ARI KAPLAN ADVISORS

nuix

DEFENDING DATA

Cybersecurity Maturity Reflects Growth in How Corporations Manage and Protect Information From Increasingly Sophisticated Threats

Defending Data:

Cybersecurity Maturity Reflects Growth in How Corporations Manage and Protect Information From Increasingly Sophisticated Threats

Contents

About Ari Kaplan

Ari Kaplan, a leading legal industry analyst, is an inaugural Fastcase 50 honoree, a finalist for ILTA's 2015 Thought Leader of the Year award, and a 2016 fellow of the College of Law Practice Management. His book, Reinventing Professional Services: Building Your Business in the Digital Marketplace, was published in Japanese, and West Academic released the second edition of The Opportunity Maker: Strategies for Inspiring Your Legal Career Through Creative Networking and Business Development in 2016.

He is the principal researcher for a variety of widely distributed benchmarking reports and has also been the keynote speaker for events in Australia, Canada, the United Kingdom, and throughout the U.S. Kaplan is also the founder of the Lawcountability® business development platform, a finalist for ILTA's 2015 Innovative Solution Provider of the Year award, and a two-time Ironman triathlon finisher.

Executive Summary

Data security is quickly maturing in response to an ever-increasing array of external and internal threats. Many organizations are changing their approach to leveraging cybersecurity intelligence through enhanced cooperation, detailed information sharing, and broad-based collaboration. By evaluating patterns in spending, vendor management, breach preparation, behavior, and leadership, corporations can replace vulnerabilities with stronger safeguards.

For the third consecutive year, Nuix engaged Ari Kaplan Advisors to interview corporate security officials to characterize shifts in the market and provide perspective that empowers effective benchmarking. This year we spoke to 29 cybersecurity executives across a range of industries—our key findings are summarized next.

Key Findings

Human Behavior is Still a Key Concern

It was not surprising that 97% of participants said human behavior was the biggest security threat in their organizations. This was a slight increase over previous surveys—93% last year and 88% in 2014. Human vulnerability was the primary reason that 34% of survey participants described themselves as "very concerned" about whether they had been breached.

Regulatory Impact on Spending Is Increasing, But Not Highest

Over the past few years, regulators have increasingly impacted spending on security for the *Defending Data* respondents. In 2014, slightly less than a quarter of respondents said the regulatory environment was a major factor driving their spending decisions; in 2015 this was the case for more than half of respondents and in this year's report it was 72%. However, it was still not the most influential factor in this year's report; respondents said the data they held (90%) and past experience (86%) were the leading factors driving their decisions. Vendor reputation (52%) rounded out the top four.

Organizations Are Spending More on Detection

Most respondents (79%) had increased their spending on data breach detection over the past year. Of the five categories in the NIST Cybersecurity Framework—identify, protect, detect, respond, and recover—detection saw an almost universal increase in spending, followed by 76% for identification and response, 62% for protection, and 48% for recovery. None of the respondents decreased spending for identification and detection, while only one did so for protection and response. One-third (34%) left spending on recovery unchanged.

Risk Reduction is the Leading Measure for IT Security Investments

When we asked respondents how they measured the return on their IT security investments, 83% selected reducing risk based on metrics such as the number and frequency of security incident alerts or data breaches. Most (79%) selected improved detection capabilities such as fewer false positives. Nearly two-thirds (62%) cited the efficiency of incident response, 55% noted the frequency of incident identification, and 48% recognized the value of protecting their brand and reputation.

A Majority Think They're Spending Enough on IT Security

In characterizing their team's spending on IT security over the past two years, 17% of respondents called it "high," 52% described it as "sufficient," and 28% noted that it was "insufficient." Some reasons for insufficient spending included lack of senior support and change management challenges.

Introduction

The air of mystery surrounding cybersecurity is dissipating. What was once a technological tempest brewing uncertainty throughout the legal and business community is now a formidable familiarity. Yet while there are many solutions, there is no single answer. Many companies have developed response plans, protective policies, and advanced protocols. However, human behavior and technological uncertainty remain prominent barriers to corporate confidence.

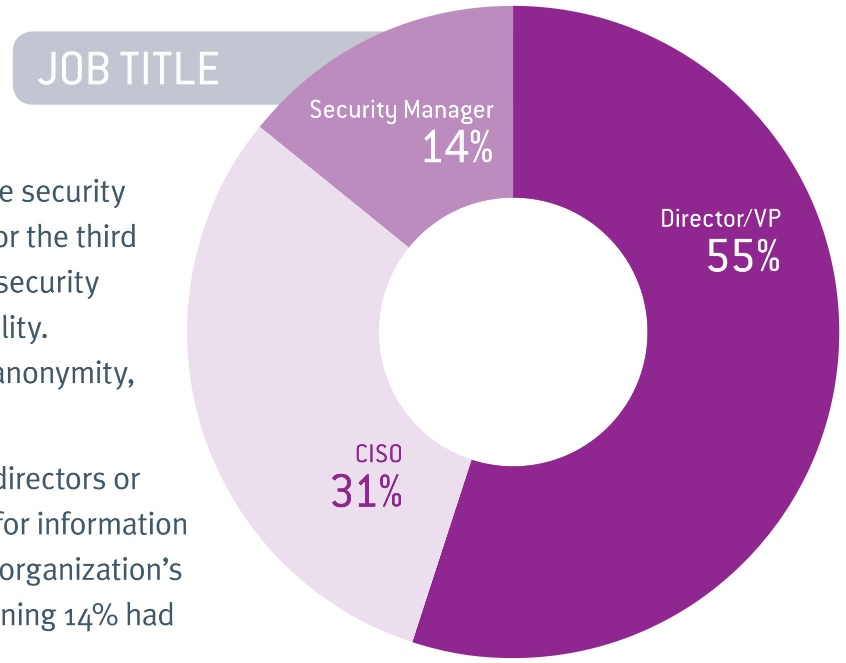
Security leaders who prepare, adapt, and respond, as well as maintain momentum in fighting those who try to access their networks fare better than their peers. The consensus is that everyone has been breached but what matters is the depth of that penetration and how long it takes to identify it.

In 2014, the first *Defending Data* report showcased general information protection trends, with a focus on guarding the perimeter and drafting policies. Last year, the 2015 study detailed the emerging insider threat phenomenon and the growing interest in security at the C-level.

In 2016, we detail the power of collaboration and its impact on spending, strategy, and systemic change. We also strive to provide clarity since “Everyone defines cybersecurity differently and has a different impression of what cybersecurity is,” according to Dr. Jim Kent, Nuix’s Global Head of Security & Intelligence.

The majority of respondents were from highly regulated industries. As a result, the perspectives included in this report reflected individuals who had a heightened sense of urgency associated with data protection and cybersecurity. Ari Kaplan also interviewed Dr. Jim Kent, the Global Head of Security & Intelligence for Nuix to balance the views of the survey participants.

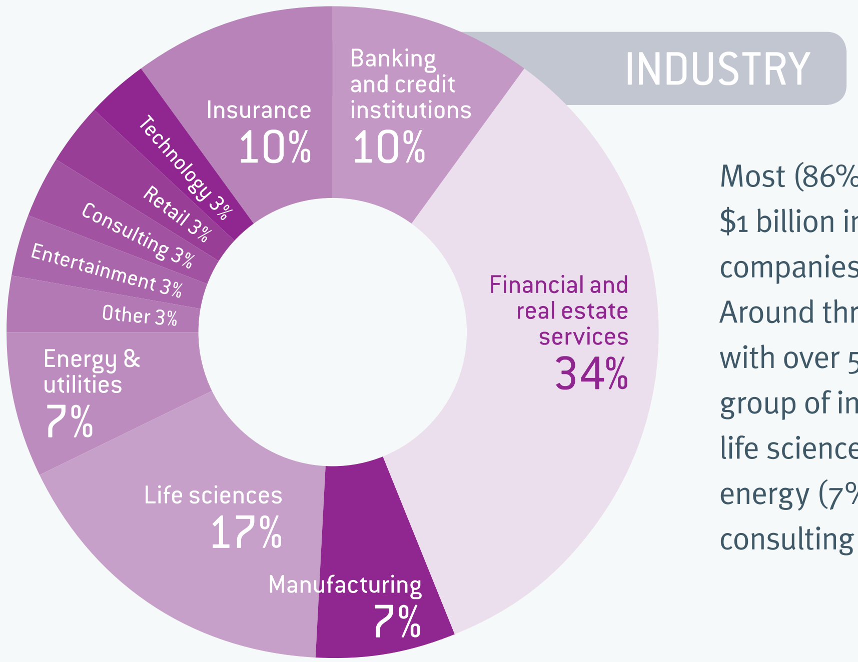
Survey Background



To track developments influencing corporate security tactics, Nuix engaged Ari Kaplan Advisors for the third consecutive year to interview 29 corporate security officials, with varying degrees of responsibility. All spoke by telephone, under condition of anonymity, between July and October of 2016.

More than half of respondents (55%) were directors or vice presidents with primary responsibility for information or cybersecurity, while 31% served as their organization’s chief information security officer. The remaining 14% had management oversight for those areas.

(Percentages may not add up to 100% due to rounding.)



Most (86%) were from organizations with over $1 billion in annual revenue and 69% are from companies with revenues more than $5 billion. Around three-quarters (72%) were from companies with over 5,000 employees. They hailed from a diverse group of industries, including financial services (34%); life sciences (17%); banking (10%); insurance (10%); energy (7%); manufacturing (7%); technology (3%); consulting (3%); retail (3%), and entertainment (3%).

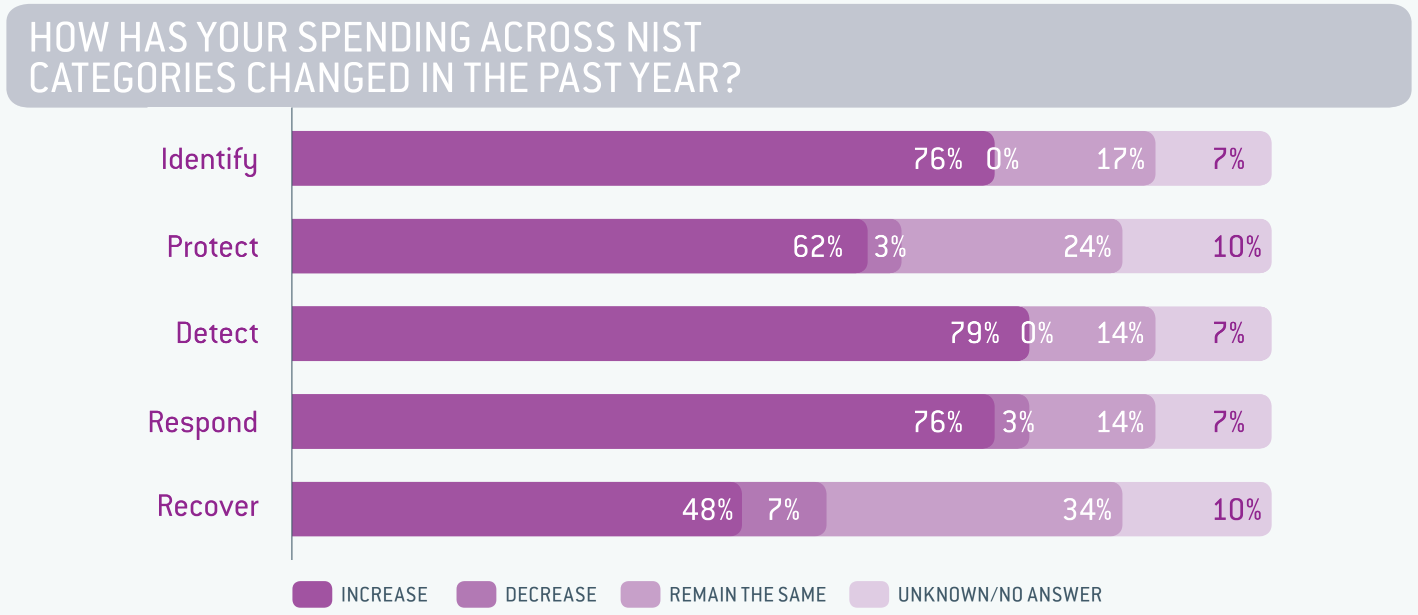
Spending Spotlights Detection and Risk Aversion

In past years, the *Defending Data* report focused on basic budgeting. Indeed, this was all that was possible in many cases; in 2014 that 46% of respondents did not know what proportion of their security budget was dedicated to managing and protecting the perimeter compared to incident response and remediation; in 2015, 39% still didn't know how their spending was apportioned.

In 2016, we asked respondents how they divided their spending among the five NIST Cybersecurity Framework categories—identify, protect, detect, respond, and recover—to offer a greater level of transparency.

Detection Spending is Highest

We found that detection received the highest investment over the past year; 79% of respondents said they were spending more in that area this year compared to last. Three-quarters (76%) had increased spending for identification and response, 62% for protection, and 48% for recovery. None of the respondents had decreased spending for identification and detection, while only one had done so for protection and response. One-third (34%) left spending on recovery unchanged.


HOW HAS YOUR SPENDING ACROSS NIST CATEGORIES CHANGED IN THE PAST YEAR?

"We have been more focused on where we can spend our time and money," advised one participant. "Now, it is about visibility and control; we have more focus on reacting quickly to what we have identified."

In fact, 97% of the software products they spent money on were in the detect, identify, and protect categories, and 97% of their IT security vendors were associated with threat detection. "You think about it and we have a tool that checks a tool, which checks a tool, whether they are gateways, alerts, and anything else," advised one respondent.

Regardless of how organizations allocate it, security spending continues to increase. "There has been a flat increase across the board," noted one respondent. "The scope of what is covered has increased as well, which equates to additional funding," explained another.

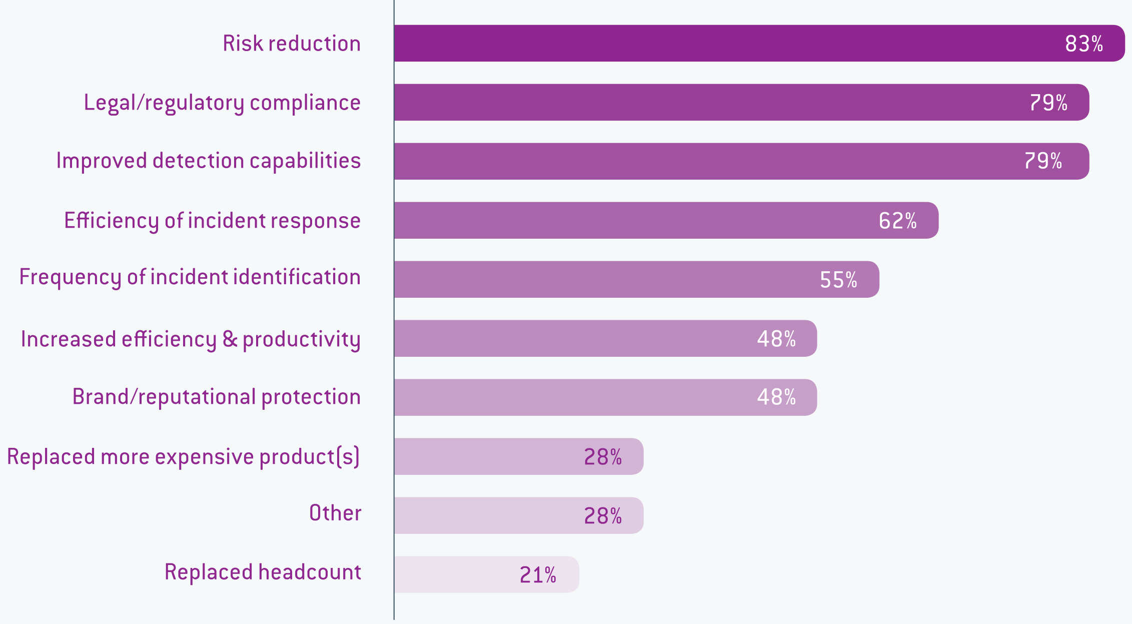
One participant described the new era as "threat hunting," noting that "Since the company is detecting and mitigating more frequently, it has to dedicate fewer resources in recovery; in addition, the cloud vendors are responsible for recovery, especially disaster recovery, and as they have that accountability, the company does not have to dedicate resources to it."

As more companies broaden their efforts, they are including behavioral analytics to better monitor their networks. "Security requires the protection and detection of the outer rim, including endpoint security, and recognizing the depth of the risk associated with offenders entering your infrastructure," says Kent. "The second half often starts the cybersecurity conversation."

Risk Reduction Drives Spending

When we asked respondents how they measured the return on their IT security investments, 83% selected reducing risk based on metrics such as the number and frequency of security incident alerts or data breaches. Most (79%) selected improved detection capabilities such as fewer false positives. Nearly two-thirds (62%) cited the efficiency of incident response, 55% noted the frequency of incident identification, and 48% recognized the value of protecting their brand and reputation.

HOW DO YOU MEASURE RETURN ON IT SECURITY INVESTMENT?



In fact, some respondents did not quantify the benefits of their investments at all. “The company does not measure profitability based on what it spends on infrastructure,” noted one participant. “We don’t measure the ROI on security spending because it is all seen as necessary insurance,” added another.

Most used some metric, however, to gauge their progress. “We show very clear associations between internal activities and a security occurrence,” remarked one security leader. “You are always looking for a cost-benefit analysis, but the key is to find a way to automate; when there are better tools on the market, it doesn’t necessarily reduce headcount, but increases performance and effectiveness,” echoed another.

Ultimately, it is about tracking and measuring. “Annually; it is based on the incidents detected and managed,” explained one respondent. “We have a very strong finance lead that works with the security team and has a very good understanding of what the team is spending and where.”

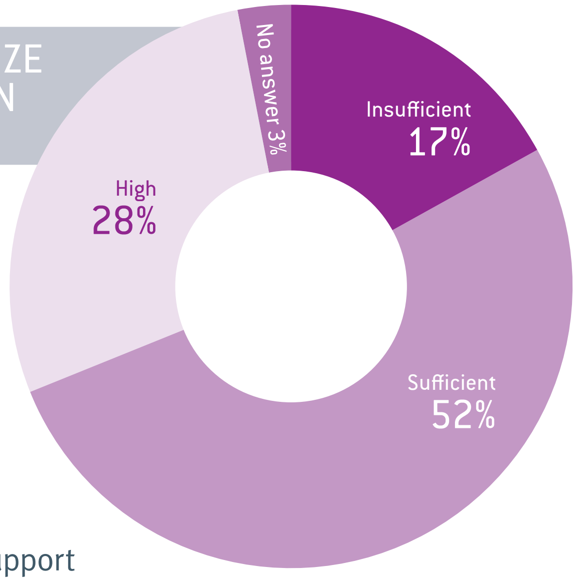
Respondents also recognize that technology has a limited life span. “You want to be on the venture capital side of security capabilities because well-established products are often defeated by [more] advanced tools,” advised one leader. “Lots of products overlap so some of the company’s metrics are used to decide whether to increase investments or remove products from their suite of tools,” added a colleague.

To begin to determine a return, you need a starting point. “The ROI is difficult unless you have an active baseline,” said one individual. “As we continue to mature, the efficiency becomes an issue in determining whether we are investing properly,” added another.

Most Think They’re Spending Enough

In characterizing their team’s spending on IT security over the past two years, 17% of respondents called it “high,” 52% described it as “sufficient,” and 28% noted that it was “insufficient.”

HOW WOULD YOU CHARACTERIZE YOUR IT SECURITY SPENDING IN THE PAST TWO YEARS?



“The question is whether what was previously sufficient is enough for tomorrow’s attack; it is an arms race,” remarked one security leader. “An argument could be that it is insufficient because we are not getting everything done in a single year, but it is sufficient because we are biting off as much as we can chew,” added another.

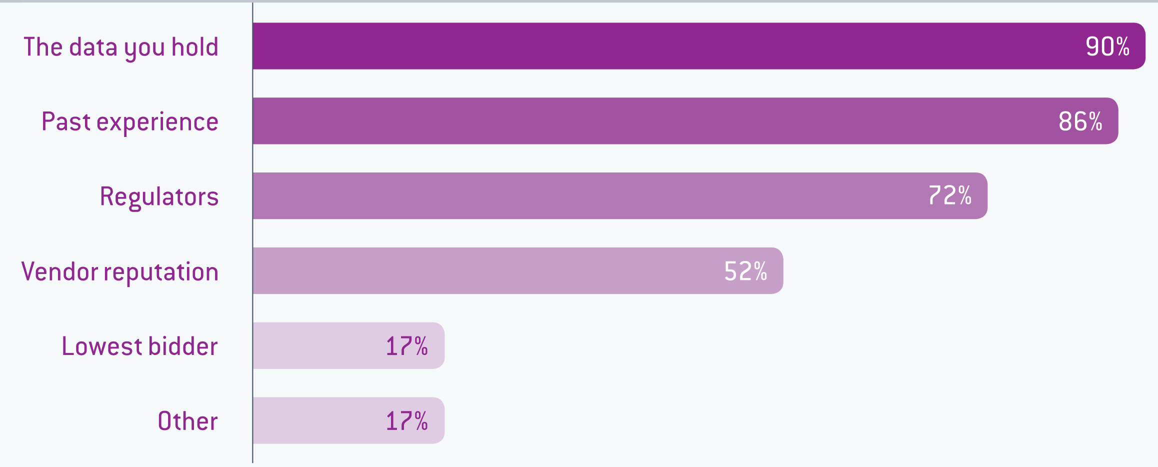
Some reasons for insufficient spending included a lack of senior support and initiative overload. “There is only so much change that our organization can absorb; we cannot take on any more projects at the moment,” noted one individual.

A participant summarized the issue: “There is no security program that is spending the appropriate resources that are required for the full security program unless you are at a Fortune five; that is why [my] company has moved toward the risk management framework.”

Regulatory Impact on Spending Is Increasing, But Not Highest

Over the past few years, regulators have increasingly impacted spending on security for the *Defending Data* respondents. In 2014, slightly less than a quarter of respondents said the regulatory environment was a major factor driving their spending decisions; in 2015 this was the case for more than half of respondents and in this year's report it was 72%. However, it was still not the most influential factor in this year's report; respondents said the data they held (90%) and past experience (86%) were the leading factors driving their decisions. Vendor reputation (52%) rounded out the top four.

WHAT DRIVES YOUR IT SECURITY BUDGETING DECISIONS?



"Reputational risk and harm are significant factors," said one participant, who echoed several others' concerns. "Everyone is waiting his or her turn to be Yahoo! and desperately hoping not to be on watch when it does happen," the individual added.

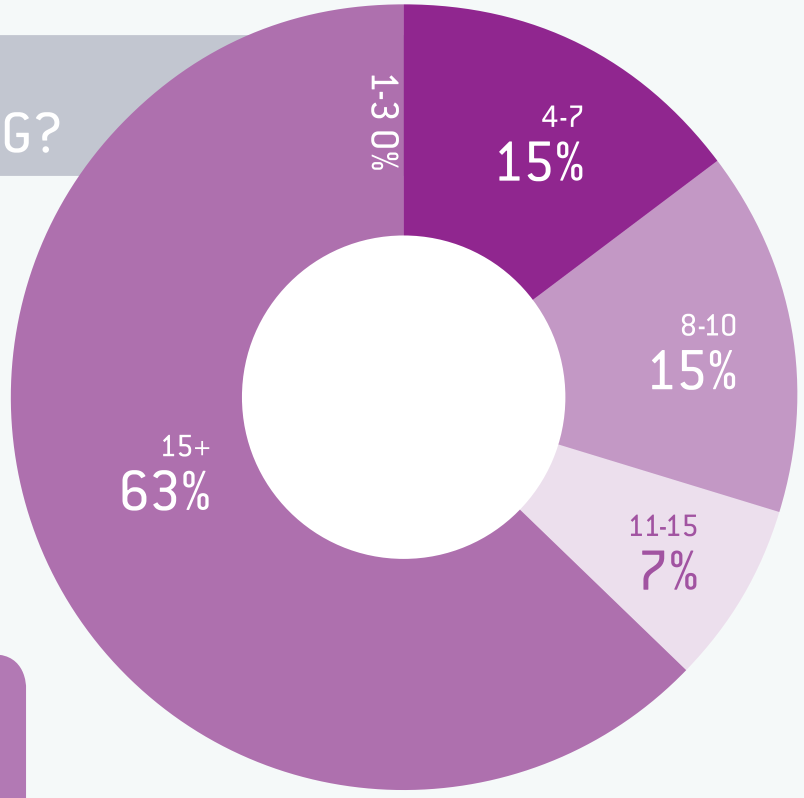
One senior leader reported that "we approach everything from a risk perspective and are scorecarding every new initiative, which is driving our budget. Another joked: "Never let a good breach go to waste; ride it out as long as you can to get the funding."

Regardless of the factors, "We are always trying to anticipate what is coming and stay ahead of the next big problem."

Technology Integration is a Challenge

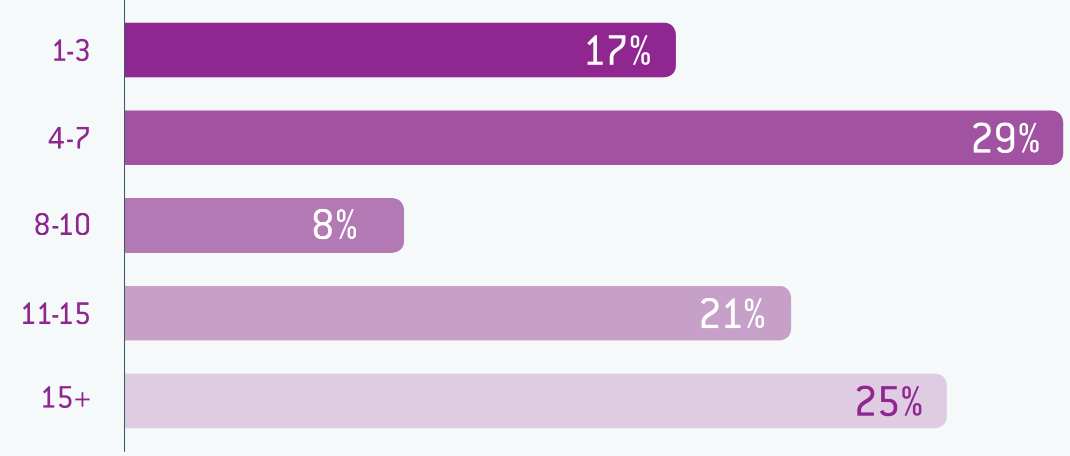
Two-thirds (66%) of survey participants said they used more than 10 software products and 38% worked with more than 10 service providers. Not surprisingly, the integration of the various vendors was generally a work in progress; only 24% described the integration between vendors as seamless. "Today, you can just switch vendors quickly if they are not working out," noted one security leader. "It is seamless, but it took some effort to get there; many out-of- the-box tools had technical limitations, which the company had to overcome," added another.

HOW MANY IT SECURITY PRODUCTS ARE YOU USING?



Regardless of the factors, "We are always trying to anticipate what is coming and stay ahead of the next big problem."

HOW MANY IT SECURITY VENDORS DO YOU CURRENTLY WORK WITH?



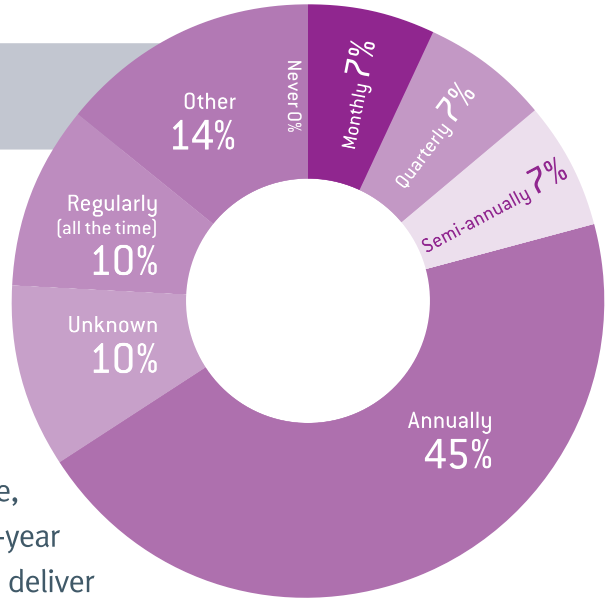
Although one participant explained that "Integration depends on the maturity of the vendor," the general consensus was that "Many of the vendors are not very seamless; sometimes there is overlap and no integration because they are all trying to compete against each other."

In fact, a few survey participants highlighted that they were planning to fully address this challenge in 2017. One explained "It is one of my nightmares; everyone wants to be proprietary and there is no open standard to ensure that a company's risk is managed properly across vendor offerings."

Given that 93% of respondents reported that their security workflow was partially automated, there is likely to be progress in this area in the next 18 months.

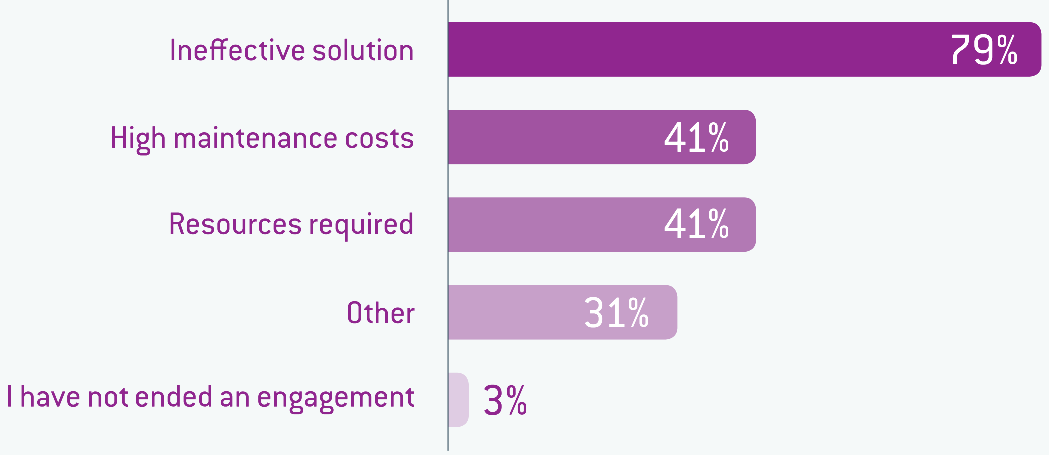
Security Vendors Must Continuously Prove Their Worth, But Clients Value Stability

HOW OFTEN DO YOU EVALUATE YOUR IT SECURITY VENDORS?



Although two-thirds of survey participants use more than 10 software tools and more than a third work with more than 10 vendors, less than half (45%) of respondents evaluate their IT vendors annually. Only 10% do so more than once a year. "The challenges are that technology changes so fast that one vendor may be appropriate now, but not a year from now," noted one participant. For that reason, "With respect to threat intelligence, because it is such a nascent thing, I refuse to sign more than a one-year deal so the vendor is evaluated multiple times per year; no one can deliver what they say they can deliver," added another respondent.

WHAT DRIVES YOU TO END YOUR ENGAGEMENT WITH A SECURITY VENDOR?



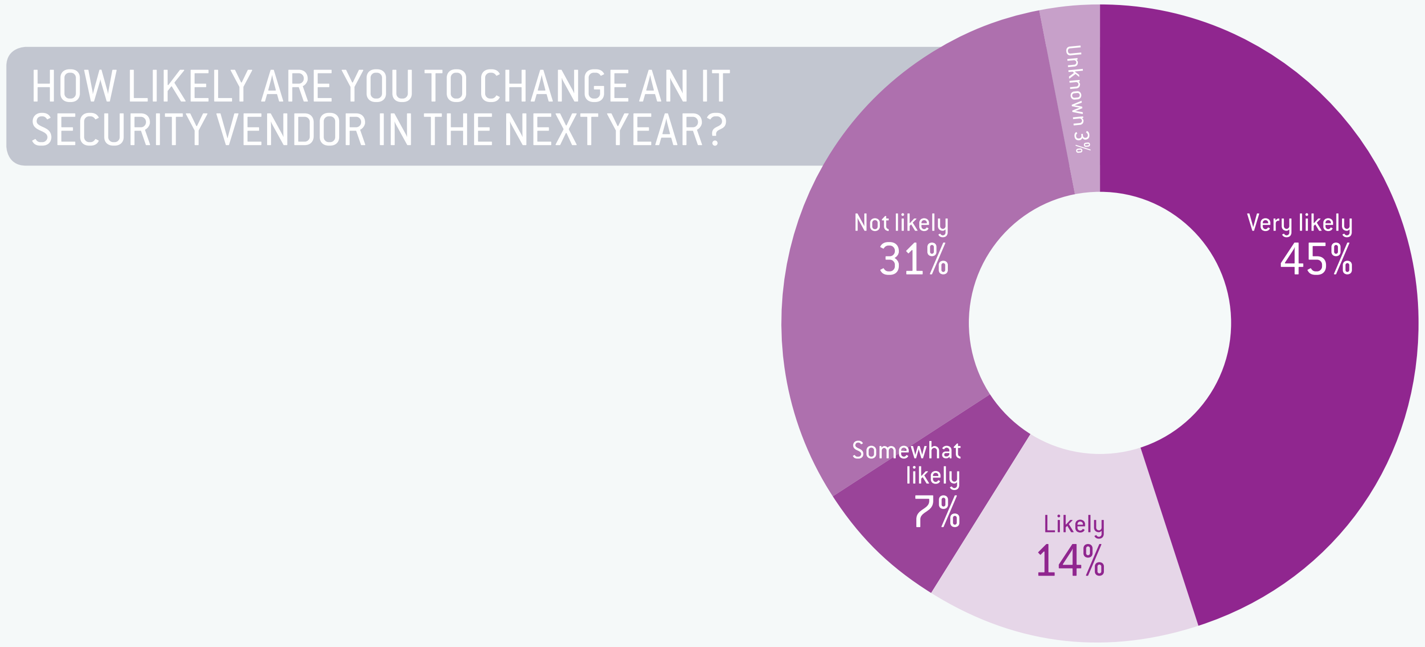
The overwhelming majority of respondents (79%) said an ineffective solution (bugs, limited capabilities, inability to meet specified needs, etc.) was most likely to drive them to end their engagement with a security vendor. High maintenance costs and the resources required were a distant second at 41%.

“Inadequate response in a crisis is the primary issue that has caused us to replace a vendor faster than anything else”

Innovation was also a key factor. “Vendors must adapt or die because they need to maintain pace with technology,” said one respondent. “If we find another product that can better meet our security needs, we will change the vendor” noted another.

In addition, support had a significant impact. “Inadequate response in a crisis is the primary issue that has caused us to replace a vendor faster than anything else,” reported a security leader. “If you have ineffective support, we will change the vendor; we don’t like high maintenance costs, but like ineffective support even less.”

In fact, almost half of the respondents (44%) said they were very likely to change an IT security vendor in the coming year, while 31% were unlikely to do so. “It is an ongoing process where we continually determine whether it meets our requirements,” said one participant. “Since we have so many vendors, there will always be a change,” another added more practically.

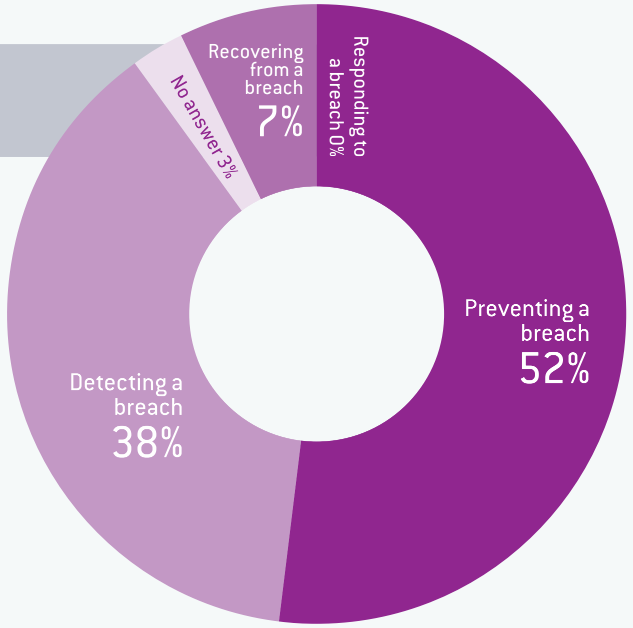


HOW LIKELY ARE YOU TO CHANGE AN IT SECURITY VENDOR IN THE NEXT YEAR?

The reality is that corporations have many options and they recognize the importance of consolidation. “Basic security services have become such a commodity so if one vendor cannot do the job, there are three lined up to help,” noted a respondent. “[My] company is in the process of consolidating around certain technology categories and we want to remove as much complexity out of our environment as we can,” added another.

Detection Gets More Money but Prevention is the Highest Priority

WHAT IS YOUR HIGHEST PRIORITY?

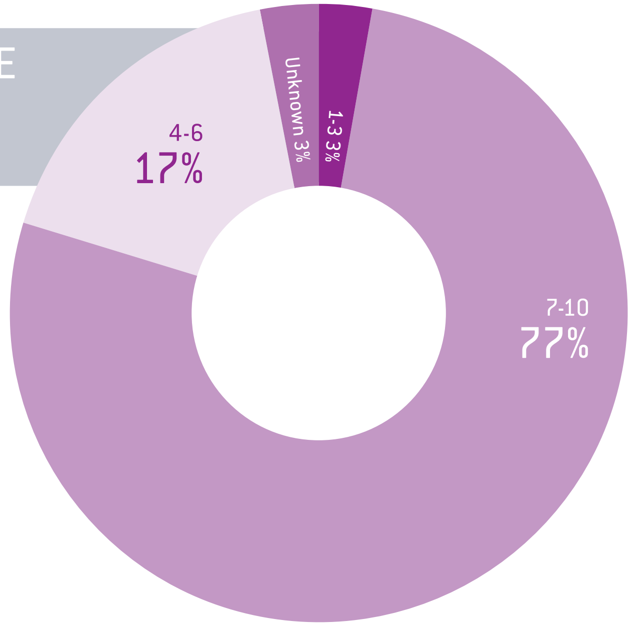


Although 79% of respondents increased their spending on detection last year (and 72% will do so next year), 52% said preventing data breaches was their top priority. Only 38% said detection was their primary focus, 7% cited recovery, and no one ranked response as their top choice. “Prevention should be first, but it is more ‘Whack-A-Mole’ so detection is often the top concern,” explained one leader.

> Ultimately, “Prevention is the most important because it negates the needs for the others, but the reality is that prevention is not always possible,” summarized one respondent. “Each is equally important and none is 100% possible.”

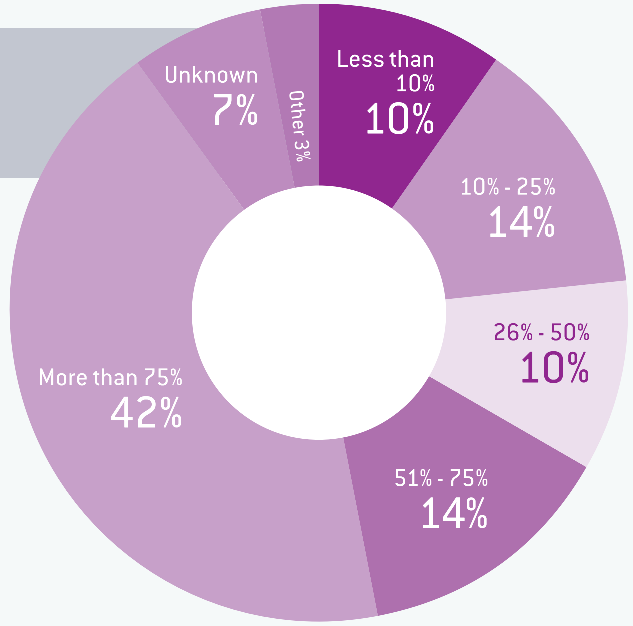
> “We operate on the premise that we have been breached, but this issue is whether the breach is disruptive,” said one participant. “The reality is that everyone has been breached, but some people choose to ignore it or are unaware,” added another. In fact, commented a third, “People who don’t realize they have been hacked have probably already been hacked.”

ON A SCALE OF 1-10, HOW WOULD YOU GAUGE YOUR ORGANIZATION’S ABILITY TO DETECT AND RESPOND TO A DATA BREACH?



Still, 77% of respondents rated their ability to detect and respond to a data breach at seven or higher (on a scale of one to 10). Almost half (41%) of respondents said they had the resources to follow up on or investigate more than 75% of their incoming alerts. “[My] company is putting a lot of emphasis on the ability to monitor and detect, and is building processes to respond quickly; I sleep well at night but there is always a risk because if someone wants to get in, they can get in,” said a respondent.

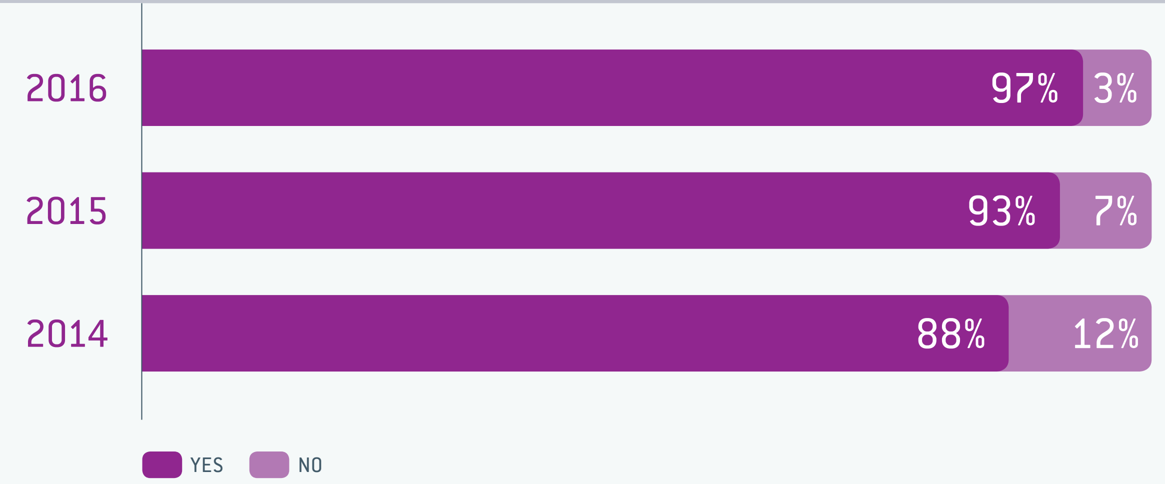
WHAT PERCENTAGE OF INCOMING ALERTS DO YOU HAVE THE RESOURCES TO INVESTIGATE?



Human Behavior Is Still a Paramount Concern

It was not surprising that 97% of participants said human behavior was the biggest security threat in their organizations. This was a slight increase over previous surveys—93% last year and 88% in 2014. Human vulnerability was the primary reason that 34% of survey participants described themselves as “very concerned” about whether they had been breached.

IS HUMAN BEHAVIOR THE BIGGEST SECURITY THREAT IN YOUR ORGANIZATION?



“The entire program is designed to account for human behavior; the company provides training to show individuals how to act and there are also policies in place to guide them,” said one participant. “Unless you train your staff to identify scams and avoid the risk, you will not eliminate security issues; education and awareness does not just rest with your internal staff, it rests with your customers as well.”

The respondents disagreed about the most effective way to change behavior. One participant noted that “performance reviews consider adherence to enterprise security policies and failure to adhere to them could result in termination or disciplinary action.” On the other hand, “The company tries to provide room for grace; if people are concerned about getting in trouble for making a mistake, they will not report to you,” countered another security leader.

“The company tries to provide room for grace; if people are concerned about getting in trouble for making a mistake, they will not report to you.”

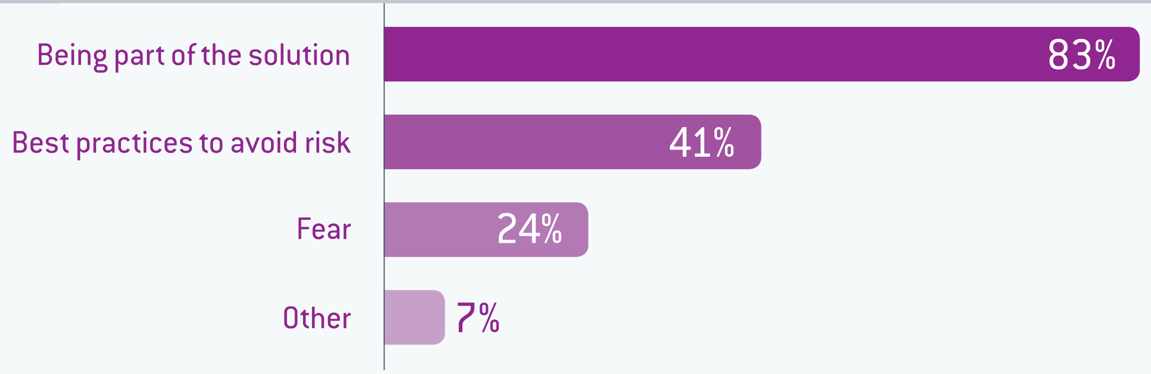
Meaningful Messaging Matters More Than Fear

Over the past few years, fear has been a common tool for communicating about security. "Human nature is such that we have an innate primal ability to respond to fear and perceive threats around us; messaging around that instinct is fairly effective because driving behavioral change exclusively around best practices is very difficult," reported one participant.

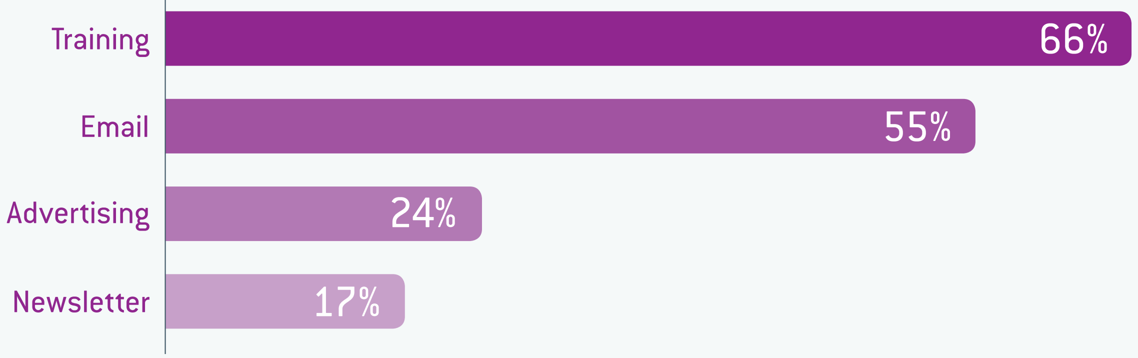
Last year, 39% of respondents chose fear over best practices to avoid risk in their security messaging, an increase from 31% in 2014. This year, only 24% used fear to convey key security ideas.

Instead, 83% of respondents encouraged employees to become part of the solution, while 41% employed best practices to avoid risk for this goal.

WHAT HAVE YOU FOUND TO BE THE MOST EFFECTIVE MESSAGING STRATEGY FOR EMPLOYEES?



HOW DO YOU COMMUNICATE TO EMPLOYEES ABOUT SECURITY?

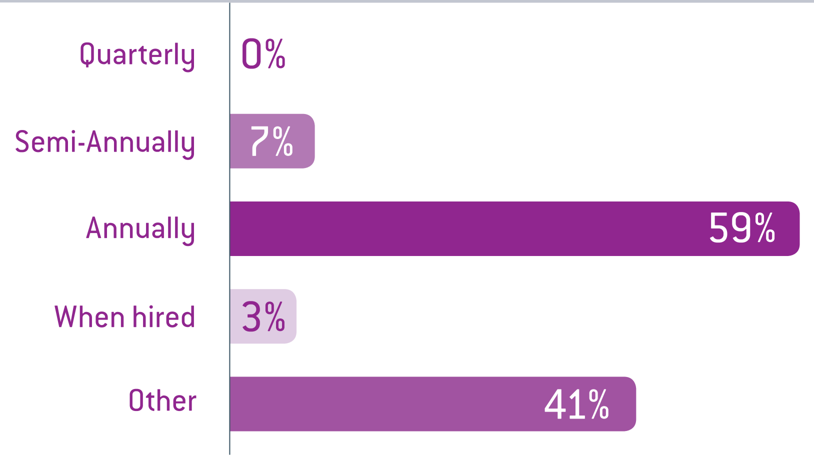


"Fear has gone away; we cannot use fear anymore, but being part of the solution is the new *en vogue* thing," said one participant. "Fear only goes so far; you get people who would ignore problems because they think the company is trying to scare them," notes another respondent.

Successful Organizations Put Policies Into Practice

Providing effective guidance is critical. Almost all respondents (93%) worked for an organization with a current data security policy and 61% of them revised their security policies annually. Three-quarters (76%) are required to read their security policies annually but 10% are never required to do so. Just under half (48%) of respondents had travel policies for senior executives and essential employees that accounted for cybersecurity concerns.

HOW OFTEN ARE EMPLOYEES REQUIRED TO READ YOUR SECURITY POLICY?

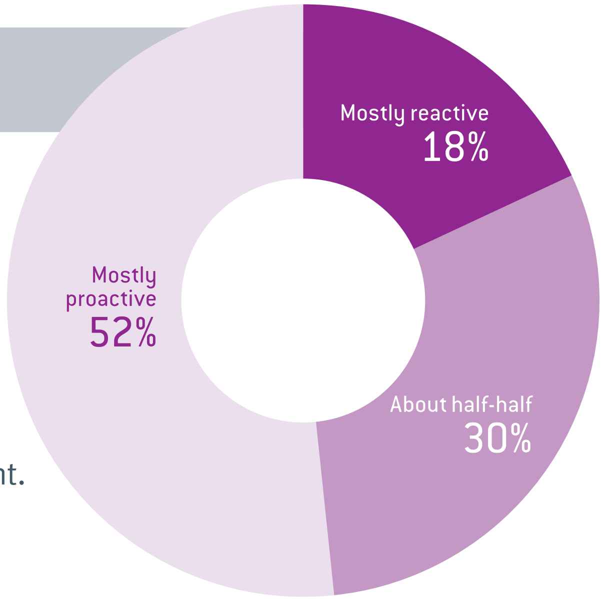


Everyone is upgrading their policies, but there are still challenges. "You can control the rule, but not the person," advised a participant. "I don't think that user education solves the problem, though it does provide a benefit; the combination of user awareness and detection increases security," added another.

Many of the respondents' employers:

- Celebrated cybersecurity awareness month
- Held annual training programs
- Provided monthly and quarterly updates
- Offered awareness training
- Tested employees with fake scenarios to determine how many individuals would click on a given link
- Mandated individualized education and enhanced testing at the user level
- Aligned information security with business units to impact behavior
- Implemented content monitoring and document classification controls for endpoints
- Studied how employees used tools to track anomalous behavior and identify incorrect access to sensitive data
- Prohibited Twitter internally because "The next big challenge will be Twitter links and I feel badly for organizations that allow them"
- Built ownership over individual security protocols because "technology cannot do it all"

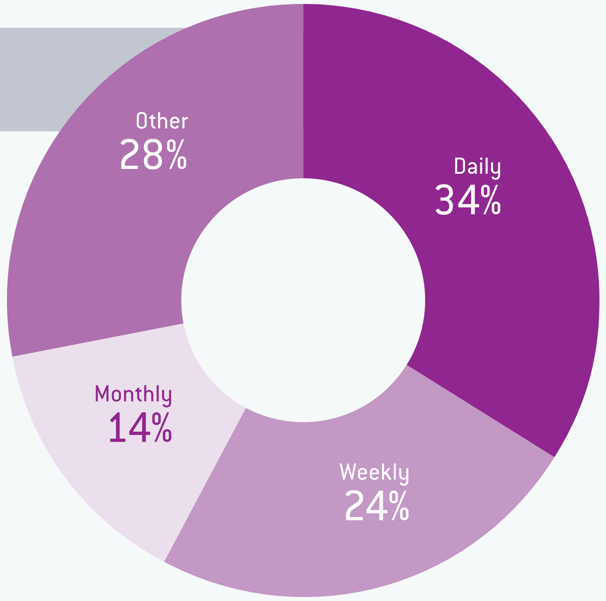
IS YOUR SECURITY STANCE REACTIVE OR PROACTIVE?



Policies have proliferated in the past year; 48% of respondents described their security stance as proactive, up from 29% a year ago. Only 17% said their actions were reactive, down from 29% in 2015. “It depends on the pillars under consideration; prevention and detection are proactive, while response and recovery are reactive,” said one participant.

Part of this shift may be the result of greater cooperation within corporations. Nearly half (45%) of respondents collaborated with other parts of the organization such as eDiscovery, in-house counsel, records management, information governance, and human resources daily, and 38% do so weekly. By contrast, only 25% interacted with their peers daily in 2015.

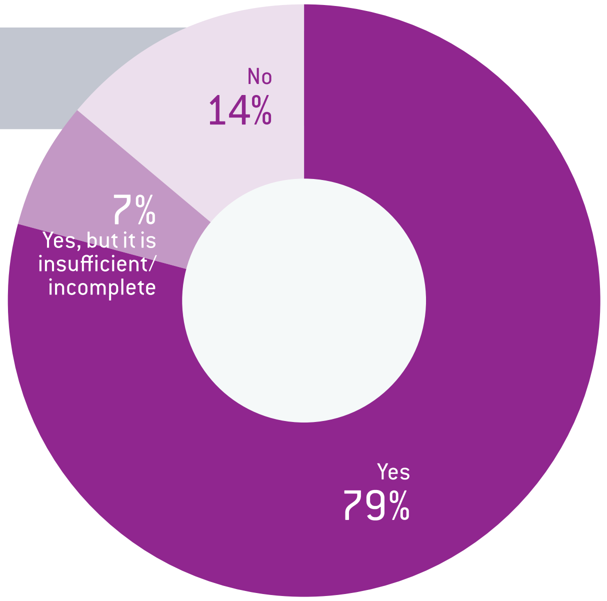
HOW OFTEN DO YOU COLLABORATE WITH OTHER PARTS OF THE ORGANIZATION?



BYOD Practice Continues to Expand

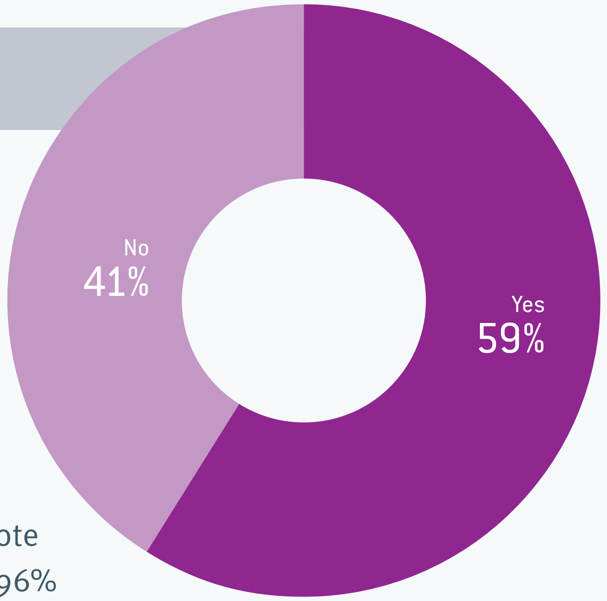
DOES YOUR ORGANIZATION HAVE BYOD POLICY?

Nearly all respondents (86%) reported having a bring-your-own-device (BYOD) policy, up from 82% last year and 69% in 2014. More than half (59%) believed those devices contained sensitive information.



DO BRING-YOUR-OWN DEVICES CONTAIN COMPANY-SENSITIVE INFORMATION?

“Many companies use a sandbox model, which does not save any information to the device; it deletes information once you close the sandbox,” remarked one official. “I don’t think the BYOD policy is strong enough to handle the situations that could arise from legal incidents,” countered another.

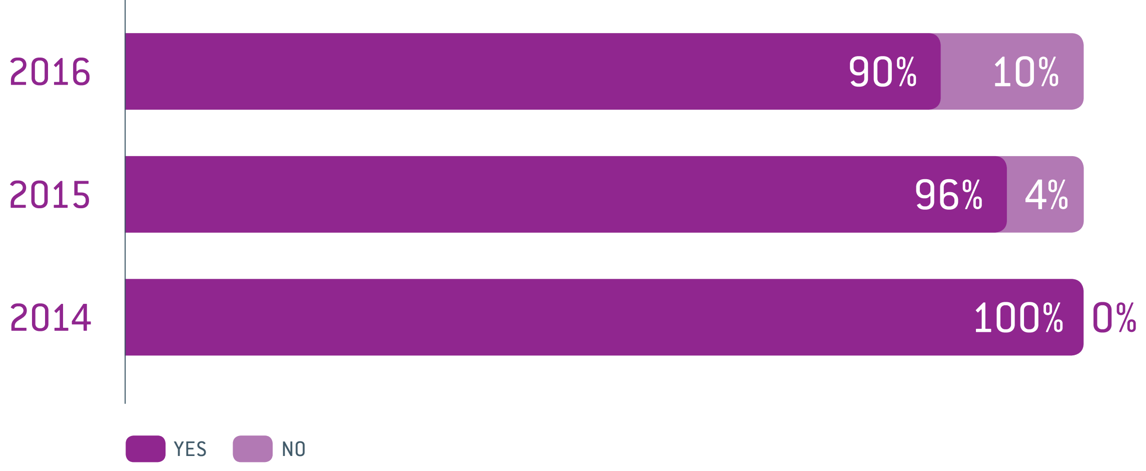


In addition, 97% of respondents’ employers permitted remote access, up from 86% in 2015 and more consistent with the 96% who allowed it in 2014. To build in stronger protections, 79% employed multi-factor authentication when doing so.

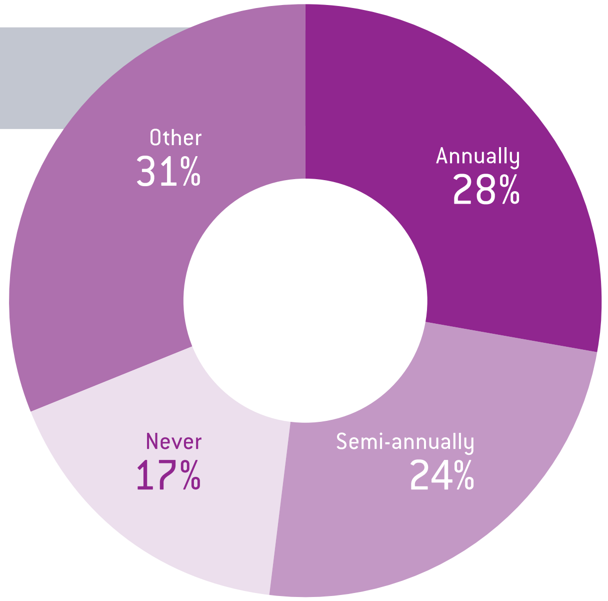
Incident Response Testing is on the Rise

Almost all respondents (90%) reported having an incident response plan, though that figure is down from 96% last year and 100% in 2014. That said, more organizations are evaluating their plans—28% of respondents said they tested their incident response programs annually, up from 18% a year ago; 24% did so twice a year, up from 21% in 2015. Surprisingly, 17% did not review their incident response plans at all.

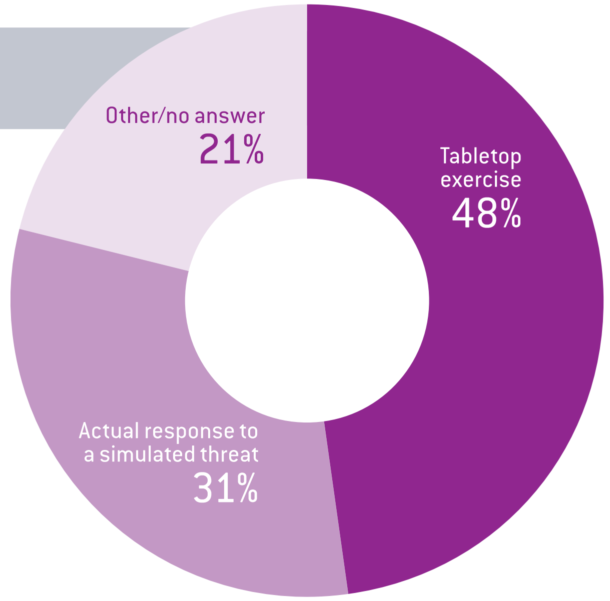
DOES YOUR ORGANIZATION HAVE AN INCIDENT RESPONSE PLAN?



HOW OFTEN DO YOU TEST YOUR INCIDENT RESPONSE PLAN?



HOW DO YOU TEST YOUR INCIDENT RESPONSE PLAN?



More than half (59%) of participants engaged in tabletop exercises this year, up significantly from the 36% who did so in 2015. Close to half (41%) promoted actual responses to simulated threats, which reflects a slight decrease from the 46% who did so in 2015.

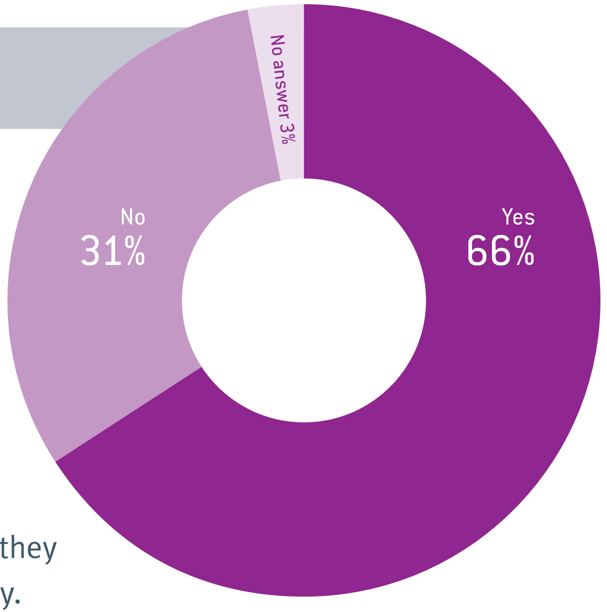
To ensure policy compliance, respondents' employers would:

- Study events and behavior outcomes
- Score individual investigations
- Measure different indicators to test proficiency and knowledge
- Measure the severity of data breaches
- Evaluate the number of potential incidents year-over-year
- Gauge employee understanding of security issues using testing tools and phish.me
- Provide random testing and computer-based training to assess familiarity with the concepts

Ultimately, "If the security team sees a large number of incidents in a given area, it investigates employee behavior and determines whether the policy was clear."

Insider Threats Remain Prevalent and Protections Are Powerful

DO YOU HAVE AN INSIDER THREAT PROGRAM OR POLICY?



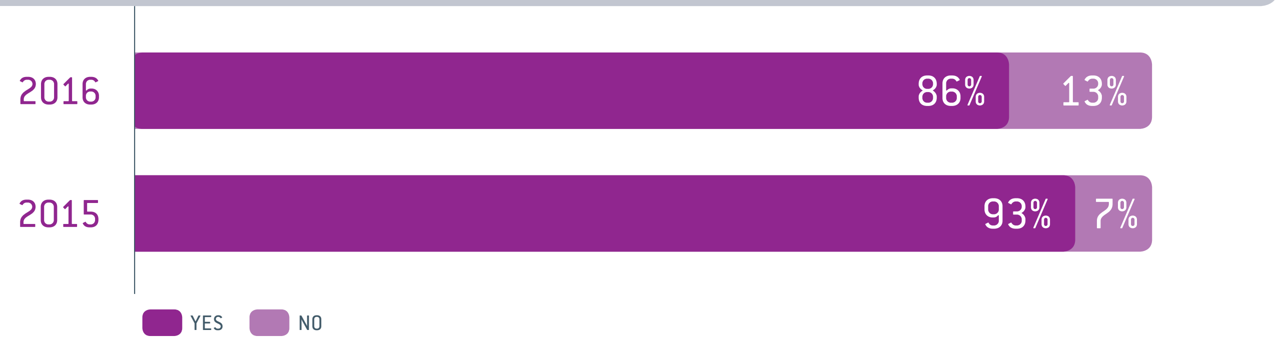
Two-thirds (66%) of respondents said they had an insider threat program or policy; 79% of those designated a senior official to oversee it and offered employee training. This reflects a decrease from the 71% of 2015 respondents with an insider threat program or policy, where 90% designated a senior official to provide oversight. Employee training, however, rose by nine percentage points over the past year. Three-quarters (74%) of respondents said they were required to report any perceived misconduct immediately.

One individual noted that *"It is difficult to ensure that people are doing what they are supposed to do."*

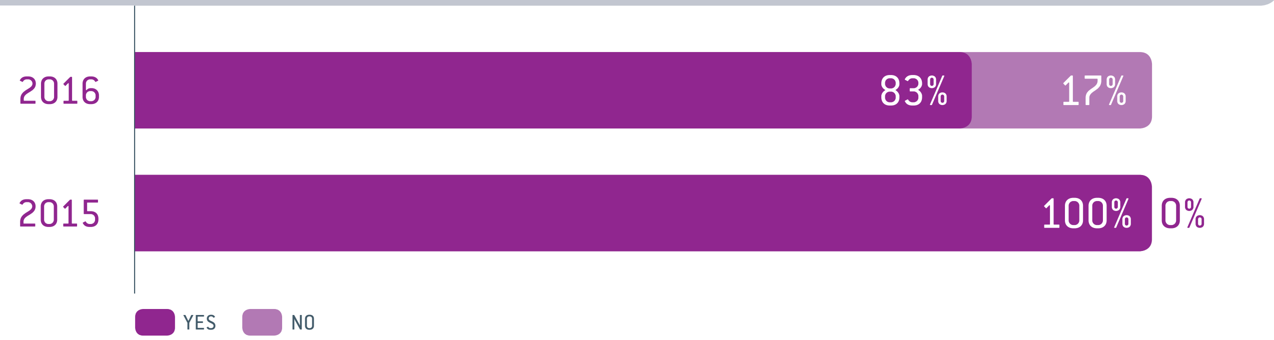
Insider Threat Tracking Techniques Are Evolving

While 86% of respondents said they could identify critical value data within their networks and 83% had the means to identify whom within their organization accessed that data, only 59% knew what people had done with the data after they had accessed it. A year ago, 69% of respondents claimed they could find out what had happened to their data, 93% could identify their critical value data, and 100% could detect who retrieved that data. This indicates a potential weakness in this area or perhaps a more realistic assessment of respondents' capabilities.

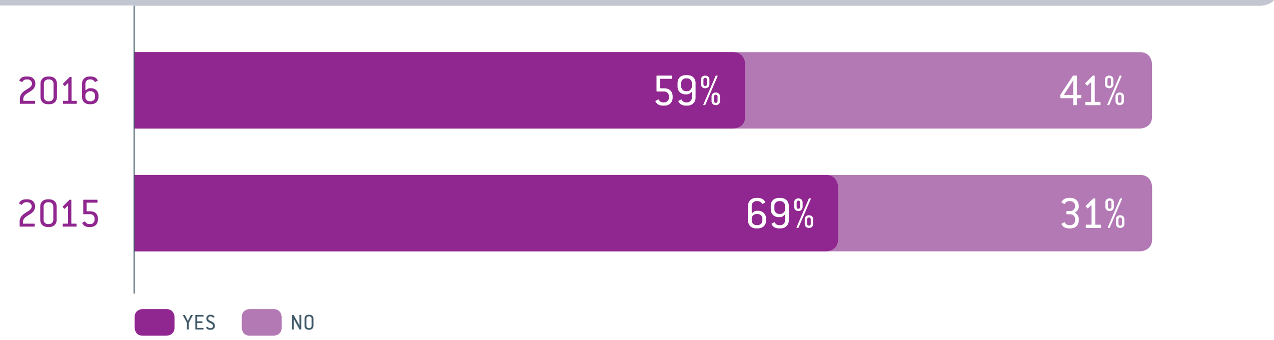
CAN YOU IDENTIFY CRITICAL VALUE DATA WITHIN YOUR NETWORK?



CAN YOU IDENTIFY WHO WITHIN YOUR ORGANIZATION ACCESSES THAT CRITICAL VALUE DATA?



DO YOU KNOW WHAT PEOPLE DO WITH THE CRITICAL VALUE DATA AFTER THEY ACCESS IT?

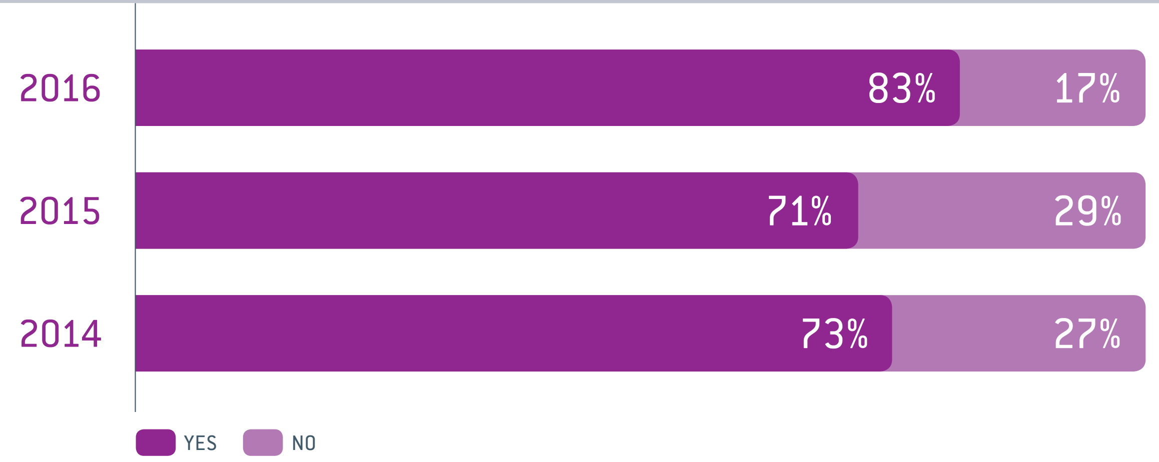


"We know when they grab it and what they do with it, but there is always a vector of unknown; for example, if someone takes a picture of a document on a screen, the security team has no way of knowing about that," acknowledged one participant. "I'm not naïve enough to think that it is perfect," added another.

Security Leaders Are More Comfortable With the Cloud

Consistent with market trends, 83% of respondents' employers had migrated data to the cloud, up from 71% did so last year and 73% in 2014. Around a third (31%) used the cloud for non-confidential data such as marketing, advertising, and creative artwork, and 28% had their email in the cloud. "When CISOs say that they don't like using the cloud, they are acting a bit two-faced because the most widely used vulnerability management tool is in the cloud," remarked one security leader.

HAS YOUR ORGANIZATION MIGRATED DATA TO THE CLOUD?



More than half (62%) of respondents cited cost as a key factor for leveraging the cloud, while 29% acknowledged its convenience and flexibility. Only 21% cited security as a factor in their decision to use or avoid the cloud. "It is more cost-effective, offers greater flexibility, and permits the enterprise to scale," said one participant. "The cloud provides cost, convenience, functionality, support, and reliability; it will all be cloud one day," added another.

Despite the general enthusiasm for the cloud, however, not everyone is convinced. "I don't trust the cloud and neither does the CIO," said one security leader. "The company is currently discussing it, but is concerned about the lack of visibility into a product since we cannot relinquish responsibility for data protection," added another.

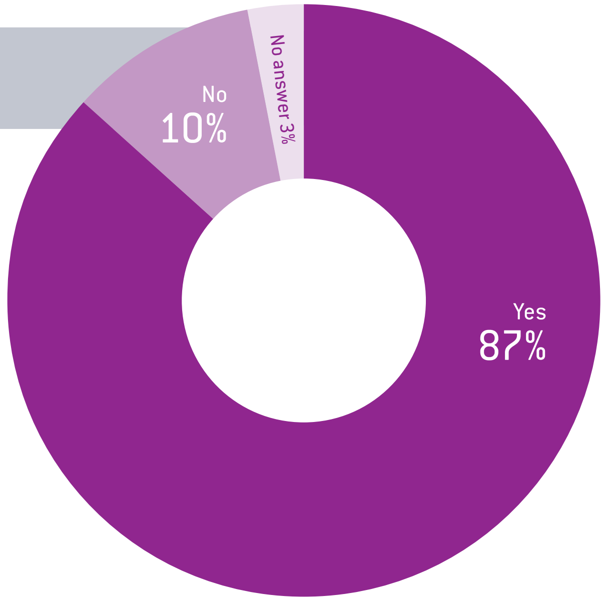
Still, 83% said they had migrated systems to the cloud, including email (24%), financial management (21%), and marketing (14%). This is a sharp increase from the 43% of respondents that had migrated systems to the cloud in 2015 and the 58% that had done so in 2014. The motivating factors for migrating certain systems to the cloud were the same as for data; 42% of respondents cited cost-control while 31% noted its flexibility and convenience. Only 17% raised the issue of security.

"Depending on who you are sharing it with, it will limit the ability to perform internal forensics," noted one participant. "The cloud provider has more sophisticated security than the company," countered another.

Cloud Concerns Persist Despite Broader Adoption

The enthusiasm aside, 86% of respondents said the cloud created unique cybersecurity concerns, which is consistent with our two previous surveys. The most common concern was a lack of control (31%) while 21% of respondents highlighted challenges accessing their organization's data. Other challenges include data management and privacy.

DOES THE CLOUD CREATE UNIQUE CYBERSECURITY CONCERNS?



"When you have internal procedures and compliance protocols there is never 100% confidence that cloud vendors will adhere to those procedures and protocols; this includes concerns about privacy," said one participant. "Disposal of data in the cloud can be difficult, particularly if you encrypt data," added another.

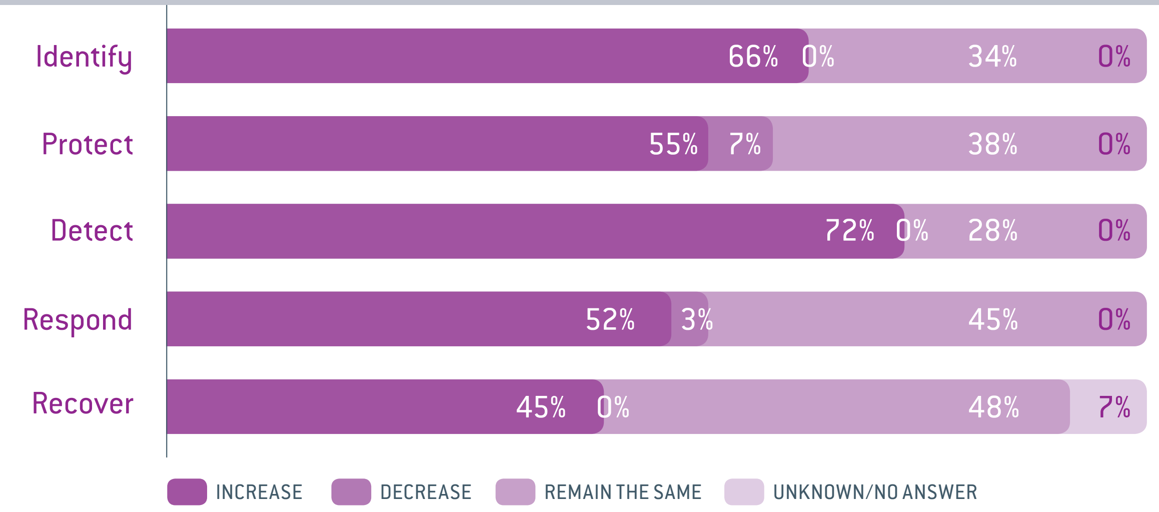
Overall, the cloud presents a challenge of alignment between the customer and the provider. "We are trusting outside entities to protect our content; as much as we insist on a level of security, we still need to depend on people whose stake is not as large as that of the company," remarked one respondent. "When you release control to a cloud provider, there is anxiety about whether you can access data when you need it and if the provider's sense of urgency is aligned with that of the company," said another.

Key concerns include:

- Losing visibility into the management of your data
- Being at the mercy of the cloud entity's data hygiene practices
- Reducing access control
- Creating confusion about what happens when the government wants an inspection
- Lacking sufficient regulatory compliance
- Varying cloud providers
- Operating in a shared environment.

Looking Forward to 2017

HOW DO YOU EXPECT YOUR SPENDING ACROSS NIST CATEGORIES TO CHANGE IN THE COMING YEAR?



Future Spending Will Increase, But Possibly Slower Than in the Past

Although spending will continue to increase, many companies have already made a significant investment in their security infrastructure so that uptick may be less dramatic than in past years. Nearly three-quarters (72%) of respondents planned to increase their spending on detection next year, followed by 66% for identification, 55% for protection, 52% for response, and 45% for recovery. None of the respondents expected to decrease spending next year on identification, detection, or recovery; only one planned to do so for response and two for protection. Around half (48%) planned to leave spending on recovery unchanged.

"[My] company has implemented a lot of security measures in the past two years so we have everything in place that we need," said one security leader citing a common theme.

Still, "[Our spending on 'identify'] will definitely increase due to the [European Union General Data Protection Regulation] and the various regulations that challenge companies to know where client data is and what type of data it is," said one respondent. In addition, another noted: "Where we are seeing increasing spending is on insider threat; it will be some form of user behavior analytics and collecting additional log sources." As a result, "Ideally response will remain low because you are doing such a good job of identifying and detecting," added a third.

Regardless of which NIST category will receive the most spending next year, many respondents are trying to stay ahead of potential problems. "We are looking at improving the efficiency of patching and hardening our system, but it is like painting the George Washington Bridge because as soon as we are done patching, we are starting to patch again; the soft cost of losing productivity from security issues is tremendous."

One participant noted the influence of the cloud on future spending. "As [my] company moves more data into the cloud, the identification of the bad material is becoming a lot more complex so I expect the identification of threats will increase."

Companies Will Align Their Data Security Policies With Their Training Initiatives

Although 93% of respondents' employers had a current data security policy, only 76% required employees to read that policy annually and 10% did not impose any responsibility to do so. In contrast, 66% of employers conveyed security messaging through regular training. As these programs evolve and expand, companies are likely to organically integrate policy provisions so that employees become more familiar with specific obligations while learning how to apply proven techniques to implement to them.

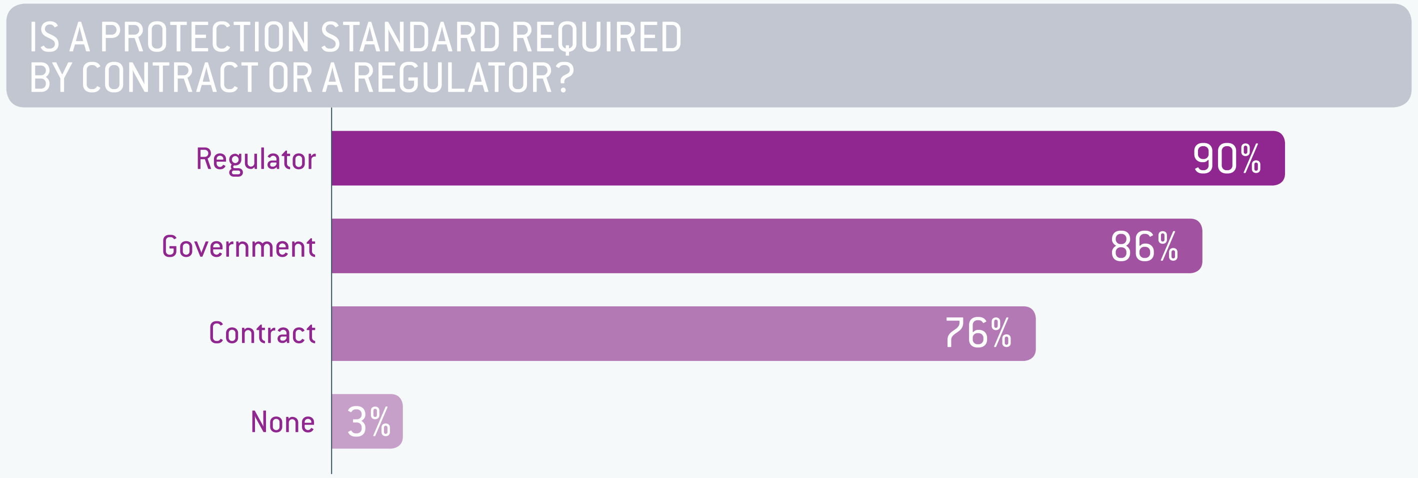
Collaboration Between Departments, Security Leaders, and Law Enforcement Will Increase and Create a More Proactive Environment

After a substantial increase in security leaders describing their efforts as "mostly proactive" and a similar reduction in those who characterized their actions as "mostly reactive," there is a shift occurring. Organizations are anticipating security challenges and responding with greater speed and effectiveness. Given the corresponding increase in collaboration among leaders within corporations (45% of respondents said they collaborated with other parts of their organizations every day) and in the broader community (93% of respondents shared and collaborated with information security executives outside of their offices), this trend is likely to continue.

"This includes law enforcement because you are starting to see the rise of cyber-defense alliances," noted one survey participant. "It is not about intellectual property or competitive advantage; it is that we are all fighting a common enemy; cyber-defense alliance programs permit sharing intelligence."

Cloud Usage Will Reach a Tipping Point of Acceptance

With 83% of respondents working for companies that have migrated data and systems to the cloud, it is likely that this trend toward widespread adoption will continue, particularly as regulatory agencies become more comfortable with the cloud. For most survey participants, a data protection standard is required by a regulator (90%), the government (86%), or contract (76%). In addition, when there is a litigation or regulatory event, 38% of companies review the data they are producing in advance to ensure that it does not contain sensitive or confidential content. All of these factors, which will impact increased usage of the cloud for review and overall data management.



Security Decision-Making is Officially a C-Suite Concern

Compliance was by far the most important issue driving respondents' decision-making; 93% cited it as an influential factor. Other factors included brand reputation (79%), budgets, and executive directives (both 69%). "Cybersecurity has become a board-level discussion; the audit committees are regularly looking at it and there is research that showcases the best technology," said one security leader. "Ultimately, cybersecurity means protecting the perimeter, knowing where your critical value data is, and protecting the inside; the reason they have always been separate is because we haven't had technology to align them."

Nuix

Nuix protects, informs, and empowers society in the knowledge age. Leading organizations around the world turn to Nuix when they need fast, accurate answers for investigation, cybersecurity incident response, insider threats, litigation, regulation, privacy, risk management, and other essential challenges.

Nuix makes small work of big data volumes and complex file formats. Our solutions combine advanced technology with the extensive knowledge of our global team of industry experts. We bring data to life with clarity and intelligence to solve critical business problems, reduce crime, and secure and manage information.

North America
USA: +1 877 470 6849

» Email: sales@nuix.com

EMEA
UK: +44 207 877 0300

» Web: nuix.com

APAC
Australia: +61 2 9280 0699

» Twitter: @nuix

nuix
Simple. Powerful. Precise.