The Gap Between Executive Awareness and Enterprise Security
Global Survey of IT Security Professionals

December 2015
Executive Summary

This report finds that more than half of security professionals today believe their company’s security can be compromised. Yet, one third of CEOs are not regularly briefed on cybersecurity and related business risks. Budget was cited as the top reason security capabilities lag need. CEOs and Execs that are informed and regularly receive status reports provide better funding and support to security teams.

Executive visibility into the performance of their security programs varies greatly by industry. The security metrics currently reported to executives are not the metrics that security professionals say represent security effectiveness. This report shows that privileged account and endpoint security are top security program priorities. Security solution selection has matured and business value is the leading consideration.
Key Findings

- 60% believe their company’s security can be breached today
- 75% cite budget as the #1 barrier to proper security
- 53% of CEOs make decisions without regard to cybersecurity
- 1/3 of CEOs are not regularly briefed on cybersecurity
- 43% of management teams aren’t provided security reports

- Executive visibility into the performance of their security programs varies greatly by industry
- Metrics considered critical indicators of security program effectiveness are often not reported
- Privileged account security edges out app security as the #2 security priority
METHODOLOGY AND PARTICIPANTS
# Goals and Methodology

<table>
<thead>
<tr>
<th>Research Goal</th>
<th>The primary research goal was to capture hard data on visibility and support of security programs at the executive level. In addition, researchers sought to determine which metrics are used to define security effectiveness.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Methodology</td>
<td>IT professional users worldwide were invited to participate in a survey on the topic of cybersecurity. The survey was administered electronically and participants were offered a token compensation for their participation.</td>
</tr>
<tr>
<td>Participants</td>
<td>A total of 304 participants that respond to IT alerts completed the global survey.</td>
</tr>
</tbody>
</table>
Participant Demographics

Role within IT

- I am an IT executive: 22%
- I am a front-line IT or technology professional: 36%
- I manage a team of IT or technology professionals: 42%

Role within Security

- IT security is a substantial part of my job: 76%
- IT security is my entire job: 24%
Company Demographics

Number Of Employees

- 500 - 1,000: 26%
- 1,000 - 5,000: 37%
- 5,000 - 10,000: 18%
- More than 10,000: 19%

Industry

- Financial Services: 16%
- Technology: 15%
- Manufacturing: 13%
- Education: 9%
- Services: 8%
- Government: 7%
- Transportation: 5%
- Retail: 5%
- Telecommunications: 5%
- Energy and Utilities: 5%
- Healthcare: 3%
- Non-profit: 1%
- Hospitality: 1%
- Other: 7%
Company Demographics

Location

- United States or Canada: 77%
- Europe: 12%
- Australia or New Zealand: 3%
- Asia: 4%
- Mexico, Central America, or South America: 4%
RESULTS
60% Believe Their Company’s Security Can Be Breached Today

Do you feel that today that your company’s security defenses are exploitable?

- Yes: 60%
- No: 22%
- I don't know: 18%
75% Cite Budget as the #1 Barrier to Proper Security

For your company, what are the top barriers to implementing cybersecurity enhancements?

- **Budget**: 75%
- **Expertise**: 52%
- **Ineffective security tools and solutions**: 34%
- **Security is not a company priority**: 28%
- **Other**: 6%
53% of CEOs Make Decisions Without Regard to Cybersecurity

Do you think your CEO makes decisions with cybersecurity in mind?

Yes 47%
No 53%
Is your CEO regularly briefed on cybersecurity, defense strategies and related business risks?

1/3 of CEOs Aren’t Regularly Briefed on Cybersecurity and Business Risks
In your opinion, does your CEO know enough about cybersecurity?

61% of CEOs Do Not Know Enough About Cybersecurity
69% Think Cybersecurity is Too Technical for CEOs

Why do you think your CEO lacks knowledge regarding cybersecurity?

- It is too technical: 69%
- It was delegated to someone else: 52%
- The CEO does not grasp the severity of security risks: 44%
- It is not viewed as strategic to the company: 37%
- It is not interesting to the CEO: 28%
- Other: 4%
Only 39% of Security Professionals Feel They are Fully Supported By Executives

How would you characterize executive management’s support for information security?

- Very supportive: adequate funding and consistently communicates importance of security across the organization
- Somewhat supportive: security still struggles to get budget sometimes but executives consistently voice a support for security
- Not supportive: security lacks necessary budget and attention in the organization
Are reports and metrics regularly provided to your executive management team to demonstrate the effectiveness of the security program?

43% of Management Teams Do Not Receive Security Status Reports

- Yes: 57%
- No: 43%
Are reports and metrics regularly provided to your executive management team to demonstrate the effectiveness of the security program?
In your opinion, which of the following metrics are critical for measuring security program effectiveness? Select up to three.

- Threat detection metrics - e.g. time to detect attempted attacks on information assets
- Risk metrics – e.g. potential costs of from security incidents
- Compliance metrics - e.g., audit findings
- Business impact metrics - e.g. impact of security on business operations
- System availability – e.g. impact of security on uptime and accessibility
- Application performance metrics - e.g, security effect on application performance
- User productivity metrics - e.g. security effect on end user productivity

Security Pros State Threat Detection & Risk Metrics Should Be Top Security Indicators
Which of the following metrics are consistently provided to executive management to demonstrate the effectiveness of the security program?

<table>
<thead>
<tr>
<th>Metric</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance metrics - e.g., audit findings</td>
<td>79%</td>
</tr>
<tr>
<td>System availability – e.g. impact of security on uptime and accessibility</td>
<td>67%</td>
</tr>
<tr>
<td>Risk metrics – e.g. potential costs of from security incidents</td>
<td>64%</td>
</tr>
<tr>
<td>Threat detection metrics - e.g. time to detect attempted attacks on information assets</td>
<td>63%</td>
</tr>
<tr>
<td>Business impact metrics - e.g. impact of security on business operations</td>
<td>62%</td>
</tr>
<tr>
<td>Application performance metrics - e.g. security effect on application performance</td>
<td>34%</td>
</tr>
<tr>
<td>User productivity metrics - e.g. security effect on end user productivity</td>
<td>25%</td>
</tr>
</tbody>
</table>
What are the top priorities for your organization’s security program over the next 12 months?

- Endpoint security: 22%
- Privileged account security: 18%
- Application security: 17%
- Threat intelligence feeds/integration: 16%
- Cloud security: 15%
- Stored data encryption: 11%
- Supply chain security: 4%
76% Indicate that Business Value is Key When Choosing Security Solutions

Which of these factors is the most important consideration in choosing new security solutions?

- Security solution effectiveness: 24%
- Equal mix of security solution effectiveness and business impact and benefits: 45%
- Business benefits – e.g. cost savings, productivity, increased uptime, etc.: 31%
What business benefits are considered when selecting a new security solution?

- Cost savings: 58%
- Minimal system performance impact: 56%
- Increased system uptime: 51%
- Increased IT team productivity: 47%
- Streamlined business processes: 42%
- Easier trouble shooting: 41%
- Fewer IT team errors: 29%
For more information…

About Dimensional Research

Dimensional Research provides practical marketing research to help technology companies make smarter business decisions. Our researchers are experts in technology and understand how corporate IT organizations operate. Our qualitative research services deliver a clear understanding of customer and market dynamics.

For more information, visit www.dimensionalresearch.com.

Contact Us:

Diane Hagglund
Principal
diane@dimensionalresearch.com
+1 (408) 203-6982

David Gehringer
Principal
david@dimensionalresearch.com
+1 (530) 902-3995

A Quirk Magazine Top 10 Research Blog:
www.dimensionalresearch.com/blog