Cyber Supply Chain Security and Software Assurance

Jon Oltsik

Senior Principal Analyst

March 1, 2011

Agenda

- Key findings
- Demographics
- The state of security at critical infrastructure organizations
- Software Assurance
- Government security involvement
- Summary

http://www.enterprisestrategygroup.com/2010/11/cyber-supply-chain-security-research-report/

Key Findings

- Lots of security incidents at critical infrastructure organizations
- Some due diligence of IT vendors*
- Software security gaining momentum but still immature*
- Critical infrastructure organizations want more help from the federal government*

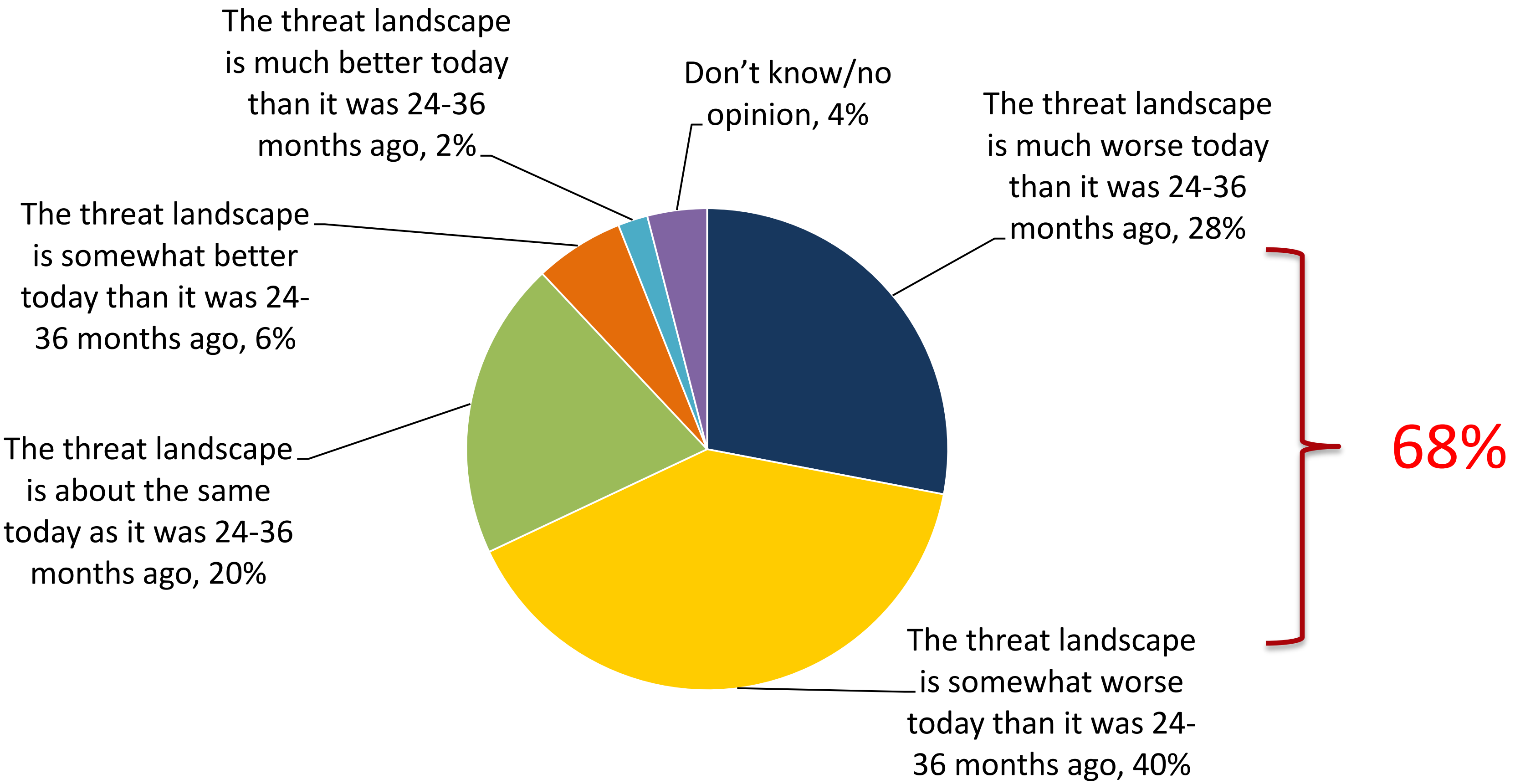
* Broad range of security behavior across the board

Demographics

- Survey of 285 security professionals working at organizations in "critical infrastructure" industries
  - 500 employees to over 20,000 employees
  - Biggest vertical representation: Financial services, health care, process manufacturing, and telecommunications
  - Heavily regulated firms
  - 26% of respondents, "very familiar" with cyber supply chain security

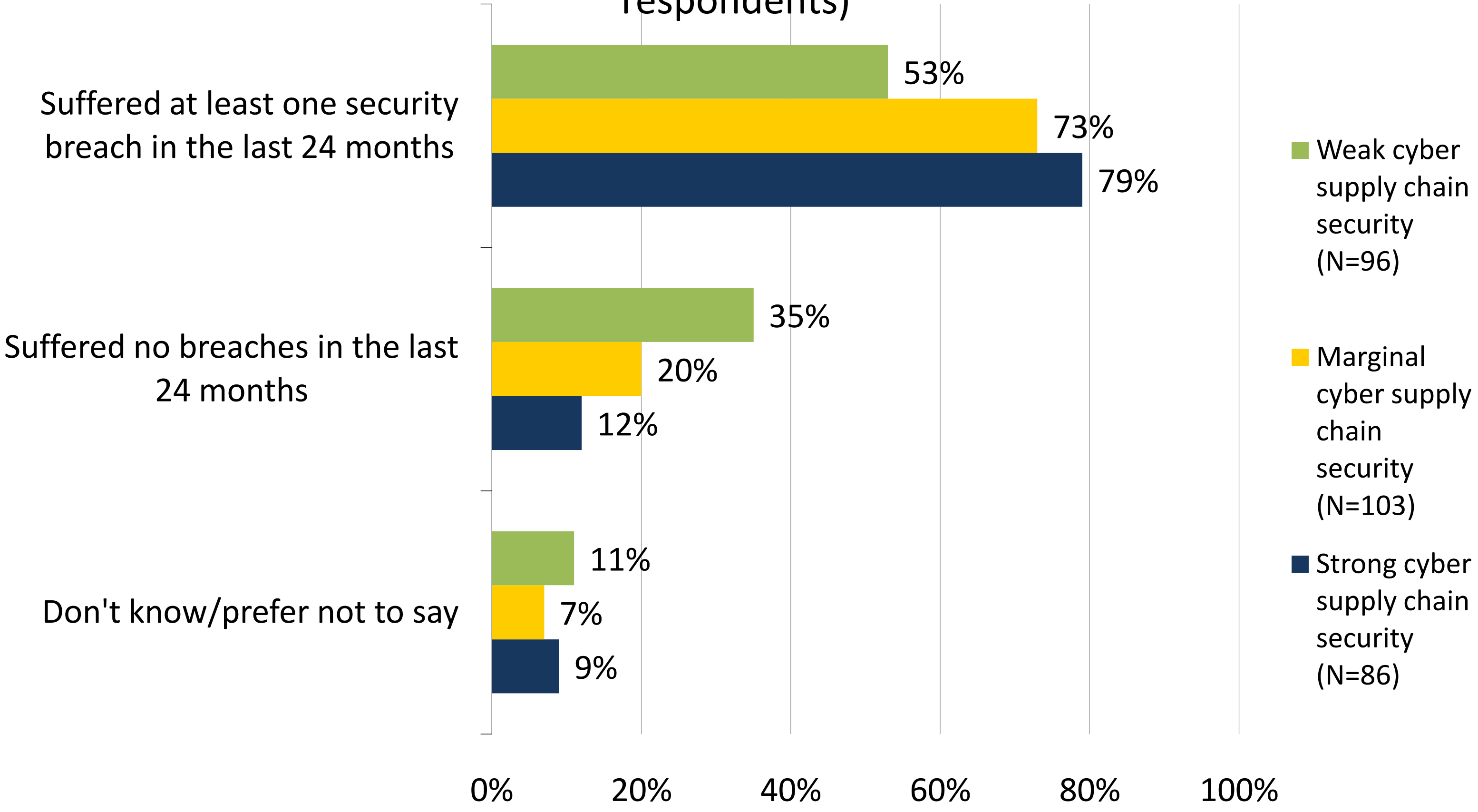
Rating of Current Cyber Security Threat Landscape

How would you rate the current cyber security threat landscape compared to the threat landscape 24-36 months ago? (Percent of respondents, N=285)



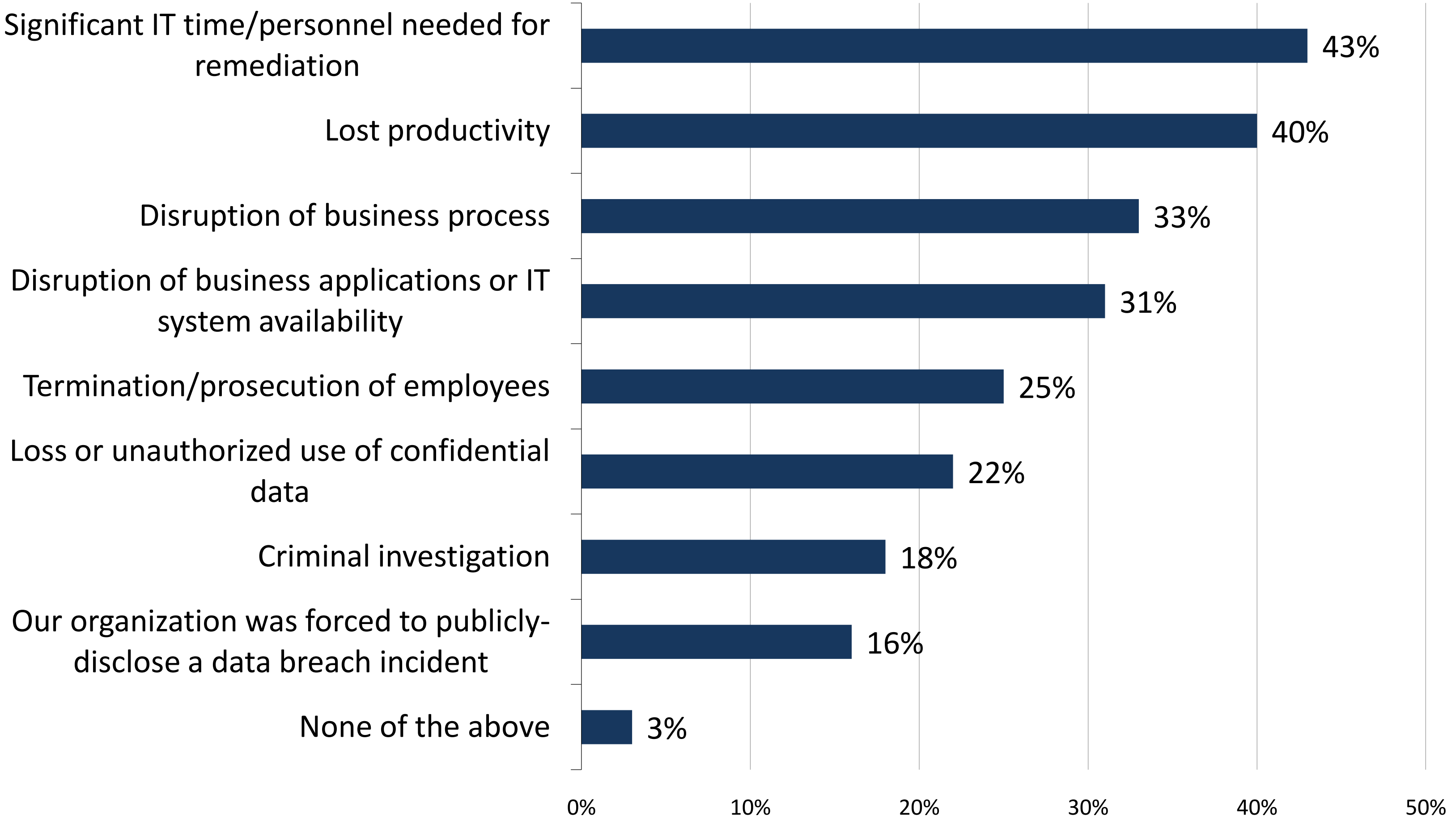
Security Breach Incidents

Has your organization experienced a security breach(es) over the past 24 months, by cyber supply chain segmentation (Percent of respondents)



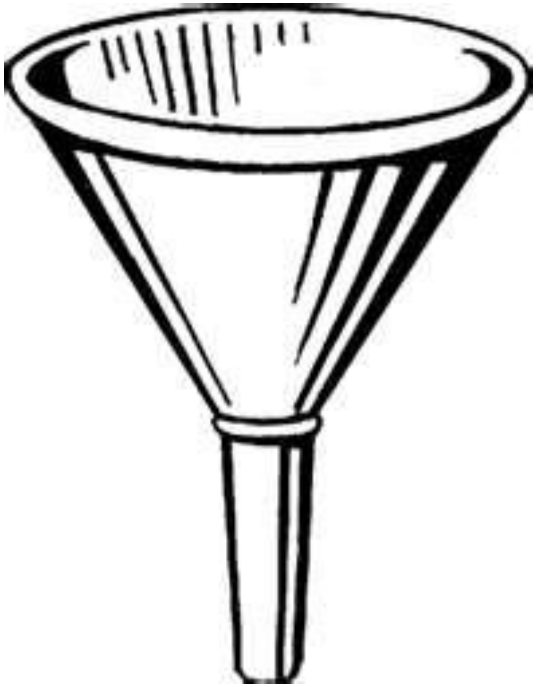
Consequences Of Security Incidents

Which – if any – of the following consequences did your organization experience as a result of this security incident(s)? (Percent of respondents, N=220, multiple respondents accepted)



Vendor Due Diligence

Total survey population of 285 = 100%



1. Population that always audit the security of their strategic software vendors

31%

2. Population that follows step #1 and also uses a standard audit process to assess all strategic software vendors

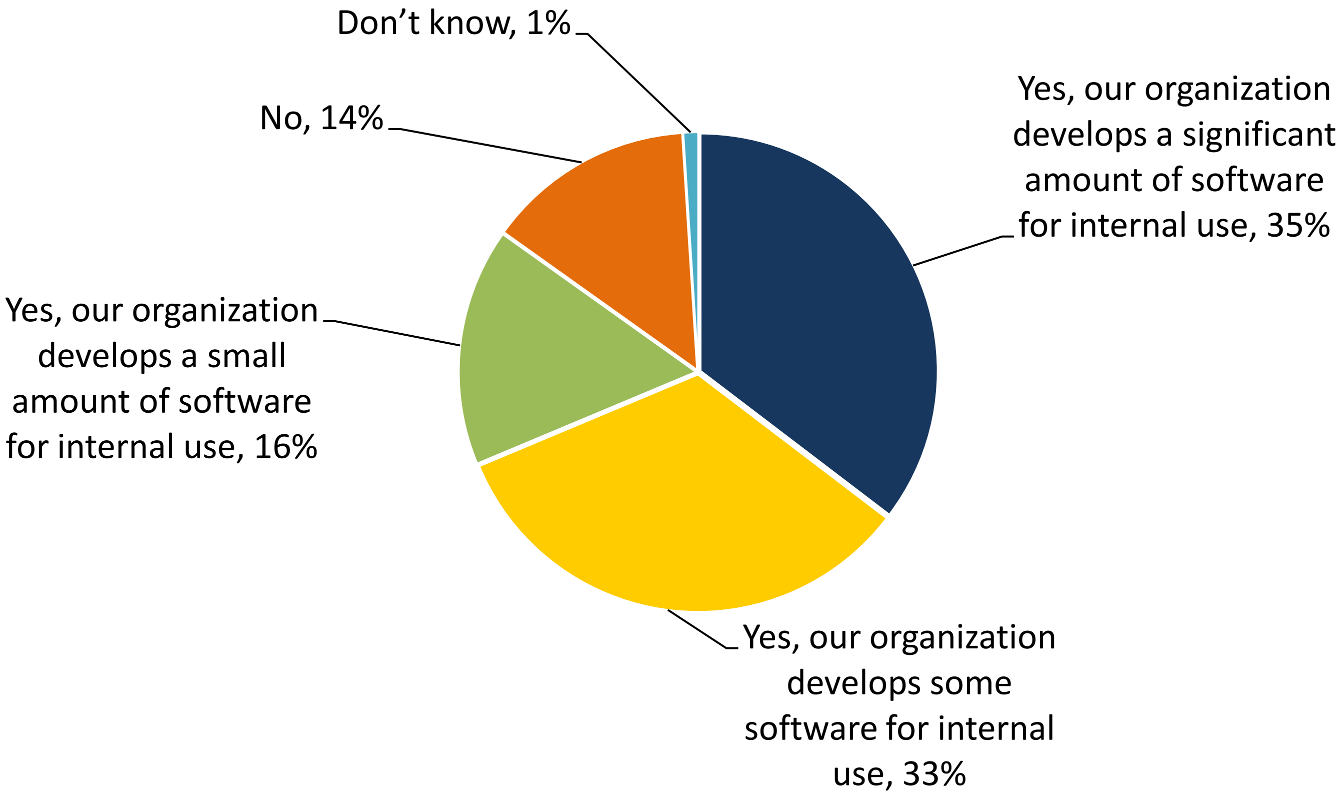
13%

3. Population that follows step #1 and #2 and also has a policy whereby the results of IT vendor security audits have a “significant impact” on procurement decisions

10%

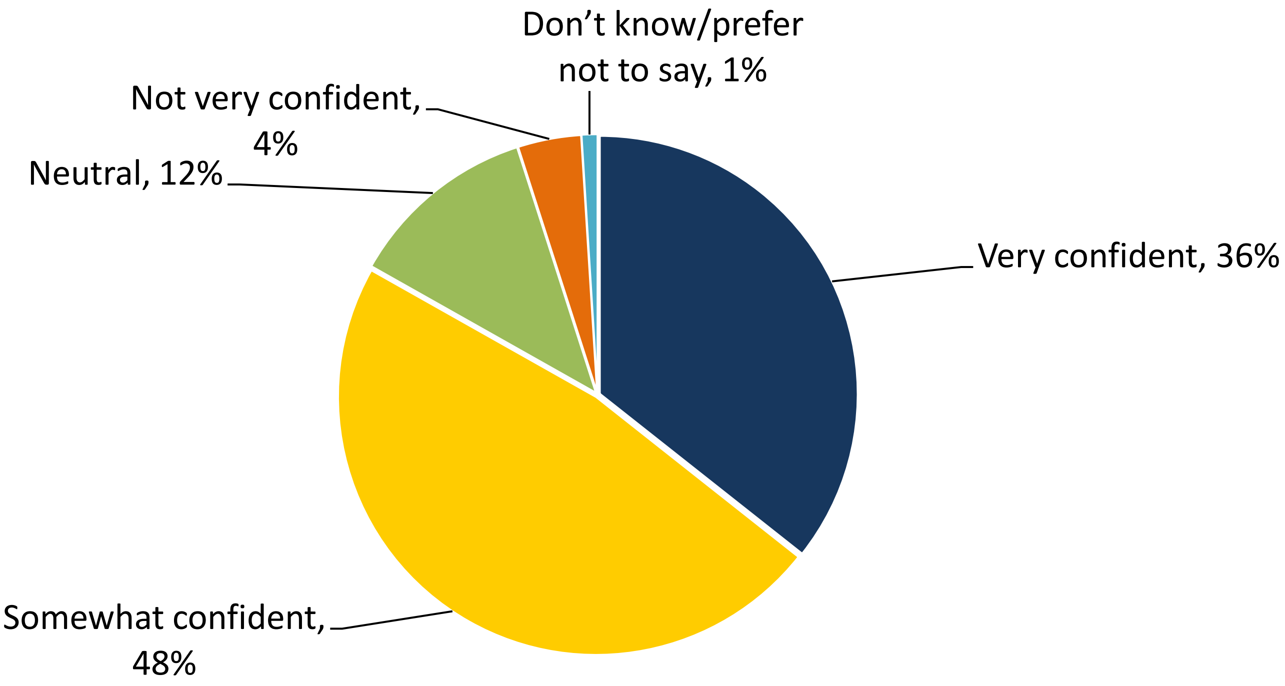
Software Development Efforts

Does your organization write its own software in order to develop custom business applications for its own internal use? (Percent of respondents, N=285)



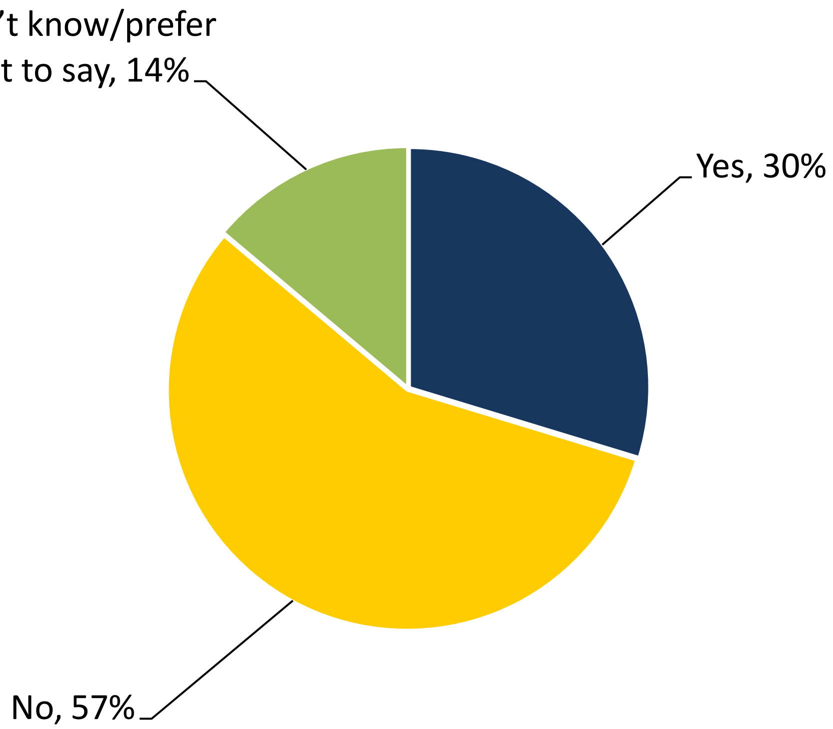
Confidence Level in Internally-Developed Software

In general, how confident are you in the security of your organization's internally-developed software (taking into account considerations such as secure design, attack surface area, coding quality, vulnerabilities, etc.)? (Percent of respondents, N=242)



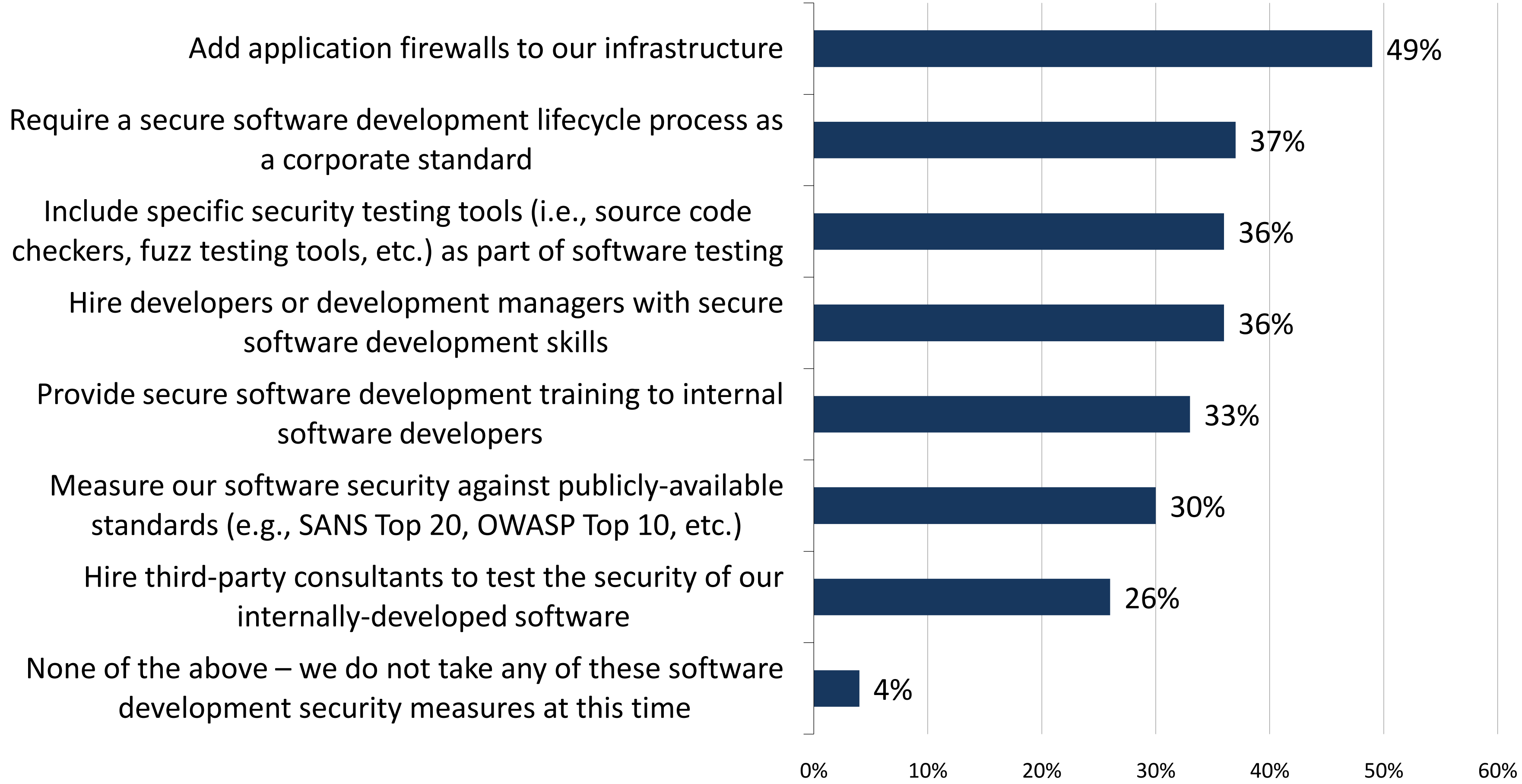
Security Incidents With Internally-Developed Software

To the best of your knowledge, has your organization ever experienced a security incident directly related to the compromise of internally developed software? (Percent of respondents, N=242)



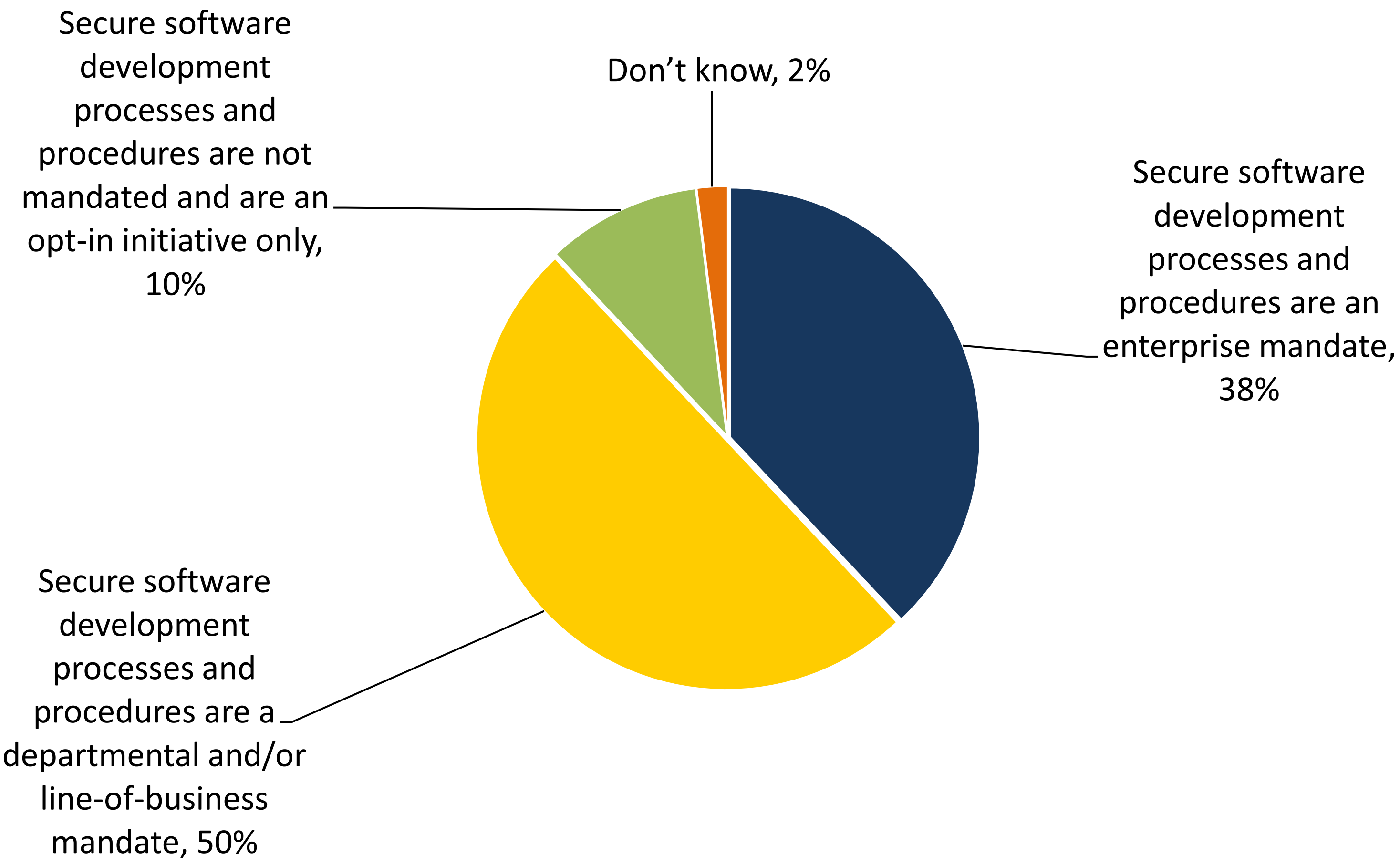
Security Activities and Software Development

Does your organization currently include any of the following security activities as part of its software development process? (Percent of respondents, N=242, multiple respondents accepted)



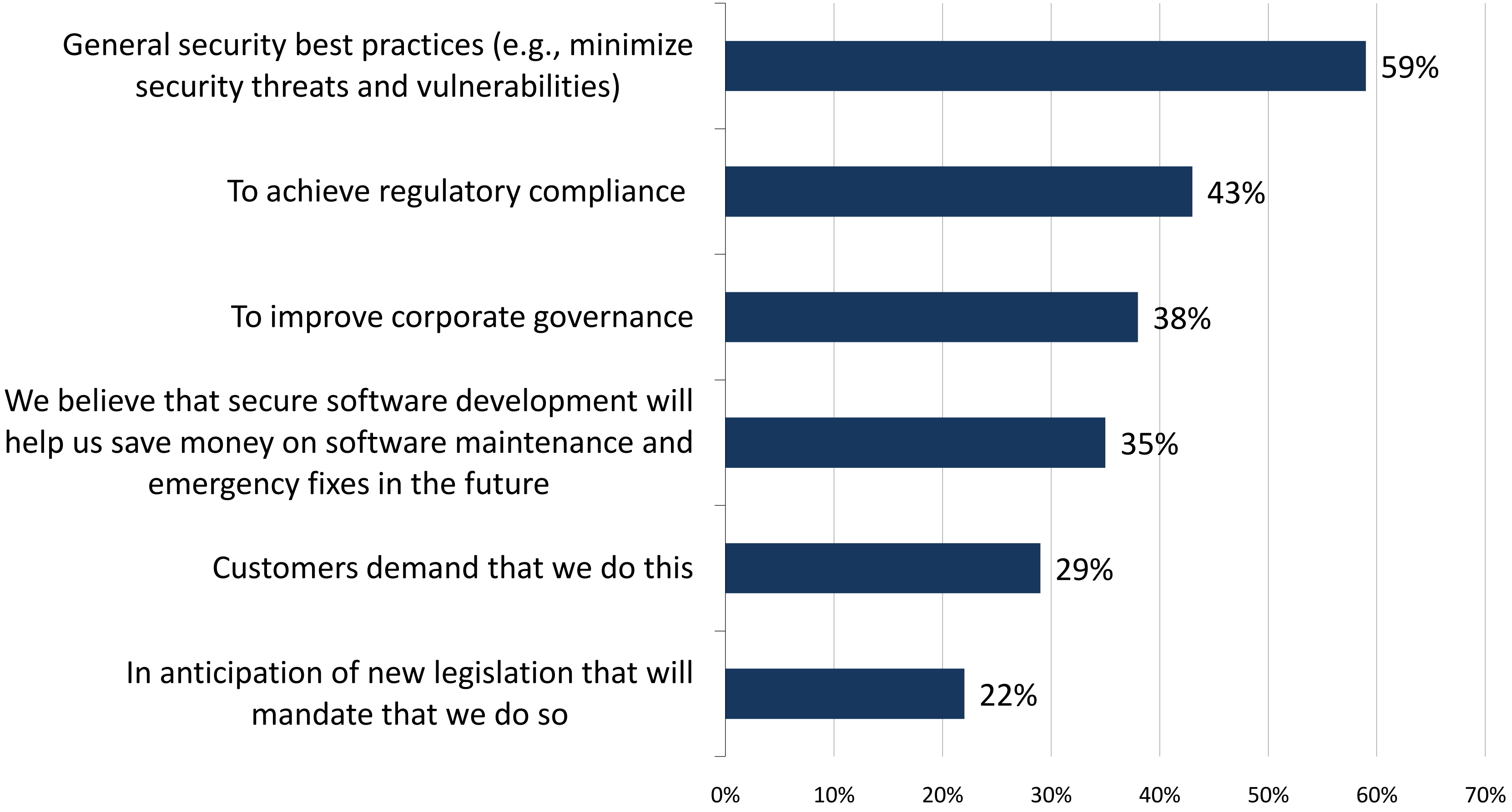
Scope of Secure Software Development

Which of the following best describes the extent of your organization's secure software development initiatives? (Percent of respondents, N=189)



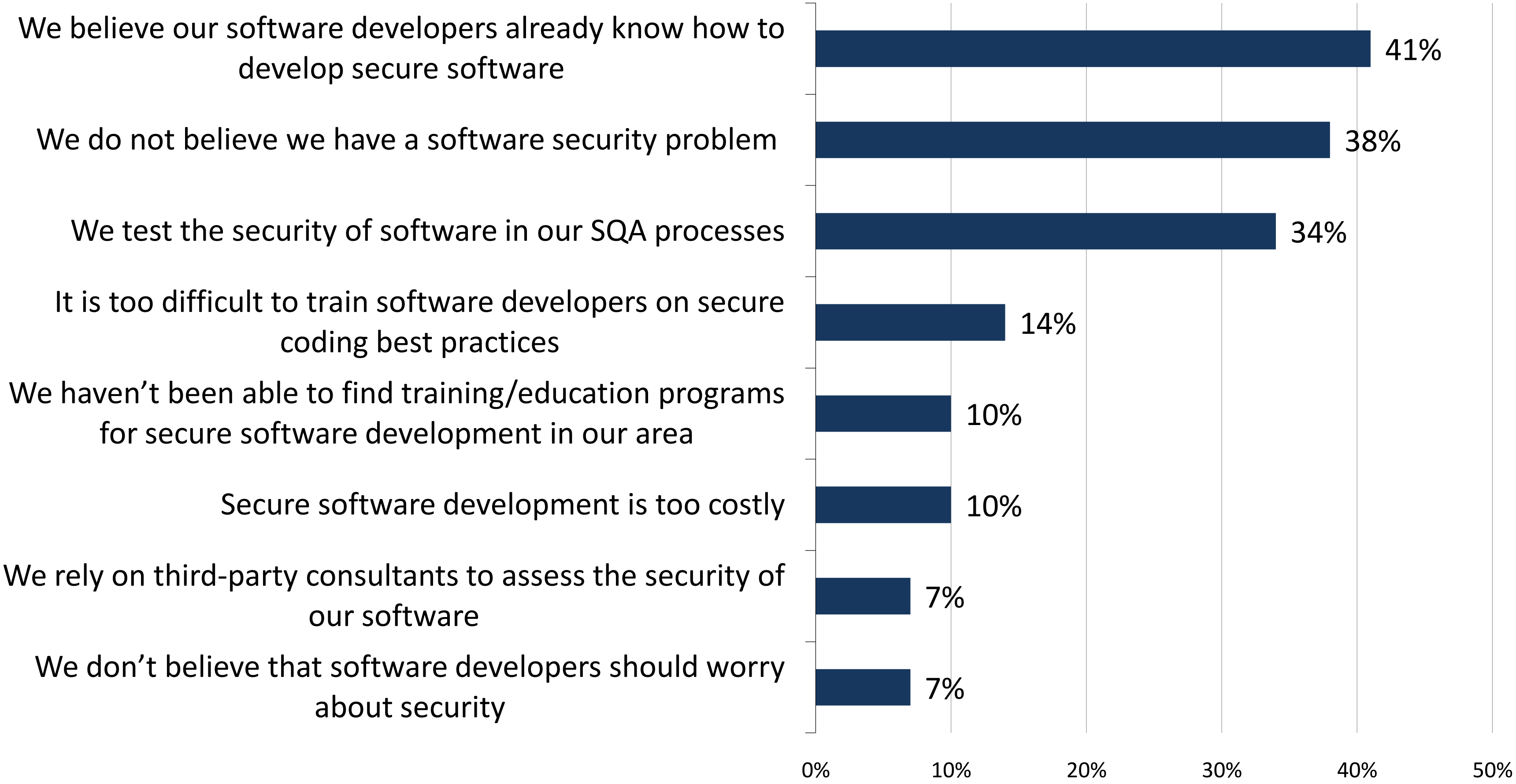
Why Secure Software Development?

In general, what would you say were the major reasons why your organization has chosen to establish a secure software development program? (Percent of respondents, N=189, multiple respondents accepted)



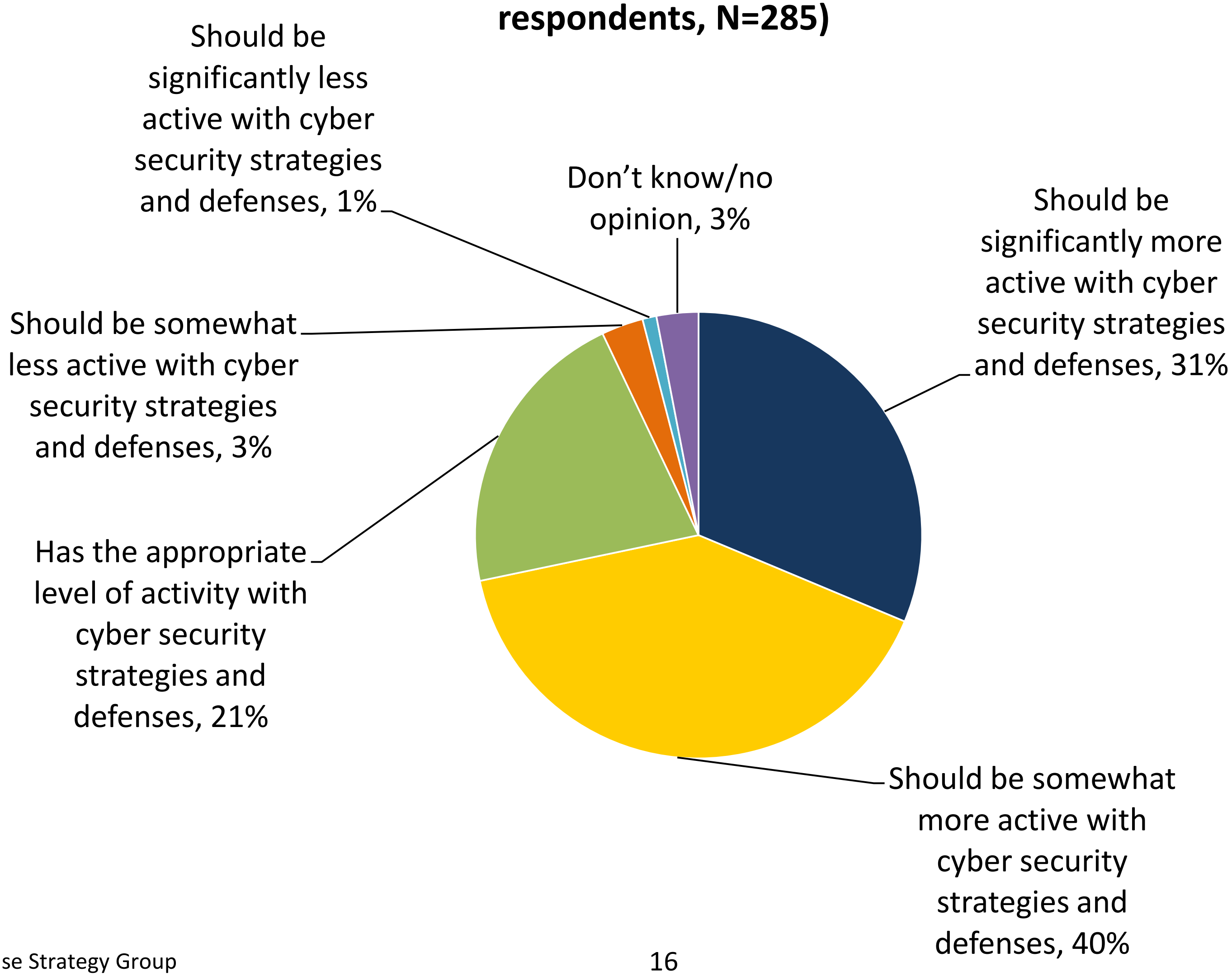
Why No Secure Software Development Program?

To the best of your knowledge, why has your organization chosen not to establish any form of secure software development program? (Percent of respondents, N=29, multiple respondents accepted)



Federal Government Involvement Preferences

Please complete the following statement by selecting one of the responses below. In my opinion, the U.S. Federal Government: (Percent of respondents, N=285)



Actions the Federal Government Should Take

- 42%: Create and publicize a “black list” of vendors with poor product security.
- 42%: Find better ways to share security information with the private sector
- 39%: Enact more stringent cyber security legislation along the lines of PCI
- 39%: Provide incentives (i.e. tax breaks, matching funds, etc.) to organizations that improve cyber security
- 36%: Amend existing laws to hold IT vendors accountable for security problems associated with their products

Takeaways

- Many critical infrastructure organizations remain vulnerable
- Cyber supply chain security is still a niche activity
- Vendor assessments remain limited
  - IT industry getting a “free pass”
- Software assurance is an “elite” activity
  - “Band-aid” approaches most popular
  - Need more best practices and training
  - Need more industry and government leadership

Thank You

Jon Oltsik – Senior Principal Analyst
jono@esg-global.com
508.381.5166

ESG
Enterprise Strategy Group

Getting to the bigger truth.™