A SANS Survey

Spends and Trends: SANS 2020 IT Cybersecurity Spending Survey

Written by **Barbara Filkins**
Advisor: **John Pescatore**

January 2020

Sponsored by:
ExtraHop

Analyst Program

Executive Summary

The total volume of spending on cybersecurity is interesting to economists and venture capitalists, but that statistic provides little value to CISOs and security operations managers. They need information about where their security peers are planning to increase or decrease investment. SANS' interviews with boards of directors have highlighted this lack of data: Board members cite the lack of such benchmarking data when CISOs present security statuses and strategic plans. To address this need, SANS conducted a targeted cybersecurity spending survey, focused on specific areas where CISOs and security managers plan to change their spending patterns.

The leading drivers for security spending are regulatory compliance, reducing incidents and breaches, and keeping up with the evolving threat landscape. These, however, only partially address the factors that respondents feel are the most disruptive to their security program. See Table 1.

Table 1. Leading Disrupters/Leading Areas to Increase Spending

Rank	Leading Disrupter	Spending Increase Emphasis
1	Increased use of public cloud infrastructure-as-a-service (IaaS) and hybrid cloud	Cloud security monitoring
2	New threats from threat actors	Network detection and response tools
3	Emerging privacy/security legislation (e.g., GDPR)	Staff skills training
4	Inability to acquire and/or maintain security-related workforce	Staff skills training

Respondents overwhelmingly prioritize improvement in staff (headcount and skills) over adding new security technologies to existing architectures. There is a realization that new tools, even if they promote future efficiencies, require skilled people to select, configure and implement them. Even if enough staff time can be freed from day-to-day firefighting, staff skills are required to test, evaluate and implement new security technologies.

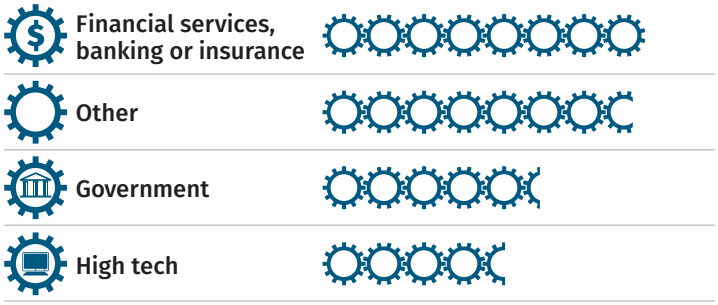
To remedy this, several things must happen. Security plans and budgets should be aligned with those of other departments—such as DevOps, the network operations center (NOC) and quality assurance (QA)—and not remain a stepchild of IT-centric spending. Only 30% of surveyed organizations have been able to accomplish this. Even more worrisome, close to 70% do not evaluate the effectiveness of their security spending, leaving CISOs and their staffs unable to justify needed expenditures to corporate management.

This paper lays the groundwork for potential improvements to help organizations match their security spend to key trends.

Survey Demographics

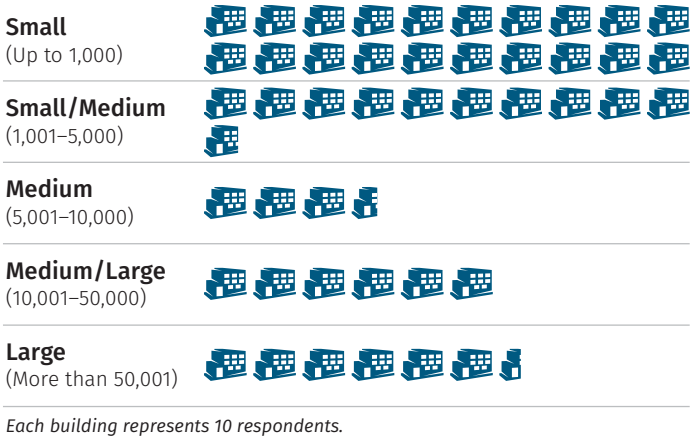
More than 450 people participated in the survey. As illustrated in Figure 1, the respondent population for this survey is oriented toward management (security and IT) as planned, with a slight tilt to financial organizations and smaller North American companies.

Top 4 Industries Represented



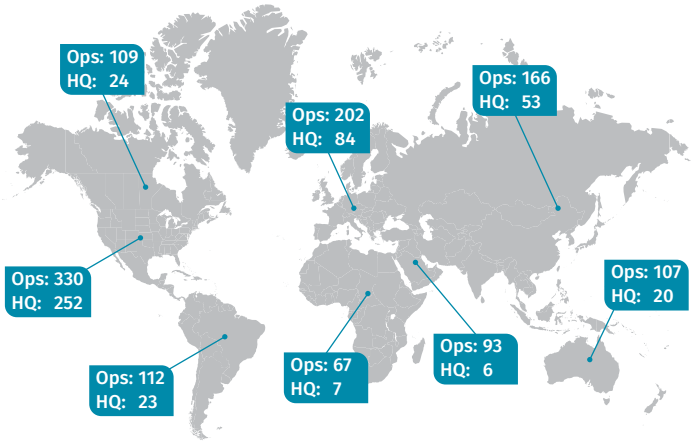
Each gear represents 10 respondents.

Organizational Size

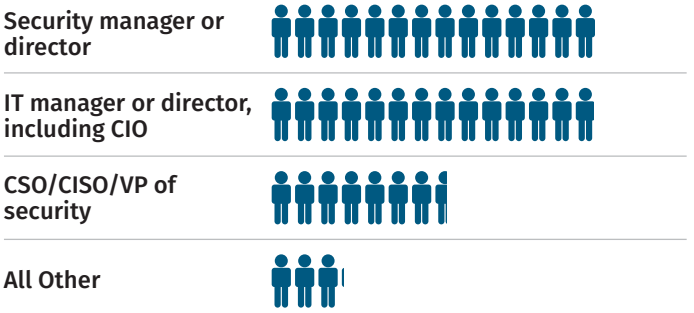


Each building represents 10 respondents.

Operations and Headquarters



Top 4 Roles Represented



Each person represents 10 respondents.

Figure 1. Key Demographic Information

In this survey, SANS concentrated on those roles that would have a hand in the development of security-focused IT budgets. Table 2 shows the resulting array of management positions, compared with all other nonmanagement roles.

In looking at the distribution of these roles while also considering company size, as shown in Figure 2 on the next page, we see that for smaller companies (i.e., 1,000 or fewer workforce members), the IT management role dominates. Smaller companies traditionally have a weak (or no) CISO role. Keep this low-end bias in mind as we examine the survey results.

Table 2. Management Roles Represented

Security manager or director	29.9%
IT manager or director, including CIO	29.6%
CSO/CISO/VP of security	16.2%
All other	24.3%

Driving the Trends

Regulatory compliance leads as the most significant factor driving organizations' current spending on cybersecurity, followed somewhat distantly by two factors that could be considered prevention. The impact of the increasingly large fines levied by the European General Data Protection Regulation (GDPR) and the California Consumer Privacy Act of 2018 (CCPA) is the likely driver behind this. Respondents, however, emphasize reducing incidents and breaches over keeping up with the evolving threat landscape, indicating a more reactive than proactive approach to cybersecurity (see Table 3).

Table 3. Leading Factors for Cybersecurity Spending

Driver	Percent Response
Regulatory compliance	69.4%
Reducing incidents and breaches	59.1%
Keeping up with the evolving threat landscape	56.9%
Maintaining our reputation in our industry sector	42.9%
Investigating and responding to security events and incidents	40.0%
Maintaining adequate security staffing and skills	39.0%
Protection of our intellectual property (IP)	33.7%
External events impacting other organizations in our industry sector	27.4%
Company financial performance or overall economic conditions	26.0%
Incidents and breaches that have occurred at our partners	20.8%

Interestingly, maintaining adequate security staffing and skills does not lead in driving security spending, although this factor definitely emerges when looking at disruptive factors. This could be because employee headcount and salaries are often seen as a separate process from budgeting, and training budgets are often allocated based on headcount.

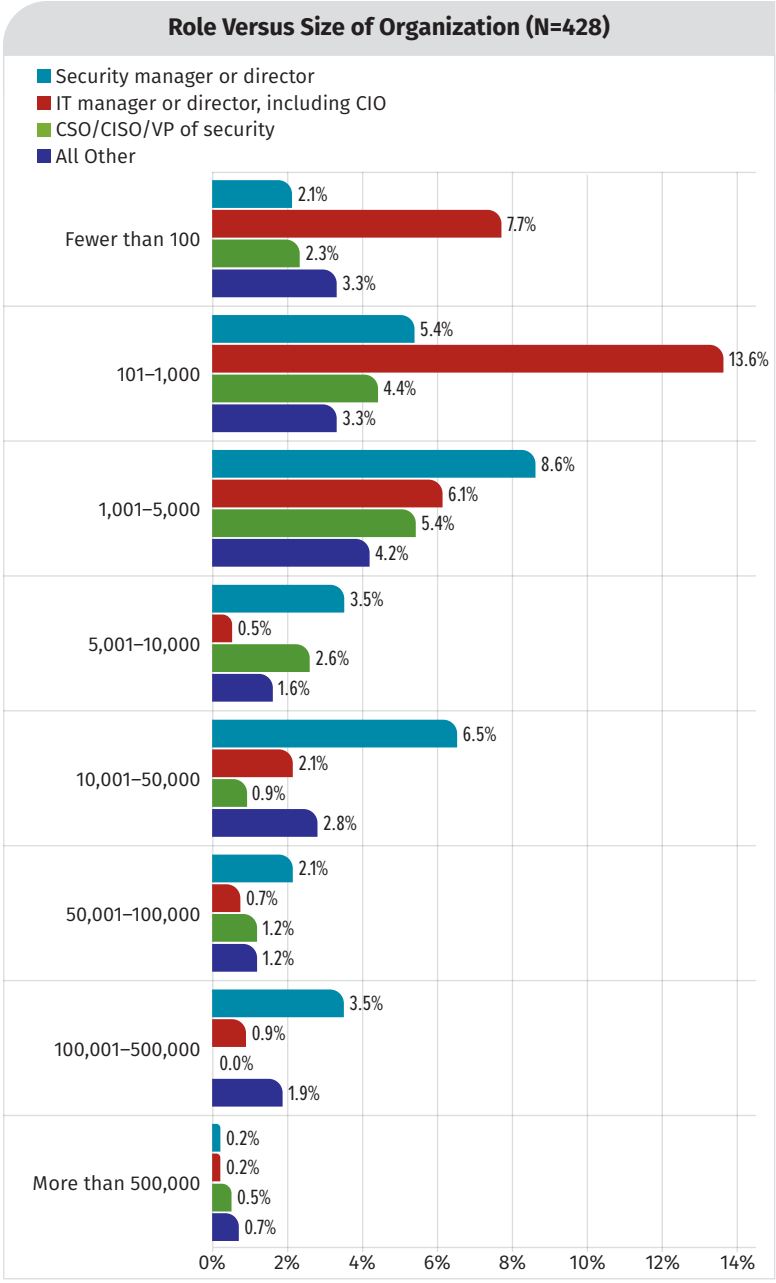


Figure 2. Role vs. Organization Size

Disruption: A Spending Point of View

Respondents consider the following as the four leading factors (noted earlier in Table 1) causing or potentially causing the most disruption to their security program in the next 12 months:

- Increased use of public cloud IaaS and hybrid cloud
- New threats from threat actors
- Emerging privacy/security legislation (e.g., GDPR)
- Inability to acquire and/or maintain security-related workforce

This ranking was generated by a weighted average for each factor based on whether a respondent felt that the factor represented the largest, the second largest or the third largest disruption. For each factor, we also captured the percentage that reported the factor as the largest disrupter.

For each of these disruptive factors, we asked respondents to rate how they saw their spending change—increase, decrease or stay the same—across several areas of technology, managed services and staff (both in headcount and skills). In all cases, decreases in spending were small (10% or less) and increases were offset by a change in "stay the same." Therefore, for the subsequent discussion we will focus on areas of increased spending.

Cloud: The Biggest Disrupter

Slightly more than 50% of respondents ranked increased use of public cloud IaaS and hybrid cloud as the largest disrupter. The movement of production workloads to IaaS has had two major and distinct impacts on traditional security operations:

- Traditional methods of security visibility and control across servers in customer-premised data centers must be extended into the virtual IaaS environment, or new methods of security visibility and control must be developed.
- The elasticity of IaaS services has allowed IT to move to rapid Continuous Integration/Continuous Delivery (CI/CD) DevOps methodologies. Security processes and controls have to be re-architected to keep up with the pace of change.

The resulting increases in overall spending are in the areas of cloud security monitoring, followed by cloud access security broker (CASB) technology, with staff skills training a close third. Across the board,

> *"Management perceived incorrectly that the cloud was inherently safe, since we have moved services such as mail off-premises we have had a large increase in phishing and [spearphishing], our attack surface has expanded dramatically, and we now need to increase our monitoring budgets accordingly."*
>
> —Survey respondent

increasing the headcount is not nearly as critical as training current staff to learn new skills. See Table 4.

Table 4. Spending Increase Trends for Use of Public Cloud Infrastructure

Technology	Overall	All Security Management	CISO	IT Management
Cloud security monitoring	70.9%	77.7%	74.4%	67.1%
Cloud access security broker CASB cloud-specific tools	52.6%	58.9%	56.4%	48.6%
Staff skills training	52.2%	53.6%	51.3%	52.9%
Strong authentication	45.7%	49.1%	69.2%	44.3%
Network detection and response tools	38.3%	35.7%	38.5%	42.9%
Data encryption	32.2%	31.3%	43.6%	34.3%
Managed services	30.4%	28.6%	17.9%	34.3%
Threat hunting	29.6%	39.3%	43.6%	24.3%
Endpoint detection and response (EDR)	27.8%	33.0%	35.9%	21.4%
Web security gateway	27.8%	25.0%	20.5%	25.7%
Security orchestration, automation and response (SOAR) tools	27.0%	32.1%	38.5%	24.3%
Endpoint protection platform	25.2%	23.2%	17.9%	22.9%
Network IPS IDS	24.3%	20.5%	33.3%	31.4%
Staff headcount	24.3%	29.5%	33.3%	15.7%
Network firewalls	23.5%	19.6%	25.6%	24.3%

The fact that respondents prioritize increasing staff skills significantly over increasing headcount to deal with the impact of IaaS is not surprising. Business use of IaaS and hybrid cloud requires re-architecting security controls and integrating with CI/CD methodologies. Skilled security staff can do so while minimizing headcount growth. Security managers recognize the need for "upskilling" to increase both effectiveness and efficiency.

What is interesting, however, is that while CISOs agree on the importance of cloud security monitoring, they emphasize the importance of strong authentication, this group's second leading choice. The fact that monitoring is rated so much more highly is recognition of the continuing obstacles to persuading IT and corporate management to require strong authentication to be used across the user population.

TAKEAWAY

Don't underestimate the cost of moving to the cloud, both initially and ongoing. It also requires some reorientation of your budget, because cloud services follow different accounting rules than on-premises architectures. More specifically, you will see a shift from the capital costs from owning assets (CAPEX) to operating costs (OPEX). Project your budgeting out a year or so to truly evaluate the total cost of ownership in moving to the cloud.

Effective Measures for New Threats from Threat Actors

Close to 40% of respondents consider new threats from threat actors to be the leading disruptive factor to their security program. The three leading related areas that show increased spending across all respondents are: network detection and response tools, staff skills training, and endpoint detection and response (EDR), followed closely by threat hunting. See Table 5.

Table 5. Spending Increase Trends for New Threats from Threat Actors

Technology	Overall	All Security Management	CISO	IT Management
Network detection and response tools	50.5%	51.9%	56.8%	49.4%
Staff skills training	50.0%	51.0%	54.1%	54.5%
Endpoint detection and response (EDR)	49.1%	60.6%	59.5%	35.1%
Threat hunting	48.2%	52.9%	59.5%	39.0%
Strong authentication	43.2%	46.2%	13.5%	42.9%
Endpoint protection platform	40.1%	42.3%	37.8%	36.4%
Network IPS IDS	36.5%	32.7%	35.1%	39.0%
Network firewalls	29.3%	26.9%	24.3%	29.9%
Cloud security monitoring	28.4%	29.8%	27.0%	28.6%
Data encryption	27.9%	26.9%	32.4%	31.2%
Staff headcount	26.6%	32.7%	24.3%	19.5%
Web security gateway	25.7%	27.9%	29.7%	24.7%
Managed services	23.4%	26.0%	16.2%	28.6%
Security orchestration, automation and response (SOAR) tools	21.6%	29.8%	35.1%	15.6%
Cloud access security broker (CASB) cloud-specific tools	15.8%	20.2%	13.5%	13.0%

Security management is looking for increased spending at the endpoints for detection and response, while IT emphasizes skills training and network-based tools. This likely represents the fact that security staff understand the benefits of deep visibility on the endpoint, while IT staff typically don't have the security expertise to make use of that visibility and also bear the brunt of user complaints about false positives and other impacts from "yet another security agent" on the endpoints.

TAKEAWAY

Spending for new threats cannot just be about budgeting for new technologies. Take into account that your organization could be unable to move off its legacy platforms in a timely manner. Security budgets should include those less-glamorous line items that often get overlooked: maintaining cyber hygiene for your older platforms, upskilling for your current workforce, and the incorporation of automated asset inventory tools to establish a solid configuration baseline for existing infrastructure.

Privacy Emerging: Impacts for Security?

Privacy demands can be considered as the business rules for security, especially in industries such as finance/banking and healthcare. With new regulations such as GDPR and the CCPA, it is not surprising that close to 30% of respondents consider emerging privacy/security legislation the leading disruptive factor to their security program. Overall, survey respondents highlighted staff skills training, data encryption and strong authentication as key areas for increased spending to address emerging privacy and security legislation. See Table 6.

Table 6. Spending Increase Trends for Emerging Privacy/Security Legislation

Technology	Overall	All Security Management	CISO	IT Management
Staff skills training	53.7%	56.1%	53.8%	45.5%
Data encryption	49.6%	47.4%	46.2%	54.5%
Strong authentication	46.3%	52.6%	61.5%	48.5%
Cloud security monitoring	39.8%	52.6%	53.8%	27.3%
Network detection and response tools	34.1%	36.8%	42.3%	33.3%
Staff headcount	29.3%	33.3%	46.2%	9.1%
Endpoint detection and response (EDR)	28.5%	35.1%	38.5%	18.2%
Endpoint protection platform	28.5%	29.8%	26.9%	21.2%
Threat hunting	24.4%	26.3%	30.8%	12.1%
Cloud access security broker (CASB) cloud-specific tools	22.8%	35.1%	34.6%	6.1%
Network IPS IDS	18.7%	12.3%	11.5%	27.3%
Web security gateway	17.9%	21.1%	19.2%	15.2%
Managed services	16.3%	17.5%	19.2%	12.1%
Security orchestration, automation and response (SOAR) tools	16.3%	22.8%	38.5%	9.1%
Network firewalls	13.8%	8.8%	7.7%	18.2%

Not surprisingly, staff skills training is the overall leading factor for increased spending. Individuals responsible for security must understand the requirements inherent in new legislation, and security professionals are not always as conversant with the privacy domain as might be required by emerging compliance demands.

Interestingly, CISOs emphasize spending for authentication and cloud security monitoring, strongly suggestive of increased focus on use of the cloud for systems that contain sensitive information. Here, it appears they are also emphasizing increasing staff headcount, buying domain knowledge as well as training for it.

On the other hand, IT management focusses on increased spending for data encryption, possibly because that is often the first line of defense requested by corporate management, even though effectively applying encryption to protect sensitive data is often not well understood.

"We are currently constrained, from a financial perspective, having to make the best of what we have got. Getting improved technology would certainly give us improved security posture, but we aren't in a position to roll out more at this stage."

—Survey respondent

In the long run, any use of data encryption will be owned and operated by IT operations, with security in an oversight role or perhaps controlling key management. The fact that IT teams with security responsibility prioritize encryption is a positive sign—CISOs need to work on convincing CIOs and IT architects to follow this lead and also prioritize encryption, applying it in accordance with how the data is being used (e.g., the process of encrypting data at rest in a database is not the same as for data in motion between two network endpoints).

TAKEAWAY

Try to build good security practices in the processes you use to handle your organizational data, especially data that is critical or sensitive. Start with a hard look at how you classify data, including the information derived from it. Then look at the processes involved: how various types are handled, transported, stored and processed. Finally, review the exposure and evaluate what methods are best for protection—encryption might not be the best option (even though called for by regulatory compliance). At this point, you can budget for the solution, taking into account people, process and technology.

Security Workforce: High Demand, Short Supply

The fourth disruptive factor comes as no surprise: the inability to acquire and/or maintain a security-related workforce. Slightly more than 30% consider this the leading factor for their organization. Table 7 shows that training trumps hiring and that the preference is for staff as opposed to outsourcing for managed services. Again, we see the leading emphasis that our IT management respondents place on staff skills training. See Table 7.

Table 7. Spending Increase Trends for Security Workforce

Technology	Overall	All Security Management	CISO	IT Management
Staff skills training	62.5%	66.2%	69.6%	64.6%
Staff headcount	49.3%	57.7%	60.9%	35.4%
Managed services	26.4%	23.9%	26.1%	29.2%
Endpoint detection and response (EDR)	22.2%	22.5%	21.7%	27.1%
Threat hunting	22.2%	21.1%	30.4%	27.1%
Cloud security monitoring	18.8%	14.1%	13.0%	27.1%
Security orchestration, automation and response (SOAR) tools	18.1%	19.7%	26.1%	20.8%
Strong authentication	16.7%	19.7%	26.1%	14.6%
Network detection and response tools	16.0%	15.5%	21.7%	20.8%
Endpoint protection platform	15.3%	15.5%	17.4%	16.7%
Network firewalls	11.1%	8.5%	17.4%	12.5%
Network IPS IDS	11.1%	11.3%	21.7%	8.3%
Data encryption	11.1%	14.1%	21.7%	10.4%
Cloud access security broker (CASB) cloud-specific tools	8.3%	8.5%	13.0%	10.4%
Web security gateway	6.9%	7.0%	13.0%	10.4%

"We need to commit funds to continuous training, in addition to [Continuous Integration (CI)/ Continuous Delivery (CD)]. The technology we use is not static; we should have no expectation that the threats we face will remain static. I do what I can to keep informed, but there is no substitute for a dedicated training experience."

—Survey respondent

TAKEAWAY

According to a respondent, "security training is getting more and more expensive and fewer companies are comfortable with investing so much money on training these personnel who could leave in the thriving job-market." However, in the SANS security operations center (SOC) survey, interviews with SOC managers showed that teams that invested in staff training—which included the ability for security operations staff to configure and use open source security tools as well as commercial products—had lower attrition rates. Security professionals are less likely to change companies and chase higher salaries when they are engaged, versus simply staring at a vendor's management screen all day.

Investment in training should be viewed as more than just having your staff acquire needed skills. Investment in quality training is considered to be a job perk by many professionals, and it can go a long way to both attracting to and retaining a quality workforce in your organization.

In the End: People Rule

Overall, 57% of respondents feel that the people arm of people, process and technology is the one general category where increased investment would provide the biggest improvement to their overall security posture, followed distantly by process (19%) and technology (18%). They also know that organizational issues or other barriers will prevent that change from taking place.

Of course, all surveys involve people—it is not surprising that people rate people as the highest priority! There is no such thing as a security program that is effective without people, but no company can afford the inefficiencies of a program that doesn't have strong processes and "force multiplication" technologies. But, in today's "gig economy" corporate management often sees increases in full-time staff as the last resort.

Table 8. How Respondents Would Allocate Additional Security Budget

Projected Allocation of Funds	Percentage
Add more staff	32.7%
Add new security technologies to the architecture	17.8%
Train existing staff	14.6%
Refine existing processes	10.8%
Upgrade existing security technologies	7.3%
Acquire additional managed or other external security services	6.2%
No change; allocate the funds according to our existing security spending profile	3.8%
Develop new processes	3.8%

We asked respondents, "If your management suddenly gave you a $200K or a 10% increase in your security budget (whichever is larger)—but you could apply the funds in only one area—where would you spend it?" Respondents overwhelmingly want to add more staff as opposed to investing in new technologies such as security orchestration, automation and response (SOAR). See Table 8.

Adding new technologies to your architecture requires investment to get started, dollars that are often not adequately budgeted for. For example, let's take security automation, part of SOAR. The truth here is that you can't automate something you don't already know how to do. Automation allows you to be more efficient and work at scale, but first you must have a combination of people and processes that are effective against real-world threats and under the particular constraints and demands of your business environment. This is the part of security that takes a tremendous amount of effort to arrive at the point where automation makes things look easy. According to the SANS 2019 survey on automation and integration, direct factors influencing investment decisions around automation include: budget and management support along with staffing concerns, for example, the overall number of staff and how the required skills are being acquired and/or kept current through training and certification. In short, a decision to automate should include a review of and justification for staff training and additional hires if deemed necessary.[1]

> *"Don't underestimate the resources needed to define the processes—in the light of more effective tools—and close the semantic gaps in the data gathered. Effective automation depends on the integration of people, process and technology."*[2]

[1] "2019 SANS Automation and Integration Survey," March 2019, www.sans.org/reading-room/whitepapers/analyst/2019-automation-integration-survey-38852, p. 10. [Registration required.]

[2] 2019 SANS Automation and Integration Survey," March 2019, www.sans.org/reading-room/whitepapers/analyst/2019-automation-integration-survey-38852, p. 3. [Registration required.]

Spending on newer technologies such as SOAR may also need a champion, one who believes in the positive effects of change and can overcome any inertia that may limit efforts to improve. One respondent expressed the thought: "We currently have a lot of human-based processes and are very reluctant to change. Increased spending in investment here would certainly help, but old habits die hard."

Using Your Security Budget Wisely

We are hearing more and more about developing a culture of security, but organizations need to consider a different allocation of dollars to accomplish this goal. An integrated security budget must align with an organization's mission/purpose much more than when it is included in the IT budget. In developing an integrated security budget, start with initiatives that provide common benefit to, for example, both security operations and development. Such initiatives ensure that both sides buy into the proposed budget and plan on nurturing these joint objectives with a clear understanding of how the dollars are being spent.

The need for security embedded in the daily workflows of the organization is there:

"We can buy tools all day, and we can teach people all day, but until we ingrain the security into the day-to-day business processes and make those processes incapable of being executed or completed [by] bypassing security measures, people will continue to do the easy thing because it's easy. I don't advocate for interrupting business or stopping daily work. I do advocate for changing how it is done. Thirty seconds spent today could save 30 days spent next month."

—Survey respondent

But the need for this approach must be demonstrated:

"Through a combination of increased awareness at the board level, as well as brief education meetings [held for] other departments, showing the impact to the business and our customers … has resulted in acceptance of needing to incorporate these things. We are not where we should be, but we are making progress in that direction now."

—Survey respondent

Only 30% of respondent organizations have been able to get security functions embedded in other departments' budgets. This is really a problem of not enough force being applied to move the hard-to-move object—generally, the security teams have been able to show the benefit of increasing security and work with other groups to reduce the business impact of reaching those higher levels. Doing so in an increasingly cloud-based IT environment requires the upskilling discussed earlier. See Figure 3.

Have you been able to get security functions embedded in other departments' budgets? (Examples: Endpoint or app security baked into DevOps; software vulnerability testing into quality assurance [QA] or software testing; network packet capture into network)

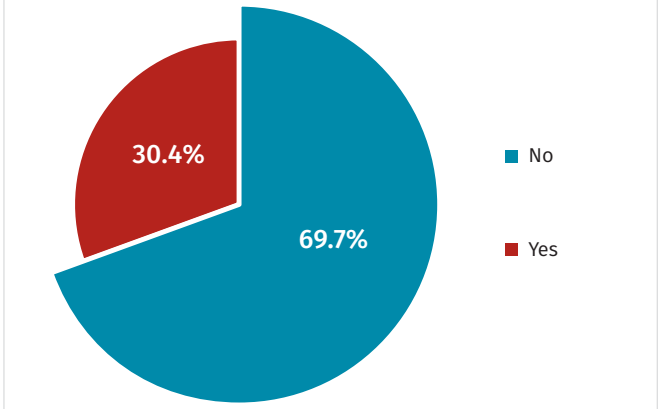


Figure 3. Security Functions and Budget

Survey results also show one large gap in spending for cybersecurity. Management thought leader Peter Drucker is often quoted as saying that "you can't manage what you can't measure." Well, you can't really evaluate the effectiveness of your security spending unless success is defined, tracked and communicated. Only 35% of respondents measure the effectiveness of their security program against the cost of investment—which means that close to 65% either don't measure or don't know whether they do.

TAKEAWAY

Don't let movement to the cloud be a lost opportunity to improve your security culture by establishing an integrated budget. Movement to the cloud presents a huge opportunity to bake security into DevOps and IaaS budgets. Find the security architect or app dev manager in charge of implementing a CI/CD pipeline and get security visibility and response integrated into the rollout.

Metrics are certainly not the only means to measure effectiveness. In fact, one respondent quipped: "Metrics are very rarely effective in convincing management in spending funding. We tend to have to use other methods." However, using metrics plus other measurements is invariably more effective than other methods alone. Surprisingly, for those respondents who evaluate the effectiveness of their security spending, not all the factors are cost-related. See Figure 4.

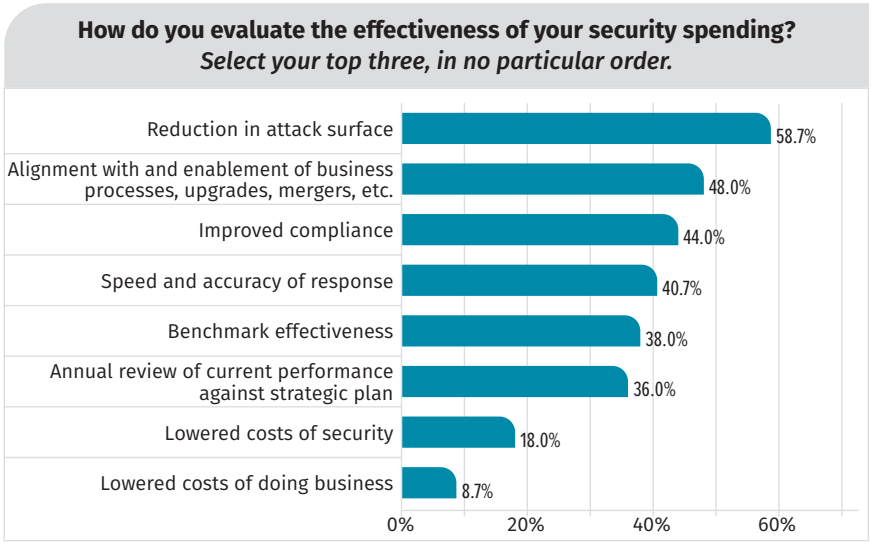


Figure 4. Evaluation for Security Spending Effectiveness

Measuring and tracking security spending effectiveness should be viewed as a critical process for any organization, especially as cybersecurity continues to grow in importance throughout all aspects of our lives. Consider these functions of measuring spending effectiveness:

1. **Aids in the planning of actual operations.** Management must consider how conditions could change and what steps to take to ensure the activities are accounted and budgeted for.
2. **Coordinates across organizational activities.** An embedded budget encourages the CISO to build relationships with other parts of the operation and to understand how the various departments/teams interact and how they all support the overall organization.
3. **Communicates security spending plans throughout the organization.** Communication ensures that key organizational stakeholders (such as the board of directors) get a clear understanding of how security activities will support the organization and how security meshes with other elements to support business growth.
4. **Controls security activities.** The term "on schedule, on budget" helps the CISO compare actual spending with the budget to control finances. Measuring the effectiveness of that spend (against budget) provides justification for the outcomes of the investment, paving the way for easier approval of future requests.

Remember, a meaningful and consistent set of effectiveness and efficiency metrics is key to persuading management to approve needed funds for security-related activities and technologies, as well as to demonstrate the business benefit from those investments.

Final Advice

Security spending needs to become smarter, especially as the move to the cloud demands a focus on being less reactive and more proactive. Organizations must be smarter about monitoring and detecting threats at both the network and the endpoint before they become incidents or breaches. They also need to understand how to protect data in accordance with business needs, not just because of regulatory compliance. At the end of the day, it's about changing culture: aligning security budgets with the needs of an organization; measuring the effectiveness of the investment; and overcoming current organizational strategy for security spending that always seems to cut corners on costs, without considering the larger impact, such as the lost productivity of expensive staff.

Beyond that, there is a tendency for management to focus on purchasing technology, rather than spending on headcount or skills. Respondents sum up the situation:

> *"People are expensive. We can't pay them what the market demands and they leave, causing a constant churn of talent. Institutional knowledge leaves with the talent, and we end up having someone who [has] only done the job here for a few months training someone who is brand new, then rinse and repeat—the cycle continues."*
>
> —Survey respondent

> *"It's easier to buy things (services, software, hardware) than to add staff. Justification to add personnel is very hard to sell to management."*
>
> —Survey respondent

But this is shortsighted for the simple reason that, as another respondent writes, "While many vendors claim to have tools that work, the reality is that most of them cost more [in required] manpower than they deliver [in value]. In my mind, throwing more money at a technological problem just barely edges out having more people."

Corporate human resources departments have long known that attrition goes down when employees are engaged and feel creative. Upskilling of employees, supporting them in creating and using homegrown and open source tools in conjunction with commercial products and services results in higher security effectiveness, decreased attrition and increased efficiencies overall.

Current processes should be evaluated for improvements and enhancements made. In parallel, developing that meaningful and consistent set of effectiveness and efficiency metrics becomes key for convincing management to approve needed funds for training and procurement, laying the basis for how the business will benefit from current and future investments.

With a skilled staff and well-defined processes now in place, the choice of which security technologies will provide the best return on investment can be driven by the particular threat environment and business constraints of your organization. Newer commercial technologies, which can be used as force multipliers, can add further increases in both effectiveness and efficiency, as well as by offloading many boring repetitive tasks from the most highly skilled analysts. Your organization will be in a much better position to evaluate the true cost of technology enhancements versus their real benefit to your security operations.

About the Authoring Team

Barbara Filkins, SANS Research Director, holds several SANS certifications, including the GSEC, GCIH, GCPM, GLEG and GICSP, the CISSP, and an MS in information security management from the SANS Technology Institute. She has done extensive work in system procurement, vendor selection and vendor negotiations as a systems engineering and infrastructure design consultant. Barbara focuses on issues related to automation—privacy, identity theft and exposure to fraud, plus the legal aspects of enforcing information security in today's mobile and cloud environments, particularly in the health and human services industry, with clients ranging from federal agencies to municipalities and commercial businesses.

John Pescatore (Advisor) joined SANS as director of emerging security trends in January 2013 after more than 13 years as lead security analyst for Gartner, running consulting groups at Trusted Information Systems and Entrust, 11 years with GTE, and service with both the National Security Agency, where he designed secure voice systems, and the U.S. Secret Service, where he developed secure communications and surveillance systems and "the occasional ballistic armor installation." John has testified before Congress about cybersecurity, was named one of the 15 most-influential people in security in 2008 and is an NSA-certified cryptologic engineer.

Sponsor

SANS would like to thank this survey's sponsor:

ExtraHop
Rise Above the Noise.