THE 2012 SURVEY

GUARDING AGAINST A DATA

Conducted by

SC MAGAZINE

Sponsored by

HP Enterprise Security

SURVIVAL OF THE FITTEST

Budgets will be tight in 2012, but two-thirds of respondents to our survey believe they've got security covered. Illena Armstrong reports.

To evolve is to survive. It is a familiar scientific concept that can be encountered just as easily in business conversations over the water cooler as it can be in classic pieces of literature.

Its place in the information security industry is about as surprising as the enduringly humble budgets that still beleaguer most IT security departments. Despite these flat or, in some cases, still declining funds, evolving to survive and perhaps even prosper through modest profit growth remains a driving force for most organizations.

However, it also is a major motivator for others. As if in salute to this Darwinian supposition, regulators and, of course, cyber criminals continue to modify their plays to advance their own causes even further.

As uncovered in *SC Magazine's* fifth annual "Guarding Against a Data Breach" survey, IT security leaders and their executive bosses, meanwhile, are pushing ahead to take on a 2012 that promises still more of the advanced cyber attacks they saw last year, an increase in audits by compliance watchdogs, and a continuation of end-users and consumers relying on an array of vulnerable technologies to conduct business.

And all these things are happening just as most economic forecasters predict a drearier year than even they had imagined only a few months ago. A recent Federal Reserve Bank of Philadelphia survey reveals that the 45 forecasters queried only expect a 2.4 percent jump of GDP growth this year versus an earlier figure of 2.6 percent. The unemployment growth rate also became less rosy in a matter of months, falling from a previous estimate of 8.8 percent to 8.6 percent.

Show me the money

According to *SC*'s *Data Breach* survey, sponsored by HP Enterprise Security, of the 488 information security pros participating, 63 percent are confident that their company's IT security departments have the power, executive support and budget/resources necessary to safeguard customer, client and other critical corporate data. This is up from last year's survey, which saw 58 percent out of 468 respondents feeling such confidence.

"Budgeting is always a tricky business," says Jeffrey Brown, global information security program manager with GE Capital. "Are your routers security devices or networking devices? Does anti-virus software fall under operating system costs or under IT security? While the allocations are not always clear, I think, in general, there's still a healthy amount of IT budget going toward meeting security needs."

Compared to last year's 36 percent, a very close 34 percent of respondents expect their budgets related to IT security projects and data leakage prevention efforts to increase. For most, this funding will remain the same, with 61 percent predicting a flat budget line. Meanwhile, 6 percent foresee a decrease.

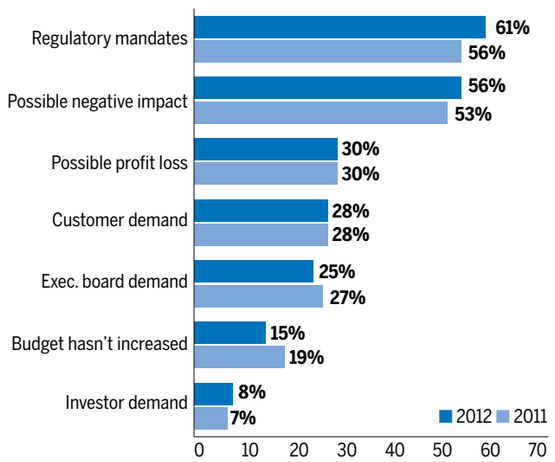
Financial pressures, then, persist, but this reality rarely changes, Brown says. That's why information security leaders must continue to make a sound business case for their efforts, ensure the money they do have is spent wisely, and tackle the top risks first. "This is basic risk management, really," he explains.

Even with these steps, though, financial support for IT security is either level or dwindling in most public and private organizations, say experts. There may be more talk going on, but there is no uptick in spending, says Bruce Bonsall, former VP and CISO with MassMutual, who is now an industry consultant.

Jerry Dixon, director of analysis at Team Cymru, and former head of US-CERT, agrees, explaining that his clients' budgets largely are consistent with last year's, with most organizations "squeezing every bit of life from their existing infrastructures."

Source: Source:gaps Where 2012 base: 488; 2011 Base: 468

Which drivers have aided in obtaining more resources for initiatives associated with safeguarding data?



Wielding the right tool

Although many organizations are leveraging the technologies they already have in place, some others are investing in various technologies that further bolster protections against newer threats, according to this year's survey results.

Last year, various types of mobile security solutions led the fray among the technologies that survey respondents were looking to deploy in 2011. These same solutions have a decent showing for possible implementation in 2012 at 41 percent. However, it seems for many security practitioners, the need to gain a better idea of what's happening on the network is overtaking some of their more longer-standing concerns. Half of the survey participants cite network monitoring solutions as top deployment priorities for the next 12 months. Another 38 percent are looking to roll out vulnerability management solutions, and 13 percent are considering security incident and event management (SIEM) deployments. (Editor's note: network monitoring, vulnerability management and SIEM solutions were not included as choices in previous *SC* data breach surveys).

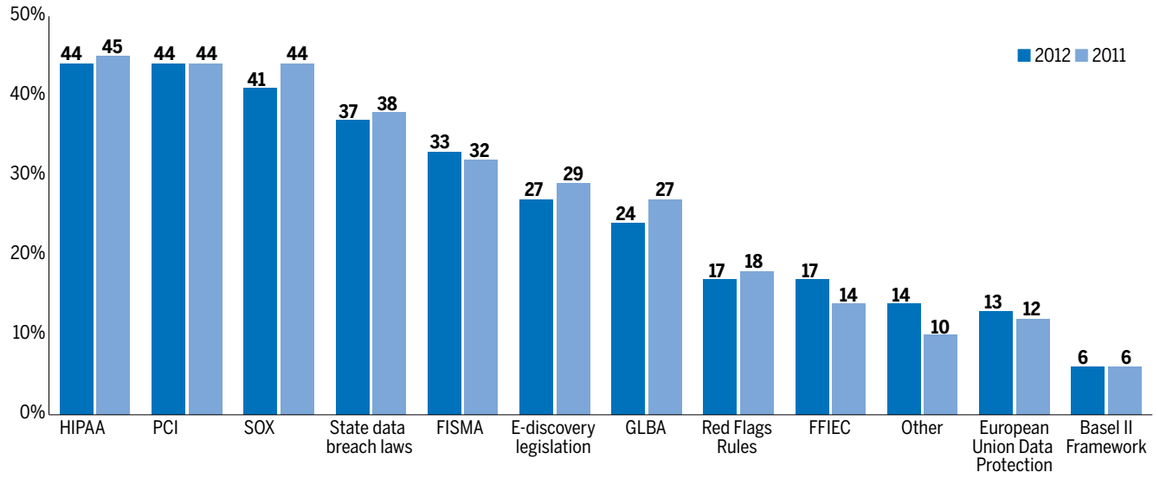
"The so-called advanced persistent threat (APT) has elevated the game," says Bonsall, adding that business leaders have accepted that they no longer can keep the bad guys out of their networks without the right tools and processes in place.

Dixon says he is seeing a large increase in the testing and purchasing of network monitoring solutions. As well, many companies are re-energizing security awareness training for their end-users since many attacks still rely heavily on social engineering methods to gain initial entree into corporate or government infrastructures.

"I think there's a real concern that current security products aren't working," he says. Companies have invested in various solutions to fortify their networks, "yet they're still having major breaches."

But, more traditional tools aren't being discounted out of hand. Alongside mobile security solutions, and now tools that provide a more holistic view of the network, survey respondents are considering for deployment this year email

Which guidelines are priorities to comply with when it comes to protecting customer/client data that is stored or shared electronically by your company?



management/content filtering (43 percent), database security (41 percent), data leakage prevention (38 percent), and web application security/secure coding (34 percent).

As companies evolve their risk management plans and the policies, processes and tools they rely on to thwart even the most advanced attacks, they also must be just as prepared for regulators who are evolving their own strategies for 2012 to better enforce compliance with mandates. It seems one way many executives are trying to accomplish this is by allocating more resources to compliance programs. Some 61 percent of security practitioners responding to *SC's* survey find that regulatory mandates are a major driver in scoring more resources for IT security projects.

"In down economies, executive [managers] are extremely conservative in expending anything that isn't absolutely key to the health and growth of the business," says longtime industry expert Becky Bace, who is president and CEO of Infidel, a network security consulting practice. "Though the loss exposures that are likely to be due to attacks or misuses are still not well understood, there is a well-quantified body of experience regarding the likelihood of fines and other costs associated with being found in non-compliance with regulations."

This seems true for just about most companies. Take, for example, Jim Routh, global head of application security at JP Morgan Chase. He says his company's IT risk budgets rose by about 15 percent in 2011, a significant jump. This likely will level off to about a five percent increase this year, but the allocations go some way in showing just how critical security and compliance are to the overall business and lead executives.

Regulatory mandates are increasingly significant, making it difficult for large organizations to get ahead of the curve and implement proactive measures," says Routh. "A new regulator 'activist' is more common as regulators get more assertive and influence each other."

Indeed, worries about increased audits rising in 2012 have been bandied about much more over the last six to 12 months. For instance, more strict enforcement of the *Health Insurance Portability and Accountability Act (HIPAA)* by the Office of Civil Rights is likely to spike this year, says Bryan Cline, vice president for Common Security Framework (CSF) development and implementation at the Health Information Trust Alliance (HITRUST).

And there are still other reasons why security pros may see more external auditors zeroing in on their companies in coming months.

"As the regulatory authorities face stressors of their own in these economic downtimes, the chances of being audited by them go up," says Bace. "They must prove to lawmakers and government watchdogs alike that they are effective in enforcing regulations within their purview, lest they be targeted for budget cuts. Add to this that IT security, under the buzzword of 'cyber,' is getting a lot of attention, and the upward trend in security budgets makes perfect sense."

Seeking help

At the same time that some security officers are seeing even the smallest of bumps in funding because of compliance mandates, they're experiencing both positives and negatives when it comes to hiring additional staffers to support their efforts, according to survey results. On the plus side, during the last year, 26 percent of respondents saw the number of people in the IT department who handle all information security efforts increase, while another 64 percent say the number of pros currently on the payroll has remained the same. On the negative side, about 75 percent of survey participants have no plans to hire for new IT security positions.

> "The upward trend in security budgets makes perfect sense."

GE's Brown says he believes that these figures might support his belief that "a lot of organizations have been going through cycles of rapid growth with the security function," which is now prompting them to re-evaluate where they are and what they really need.

"Also, security responsibilities are beginning to work their way into other areas of the organization. Developers, network administrators, database administrators and systems personnel are all inheriting more and more security responsibiliteis rather than building these functions into a centralized security team," he says.

Some experts believe such changes can prove detrimental by making overall corporate security weaker. Also, these developments could lead to even less funding specifically dedicated to security in the future.

Outsourcing and cloud computing may be impacting hiring too, which would reduce the numbers of staffers needed, says Jeff Combs, owner of security recruiting company J. Combs Search, and director of recruiting at Acumin.

"Every company is different, but given the uncertain economic climate, there will continue to be cost-cutting and consolidation – often at the expense of providing adequate security and IT risk management controls," Combs says.

On a more positive note, Team Cymru's Dixon says that while he is seeing more companies looking at managed security services because of limited budgets, many larger organizations are indeed hiring for a slew of technical security posts to cover firewall administration, network monitoring, and more. Given all the high-profile breaches that have occurred, worries about becoming the next publicized victim are pushing companies to staff up, he says.

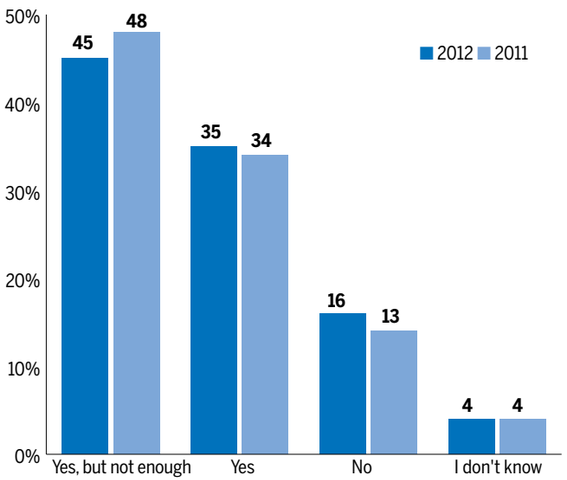
"Let's be honest, they've been understaffed for years," he says.

Cheap tricks

Companies are relying on still other ways to fend off evolving attackers and be prepared for an increase in external audits by regulators. One major step toward meeting some basic security needs and staying in compliance is through the implementation of security training and awareness programs for end-users.

Compared to last year, there was an ever-so-slight increase in the number of *SC's* data breach survey respondents who have

Have you strengthened your security awareness and training for corporate employees to help safeguard customer, client and other critical corporate data?



ON THE HORIZON:
A national data breach law

Support by information security professionals for the passage of a national data breach law remains mixed, but few say such a law actually would impede their abilities to do their jobs.

Only 33 percent of practitioners participating in *SC Magazine*'s "Guarding against a data breach" survey believe that the passage of a federal data breach notification law would help them in their security efforts to protect customer or client data, while another 33 percent say it would not.

Meanwhile, almost half of respondents believe the national law would not impede or hurt their strides in securing critical data. A mere 17 percent say it would, with another seven percent agreeing with this sentiment, but noting the negative impact would be limited.

André Gold, head of technology operations and security at AutoTrader.com, agrees that such a law would do little to help organizations with their security efforts, especially in the ways that others, such as *Sarbanes-Oxley* or the *Health Insurance Portability and Accountability Act (HIPAA)*, have.

"That said, I think organizations would welcome a national law, as it would add consistency to the notification process," he says. "Due to the numerous state statues out there, organizations have had to spend a disproportionate time staying up to date with the state statutes versus helping their organizations manage risk."

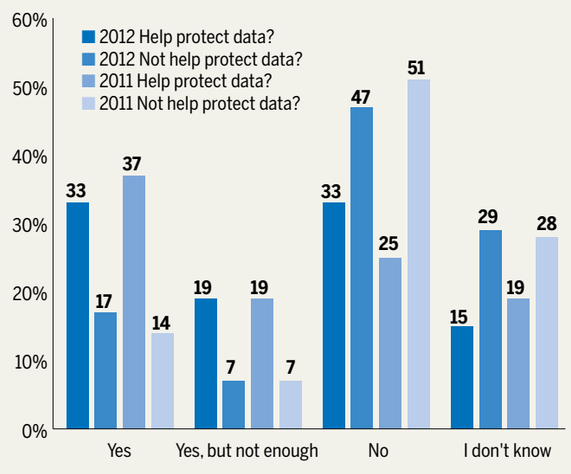
Currently, there are quite a few commonalities in many of the state laws, but challenges still exist when searching for a common ground because of some remaining differences, says Erik Avakian, chief information security officer for the state of Pennsylvania.

"Additionally, due to the nature of the economy, buy-in from the states can only occur if such federal legislation does not create any unfunded mandates that may prove burdensome during these tough financial times," he says.

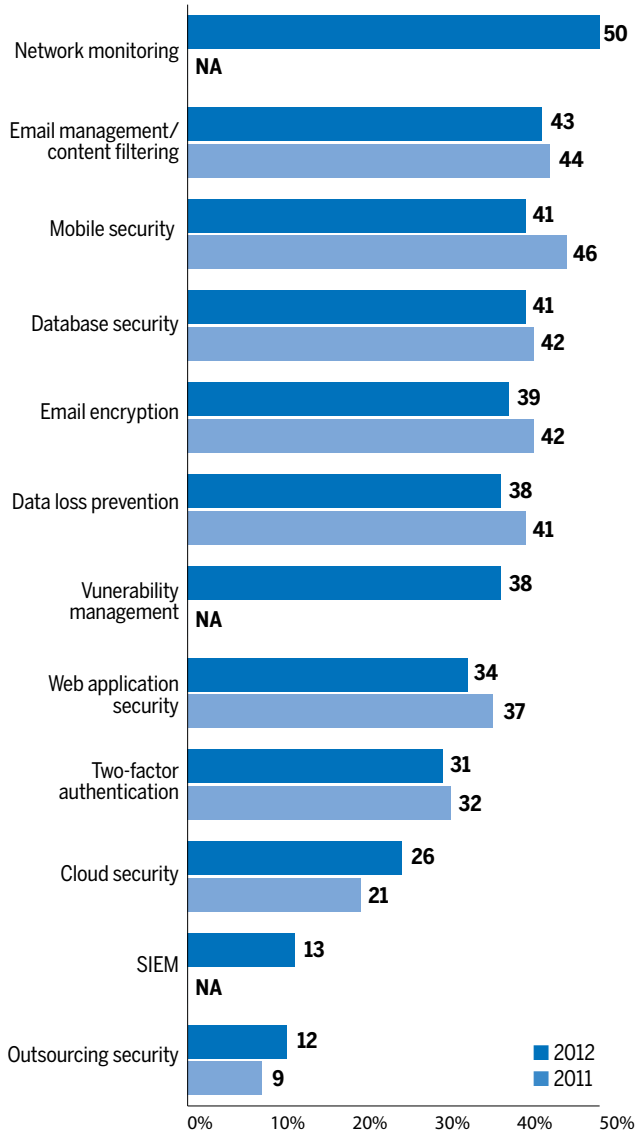
Another problem that might halt passage of a federal law is that this year will be a busy one politically.

"I don't see a national data breach notification law being passed in an election year," says Gold. "Our representatives have more material things to focus on, like getting Americans back to work."

Would the passage of a national data breach notification law help in your security efforts?



Which security solution is your company considering deploying to help safeguard data in the next year?



strengthened their end-user security training. Among their training methods, 70 percent of respondents send email updates to staff on information security/data theft; 57 percent offer periodic online training for employees; 55 percent provide regular, live training sessions for workers; 49 percent have newsletters on information security/data theft; and 13 percent turn to annual salary reviews that account for adherence to internal information security rules/guidance.

"Companies are realizing that it takes training to change culture," says Gene Fredriksen, CISO of Tyco International. "It's a cheap control. It also demonstrates due diligence."

On top of giving more attention and dollars to staff training, companies are looking harder at the perceived benefits and cost-savings associated with securitiy services. Among the other solutions that companies are considering making part of their programs this year, 12 percent of respondents are looking to outsource security. Another 26 percent are pondering cloud security services.

"This, in some ways, reflects the lead edge of the impact of the cloud," says Bace. "When key IT functions are outsourced, a lot of the security provisions are either included as part of the function or else implemented by selection of a specific option in the service agreement. This requires a different sort of professional with skills that may not be served by current models."

But, cloud services, overall, are still young. Plenty of areas of concern exist that must be addressed before more organizations begin relying on them.

"Cloud is the only real sea change I see looking toward the future, and there is still little sense of how it will ultimately affect life in the IT and IT security trenches," says Bace.

Yet, of the 488 respondents to the survey, more than a quarter (28 percent) say they are storing sensitive data in the cloud, with 18 percent using private clouds, 3 percent enlisting public clouds, and 7 percent relying on security-as-a-service (SaaS) providers.

Future

Cloud services, web applications, mobile devices and social networking all continue to be vectors of attack causing major concern for corporate executives, say experts. Then, there are the attack types to worry about: APTs, social engineering, malware and loads of others, which all are spearheaded by more sophisticated and often organized cyber criminals, hacktivists or state-sponsored attackers.

"This is why we're seeing an increased emphasis on protections against APTs [through] network monitoring, SIEMs/PIEMs and vulnerability management, and social engineering [through] education training and awareness," says Cline.

But, more than the investments in technologies and policies, security pros must continue to make the business case for their programs. Without this, the executive support they seek will continue to elude them.

"As the economy continues to struggle, the temptation will always be to cut from less tangible, non-revenue-generating areas like information security," says GE's Brown. "This is where security leaders need to keep abreast of the threat landscape, align their security objectives with business strategy, and, ultimately, know which budget battles they can concede and which they can't." ■

The methodology for this year's study was as follows: Email invitations were sent to approximately 50,000 IT security professionals. A total of 488 respondents completed the survey online, between Oct. 19 and Nov. 10. The results are not weighted, and the margin of error is +/- 3.7 percent.