SC MAGAZINE Security Brief

Nearly two-third of respondents to a new SC Magazine survey said they were in the process of implementing security analytics.

Analyze this!

Sponsored by

sas

Analyze this! Analytics for the midrange enterprise

Midsized firms are taking advantage of network analytics. Sometimes, however, they just call it something else. Jesse Staniforth reports.

Understanding security analytics can be a daunting job. It is more than just analyzing log files but it is less than a full-blown information security platform. In fact, according to Anton Chuvakin, research vice president for security and risk management at Gartner, it is not yet even a "market," but rather still just a "concept" that has yet to define best practices.

In a survey of 937 IT and security professionals conducted by *SC Magazine* in February, nearly two of three respondents were in the process of implementing security analytics – only 36 percent said they were not planning an analytics program. While that 36 percent remains a large number, it indicates a majority shift toward understanding the necessity of implementing analytics at a corporate level. Most respondents were at the planning stage rather than implementation: a combined 25 percent presently were implementing or have already implemented an analytics program, while a combined 40 percent were planning to implement such a program over the next six to 24 months.

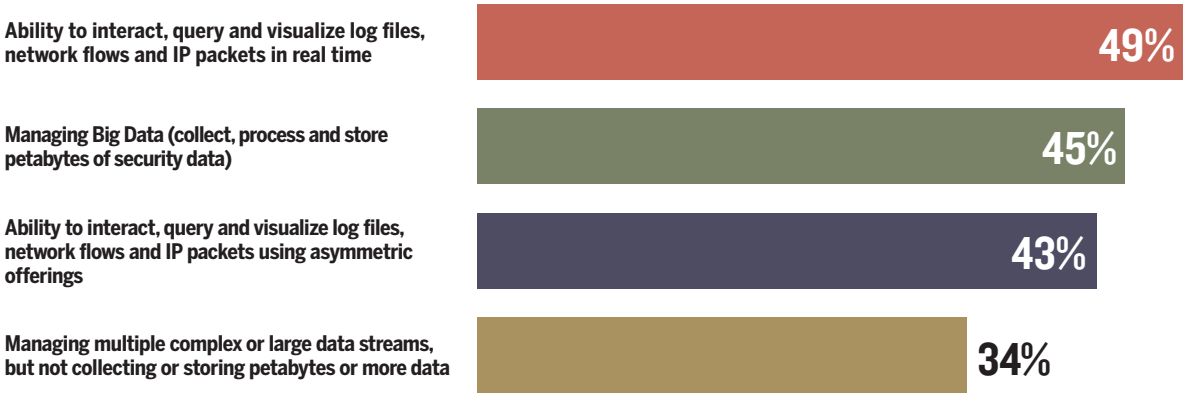
Curiously, while the survey generated nearly 1,000 responses, it ultimately represents smaller companies more densely than larger ones. Some 72 percent of those taking the survey were drawn from companies of 1,000 or fewer employees, 10 percent from companies with 1,001 to 5,000 employees, and 17 percent from companies with more than 5,001 employees. The demographics shift a bit when respondents are carved out by revenue size. Again, 70 percent had revenue of less than $100 million, while the remaining 30 percent was split almost evenly between firms with $100 million to one billion in revenue and $1 billion and more in revenue.

This slanting in the survey toward small- to mid-size enterprises (SMEs) was its own kind of good news; whereas security analytics have traditionally been the domain of larger industries, it's clear that the world of the SME is waking up to the merits of understanding its own network activity. However, that means these companies are entering into the same, wider debate about policies and procedures that has been ongoing for some time in large enterprises

31%

of survey respondents currently implementing analytics say they would like post-event security forensics and root-cause analysis.

How do you define security analytics?



Analyze this!

that generally have more mature and larger network security and IT departments with substantially larger budgets.

While network analytics is often considered an application for enterprises managing Big Data and feeding massive data flows into expensive and complex security information and event management (SIEM) applications, Chuvakin told attendees at the RSA Conference 2016 in San Francisco that while SIEM is common in analytics environments, it is not required. That bodes well for the smaller, less sophisticated enterprise without the budget or staff to manage, maintain and configure SIEMs.

Operational vs. strategic

When asked to distinguish whether operational analytics (those that explore specific network and events and detect emerging threats) or strategic analytics (those that enable you to assess your security performance over time and make policy or spending decisions) were more important, an overwhelming majority of respondents – 69 percent – say they value "both equally." However, in practice, respondents report a more pragmatic shift toward operational analytics – 69 percent of respondents' programs focus on operations versus only 31 percent of those that were strategic in their aims.

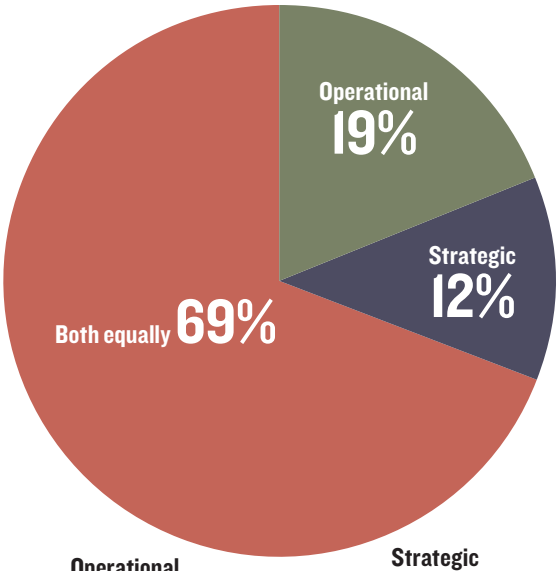
To Adam Ely, faculty member at Boston's Institute for Applied Network Security (IANS), those numbers seem inevitable. "I know there are so many companies where teams are just down in the weeds on a daily basis," Ely says. "They're trying to solve individual problems, trying to look at individual attacks or threats – that's really where they are on the maturity curve. So to see that degree of focus on the operational and the tactical, that makes a lot of sense."

> "Most security practitioners are focused on identifying and stopping threats."
>
> – Joseph Blankenship, senior analyst, Forrester

Many of these organizations don't have the staff, time and resources to step back and think about the larger picture, Ely says. They don't really have a security program management. "It's more 'we do security' rather than 'we plan the architecture of how we will be secure.'"

Joseph Blankenship, a senior analyst at Forrester serving security and risk professionals, concurs. "Most security practitioners are focused on identifying and stopping threats, so it follows that most respondents are using security analytics tools for that purpose," explains Blankenship. Security analytics tools overall do a pretty good job of reporting, he says, but could evolve by showing how the tools improve time to detection/remediation over time. "Shortening time to detection will allow security teams to reduce the

Which type of security analytics is most important to you?



26%

of those survey respondents currently implementing analytics say they would prioritize multi-layer analysis.

Analyze this!

impact of breaches," he explains. "Being able to visually demonstrate that capability will be extremely helpful for assessing performance and adjusting security strategy."

For Gartner's Chuvakin, the split is simply a matter of availability. "There are more operations since operations/tactical is easier," he says. "There are more tools that deal with details. Hence operational/tactical security analytics is more popular."

However, Adnan Amjad, a partner at Deloitte in Texas and leader of the firm's Vigilant Cyber Threat Management practice, says a focus on operational analytics comes at the cost of the quality of the data. "Operational analytics gives me the ability to go out and detect what's happening in my environment," Amjad says, "but the strategic stuff will allow me to predict and hunt. Operational analytics gives me atomic indicators: caches, IP addresses and so forth. The half-life of atomic indicators is fairly insignificant."

But, he adds, if he starts identifying tools, techniques and processes (TTPs) that attackers are using, that allows him to hunt and predict what's happening in his environment. "[In] most organizations, their analytics from a cyber perspective are still focused on indicators of compromise (IoCs) or atomic indicators, whereas they need to be focused on *TTPs*. Detecting [attackers] may not even mean anything. You really have to hunt them, predict where they're going to pop up and neutralize them in your environment."

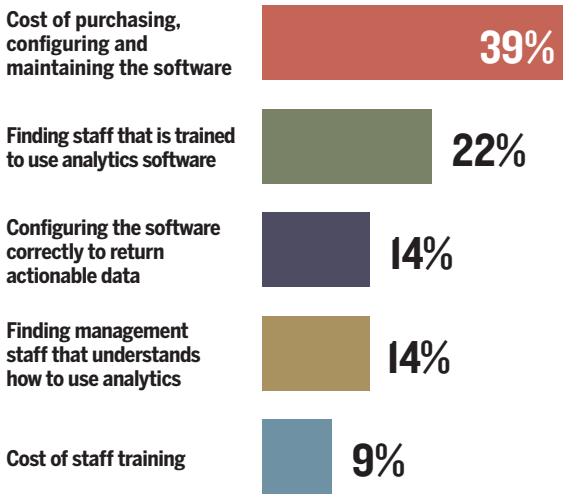
The wish list

Of those survey respondents currently implementing analytics, 31 percent say they would like post-event security forensics and root-cause analysis, 26 percent say they would prioritize multi-layer analysis, 25 percent want to add threat reporting and visualization, 11 percent want to be able to compare local data with cloud-based intelligence networks, while seven percent desire compliance reporting.

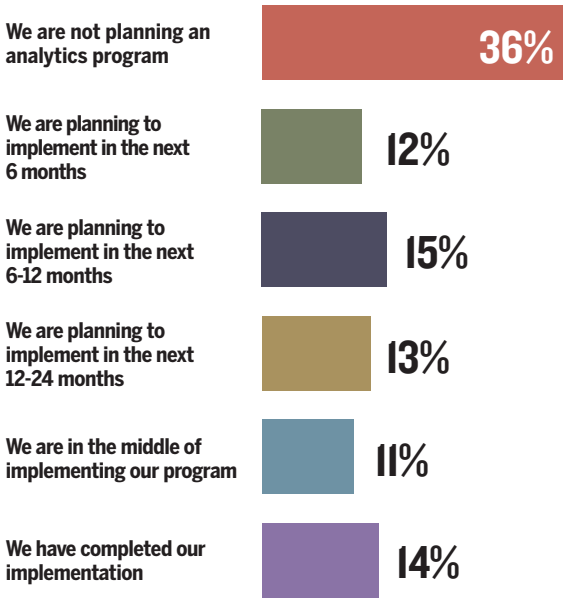
Most analysts agree that those who found their analytics software did not provide adequate post-event forensics, and root cause analysis might have a problem in the configuration of the software rather than in the software itself.

"In most cases," says Chuvakin, "the

What are the top three key challenges to implementing analytics?



At what stage are you in your security analytics program?



36%

of survey respondents placed external threats at the top of their list of short- and long-term security priorities.

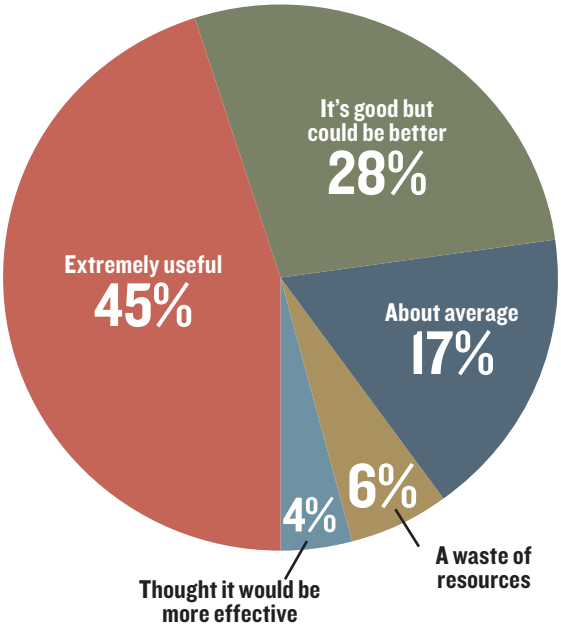
Analyze this!

software is not being used efficiently. There were unrealistic expectations or needed skilled resources are not available."

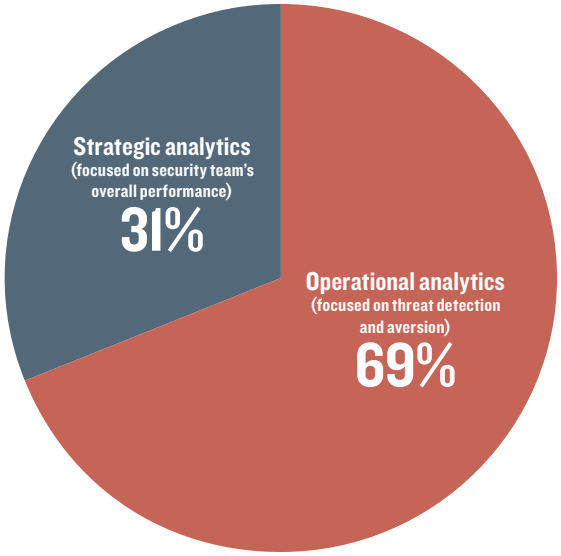
Knowing what data needs to be considered, Blankenship notes, is an important part of the process of getting value out of forensics/root cause analysis. "If users aren't getting the data they need, they should first examine the data sources they're taking in," he explains. "It's entirely possible that they aren't looking at the users and endpoints where a lot of the malicious activity takes place.

Most analytics tools, he says, now provide flexible searching and fairly robust event information for forensics use. Of course, these tools are only as good as the data

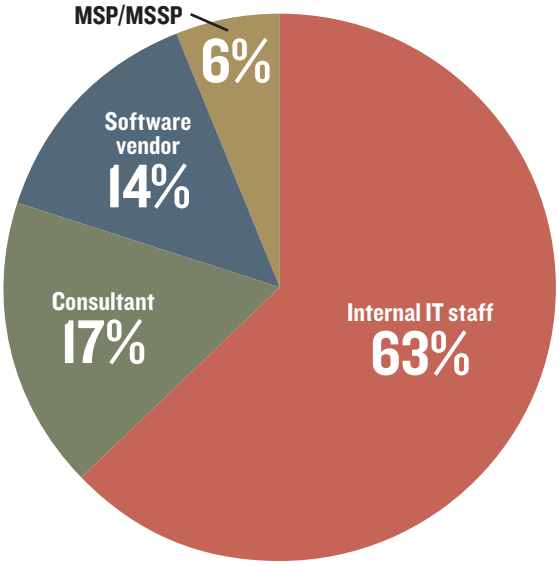
How effective is your analytics implementation?



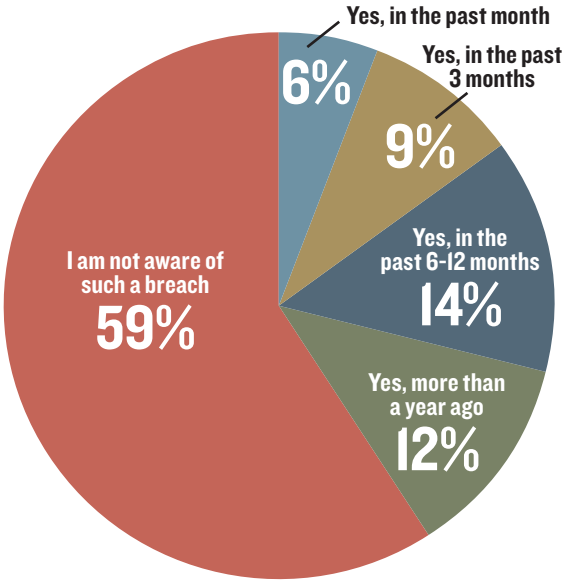
What did your analytics program focus on?



Who configured your analytics software?



Are you aware of any cybersecurity breaches within your organization?



22%

of respondents with revenue greater than $1 billion have fully implemented security analytics.

Analyze this!

they're receiving.

That's easy enough to say, but a far harder thing to put into practice, says Mike Spanbauer, NSS Labs vice president of security, test and advisory. "It would be a very savvy and capable organization to actually grab all [these data sources]," Spanbauer says, "because of the operational complexity and the encumbrance of the labor involved. Each one of these is a fair multiplier. With every level added you potentially introduce an extra level of logic – a nesting that just demands more talent, or at least a different mindset and approach, and certainly more science around stitching these together."

At the same time, says Amjad, limited human resources make a big difference in how teams can make the most of their analytics systems and results. "What's lacking in most cases are the people," he explains. "I don't necessarily mean people with the right skills. It's 'How much time can I get?' Today the way most of these analytics programs are set up, there's so much information coming every single day that your level one [analyst] is getting bombarded, but even your level two and level three analysts are still getting so much information that they're focused on a bunch of false positives they're trying to get out of the way."

While Amjad notes that the advent of cognitive computing likely will shift the workload of level one analysts away from more predictable tasks that can be automated, the process of sifting through false-positives is a reality for the time being.

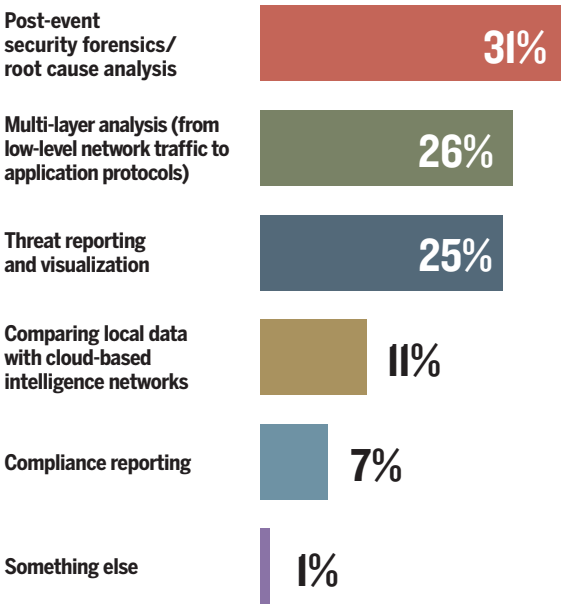
However, notes Christopher Burgess, CEO at Prevendra, there are certain measures of worth in analytics packages. "If your analytic packages cannot trace the route of the visiting packet as it comes into your network, it might be time to upgrade," Burgess says. "If your analytic package can't work with disparate data sets – such as network login, application login and data base login and tell you if the same IP address was used on all three or if the same IP address but different users were used on one of the three – then you might want to upgrade. If your analytic package can't trigger automated actions – or reactions – according to easily understandable and configurable rules, then it might be time to upgrade. This is not rocket science, but it is close."

Getting priorities straight

In ranking their top short-term and long-term security priorities, respondents placed external and unknown threats high on the list at 36 percent and 16 percent, respectively, for short-term priorities, and 29 percent and 31 percent, respectively, for long-term priorities. By contrast, internal threats were ranked far lower (nine percent in the short-term and 11 percent in the long-term), as were known threats (12 percent in the short-term and 10 percent in the long-term). While some analysts say these numbers were roughly what they expected, Ely believes they are predicated on the threat of the zero-day threat, which he argues is closer to myth than to reality.

"The fact is that most breaches happen based on some known

What would you like your analytics software to do that it currently doesn't?



69%

of respondents said that when given the choice, their enterprise's security analytics leaned more toward operational rather than strategic analytics.

Analyze this!

vulnerability," he says. "It's really interesting that there's all this talk about the unknown threat, the zero-day. But good, basic patch management and vulnerability analysis – these are indispensible [and] still the most highly valuable things that teams can do."

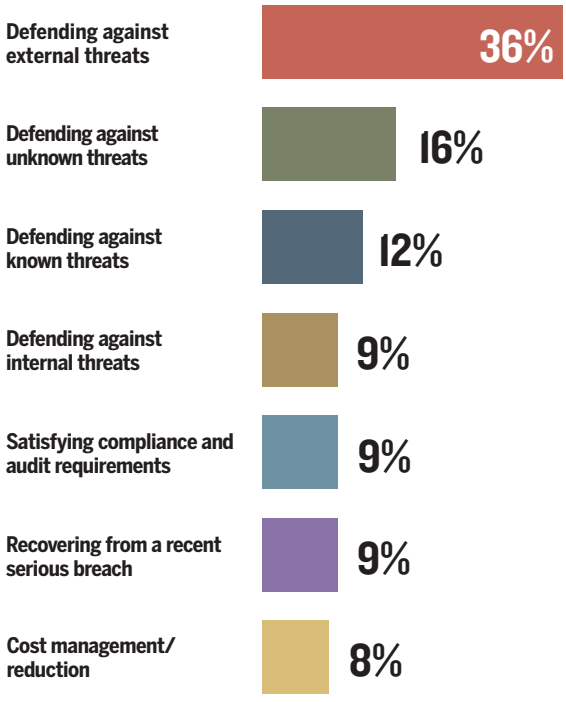
The survey unveiled that other analysts, meanwhile, were concerned about the relative lack of interest in internal threats. Blankenship warns that security teams need to be reassessing their areas of emphasis constantly. "Myopic focus on short-term priorities may also not bode well for security teams over the long haul," he says. "As threats evolve, security strategy and controls have to evolve along with them."

For that reason, Mike Weber, vice president of Denver-based Coalfire Labs, expresses alarm at the low interest in internal threats, which he says is the growing area of interest for those involved in penetration testing and vulnerability scanning. He says that his company is increasingly being asked to emulate internal threats in attempting to gain some form of entry, often by attacking internal individuals with phishing or social engineering.

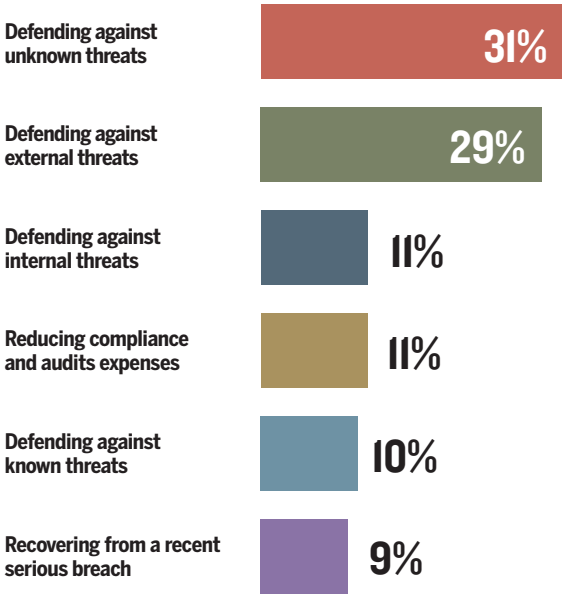
"Once they've got that level of access through that covert entry, attackers appear normal," Weber explains. "They don't set off any alarm bells; they look like what a normal user would look like so they blend into the regular traffic. The strike is after the covert entry, after they've gone quiet for a period of time and gotten access to your sensitive data to exfiltrate it. It can be a long period of time between those. There can be some tells that can be identified through correlation of data across

> "Once they've got that level of access through that covert entry, attackers appear normal."
>
> – Mike Weber, VP, Coalfire Labs

What is your top short-term security priority?



What is your top long-term security priority?



27%

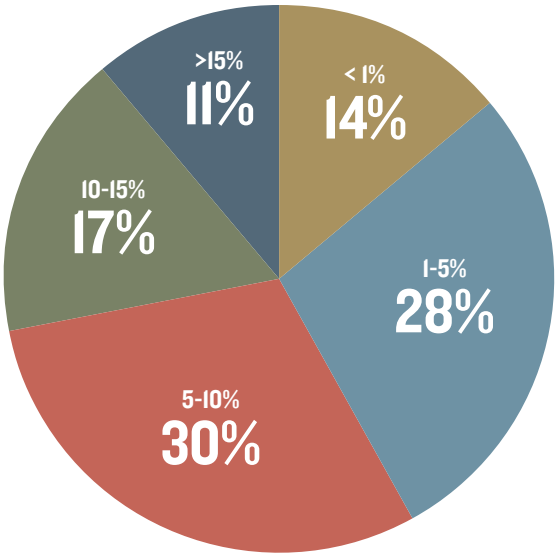
of respondents with revenue greater than $1 billion wanted their analytics software to do compliance reporting – significantly greater results than the other revenue categories.

Analyze this!

the enterprise, but most external hackers look like an internal threat right before they make their big exfiltration."

Security professionals recognize that many of those adopting analytics might feel uncertain about how to make sure their defenses are robust enough. "The best way to test a good analytics or security operations program is to emulate the threat," says Weber. "Not just tabletops. As you up the game and get to simulations and real response exercises, having those adversarial threats emulated through penetration testing or red-team type activities, with a definite goal in mind, and you perform those tests in a blind or double-blind manner, that can really tell you where your investment is paying off, both from the security analytics package and the team of responders that are going to do something with this data."

What proportion of your IT budget is spent on security?



IANS's Ely says that security should be undertaken no differently than developers test their code. "Developers write a piece of code," he says, "and then write a unit-test, which they test themselves and hand to QA, so with every build they run that unit-test and make sure each one of those things works. Not only that it works correctly, but that it also catches and handles the false cases that it's testing to the negative."

This kind of penetration testing, Ely notes, has been industry-standard in security for a long time, and can easily be applied to determining whether or not analytics are working well. "Did we detect the breach?," he asks. "Can we walk it backwards? How much data do we have here? Can we tell what they actually did? The pen test is a great scenario because we can actually talk to the real attacker, the pen tester, and walk through to figure out what we missed and didn't miss," he says.

Ely acknowledges that these testing schemes are expensive. However, he says they're worth it for those who can afford them. And for those who can't, he counsels running tools that should look like attacks.

"Use vulnerability scanning products and system management products that update files," he says. "Have people login from around the world who fail logins by utilizing the normal events that happen in the organization – maybe using them a little bit differently. There's a server and a file that has been changed. Did I see that? Could I detect that our file-management software changed this random file? Let me go replay that in the log as if that was an attack."

Getting past the fear factor

Complexities aside, now's the time for even smaller businesses to begin making analytics a part of their institutional structure, says Theodore Claypoole, an attorney and partner of Womble Carlyle's Intellectual Property Group in Charlotte, N.C. But that, he cautions, is a process that needs a structure of its own since newcomers might be able to derive some information about their performance from the numbers without being able to really grasp the benefits that analytics offer.

30%

of respondents said five to 10 percent of their IT budget is spent on security.

Analyze this!

"One of the things that I believe helps, especially if you're at an early stage, is to have an organization within your company that has a leader whose job it is to appropriately use analytics," explains Claypoole. In smaller companies, this could simply be one of several duties given to a manager. He says that person to whom this task would be delegated would have strategic, operational, administrative and financial knowledge and responsibilities.

This person would be tasked with figuring out how to make the entire organization run better and to explain the process and numbers – such as sales, inventory and other financial statistics – to other members of the team. Under the direction of this single manager, analytics can be used as a simple process, something that smaller organizations might need to think about only once a month, Claypoole notes.

"You sit down with the numbers that you have and you do a self-evaluation," he says.

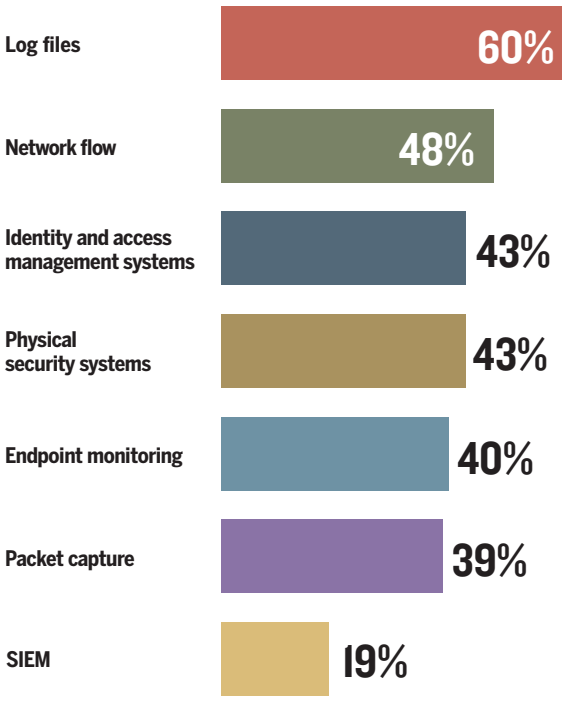
"And then you start looking at what more in additional numbers might make it interesting to you, and what tools are out there for a small business that might be able to do that. You can look at a different set of numbers or add in a different set of numbers every six months: sales numbers, inventory numbers, maybe just deeper numbers for the things you're looking at now."

Because analytics "sounds like something you shouldn't have to deal with as a small company," he encourages people to rename the process.

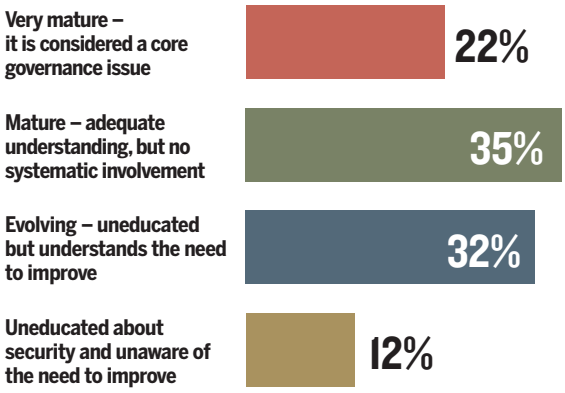
"Instead, call it something like 'self-evaluation.' That's really what you're doing: looking at the deeper levels of self-evaluation," says Claypoole. "That has to be something you should do every so often – take a look at your [data] and where you're going and determine how you might be able to get to the next step. Everybody does that from a financial standpoint, at least a little bit. All companies do. You wouldn't survive if you didn't know if you were making or losing money, what was making you money and what wasn't."

Further, Claypoole says companies should formalize the process of determining what's going on within the corporate network and visualizing data flows for potential breaches. "For small- and medium-sized businesses, analytics are not out of reach – and they're something you should be doing anyway. It's just that you call it self-analysis." ■

What data sources are available within your organization, should a security analytics program happen?



How would you describe the board's attitude to data security in your organization?



60%

of respondents said log files are the data source available within their organization should a security analytics program happen.

Masthead

EDITORIAL
VP, EDITORIAL Illena Armstrong
illena.armstrong@haymarketmedia.com
ASSOCIATE EDITOR Teri Robinson
teri.robinson@haymarketmedia.com
SPECIAL PROJECTS EDITOR Stephen Lawton
stephen.lawton@haymarketmedia.com
MANAGING EDITOR Greg Masters
greg.masters@haymarketmedia.com

DESIGN AND PRODUCTION
ART DIRECTOR Michael Strong
michael.strong@haymarketmedia.com
PRODUCTION MANAGER Brian Wask
brian.wask@haymarketmedia.com

SALES
VP, PUBLISHER David Steifman
(646) 638-6008 *david.steifman@haymarketmedia.com*
REGION SALES DIRECTOR Mike Shemesh
(646) 638-6016 *mike.shemesh@haymarketmedia.com*
WEST COAST SALES DIRECTOR Matthew Allington
(415) 346-6460 *matthew.allington@haymarketmedia.com*