TECHGUIDE

SIM

A global look at security information and event management systems

TechTarget®

SIM ROAD MAP

CASE STUDY

CLOUD SERVICES

BUSINESS OF SIM

Some CISOs Consider Ripping Out or Augmenting Outdated SIEM Systems

Outdated SIEM systems were difficult to deploy and costly to maintain, according to one expert. Today, CISOs are considering highly integrated, lightweight systems with more automation. **BY ROBERT WESTERVELT**

ENTERPRISES WITH OLDER security information event management (SIEM) systems are taking a second look at their hardware, according to experts, and in some cases, businesses are mulling over whether to augment SIEM systems with additional tools, or rip-and-replace systems altogether.

Gregg Woodcock of communications services provider MetroPCS Wireless Inc., sees log correlation and analysis as an integral part of running an efficient and secure business.

In fact, the Dallas-based software engineer sees so much value in correlating and analyzing logs, he founded and chairs a Dallas-based user group devoted to Splunk, a search tool that can take in many types of log data, from customer transactions to network activity, and call-record data, correlate it, and analyze it to discover valuable intelligence. The tool has become so popular, according to Woodcock, that many of the members of the Splunk user group are at organizations that have security information and event management (SIEM) systems in place, but want to use Splunk as a Google-type search bar to augment them.

MetroPCS used Splunk to monitor for terms-of-service violators of its free international phone calling plan. Woodcock said users were instantly able to see where traffic was going and how much it was costing the company. People violating the terms of service for using the free international calling for business use, were detected quickly from the call log data and were cut off before expenses got out of control, Woodcock said.

"The amazing thing is the speed at which it can do the things it does and the insight it provides to everyone who uses it," Woodcock said. "It is in essence, Google for your logs; it ingests them in real-time and time stamps them and then it allows you to do just about anything with it using a UNIX-like set of search commands."

Splunk added support for security monitoring in 2010. It can also generate alerts in real time. The fact that it is being used by hundreds of people to augment existing SIEM systems is a sign that many early SIEM deployments were either too complicated to configure correctly, or had too many constraints to get valuable intelligence from the system, Woodcock said. "With Splunk, you dump data in and impose ad hoc schemas on the data that may only be useful to you and go from sorting to search and it's a radical change," he said. "With many other products you have to do development to have a data schema that you can use."

Early SIEM implementations were cumbersome to deploy and took two to three years in some cases.

Currently, most SIEM systems are set up for their compliance and reporting capabilities, and many continue to be deployed to meet that minimum use case, said Bill Sieglein, CEO at the CISO Executive Network. Sieglein recently completed a series of roundtable sessions with Fortune 1000 CISOs on security operations, including log management and SIEM. He said many CISOs are wondering whether or not to rip and replace their outdated SIEM systems with newer SIEM technology to create an intelligence platform.

"In almost every case, the implementations were longer and more expensive than they originally anticipated," Sieglein said. "They are right now trying to justify the continued license renewal to get more value out of it for the purposes of risk management and situational awareness."

Early SIEM implementations were cumbersome to deploy and took two to three years in some cases with three quarters of the cost going to professional services for deployment assistance, Sieglein said. Today, more lightweight systems are being considered—SIEM platforms from McAfee (NitroSecurity),

SIM ROAD MAP

CASE STUDY

CLOUD SERVICES

BUSINESS OF SIM

IBM (Q1 Labs) and LogRhythm, which promise faster implementations and more out-of-the-box automation, Sieglein said.

For organizations that made a substantial investment in SIEM, many are sharing stories about how difficult the journey has been, Sieglein said. For businesses dedicated to reviewing logs, it took a large number of staff to not only watch for events but also to manage the system so it isn't overwhelmed by the log data. The system had to be kept fully patched and someone needed to understand how to do specialized reporting in order to get value out of the system.

The focus now is to better manage the data sources and automate the analysis.

"There were complaints that SIEM 1.0 requires a lot of babysitting just from a systems perspective," Sieglein said. "It didn't allow for resources to be dedicated to staring at the glass and watching events. Now SIEM 2.0 promises faster implementation, a lot less system management where resources and time can be dedicated to using the analytics and actually taking action based on the types of alerts that they are seeing."

Chris Petersen, co-founder and CTO of LogRhythm agrees that early implementations were sometimes nightmarish to deploy and maintain, and often were left running in a poorly configured state to meet a specific compliance mandate.

SIEM was initially designed to solve the massive amounts of data generated by intrusion defense systems by trimming the IDS data down to something that was more manageable and actionable, Petersen said. SIEM vendors made it more complicated by adding a fuller spectrum of log data from the network layer, the device layer and the application and database layers. The focus now is to better manage the data sources and automate the analysis. "The goal today is to detect a broader class of events from insider threats, sophisticated intrusions and deeply embedded breaches by making that forensic layer immediately accessible," Petersen said.

SIEM vendors have learned that it's not feasible to expect companies to do

SIM ROAD MAP

CASE STUDY

CLOUD SERVICES

BUSINESS OF SIM

manual log analysis, he said. “Nobody has the perfect solution; these are complex problems,” Petersen said. “What we do have today is more information to look at than we’ve ever had before. If we can analyze it correctly and creatively via different techniques…we put the intelligence into the system to point customers to places to go investigate and have a thorough experience to quickly arrive at a conclusion and course of action.”

The late Eugene Schultz, a noted network security expert, warned in 2009 that SIEM vendors needed to address the complexity of installing SIEM. Schultz, a strong believer in the merits of SIEM technology, said “the availability of good technology is by no means any guarantee that people will buy it.” Most SIEM products require months of tuning after the initial installation, he wrote in a blog entry on why the SIEM market isn’t doing better. “One well-selling SIEM tool can require the installation and maintenance of four separate machines on the network and has so many functions that many levels of menu traversal are required to get to some of the most basic functions. Troubleshooting SIEM tools is generally no picnic, either,” he wrote.

Organizations considering a broad SIEM deployment need to have the ability to conduct a robust test and evaluation process of SIEM products.

Organizations considering a broad SIEM deployment need to have the ability to conduct a robust test and evaluation process of SIEM products, said Bill Bradd, assistant division chief for the Office of Technical Security of Information Security at the U.S. Census Bureau. It’s an investment in technology, but also people knowledgeable in maintaining and monitoring the system, Bradd said.

The U.S. Census Bureau has been building out the capabilities of its Sensage SIEM system from collecting about 150 systems about five years ago when the scope was primarily regulatory compliance to more than 2,800 network devices and servers today as part of a broader information security strategy. That meant acquiring new hardware to handle the massive amounts of log data,

SIM ROAD MAP

CASE STUDY

CLOUD SERVICES

BUSINESS OF SIM

working with system owners to feed the data into the SIEM system, and a development team to create scripts to take in and parse the various system logs, Bradd said. The SIEM system can audit system log data from Unix and Linux servers, Windows event logs, network firewalls and routers and switches.

“The volume of data is always a concern,” Bradd said adding that tuning is always an issue, but that the Census Bureau was able to get it under control. “If you know you’ve got an application that is going to generate a certain kind of alert, it’s not a difficult process to tune that out.”

Bradd said the Census Bureau also plans to send alerts to system owners so a network engineer in charge of maintaining routers and switches can investigate an alert and report back within 72 hours whether it is an event that can be remediated internally or if it is a serious security problem that requires reporting and a full investigation. The built-out system has been used to find misconfiguration issues and detect malware infected machines and trace the malicious code back to the site the user visited, Bradd said. From server perspective, the Census Bureau is monitoring individual user activity to determine if an attacker is conducting a brute-force password attack on an employee account or if an employee has simply forgotten their password.

> *“To get something out of a tool, you have to invest time and effort into people.”*
>
> **—BILL BRADD**
> assistant division chief,
> U.S. Census Bureau

“To get something out of a tool, you have to invest time and effort into people,” Bradd said.

There are signs that vendors have addressed some of the problems with earlier releases. The experience has been fairly smooth for one Canadian firm that deployed a newer LogRhythm system in February 2011. The firm, Cara Operations Ltd., which operates 650 restaurants, mostly corporate and franchise locations, deployed the SIEM system to monitor its payment systems for PCI DSS compliance. “We know it’s capable of doing more than PCI compliance, but ultimately PCI was behind the decision to move forward with it,” said Rik

SIM ROAD MAP

CASE STUDY

CLOUD SERVICES

BUSINESS OF SIM

Steven, project manager information technology at Cara.

The company uses a managed security services provider (MSSP) to monitor the system and handle alerts. While the MSSP monitors the system 24 hours a day, an IT professional within Cara is acting as a threat analyst to monitor the system internally. Restaurants span across five time zones, so the use of the MSSP was much needed, Steven said.

A team rolled out the system in about two months, deploying software agents at the company's various locations. At first there was too much information and Steven said the company had to do some tuning over several months to "dial-back" and focus only on the compliance. "It's easy to get overwhelmed with the fact that it tells you so much information," Steven said.

> *"It's easy to get overwhelmed with the fact that it tells you so much information."*
>
> **—RIK STEVEN,** project manager information technology, Cara

The plan is to expand the system overtime to generate more reports and use newer features that can proactively address problems it identifies, Steven said.

"It's been a big investment to get this in so we want to make sure we get our money's worth out of it," Steven said. "There's a great deal of information it can tell us and we've only scratched the surface on the reporting that can come out of it even with just the basic canned reports." ■

SIEM Deployment Shows Patience Is Required

Williams Lea's SIEM is already helping reduce manual log reviews. But there's still a lot of work to be done before the SIEM can be fully deployed. **BY RON CONDON**

SIM ROAD MAP

CASE STUDY

CLOUD SERVICES

BUSINESS OF SIM

THERE IS A lot of pressure on organisations these days to make better use of their system logs. Logs help ward off dangers by offering real-time alerts, they provide system troubleshooting or forensic evidence after a security breach, and many compliance standards insist that logs be kept and managed.

Yet many organisations fail to use logs effectively. As the recently published Verizon Data Breach Investigations Report showed, only 8% of breaches are discovered by the victim organisation itself, an indicator of missed opportunities to more promptly and thoroughly analyse log data to identify malicious activity on their networks.

Why is this happening? The short answer is log management is hard to do, according to Andrew Allison, information security manager at business process outsourcing company Williams Lea. Employing a security information and event management (SIEM) system can help immensely, but it can take a lot of time and effort to get the SIEM working effectively, Allison said.

EARLY STAGES OF SIEM IMPLEMENTATION

Allison joined London-based Williams Lea nine months ago. As the information security manager, Allison immediately set about choosing a security and incident event management (SIEM) system to help take control of log management. He took an objective view of the full range of products and services available across the market with a goal of selecting the best-in-class based on defined requirements. After a four-month process, he selected LogRhythm because the company bundled in a file integrity module (FIM) without extra charge. The FIM helps ensure configuration files are protected and files at rest are not tampered with.

The SIEM deployment began in December, but full implementation won't be complete for several months. "People think that by installing SIEM it will fix everything, but no, there is a lot of work involved to ensure it works effectively," Allison said.

His company's network supports around 2,500 users, many of whom are often out of the office or working remotely. The business also has a steady staff turnover since contractors are hired for certain projects and work in offices throughout the UK. This means one of Allison's biggest challenges is managing privileges and access rights of employees and making sure rights are withdrawn when people leave the company.

The FIM helps ensure configuration files are protected and files at rest are not tampered with.

In the past, this was accomplished by going through the logs manually. Logs were written first to local and then to remote back-end drives where they were kept mainly for archiving purposes.

"We'd usually only look at the logs when there was an issue. And we would also take random samples to check for failed logins on the FTP servers, for example," Allison said.

BENEFITS FROM THE SIEM

Williams Lea's SIEM system is already helping alleviate some of the manual log review work by generating reports on unused Active Directory accounts and failed login events. It has also helped to take control of users with admin rights, and to address the issue of generic login credentials.

However, there's a long way to go before the organisation can get full value from the SIEM, Allison said. Even with a top-of-the-range LogRhythm appli-

SIM ROAD MAP

CASE STUDY

CLOUD SERVICES

BUSINESS OF SIM

ance with 3.99 terabytes of disk space, and another for failover, he said the systems could soon be overwhelmed if each network device is not tuned properly. For example, his Juniper edge firewalls are currently clocking 80 events every second. Allison said that with better configuration, that figure can be reduced. Another perennial problem is developers who set devices to debug mode and then fail to switch them back, leaving them to spew out unneeded event logs.

"I used another SIEM product at my last company and we had the same issue," Allison said. "If you just put in a SIEM and let it run, you can run out of disk space very quickly if you haven't tuned the devices on the network. It takes a lot of time to do that. We installed our SIEM three months ago and we are still only a third of the way through the process."

When fully configured, the SIEM will be able to create alerts by sending SMS messages or emails to the appropriate person as soon as a problem occurs.

FUTURE SIEM PLANS

Once that process is complete, there will still be other jobs to do. For example, the company's intrusion prevention system (IPS) logs do not yet feed into the SIEM, although that's part of the long-term plan.

"We can't handle that at the moment because of the sheer amount of data the SIEM logs," Allison said. "We have one guy who spends four or five hours a week tuning and tweaking the SIEM, getting rid of false positives."

Similarly, when fully configured, the SIEM will be able to create alerts by sending SMS messages or emails to the appropriate person as soon as a problem occurs. But as Allison said, every alert condition first has to be defined and documented.

"You have to go through all the rules and make decisions about what you do and don't want to trigger an event, and that takes a lot of time," he said. "Then each rule has to be written into your policy, with the reasons for doing it, so someone else can see why a decision was made, especially if you get a breach."

SIM ROAD MAP

CASE STUDY

CLOUD SERVICES

BUSINESS OF SIM

Allison has no doubt that once all this essential groundwork is done, the job of managing the network will be considerably easier and less labour-intensive. The process of base lining the network using the SIEM system has also been very revealing, he said, and it is helping to throttle back the number of events generated by each device without damaging security.

In addition, the SIEM will help the company demonstrate compliance with a range of standards, including PCI DSS and ISO 27001. However, as Allison said, compliance should be a natural by-product of adopting security best practices.

"Any good information security person will want to know what's going on in their network," he said. "SIEM can help provide the visibility you need. It is a very powerful and useful tool, but it's not a silver bullet. You still need to do the work." ■

More Companies Eyeing SIEM in the Cloud

A cloud service can help companies get around some hurdles with SIEM systems. **BY ROBERT LEMOS**

SIM ROAD MAP

CASE STUDY

CLOUD SERVICES

BUSINESS OF SIM

COMPLIANCE REQUIREMENTS AND growing concerns over more targeted and sophisticated attacks have boosted interest in security information and event management systems. However, the complexity and cost associated with SIEMs have organizations looking to SIEM in the cloud as a way to overcome those challenges.

While companies need to have a greater ability to monitor their systems and generate compliance reports to meet regulatory requirements, SIEM systems are typically expensive to deploy and complex to operate and manage. No wonder larger enterprises have been the core adopters of the information security systems. Midsized companies and small businesses have not had the technical skills to broadly deploy SIEM internally, said Jon Oltsik, principal analyst with the Enterprise Strategy Group.

Turning security information and event management into a cloud service allows small and midsized companies to avail themselves of the benefits of the systems, he said.

“It is typical that companies go from manual log analysis, to log management, to SIEM,” Oltsik said. “Typically, when you cross that bridge to SIEM, you are getting to a sophisticated and complex product—cloud can simplify that.”

STREAMLINING SIEM VIA THE CLOUD

SIEM systems combine security information management capabilities to collect logs and report on compliance with security event management capabilities to collect security-related events and analyze them to detect potential

SIM ROAD MAP

CASE STUDY

CLOUD SERVICES

BUSINESS OF SIM

attacks. While compliance has traditionally driven SIEM adoption, concerns over advanced threats has become a stronger incentive to purchase the systems, according to analyst firm Frost & Sullivan, which predicts the worldwide market for SIEM systems will grow to $1.3 billion in 2015, up from $680 million in 2009.

Due to the relative complexity and expense of SIEM systems from major players such as HP, RSA, the Security Division of EMC and Q1 Labs, smaller businesses typically use managed security service providers that have SIEM capabilities built in. Yet a number of startups are also aiming to fill the gap in the SMB market. Companies like Alert Logic Inc. and Sumo Logic Inc. are attempting to provide the benefits of a well managed SIEM system with the simplicity of the cloud.

While compliance has traditionally driven SIEM adoption, concerns over advanced threats have become a stronger incentive to purchase the systems.

Houston-based Alert Logic, for example, deploys sensors into the customer's network to collect log and event data, but shifts the operations and management to the cloud, said Urvish Vashi, vice president of marketing at the vendor.

"The heavy lifting—the data correlation and analysis—happens in the cloud," he said.

Smaller businesses are not the only ones that can benefit from cloud, added Vab Goel, the founder and former CEO of Virtela Technology Services Inc., a Greenwood Village, Colo.-based network and security management provider. Larger enterprises stand to save significantly by allowing a cloud provider to manage their security information infrastructure, he said.

"Most of the time, enterprises are trying to do it themselves, and they are finding that is taking too much time and is too complex," he said. "When they are global—and 50% of revenue is outside of America—you need staff that is online 24/7."

SIM ROAD MAP

CASE STUDY

CLOUD SERVICES

BUSINESS OF SIM

SIEM IN THE CLOUD HAS ITS OWN ISSUES

However, cloud providers have to do more to assuage the security concerns of potential customers. Turning over internal security data to a cloud provider requires trust, and nearly half of all users of cloud services desire more clarity on providers' security precautions, according to Gartner.

Another problem with pushing SIEM into the cloud is that targeted attack detection requires in-depth knowledge of internal systems, the kind found in corporate security teams. Cloud-based SIEM services may have trouble with recognizing the low-and-slow attacks, said Mark Nicolett, vice president with research firm Gartner.

> *Cloud-based SIEM services may have trouble with recognizing the low-and-slow attacks.*

In targeted attacks, "90% of the time that organizations were breached, attackers created only a relatively small amount of activity," he said. "To see that evidence, you need to know the environment. Cloud services may not be able to do that." ■

India Inc Guns for SIEM Tools as Maturity, Viability Drive Growth

SIEM tool adoption in India is on the rise, on the wings of growth in the demand for SIEM systems. BY VARUN HARAN

SIM ROAD MAP

CASE STUDY

CLOUD SERVICES

BUSINESS OF SIM

THE SECURITY INFORMATION and event management (SIEM) tool is one of the lynchpins of a robust security framework for many Indian organizations. While these solutions have been around for a long time, increasing maturity of solutions, aided by compliance and regulatory requirements is finally resulting in an increasing number of Indian organizations getting on to the SIEM bandwagon.

Earlier, it took considerable technical expertise from an organization's part to implement and manage SIEM tools—lengthy sales and training cycles added to the adoption woes. As a result, the cost and effort that went into this exercise could not be justified for most businesses. In recent times, trends like the availability of SIEM tools as managed security services is putting them within the grasp of organizations.

DRIVERS OF THE INDIAN SIEM CART

Over the last two years, regulatory drivers have played a major role towards SIEM adoption in India. Measures mandated by the Unified Access Service License (UASL) security amendments in the telecom sector and the Reserve Bank of India (RBI) guidelines for the banking vertical, have spurred growth in the SIEM market. Organizational push towards initiatives like ISO 27001 certification, as well as compliance requirements like HIPAA, PCI DSS and GRC initiatives has also contributed to the demand.

As A R Vijay Kumar, the VP and global information security leader at Indian BP major Genpact points out, SIEM tools are critical for organizations because of the constantly evolving threat landscape. With cyber threats like advanced persistent threats (APT) and botnets, organizations are starting to rely on the in-depth analysis mechanisms provided by SIEM tools. “An SIEM tool helps when it comes to understanding the root cause of an incident better and faster,” said Satish Das, the chief security officer and VP (Enterprise Risk Management) at Cognizant.

In addition to businesses that opt for SIEM tools to meet their regulatory requirements, many organizations have now matured to a level where they require an SIEM tool, said Sumeet Singh, a security consultant and SIEM expert. Kumar agrees on this front, as he points out that maturity levels have gone up—at the organizational as well as for SIEM solutions.

Cognizant and Genpact have been using SIEM tools for many years, given the high level of technical expertise available in-house—since 2002 and 2004, respectively. Cognizant has its home-bred SIEM tool based on open source frameworks, as well as a commercial off-the-shelf product acquired two years ago. However, Das takes a contrarian view as he opines that the market for SIEM products is set to decline with the advent of cloud computing and managed services.

INDIA INC’S VIEW OF SIEM

Many Indian companies look at SIEM tools as a point-in-time solution, even as the global focus is on deriving business value from these solutions. Since SIEM tools can be expensive, Indian organizations still need to determine how it can contribute to the business in ROI terms. As a result of this expectation mismatch, large scale SIEM adoption is still at a nascent stage.

Different industry verticals approach SIEM requirements in their own ways. Large PSU banks which typically tend to be conservative go for captive security operation centers (SOC) with in-house expertise to manage SIEM tools for complete control. “Until two years ago, people didn’t have much confidence in Indian managed service providers for SIEM, since they were not able to cater to volumes, or weren’t as dependable,” said Singh.

SIM ROAD MAP

CASE STUDY

CLOUD SERVICES

BUSINESS OF SIM

It must be mentioned at this point that many Indian companies seem comfortable outsourcing SIEM tool implementation and operation to managed service providers (MSP). Outsourcing is the trend in verticals like IT/ITES and telecom, since it is difficult to build all capabilities required to manage complex SIEM tools in-house. There is a shift in the way SIEM tool implementation is approached in India, with focus on SLA-based delivery rather than reliance on in-house expertise.

A case in point is Axis Bank, one of India's largest private banks, which uses ArcSight as its SIEM product. The SIEM tool is run out of a remote SOC managed by Paladion, the bank's managed security provider (MSP). The MSP owns SIEM licenses and manages the 24x7 operation. "It is better to outsource a specialized function because it is difficult to acquire and upgrade in-house skills to keep pace with the constantly evolving threat landscape," said Nabankur Sen, the CISO of Axis Bank. Sen prefers to depend on domain experts for such critical functions. Another advantage of going for an MSP is the basket of services. Axis benefits from add-on services like phishing monitoring, log referral and watermarking, which accompanies the bank's three year SLA with Paladion.

Outsourcing is the trend in verticals like IT/ITES and telecom, since it is difficult to build all capabilities required to manage complex SIEM tools in-house.

Post SIEM tool implementation, analysis and monitoring at Axis have become comprehensive and structured, with daily reports. The situational awareness brought by this solution helps Sen assure the business in a tangible manner, when it comes to the bank's infosec posture. "Whether in-house or outsourced, log analysis is a critical function that everybody has to implement—the sooner, the better," said Sen.

From the governance perspective, Indian companies are seeing benefits from implementing SIEM tools. These include gains like accountability, better incident and fraud handling, forensic capabilities, non-repudiation, and calcula-

SIM ROAD MAP

CASE STUDY

CLOUD SERVICES

BUSINESS OF SIM

tion of essential security metrics. “For an organization like Genpact, dealing with multiple compliance requirements, maintaining different frameworks and managing audits requirements will be impossible without SIEM tools,” said Kumar.

WHAT INDIAN COMPANIES WANT FROM SIEM

The requirements from SIEM solutions across Indian industry segments aggregate around ease of integration and autonomous detection of anomalies. Autonomous detection will reduce manpower involvement and decrease reaction time. The next SIEM trend is toward tighter integration of SIEM tools with technologies like workflow management and data loss prevention (DLP). While an SIEM solution was just another bullet item in the security space earlier, it is now moving to focal point for the integration of other security tools.

According to Singh, most vendors still think of requirements as product features, and fail to understand the requirements of an SIEM tool from an organizational perspective. This creates bottlenecks for practitioners like Kumar who expect consolidation and simplification of SIEM tools for easier implementation and maintenance. On this front, Kumar cites the example of how Genpact has to deal with separate clients for different OS platforms. Rather than have third-party add-ons, Kumar requires converged solutions focusing on usability.

At the moment, many Indian organizations approach SIEM as a product, and this needs to change. Organizations today need to start looking at an SIEM tool as a solution for monitoring, accountability and proactive incident monitoring. Many Indian companies have now begun performing quality assessments of their SIEM environments as a result of this realization. This is essential to get a business return on SIEM investments. ■

SIM ROAD MAP

CASE STUDY

CLOUD SERVICES

BUSINESS OF SIM

***Robert Westervelt** is the news director for TechTarget's Security Media Group.*

***Ron Condon** is TechTarget's Security Media Group UK bureau chief.*

***Robert Lemos** is an award-winning technology journalist, who has reported on computer security and cybercrime for 15 years. He currently writes for several technology publications.*

***Varun Haran** contributes to SearchSecurity.in and SearchDataCenter.in. He holds a bachelor's degree in economics and a post graduate diploma in journalism from ACJ, Chennai.*

TechTarget®

This Technical Guide on SIM is a SearchSecurity.com e-publication.

Michael S. Mimoso
Editorial Director

Eric Parizo
Senior Site Editor

Robert Westervelt
News Director

Marcia Savage
Site Editor

Ron Condon
UK Bureau Chief

Kara Gattine
Senior Managing Editor

Doug Olender
Vice President/Group Publisher
dolender@techtarget.com

Peter Larkin
Associate Publisher
plarkin@techtarget.com

TechTarget
275 Grove Street, Newton, MA 02466
www.techtarget.com

About TechTarget: TechTarget publishes media for information technology professionals. More than 100 focused websites enable quick access to a deep store of news, advice and analysis about the technologies, products and processes crucial to your job. Our live and virtual events give you direct access to independent expert commentary and advice. At IT Knowledge Exchange, our social community, you can get advice and share solutions with peers and experts.