2013 IT Security Benchmark Summary Report

Crowdsourced Survey Uncovers Key Security Program, Budget and Job Trend Data for CISOs and Security Leaders

WISEGATE RESEARCH REPORT
Introduction

Benchmarking against similar organizations provides IT leaders with powerful tools to analyze departmental performance and gain executive management support. Since no universal standards for security programs exist, benchmarking can help chief information security officers (CISOs) and other senior security leaders measure their programs’ effectiveness and communicate to upper management how the company’s security posture and programs compare against similar organizations.

As a crowdsourced benchmark survey commissioned by Wisegate members—who are senior-level IT security practitioners—the publication of the *Wisegate 2013 IT Security Benchmark Report* aims to provide useful guidance and a clear benchmark for IT security. The survey was developed by a group of veteran CISOs and facilitated by Wisegate to uncover the relevant and comprehensive benchmark data security leaders need to improve the effectiveness of security programs, demonstrate business value and gain executive support for new programs or underfunded initiatives.

*Wisegate Membership Has Its Advantages*

Learn how your peers use Wisegate to conduct research and trade IT knowledge.

Wisegate members are some of the most experienced IT and security executives and managers in the world. They work for multi-national corporations, educational institutions, government and non-profit agencies across virtually every major industry. Because of their positions and levels of responsibility, Wisegate members are often on the forefront of addressing new issues and challenges related to the use of information technology and the protection of enterprise data—and they trade the knowledge they’ve gained through experience using Wisegate.

Sharing the Wisdom of IT Experts

» Wisegate doesn’t allow vendors, analysts or IT rookies join.
» 100% of members are senior-level (IT executive, director or manager).
» 89% of members have 16+ years experience in IT.

*Schedule your tour today!* @ wisegateit.com/resources/book-a-tour
The *Wisegate 2013 IT Security Benchmark Report* was compiled from survey responses from over 100 North American senior-level security practitioners representing multiple major industry segments. To assist with the planning and security efforts of IT leaders, the report offers analysis of key factors that influence the effectiveness of security programs in the following areas:

» **Making the Security Grade**—How companies stack up on overall security posture and program maturity. And what the highest rated companies have in common.

» **Managing Risk**—A comparison of risk tolerance ratings and how company size, industry and security posture influence an organization’s tolerance for risk.

» **Security Processes, Policies, Software and Systems**—What are the most commonly used security processes, policies, software and systems.

» **Information Security Office Structures and Staffing**—How InfoSec offices are structured, supported and staffed.

» **InfoSec Involvement in IT Operations**—A measurement of InfoSec’s influence over network services, incident management and end-user access functions.

» **Spending on Information Security**—How much IT budget is dedicated to security and which company demographics impact security budgets.

» **CISO Career Challenges**—Are senior-level security practitioners satisfied with their job, compensation package and career decisions? And what factors contribute to a feeling of job insecurity or high levels of stress.

**Key Findings**

The *2013 IT Security Benchmark Report* uncovers insightful security program, budget and career data that can be used by CISOs and IT leaders to improve their security programs, demonstrate business value and build executive support for new programs or under-funded initiatives.

Many correlations between company demographics and security posture have been analyzed to help companies compare their business processes and performance metrics to industry norms and best practices. As a crowdsourced survey commissioned by Wisegate members, only survey participants and Wisegate members have access to the full survey findings. However in this summary report, Wisegate makes a portion of the *2013 IT Security Benchmark Report*’s key findings available to the broader Information Security community.
Making the Security Grade

As more and more organizations appoint CISOs and increase investments in IT security, there is a reasonable expectation that threats will be addressed—but how can the success of a security program be measured? And how can security programs be improved?

To help answer these critical questions, Wisegate members structured the *2013 IT Security Benchmark Report* to examine which factors enhance the effectiveness of security programs and highlight commonalities between companies with above average security grades.

**Report Highlights**

- When asked, "How would you grade your organization’s overall security posture and maturity?" 56% of participants gave their company an “A” or “B” grade for security posture—indicating a *Strong Security Posture*.
- 45% of participants gave their company a high grade for program maturity.
- 78% of companies with strong security postures also scored high on security maturity.
- *Banking & Financial Services* earned the highest average *Security Posture Grade* at 4.08 on a 5-point scale, while *Manufacturing* reported the lowest grade average at 2.63.

Managing Risk

As more and more companies adopt a risk-based approach to security, it can be helpful to understand the factors that impact an organization’s tolerance for risk and know how companies with similar demographics compare.

The *2013 IT Security Benchmark Report* provides a comparison of risk tolerance ratings across participants and offers analysis of how company size, industry and security posture influence an organization’s tolerance for risk.

**Report Highlights**

- *Banking & Financial Services* had the lowest average risk tolerance rating at 2.00 on a 5-point scale (30% below the survey average of 2.84) and *Education* reported the highest risk tolerance rating at 3.29 (14% above survey average).
- Companies with a strong security posture have a 19% lower tolerance for risk in comparison to companies with weaker security postures.
Security Processes, Policies, Software and Systems

Security processes, policies, software and systems are the building blocks of information security programs and provide information security teams with the arsenal of tools they need to protect data against various threats.

The 2013 IT Security Benchmark Report provides a benchmark of security processes, policies, and technologies to examine which methods are most commonly used by companies. Further, the report differentiates adoption rates between companies with weak and strong security postures to help identify the factors that may have the strongest impact on security program effectiveness.

Report Highlights


» Formal End-User Training and Network Access Controls were used nearly 40% more often in companies with stronger security ratings.

» Identity Governance Systems had the least number of users with only 28% of participants reporting adoption followed by Code Review Systems and IT GRC Software at 37% each.

» Companies with stronger security postures have 1.5 times more processes, policies, software and systems than companies with weaker security postures.

Information Security Office Structures and Staffing

InfoSec reporting structures, security staffing and the level of departmental support can have an impact on the effectiveness of security programs.

The 2013 IT Security Benchmark Report provides data on how information security offices are organized and staffed along with analysis of how InfoSec is supported and formalized through organizational structures.

Report Highlights

» 75% of companies have an official Information Security Officer.

» 62% of Information Security Offices report to the CIO. Less popular reporting structures include the COO (7%), CRO (5%), CEO (3%) and CFO (1%), while 22% indicated they use Other reporting structures.

» IT staff outnumber security practitioners on average by a ratio of 24:1.
Companies with weaker security postures report 41% less upper non-IT management engagement and 24% less CIO engagement than companies with stronger security postures.

Only 35% of companies have Requirements and Allowances for Security Office Education

InfoSec Involvement in IT Operations
The primary goal of InfoSec is to defend information from unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction. But how the information security office carries out this goal and the role the department plays within related IT operation functions varies greatly across companies.

The 2013 IT Security Benchmark Report quantifies the level of responsibility InfoSec has over standard IT operations—from full responsibility to no involvement—and measures InfoSec’s influence within various IT functions including network services, incident management and end-user access.

Report Highlights
- 44% of InfoSec departments take full responsibility for Intrusion Detection.
- Less than 50% of InfoSec offices play a strong role in Mobile Device Management.
- 40% of InfoSec offices do not have responsibility for Physical Security.

Spending on Information Security
Handling a security budget is a tricky business as most security departments operate under very tight budget constraints, while every year there are new threats and new technologies that demand attention. Unexpected surprises can derail even the most well thought out budget.

The 2013 IT Security Benchmark Report analyzes how organizational dynamics such as vertical industry, revenue, and size of company affect budgeting.

Report Highlights
- On average, 7.5% of the IT budget is spent on security.
- As a percentage of IT budget, Banking & Financial Services spends the highest and Government spends the lowest on security at 10% and 2% respectively.
- Companies with less than 1,000 employees spend 2.5 times more of the IT budget on security than companies with 20,000 or more employees.
CISO Career Challenges
The role of CISOs is expanding and their influence in organizations is increasing, but so are their challenges. As the CISO’s role shifts from glorified IT security administrator—babysitting firewalls and cleaning malware from infected systems—to holistic risk management, CISOs are under tremendous pressure to stop fire-fighting security breaches and start anticipating the fires before they start.

The 2013 IT Security Benchmark Report examines the impacts of these changes by analyzing job satisfaction, job security and levels of stress. Further the report assesses whether company demographics, corporate culture or security posture have any influence over the career challenges CISOs face.

Report Highlights
» One-third of respondents are not satisfied with their current job.
» 31% of respondents are not satisfied with their compensation package.
» 8% of security practitioners report a lack of job security.
» 71% of respondents say their job is Very Stressful or Stressful.

Full Survey Findings
This summary report presents a portion of Wisegate’s benchmark survey findings. Full survey findings and more detailed analysis are included in the 2013 IT Security Benchmark Report—which is available to Wisegate members. Wisegate members are senior-level information technology professionals or other senior-level professionals with IT-related roles—responsible for information technology and related matters at the corporate or enterprise level within their organizations. If you are a senior IT professional working for a company that does not sell IT products or services, you may be eligible to join Wisegate. Learn more about Wisegate at wisegateit.com.
Wisegate 2013 IT Security Benchmark Report Highlights

Wisegate 2013 IT Security Benchmark Report Highlights

Weak Security Posture
Companies with Weaker Security Postures have fewer processes, systems and software.

Strong Security Posture
Companies with Stronger Security Postures are more likely to train end-users and deploy network access control.

Less Management Engagement
Companies with Weaker Security Postures have less Management Engagement.

Higher Program Maturity
Companies with Stronger Security Postures also have Higher Program Maturity.

Risk Tolerance
-1.1% education
-30% banking & financial services
-3% government
-1.5% insurance
+1.3% manufacturing
2.84 Survey average

Career Challenges
33% Senior-level InfoSec Practitioners are not satisfied with their current job
8% Senior-level InfoSec Practitioners lack of job security
71% Senior-level InfoSec Practitioners say their job is stressful
31% Senior-level InfoSec Practitioners are not satisfied with their compensation

Spending on Information Security
<1,000 employees 10% vs. 4% +50,000
Smaller companies spend more IT Budget on Security 2.5x

Source: Wisegate, September 2013
In Closing...

CISOs and other senior security leaders face many challenges in their career—including measuring their program’s effectiveness and communicating to upper management how their security posture and programs compare against similar organizations.

As a Wisegate member commissioned research study, the *Wisegate 2013 IT Security Benchmark Report* is an example of how IT leaders are harnessing the power of the crowd to gain trusted, timely, relevant and affordable access to the collective knowledge and experience of peers. Wisegate is part of something bigger than itself—the democratization of the IT research market. We help facilitate the transfer of knowledge between members and the broader IT community to help shift who has a voice and who holds the power in the $4 trillion IT marketplace.

**IT experts. Trading IT knowledge.**

Wisegate is an IT expert network and information service that provides senior-level IT professionals with high quality research and intelligence from the best source available—their peers. Through live roundtable discussions, detailed product reviews, online Q&A and polls, and timely research reports, Wisegate offers a practical and unbiased information source built on the real-world experience of veteran IT professionals. No analyst theories or vendor bias to cloud the information, just clear and straightforward insight from experienced IT leaders.

Would you like to join us? Go to [wisegateit.com/request-invite/](http://wisegateit.com/request-invite/) to learn more and to submit your request for membership.