable organization in a growingly competitive marketplace, each financial services organization – and most other corporations for that matter – will need to get in line with these various laws and regulations. Failing to do this, along with developing the clear understanding that information security underpins sound business practices today, only will result in high fines and punishments for non-compliance. ■

For more information, please contact Illena Armstrong, editor-in-chief, SC Magazine, *at illena.armstrong@haymarketmedia.com.*

5.1m

patient records have been breached as of July 23, 2010, according to an analysis by Health Information Privacy/ Security Alert (HIP/SA)

REDUCE COMPLIANCE CHALLENGES WITH TRIPWIRE SOLUTIONS

tripwire™
TAKE CONTROL.

The banking and financial services industry faces tremendous scrutiny by both domestic and international regulatory bodies. PCI, SOX, FFIEC and GLBA regulations and mandates aim to ensure the integrity of financial reporting information and the privacy and protection of personal information stored and transmitted in bank information systems.

It's a challenge to know where this data is stored and what controls are already in place to protect it. On top of that, ongoing risk assessments require that those controls be tested routinely. The challenge is further compounded by the complexity of the organizations in terms of the geographic distribution of offices, data centers and business units, the state of ongoing mergers and acquisitions, and the data-intensive business processes.

Tripwire solutions provide IT security and compliance automation to deliver intelligent change event management, enforce standards and policies, and remediate non-compliant configurations to protect valuable and sensitive data. Our comprehensive solutions help maintain a secure IT system by:

- Generating out-of-the-box policies for critical regulations and standards such as PCI, SOX, GLBA, FFIEC and SAS70.
- Continuously addressing vulnerabilities one-by-one across the data center and virtual environments until the organization moves into a known and trusted state.
- Providing dynamic change intelligence to prioritize changes or events of interest that cause you to drift out of compliance with built-in, real-time configuration control.
- Instantly alerting you to all changes or suspicious events that could take you out of compliance.
- Securely recording and generating reports representing current, historical and trend analysis of IT configuration changes and log events to enable audit preparedness.
- Automating the repair of configurations that have fallen out of compliance and returning them to a secure and compliant state.

tripwire ENTERPRISE

tripwire LOG CENTER

©2010 Tripwire, Inc. | 101 SW Main St., Ste. 1500 | Portland, OR 97204 | Main: 503.276.7500 | www.tripwire.com

Tripwire is a leading global provider of IT security and compliance automation solutions that help businesses and government agencies take control of their entire IT infrastructure. Thousands of customers rely on Tripwire's integrated solutions to help protect sensitive data, prove compliance and prevent outages. Tripwire® VIA™, the comprehensive suite of industry-leading file integrity, policy compliance and log and security event management solutions, is the way organizations can proactively achieve continuous compliance, mitigate risk and improve operational control through Visibility, Intelligence and Automation.

Learn more at www.tripwire.com and @TripwireInc on Twitter.

Thawte is a leading global Certification Authority. Our SSL and code signing digital certificates are used globally to secure servers, provide data encryption, authenticate users, protect privacy and assure online identifies through stringent authentication and verification processes. Our SSL certificates include Wildcard SSL Certificates, SGC SuperCerts and Extended Validation SSL Certificates.

Learn more at www.thawte.com

Masthead

EDITORIAL
EDITOR-IN-CHIEF Illena Armstrong
illena.armstrong@haymarketmedia.com
DEPUTY EDITOR Dan Kaplan
dan.kaplan@haymarketmedia.com
MANAGING EDITOR Greg Masters
greg.masters@haymarketmedia.com
DESIGN AND PRODUCTION
ART DIRECTOR Brian Jackson
brian.jackson@haymarketmedia.com
SENIOR PRODUCTION Krassi Varbanov
krassi.varbanov@haymarketmedia.com

U.S. SALES
ASSOCIATE PUBLISHER, VP OF SALES Gill Torren
(646) 638-6008 *gill.torren@haymarketmedia.com*
EASTERN REGION SALES MANAGER Mike Shemesh
(646) 638-6016 *mike.shemesh@haymarketmedia.com*
WESTERN REGION SALES MANAGER Matthew Allington
(415) 346-6460 *matthew.allington@haymarketmedia.com*
NATIONAL INSIDE SALES EXECUTIVE Brittany Thompson
(646) 638-6152 *brittany.thompson@haymarketmedia.com*