

ASIS/SIA Risk Assessment Survey

Results and Analysis



© 2007 ASIS Foundation

This report was funded by the ASIS Foundation, based on research performed jointly by the ASIS Foundation, Security Industry Association, and *Today's Facility Manager* magazine.

For additional copies, please contact the ASIS Foundation, 1625 Prince Street, Alexandria, Virginia 22314-2818, USA. Telephone: 703-519-6200. www.asisfoundation.org.

This report was produced by Peter Ohlhausen, President, Ohlhausen Research, Inc. (www.ohlhausen.com), with valuable assistance from Shayne Bates, CPP, and Linda Yelton.

Contents

Foreword	1
Executive Summary	2
Survey Description	2
Key Survey Results and Findings	2
Themes for Future Research	3
1. This Report	4
2. Survey Description.....	5
Respondents	5
Background on Risk Assessment	6
3. Key Survey Findings	8
4. Implications and Issues for Further Research	12
5. Detailed Survey Results	14

Foreword

To safeguard life, physical assets, and information, it is essential to

- identify risks and vulnerabilities,
- establish the likelihood of various loss events, and then
- develop ways to minimize or eliminate such events.

Thus, every security manager or facility manager should know how to conduct a risk assessment. Fortunately, that knowledge is readily available. ASIS International has contributed to the security body of knowledge with its *General Security Risk Assessment Guideline*, available free at www.asisonline.org/guidelines/guidelinesgsra.pdf. The guideline describes the seven major steps in conducting a security risk assessment.

Clearly, risk assessment is important, but the real question is this: Are U.S. security practitioners actually conducting risk assessments, and, if so, how are those risk assessments being used? It is commonly held that security measures are often a knee-jerk response to events, budgets are denied because security is not a priority, and “guards, guns, and cameras” are often applied without careful thought. Until now, the actual use of risk assessment by security practitioners had not been researched in a scientific fashion.

That information gap led me to suggest a study to learn what is actually happening in corporate America. The study employed a survey, which, as this report shows, produced compelling results.

I am truly grateful for the support that many parties provided in this project. First, thanks must be given to the ASIS Foundation, which shared the belief that such research was a priority, and to the Foundation’s director, Bob Rowe, who not only managed the process from inception to conclusion but also assisted with survey development. Thanks are also due to the Security Industry Association (SIA) team of Mark Visbal and Linda Yelton for developing the survey, and to *Today’s Facility Manager* magazine for publishing it. The ASIS Business Practices Council provided invaluable input on the survey questions. My employer, Koffel Associates, Inc., generously donated a significant portion of my time, and Gage-Babcock & Associates, Inc., supported the project through a donation to the ASIS Foundation.

With this research, security professionals and facility managers can now better understand the actual practice of risk assessment in the security field. Such knowledge provides an opportunity to learn from the experiences of others and then to craft—and encourage others to craft—more effective risk and response programs on the basis of fact.

Shayne P. Bates, CPP
September 2007

Executive Summary

Until now, the interaction between security spending decisions and security practitioners' use of formal risk assessment was known only through anecdotes. This report presents the findings of a survey designed to provide hard data on the subject.

Survey Description

The ASIS Foundation and the Security Industry Association teamed up to develop a 28-question survey on the use of risk assessment by persons with security responsibility. *Today's Facility Manager* magazine e-mailed 23,000 subscribers and asked those with security responsibility to answer the survey on-line. During the two-week response window, 215 completed responses were received.

Not all companies elevate security to a separate position. Survey respondents were predominantly managers or directors of facilities, and 10 percent had the word "security" in their title. About three out of four explicitly claimed responsibility for security budget and buying (selection) decisions.

The survey covered a comprehensive variety of industries and locations. Respondents' sites featured populations ranging from less than 100 to more than 1,000 people per facility, space ranging from less than 100,000 square feet to more than 10,000,000 square feet, campuses including 1-100+ buildings, and annual security budgets ranging from less than \$50,000 to \$5,000,000 or more.

The survey's primary focus was this:

How and to what extent are risk assessments *actually* performed, and how do they affect spending decisions?

Key Survey Results and Findings

The survey provides a number of valuable, potentially actionable insights. These are some of the most significant:

- The majority of respondents perform risk assessments at least every two years, but about one-third do not conduct risk assessments often or regularly.
- Although security practitioners generally favor prevention, three out of four respondents state that loss events—not risk assessments—are the most popular trigger that leads to security upgrades.
- One-third of security practitioners who perform risk assessments believe their assessments are futile and could not be the basis of a security upgrade.
- Between one-third and one-half of respondents do not install security equipment or make other security upgrades in response to a risk assessment.
- About one-third of respondents fail to conduct cost-benefit analyses when evaluating options to mitigate risk.

- A thoroughly completed risk assessment would likely minimize the top three barriers to the purchase of security systems, which are:
 - budget limits (a barrier for four out of five respondents)
 - management directives (barrier for nearly half)
 - ROI not justified (barrier for 3 out of 10)
- Less than half of respondents measure the effectiveness of security systems after installation.

Themes for Future Research

Like all surveys, the ASIS/SIA Risk Assessment Survey has its limitations. Nevertheless, its findings raise several themes and issues that may be worthy of future research. For example, are organizations spending their security budgets less efficiently by basing spending decisions on loss events rather than on risk assessments? Why do many practitioners fail to conduct regular and frequent risk assessments? And why do so many risk assessments fail to lead to security upgrades?

Research could also examine what is more effective in ensuring adequate security funding: formal risk assessments or stories of loss events. It would also be useful to learn whether regular and frequent risk assessments are a cause or effect of high-quality security programs. An additional topic for future research would be the issue of why most security upgrades go unevaluated.

1. This Report

In fall 2006, the ASIS Foundation, working with the Security Industry Association (SIA) and *Today's Facility Manager* magazine, conducted a survey to learn about the risk assessment practices of security practitioners. Respondents—people with security responsibility for their organizations—offered a bounty of information. They

- revealed their greatest security concerns,
- judged their own programs,
- stated whether, how, and how often they conduct risk assessments,
- rated the significance and effectiveness of risk assessments conducted before security upgrades, and
- stated whether they perform cost-benefit analyses before spending funds for security products and services.

This report on the ASIS/SIA Risk Assessment Survey is divided into the following sections:

- **Survey Description:** the survey's purpose, origin, funding, methodology, and respondents
- **Key Survey Findings:** the most significant and interesting results from the survey
- **Implications and Issues for Further Research:** issues and questions raised by the survey results
- **Detailed Survey Results:** tabulated responses to the survey's questions

A separate report by the Security Industry Association (www.siaonline.org), titled "End-User Insights: A Study of Security Buying Practices," subjects the survey data to a different analysis, emphasizing budgets and the process of selecting and purchasing security equipment.

2. Survey Description

The ASIS/SIA Risk Assessment Survey was conducted to provide a greater understanding of security practitioners' use of risk analysis in their security spending decisions. The study was funded jointly by ASIS and SIA, and the survey instrument was produced by the two associations working in concert.

A link to the 28-question survey was e-mailed to approximately 23,000 subscribers of *Today's Facility Manager* magazine. Recipients were asked to complete the survey only if they had security responsibility. The e-mail asked those without security responsibility to forward the e-mail to persons who did have that responsibility. Survey recipients had the period of September 25, 2006, to October 9, 2006, to respond. They were offered a chance to win a \$200 gift certificate for participating. *Today's Facility Manager* received 215 completed surveys, a response rate of about 1 percent.

Respondents

Survey respondents represented most types of security practitioners working in the United States. Although they reported a variety of job titles (10 percent of which contained the word "security," as in chief security officer), all respondents, by completing the survey, implicitly claimed to have security responsibility for their organizations. Moreover, 77 percent explicitly claimed responsibility for security budget decisions, while 72 percent said they had security buying (selection) responsibility. It is suspected that the rest generally had other, non-budgetary security responsibilities.

Overall, most respondents were managers or directors of facilities, as would be expected of subscribers to *Today's Facility Manager*. A survey solely of specialized, dedicated security managers might have yielded somewhat different results. However, the present sample may actually be more representative of the way security is practiced in all types of organizations across the United States. Clearly, not all companies elevate security responsibility to a separate position. Given the implicit and explicit indications that the respondents had security responsibility for their organizations, this report will use the general term "security practitioners" to describe survey respondents.

Respondents and their organizations represented a broad cross-section of the following:

- **Industries:** agriculture, education, entertainment venues, financial/legal/business professional services, government, health care, hospitality, industrial/manufacturing, information technology/telecommunications/high tech, retail outlets, senior facilities/assisted living, theme parks, warehousing, and many others
- **Occupancy:** ranging from less than 100 to more than 1,000 people
- **Square footage:** ranging from less than 100,000 square feet to more than 10 million square feet
- **Building types:** stand-alone, low-density office park, high-density high-rise, industrial complex, and others

- **Number of buildings in complex:** ranging from 1 to more than 100
- **Security hardware and software in use:** alarm monitoring, barriers, closed-circuit television/digital video, electronic access control, electronic article surveillance, electronic gate access control systems, emergency phones, fire alarms, information security products, intrusion detection systems, lock hardware, medical alert systems, panic buttons, and many others
- **Security policies and similar measures:** background investigations, incident databases, drug screening, and others
- **Risks faced:** computer intrusions (from internal and external sources), physical risks to people and property (from internal and external sources), environmental catastrophes, explosions, fires, and others
- **Security budgets:** ranging from less than \$50,000 to more than \$5 million

These respondents are clearly the very people who should regularly conduct risk assessments and reap the advantages thereof.

Background on Risk Assessment

According to the ASIS *General Security Risk Assessment Guideline*,¹ risk assessment is the “process of assessing security-related risks from internal and external threats to an entity, its assets, or personnel.”

The key elements of the ASIS *General Security Risk Assessment Guideline* are as follows:

1. Understand your organization and identify the people and assets at risk.
2. Specify loss risk events/vulnerabilities.
3. Establish the probability of loss risk and frequency of events.
4. Determine the impact of the events.
5. Develop options to mitigate risks.
6. Study the feasibility of implementation of options.
7. Perform a cost-benefit analysis.

The guideline then calls for ongoing reassessment of risks.

It is commonly held that risk assessment is an essential part of a security practitioner’s responsibilities. As the ASIS Assets Protection Course notes:²

¹ www.asisonline.org/guidelines/guidelinesgsra.pdf.

² www.asisonline.org/store/program_detail.xml?id=2177307.

The core of all modern security operations is the need to provide cost-effective protection. Without well-executed risk assessment, valuable security resources can be wasted or misdirected.

In short, security practitioners are urged to conduct risk assessments, and the preceding steps constitute a recommended method of doing so. The survey was conducted to determine how and to what extent risk assessments are actually performed in practice.

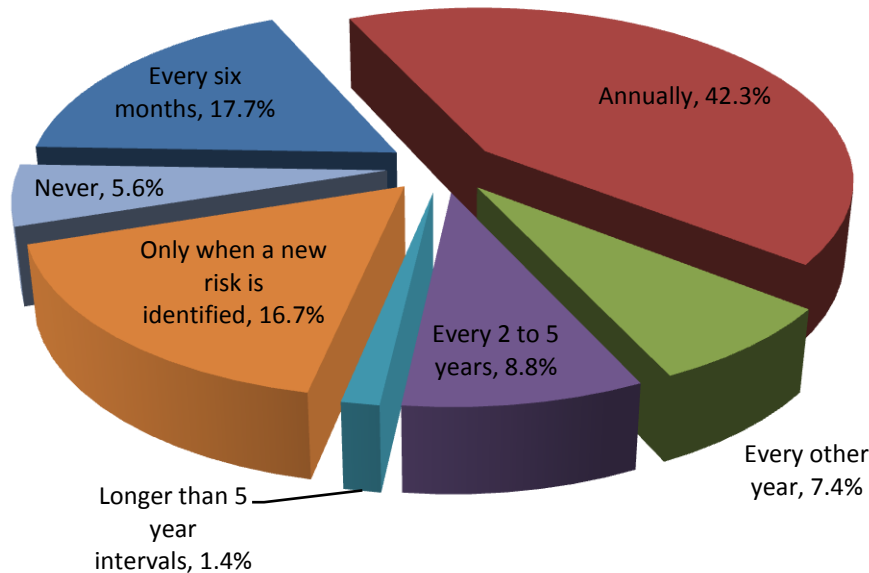
3. Key Survey Findings

This section presents the most notable findings from the survey data. Complete results of the survey are presented in this report’s final section, “Detailed Survey Results.”

The majority of respondents perform risk assessments at least every two years, and much of the time they and their organizations base security spending decisions on those assessments. That finding is to be expected, as risk assessment is widely promoted as a basis on which security decisions should be made. *A more surprising finding is that a sizeable percentage of people with security budgeting and buying responsibility do not conduct risk assessments often or regularly.*

1. One-third of respondents do not regularly and frequently conduct risk assessments.

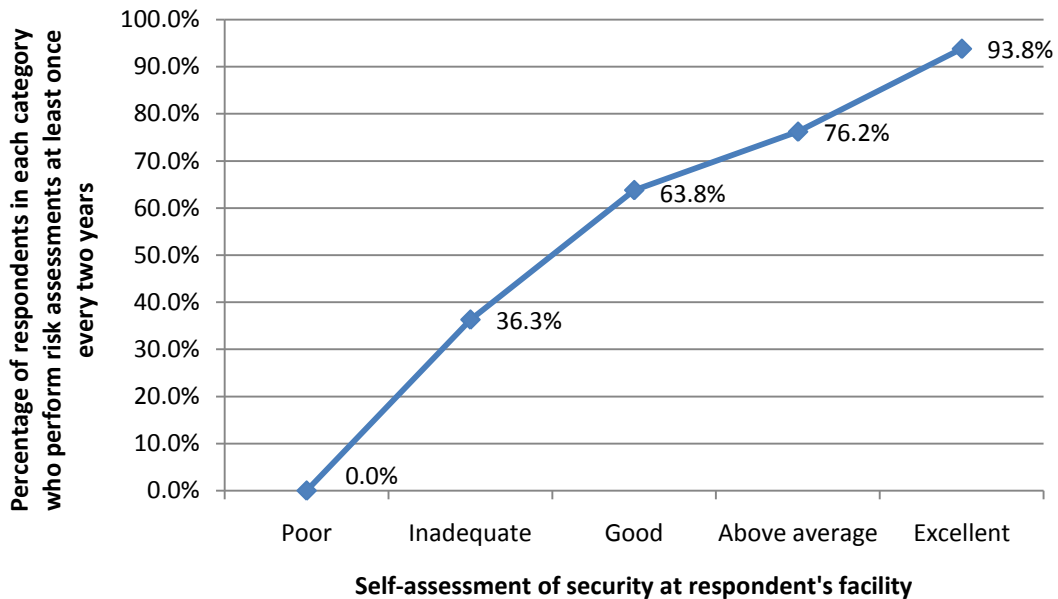
The survey’s Question 12 asked, “How often does your organization perform a risk assessment procedure to assess security-related risks from internal and external threats to your facility, its assets, and/or personnel? Choose the closest fit.” The responses are below:



As the chart shows, 67.4 percent of respondents conduct risk assessments at least every two years—and most members of that group conduct risk assessments once a year or more. Surprisingly, 17.7 percent of all respondents reported conducting risk assessments every six months. However, 32.46 percent—basically one-third—of respondents do not routinely conduct risk assessments at least every two years. Among that subset, about half said they conduct risk assessments only when a new risk is identified.

The survey data showed some interesting tendencies among respondents who conducted risk assessments at least once every two years (classed in this report as “regularly and frequently”):

- They tended to have the word “security” in their titles. Eighty percent of respondents with the word “security” in their titles conducted risk assessments at least once every two years. By contrast, only 66 percent of respondents whose titles were “facility manager” or “other” conducted risk assessments that often.
- Regular, frequent risk assessment is more common in certain industries than others. Eight-six percent of respondents from the hospitality industry conducted risk assessments at least once every two years, as did 84 percent of health care respondents and 82 percent in financial/legal/business professional services. By contrast, only 61 percent of respondents in industrial/manufacturing sites conducted risk assessments that often, as did 63 percent from the educational field and 67 percent of government respondents. Rates calculated for other industries are not reliable because of the sample size.
- Respondents who used information security products were more likely than others to conduct risk assessments at least once every two years. Eighty-four percent of them did so, compared to 65-75 percent of those who used various other methods.
- Similarly, respondents who said their businesses would suffer greater consequences from information damage or loss than from property damage or loss were more likely to conduct regular, frequent risk assessments. Seventy-three percent of those naming information damage or loss conducted risk assessments at least once every two years, as opposed to 61 percent of those naming property damage or loss.
- There was a direct relationship between respondents’ rating of security at their facilities and whether they performed risk assessments at least once every two years. The following chart shows the relationship:



The chart shows that none of the respondents who assessed their security as poor conducted regular, frequent risk assessments. By contrast, nearly all of the respondents who assessed their security as excellent did so.

2. Security upgrades are more likely to be driven by loss events at respondents' facilities or other locations than by risk assessments.

The most common factors that respondents said could lead to security upgrades are a loss at the respondent's facility (named by 86.0 percent), a loss at another location (named by 64.7 percent), and a risk assessment (named by 63.7 percent). Security practitioners generally favor prevention, yet the two most common factors that lead to security upgrades are reactive in nature (losses at one site or another).

3. One-third of respondents who conduct risk assessments feel their risk assessments are futile—that is, that the risk assessments could not be the basis for a security upgrade.

Almost all respondents (94.4 percent) conduct risk assessments at least sometimes, yet less than two-thirds (63.7 percent) believe a risk assessment could potentially lead to security upgrades. Thus, roughly a third of respondents who conduct risk assessments do not believe those risk assessments could lead to security upgrades.

4. Roughly half of respondents have never installed security equipment in response to a risk assessment. About one-third of respondents do not make security upgrades (a broader category) in response to a risk assessment.

The survey's Question 17 asked about the factors that have led to installation of security equipment at respondents' facilities. Only half (52.6 percent) of respondents have installed security equipment at their facilities in reaction to a risk assessment. That means that for roughly half of respondents, a risk assessment has never led the decision to purchase security equipment. Question 18 asked about a broader category, security upgrades (which could involve services and procedures in addition to equipment). By far the largest drivers of security upgrades are incidents (named by 72.1 percent of respondents) and risk assessments (named by 69.8 percent). Even considering the broader category of security upgrades, not just equipment, almost one-third of respondents had never used a risk assessment to drive those upgrades.

5. About one-third of respondents failed to conduct cost-benefit analyses, a key part of risk assessment.

About two-thirds (65.1 percent) of respondents perform a cost-benefit analysis when evaluating options to mitigate risk. That suggests that one-third of respondents (including some who say they are not sure whether they perform cost-benefit analyses) fail to conduct cost-benefit analyses, a key part of risk assessment, when evaluating options to mitigate risk.

6. All of the top three barriers to the purchase of security systems are types of problems that would likely be minimized by the use of a thorough risk assessment.

The survey's Question 27 asked respondents which factors constitute barriers to their purchase of security systems. The top three barriers were:

- budget limits (named by 81.9 percent of respondents)
- management directives (named by 44.7 percent)
- "ROI not justified" (named by 30.2 percent)

Those top three barriers are all likely to be minimized by the use of a thorough risk assessment, which includes a cost-benefit analysis—a concept dear to those who set those budget limits, issue management directives, and decide whether the return on investment is adequate.

7. Less than half of respondents measure the effectiveness of their security projects after installation.

Only 43.3 percent of respondents measure the effectiveness of their security systems at reducing assessed risks. This type of reassessment is urged by the *ASIS General Security Risk Assessment Guidelines* but does not seem to be widely practiced.

4. Implications and Issues for Further Research

The ASIS/SIA Risk Assessment Survey answers some questions about security practitioners' use of risk assessment and, at the same time, raises other questions. The following are some possible implications of the survey, along with issues for further research:

- **For a substantial minority of security practitioners, there is a disconnect between risk assessment and security upgrades.** Many upgrades are implemented without performance of risk assessments, and many risk assessments are deemed futile—incapable of leading to upgrades.
- **Failure to conduct risk assessments (including the important step of cost-benefit analysis) may be reducing organizations' level of security.** If security practitioners do not perform risk assessments, they may not receive the funding they need because they do not provide senior management with clear and present danger data. Greater use of risk assessment may bring more security programs into the mainstream of their organizations' business operations. The survey suggested that actual loss events (at the respondent's facility or elsewhere) were most likely to lead to security upgrades—more likely than risk assessments. However, when actual loss events cannot be used to gain support for security upgrades (for example, if no loss events have happened recently), security practitioners could rely on risk assessments to build the case for security upgrades. Scaring top management with stories of loss events may work sometimes, but in the long run, businesspeople are likely to prefer basing their decisions on formal, numerical risk assessments.
- **Basing security spending decisions on loss events may lead to less efficient spending than when security spending decisions are based on risk assessments.** It would seem that basing security spending decisions on the occurrence of loss events may tend to focus security spending on prevention of those types of loss events only. However, as a risk assessment might show, those loss events may not be the most damaging or the most likely to occur in the future.
- **It is unknown why many security practitioners fail to conduct regular and frequent risk assessments.** Perhaps they feel unqualified to carry out security responsibilities, lacking security training; perhaps they know risk assessment is important but do not know how or when to perform it; or perhaps they are discouraged by the occasional failure of risk assessments to win funding for security upgrades.
- **The likelihood of conducting regular and frequent risk assessments varies directly with the self-reported quality of a security practitioner's security program.** It could be useful to learn why. Is a security program excellent because the security practitioner conducts regular and frequent risk assessments? Or does the security practitioner conduct such assessments because they are expected in excellent programs?
- **It is surprising that one-third of respondents who perform regular and frequent risk assessments feel those assessments are futile in terms of leading to security upgrades.** It would be useful to explore possible reasons for that condition. If ob-

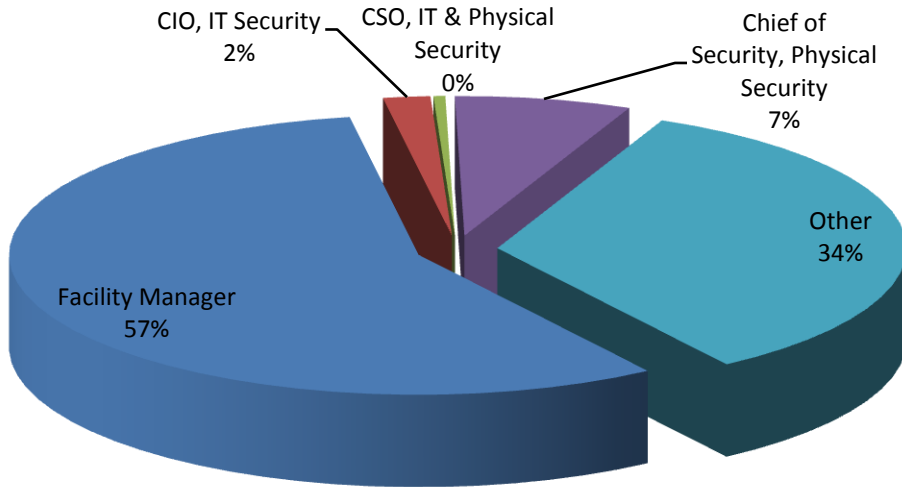
stacles to the effective use of risk assessments are identified, it might be possible to overcome them. It may be that senior managers with limited knowledge of security techniques and issues do not feel qualified to make security upgrade decisions based on risk assessments.

- **Many security upgrades go unevaluated.** Are security practitioners neglecting the recommended practice of ongoing reassessment because they are unaware of its importance, because they do not know how to perform such evaluations, or perhaps because they feel the outcome will be of little use in supporting future purchases? If the reasons can be discerned, it may be possible to suggest ways of overcoming those obstacles.

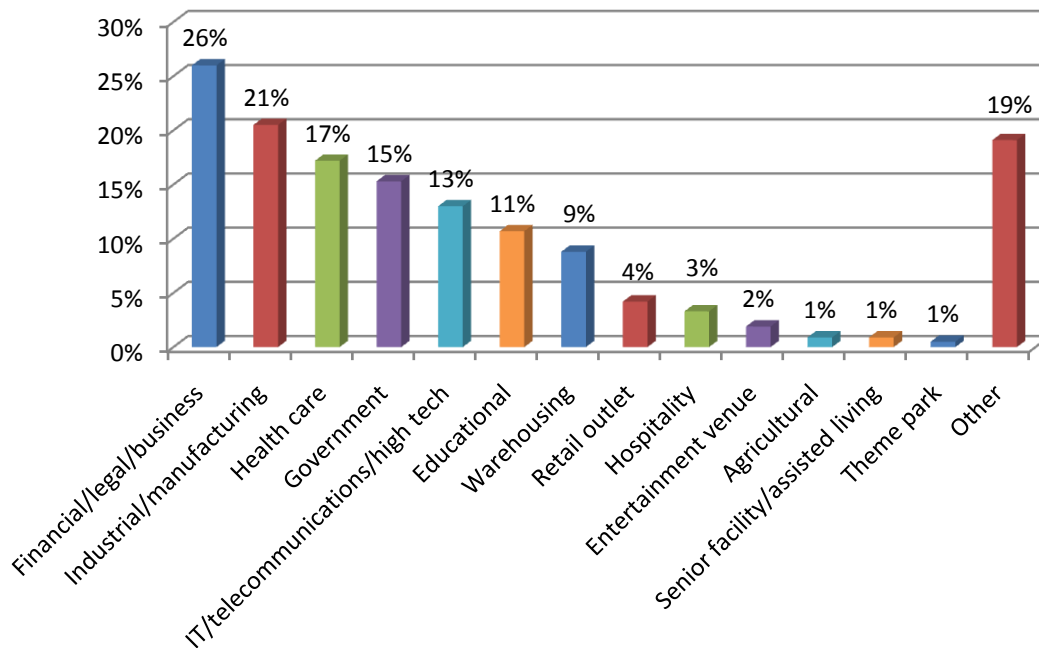
5. Detailed Survey Results

This section provides the direct results of the survey, not grouped, interpreted, or cross-tabulated.

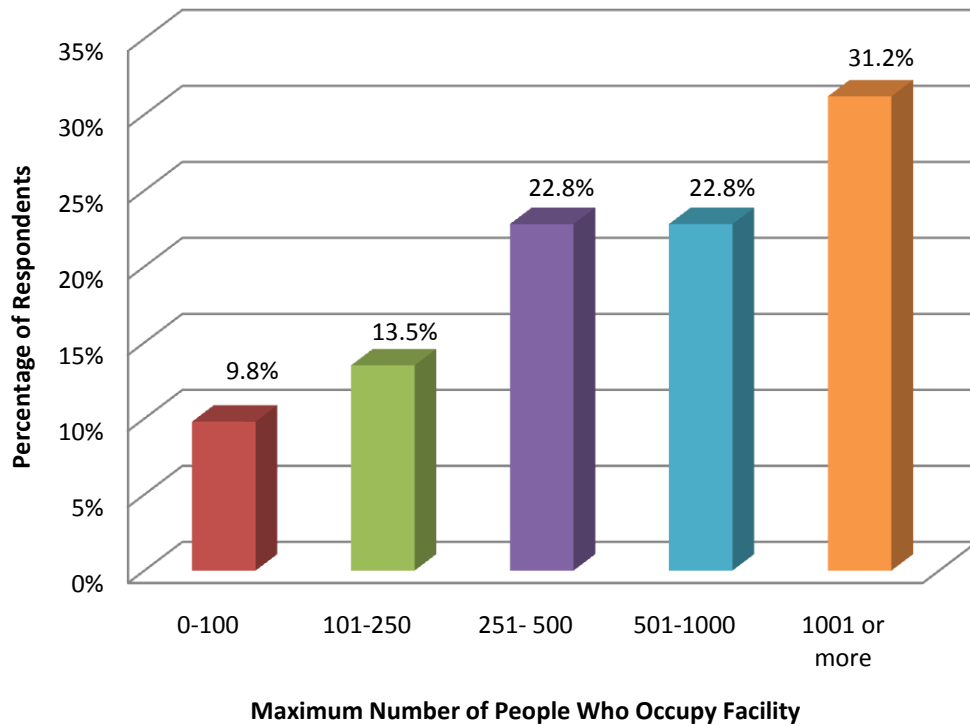
1. What is your job title?



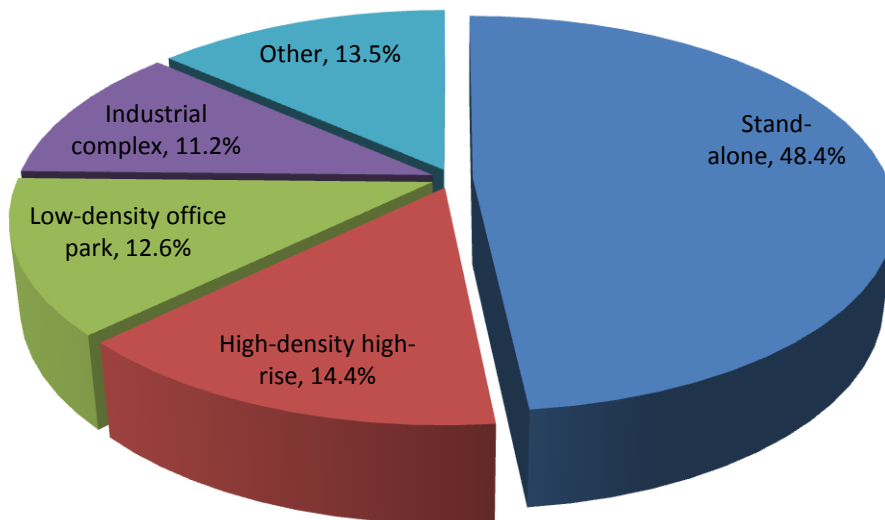
2. Please select the type of business(es) that occupy the facility you manage. Choose as many as apply.



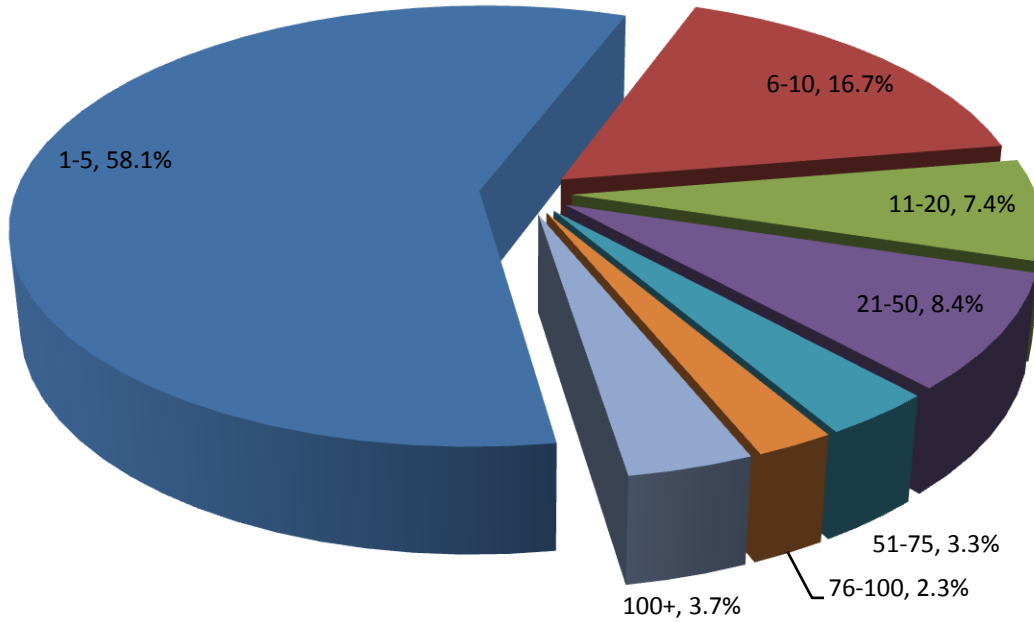
3. From the choices below, please estimate the maximum number of people who occupy the facility you manage at any given time.



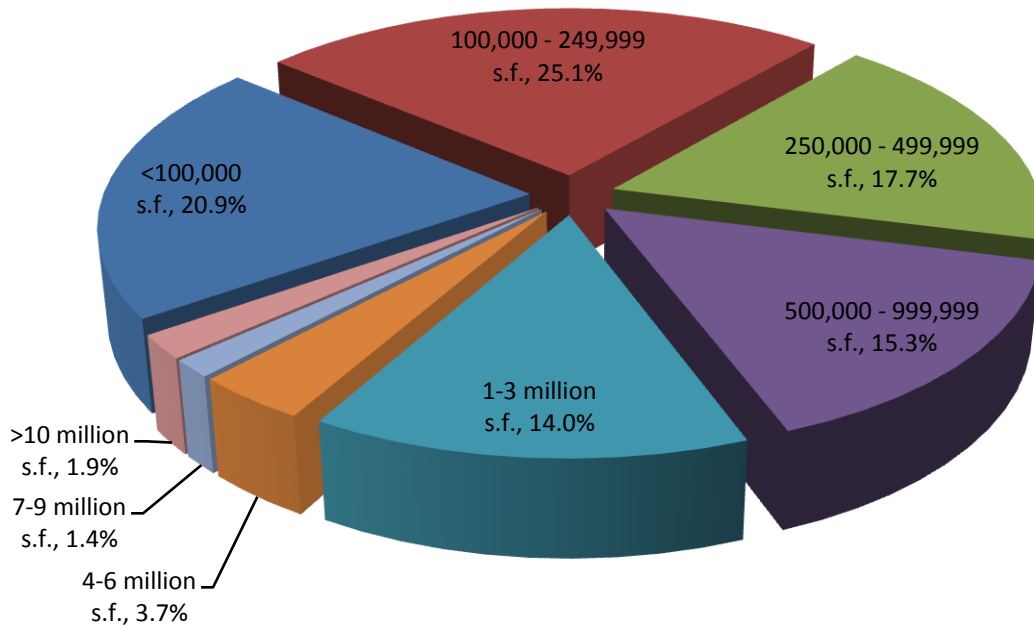
4. From the choices below, please select the type of building that best matches the facility you manage. Please choose only one.



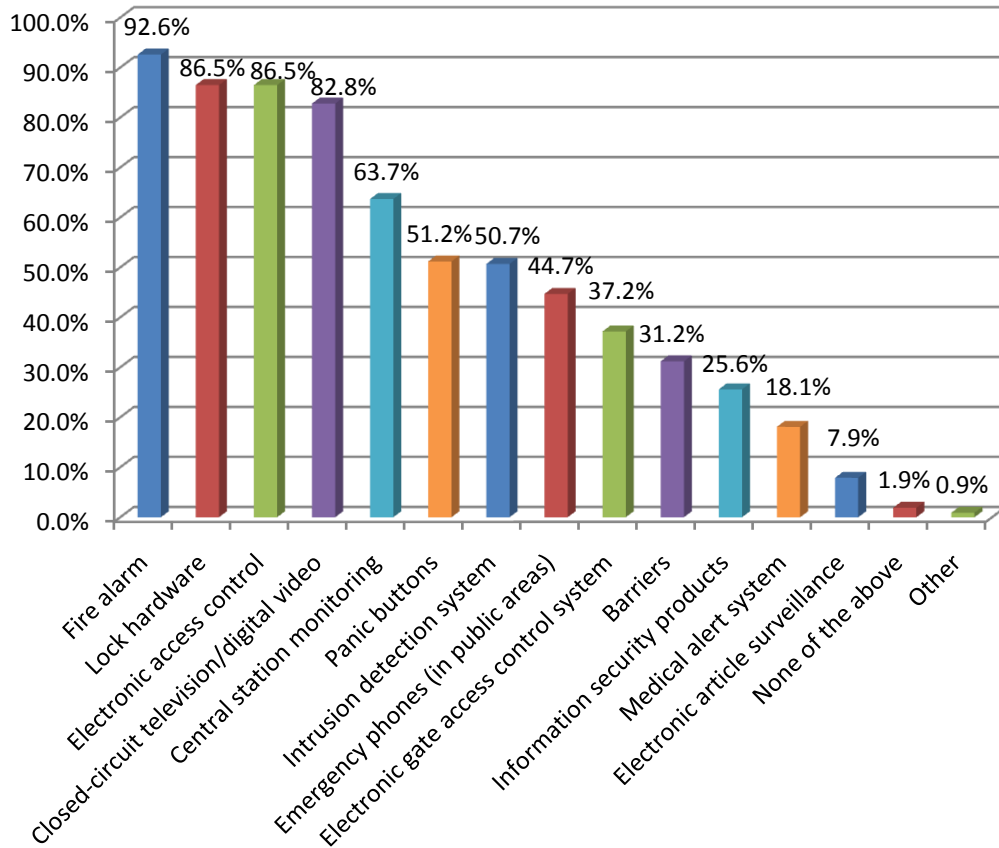
5. From the choices below, please select the number of buildings you manage in your complex.



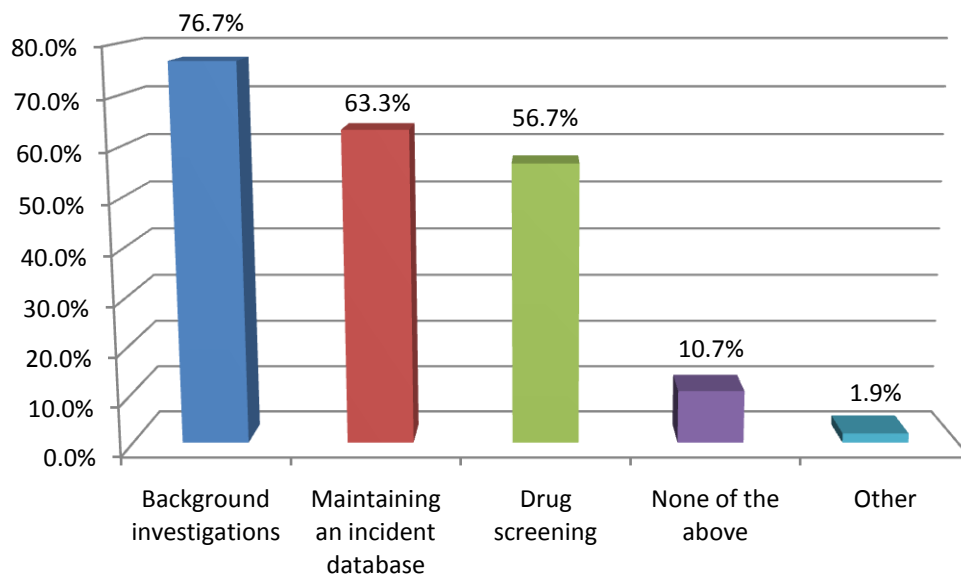
6. To your best knowledge, what is the square footage of the facility you manage? Please choose from the ranges offered below.



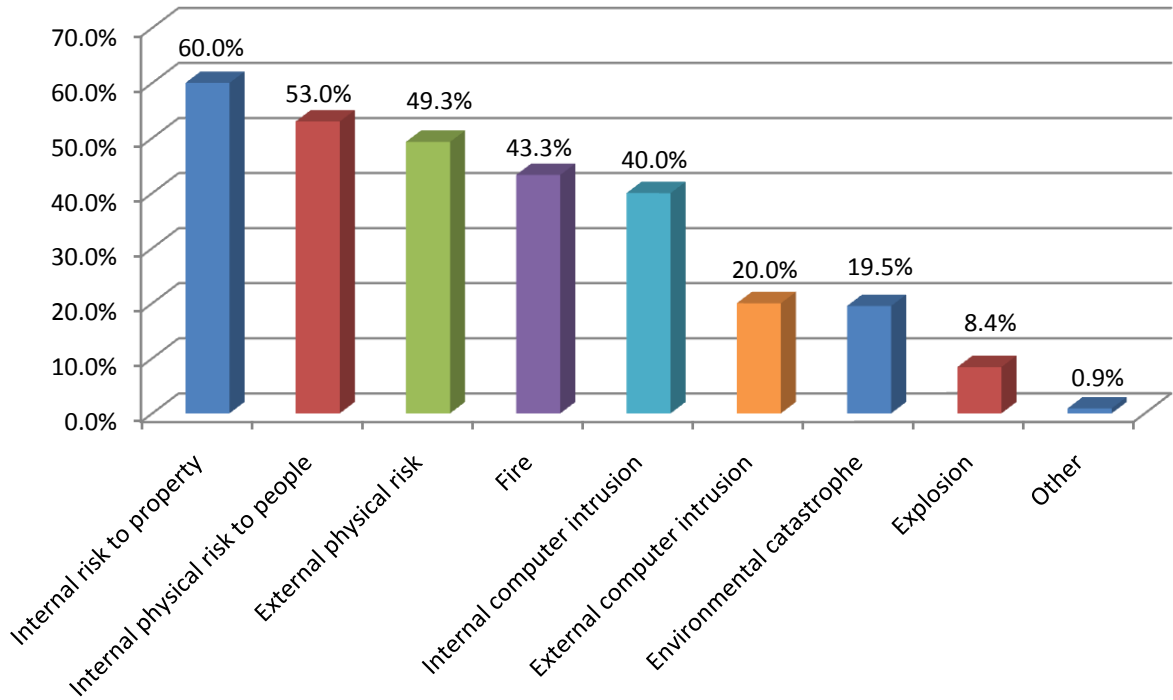
7. Which of the following security hardware or software devices, if any, are already in operation at the facility you manage? Check all that apply.



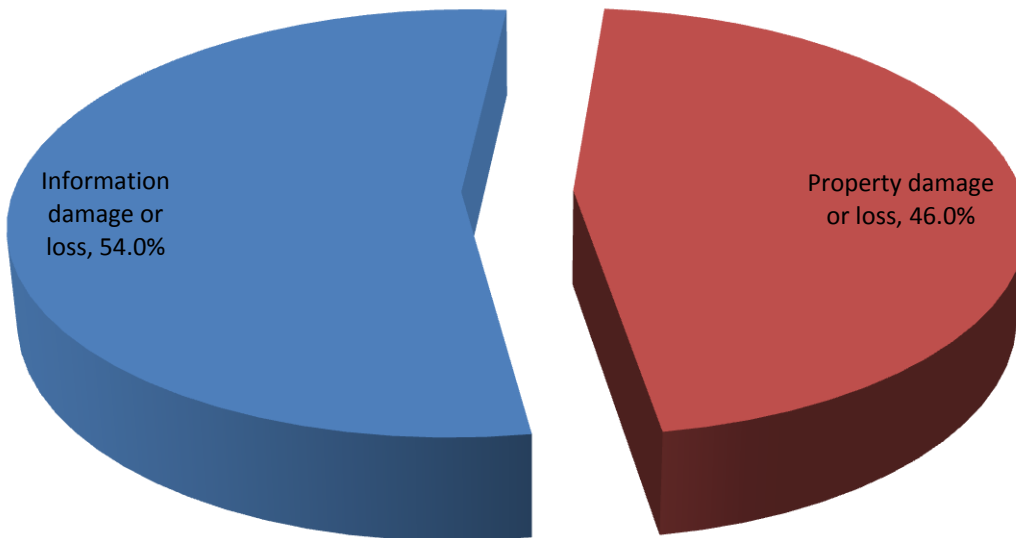
8. Which of the following policies and non-hardware security systems do you use?



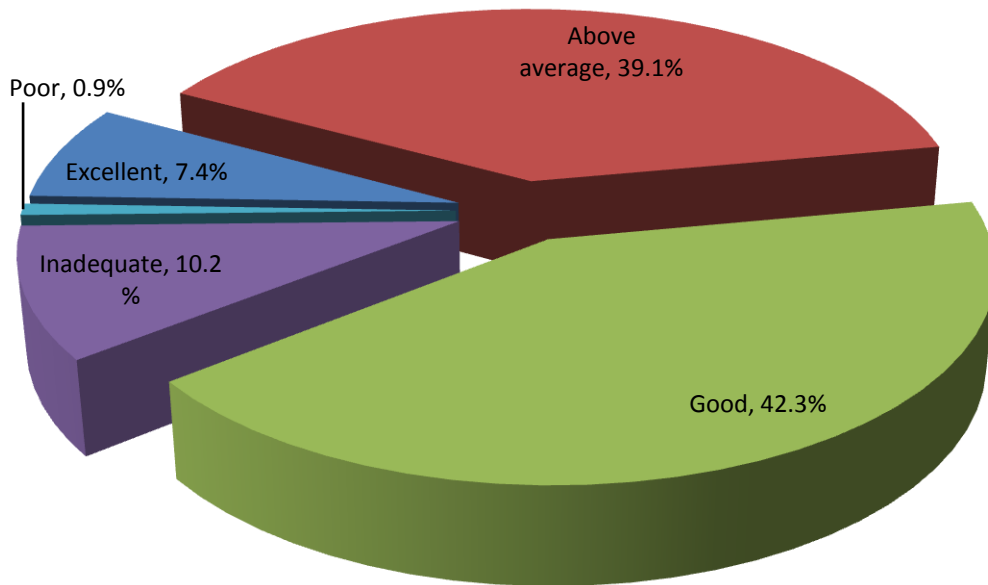
9. From which of the following is the facility you manage most at risk? Check the top three.



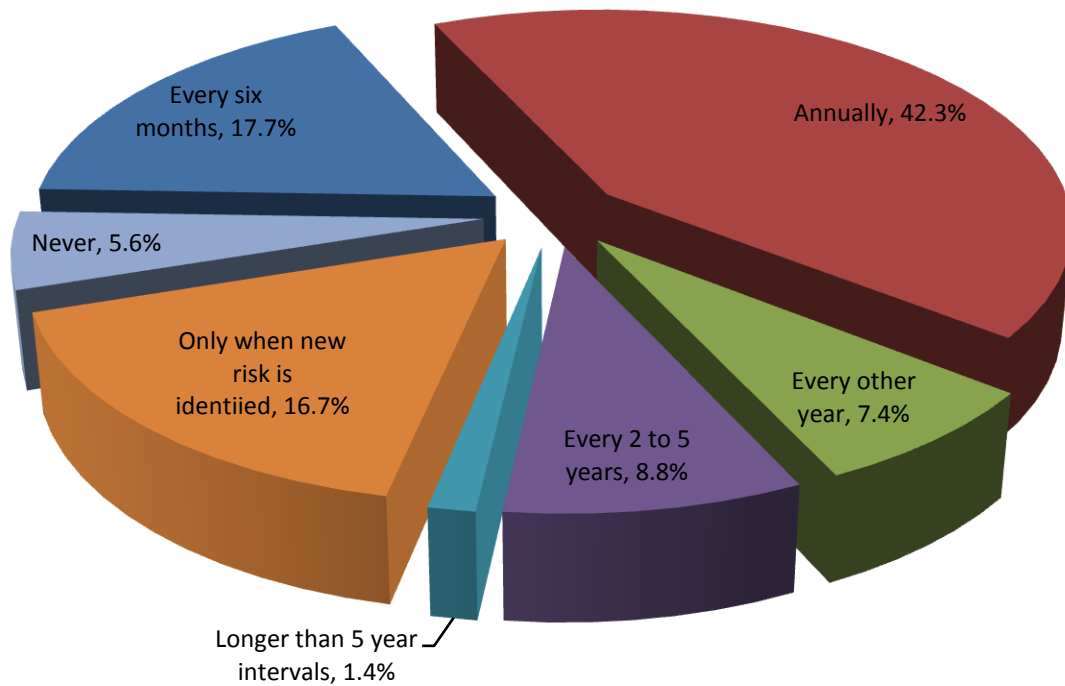
10. In the event of damage or loss, which would have the greater consequence to the business?



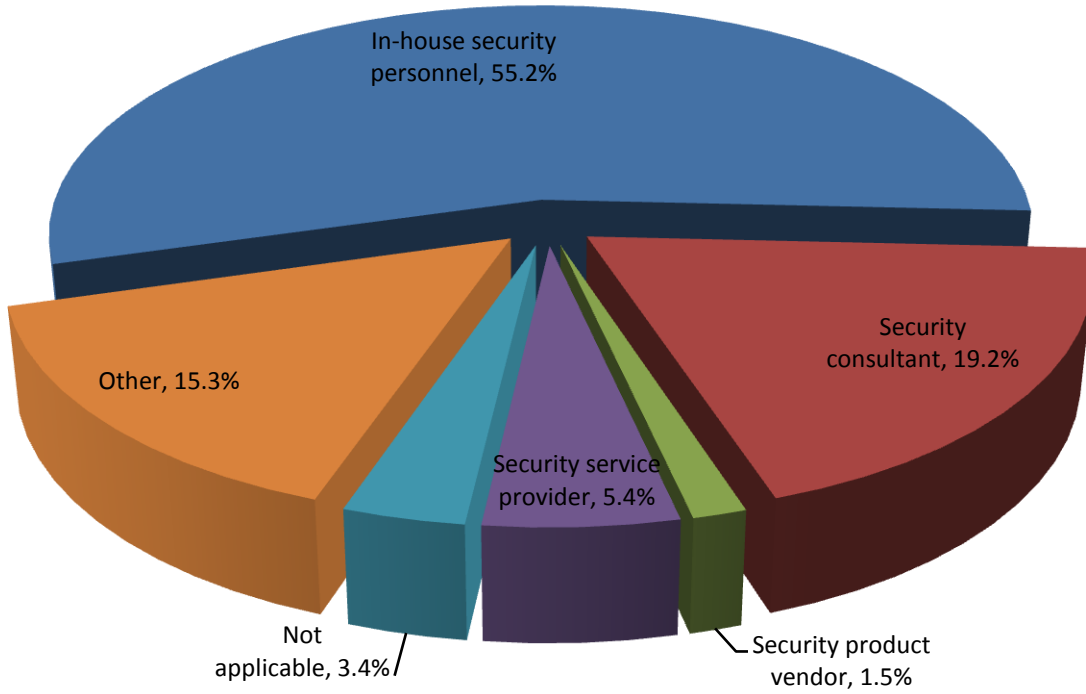
11. In your view, please rate the security at the facility you manage from excellent to poor.



12. How often does your organization perform a risk assessment procedure to assess security-related risks from internal and external threats to your facility, its assets, and/or personnel? Choose the closest fit.

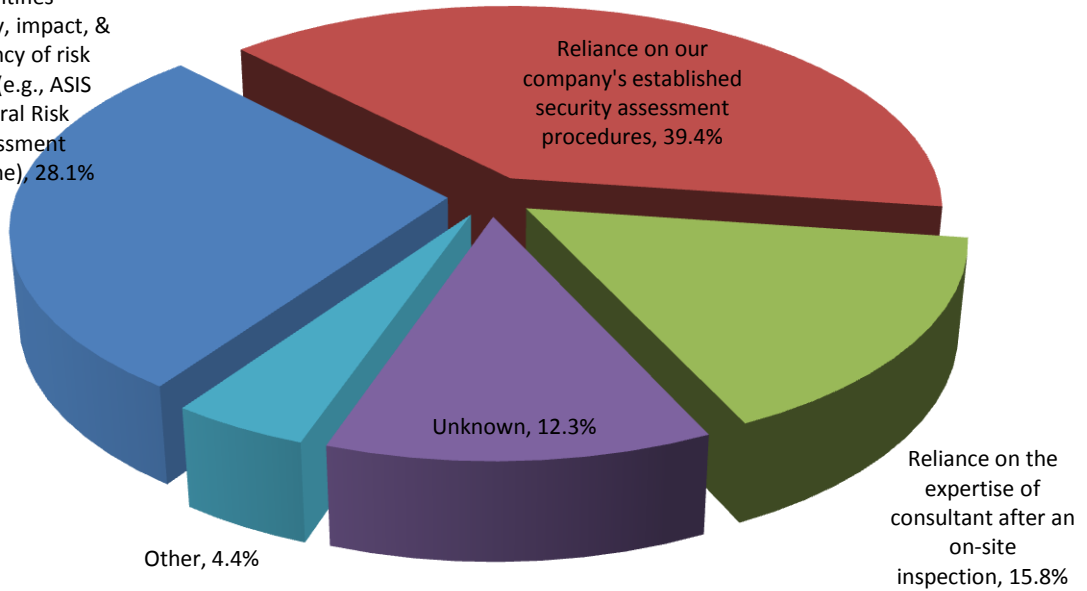


13. Who performs the risk assessment?

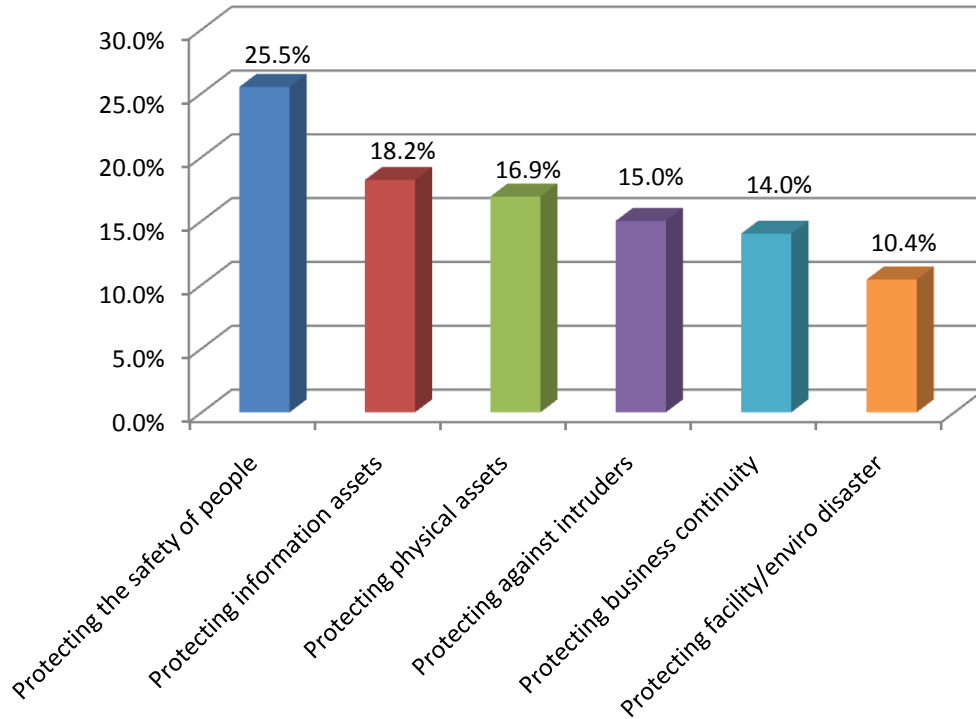


14. What methodology is used in performing your risk assessment?

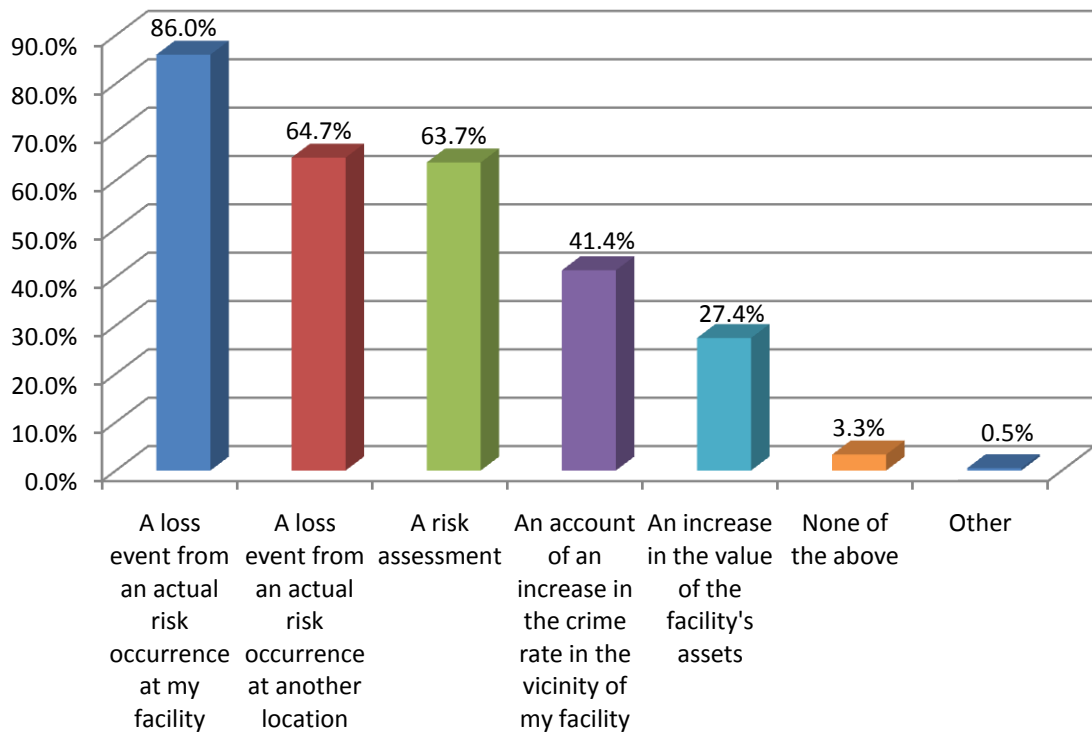
A professionally recommended method that logically identifies possibility, impact, & frequency of risk events (e.g., ASIS General Risk Assessment Guideline), 28.1%



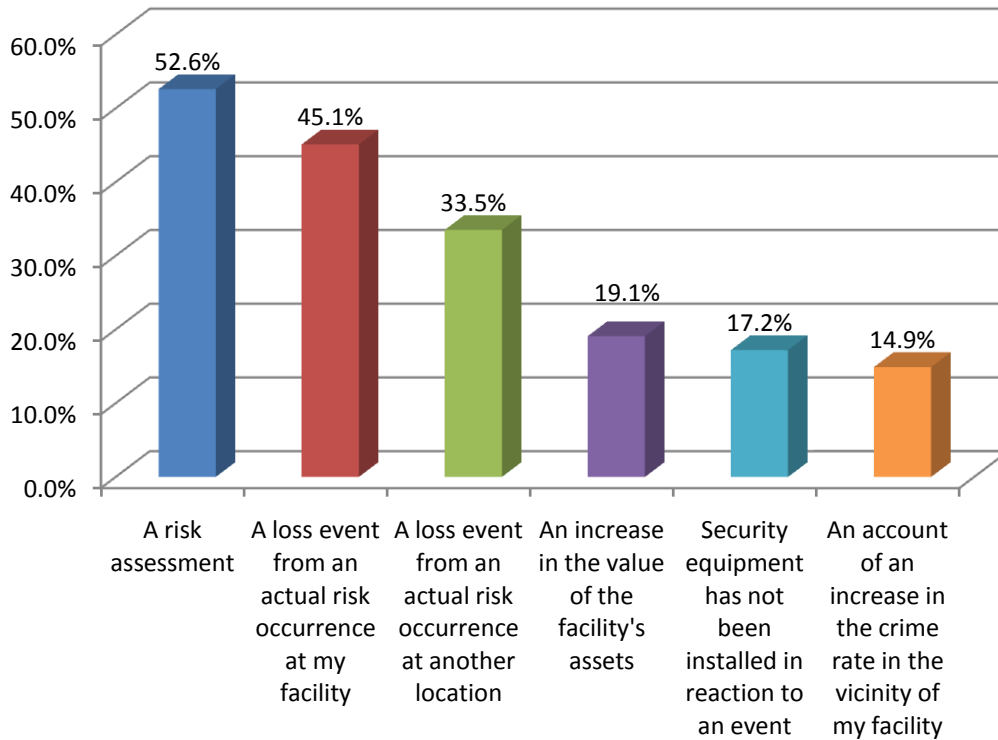
15. On which of the following does your risk assessment place the most emphasis?



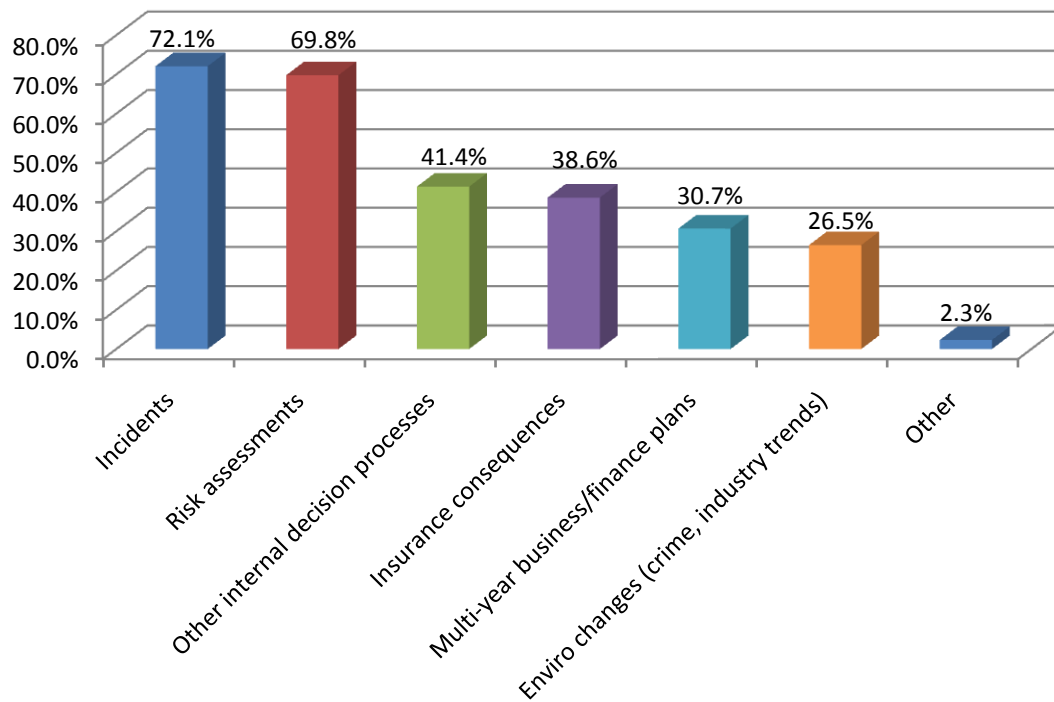
16. In your opinion, would any of the following incidents cause security upgrades to be implemented at the facility you manage? Check all that apply.



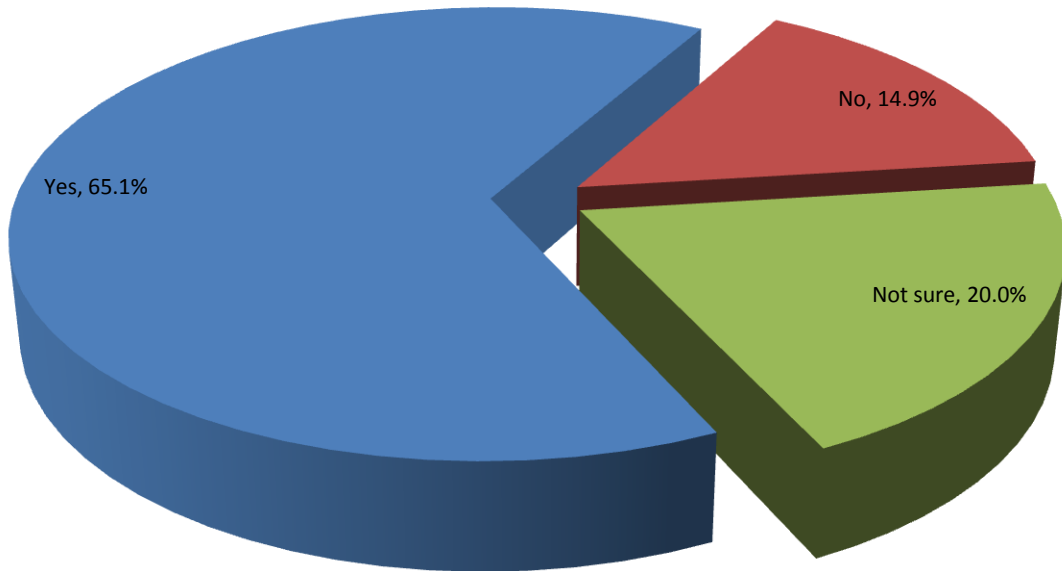
17. Has security equipment been installed at the facility you manage in reaction to one or more of the following incidents? Check all that apply.



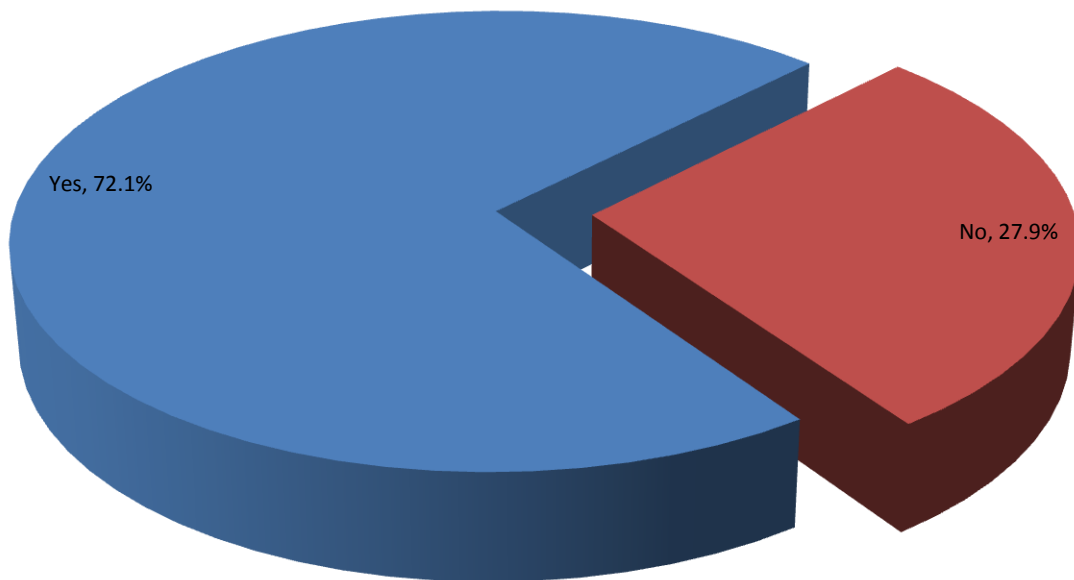
18. On what basis are decisions to make security upgrades initiated? Check all that apply.



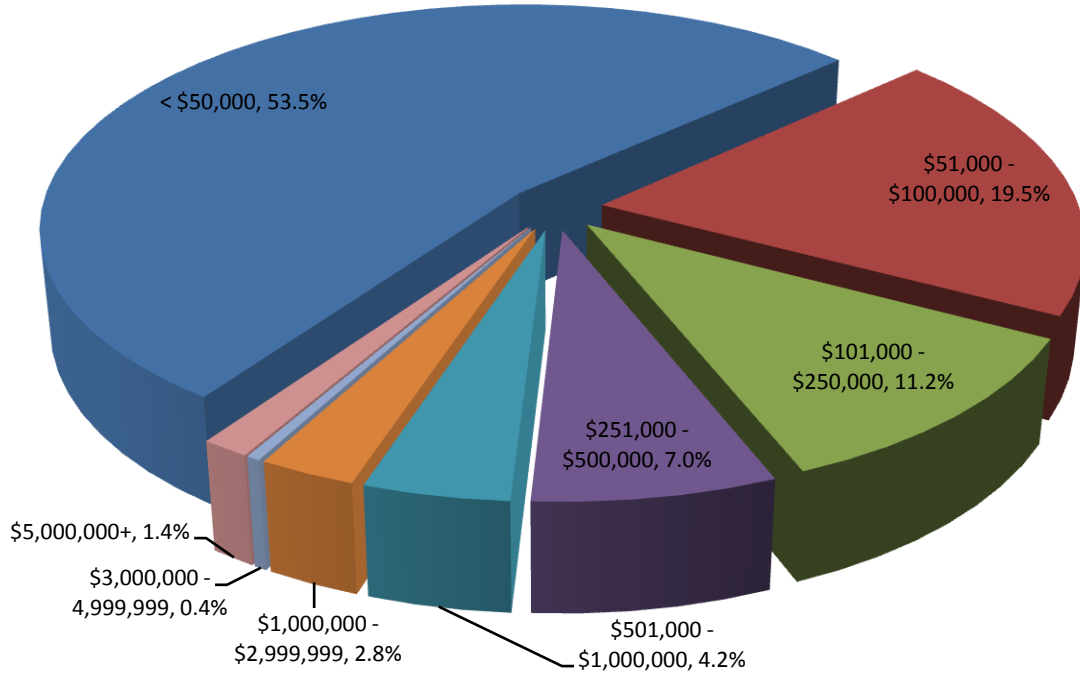
19. When evaluating options to mitigate risks, is a cost/benefit analysis performed?



20. As a building facility manager, do you have responsibility for making budget decisions about security requirements for your facility?

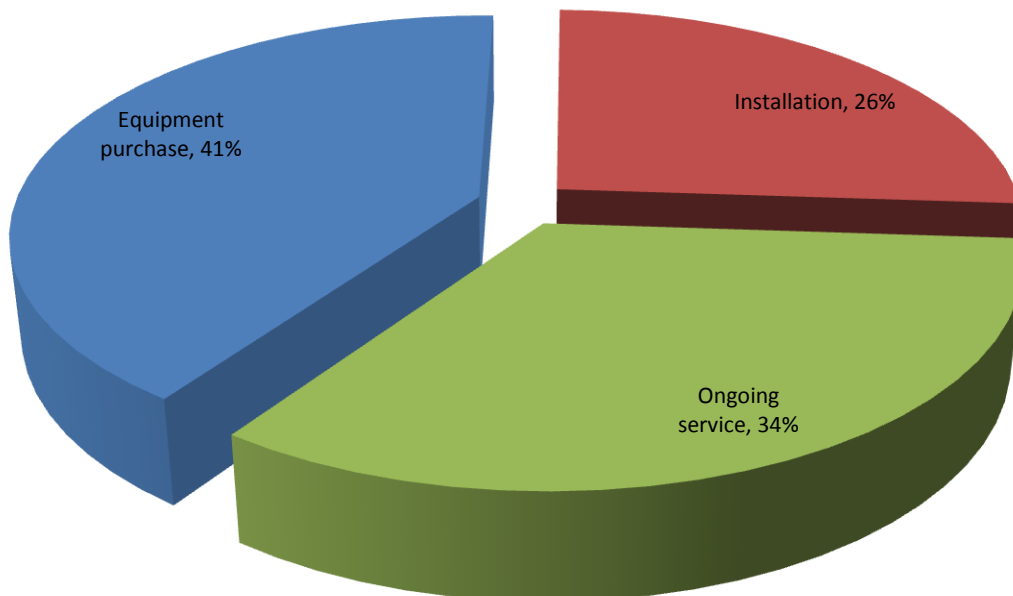


21. To your best knowledge, what is the annual budget for the purchase, installation, and service of electronic security equipment at your facility? (This excludes guard force operation.)

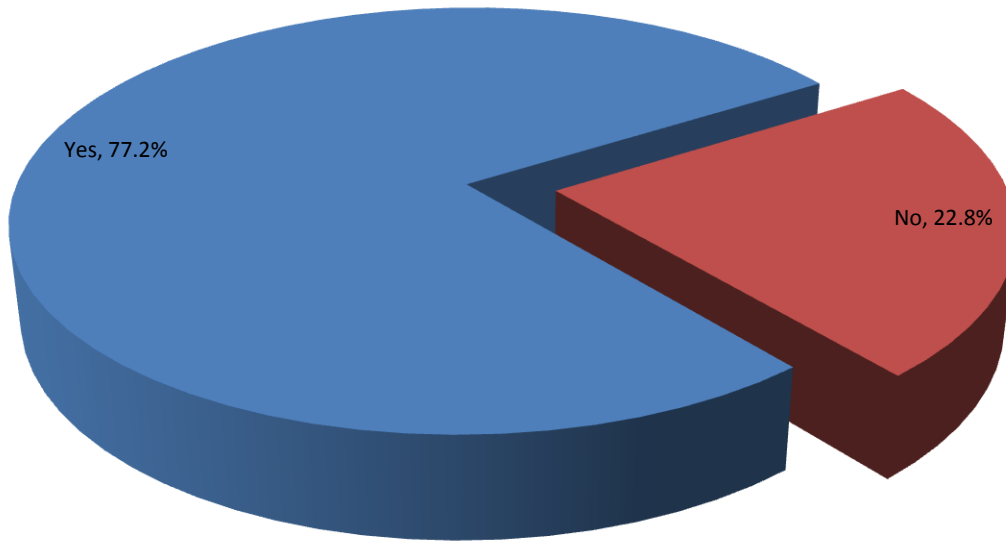


22. With regard to the budget in the previous question, to your best knowledge, what percent is allocated to the purchase of equipment, installation of equipment, and on-going service (maintenance and human resources, excluding guard services)? The total of all three must equal 100 percent.

Approximate figures based on mean responses:



23. Do you have responsibility for making buying decisions about security equipment and/or service purchases?

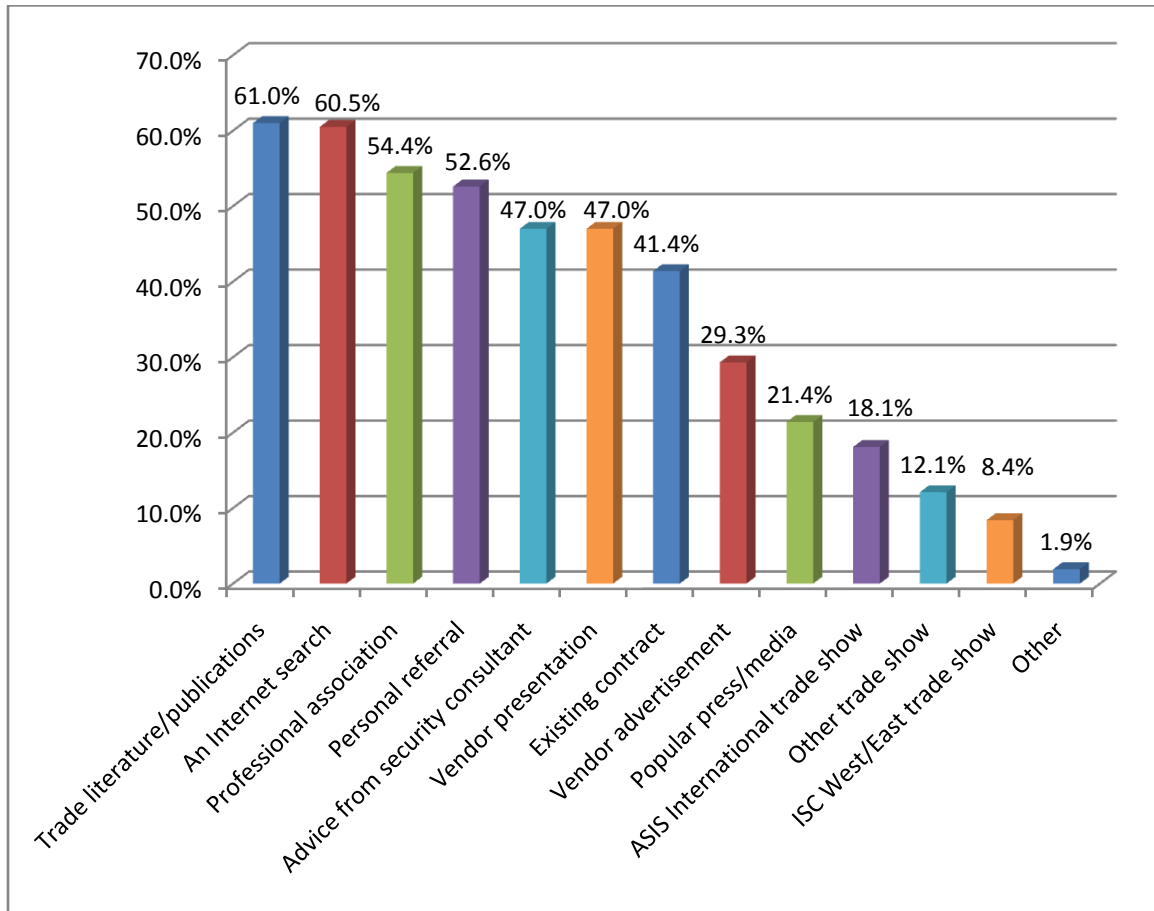


24. If not, please specify the job title of the person who oversees the process of security system and service purchases.

Answers included the following titles:

- | | |
|---|--------------------------------|
| board of directors | director of security |
| business manager | district manager |
| chief executive officer | executive director |
| chief operating officer | facility manager |
| chief security officer | facility director |
| corporate manager of facilities & loss prevention | general manager |
| design and construction manager | human resources manager |
| director of environmental care | manager of electronic security |
| director of house services | owner |
| director of loss prevention | office director |
| director of operations | project manager |
| director of protection services | risk manager |
| director of public safety | safety & risk manager |
| director of safety & security | security manager |
| | security officer |

25. Which of the following sources are used to research information about security products and services for the facility you manage? Check all that apply.

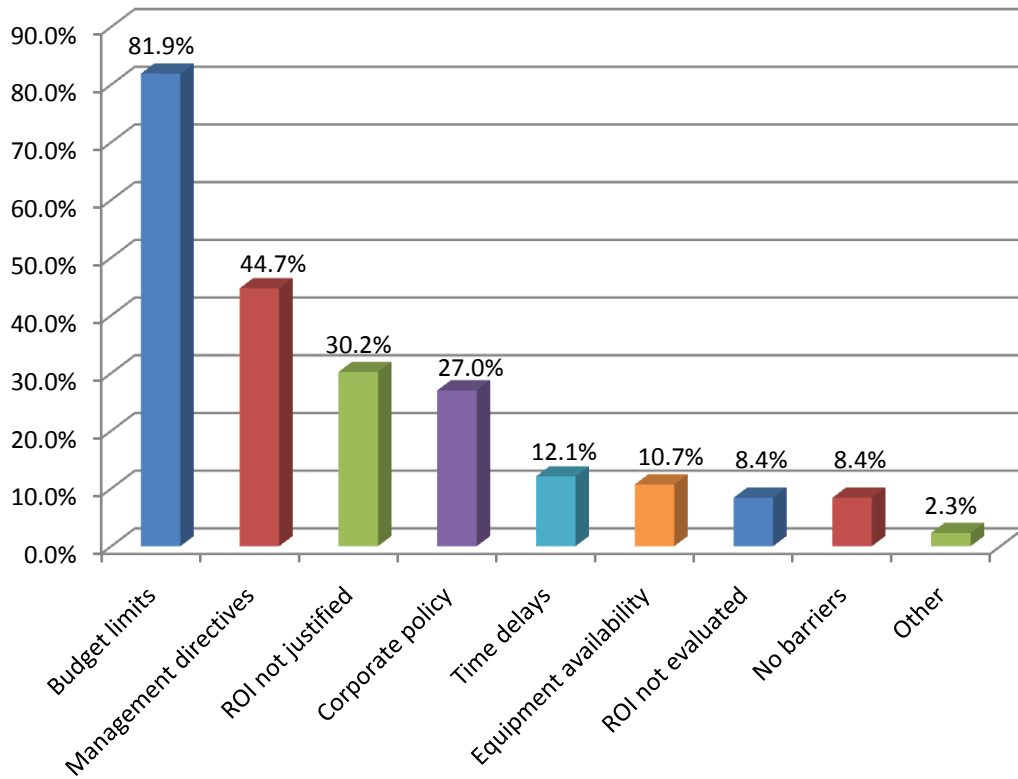


26. Rank in chronological order the steps that are performed when purchasing security. Ignore those not used.

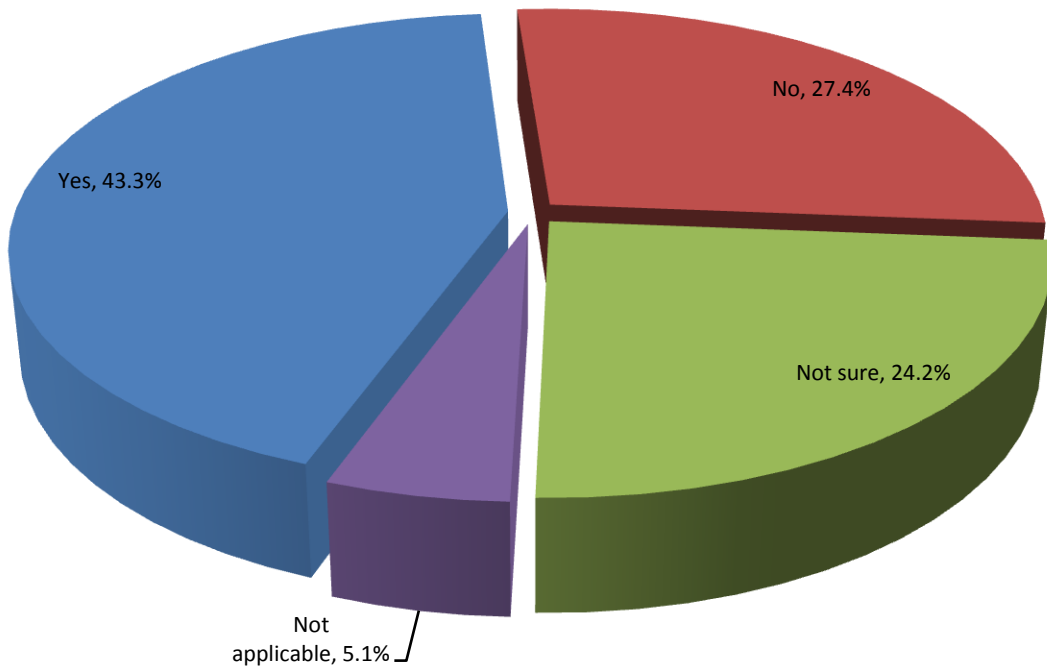
Collectively, respondents tend to perform the following steps, in this order:

1. Assess risk.
2. Analyze needs.
3. Develop budget.
4. Design specifications.
5. Solicit bids.
6. Obtain budget approval.
7. Retain consultant.
8. Hire contractor.

27. Which of the following barriers or deterrents to the purchase of a security system do you experience? Please check all that apply.



28. At your facility, is the effectiveness of the security project against the risk assessment measured after the installation?



2007 ASIS Foundation Board

President

Linda F. Florence, CPP
Vice President
Soaring Eagle Enterprises
Las Vegas, NV

Vice President

Judith Green Matheny, CPP
Vice President
Lehman Brothers Corporate Security
Littleton, CO

Secretary/Treasurer

David C. Davis, CPP
Director, Division Security
Northrup Grumman
San Bernardino, CA

Eduard J. Emde, CPP
Manager, Consultancy
Interseco
The Hague, Netherlands

Peter J. Mazzaroni, CPP
Manager, Community Affairs/Site Services
Roche Carolina
Florence, SC