A TRUSTWAVE SURVEY REPORT

Money, Minds and the Masses

A Study of Cybersecurity Resource Limitations

Trustwave®

Money, Minds and the Masses

A Study of Cybersecurity Resource Limitations

Executive Summary

A fast-moving confluence of skills shortages, worsening threats and disproportionate spending habits is leaving organizations increasingly vulnerable to data breaches, malware, phishing and a variety of other information security problems that can have serious or even devastating consequences.

Specifically:

- Most organizations have difficulty finding a sufficient number of experienced IT security people to fill key positions, and in discovering individuals with the specialized skills sets necessary to address increasingly sophisticated threats, complex technologies and intensive compliance requirements.
- At the same time, organizations are more vulnerable than ever to zero-day, advanced and emerging security risks because there are not enough people to address problems in a timely or adequate manner, and because cybercriminals are motivated by large profits enabled by a vibrant underground marketplace.
- Meanwhile, IT organizations are budget-constrained and feel a lack of support from senior management, either because corporate leaders are not yet convinced of the severity of the security threats they face or because the funds simply are not available to fully and appropriately bankroll IT security requests.

To better understand these issues, Osterman Research prepared a report titled “Money, Minds and the Masses: A Study of Cybersecurity Resource Limitations” on behalf of Trustwave. From August to September 2016, Osterman surveyed 147 IT security decision makers, influencers and recommenders in primarily mid-sized and large organizations in North America to understand the challenges they face around recruitment of IT security talent, identification of the skills sets they require, the level of control they have over their IT security budgets, and other pertinent matters related to IT security management. The result was a candid and somewhat disconcerting look at the current state of IT security resource impediments and the drivers and solutions that surround them.

Key Takeaways

Here are the primary findings from the survey:

- **A good IT security staffer is hard to find**
  Finding and recruiting talented IT security staff members with the right skills sets is a "significant" or "major" challenge for 57 percent of organizations. Retaining these people is also viewed as a difficult problem by more than a third of respondents (35 percent).
- **IT security teams lack the necessary talent to meet today's threats**
  More than six out of 10 respondents report that half or fewer of their security staff have the specialized skills and training to address more complex security issues. And only one in nine of those surveyed believe it is "very likely" they will have IT security staff available to meet their security demands in the future.
- **Experience is preferred over education**
  While holding certifications and degrees are important attributes of IT security job candidates, respondents believe the most vital factor to job performance success is their experience.
- **Throwing bodies at the problem isn't going to cut it**
  More than three times as many respondents would rather grow their staff's skills and expertise than grow the number of people on their team.
- **Mundane activities are a major time sink**
  Forty percent of IT security departments spend the most time on routine system maintenance and update activity, leaving much less time for addressing emerging and evolving threats, security vulnerability testing, incident/threat response, and communication with the executive team.
- **Skills are lacking in key areas of IT security**
  Not surprisingly, 40 percent of respondents believe that their skills sets around emerging and evolving threats are the least adequate, while their skills sets around routine maintenance are considered the most adequate. This reveals that IT security jobholders are good at the basics, but require additional acumen around the more esoteric demands of the profession which, if not done right, could be damaging to the organization.
- **Most IT security leaders lack adequate control over their security budget**
  Only about one-quarter of respondents have "complete" control over their annual IT security budget. Moreover, seven out of 10 at least sometimes – or more frequently – have disagreements with their senior management on budgeting and staffing issues. This has led to a situation in which fewer than 30 percent of respondents feel "fully supported" by the senior managers in their company.
- **Security is not the major spending area for IT**
  When it comes to spending on security, protecting email and endpoints are the top two areas in which respondents feel they should be spending their money. But security doesn't generally earn a big piece of the pie: Nearly three out of four IT departments spend no more than one-quarter of their IT budget on security.
- **IT security disciplines requiring the most skills receive uneven funding**
  Security testing (which includes vulnerability scanning and penetration testing) and incident response rank as the two areas of IT security requiring the most skilled personnel, but they rank in the bottom three of areas that IT security decision makers believe should receive the most funding. Likely as a result, many organizations delegate responsibility for these security functions to an outside vendor.
- **IT security pros have difficulty anticipating future skills needs**
  One-third of respondents report they have trouble identifying the IT security skills and competencies they need, and nearly one-half believe this problem is going to get worse.
- **Breaches and compliance violations can get people fired**
  The three offenses that are most likely to result in the termination of an IT security staff member are all related to data breaches or compliance violations. Moreover, two-thirds of organizations consider the failure to meet regulatory compliance requirements leading to a large fine or other penalty as a "fireable" offense.

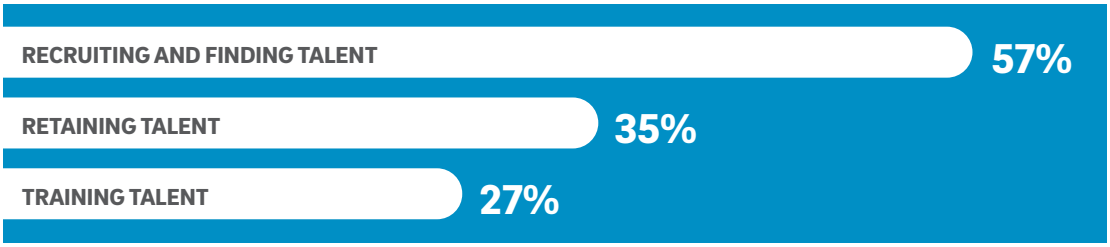
Survey Findings

The Biggest Challenge Is Finding the Right Talent

Fifty-seven percent of the respondents to this survey consider recruiting and finding IT talent to be a significant challenge or major challenge, as shown in Figure 1. Other key challenges include retaining and training talent.

Figure 1
Biggest Challenges Related to IT Security Staffing

Percentage Considering it a "Significant" or "Major" Challenge



Source: Osterman Research, Inc.

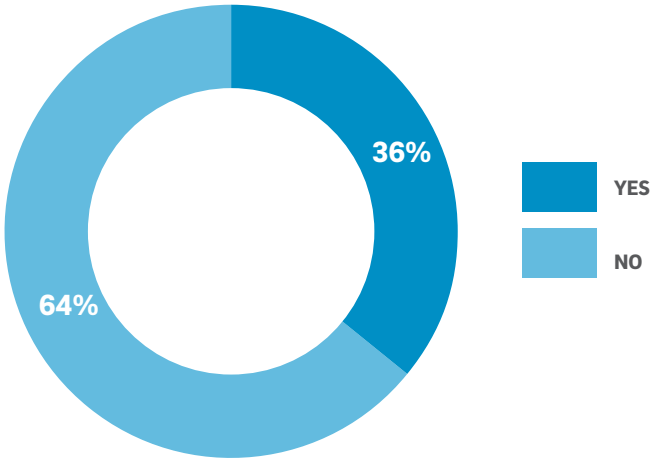
There has been a substantial amount of media coverage of the "IT security skills shortage" – in fact, a web search of the term reveals more than three million results. The inability to discover IT security staff members with the right skill sets should not be understated: An analysis by Computer Science Zone found that from 2016 to 2026, there will be approximately one million more computer science and related jobs than there are computer science students . While IT staff members can come from educational backgrounds other than computer science, the Computer Science Zone findings are but one example of the serious nature of the talent gap.

So, what are the implications? There are several, but the most serious one is that cyberattacks and data breaches may become more common simply because there are not enough adept IT professionals available to monitor and respond to potential security incidents. Moreover, because security testing, incident response and threat monitoring are the three IT security disciplines requiring the greatest skill sets (a key survey finding discussed later in this report), the talent shortage could render organizations substantially more vulnerable to threats, particularly new and innovative ones, unless the status quo changes. Organizations unable to identify vulnerabilities or monitor and react to alerts in a timely manner could result in attackers more easily penetrating corporate defenses.

A Perception of High Turnover Among IT Security Staff

Our research found that 36 percent of the respondents surveyed believe that turnover is higher among IT security professionals than it is in other parts of the organization, as shown in Figure 2.

Figure 2
Do you believe turnover is higher in IT security than in other parts of your company?



Source: Osterman Research, Inc.

This is also an important finding of the research, since it serves to amplify the negative impact of the IT skills shortage discussed above. In short, an inability to find the right IT people with the adequate skills is a serious problem that is exacerbated by an inability to retain these people for long periods. The problem becomes more serious during prosperous economic times when budgets are available to hire IT security staff members, resulting in increased competition for capable hands. These staff members are more likely to bolt for higher paying jobs elsewhere.

Illustrating the availability of job openings for the position of just "IT Security," a search of job site Indeed.com in mid-October 2016 revealed large numbers of openings in each of the following top 10 metro areas in the United States:

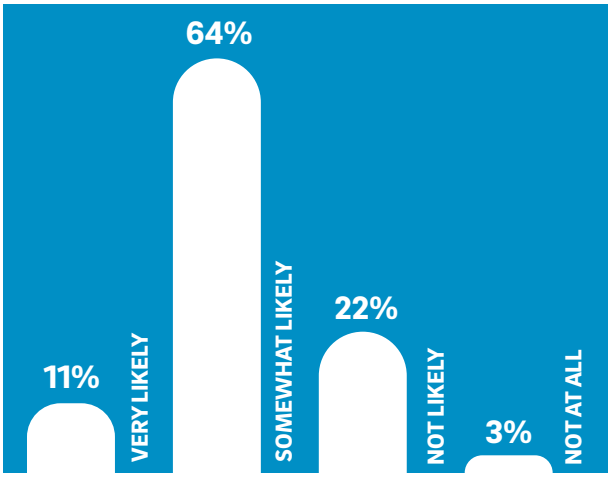
- **New York:** 8,726
- **Los Angeles:** 5,505
- **Chicago:** 4,195
- **Dallas-Fort Worth:** 4,299
- **Houston:** 2,002
- **Washington, D.C.:** 18,795
- **Philadelphia:** 3,394
- **Miami:** 2,267
- **Atlanta:** 3,649
- **Boston:** 4,838

The fact that there are currently about 58,000 IT security job availabilities in just the top 10 metro areas in the United States is but one illustration of just how much in demand IT security professionals are, which makes retaining them that much more difficult.

Many Don't Have Talent Available

As shown in Figure 3, IT security professionals are concerned about their ability to have the talent available to meet new demands placed on the security department. Only one in nine IT security professionals believes that it is "very likely" that their organization will have the talent available to meet increasing demands placed on it, while the majority believes if it is "somewhat likely" that they could meet these demands. However, one-quarter of security professionals believe that it is "unlikely" or "not at all likely" that they will be able to meet increasing demands.

Figure 3
Likelihood That IT Will Have Available Staff to Meet Increased Security Demands



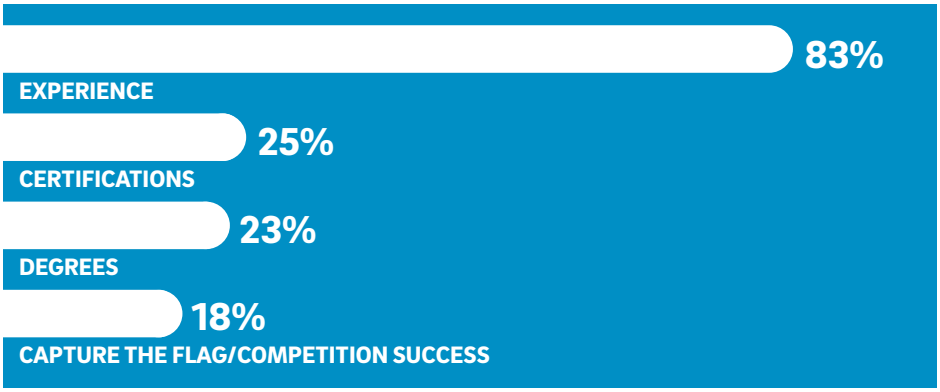
Source: Osterman Research, Inc.

Experience Is Paramount

As shown in Figure 4, experience is, far and away, the most important consideration for IT security job candidates. More than four in five respondents believe that experience is valued "significantly" or "a great deal", while certifications, degrees and competitive success are considered to be much less important.

Figure 4
Attributes Valued Most in a Job Candidate

Percentage Responding Valued "Significantly" or "a Great Deal"



Source: Osterman Research, Inc.

While certificates, degrees and other metrics will continue to be important factors for employers in the IT security space, experience continues to be the dominant criteria that employers will focus on as they evaluate jobseekers. The problem, however, is that finding people with the experience in the right areas will continue to be more difficult as demand for these individuals increases and as the number of people with meaningful experience in the most highly specialized areas remains relatively small. This means that organizations will need to somehow find the skills necessary to manage their IT capabilities, particularly in areas focused on security that can have the greatest impact on the business.

Skills Around New Threats Is Lacking

Respondents were asked about the adequacy of their in-house skills and capabilities in the context of various security-related capabilities. As shown in Figure 5, when asked to rate their organization's skills on a scale of 1 (least adequate) to 5 (most adequate), 40 percent indicated that their skill sets around emerging and evolving threats are least adequate, while nearly three in five believe that their abilities around system maintenance and updates are among the most adequate.

Figure 5
Perceived Adequacy of Various In-House Skills and Capabilities Relative to Their Ability to Respond to Various Issues and Responsibilities

Ranked by 1 (Least Adequate) to 5 (Most Adequate)

Activity	1 Least Adequate	2	3	4	5 Most Adequate
System maintenance and updates	13%	12%	16%	56%	3%
Emerging and evolving threats	40%	24%	24%	13%	1%
Security vulnerability scanning and testing	19%	28%	35%	16%	1%
Incident and threat response	19%	35%	30%	16%	0%

Note: Totals may not add to 100% because figures have been rounded.

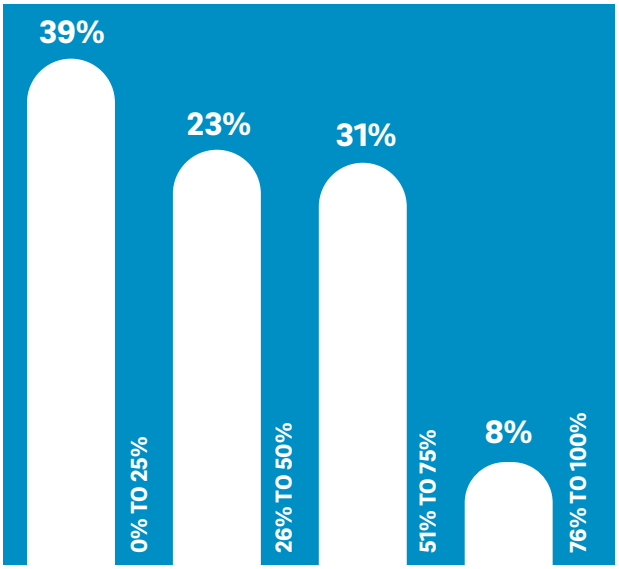
Source: Osterman Research, Inc.

The fact that IT organizations rate themselves least adequate in the context of emerging and evolving threats underscores the fact that they spend the least amount of time managing issues related to these threats, as shown in Figure 8.

Most Lack Key Skills and Training

To properly address the variety of complex IT security issues that most organizations face today, IT staff members must have specialized skill sets and training. However, our research found that for 39 percent of respondents, no more than 25 percent of IT staff members have the requisite skills and training needed to address security threats, as shown in Figure 6. In fact, in only a minority of the organizations surveyed did most IT staff members have adequate skills and training to address more advanced threats.

Figure 6
Proportion of Staff That Has Specialized Skills and Training to Address More Complex IT Security Issues



Note: Totals may not add to 100% because figures have been rounded.

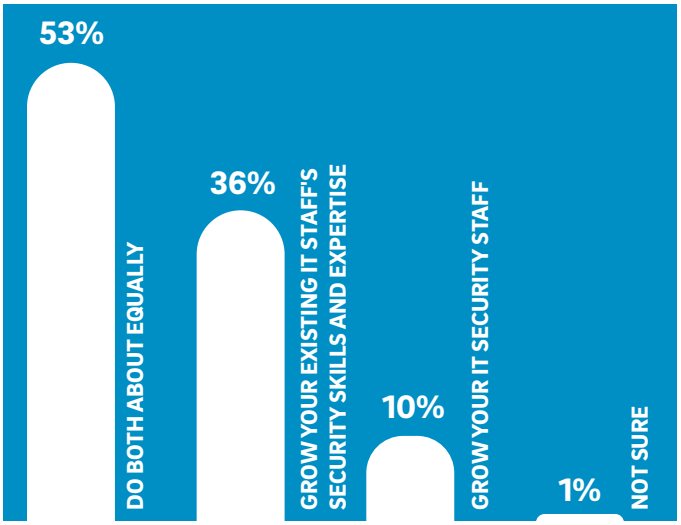
Source: Osterman Research, Inc.

The data in the figure above represents a fairly serious problem for many organizations, since only about two in five organizations find that more than one-half of their IT staff members can address more complex IT security issues. This means that the tasks associated with managing complex security issues falls on a relatively small number of IT staffers in an organization. If these people depart to work elsewhere – which they are more likely to do given the demand for their skills – this leaves the organization even more vulnerable to security problems because they might not be fully able to satisfy their demands with the remaining in-house staff members.

Growth in Staffing and Skills Are Considered Equally Important

The research found that while 10 percent of respondents would most prefer to grow the number of staff members they have available, more would rather grow their staff's skills, while the majority would rather do both about equally, as shown in Figure 7.

Figure 7
Preferences for Growing IT Staff Numerically or Growing IT Staff's Security Skills and Expertise



Source: Osterman Research, Inc.

The skills shortage means that organizations need to find bodies to fill available slots. But it also means that they need to find bodies that have the right skills and expertise, both of which are more difficult to accomplish in a competitive market. Because of the skills shortage in IT security, coupled with the very low unemployment rate for IT staff members resulting from significant demand for them, Osterman Research believes that organizations will use managed security services to fill the gaps. These services will provide organizations with the necessary skills and expertise to help deal with advanced security threats without having to find, hire and train IT staff members.

System Maintenance Is The Biggest Time Sink

Respondents were asked to rank five different activities in terms of how much time they spend on them – on a scale of 1 (the least time spent) to 5 (the most time spent). As shown in Figure 8, 40 percent of respondents gave a "5"/most time spent to system maintenance and updates. These professionals spent the least time on communicating with their executive team about their security posture and needs.

Figure 8
Time Spent by IT Dealing with Various Issues

Ranked by 1 (Least Time) to 5 (Most Time)

Activity	1 Least Time	2	3	4	5 Most Time
System maintenance and updates	17%	16%	14%	14%	40%
Communicating with our executive team about our security posture and needs	41%	15%	12%	10%	21%
Emerging and evolving threats	14%	20%	25%	23%	17%
Security vulnerability scanning and testing	7%	27%	21%	34%	12%
Incident and threat response	18%	24%	25%	21%	11%

Note: Totals may not add to 100% because figures have been rounded.

Source: Osterman Research, Inc.

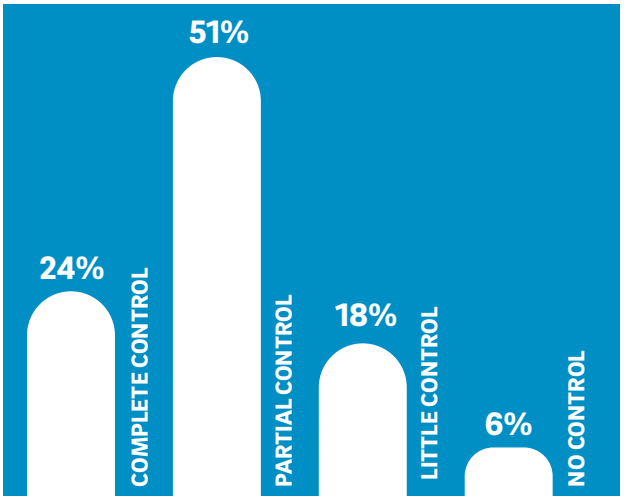
The data in Figure 8 reveals that the relatively mundane tasks associated with normal IT operations consume the most time for security staff, instead of the more esoteric (and, arguably, the most important) tasks associated with protecting the organization from new threats, responding to incidents or testing for vulnerabilities. Moreover, the IT security team spends the least time communicating with senior management about security-related issues, which may explain why IT and senior management are so frequently at odds about budget and staffing issues (which is discussed more below).

One remedy for the problem is simply to outsource some of the more complex tasks that require highly specialized skills, such as dealing with new threats and scanning for vulnerabilities, to managed security services providers or consultants, leaving internal staff more time to address the more traditional management issues in their applications and systems. For particularly resource-challenged organizations requiring soup-to-nuts IT expertise, managed security services providers can handle a wide variety of elements, from basic monitoring and safeguarding all the way up to more advanced protection.

Most Do Not Have Full Control Over Their IT Security Budgets

Our research discovered that only 24 percent of respondents believe that they have complete control over their annual IT security budget, while another 51 percent believe that they have partial control, as shown in Figure 9. Somewhat more alarming, 24 percent believe they have little to no control over their IT security budgets. Moreover, as shown in Figure 10, seven out of 10 organizations experience disagreements between IT and senior management on budget and staffing issues, which likely leads to this lack of control.

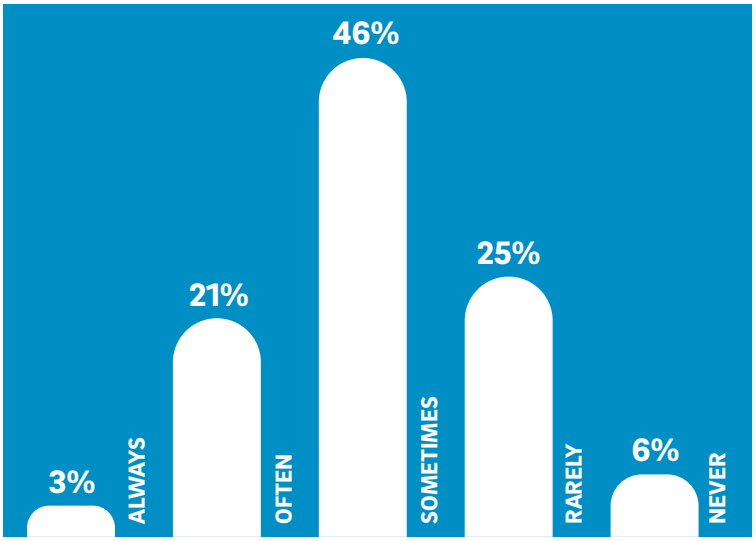
Figure 9
Perceived Level of Control Over the Annual IT Security Budget



Note: Totals may not add to 100% because figures have been rounded.

Source: Osterman Research, Inc.

Figure 10
Frequency with Which IT Security and the C-Suite Disagree on Budgeting and Staffing Issues



Note: Totals may not add to 100% because figures have been rounded.

Source: Osterman Research, Inc.

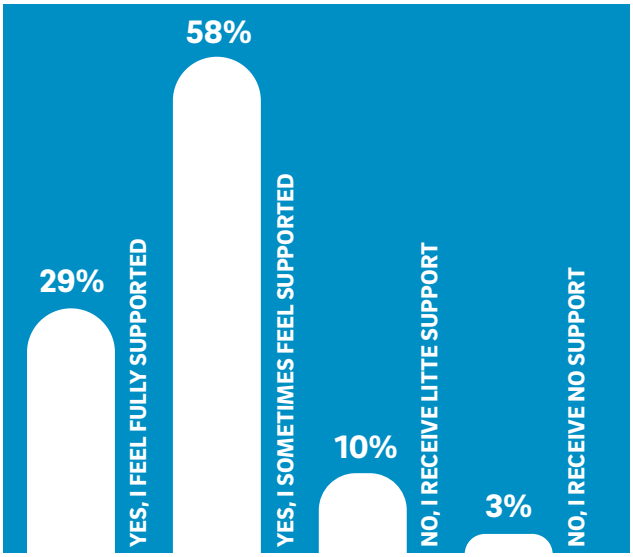
Not having full control over a budget is not all that surprising for any function within an organization, but it can lead to serious complications if IT security management does not have the funds available to hire the right people or if senior management will not approve higher levels of spending that security leaders believe they need. More troubling for nearly one-quarter of IT organizations – as noted above – is that they have little or no control over their budget, making their problems potentially worse.

Disagreements between IT and senior management on budgets and staff requirements can result in a wide range of quandaries, including many that have already been discussed in this report:the inability to find the appropriate personnel, the inability to identify needed skill sets and excessive turnover of security staff.

Most in IT Security Do Not Feel Fully Supported

Most respondents do not feel fully supported by senior management. As shown in Figure 11, only 29 percent feel "fully supported" by their board and C-suite leaders in the context of budget and staffing decisions.

Figure 11
Level of Perceived Support from the Board and C-Suite Regarding Budgeting and Staffing Issues



Source: Osterman Research, Inc.

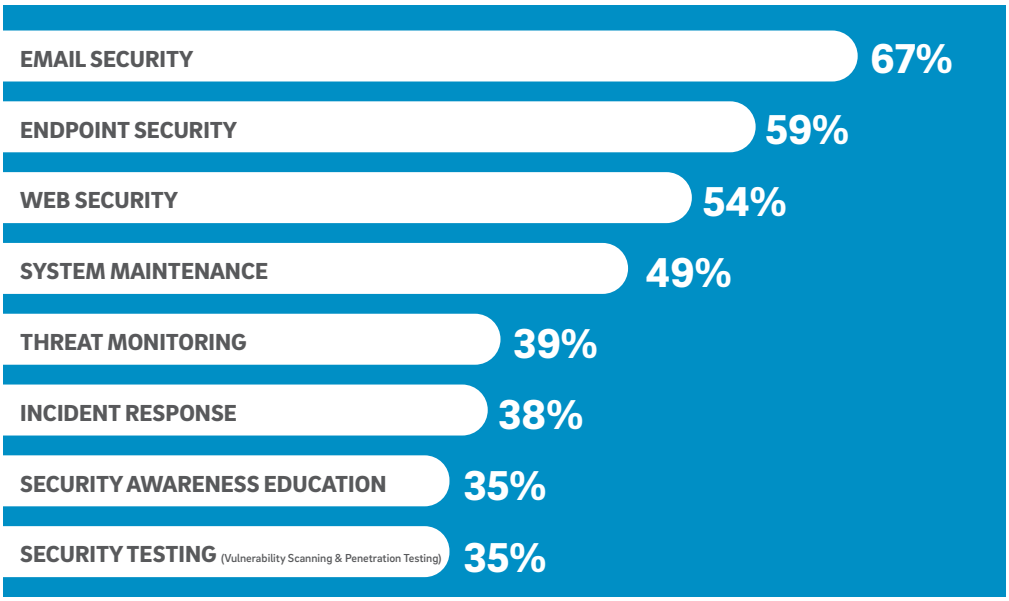
The data in the figure above roughly mirrors the data on budgetary control in Figure 9, indicating that respondents who do not have control over their budget are unlikely to feel that senior managers and the board of directors are supporting them in their efforts.

Email and Endpoint Security Are the Top Two Spending Priorities

Survey respondents rated on a scale of 1 to 7 the various focus areas of IT security spending in terms of which should be funded, where 1 is "should not be funded at all" and 7 is "should be funded heavily". As shown in Figure 12, the areas that respondents believe should be most heavily funded are email security and endpoint security. The areas that these individuals feel should receive the least funding are security testing and security awareness education.

Figure 12
Views on Which Areas of IT Security Should be Funded Most

Percentage That Should be Funded "Significantly" or "Heavily"



Source: Osterman Research, Inc.

The data to begin the figure above is not surprising given that email, endpoints and the web are primary threat vectors for various types of serious threats, including phishing, ransomware and malware. The majority of respondents feel these areas should be significantly or heavily funded. After that, however, the results point to uneven spending, especially for areas like threat monitoring, incident response, security awareness education and security testing – despite the fact that implementing these practices can yield tremendous benefits and that they carry more value than ever before given today's sophisticated threat climate.

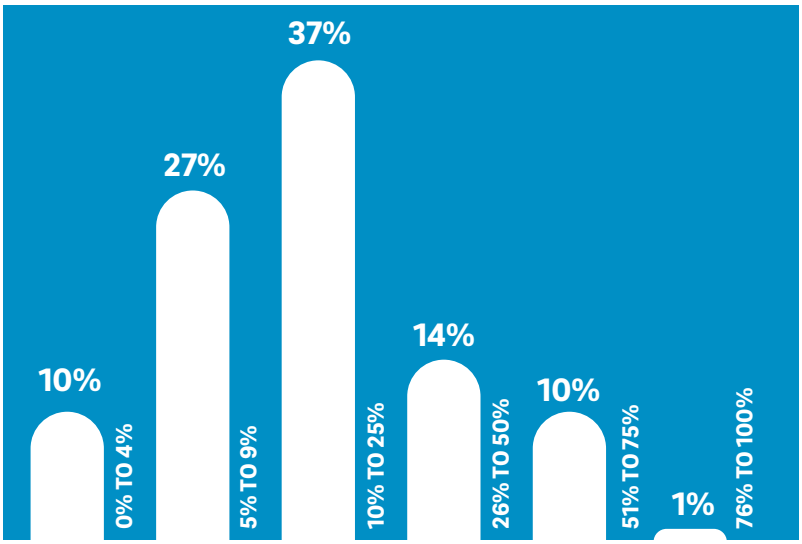
For example, performing vulnerability scanning and penetration testing can uncover major flaws in databases, networks and applications that could lead to attacks and compromises. Security awareness education, meanwhile, can provide measurable and significant benefits by bolstering the ability for users – the first line of defense in any security infrastructure – to become more sensitive to potential threats and reduce the number that can successfully infiltrate an organization. Organizations that do recognize the importance of these underfunded areas tend to delegate the responsibility to an outside vendor.

Security Is Not The Primary IT Spending Priority

As shown in Figure 13, only 25 percent of the organizations surveyed report that they spend more than one-quarter of their IT budget on security and related expenditures. In fact, a plurality spends only 10 to 25 percent of their IT budgets on security, and most of the rest spend only between five and nine percent.

Figure 13
Proportion of IT Security Budget That Goes to Security

Note: Totals may not add to 100% because figures have been rounded.



Source: Osterman Research, Inc.

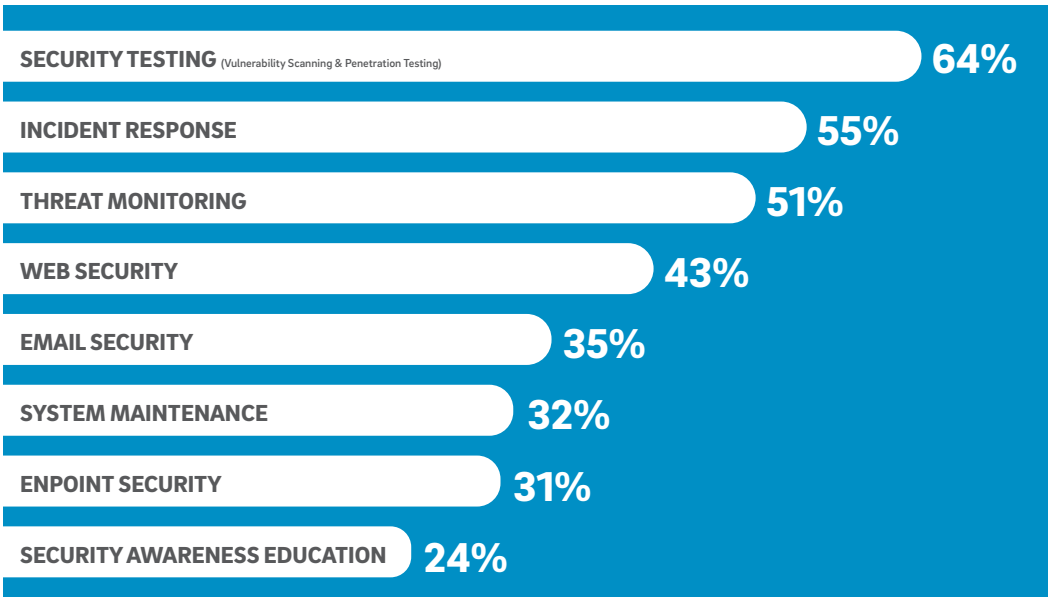
The fact that most organizations spend relatively little on security, compared to other IT expenditures, is problematic considering inadequate security can lead to potentially catastrophic events, such as major data breaches, loss of intellectual property and, in rare cases, the closure of a business.

Security Testing Requires The Most Skilled People

Interestingly, the areas in which respondents feel there should be the greatest level of funding are not the areas that they believe requires the most skilled personnel. For example, as shown in Figure 14, security testing, incident response and threat monitoring are the three areas that require the most skilled staff members, but they are among the areas that respondents believe should receive the least funding.

Figure 14
Areas of IT Security That Require the Most Skilled IT Staff Members

Percentage Responding "Skilled" or "Highly Skilled"



Source: Osterman Research, Inc.

Not surprisingly, respondents rightly believe that security vulnerability testing, incident response and threat monitoring represent a set of highly specialized skills that not all organizations possess. This points to the need for funding and hiring the right people with the necessary skills sets, or outsourcing these critical tasks to specialist providers that already possess the experience, expertise and intelligence to handle them on behalf of organizations. Given the difficulties associated with the former, particularly in highly competitive markets, many organizations would be wise to consider and pursue the latter.

Identifying Skills Will Become More Difficult

As shown in Figure 15, one-third of respondents have trouble identifying the IT security skills and competencies that their organization need today, while 57 percent do not have these types of troubles and another 10 percent simply are not sure. However, security professionals anticipate that in the future they will have even more challenges than they do now: 46 percent expect to have trouble identifying the security skills they need, while 37 percent believe they won't have these problems and 17 percent just aren't sure, as shown in Figure 16.

Figure 15
Do you have trouble identifying the IT security skills and competencies that you need in your organization today?

Source: Osterman Research, Inc.

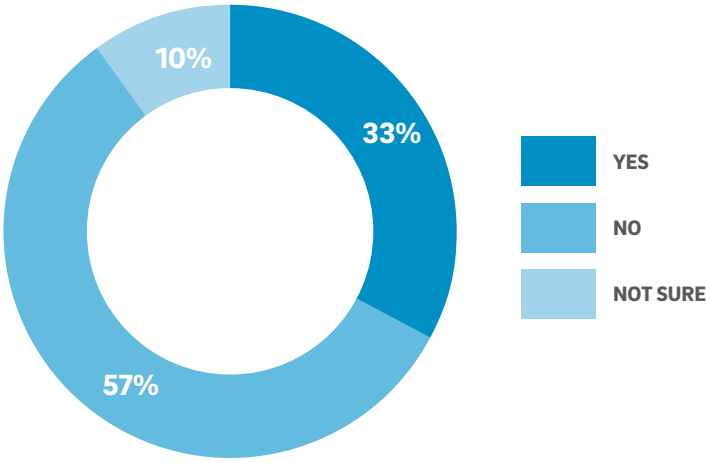
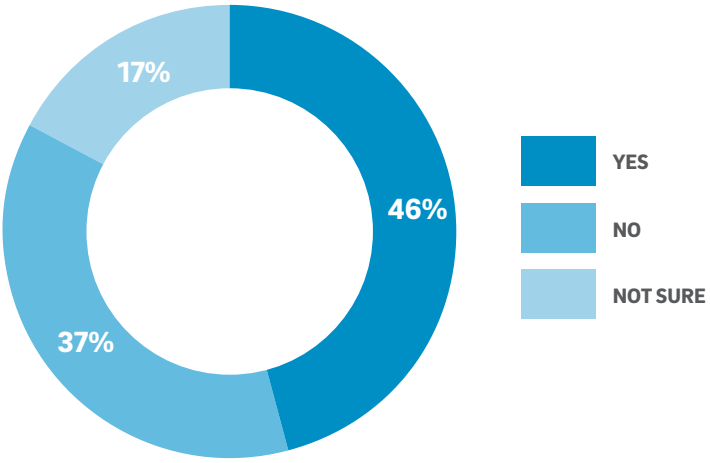


Figure 16
Do you anticipate that in the future you will have more trouble than you do now in identifying the IT security skills and competencies that you need in your organization?



Source: Osterman Research, Inc.

The first step in finding appropriate IT security personnel is the ability to identify the skills that are essential in these individuals so that they can provide the most benefit to an IT department. This is a serious issue, since an inability to identify the skills needed, combined with a failure to discover people who possess these skills, can lead to the IT security team being unable to fully protect and properly manage an organization's infrastructure.

What Can Get an IT Staffer Fired?

This survey has devoted ample attention to the complexities and hardship involved with identifying and hiring desirable security personnel. But what about the flip side? We provided survey respondents with a laundry list of actions that, if committed, would constitute a "fireable" offense for an IT leader. Far and away among these, as shown in Figure 17, is a security staffer's failure to meet regulatory compliance obligations that results in a major fine or some other penalty. However, a significant proportion of respondents also indicated that a particular technology investment that leads to a data breach, a breach that becomes public or even a failure to modernize an organization's security program could, in some cases, result in the termination of security pro.

Figure 17
Offenses That Would Be Considered "Fireable"

Offense	% of Organizations
Failure to meet regulatory compliance that led to large fine or other penalty	68%
Tech investment that leads to a security breach	39%
Data breach that does become public	38%
Failure to modernize your organization's security program	33%
Data breach whose cause cannot be determined	21%
Data breach that does not become public	17%
Failure to meet project deadlines	15%
Authorizing tech investments that are demonstrated not to scale to meet tomorrow's demands	13%
Security product/program investment that fails	13%
Other	3%
None of the above	12%

Note: Respondents could choose any of the options listed above and add additional offenses in the survey.

Source: Osterman Research, Inc.

The top three fireable offenses are all related to some sort of security- or data breach-related incident, underscoring the critical importance of activities that can reduce the likelihood of a breach: identification of new and emerging threats, threat monitoring, incident response and security vulnerability testing.

Summary and Key Issues to Consider

Organizations are facing a serious shortage of IT security staff members, both in terms of the number of people that are available to fill needed positions and the specialized skills that these people need to have. A failure to adequately source IT capabilities can lead to a range of problems, not least of which are data breaches and compliance violations. Both of those can lead to serious repercussions for an organization. Every IT department needs to work closely with senior management to find ways to address these challenges, either by finding the right personnel or through partnering with managed security services providers that can help fill the gaps and amplify protections.

About the Survey

Osterman Research conducted an online, primary market research survey in August and September 2016 using its survey panel of IT decision makers and influencers. A total of 147 surveys were completed. To qualify for the survey, respondents had to be decision makers, influencers or recommenders in the context of their organizations' IT security infrastructure and management. Of the 147 who completed the survey, 74 were decision makers, 49 were influencers and 24 were recommenders.