Information Security Teams Drastically Underfunded, Understaffed

Article By:

Hilary Tuttle

As the information security industry's hackers, IT professionals, technology developers and even Hillary Clinton's campaign descend on Las Vegas for this year's Black Hat conference, Black Hat has released the results of a survey from last year's convention, offering an insider's look at the state of cyberrisk. The report offers a failing report card for current investment on cyberrisk and some key feedback for the C-suite about current risk exposure.

The Rising Tide of Cybersecurity Concern is the second annual Black Hat attendee survey. Last year's results included the alarming findings that 72% of respondents felt it likely that their organizations would have to deal with a major data breach in the year ahead, while approximately two-thirds of respondents said they did not have enough staff, budget, or training to meet those challenges.
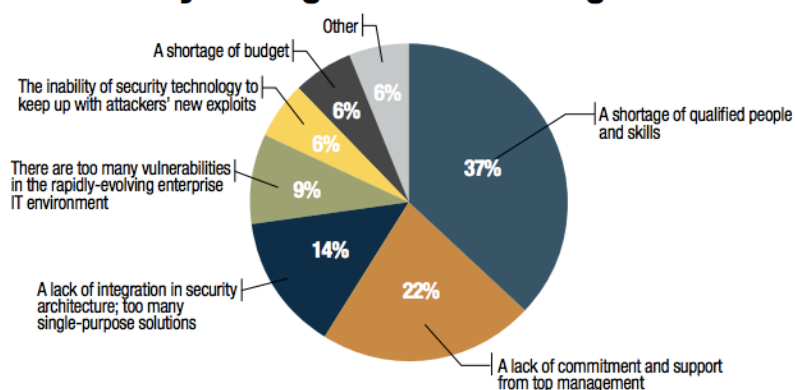
Unfortunately, these top security experts have only grown more concerned. As cyberrisks proliferate – and attention from the C-suite increases – 15% "have no doubt" they will have to respond to a major security breach in the next year, with another 25% considering it highly likely and 32% calling it somewhat likely.

Yet information security teams are not getting the funding, staffing or training they need to combat this top risk. Only 26% of those polled said they have enough staff to simply defend against current threats. Black Hat reports some 63% of security professionals say their departments do not have enough budget to defend their organizations against current threats, with 20% saying they are "severely hampered" by a lack of funding.

The training critical to effectively managing evolving cyberrisks also presents a considerable concern for many security professionals. Two-thirds of respondents said they feel they do not have enough training and skills they need to perform all of the tasks for which they are responsible — up from 64% last year. Ten percent of respondents said they feel "ill-prepared" for many of the threats and tasks they face each day.

Experts considered the top new cyberrisks:

What is the primary reason current enterprise IT security strategies and technologies fail?

Other — 6%
A shortage of budget — 6%
The inability of security technology to keep up with attackers' new exploits — 6%
There are too many vulnerabilities in the rapidly-evolving enterprise IT environment — 9%
A lack of integration in security architecture; too many single-purpose solutions — 14%
A lack of commitment and support from top management — 22%
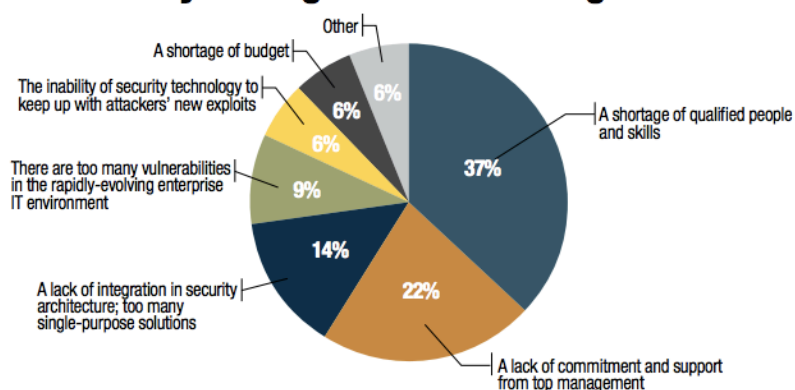A shortage of qualified people and skills — 37%

Base: 250 respondents in 2016; not asked in 2015
Data: UBM survey of security professionals, June 2016

The weakest links in enterprise security:

When asked why security initiatives fail, some 37% of respondents (a plurality) pointed toward this shortage of qualified people and skills, with a lack of commitment and support from top management the second-most frequently cited response at 22%.

"Organizational priorities such as compliance and risk measurement consistently reduce the time/budget available for security professionals to resolve issues they consider the most critical," Black Hat noted. "These pressing issues include targeted attacks, social engineering, and internal application security troubleshooting. Although the 2015 report revealed this trend, rather than a reverse in expenditure behavior, the issue has continued to increase."

Additional findings from the survey include:

- 37% see the re-emergence of ransomware as the greatest new threat to appear in the last 12 months
- The attacker that 36% of security professionals fear most is the one with internal knowledge of the organization
- While the emergence of the Internet of Things (IoT) has garnered much attention in recent years, only 9% of those surveyed are currently concerned with IoT security. However, 28% believe this will be a concern two years from now. This ranking has not altered since 2015.

Risk Management Magazine and Risk Management Monitor. Copyright 2025 Risk and Insurance

Source URL:https://natlawreview.com/article/information-security-teams-drastically-underfunded-understaffed