Cisco Systems Bi-Annual Security Research

Security Solutions Marketing and InsightExpress

June 2010
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Background &amp; Research Objectives</td>
<td>3</td>
</tr>
<tr>
<td>Methodology</td>
<td>4</td>
</tr>
<tr>
<td>Conclusions / Implications for Business</td>
<td>5</td>
</tr>
<tr>
<td>Key Findings</td>
<td>6</td>
</tr>
<tr>
<td>Detailed Findings</td>
<td>10</td>
</tr>
<tr>
<td>Respondent Profile</td>
<td>49</td>
</tr>
<tr>
<td>Study Team Contact Information</td>
<td>57</td>
</tr>
</tbody>
</table>
Background & Research Objectives

- Cisco Systems initiated the following research to gather insights and feedback surrounding security among key IT Security Decision Makers / Contributors.

- The focus of this research is on IT security issues related to tracking vulnerabilities and policy enforcement in the corporate environment.

- The report that follows summarizes feedback and insights from IT Security Decision Makers / Contributors in aggregate and across 5 countries: United States, Germany, China, India and Japan.
Methodology

Timing, Sample Qualifications & Analysis

- This report discusses findings for 512 IT security decision makers / contributors who completed an online survey from April 2 - 14, 2010.

- Respondents were screened to ensure an international sample (US, Germany, China, India & Japan) of IT professionals who:

  - Have at least some role in setting corporate security policies and/or making security-related IT purchase decisions for their company’s network.

  - Work for companies of at least 100 employees or more.

- Significant differences at the 95% confidence level between country subgroups are noted with capital letters (A/B/C/D/E) throughout the report.
Conclusions / Implications for Business

- Based on key findings, IT Security Decision Makers (ITSDMs) in the US, China & India pose the best opportunity for Cisco.
  
  - Unlike those in Germany and Japan, ITSDMs in the US, China & India use a variety of solutions to track vulnerabilities including CISCO IntelliShield Alert Manager to learn about employees’ network behaviors.
  
  - IT security professionals within these countries have determined that employees are using unsupported applications and personal devices; and have experienced a loss of information due to this activity. In spite of this, significant proportions – particularly in China and India – indicate a likelihood of allowing the use of personal devices on the enterprise network in the next 12 months.
    
    - Further, relative to other countries, significant proportions of ITSDMs in India report their organization has no process in place to lock employees from access if needed and they do not restrict what employees bring onto the network.
  
  - ITSDMs in the US, China & India indicate concern that overly strict security policies can have a negative impact on the hiring and retention of employees under age 30.

- Relative to other countries, ITSDMs in Germany and Japan reflect weaker involvement in assessing vulnerabilities, lower instances of discovering employee use of unsupported applications or network devices and are unlikely to permit use of personal devices on the enterprise network in the next year.
Key Findings
Key Findings for IT Security Decision Makers

- The vast majority (88%) of IT Security Decision Makers (ITSDMs), driven by those in the US, have centralized controls / technology / processes in place for updating employees’ software.
  - Roughly 7 in 10 ITSDMs have employee training (73%) or automatic deployment solutions (68%).
  - Relative to other countries, use of automatic deployment solutions tends to be driven by ITSDMs within the US, while employee training tends to be driven by those in China. Vulnerability testing tends to be used by significantly larger proportions of ITSDMs in the US and China compared to Germany, India and Japan.

- A variety of solutions are used to track vulnerabilities to make sure applications are properly updated.
  - More than 4 in 10 ITSDMs use vendor notifications (48%), Symantec Threat Alert (46%), security mailing lists (44%), or third party advisory services (43%). Nearly 4 in 10 use Cisco IntelliShield Alert Manager (38%).
  - The largest proportion of ITSDMs in the US tend to use Symantec Threat Alert (66%) to track vulnerabilities, while a similar proportion in China tend to use third party advisory services (64%). ITSDMs in Germany and Japan tend to indicate weaker use of solutions that track vulnerabilities.

- Relative to other available solutions, ISS Internet Security Systems is the solution used for enterprise vulnerability scanning by the largest proportion of ITSDMs (33%).
  - Use of this solution tends to be driven by ITSDMs in China and the US. Significantly larger proportions of ITSDMs in Germany and Japan don’t use any devices for enterprise vulnerability scanning.

- The vast majority of ITSDMs are conducting some type of assessment to monitor employees’ technology use.
  - The largest proportions conduct them to learn what security applications employees are running (63%) or what operating systems employees are running (58%). Relative to other countries, significant proportions of ITSDMs in Germany and Japan are not conducting assessments.
Key Findings for IT Security Decision Makers

- More than half of ITSDMs (56%), driven by those in the US, China and Japan, have determined that employees have been using unsupported applications.
  - Among them, the largest proportion has discovered employees using social networking (68%).
  - In the US more than 6 in 10 ITSDMs have discovered use of collaborative applications such as Google apps. In India, about 3 in 4 (74%) have discovered employees using unsupported peer to peer applications.

- About 4 in 10 (41%) have determined that employees have been using unsupported network devices. However in Germany, 3 in 4 (74%) indicate that they have not.
  - Four in 10 (40%) ITSDMs have experienced a breach or loss of information due to an unsupported network device (40%), driven by ITSDMs in China and India.
  - In line with other findings, the vast majority of ITSDMs in Germany (92%) say they have not experienced a breach or loss of information due to an unsupported network device.

- More than half of ITSDMs (53%), driven by those in the China and India, indicate their organization is very likely or likely to allow use of personal devices on the enterprise network in the next 12 months.
  - In Germany, 72% indicate this is unlikely (or very unlikely).

- The majority of ITSDMs indicate their organization has a complete technical process in place to lock employees from all access if needed (74%) and restrictions on what employees bring onto the network (79%).
  - In contrast, nearly half of ITSDMs in India (46%) indicate their company does not have a process in place to lock employees from access; and 3 in 10 (31%) do not restrict what employees bring onto the network.
Key Findings for IT Security Decision Makers

- Among ITSDMs from companies that impose restrictions, the largest proportion (75%) enforces regulations through a policy that has consequences for those who breach, driven by ITSDMs in the US and China.
  - The IT Department is responsible for setting, maintaining and communicating company security policies according to 75% of ITSDMs.
  - However in the US, China and Japan, significantly larger proportions indicate that a “security team” is responsible; and in the US 4 in 10 (41%) say it is the job of Human Resources.

- Policies tend to be enforced through training (62%) or URL filtering (57%).
  - Country variations are evident on policy enforcement. A significant proportion of ITSDMs in Japan use training (71%), while 8 in 10 in China (79%) use URL filtering.
  - Monitoring-only tends to be more prevalent in the US (53%) and India (51%) compared to other countries; and roughly half of ITSDMs in the US (52%) and China (50%) use DLP technology.
  - Nearly half of ITSDMs (48%) are running an automatic policy enforcement solution such as NAC, however a significant proportion of ITSDMs in Germany indicate that they do not.

- The majority of ITSDMs (71%), driven by those in India and China, recognize that overly strict security policies can have a negative impact on the hiring and retention of employees who are under the age of 30.
  - Roughly 4 in 10 ITSDMs in Germany (39%) and Japan (42%) perceive they have no impact at all.

- Along with Social Networking (51%), more than half of ITSDMs indicate perceiving the biggest IT risk to their organization is unauthorized users (55%).
  - About 3 in 10, driven by a significantly larger proportion in Germany (54%), rate unauthorized users as the #1 greatest risk to their organization.
Detailed Findings
Nearly 9 in 10 IT Security Decision Makers indicate their company has centralized controls / technology / processes in place for updating employees’ software.

Centralized Processes for Software Updates

(Total, n=511)

Company Has Centralized Controls / Technology / Processes

Yes, 88%

No, 12%

Q12. Do you have centralized controls/technology/processes in place for updating employees’ software?
More than 9 in 10 IT Security Decision Makers in the US have centralized processes for software updates – significantly more relative to those in Germany.

Q12. Do you have centralized controls/technology/processes in place for updating employees’ software?

Base: (US, n=102; Germany, n=101; China, n=107; India, n=100; Japan, n=101)
A/B/C/D/E indicate significant differences at the 95% confidence level.
The largest proportions of IT Security Decision Makers currently have employee training or automatic deployment solution(s) in place for software updates.

### Types of Controls / Processes
(Total, n=450)

- **Employee training**: 73%
- **Automated deployment solution(s)**: 68%
- **Vulnerability testing**: 54%
- **Employee self-patching**: 43%
- **Other**: 0%
Compared to Germany and India, a significantly large proportion of IT Security Decision Makers in China have employee training in place, while automated deployment solutions tend to be driven by ITSDMs in the US.

**Types of Controls / Processes**

**(By Country)**

- **Employee training**
  - US (A): 78%
  - Germany (B): 68%
  - China (C): BD 82%
  - India (D): 64%
  - Japan (E): 71%

- **Automated deployment solution(s)**
  - US (A): BCDE 85%
  - Germany (B): 65%
  - China (C): 61%
  - India (D): 70%
  - Japan (E): 57%

- **Vulnerability testing**
  - US (A): 68%
  - Germany (B): 48%
  - China (C): BDE 69%
  - India (D): 44%
  - Japan (E): 39%

- **Employee self-patching**
  - US (A): B 51%
  - Germany (B): 24%
  - China (C): B 41%
  - India (D): B 44%
  - Japan (E): B 55%

Relative to other countries, only a small proportion of ITSDMs in Germany have employee self-patching in place.

**Q13. What types of controls/processes does your company currently have in place? (Please select all that apply)**

*Base: (US, n=95; Germany, n=84; China, n=94; India, n=90; Japan, n=87)*

A/B/C/D/E indicate significant differences at the 95% confidence level.
Nearly half of IT Security Decision Makers from the total sample tend to track vulnerabilities internally through vendor notifications to make sure applications are properly updated.

**Tracking Vulnerabilities**

(Total, n=511)

- Vendor notifications: 48%
- Symantec Threat Alert: 46%
- Security mailing lists: 44%
- Third party advisory services: 43%
- Cisco IntelliShield Alert Manager: 38%
- SANS: 25%
- Other: 3%

Q14. How do you track vulnerabilities internally to make sure applications are properly updated? (Please select all that apply)
Relative to Germany and Japan, significantly larger proportions of IT Security Decision Makers in the US, China and India use Cisco IntelliShield Alert Manager.

Q14. How do you track vulnerabilities internally to make sure applications are properly updated? (Please select all that apply)

Base: (US, n=102; Germany, n=101; China, n=107; India, n=100; Japan, n=101)

A/B/C/D/E indicate significant differences at the 95% confidence level.
One in three IT Security Decision Makers reports using ISS Internet Security Systems for enterprise vulnerability scanning.

**Enterprise Vulnerability Scanning**
(Total, n=511)

- ISS Internet Security Systems: 33%
- Core Impact: 14%
- Retina/eEye: 10%
- Nessus/Tenable: 9%
- Qualys: 8%
- NMAP: 6%
- Other: 2%
- None of these: 19%

Q15. What do you use for enterprise vulnerability scanning?
Relative to other countries, use of ISS Internet Security Systems for enterprise vulnerability scanning tends to be driven by significant proportions of IT Security Decision Makers in China and the US.

Enterprise Vulnerability Scanning
(By Country)

ISS Internet Security Systems
- BDE 42%
- ABDE 57%
- 17%
- 21%

Qualys
- 8%
- 3%
- 6%
- 9%

Core Impact
- 16%
- 15%
- 7%
- CE 25%
- 10%

NMAP
- 3%
- 7%
- 2%
- 8%
- 9%

Retina/eEye
- 4%
- 6%
- 11%
- AB 17%
- 10%

Other
- 0%
- 3%
- 1%
- 0%
- 5%

Nessus/Tenable
- B 11%
- 2%
- B 10%
- B 14%
- 6%

None of these
- CD 17%
- ACD 39%
- 7%
- 5%
- ACD 31%

Significantly larger proportions of ITSDMs in Germany and Japan are not using any of these solutions for enterprise vulnerability scanning.

Q15. What do you use for enterprise vulnerability scanning?
Base: (US, n=102; Germany, n=101; China, n=107; India, n=100; Japan, n=101)
A/B/C/D/E indicate significant differences at the 95% confidence level.
More than half of IT Security Decision Makers are conducting assessments to determine what security apps (and types of non-security apps), operating systems, and types of devices employees are running.

Conducting Assessments
(Total, n=511)

- What security applications employees are running: 63%
- What operating systems employees are running: 58%
- What types of devices employees are running: 53%
- What types of (non-security) applications employees are running: 53%
- At what locations employees are working: 28%
- None of the above – not conducting assessments: 9%

Q16. Are you conducting assessments to determine any of the following: (Please select all that apply)
Compared to other countries, larger proportions of IT Security Decision Makers in China tend to be conducting assessments to determine what security apps, operating systems, and types of devices employees are running.

**Conducting Assessments**

(By Country)

<table>
<thead>
<tr>
<th>What security applications employees are running</th>
<th>What types of (non-security) applications employees are running</th>
<th>At what locations employees are working</th>
<th>None of the above – not conducting assessments</th>
</tr>
</thead>
<tbody>
<tr>
<td>US (A)</td>
<td>Germany (B)</td>
<td>China (C)</td>
<td>India (D)</td>
</tr>
<tr>
<td>68%</td>
<td>49%</td>
<td>52%</td>
<td>51%</td>
</tr>
<tr>
<td>49%</td>
<td>72%</td>
<td>54%</td>
<td>63%</td>
</tr>
<tr>
<td>BD</td>
<td>BE</td>
<td>E</td>
<td>BD</td>
</tr>
<tr>
<td>B</td>
<td>64%</td>
<td>E</td>
<td>B</td>
</tr>
<tr>
<td>B</td>
<td>63%</td>
<td>E</td>
<td>51%</td>
</tr>
<tr>
<td>B</td>
<td></td>
<td>E</td>
<td>51%</td>
</tr>
<tr>
<td>B</td>
<td></td>
<td>E</td>
<td>51%</td>
</tr>
<tr>
<td>E</td>
<td></td>
<td>E</td>
<td>51%</td>
</tr>
<tr>
<td>E</td>
<td></td>
<td>E</td>
<td>51%</td>
</tr>
<tr>
<td>E</td>
<td></td>
<td>E</td>
<td>51%</td>
</tr>
<tr>
<td>E</td>
<td></td>
<td>E</td>
<td>51%</td>
</tr>
<tr>
<td>E</td>
<td></td>
<td>E</td>
<td>51%</td>
</tr>
<tr>
<td>E</td>
<td></td>
<td>E</td>
<td>51%</td>
</tr>
<tr>
<td>E</td>
<td></td>
<td>E</td>
<td>51%</td>
</tr>
<tr>
<td>35%</td>
<td>28%</td>
<td>29%</td>
<td>16%</td>
</tr>
<tr>
<td>CD</td>
<td></td>
<td>CD</td>
<td></td>
</tr>
<tr>
<td>18%</td>
<td></td>
<td>CD</td>
<td></td>
</tr>
<tr>
<td>BD</td>
<td></td>
<td>CD</td>
<td></td>
</tr>
<tr>
<td>41%</td>
<td></td>
<td>CD</td>
<td></td>
</tr>
<tr>
<td>B</td>
<td></td>
<td>CD</td>
<td></td>
</tr>
<tr>
<td>54%</td>
<td></td>
<td>CD</td>
<td></td>
</tr>
</tbody>
</table>

**Q16. Are you conducting assessments to determine any of the following: (Please select all that apply)**

*Base: (US, n=102; Germany, n=101; China, n=107; India, n=100; Japan, n=101)*

A/B/C/D/E indicate significant differences at the 95% confidence level.
More than half of IT Security Decision Makers from the total dataset have determined that employees have been using unsupported applications.

Q17. Have you determined that employees have been using unsupported applications?

Use of Unsupported Applications  
(Total, n=511)

Company has determined Employees use of unsupported applications

Yes, 56%

No, 37%

N/A, 7%
Relative to IT Security Decision Makers in Germany and India, significantly larger proportions in the US, China and Japan have determined that employees have been using unsupported applications.

Use of Unsupported Applications
(By Country)

- **US (A)**
- **Germany (B)**
- **China (C)**
- **India (D)**
- **Japan (E)**

Q17. Have you determined that employees have been using unsupported applications?

Base: (US, n=102; Germany, n=101; China, n=107; India, n=100; Japan, n=101)

A/B/C/D/E indicate significant differences at the 95% confidence level.
Among those who have identified use of unsupported applications, nearly 7 in 10 IT Security Decision Makers indicate they have discovered employees using social networking applications.

<table>
<thead>
<tr>
<th>Types of Unsupported Applications</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social networking</td>
<td>68%</td>
</tr>
<tr>
<td>Collaborative applications (such as Google Apps)</td>
<td>47%</td>
</tr>
<tr>
<td>Peer to peer</td>
<td>47%</td>
</tr>
<tr>
<td>Cloud applications (such as Amazon S3)</td>
<td>33%</td>
</tr>
<tr>
<td>Other</td>
<td>4%</td>
</tr>
</tbody>
</table>

Q18. What types of unsupported applications have you discovered? (Please select all that apply)
Among those who have identified use of unsupported applications, usage of various types tends to be more highly reported in the US relative to other countries.

Types of Unsupported Applications

(By Country)

- Social networking
  - US: 79%
  - Germany: 67%
  - China: 65%
  - India: 56%
  - Japan: 56%

- Collaborative applications (such as Google Apps)
  - US: 66%
  - Germany: 42%
  - China: 38%
  - India: 49%
  - Japan: 39%

- Peer to peer
  - US: 53%
  - Germany: 30%
  - China: 49%
  - India: 49%
  - Japan: 33%

- Cloud applications (such as Amazon S3)
  - US: 43%
  - Germany: 21%
  - China: 32%
  - India: 32%
  - Japan: 27%

- Other
  - US: 3%
  - Germany: 5%
  - China: 0%
  - India: 0%
  - Japan: 13%

Significantly larger proportions of ITSDMs in India have discovered unsupported use of peer to peer applications.

Q18. What types of unsupported applications have you discovered? (Please select all that apply)

Base: (US, n=68; Germany, n=43; China, n=69; India, n=43; Japan, n=64)

A/B/C/D/E indicate significant differences at the 95% confidence level.
About 4 in 10 IT Security Decision Makers from the total dataset have determined that employees have been using unsupported devices.

Use of Unsupported Network Devices
(Total, n=511)

- Yes, 41%
- No, 51%
- N/A, 8%

Q19. Have you determined that employees have been using unsupported network devices?
Relative to other countries, a significantly larger proportion of IT Security Decision Makers in Germany have not determined that employees have been using unsupported network devices.

Use of Unsupported Network Devices
(By Country)

- US (A)
- Germany (B)
- China (C)
- India (D)
- Japan (E)

Q19. Have you determined that employees have been using unsupported network devices?

Base: (US, n=102; Germany, n=101; China, n=107; India, n=100; Japan, n=101)

A/B/C/D/E indicate significant differences at the 95% confidence level.
Four in ten IT Security Decision Makers report their company has lost information due to unsupported network devices.

Breach or Loss of Information
(Total, n=511)

- Company has lost info due to use of unsupported network devices: 40%
- No: 60%
Loss of information due to unsupported network devices tends to be least prevalent in Germany and most highly reported in China and India.

**Breach or Loss of Information**
(By Country)

- **US (A)**
- **Germany (B)**
- **China (C)**
- **India (D)**
- **Japan (E)**

**Yes**
- US (A): 40%
- Germany (B): 8%
- China (C): 61%
- India (D): 63%
- Japan (E): 26%

**No**
- US (A): 60%
- Germany (B): 92%
- China (C): 39%
- India (D): 37%
- Japan (E): 74%

Q20. Have you ever had a breach or loss of information due to unsupported network device?
*Base: (US, n=102; Germany, n=101; China, n=107; India, n=100; Japan, n=101)*

A/B/C/D/E indicate significant differences at the 95% confidence level.
More than half of IT Security Decision Makers report being likely or very likely to allow use of personal devices on enterprise networks in the next year – 7 percent already do.

Likelihood to Allow Use of Personal Devices on Enterprise Network
(Total, n=511)

- Net Very likely / likely, 53%
- 74%
- Very likely: 14%
- Likely: 39%
- Unlikely: 20%
- Very unlikely: 21%

Q21. How likely are you to allow use of personal devices on enterprise network in the next 12 months?
Relative to other countries, significantly larger proportions of IT Security Decision Makers in China and India report a likelihood of allowing personal devices in the next 12 months.

**Likelihood to Allow Use of Personal Devices on Enterprise Network**

By Country

- **US (A)**
- **Germany (B)**
- **China (C)**
- **India (D)**
- **Japan (E)**

Q21. How likely are you to allow use of personal devices on enterprise network in the next 12 months?

Base: (US, n=102; Germany, n=101; China, n=107; India, n=100; Japan, n=101)

A/B/C/D/E indicate significant differences at the 95% confidence level.
About 3 in 4 IT Security Decision Makers tend to have a complete technical process in place to lock employees from all access if needed.

Q22. Do you have a complete technical process in place to lock employees from all access if needed?
Compared to other countries, a significantly smaller proportion of IT Security Decision Makers in India have a complete technical process in place to lock employees from all access if needed.

Prohibiting Access
(By Country)

US (A)  Germany (B)  China (C)  India (D)  Japan (E)

Q22. Do you have a complete technical process in place to lock employees from all access if needed?
Base: (US, n=102; Germany, n=101; China, n=107; India, n=100; Japan, n=101)
A/B/C/D/E indicate significant differences at the 95% confidence level.
About 8 in 10 IT Security Decision Makers report restricting what employees bring onto the network.

Q23. Do you restrict what employees bring onto the network?

Network Restrictions
(Total, n=511)

Company restricts what employees bring onto the network

Yes, 79%

No, 21%
Relative to the US and Germany, significantly smaller proportions of IT Security Decision Makers in India restrict what employees bring onto the network.

Network Restrictions
(By Country)

Q23. Do you restrict what employees bring onto the network?
Base: (US, n=102; Germany, n=101; China, n=107; India, n=100; Japan, n=101)
A/B/C/D/E indicate significant differences at the 95% confidence level.
Among those who impose limitations, 3 in 4 IT Security Decision Makers have a policy with consequences for those who breach network restrictions.

**Network Restrictions**
(Total, n=402)

- **Policy with consequences for those who breach**: 75%
- **Physical enforcement (disconnection from network)**: 40%
- **Written policy without consequences**: 34%
- **Other**: 0%

Q24. How do you restrict what employees bring onto the network?
While the largest proportions of IT Security Decision Makers restrict access with a policy, more than 4 in 10 in India and Japan use physical enforcement.

Q24. How do you restrict what employees bring onto the network?

Base: (US, n=85; Germany, n=88; China, n=78; India, n=69; Japan, n=82)

A/B/C/D/E indicate significant differences at the 95% confidence level.
3 in 4 IT Security Decision Makers indicate that it is the responsibility of the IT Department to set, maintain and communicate company security policies.

Responsibility for Security Policies
(Total, n=511)

- **IT Department**: 75%
- **Security team**: 41%
- **Senior executive**: 29%
- **Human Resources**: 26%
- **Other**: 1%

Q25. Who is responsible for setting, maintaining and communicating company security policies? (Please select all that apply)
Compared to other countries, significantly greater proportions of IT Security Decision Makers in the US, China, and Japan indicate it is the responsibility of a “security team” to set, maintain and communicate company security policies.

Responsibility for Security Policies
(By Country)

- **IT Department**
  - A: 84%
  - B: 75%
  - C: 74%
  - D: 69%
  - E: 50%

- **Security team**
  - A: 27%
  - B: 24%
  - C: 28%
  - D: 46%
  - E: 57%

- **Senior executive**
  - A: 31%
  - B: 34%
  - C: 37%
  - D: 17%
  - E: 17%

- **Human Resources**
  - A: 16%
  - B: 26%
  - C: 28%
  - D: 19%
  - E: 17%

- **Other**
  - A: 1%
  - B: 0%
  - C: 1%
  - D: 1%
  - E: 1%

Q25. Who is responsible for setting, maintaining and communicating company security policies? (Please select all that apply)

Base: (US, n=102; Germany, n=101; China, n=107; India, n=100; Japan, n=101)

A/B/C/D/E indicate significant differences at the 95% confidence level.
The largest proportions of IT Security Decision Makers tend to enforce security policies through training and URL filtering.

**Policy Enforcement**  
*(Total, n=511)*

- **Training**: 62%
- **URL filtering**: 57%
- **Monitoring only**: 41%
- **DLP (content/context monitoring) technology**: 39%
- **We don’t enforce**: 3%
- **Other**: 0%

Q26. How do you enforce your security policies? (Please select all that apply)
While training tends to be the most prevalent method of security policy enforcement in most countries, about 8 in 10 IT Security Decision Makers in China use URL filtering.

![Policy Enforcement](image)

**Q26. How do you enforce your security policies? (Please select all that apply)**

*Base: (US, n=102; Germany, n=101; China, n=107; India, n=100; Japan, n=101)*

A/B/C/D/E indicate significant differences at the 95% confidence level.
Nearly half of IT Security Decision Makers from the total sample indicate running an automatic policy enforcement solution (such as NAC).

Q27. Are you running an automatic policy enforcement solution (such as NAC)?

**Automatic Policy Enforcement Solutions**
(Total, n=511)

- **Company runs automatic policy enforcement solutions**
  - Yes, 48%
  - No, 52%
Use of automatic policy enforcement solutions (such as NAC) tend to be significantly less prevalent in Germany relative to other countries.

Q27. Are you running an automatic policy enforcement solution (such as NAC)?

Base: (US, n=102; Germany, n=101; China, n=107; India, n=100; Japan, n=101)

A/B/C/D/E indicate significant differences at the 95% confidence level.
About 7 in 10 IT Security Decision Makers agree that overly strict security policies can have a negative impact on the hiring and retention of employees who are under the age of 30.

**Impact of Policies on Hiring & Retention**

(Total, n=511)

Net, Yes 71%

- Yes, quite a significant impact: 28%
- Yes, but just a moderate impact: 43%
- No, no impact at all: 24%
- Not sure: 5%

Q28. Do you believe overly strict security policies can have a negative impact on the hiring and retention of employees who are under the age of 30?
Nearly half of IT Security Decision Makers in India are concerned that overly strict security policies can lead to a significant negative impact on the hiring and retention of employees who are under the age of 30.

Impact of Policies on Hiring & Retention
(By Country)

- US (A)
- Germany (B)
- China (C)
- India (D)
- Japan (E)

Q28. Do you believe overly strict security policies can have a negative impact on the hiring and retention of employees who are under the age of 30?

Base: (US, n=102; Germany, n=101; China, n=107; India, n=100; Japan, n=101)

A/B/C/D/E indicate significant differences at the 95% confidence level.
The largest proportions of IT Security Decision Makers from the total sample tend to perceive that unauthorized users, social networking and new applications are the leading IT risks to their organization.

<table>
<thead>
<tr>
<th>Leading IT Risks</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized users</td>
<td>55%</td>
</tr>
<tr>
<td>Social networking</td>
<td>51%</td>
</tr>
<tr>
<td>New applications</td>
<td>47%</td>
</tr>
<tr>
<td>Unsupported other devices</td>
<td>44%</td>
</tr>
<tr>
<td>Unsupported mobile devices</td>
<td>40%</td>
</tr>
<tr>
<td>Collaborative applications such as Google Apps</td>
<td>33%</td>
</tr>
<tr>
<td>Cloud applications</td>
<td>30%</td>
</tr>
</tbody>
</table>

Q29. What do you perceive to be the biggest IT risk to your organization? (select top 3)
The largest proportion of IT Security Decision Makers in the US perceive social networking as the leading risk, Germany and India perceive unauthorized users as the leading risk, and in China and Japan new applications are perceived as the leading risk.

### Leading IT Risks (By Country)

<table>
<thead>
<tr>
<th>Category</th>
<th>US (A)</th>
<th>Germany (B)</th>
<th>China (C)</th>
<th>India (D)</th>
<th>Japan (E)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized users</td>
<td>56%</td>
<td>51%</td>
<td>44%</td>
<td>54%</td>
<td>70%</td>
</tr>
<tr>
<td>Social networking</td>
<td>64%</td>
<td>50%</td>
<td>37%</td>
<td>51%</td>
<td></td>
</tr>
<tr>
<td>New applications</td>
<td>36%</td>
<td>37%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unsupported mobile devices</td>
<td></td>
<td></td>
<td>31%</td>
<td>31%</td>
<td>50%</td>
</tr>
<tr>
<td>Collaborative applications such as Google Apps</td>
<td>29%</td>
<td>30%</td>
<td>42%</td>
<td>30%</td>
<td>34%</td>
</tr>
<tr>
<td>Unsupported other devices</td>
<td>43%</td>
<td>51%</td>
<td>50%</td>
<td>27%</td>
<td>50%</td>
</tr>
<tr>
<td>Cloud applications</td>
<td></td>
<td></td>
<td>28%</td>
<td>32%</td>
<td>37%</td>
</tr>
</tbody>
</table>

Q29. What do you perceive to be the biggest IT risk to your organization? (select top 3)

Base: (US, n=102; Germany, n=101; China, n=107; India, n=100; Japan, n=101)

A/B/C/D/E indicate significant differences at the 95% confidence level.
About 3 in 10 IT Security Decision Makers from the total sample tend to perceive unauthorized users as the #1 IT risk.

<table>
<thead>
<tr>
<th>#1 IT Risk</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized users</td>
<td>31%</td>
</tr>
<tr>
<td>Social networking</td>
<td>19%</td>
</tr>
<tr>
<td>New applications</td>
<td>15%</td>
</tr>
<tr>
<td>Unsupported other devices</td>
<td>10%</td>
</tr>
<tr>
<td>Unsupported mobile devices</td>
<td>9%</td>
</tr>
<tr>
<td>Collaborative applications such as Google Apps</td>
<td>9%</td>
</tr>
<tr>
<td>Cloud applications</td>
<td>8%</td>
</tr>
</tbody>
</table>

Q30. What do you perceive to be the #1 risk?
For all 5 countries, IT Security Decision Makers perceive that unauthorized users is the #1 IT risk, driven by a significant proportion in Germany.

Q30. What do you perceive to be the #1 risk?

Base: (US, n=102; Germany, n=101; China, n=107; India, n=100; Japan, n=101)

A/B/C/D/E indicate significant differences at the 95% confidence level.
Respondent Profile
Two-thirds of IT Security Decision Makers are the **primary** decision maker for their company’s network.

**Role in IT Decision Making**
(Total, n=511)

- **65%** I am the primary decision maker
- **14%** I always influence such decisions, but I am not the primary decision maker
- **9%** I often influence such decisions, but I am not the primary decision maker
- **12%** I sometimes influence such decisions, but I am not the primary decision maker

Q8. Which of the following best describes your role in setting corporate security policies and/or making security-related IT purchase decisions for your company’s network?
The vast majority of IT Security Decision Makers in India and more than 7 in 10 in the US have the primary responsibility for their company’s network.

Q8. Which of the following best describes your role in setting corporate security policies and/or making security-related IT purchase decisions for your company’s network?

Base: (US, n=102; Germany, n=101; China, n=107; India, n=100; Japan, n=101)

A/B/C/D/E indicate significant differences at the 95% confidence level.
About 4 in 10 IT Security Decision Makers from the total sample come from companies with 1000+ employees worldwide.

<table>
<thead>
<tr>
<th>Number of Employees Worldwide</th>
<th>(%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Under 20</td>
<td>0%</td>
</tr>
<tr>
<td>20-99</td>
<td>0%</td>
</tr>
<tr>
<td>100-249</td>
<td>17%</td>
</tr>
<tr>
<td>250-499</td>
<td>17%</td>
</tr>
<tr>
<td>500-749</td>
<td>11%</td>
</tr>
<tr>
<td>750-999</td>
<td>16%</td>
</tr>
<tr>
<td>1000 - 9,999</td>
<td>27%</td>
</tr>
<tr>
<td>10,000</td>
<td>12%</td>
</tr>
<tr>
<td>Don’t Know/Not Sure</td>
<td>0%</td>
</tr>
</tbody>
</table>

39% Have 1000+ employees worldwide

Q9. Approximately how many people does your company employ at all of their locations, worldwide?
The largest proportions of IT Security Decision Makers tend to come from companies of 1000-9,999 employees with the exception of India – where companies tend to be slightly smaller.

Q9. Approximately how many people does your company employ at all of their locations, worldwide?

Base: (US, n=102; Germany, n=101; China, n=107; India, n=100; Japan, n=101)

A/B/C/D/E indicate significant differences at the 95% confidence level.
## Industry Representation

<table>
<thead>
<tr>
<th>Industry Representation</th>
<th>Total</th>
<th>US (A)</th>
<th>Germany (B)</th>
<th>China (C)</th>
<th>India (D)</th>
<th>Japan (E)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>511</td>
<td>102</td>
<td>101</td>
<td>107</td>
<td>100</td>
<td>101</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>19%</td>
<td>27%BD</td>
<td>14%</td>
<td>18% D</td>
<td>7%</td>
<td>31% BCD</td>
</tr>
<tr>
<td>IT Consulting</td>
<td>8%</td>
<td>11%</td>
<td>11%</td>
<td>7%</td>
<td>3%</td>
<td>8%</td>
</tr>
<tr>
<td>Construction</td>
<td>8%</td>
<td>1%</td>
<td>5%</td>
<td>7%</td>
<td>21% ABCE</td>
<td>9% A</td>
</tr>
<tr>
<td>Finance, Banking, Accounting</td>
<td>8%</td>
<td>13% D</td>
<td>8%</td>
<td>8%</td>
<td>2%</td>
<td>11% D</td>
</tr>
<tr>
<td>Health/Medical</td>
<td>5%</td>
<td>8%</td>
<td>2%</td>
<td>3%</td>
<td>8%</td>
<td>2%</td>
</tr>
<tr>
<td>Internet, Computer or Communications Software</td>
<td>5%</td>
<td>2%</td>
<td>0%</td>
<td>21% ABDE</td>
<td>2%</td>
<td>1%</td>
</tr>
<tr>
<td>Pharmaceutical</td>
<td>4%</td>
<td>0%</td>
<td>3%</td>
<td>2%</td>
<td>13% ABCE</td>
<td>1%</td>
</tr>
<tr>
<td>Software Development</td>
<td>4%</td>
<td>2%</td>
<td>3%</td>
<td>7% D</td>
<td>0%</td>
<td>5%</td>
</tr>
<tr>
<td>Transportation</td>
<td>4%</td>
<td>4%</td>
<td>6%</td>
<td>5%</td>
<td>3%</td>
<td>2%</td>
</tr>
<tr>
<td>Education (Higher Ed)</td>
<td>3%</td>
<td>3%</td>
<td>3%</td>
<td>2%</td>
<td>5%</td>
<td>2%</td>
</tr>
<tr>
<td>Retail (Non-computer)</td>
<td>3%</td>
<td>5%</td>
<td>5%</td>
<td>2%</td>
<td>0%</td>
<td>5%</td>
</tr>
<tr>
<td>Business consulting</td>
<td>2%</td>
<td>5%</td>
<td>2%</td>
<td>0%</td>
<td>0%</td>
<td>2%</td>
</tr>
<tr>
<td>Government (Local/State)</td>
<td>2%</td>
<td>0%</td>
<td>5%</td>
<td>2%</td>
<td>1%</td>
<td>4%</td>
</tr>
<tr>
<td>Hospitality</td>
<td>2%</td>
<td>1%</td>
<td>1%</td>
<td>2%</td>
<td>3%</td>
<td>1%</td>
</tr>
<tr>
<td>Insurance/Real Estate/Legal</td>
<td>2%</td>
<td>4%</td>
<td>2%</td>
<td>1%</td>
<td>2%</td>
<td>2%</td>
</tr>
<tr>
<td>Internet, Computer or Communications Hardware</td>
<td>2%</td>
<td>0%</td>
<td>1%</td>
<td>7% AD</td>
<td>0%</td>
<td>1%</td>
</tr>
<tr>
<td>Shipping/Handling/Importing &amp; Exporting/Trucking</td>
<td>2%</td>
<td>2%</td>
<td>2%</td>
<td>2%</td>
<td>1%</td>
<td>3%</td>
</tr>
<tr>
<td>Education (K - 12)</td>
<td>1%</td>
<td>2%</td>
<td>1%</td>
<td>0%</td>
<td>1%</td>
<td>0%</td>
</tr>
<tr>
<td>Entertainment</td>
<td>1%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>3%</td>
<td>1%</td>
</tr>
<tr>
<td>Government (Federal)</td>
<td>1%</td>
<td>1%</td>
<td>4%</td>
<td>0%</td>
<td>1%</td>
<td>0%</td>
</tr>
<tr>
<td>Market Research</td>
<td>1%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>3%</td>
<td>1%</td>
</tr>
<tr>
<td>Non-Profit Organization</td>
<td>1%</td>
<td>2%</td>
<td>2%</td>
<td>1%</td>
<td>1%</td>
<td>0%</td>
</tr>
<tr>
<td>Travel</td>
<td>1%</td>
<td>0%</td>
<td>2%</td>
<td>0%</td>
<td>2%</td>
<td>0%</td>
</tr>
<tr>
<td>Utilities</td>
<td>1%</td>
<td>0%</td>
<td>3%</td>
<td>1%</td>
<td>1%</td>
<td>0%</td>
</tr>
<tr>
<td>Media/Marketing/Advertising</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Other</td>
<td>10%</td>
<td>8%</td>
<td>16% C</td>
<td>3%</td>
<td>17% C</td>
<td>9%</td>
</tr>
</tbody>
</table>

Q10. Which of the following industries are you in?
Nearly 7 in 10 IT Security Decision Makers from the total sample are at manager-level or higher at their organization.

### Job Title

(Total, n=511)

- **Manager**: 38%
- **Director**: 15%
- **Vice-President**: 6%
- **C-level executive**: 9%
- **Administrator**: 10%
- **Consultant**: 3%
- **Department Head**: 15%
- **Other**: 5%

68% Manager-level or higher at their organization

Q11. Which of the following best describes your job title?
Compared to other countries, significantly larger proportions of IT Security Decision Makers in Japan and the US are C-level executives.

Q11. Which of the following best describes your job title?

Base: (US, n=102; Germany, n=101; China, n=107; India, n=100; Japan, n=101)
A/B/C/D/E indicate significant differences at the 95% confidence level.

Network Systems
Success Deck
© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public
Study Team Contact Info

Fred Kost
Director of Marketing, Security Solutions
(408) 853-6098
frkost@cisco.com

David Oro
Public Relations Manager
(707) 558-8585
daoro@cisco.com