C-SUITE 360

FALL 2016

SPECIAL REPORT:

IT Security's Looming Tipping Point

Even as security draws board-level attention, many IT professionals give their organizations' infosec practices low marks. Find out how to tip the balance in the right direction. »

by the editors of

CIO COMPUTERWORLD CSO

FROM IDG

Welcome to the First C-Suite 360!

RIGHT NOW YOU'RE asking yourself, "What's a C-Suite 360?" Let us explain: CIO, CSO and Computerworld editors are collaborating on the creation of a small but unique stream of content. The "C-Suite" represents the combined audience of all three publications. The "360" means we're offering a panoramic, 360-degree review of everything there is to see. So think of a C-Suite 360 report as a package that offers a comprehensive picture of a particular technology market – in this case, IT security.

For this report, the editorial teams of the three publications joined forces to survey IT and business leaders about the state of information security. The results of our research show cause for cautious optimism. On the one hand, it's troubling that half of survey respondents gave security at their organization a grade of C or worse. On the other hand, 65% of them said senior business management is focusing more attention on infosec than it has in previous years, and 77% said they expect to see more attention paid to security in the next one to three years.

Inside you'll find more survey results as well as guidance on a range of issues faced by organizations looking to ramp up their security game, from aligning security needs with business goals to crafting an infosec model that stays on top of new threats without overwhelming users.

– Scot Finnie, editor in chief, Computerworld
– Joan Goodchild, editor in chief, CSO
– Dan Muse, editor in chief, CIO

by the editors of

CIO COMPUTERWORLD CSO
FROM IDG

C-SUITE 360: Special content from the editors of CIO, CSO and Computerworld

EDITORIAL

Editor in Chief, CIO
Dan Muse

Editor in Chief, CSO
Joan Goodchild

Editor in Chief, Computerworld
Scot Finnie

Editor, Computerworld
Ellen Fanning

Managing Editor, Features, Computerworld
Valerie Potter

Managing Editor, Special Projects, CIO and CSO
Amy Bennett

Editorial Project Manager, Computerworld
Mari Keefe

Managing Editor, Copy and Production
Bob Rawson

Art Director
Steve Traynor

IDG

IDG
492 Old Connecticut Path
P.O. Box 9208
Framingham, MA 01701-9208
(508) 879-0700

CEO, IDG Communications Worldwide
Michael Friedenberg

C-SUITE 360°

Navigating the Muddy Waters of Enterprise Infosec

Information security finally has executives' attention, but aligning with business needs is still challenging.

BY STACY COLLETT

Executives at Booz Allen Hamilton learned the importance of information security the hard way back in 2011 when the hacker group Anonymous claimed that it had penetrated one of Booz Allen's servers and had deleted 4GB of source code and released a list of more than 90,000 military email addresses and encrypted passwords.

The breached server turned out to be a development environment containing test data, "but that didn't really matter; it was a wakeup call," says Michael Waters, director of information security at the consulting firm and government contractor. "It was a pretty unpleasant experience, but it did galvanize substantial investment – both capital and HR – in getting things done. The firm looked around and said, 'We have been working on this, but we need to put more toward it.'"

Over the next year, Waters' information security staff grew from 12 to 70 employees, budgets increased, and processes and governance improved significantly. But a security plan is never "finished," and in 2013 Booz Allen received a second jolt – this time in the form of an insider

ED DUNENS

threat – when recent hire Edward Snowden, working under contract to the NSA, leaked highly classified documents describing government surveillance programs.

Booz Allen promptly fired Snowden and further honed its infosec program – a practice that continues to this day, says Waters. "We constantly update our information security procedures, no matter what the circumstances, and we also are continuing to strengthen our ethics and compliance program every year," he says.

Today, Waters would put his infosec program on par with those of the world's biggest enterprises, but he would have preferred to get there without those pivotal events.

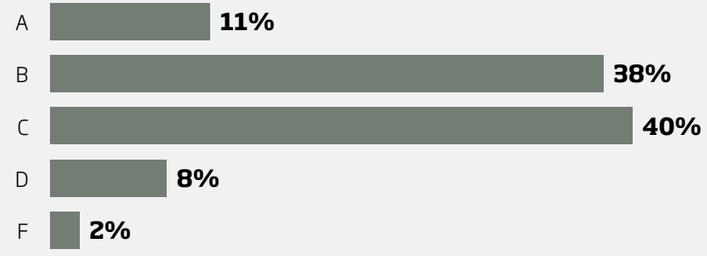
Many companies today hope to avoid similar high-profile wakeup calls. After years of news about disastrous breaches, information security has finally gotten the attention of upper management. Two-thirds of 287 U.S. respondents to a survey conducted by CSO, CIO and Computerworld said that senior business executives at their organizations are focusing more attention on infosec than they were in the past. And most of the respondents said they expect that focus to continue. Yet IT leaders still face challenges when it comes to aligning security goals with the needs of business, including justifying costs, defining risks, and clarifying roles and responsibilities.

Half of the survey respondents said security-related efforts account for less than 10% of their IT budgets, and nearly three-quarters said security efforts account for less than 25% of IT's time. And while half of those polled said they'd grade their organization's security practices as an A or B, an equal portion would choose C, D or F.

So how can enterprises get from where they are today to having a cohesive, funded and fully implemented information security program? IT leaders and analysts share tips for navigating these muddy waters and protecting the organization from threats.

Security Report Card

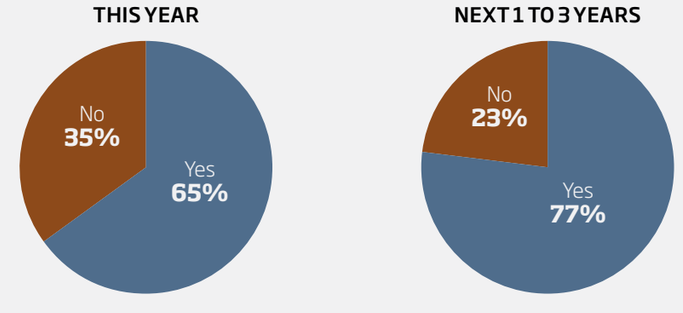
How would you grade your organization's security practices?



BASE: 287 RESPONDENTS. PERCENTAGES DO NOT ADD UP TO 100 BECAUSE OF ROUNDING.

Infosec in the Spotlight

Is senior business management at your organization focusing more attention on information security this year than in prior years? Do you expect management to be more focused on infosec in the next 1 to 3 years?



BASE: 287 RESPONDENTS

Emphasize Awareness

About a year ago, customers of sales and marketing advisory firm SiriusDecisions started asking questions about the security of the information they share with the Wilton, Conn.-based company. With all the news about data breaches, they were concerned that a weak link might jeopardize the competitive intelligence they shared.

Vice president of IT Jonathan Block knew the firm's infosec policies and procedures were sound. Sirius-

Decisions operates entirely in the cloud, relying on big-name vendors whose security practices far exceed what the firm could do on its own. But he says the growing number of client inquiries, along with a slew of highly publicized security breaches at other companies, "lit a fire under us," underscoring the importance of information security both internally and for the firm's clients.

Today, SiriusDecisions shares detailed information with customers about its service providers' security certifications and audits, trains every employee on information security awareness, especially social engineering – its biggest threat today – and earmarks 10% of its IT budget specifically for infosec initiatives.

Why Security Is Under Scrutiny

What is driving your organization's increased focus on information security?

BASE: 233 RESPONDENTS AT ORGANIZATIONS THAT ARE PLACING A GREATER FOCUS ON SECURITY NOW OR ARE EXPECTED TO DO SO IN THE NEXT 1 TO 3 YEARS. MULTIPLE RESPONSES ALLOWED.

> **"The frequency and severity of attacks are always going to increase, but we've identified the type of attacks that do the most damage, and we focus our efforts on those."**
>
> –JONATHAN BLOCK, VICE PRESIDENT OF IT, SIRIUSDECISIONS

Asked to grade the firm's efforts, Block says , "I'd give us a solid B. Our goal is to try to get ahead of a lot of these things. The frequency and severity of attacks are always going to increase, but we've identified the type of attacks that do the most damage, and we focus our efforts on those."

Create a Communication Channel

At Wells Fargo, executives are much more knowledgeable about information security than they were four years ago, says chief information security officer Rich Baich, who became the bank's first CISO in 2012.

Much of the improvement centers around better collaboration and communication between technical and nontechnical staff, business units and executives, he says. To help get there, Wells Fargo realigned its security hierarchy. In January 2015, Baich began reporting to the chief risk officer instead of the CIO to emphasize security's risk-based focus and to improve transparency with the board of directors.

"I'm not in technology," Baich says. "[The new hierarchy] allowed us to effectively create a communication channel that helped people understand the language of security, the importance of security, how it fits into the larger, overall risk management construct – and ultimately helped drive and make this part of our culture, [in which] every individual team member is a risk manager."

Baich would not assign a letter grade to Wells Fargo's information security program, saying that even a good grade might invite scrutiny from prospective hackers. But Elvis Moreland, who worked at the bank as an independent cybersecurity contractor from November 2015 to

May 2016, applauds the steps Wells Fargo has taken to boost security, including its move to adopt federal NIST cybersecurity standards, which he helped plan as part of the bank's hybrid security framework. "They'll work their way up to a B easily" if those efforts continue, he says.

Moreland recommends the NIST cybersecurity framework because it applies to both the private sector and the federal government, and because it offers three decades of documented lessons learned that can be applied to any organization. "It's hundreds of millions of dollars in free research," says Moreland, who is now a senior cyber-security and risk management consultant at Atos BDS North America. "Companies would cover 80% of the security vulnerabilities and weaknesses we see today" just by realigning the security hierarchy and adopting the NIST framework, he adds.

Aligning Business and Infosec Goals

Top challenges faced by organizations in aligning information security aims with business needs:

BASE: 287 RESPONDENTS. MULTIPLE RESPONSES ALLOWED.

Give It a Spin

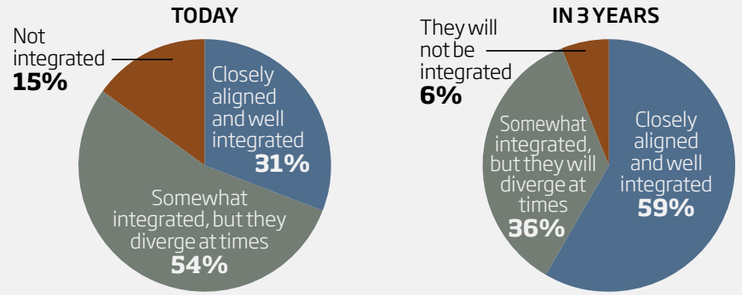
Even before the 2011 attack, Waters had been working on Booz Allen's information security framework. However, "it was challenging to get the attention and budget I needed," he recalls.

He soon learned that the tone and perspective he used to communicate infosec needs to the IT department, executives and business units were critical to getting things done.

Today, Waters says that when he and his team discuss security needs with their business colleagues, they might say, "It's not that I want you to do something, but it's this new regulation we need to comply with, and I can help you figure out how to do it." Or, "Outside attackers are trying to steal our data or wreck our systems; I'm here to help implement the protections and controls because of these outside forces."

Aligning IT and Infosec Strategies

How tightly integrated are infosec strategy and IT strategy at your organization today? How tightly integrated do you expect they will be 3 years from now?



BASE: 104 RESPONDENTS WHOSE ORGANIZATIONS HAVE DEDICATED INFOSEC TEAMS. PERCENTAGES MAY NOT ADD UP TO 100 BECAUSE OF ROUNDING.

Spend Wisely

Gary Vause, founder and president of cybersecurity consultancy VSC, says many companies keep tight caps on their infosec budgets because they expect to need resources to put out the next security fire. "They know it's coming, but rather than be preventive, they choose to be reactive," he says.

On the other hand, he cautions, throwing money at the problem isn't the answer either. Developing an understanding of a company's security maturity level – a

view that includes people, processes and technology – can help organizations prioritize budgets based on the most critical vulnerabilities, he says.

Emily Mossburg, principal of Deloitte's Resilient Services practice, agrees that it's not about spending more money. The question, she says, is this: "Are you prioritizing the things that could actually hurt your business the most?" And are you remediating the areas where your business is the most vulnerable? She advises focusing on the areas where "the threat actors are really after your business and, ultimately, where the impact would be the greatest."

Make It Real

Companies often look at the easy-to-identify, tangible losses in a data breach, such as the number of records with personally identifiable information. Those should certainly be protected, Mossburg says, but less obvious losses could actually prove costlier.

In June, Deloitte released a report that uncovers 14 business impacts of a cybersecurity incident, half of which are hidden costs, including loss of intellectual property, devaluation of your trade name and lost contract revenue. Those hidden costs can be far more expensive than the initial triage and damage control expenses, and they can go on for years.

In one hypothetical model that Deloitte created based on its experiences with customers, the cost to a healthcare company that lost a significant number of medical records was more than $1.6 billion. Of that figure, only 3.5% of the costs were considered "above the surface" tangibles that are generally expected in the wake of a cyberattack, such as post-breach customer protection services and cybersecurity improvements.

> **"When you can articulate a risk that the business and board of directors agree with, then you can come up with a plan to mitigate and manage that risk."**
>
> –MICHAEL EISENBERG, VICE PRESIDENT IN THE OFFICE OF THE CISO, OPTIV

The remaining 96.5% of the costs were for less tangible hits, such as lost customer relationships and increases in insurance premiums. Such "beneath the surface" costs often come as a shock for companies in the post-breach remediation process.

"We need to make this real for people," Mossburg says. "It's very important to understand the industry, the nuances to the types of systems they use, their interconnectedness to third parties, the types of data they have, how they're using it and what that might be." All those contributing factors, along with the type of incident, make scenarios unique for every company. "We've had a lot of conversations [with clients] on what are the scenarios that they should be modeling for themselves," she says.

Articulating risks is an important first step, says Michael Eisenberg, vice president in the office of the CISO at cybersecurity solutions provider Optiv. "When you can articulate a risk that the business and board of directors agree with, then you can come up with a plan to mitigate and manage that risk" – a plan that includes additional funding and resources, he says.

Writing on the Wall

Five years after the Anonymous breach at Booz Allen, Waters still displays a framed copy of the *Washington Post* article about the attack on his office wall. "For me and my leadership team," he says, "it's a reminder that this is never allowed to happen again."

Stacy Collett is a contributing writer for CSO and Computerworld, covering a variety of security and risk issues.

SECURITY CHALLENGE:

Wearing Multiple Hats in IT

Handling both security and IT duties involves a daily balancing act for the resource-constrained IT organizations that must take this approach. But along with the challenges, there can also be benefits. BY BOB VIOLINO

Are you taking on multiple job responsibilities at your company, including some aspects of information security? If so, you're not alone. At many organizations, IT professionals are being asked to handle a variety of security tasks and functions. For them, wearing multiple hats can create both opportunities and stress.

In a recent online survey of 287 IT and business professionals conducted by CSO, CIO and Computerworld, a majority of respondents (54%) said the IT department handles information security at their organization.

In contrast, only 17% said that a dedicated group handles information security. An additional 14% said information security is handled by a mixed team that includes IT and infosec workers, and 6% said their organization has a dedicated security team that includes infosec. That means only 37% of the respondents work at organizations with dedicated infosec professionals, which might explain why many organizations have a hard time keeping up with security.

People who wear multiple IT and security hats – or who oversee such workers – aren't necessarily happy about the situation or what it means for their organizations' security

THINKSTOCK

programs. But they're finding ways to cope.

National FFA, an organization that promotes career success through agricultural education, has increased efforts to secure its systems and data considerably in recent years, says Joel Gibbons, National FFA's director of IT and compliance.

Gibbons is responsible for all technology operations and development, as well as security for the 150-person organization. "My operations team includes a security lead who handles the daily security operations," Gibbons says. "Specifically in the security area, I handle mostly communications, training, policy and strategy."

Security has always been important to National FFA, "but the visibility of security efforts has changed, in part due to the large data breaches that have [made] headlines over the past two years," Gibbons says. "In the past, a CEO could simply have faith in the efforts of security professionals in the company. Now, the CEO needs to know more to be able to answer specific questions about how we are securing whatever needs securing inside the organization's perimeter."

"In a small organization, I can't always afford to let my security folks focus solely on security. There are always other things they need to do."

–JOEL GIBBONS, DIRECTOR OF IT AND COMPLIANCE, NATIONAL FFA

With Gibbons and his team of 14 handling multiple aspects of both IT and security, ensuring that data is safe can be a struggle.

"Security is a full-time job, and then some," Gibbons says. "In a small organization, I can't always afford to let my security folks focus solely on security. There are always other things they need to do. That can have a negative impact on security. Or, it can have a negative impact on any other things they aren't doing because security efforts take so much of their time. It's a daily balancing act."

To address this challenge, National FFA uses tools that automate mundane security activities to take some of the burden off of the IT team's security specialists.

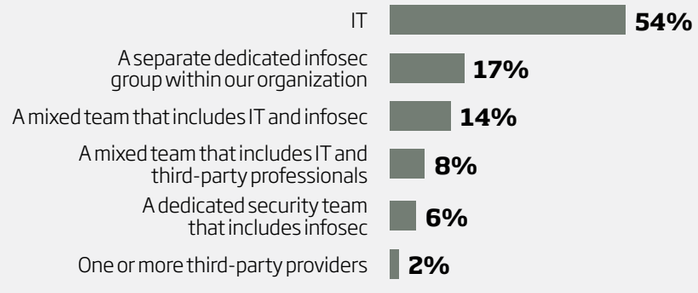
"We utilize external partners to help augment, but not replace, our in-house security expertise," Gibbons says. "We know that we are never secure enough. We have to continue to improve. We also know that we will probably not be 100% successful."

Given that reality, the organization has contingency plans in place for dealing with incidents when they occur. "It's only a matter of time before someone finds an access point that we've missed," Gibbons says. "That's just the nature of the game these days."

Also juggling multiple roles is the director of IT at a mid-size financial services firm based in the New York metro area, who manages cybersecurity in addition to all of the

IT in Charge

Who is primarily responsible for information security within your organization?



BASE: 287 RESPONDENTS. PERCENTAGES DO NOT ADD UP TO 100 BECAUSE OF ROUNDING.

daily functions of the technology department, including the help desk, desktop support, engineering and development.

The director, who asked that his name and company not be identified, says his responsibilities have increased considerably "as the outside technology landscape has evolved over the last five years." The role, he adds, has morphed "from a traditional CIO position into an all-encompassing CIO/CSO management role, where the need to stay ahead of what is occurring in the technology/cybersecurity space is required."

One of the challenges is maintaining tight security "in a world where end users expect the same level of accessibility that they enjoy at home," the director says. "End users do not fully comprehend the need for restrictions to their office internet access. The most difficult challenge is cybersecurity awareness and training, instructing end users to think before they click and changing the mindset."

Executives at the 140-person financial services firm are aware of the threats posed by nefarious actors, "and we agree that it is best to remain more secure and ensure business operability than to become the next firm on a list of compromised or breached companies," he says. "Our firm employs the concept of erring on [the side of being] more secure with limited third-party accessibility to the extent that is practicable."

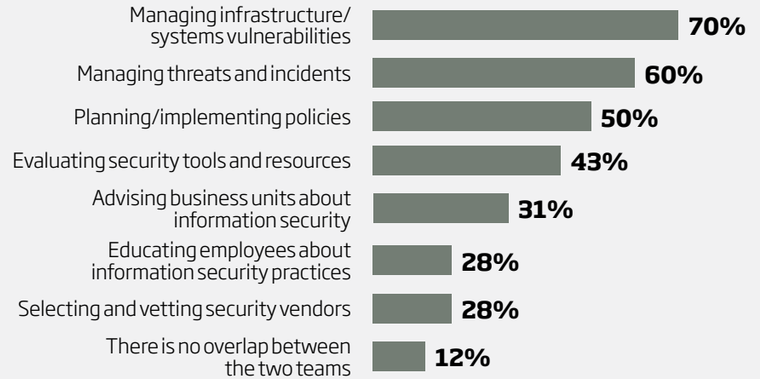
As a result, the firm limits access to any non-business-related sites or services – including all third-party email, cloud storage and video streaming services.

Still, it has been a struggle for the IT director to fulfill his expanded responsibilities with his team of four IT workers. "We are now being asked to be the gatekeepers of all technology, not only ensuring we are keeping the lights on, but now also policing the entire organization – from firewall perimeter to inbound and outbound persistent threat management," he says. "I have had to learn the dark side of the web with regard to security in order to understand how to protect our assets from persistent external threats and end user fallibility."

At Green Clinic Health System (GCHS), a physician-owned healthcare system in northern Louisiana, Jason

Overlapping Responsibilities

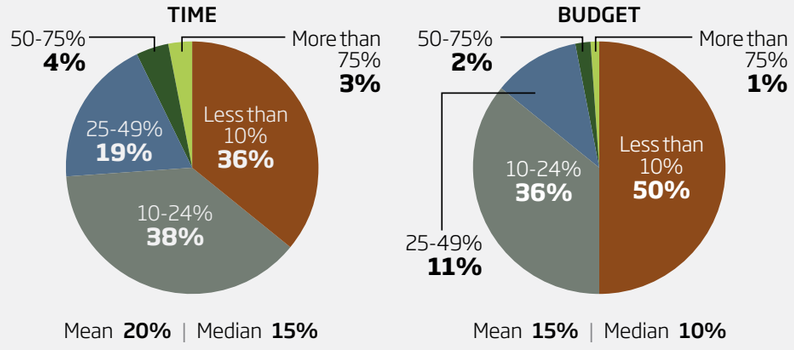
Where do IT and the infosec team overlap, if any overlap exists?



BASE: 104 RESPONDENTS WHOSE ORGANIZATIONS HAVE DEDICATED INFOSEC TEAMS. MULTIPLE RESPONSES ALLOWED.

IT's Security Expenditures

What percentage of IT's time and budget are devoted to security-related efforts?



BASE: 183 RESPONDENTS IN ORGANIZATIONS WHERE IT AND/OR THIRD-PARTY PROVIDERS ARE PRIMARILY RESPONSIBLE FOR INFORMATION SECURITY

Thomas serves as CIO, director of IT and HIPAA security officer, meaning he ensures that GCHS complies with the terms of the Health Insurance Portability and Accountability Act. With four full-timers and one part-time staffer, his department handles all aspects of IT and telecommunications for the system's five facilities, and also serves as the internal cybersecurity department for the 450-person organization.

"I often joke that if it plugs into the wall, it falls under my purview," Thomas says. "But that's less of a joke and more of a friendly way of telling people which department to call first."

This wide-ranging role does provide some benefits from a security standpoint. "Since I lead the IT department as well in my capacity as IT director, I have the day-to-day visibility into operations and challenges that allows me to bring concerns regarding organizational operations and security directly to upper management, and guide or develop the necessary tools, policies and procedures to address any issues or needs," Thomas says.

THINKSTOCK

One example of how the combined IT/security role proved to be a benefit was in the deployment of an electronic health records system several years ago. "With that implementation came a serious review and rework of our technical policies and capabilities to support secure electronic access to records," Thomas says.

But that doesn't mean there aren't significant challenges, and one of the most recent has been around the acquisition of new medical practices. "Sometimes there are political challenges I have to confront as CIO, such as trying to explain to a physician why he or she can't continue to do something the way they used to do it when they were a stand-alone practice," Thomas says.

At other times, there are technical issues such as those that arise with the potential reuse of existing workstations and the associated tasks of auditing current configurations to ensure they are free of malware and capable of supporting security policies and software.

Good communication is key to meeting the challenges. "We have weekly management meetings to discuss current issues around the organization," Thomas says, "and many times security issues are brought up and plans are formed to resolve those issues."

Bob Violino is a freelance writer based in New York.

PEXELS

How Flexible Should Your Infosec Model Be?

Organizations need to stay on top of a fast-shifting threat landscape by updating their security policies – without badgering users into a state of noncompliance. BY BETH STACKPOLE

Security is a top priority at the Bank of Labor, but the financial institution updates its formal information security policy only once a year, maybe twice, regardless of what's happening in the ever-changing threat landscape.

That's not to say that the union bank ignores emerging threats such as new malware variants or phishing schemes, says Shaun Miller, the bank's information security officer. On the contrary,

the organization, which has seven branches in the Kansas City, Kan., area plus an office in Washington, routinely tweaks its firewalls and intrusion-protection systems in response to new and active threats. To avoid fatiguing its 120 users, however, it refrains from formalizing new policies more frequently.

"The purpose of our policies is to be at a high level, not to cover every eventuality out there," says Miller. "We update procedures for tactical day-to-day stuff, but when it comes to our strategic direction on security going forward, we change our policies in a limited fashion so as to not overwhelm users."

The Bank of Labor isn't alone. Given how fast the threat landscape changes, it can be difficult for a company to modify something as rigid as a corporate security model to keep pace with every new attack vector. In a recent survey of 287 U.S.-based IT and business professionals conducted by Computerworld, CIO and CSO, 33% of the respondents said that they work for organizations that have had the same model for information security management in place for five or more years. Meanwhile, 23% said their model had been in place for three to five years, 33% said one to three years, and just 11% said less than a year.

However, 50% of those polled said their organizations are considering making changes to their infosec management models. When members of that group were asked what factors are driving their employers to contemplate a change, the top three responses were concerns about breaches and data loss (cited by 78% of the 144 respondents), technology advancements and upgrades (53%), and regulatory compliance (49%).

How often to adopt infosec policy changes is a conundrum. Companies need to come up with a way to remain flexible, to ensure that their policies and procedures reflect the current threat landscape, yet they can't hand down so many new rules and restrictions that they frustrate users and inadvertently compel them to consider bypassing corporate rules, explains Kelley Mak, an analyst at Forrester Research.

> **"The purpose of our policies is to be at a high level, not to cover every eventuality out there."**
>
> –SHAUN MILLER, INFORMATION SECURITY OFFICER, BANK OF LABOR

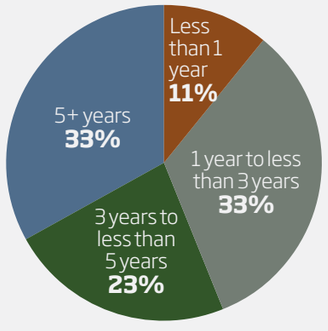
At the same time, companies have to strike a balance between using firefighting tactics to address the most current threats and treating information security policy as a holistic strategy, Mak says. "It's not as simple as taking the data and making a new policy, because you have to make sure information workers aren't upset," he says. "The more restrictions you put in place, the more likely someone is to go around it."

Filling Day-to-Day Gaps

That's exactly what Miller is trying to avoid. The Bank of Labor maintains an information security policy that addresses high-level issues, including the bank's overall stance on security and broad rules, such as a mandate requiring employees

Years of Practice

How many years has your current model for information security management been in place?



BASE: 287 RESPONDENTS

to use passwords to access data. The policies, which are put in place only after board approval, don't get into the weeds of the technology or spell out details such as the exact character requirements for passwords (which might change over time, anyway).

To complement the broad policies, Miller's group regularly modifies rules to tackle current security gaps. Most recently, the security team blocked the use of Flash software because of its well-publicized vulnerabilities, and because it's rarely used in business-related websites anymore. "We don't consider that a change to policy," Miller says. "Our board of directors approves policy, and they don't know what Flash is or what it does. It's just an example of a simple, day-to-day business response to threats as needed."

To keep people in the loop about updates, Miller sends email messages announcing changes and explaining why they're important. Saying he often includes links to background information, Miller explains that making sure people understand why the changes are necessary and being clear about the risks has been instrumental in preventing user frustration and ensuring that employees are willing to comply with even with small policy changes.

Test, Test, Test

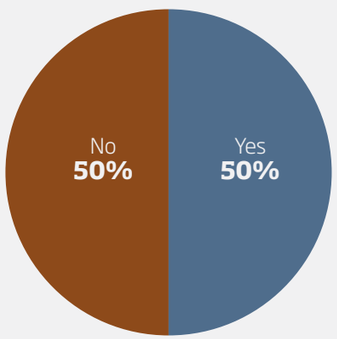
Devin Meade, senior systems manager in charge of security at Frankfurt Short Bruza (FSB), says he prefers to keep security policy fluid because the architectural engineering planning firm is relatively small (it has 150 users) and because it isn't directly affected by regulatory requirements. While FSB does have a formal security policy that is approved by the board of directors, Meade and his team make frequent recommendations for new procedures, using a small steering committee of about a half-dozen users to solicit feedback before rolling out the changes to a wider user audience.

"Our standard way of doing patches or making changes to our security stance is to test them out on a machine to see how they work and to roll them out to a representative group of people," he explains. That steering committee then tests the changes to determine what will work and what won't for FSB's users.

For example, Meade and his team recommended bumping up encryption. But during the steering committee's tests, the changes were found to make VPN access too unstable and slow, so Meade's team went back to the drawing board. It was a similar story when the team tried to

Time for a Change?

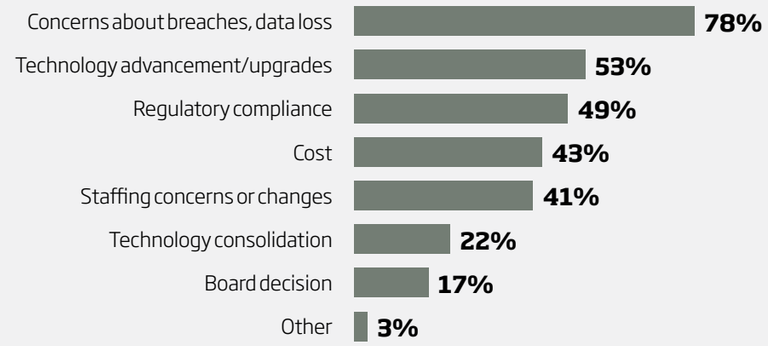
Is your organization considering making any changes to your current model for information security management?



BASE: 287 RESPONDENTS

Change Agents

Top factors influencing organizations' decisions about changing their infosec management models:



BASE: 144 RESPONDENTS WHOSE ORGANIZATIONS ARE CONSIDERING MAKING CHANGES TO THEIR INFOSEC MANAGEMENT MODEL. MULTIPLE RESPONSES ALLOWED.

enforce URL whitelisting and blacklisting to restrict user access to certain "not safe for work" sites. That move, Meade says, didn't work out as anticipated because the technology involved wasn't mature enough at the time.

Only after being approved by FSB's steering committee do infosec policy or procedure changes get implemented across the company. "My job is to inform [the executive team and business sponsors] about what we can do and what the process would be if we made the changes," Meade says. "Because we're a small firm, we can make modifications as the technology changes."

Most organizations aren't as nimble as FSB and don't update security policies often enough, and many don't test-drive changes to gauge what's effective and not too cumbersome, says Forrester's Mak. "You don't find a lot of organizations doing the right amount of testing to identify vulnerabilities, so there's not an accurate understanding of what the effect is on the environment from the human side," he says.

Mak advises companies to create security awareness programs that not only provide direction to employees, but also underscore the importance of embracing a serious security culture.

Getting Users on Board

That approach will soon to be in place at Fay School. Like the Bank of Labor, the school makes frequent minor updates to its infosec procedures to keep up with emerging threats but enacts major policy changes only a few times a year to avoid overwhelming users, says Joseph Adu, director of technology at the Southborough, Mass., private school, which serves grades pre-K to 9. Abu, who came on board a year ago from the for-profit sector, is drawing on his experiences in the business world as he develops the school's IT policies. Among other things, he's making a concerted effort to help employees feel invested in security.

This academic year, the school's 150 staffers and faculty members will take part in both in-person and digital training sessions that will be repeated annually to cover important infosec policy changes, Adu says. In addition, a new plan in effect this year calls for new employees to undergo security awareness training as soon as they are hired. Infosec training will also eventually be incorporated into the school's new-hire orientation process. That means newcomers will know right off the bat that sharing personal information en masse via email is prohibited, and they will understand how the school classifies particular types of data and why, among other things.

> **"The hardest part is getting people to realize that a lot of responsibility falls on them as end users."**
>
> –JOSEPH ADU, DIRECTOR OF TECHNOLOGY, FAY SCHOOL

Adu says presenting security policies at the point of hire is a way of indoctrinating users into the corporate culture and makes them feel accountable for upholding security best practices. Also, people are generally more open to direction when they first come on board, so they're more likely to accept and abide by the policies. (The school also holds short training sessions for its 400 students to cover security basics, such as a rule against sharing passwords.)

"We're trying to create a culture where people know they can count on the IT department to keep them abreast of what's going on," Adu says. "But they also need to understand that data security is an important part of working at this [organization] and they have a role. The hardest part is getting people to realize that a lot of responsibility falls on them as end users."

Beth Stackpole is a frequent contributor to Computerworld and CIO.

Why (and When) Outsourcing Security Makes Sense

Offloading security strategy and day-to-day operations to a managed security service provider can free up IT resources. But be prepared: It's not an entirely hands-off proposition. BY BETH STACKPOLE

Phenix Energy Group, an oil pipeline operator and construction company, is preparing to take its IT infrastructure from zero to 60 in a matter of months. To get a years-in-the-making pipeline project off the ground, the company is preparing to grow from a relatively small office environment to a data center setting of 75 servers and 250TB of storage. As a result, security, which hasn't been a top priority, is suddenly a big deal, according to CIO and COO Bruce Perrin.

Given the high stakes – a downed system could cost about $1 million an hour – Perrin has spent the past five years researching options. While he'd prefer to run security in-house as part of an on-premises data center, Perrin is leaning toward outsourcing the function, at least initially, because he doesn't have time to staff up a dedicated information security department in the few scant months before the pipeline goes online.

THINKSTOCK

"This project is huge. No one person is capable of managing this kind of IT deployment in 90 days," says Perrin, who's evaluating IT security value-added resellers and managed security service providers (MSSP). "I don't have an alternative to outsourcing – I need to bring someone in who can provide the security level we need and help us with the deployment, with the ultimate goal of moving everything to on-premises."

Why Outsourcing Security Makes Sense

Just like Phenix Energy Group, many small and midsize companies are gravitating toward an outsourced model for security and day-to-day operations, given the increasing number of data breaches and the heightened focus on risk. In a recent survey of 287 U.S.-based IT and business professionals conducted by CIO, CSO and Computerworld, 56% of the respondents said that their organizations are enlisting outside consultants to help with information security strategy, and 40% said they're turning to MSSPs.

According to the survey, the top functions being outsourced are penetration testing/threat assessments (cited by 70% of the 190 respondents who said they're turning to consultants and MSSPs), spam filtering (46%), threat intelligence (40%), log monitoring (34%), anti-DDoS/web application firewall protections (27%), business continuity and disaster recovery (26%) and awareness training (22%).

Outsourcing security functions appeals to small and midsize shops in particular because their resources are often already stretched thin and most lack the bandwidth to adequately perform security functions, experts say. Smaller organizations are also less likely to have people with specialized security skills who can focus on staying on top of a continually shifting landscape.

> **"Security ends up being sliced up and doled out to 10% of several people's jobs."**
>
> –BRENDAN O'MALLEY, IT CONSULTANT

Other developments that push companies toward outsourcing security include the increase in the number of malicious hackers and the proliferation of products designed for enterprise security, according to Garret Bekker, a senior security analyst at 451 Research. Both trends make security difficult to manage for smaller organizations, he says.

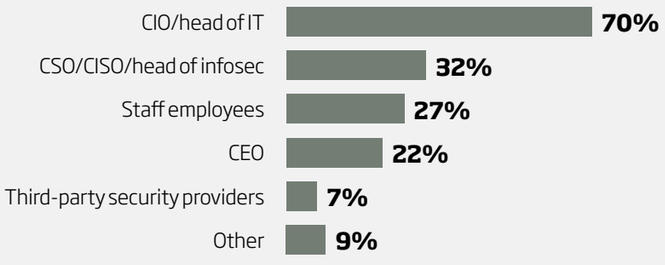
"The inevitable conclusion is companies increasingly have to rely on security handled by an MSSP because they can't keep up – they just don't have the bandwidth," says Bekker, who maintains that time saved is the primary benefit of outsourcing, far higher than cost savings on the list of advantages.

Outsourcing: Not an Either-Or Proposition

Brendan O'Malley, a serial CIO at midsize organizations and now a consultant, says the outsourced or managed services model works because there is often no one other than the CIO dedicated to security, which opens a

CIOs on the Hook for Breaches

If a data breach happens at your organization, who will be held responsible?



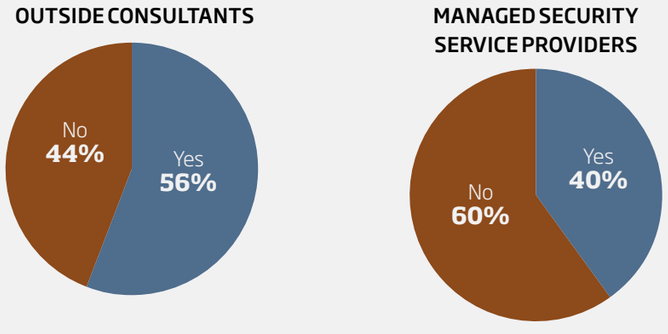
BASE: 287 RESPONDENTS. MULTIPLE RESPONSES ALLOWED.

company up to risk. "Security ends up being sliced up and doled out to 10% of several people's jobs, but because no one beyond the CIO is responsible, it's very tough to make progress or to stay on top of it the way you have to," he explains. "You absolutely need to have some kind of outside support."

For Blackhawk Community Credit Union, getting a helping hand from outside providers, including an MSSP, not only helps offload some security work, it also means the organization has 24/7, 365-days-a-year coverage from a highly trained set of eyes. Richard Borden, Blackhawk's vice president of IT, says his eight-person staff wouldn't be able to provide that kind of service, because they have to handle all types of IT issues, security included, for more than 150 users.

Outside Help

Do you use outside consultants or managed security service providers to assist with your information security strategy?



BASE: 287 RESPONDENTS

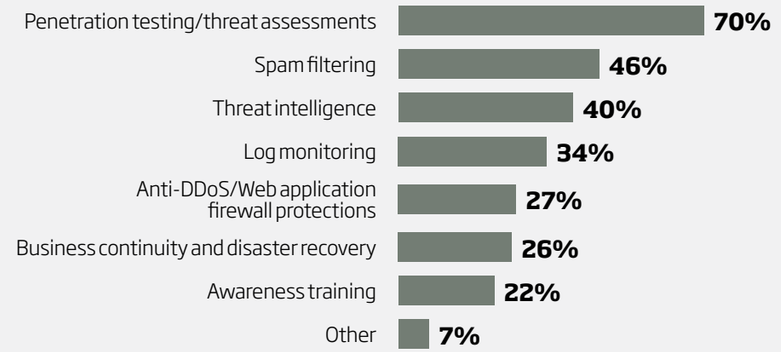
Instead of offloading everything to an MSSP, however, the credit union takes a three-pronged approach, doing security strategy and policy planning on its own, enlisting consultants to perform specialized functions, such as periodic firewall reviews, and leaning on its MSSP – in this case, Dell SecureWorks – for meat-and-potatoes functions like managing the firewall and the intrusion-protection system, Borden says.

"They can see global trends across all the clients and feeds they get, which gives me added confidence, so I don't stay up at night worrying about the network," he says. "If these folks see something spikey, they will get in touch with me."

The alert process is where outsourcing can get tricky for smaller shops, and the potential complications could undermine the value of using an MSSP. While outsourcing log monitoring and firewall management to a third party will provide a window into possible problems, outsourcers may have difficulty discerning between real security problems and noise because they lack insight into the inner workings of an organization and its typical user behaviors, says Jeff Pollard, an analyst at Forrester Research.

What's Being Outsourced

Top information security duties or services being outsourced to third parties:



BASE: 190 RESPONDENTS WHOSE ORGANIZATIONS USE OUTSIDE CONSULTANTS OR MANAGED SECURITY SERVICE PROVIDERS TO ASSIST WITH INFOSEC. MULTIPLE RESPONSES ALLOWED.

Outsourcers Need Help

In order to squeeze the most value from outsourced security services, Pollard says it's incumbent upon companies to put processes and communications channels in place so they can provide input to MSSPs to give them the right context for evaluating alerts.

Moreover, companies that work with service providers should also be prepared to explore and troubleshoot more events, because MSSPs usually do a better job than internal staffers when it comes to detecting suspicious activity, he explains.

"MSSPs have lots of visibility across clients and can make that relevant for each, but what they don't understand are the unique things in your organization – the micro versus macro issues, or which business units are most sensitive," Pollard says. "Companies need someone internally to serve as the liaison."

Choose Carefully

But being a liaison can be time-consuming. Ask Wes Farris, the information security officer and MSSP liaison at the Harris Center for Mental Health and IDD. He has so much else on his plate that he can only spend a limited amount of time working with the MSSP to fine-tune log monitoring and alerts to reflect the working habits of his users and the business.

"To get more value out of this service, we should be proactively tuning it, and I don't have time. It's a full-time job," he says, adding that the center can't afford to hire an additional full-time employee to focus on the liaison's role.

As with any vendor relationship, Farris and others say it's important to manage your MSSP and hold it accountable. Farris recommends choosing a partner with expertise in your specific industry. Doing the due diligence to select the right service provider is critical, given the importance of IT security – and because it's difficult to cut ties and move to another provider if things don't work out, he says.

"Once you execute a managed services contract where you are monitoring hundreds or thousands of devices, it's not easy to rip and replace," Farris says. "You have to make sure this is a company you want to use, that the tool sets are expansive and that the people working there are those you can trust."

"What [MSSPs] don't understand are the unique things in your organization – the micro versus macro issues, or which business units are most sensitive."

–JEFF POLLARD, ANALYST, FORRESTER RESEARCH

How the Survey Was Conducted

This special report is based on an online survey conducted by CIO, Computer-world and CSO from March 25 through May 23, 2016, among readers and customers of the three publications who responded to newsletter and email solicitations. The survey explored the interaction of information security and traditional IT teams in enterprises today: Who's responsible for which security duties, where roles and responsibilities overlap, and what challenges organizations face in aligning infosec concerns with IT strategy and business goals. Only the responses of those who indicated that they currently resided in the United States were tallied, for a total of 287 qualified responses. Some 83% of the qualified respondents are IT leaders or professionals, 11% are business managers, and the remaining 6% perform other business functions.

Beth Stackpole is a frequent contributor to CIO and Computerworld.