PulseReport
GATEPOINT RESEARCH

Enterprise Software Security Strategies

Summary Results • October 2014

Program Overview

- Between June and September, 2014, Gatepoint Research invited IT and Security executives to participate in a survey themed *Enterprise Software Security Strategies.*
- Candidates were invited via email and 300 executives have participated to date.
- Management levels represented were predominantly senior decision makers: 22% held the title CxO or VP; 56% were Directors, and 22% were Managers or Analysts.
- Survey participants represent firms from a wide range of industries including business, financial, and consumer services, education, healthcare, media, and manufacturing.
- 50% of the responding organizations are in the Fortune 1000. 18% had annual revenues between $500 million and $1.5 billion, 8% between $250 and $500 million, and 21% less than $250 million.
- 100% of responders participated voluntarily; none were engaged using telemarketing.

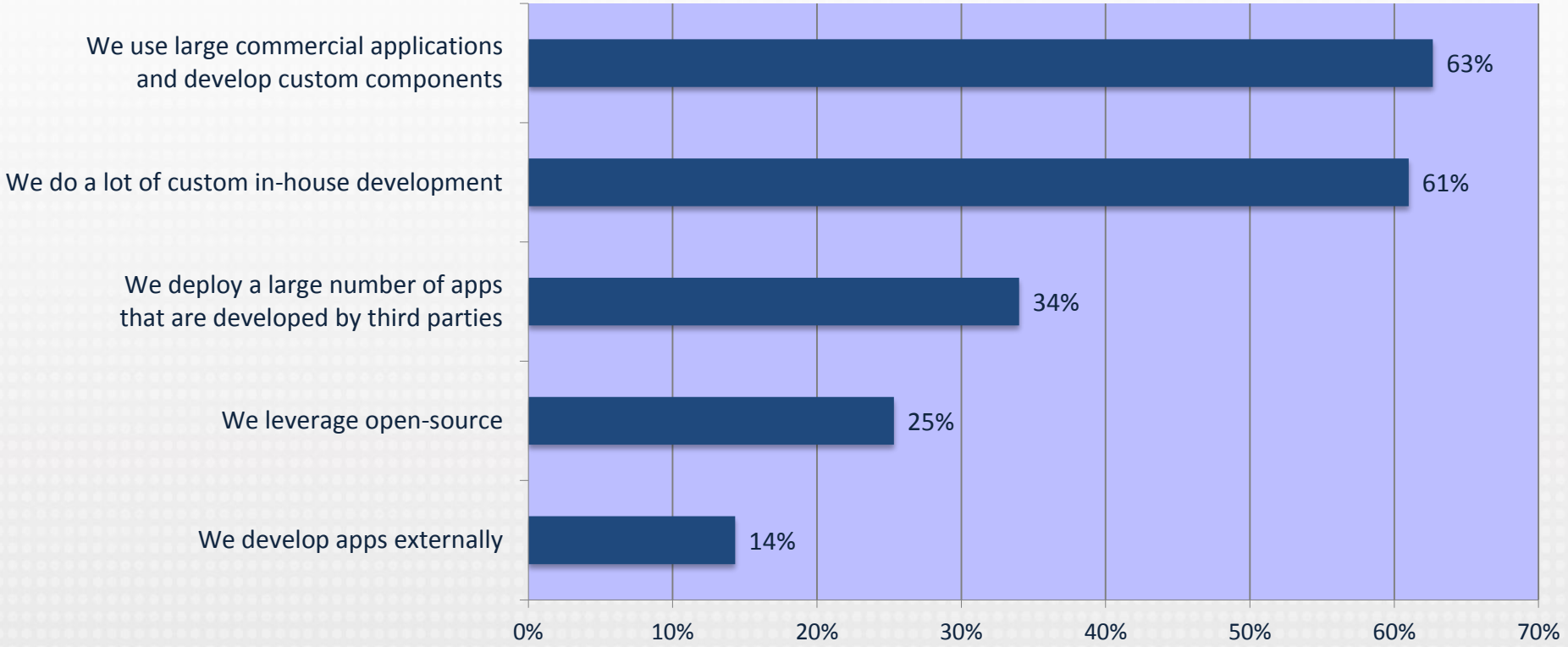
Observations and Conclusions

- **Application-related security breaches are a primary concern for surveyed IT and security executives**: 68% report that they are “very” or “critically concerned” about security issues within its applications.
- **Risk is exacerbated through the deployment of externally developed software that can’t be easily controlled**:
  - 63% use large commercial applications and develop custom components for those applications.
  - 34% deploy a large number of apps that are developed by third parties; 23% say more than half of their code is developed externally
  - Additionally, a high number of organizations rely on outsourced development including open source with 47% saying more than a quarter of their applications are developed externally
- **Despite these risks, outdated approaches to security persist:**
  - While 74% of responders report that they are doing some penetration testing (with a majority of testing being outsourced) for assessing the security of the web applications, a majority of enterprises (66%) focus on perimeter defenses (firewalls, encryption, virus protection), but have not invested in software security.

Observations and Conclusions

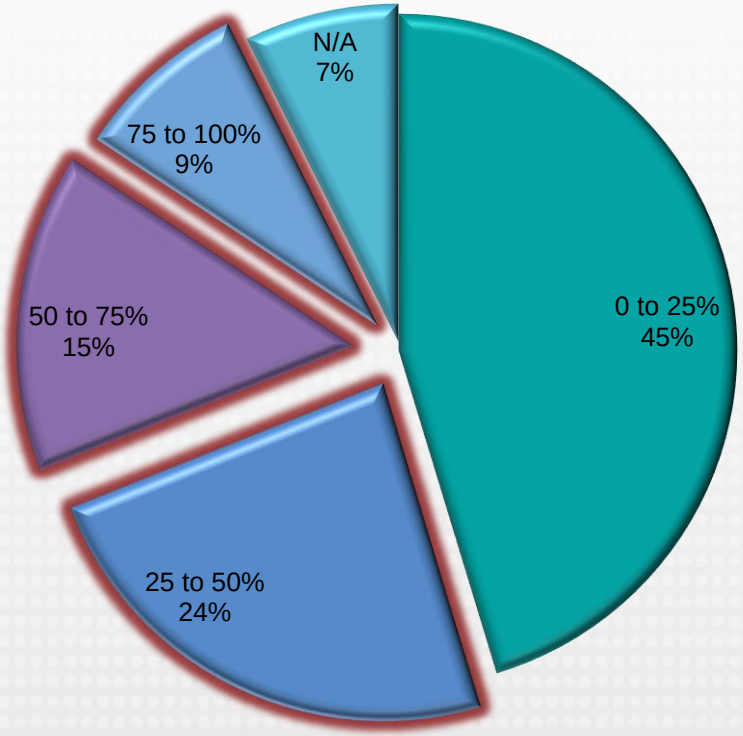
- **Stakeholder buy-in is a major hurdle to software security – 48% cite it as a top challenge to achieving software security goals. Other challenges include:**
  - Understanding the full risk in the portfolio (42%)
  - Keeping up with demand for deploying new apps (51%)
- **Confidence in software security is generally low:**
  - 52% admit to feeling not particularly upbeat or generally negative about the security of the software running in their business.
  - When asked about how they feel about the future of cyber attacks and hacking sophistication, 59% say every security professional needs to be on their game and 47% report that threats are expanding.
- **Despite the lack of confidence in the current security situation, senior management is waking up to security of business software and applications as a serious issue:**
  - 50% say they are beginning to set clear objectives and goals for business software and applications

How does your organization currently procure, build, and integrate software applications?



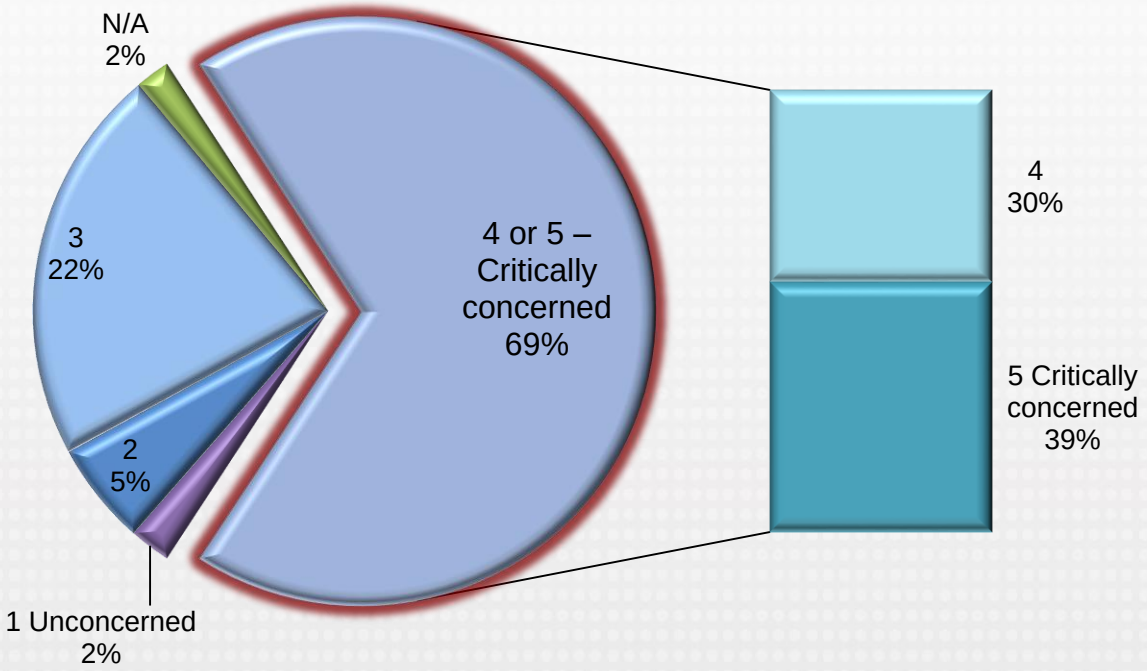
Surveyed organizations use a lot of customization to build, and integrate software applications: 63% use large commercial applications and develop custom components; 61% do a lot of custom in-house development.

What percentage of apps are developed externally?



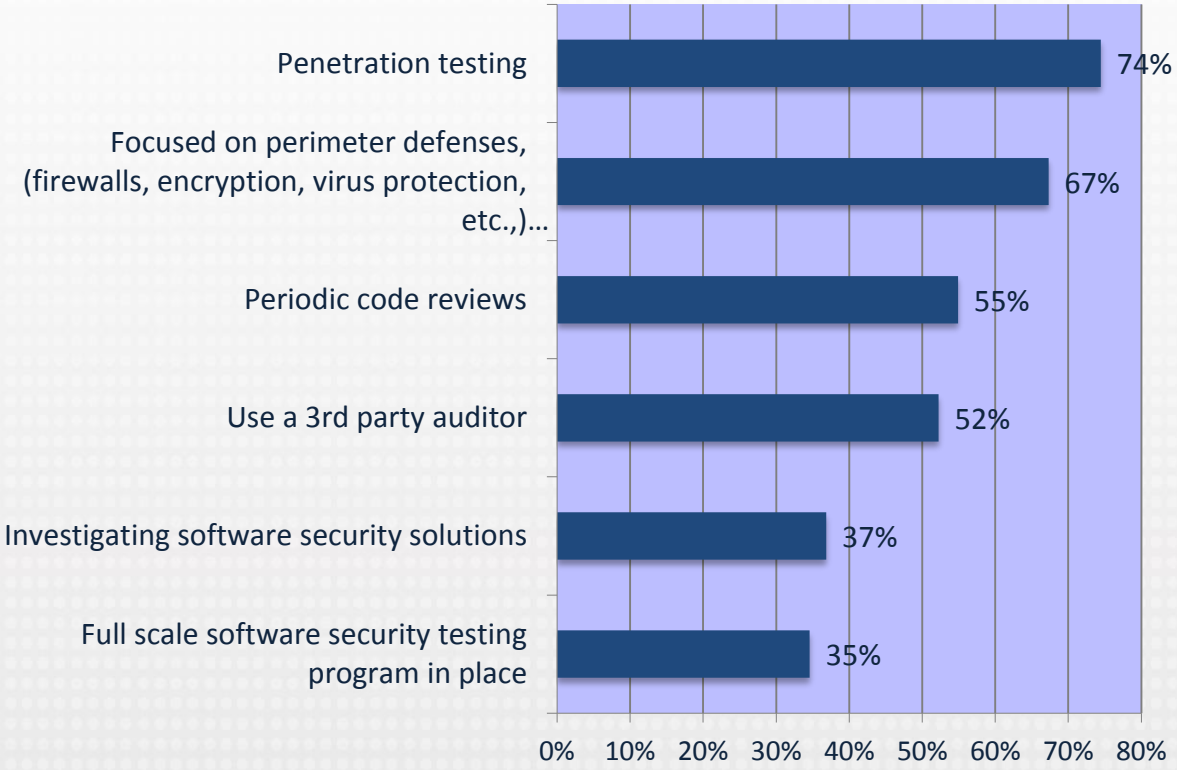
47% develop more than a quarter of their apps externally, and of those 23% develop more than half their apps externally.

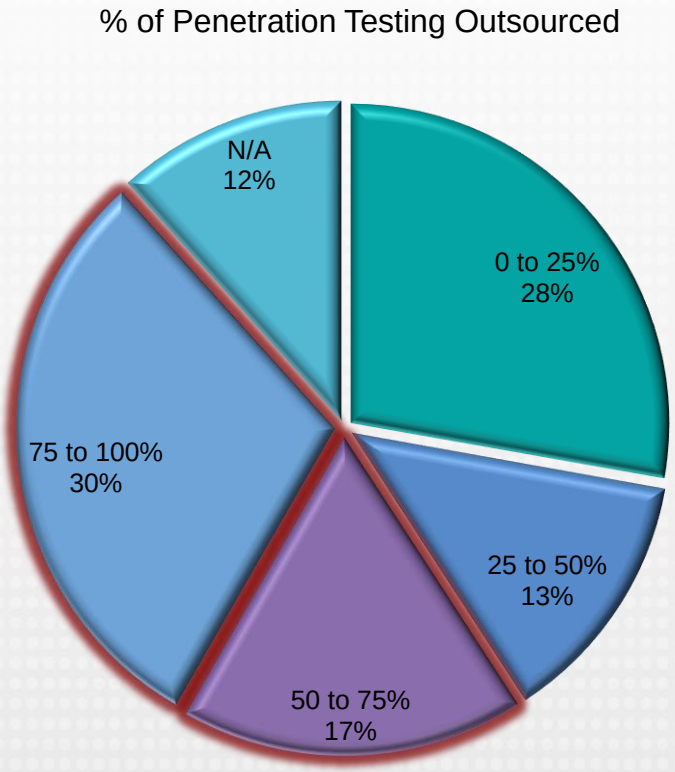
An estimated 84% of all security breaches are application-related, not firewall violations. To what extent is your organization focused on addressing security issues in its applications?
(Rate on a scale of 1-5, 1=unconcerned, 5=critically



69% report that they are very or critically concerned about security issues in its applications.

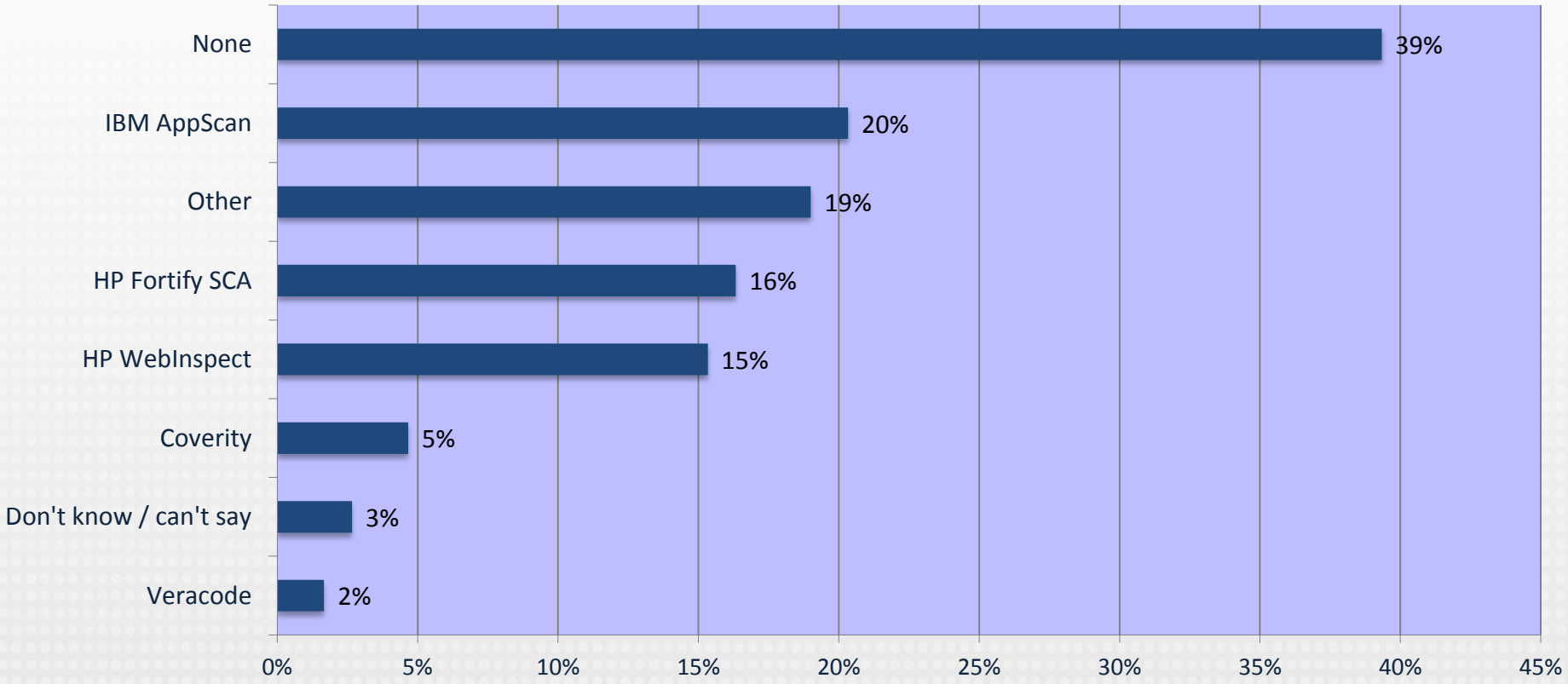
What are you doing to improve security at the application level?





Top method for improving security at the app level is penetration testing (74%). 47% outsource more than half their penetration testing.

Which software security products or solutions are you using to help protect the code of your custom-developed applications?



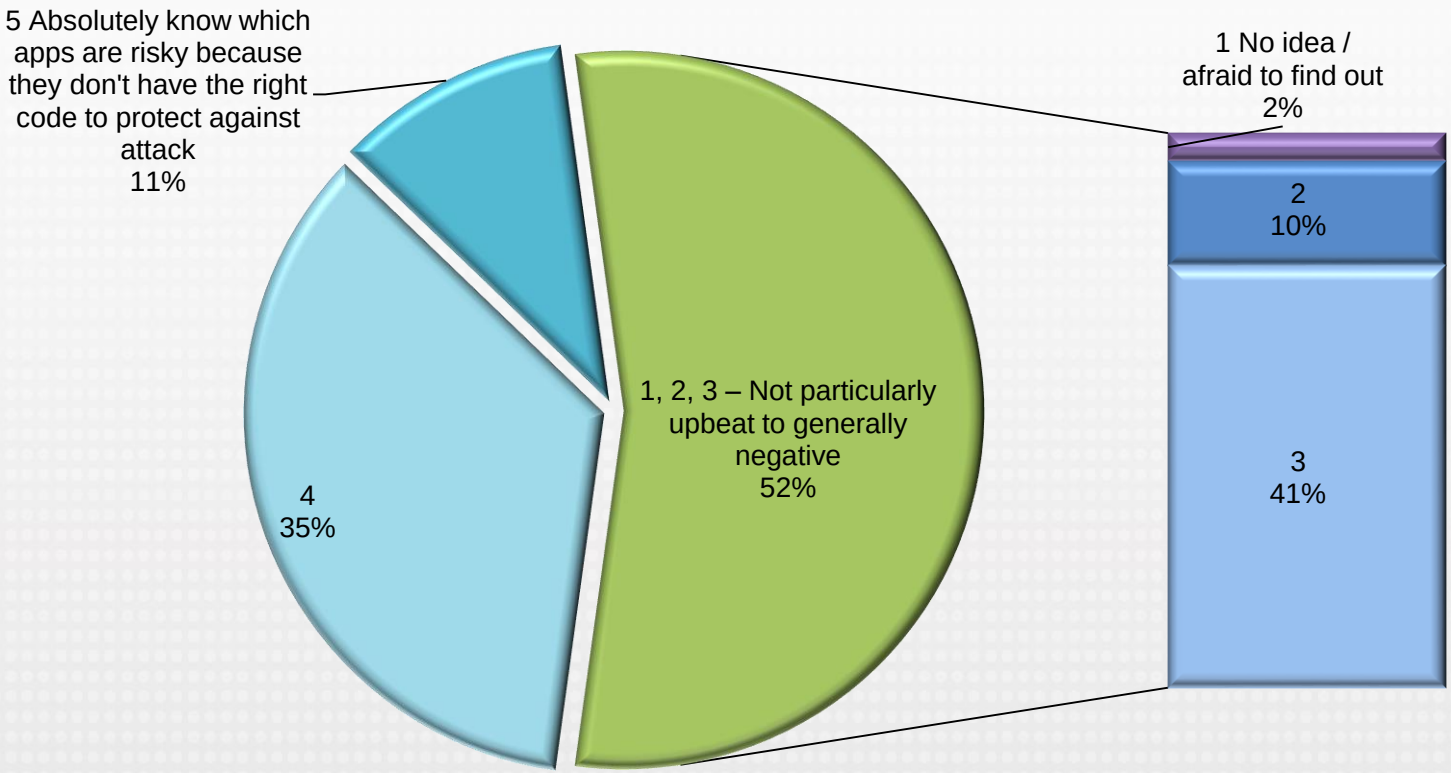
An astonishing 39% admit that their organization is not using any software security products or solutions to lock down custom code.

What are the top challenges you face in achieving your software security goals?

Stakeholder buy-in (48%), understanding the full risk in the portfolio (42%), and keeping up with demand for deploying new apps (51%) are top challenges cited with regards to achieving software security goals.

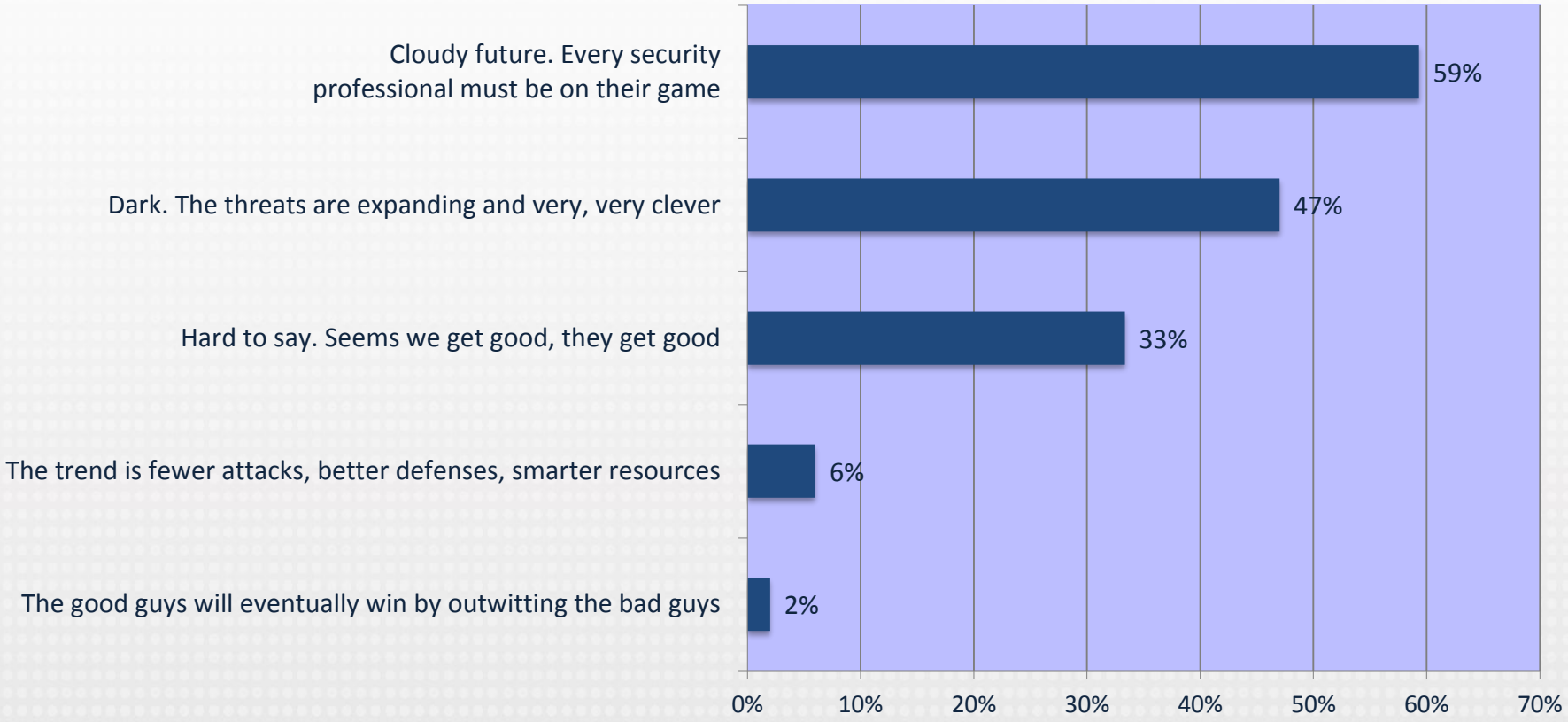
In light of the challenges you've identified, how do you feel about the security of the software running your business?

Rate on a scale of 1-5, (1= I have no idea and I'm afraid to find out. 5= I know with confidence which applications put us at risk because they lack the code to protect us against attacks.)



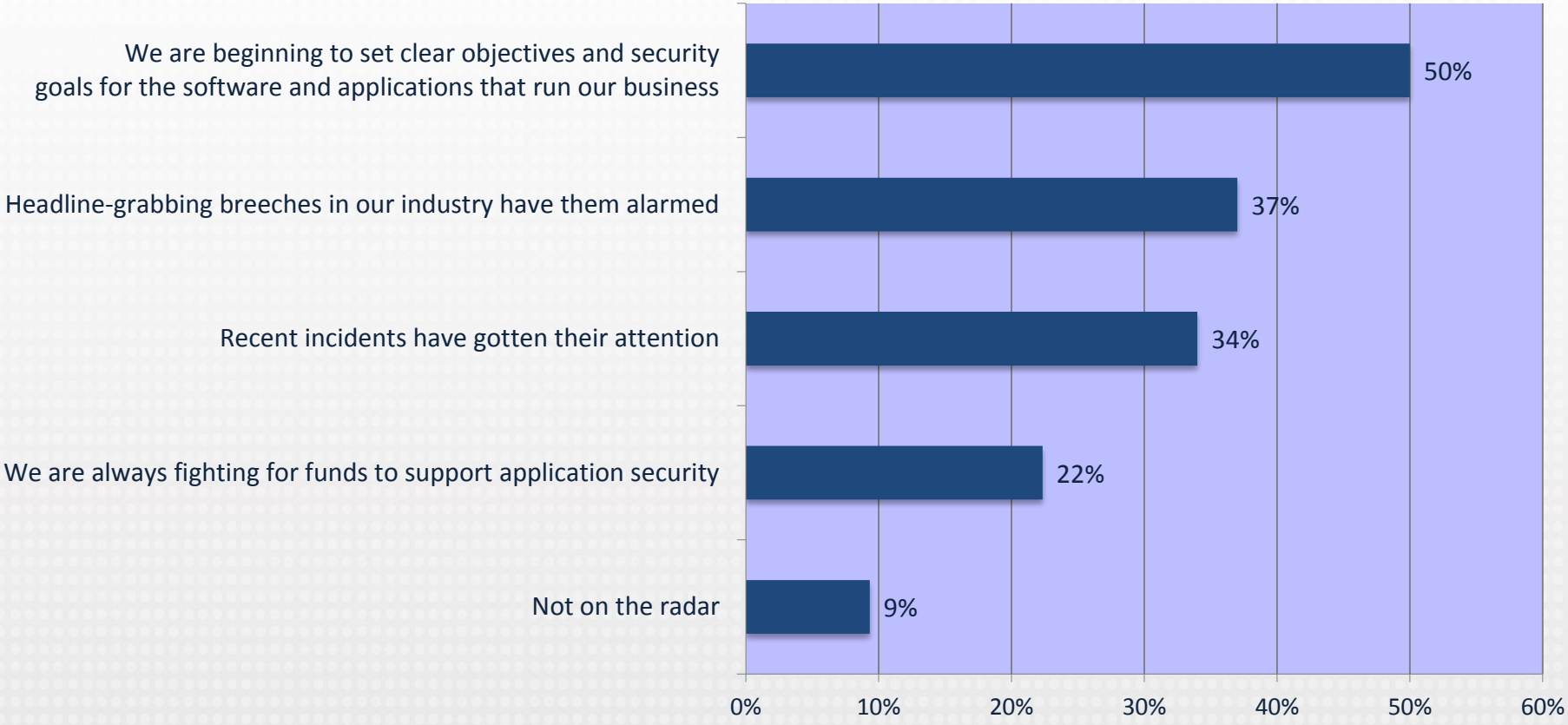
52% admit to feeling not particularly upbeat or generally negative about the security of the software running in their business.

What do you feel is the future of cyber attacks, hacking sophistication, etc.?



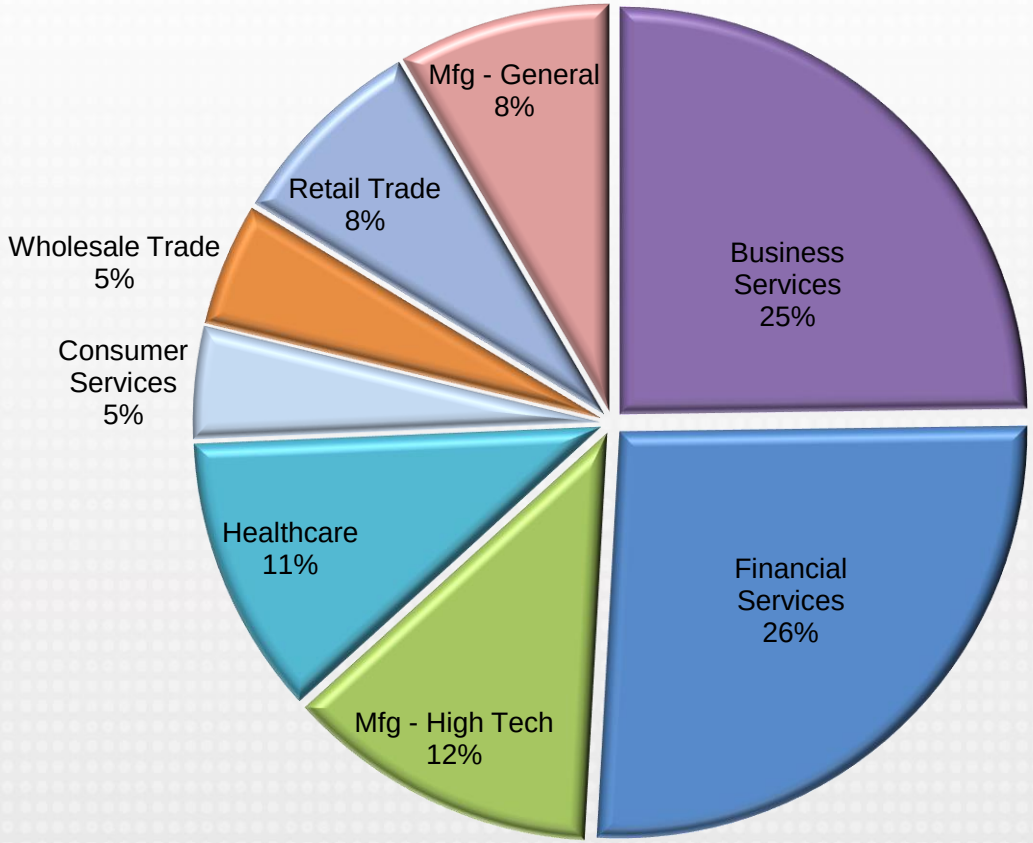
IT security execs expect to see increased cyber attacks and expanding sophistication in hacking.

How does senior management regard application security?



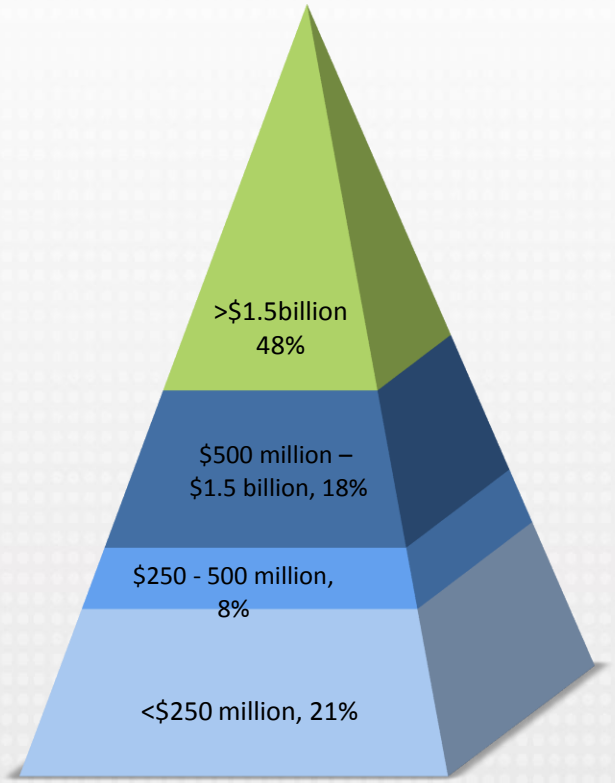
Senior management is waking up to security as a serious issue – 50% say they are beginning to set clear objectives and goals for business software and applications.

Profile of Responders: Industry Sectors



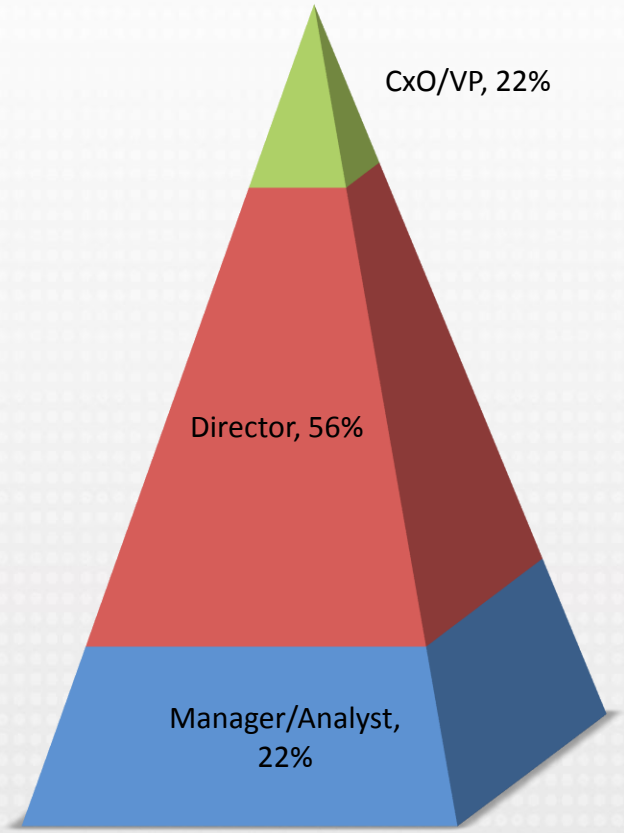
Responders come from a wide range of industries

Profile of Responders: Revenue



Responders represent companies from a wide range of revenue sizes.

Profile of Responders: Job Level



Survey participants are senior IT and Security staff and executives.

HP Fortify is an Application Security Testing solution that identifies and prioritizes security vulnerabilities in software so that issues are fixed and removed quickly before they can be exploited for cybercrime.

HP Fortify combines the most comprehensive static and dynamic testing technologies with security research from HP's global research team and can be deployed in-house or as a managed service to build a Software Security Assurance program that meets the evolving needs of today's IT organizations