

# SAFELIGHT

## SECURITY ADVISORS

Survey Results:

### **Information Security Training Lacking**

*Two out of three IT security professionals say the risk of data or systems breaches is related to a lack of training.*

IT security professionals ranked the threat of a data breach and the resulting damage to their company brand, and loss of customer loyalty and sales as the top business driver for information security training. Though surprisingly, the majority of companies do not have formal training programs to educate staff, according to Safelight Security Advisors' survey. Two out of three companies directly link data or systems breaches, or the risk of them, to a lack of security training at their organizations. Yet, the state of security training is fairly bleak even with information security programs in place. Only half of companies who rate themselves a low risk for a data or systems breach say their information security policies are effective at helping to prevent them. Often times security training courses are available, but not required for those on the front lines of information security: a company's IT and development staff.

In this survey, 60 IT security decision makers from a range of industries were asked how their companies are integrating people into their information security strategies and what practices are most effective. They were asked to estimate their current risk for a data or system breach and were categorized as either a low or high risk company. A data or systems breach was defined as including the accidental loss of control over sensitive data to malicious theft of data by insiders or external threats. They also responded to questions about the effectiveness of their organization's security programs in people, process and technology areas, the security awareness of their management teams and the effectiveness of training IT and non-IT staff as well as IT and non-IT vendors and contractors.

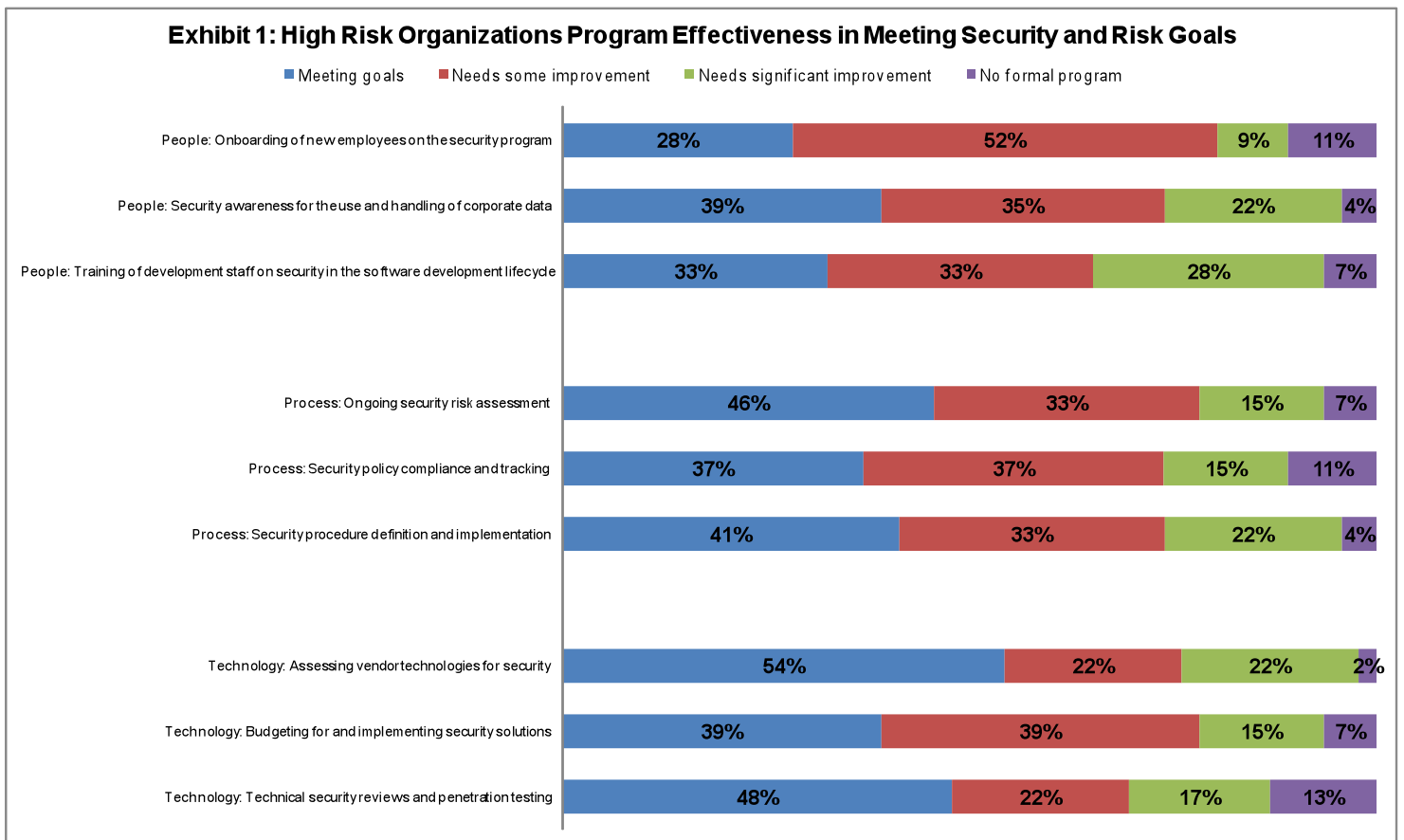
Companies at a low risk of a data breach were much more likely to say their people and process information security training programs were meeting their security and risk goals: 70 percent of low risk organizations on average versus less than 40 percent of high risk organizations. There is much less of a difference between low and high risk companies when it comes to how they

rate the effectiveness of technology areas, specifically how well they assess vendor technologies for security, budget for and implement security solutions and technical security reviews and penetration testing. In today’s tough economic climate where expensive technology investments may be temporarily on hold, smaller, incremental investments targeted at training personnel on security awareness and compliance, as well as processes for ongoing security risk assessment, security procedure definition and implementation, and compliance tracking, may return significant reductions in risks for companies.

**People and process issues trump technology concerns for high risk companies**

People and process training is not meeting high risk companies’ security and risk goals, and the survey indicates that they are a higher concern on average than technology issues (Exhibit 1). Lack of initial training of new employees, and training related to use and handling of corporate data are top people issues. More than 60 percent of IT security professionals who categorized their companies as at a high risk of a data or systems breach said that risk is related to lack of initial training of new employees. 57 percent said the way their companies train employees on the use and handing of corporate data needs “significant” or “some” improvement. Fifteen percent of organizations have no formal programs to address either issue.

High risk firms also cited process issues as needing some or significant improvement: ongoing

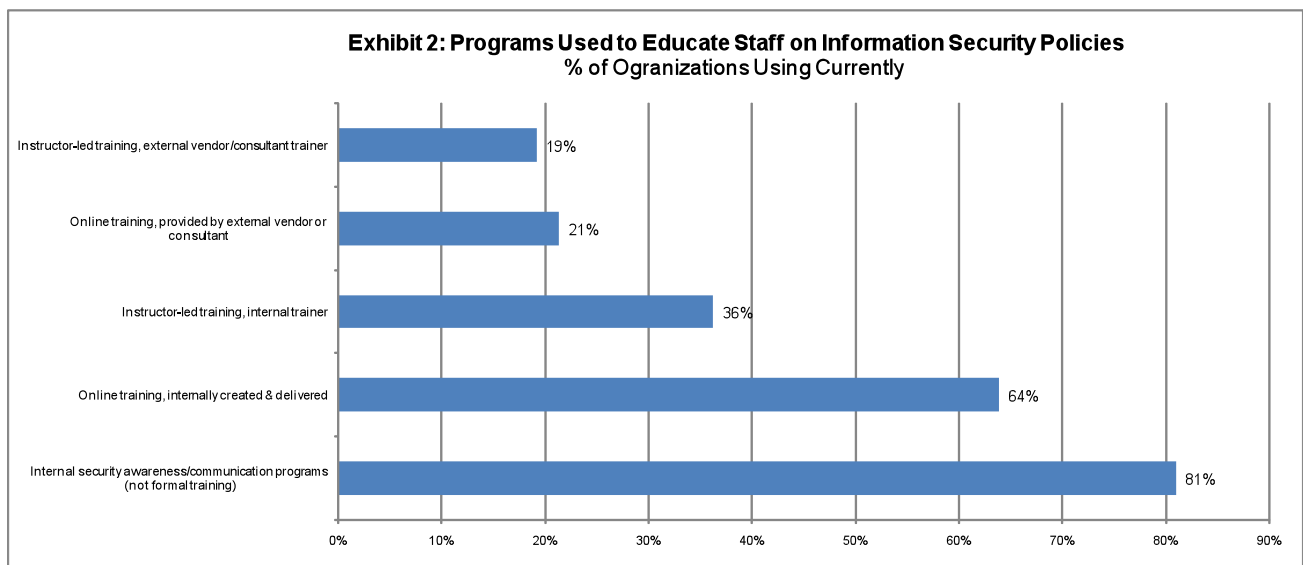


security risk assessment (48 percent); security policy compliance and tracking (52 percent) and security procedure definition and implementation (55 percent).

### Informal and “do-it-yourself” (DIY) security training dominates

Informal training and DIY dominates the corporate IT training landscape. More than 80 percent don't have a formal information security training program in place to educate staff on security policies (Exhibit 2). When companies did conduct formal training, they did it themselves: most often using internally-created online training and instructor-led training by internal staff.

Companies only used external training 20 percent of the time with the majority of that training dedicated to IT staff.



### The most risky and best trained

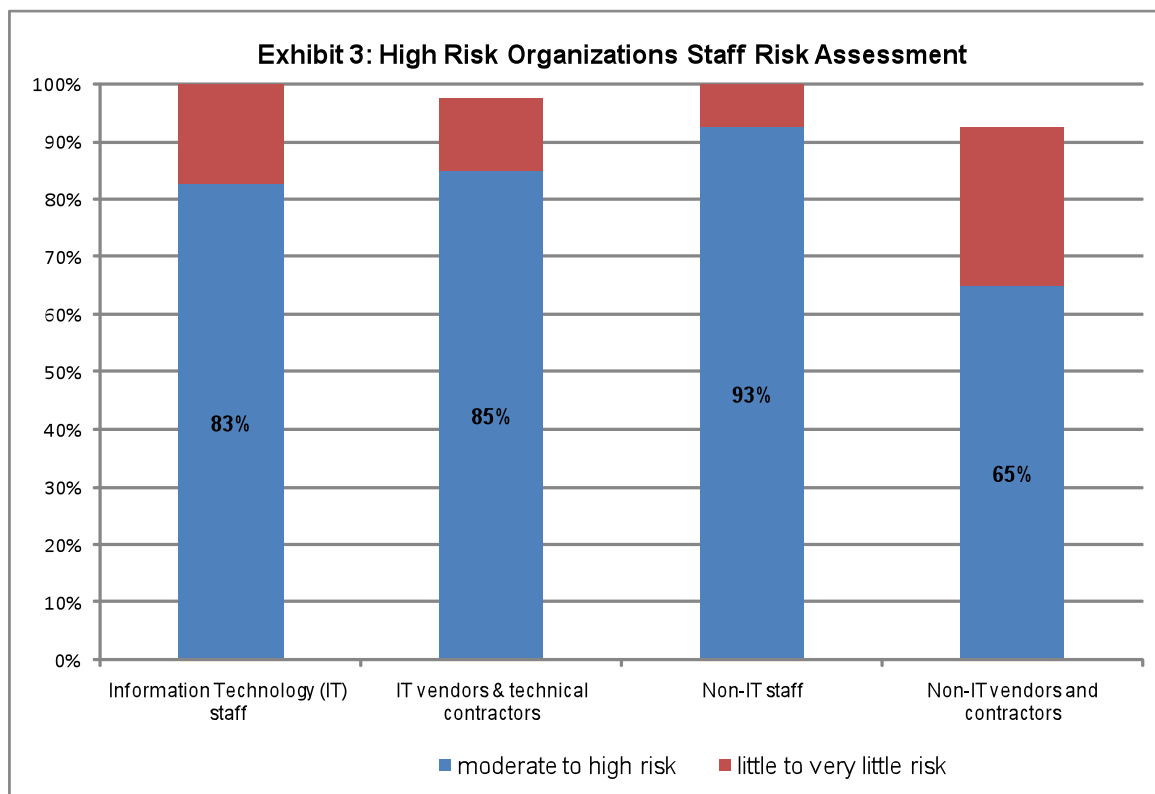
When asked to rate which four staff categories present the greatest information security risk to the company, security professionals agree that they are at the highest risk from IT vendors and technical contractors. With only 20 percent of high risk companies rating their security training as effective, it is not surprising that the majority of them say that *all* staff, whether internal or external, present a moderate or high information security risk (Exhibit 3).

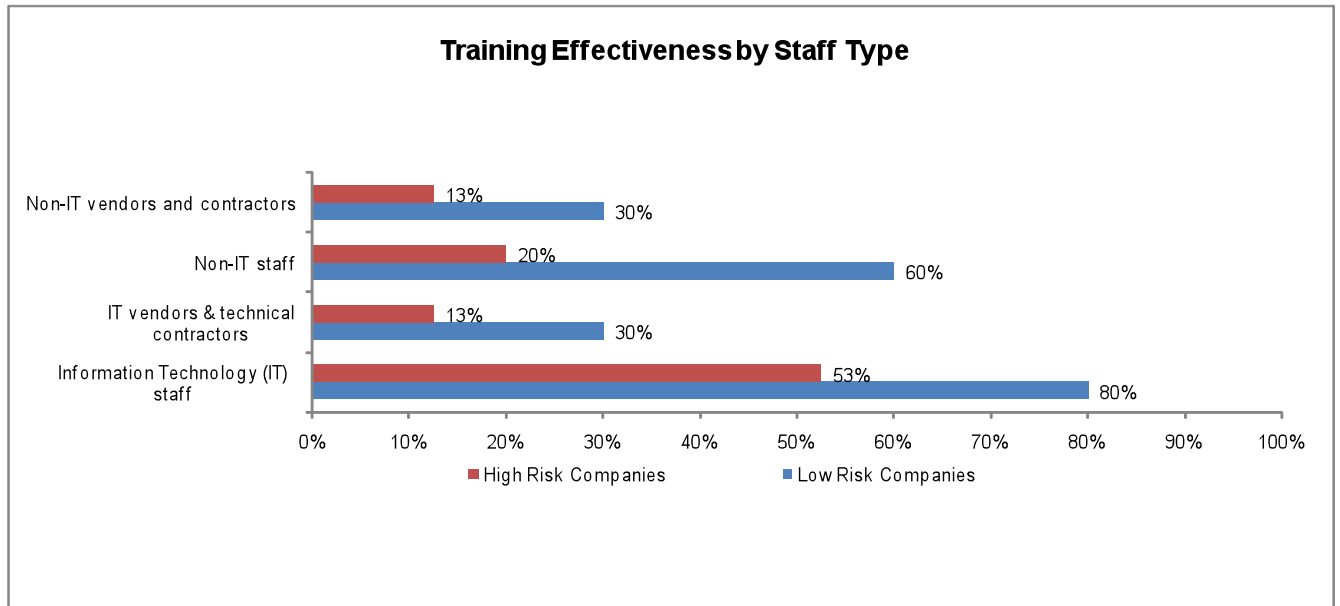
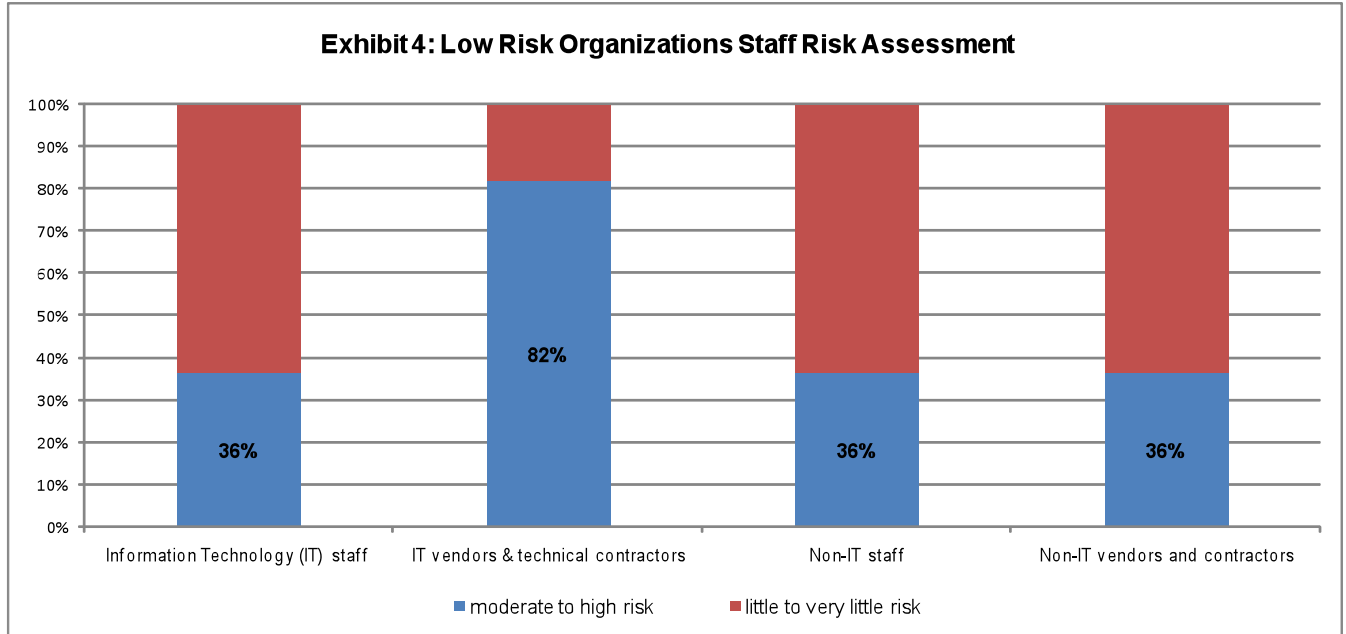
In contrast, only a third of low risk companies said they are at a moderate to high risk from their IT staff, non-IT staff, vendors and contractors. One reason is that they are doing a better job

training them. Eighty percent rate their training of IT staff, as effective or very effective; 60 percent say non-IT staff training is effective; and 30 percent rate say non-IT vendor and contractor training is effective (Exhibit 4).

A reason why high risk companies' IT staff security training is not effective may be that companies are making courses available, but not requiring staff to take them. Of the 13 application, data and infrastructure courses listed in the survey only one course, Application Security Fundamentals, is required by more than 30% of appropriate staff.

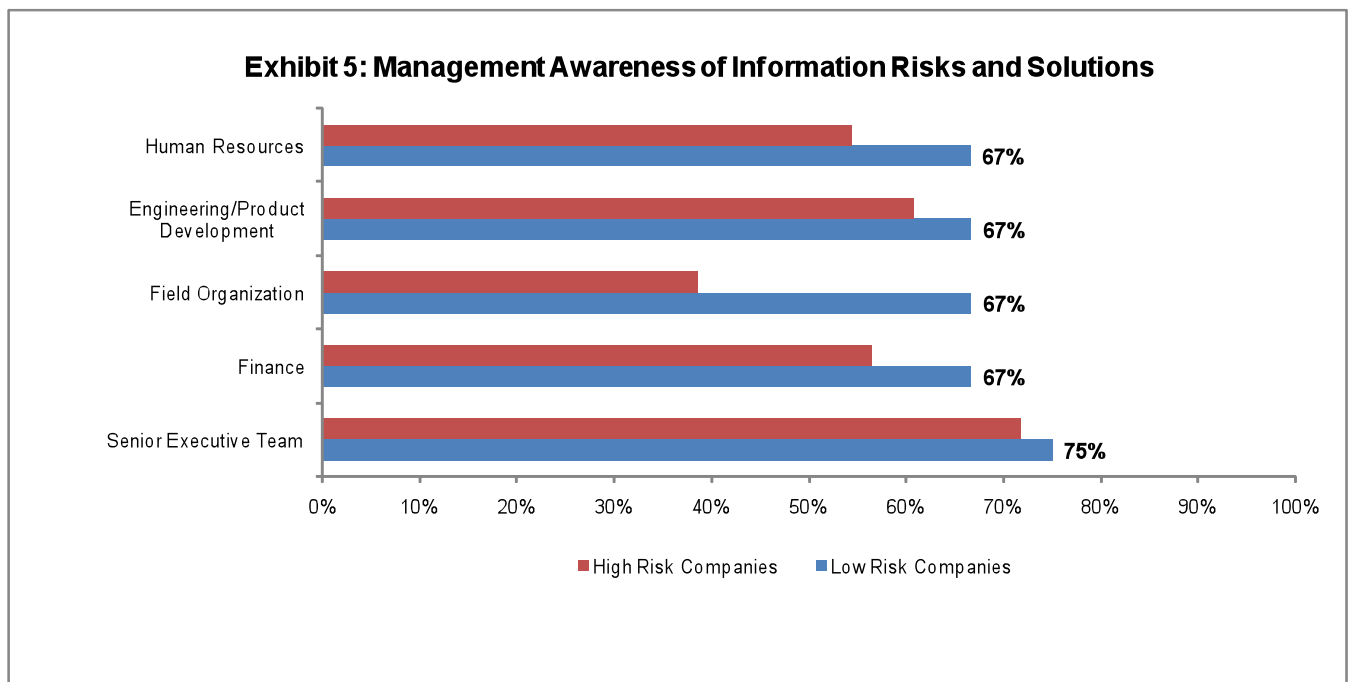
Companies are reducing their risk from IT vendors is by requiring a security pre-screening assessment. Even with screenings to help them determine where the gaps are, when companies do implement training of this group, they don't think it's very effective, nor do they think they are doing a good job training non-IT vendors. Training of non-IT vendors and contractors, non-IT staff and IT vendors and contractors is only effective in 20 percent or less of these high risk companies.





**Management team engagement and techniques used**

Both low and high risk companies engage the senior executive team in their information security awareness programs while two thirds of low risk companies engage all of their management teams in their information security awareness programs, including human resources, engineering/product development, finance and the field organization (Exhibit 5). One area where high risk companies fall behind is the field organization, with the next greatest gap between high and low risk companies being human resources. The tools companies most often used to engage the management teams on information security programs and issues were presentations and seminars. The survey indicates that low risk companies tend to employ more proactive techniques such as dashboards and creative organization-specific tools versus high risk companies which use more reactive tools, including incident reports and analyst reports.



## Looking ahead

- Effective people and process training can lower a company's security risk. Some of the gaps that companies need to fill include make more of the training courses they offer to IT staff a requirement, focusing more effort on training non-traditional staff categories such as the field organization, and those presenting the greatest risk to the organization: IT vendors and technical contractors.
- Companies equate data or systems breaches or the risk of them to a lack of security training, but the majority has not put formal training programs in place. Given the increase in data and system breaches and the fact it's a top business driver for security training, we expect that more companies will put a focus on formalizing their IT security awareness training efforts.
- The survey finding show that organizations at a low risk for a data or systems breach have put in place a series of best practices to address the people and process areas of their information security programs. These include the following:
  1. Possess strong people training and process information security programs that meet their organization's goals
  2. Have adequate budget to address information security awareness and prevention
  3. Engage all of the management teams in their organization in the information security programs
  4. Use proactive versus reactive techniques to engage their leadership teams
  5. Reduce their vendor/contractor risk with effective training and required security screenings
  6. Establish a good understanding of information security policies with non-IT staff and non-IT vendors and contractors