IT Security Trends for 2015:

Gaining insight into the demand and the difficulties

Buyers of IT security solutions are wrestling with a complex tradeoff between data security, customer expectations, and business innovation.

GATEPOINT RESEARCH

Contents

One of the most visible and highest-risk issues organizations face today is that of IT security. Meeting customer expectations demands business processes become increasingly digitized, while apps are developed to facilitate and enhance user engagement.

The 'Big Picture'

Amazon and Apple have set the bar for customers who now have expectations of a seamless digital experience. Yet, the challenge is also internal to organizations: a significant proportion of corporate data sharing now occurs in the cloud, and data vulnerability is at an all-time high with the vast majority of today's workforce having remote and mobile access.

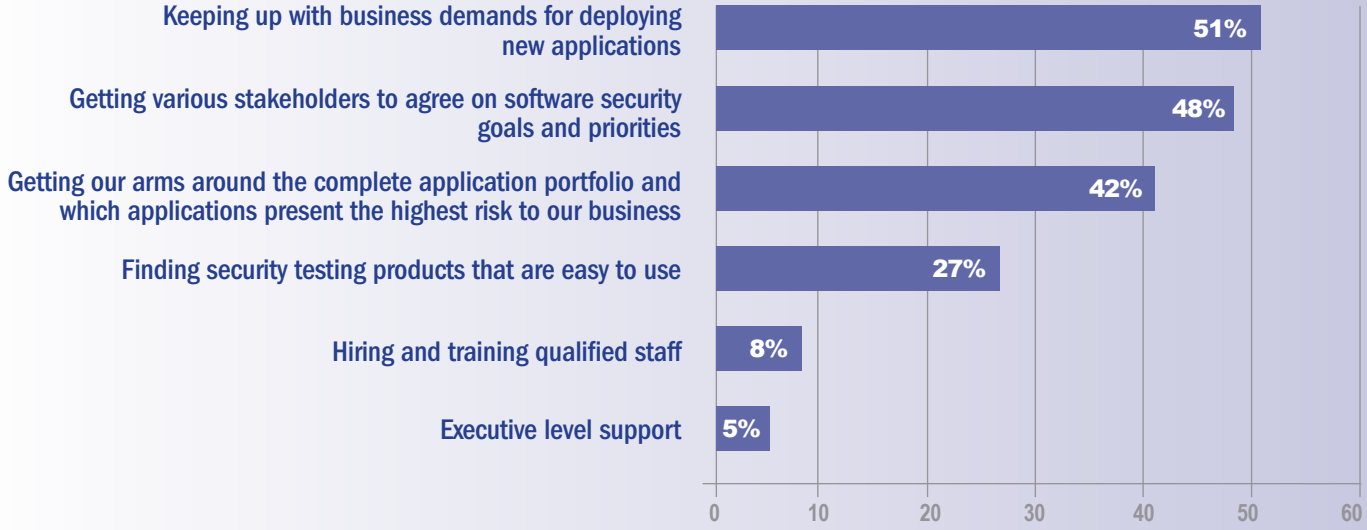
In this developing digital business context, data breaches and cyberattacks are an escalating and significant threat to organizations in the midst of transformation—a point dramatically underscored recently by the Sony Pictures data breach. Consequently, business leaders are forced to weigh risk and reward, calculating the complex trade-off between data security, customer expectations, and business innovation.

To provide insight into current trends and challenges in the IT Security market, Gatepoint Research conducted several surveys in 2014 among IT and Security executives at leading global firms. This brief synthesizes the findings from these surveys, highlighting the biggest challenges and concerns shared by buyers of IT Security, while recommending vendor actions to help buyers achieve their security goals.

Top 3 Security Challenges

Over the summer of 2014, IT and Security executives were asked, "What are the top challenges you face in achieving your software security goal?" (Figure 1)

Figure 1 What are the top challenges you face in achieving your software security goals?



1. Momentum

The collective Gatepoint Research findings indicate an increasing momentum behind the mobilization of the enterprise and the subsequent pressures felt at both the strategic and tactical levels to keep up with this momentum. These findings are supported by outside surveys conducted this year. At the tactical level, a recent independent survey of US and UK application development directors and managers (*Opinion Matters, October 2014*), revealed that "organizations are currently struggling with a significant mobile backlog and unable to cope with business demands."[i]

Likewise, this mounting pressure on the enterprise was clearly illustrated at the strategic level earlier this year in a Gartner survey of more than 2300 global CIOs. The Gartner survey found that "51 percent of CIOs are concerned that the digital torrent is coming faster than they can cope and 42 percent don't feel that they have the talent needed to face this future."[ii]

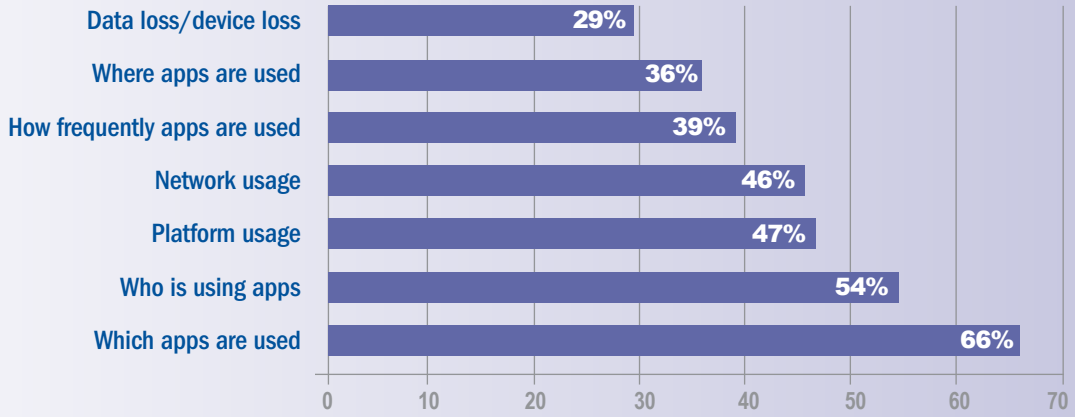
Yet, as evidenced by the Gatepoint results illustrated in figure 1, inherent in this pressure to mobilize is the challenge it poses to properly safeguard the enterprise, its stakeholders and customers by addressing the very real and pressing issue of IT-related security threats. Consequently, buyers of IT Security solutions are caught between the competing goals of rapid, yet secure quality application deployments.

2. Stakeholder agreement

Various Gatepoint Research findings give evidence to this tension among stakeholders, where conflicting priorities are revealed when comparing responses between strategic- and tactical-level perspectives. A McKinsey article (*Why senior leaders are the front line against cyberattacks, June 2014*[iii]) suggests several challenges exist in gaining widespread stakeholder agreement on IT security goals and priorities:

- *"Executives must accept a certain level of cyberattack risk."* Competitiveness and innovation, at least to some degree, requires determining a measure of acceptable risk. Gaining consensus on what that means in practical application is a tricky endeavor.
- *"The implications of cybersecurity are pervasive."* IT systems and applications are so fully integrated in the organization now that all functions are affected, bringing multiple and varied stakeholders to the table.
- *"Cybersecurity risk is difficult to quantify."* Communicating urgency and agreeing on goals and priorities is difficult when there is no clear, objective method of assessing the risk and the value of the associated mitigation tactics. Adding to the quantification challenge is the fact that the perceived level of risk is constantly in flux. Yet, as the fallout from the recent cyberattack on Sony Pictures painfully illustrates, the simple act of publicizing breached data can result in untold—and possibly irrecuperable—damages.

Figure 2 Do you have visibility into the following metrics for your mobility program?



3. App management & visibility

Rounding out the top three challenges impeding IT Security buyers from achieving their security goals is the issue of accurately assessing their application portfolio, and knowing which apps present the highest risk to their businesses. In fact, one Gatepoint Research survey this year explored precisely how much visibility survey respondents had into various aspects of their mobility program—responses indicate that over 70% of respondents have no visibility into security and data leaks (figure 2). These findings suggest a strong need for the creation and integration of security management metrics. IT Security solution vendors need to help their buyers explore the question of how effectively their mobile app development teams are addressing the critical issue of security.

GATEPOINT RESEARCH

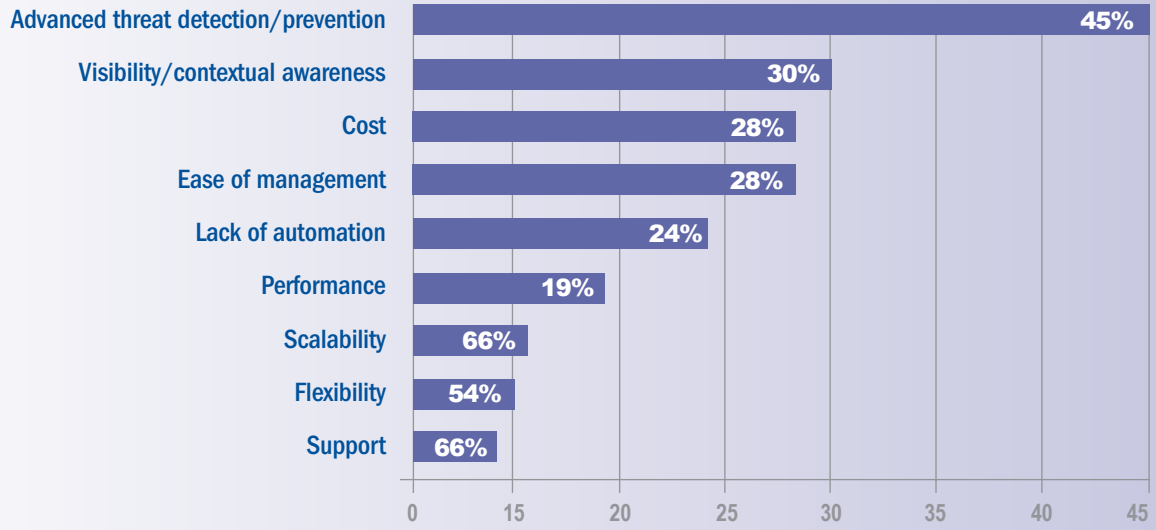
Top 3 Concerns Regarding Current Security Solution

During the fall of 2013, survey participants were asked, "Do you have concerns about specific aspects of your current security solution?"

1. Advanced threat detection/prevention

Looking ahead to 2015, Gatepoint Research survey respondents are clearly concerned: IT security executives overwhelmingly expect to see an increased pace and sophistication of cyberattacks. In fact, only 8% of respondents are optimistic for an improvement in cyberattack trends. These results are in keeping with joint research this past year from McKinsey and the World Economic Forum. Their findings, detailed in their report (*Risk and responsibility in a hyperconnected world: Implications for enterprises*[iv]), indicate that "[n]early 80 percent of technology executives said that they cannot keep up with attackers' increasing sophistication." As recent news headlines illustrate, these concerns are not misplaced; the cyberattack on Sony Pictures has at once shown how vulnerable global organizations are, as well as how easily they can be manipulated, potentially inviting an upsurge in cyberattacks. In this new, grimmer outlook for 2015, IT Security solution vendors need to help their buyers feel safer by helping them make productive gains on attackers.

Figure 3 Do you have concerns about specific aspects of your current security solution?



2. Visibility & control

Digging deeper into the issue of visibility, survey respondents were asked to indicate their satisfaction with the visibility and control provided by their current security solution regarding various aspects of their environment. Two areas stood out as lacking: 'social media' and 'mobile devices.' As businesses increasingly avail themselves of social media tactics to promote their brand and engage target audiences, IT Security vendors must integrate better visibility and control features into the full security ecosystem to help buyers more effectively mitigate risks. Likewise, buyers are seeking security solutions that help them better assess and address the threats posed by BYOD trends.

3. Ease of management & cost (tied)

To some degree, 'ease of management' is inherently related to cost, implying both effectiveness and efficiency. Yet, so too, are both issues inherently related to security. Implied in a user-friendly, easily-managed system, is one that is at once more reliable with smooth, regular security updates, more productive in its availability, and therefore more effective and efficient in minimizing security threats, safeguarding—among other things—the bottom line. By highlighting the benefits to the entire organization, vendors can focus their buyers on the lower total cost of ownership, rather on the initial purchase price.

The Opportunity

Looking towards 2015, IT Security solution vendors have an opportunity to capitalize on the security challenges and mobility momentum overwhelming the majority of organizations. Especially in the context recent high-profile and damaging events, businesses more keenly understand the clear and present danger posed by data breaches, with their primary concerns being diminished brand reputation, as well as damaged customer loyalty. And while IT security is a prime strategic imperative, aligning the organization to effectively address this critical issue is proving a significant hurdle for businesses to overcome. Meanwhile, cyber threats are growing in number and sophistication. Through a customer education program focused on the issues buyers are concerned with and challenged by, as well as those issues, skills, and threats they are failing to keep up with, vendors can help their buyers navigate the complexity of calculating the critical tradeoffs between data security, customer expectations, and business innovation.

[i] http://www.outsystems.com/company/news/2014/mobile-trend-statistics/

[ii] http://www.gartner.com/newsroom/id/2649419

[iii] http://www.mckinsey.com/insights/business_technology/why_senior_leaders_are_the_front_line_against_cyberattacks

[iv] http://www.mckinsey.com/insights/business_technology/risk_and_responsibility_in_a_hyperconnected_world_implications_for_enterprises