CompTIA

INFORMATION SECURITY TRENDS

FULL REPORT

RESEARCH

ELEVENTH ANNUAL • NOVEMBER 2013

www.comptia.org

About this Research

CompTIA's *11th Annual Information Security Trends* study builds on previous CompTIA research in the cybersecurity space, further exploring trends, challenges and opportunities. The objectives of this research include:

- Track changes in information security practices, policies, threats, breaches over time
- Identify drivers and inhibitors IT decision makers use when evaluating security tech
- Gain insights into the security issues associated with emerging technology
- Understand the role that the IT channel is playing in cybersecurity

This study consists of four sections, which can be viewed independently or together as sections of a comprehensive report. The individual sections and full report can be viewed at the security research page on the CompTIA website.

Section 1: Market Overview

Section 2: Changing Security Mindsets

Section 3: Securing Emerging Technology

Section 4: IT Channel Perspectives

This study was conducted in two parts.

Part I: End User
Quantitative online survey of 500 IT and business professionals in the United States involved in IT decision-making (aka end users). Data collection occurred during September 2013. The margin of sampling error at the 95% confidence level for the U.S. results is +/- 4.5 percentage points. Sampling error is larger for subgroups of the data.

Part II: Channel
Quantitative online survey of 500 IT firms in the United States (aka channel). Data collection occurred during April 2013. The margin of sampling error at the 95% confidence level for the results is +/- 5.0 percentage points. Sampling error is larger for subgroups of the data.

As with any survey, sampling error is only one source of possible error. While non-sampling error cannot be accurately calculated, precautionary steps were taken in all phases of the survey design, collection and processing of the data to minimize its influence.

CompTIA is responsible for all content contained in this series. Any questions regarding the study should be directed to CompTIA Market Research staff at research@comptia.org.

CompTIA is a member of the Marketing Research Association (MRA) and adheres to the MRA's Code of Market Research Standards.

CompTIA

INFORMATION SECURITY TRENDS

SECTION 1: MARKET OVERVIEW

RESEARCH

ELEVENTH ANNUAL • NOVEMBER 2013

www.comptia.org

Key Points

- IT security is consistently a top priority for companies, and many companies expect to increase their focus in this area. Twenty-eight percent of firms view security as a significantly higher priority today compared to two years ago, and 37% of firms expect security to be a significantly higher priority two years from now. With Gartner projecting the worldwide security technology and services market to reach $67.2 billion in revenue in 2013, this priority is clearly resulting in dollars spent.

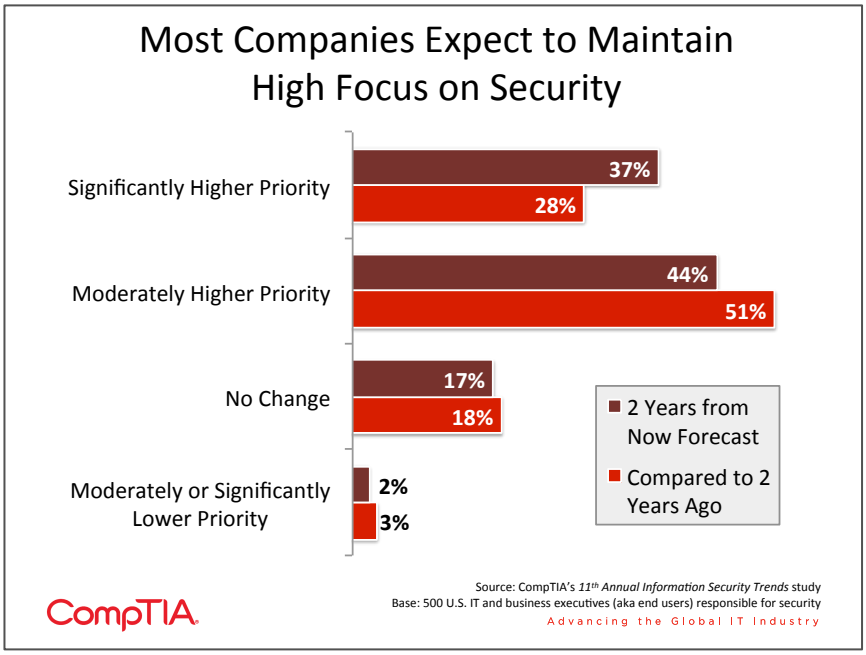
- New threats are entering the security landscape, such as Advanced Persistent Threats (APTs), Denial of Service (DoS) attacks, and IPv6 attacks. However, most companies still view hacking and malware as the preeminent threats. Companies will need to take a broader view of threats as they utilize new technology.

- The human element has become a major piece of security planning. Not only does human error account for the majority of root cause in security breaches, but companies are also finding difficulty in securing security professionals with the right skill mix. Cloud security, mobile security, data loss prevention, and risk analysis are four areas where skills are seen to be lacking. Certification is one path to ensuring the proper skills—according to the 2013 Global Information Security Workforce Study conducted by (ISC)2, 70% of companies view certification as a reliable indicator of competency when seeking to fill gaps.

The Importance of Information Security

As businesses enter an era of IT driven by cloud computing and mobile devices, they are discovering that they must alter their views on technology to account for the new options available. Technology is becoming more of a driving force for organizational goals instead of simply being used as a support mechanism. As this happens, digital data becomes much more critical and business processes can potentially transform as new models are used. In such an environment, the approach and methodology for IT security will also change.

CompTIA's *11th Annual Information Security Trends* study explores the different ways in which companies may be changing their approach to security. In general, much of the data is consistent with the findings from last year, indicating that businesses may be in a period of discovery with new technology models, and the changes to security will follow. Anecdotal evidence supports this, with security experts describing situations where a technology has been pursued for business purposes, then more thorough security analysis being performed once a process was underway.



One foundational constant in the midst of all this change is the priority that companies place on security. Security consistently ranks as a top IT priority in CompTIA surveys covering a range of technology topics. Furthermore, a significant number of firms report that security is gaining even more focus in recent years and as they look into the near future. Larger companies tend to display an even greater sensitivity to security concerns than their smaller counterparts—35% of large companies (500+ employees) rate security as a significantly higher priority today compared to two years ago, and 47% of large companies expect to place a significantly higher priority on security over the next two years.

These large companies may be more aggressive with security for a number of reasons: their risk tolerance may be lower, they may be more concerned about proprietary information, or they may believe that they are more likely to be targeted by attackers. Smaller companies, though, should not assume they are immune to security threats. Symantec's Internet Security Threat Report Volume 18 in April 2013 revealed a 42% increase in targeted attacks, with 31% of attacks targeting small businesses. This is just one of many alarming statistics surrounding the rate and cost of cybercrime:

- McAfee Labs reports that over 18 million new types of malware have been collected in 2013, bringing the total number of strains collected to 147 million. In addition, the number of mobile malware samples collected through the first half of 2013 matched the number of samples collected throughout all of 2012.
- Phishing continues to be an area of major concern as well. According to survey results released by Kaspersky Labs in June 2013, 37.3 million Internet users have been targets of phishing attacks over the past 12 months. This represents an 87% increase over the previous year.
- While security appears to no longer be a major hurdle for companies making cloud migrations—approximately 90% of companies in CompTIA's *4th Annual Trends in Cloud Computing* study claim cloud usage of some sort—it remains a sticking point for full production in the cloud. In October 2013, Adobe suffered a breach in which 2.9 million customer accounts were compromised, demonstrating that vulnerability in cloud-based systems is a serious concern.
- According to the fourth annual Cost of Cybercrime Study conducted by the Ponemon Institute, the average annual cybercrime cost to US business was $11.6 million, and the average time required to recover from a breach was 32 days. Over the four years of the study, cybercrime costs have risen by a factor of 78%, and recovery time has increased by 130%.
- On a global level, a study by the Center for Strategic and International Studies estimates that cybercrime losses fall between $300 billion and $1 trillion. The study takes a comprehensive view of costs incurred, including areas such as loss of intellectual property, opportunity costs, and reputational damage. In addition, the report connects malicious cyber activity with job loss, estimating that 508,000 US jobs are lost each year due to cybercrime.

InfoSec Spending Projections

- Gartner expects the worldwide security technology and services market to reach $67.2 billion in revenue in 2013. This represents an increase of 8.7% from 2012, and Gartner predicts continued growth to $86 billion in 2016.
- SNS Research reports that global spending on mobile security will total $9 billion in 2013. This includes measures taken for devices (such as client software for blocking mobile malware) as well as network safeguards (such as integrated security appliances or content gateways).
- It is difficult to quantify spending on cloud security, since many steps that companies take in this area involve changes of policy rather than specific investments. However, the provision of security services through the cloud (also known as Security as a Service) is projected to account for $9 billion in revenue by 2017, according to Infonetics Research.
- The channel figures to be a major player as companies invest in security. CompTIA data shows that 88% of channel firms with security offerings expect growth in security-related revenue over the next 12 months, with 23% of firms expecting significant growth (10% or more). These expectations were evenly balanced across various types of channel firms, including IT solutions providers, integrators, and managed service providers.

It is clear to see why companies view security as a top priority, and this focus will drive the expected spending in this area. However, it is less clear that companies are fully aware of which actions to take in order to build an appropriate security posture for a new era of IT. Emerging technologies are driving businesses to transform internal processes, including taking a new approach to security. Sections 2 and 3 of this report examine this in more detail, and section 4 provides an overview of channel involvement in the security arena.

Threats and Defenses

One of the major challenges in maintaining a strong security posture over time is the constant evolution of the threats one must guard against. In addition to methods such as malware and phishing that have been employed for some time and remain effective for attackers, many new forms of attack are springing up in attempts to take advantage of changes in technology.

- With the vast majority of businesses having some type of Internet portal, Advanced Persistent Threats (APTs) and Denial of Service (DoS) attacks have become popular techniques for attackers trying to gather information or disrupt availability of services.
- The explosion of iPhones and iPads has had a ripple effect in the laptop market, as MacBook market share has steadily grown. Unfortunately, that success creates a viable target, and the well-reported April 2012 outbreak of the Flashback Trojan infecting 600,000 Macs indicated that the target may have grown large enough. Indeed, 2013 has seen several additional strands of Mac malware, such as macs.app and Tibet.
- As the IPv6 protocol becomes more widely adopted, it will also grow into a viable target. Cyber criminals will be able to exploit any vulnerability found in the protocol as well as instances where system administrators have left openings during their transition from IPv4. In June 2013, website protection/optimization firm Cloudflare reported seeing a significant increase in IPv6 attacks in the previous two months.

Assessing the Cybersecurity Landscape

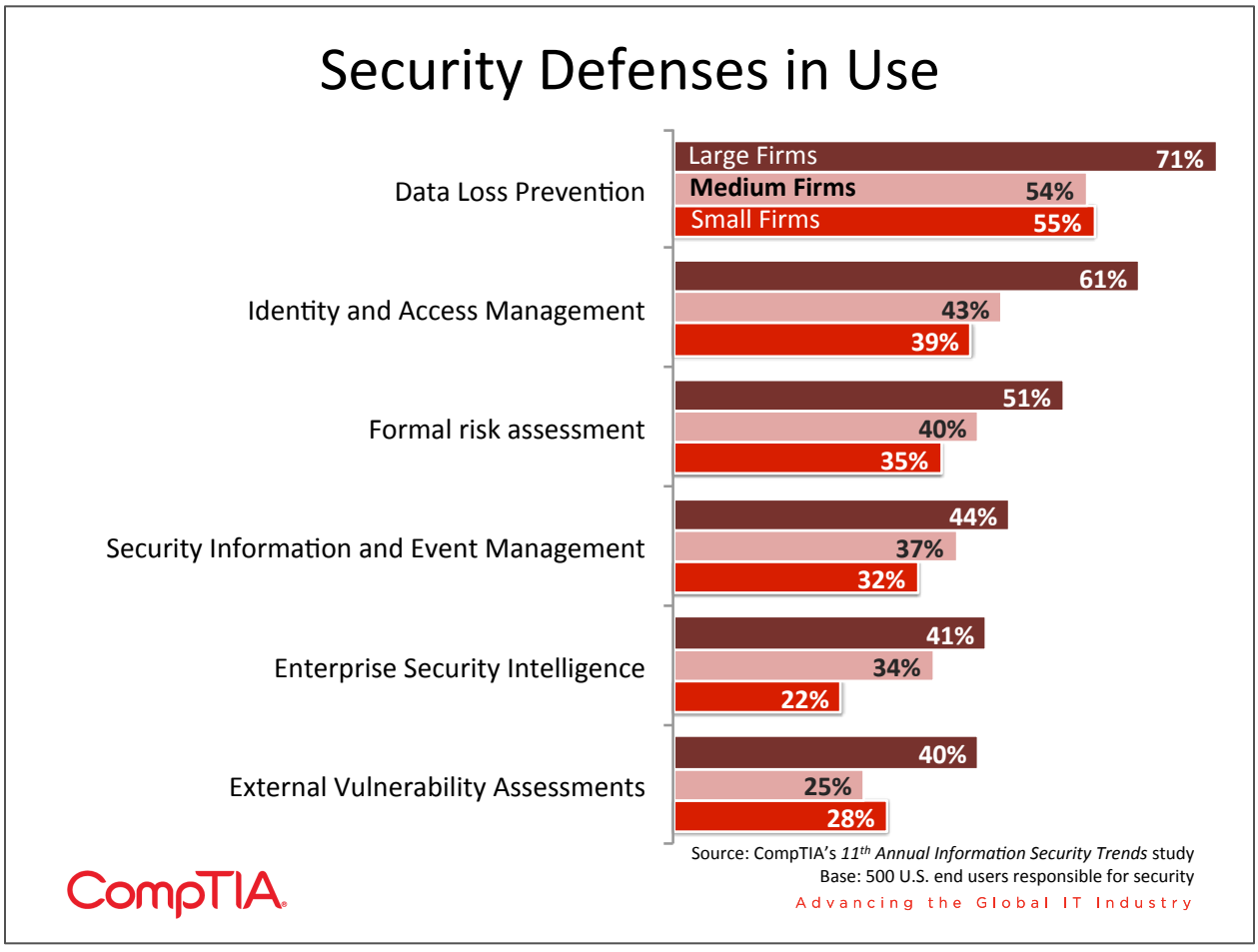
	Security Concern		Change in Trend	
Security Threats	Moderate Concern	Serious Concern	No Change / Less Critical Today	More Critical Today
Malware (e.g. viruses, worms, trojans, botnets, etc.)	38%	53%	52%	48%
Hacking (e.g. DoS attack, APT, etc.)	42%	44%	53%	47%
Social engineering/Phishing	45%	37%	62%	38%
Data loss/leakage	46%	35%	70%	30%
Understanding security risks of emerging areas, i.e. cloud, mobile, social	49%	32%	61%	39%
Physical security threats (e.g. theft of a device)	42%	28%	72%	28%
Intentional abuse by insiders, i.e. staff, contractors	42%	26%	76%	24%
Lack/inadequate enforcement of company security policy	45%	23%	77%	23%
Lack of budget/support for investing in security	42%	23%	76%	24%
Human error among IT staff	47%	22%	80%	20%
Human error among general staff	55%	21%	76%	24%

Source: CompTIA's *11th Annual Information Security Trends* study
Base: 500 U.S. end users responsible for security

CompTIA
Advancing the Global IT Industry

Given this change in the threat landscape, it is somewhat surprising to see that the levels of concern for a wide range of threats remain virtually unchanged from last year, where malware and hacking are by far the greatest concerns and there does not appear to be a balanced attitude across all types of threats. Larger companies have more awareness that many types of threats can be a concern—small businesses consistently reported a lower level of concern or less belief that threats are more critical today.

A wide range of threats implies a need for a wide range of defenses. In line with viewpoints on threats, companies are not displaying any greater tendency to use a diverse set of defenses than in the prior year. Data Loss Prevention (DLP) still has the highest adoption rate among newer defense techniques, likely due to companies' greater reliance on data and the desire to track data more closely as it moves between cloud providers and mobile devices. All other defenses, though, have been adopted by less than half of the population.

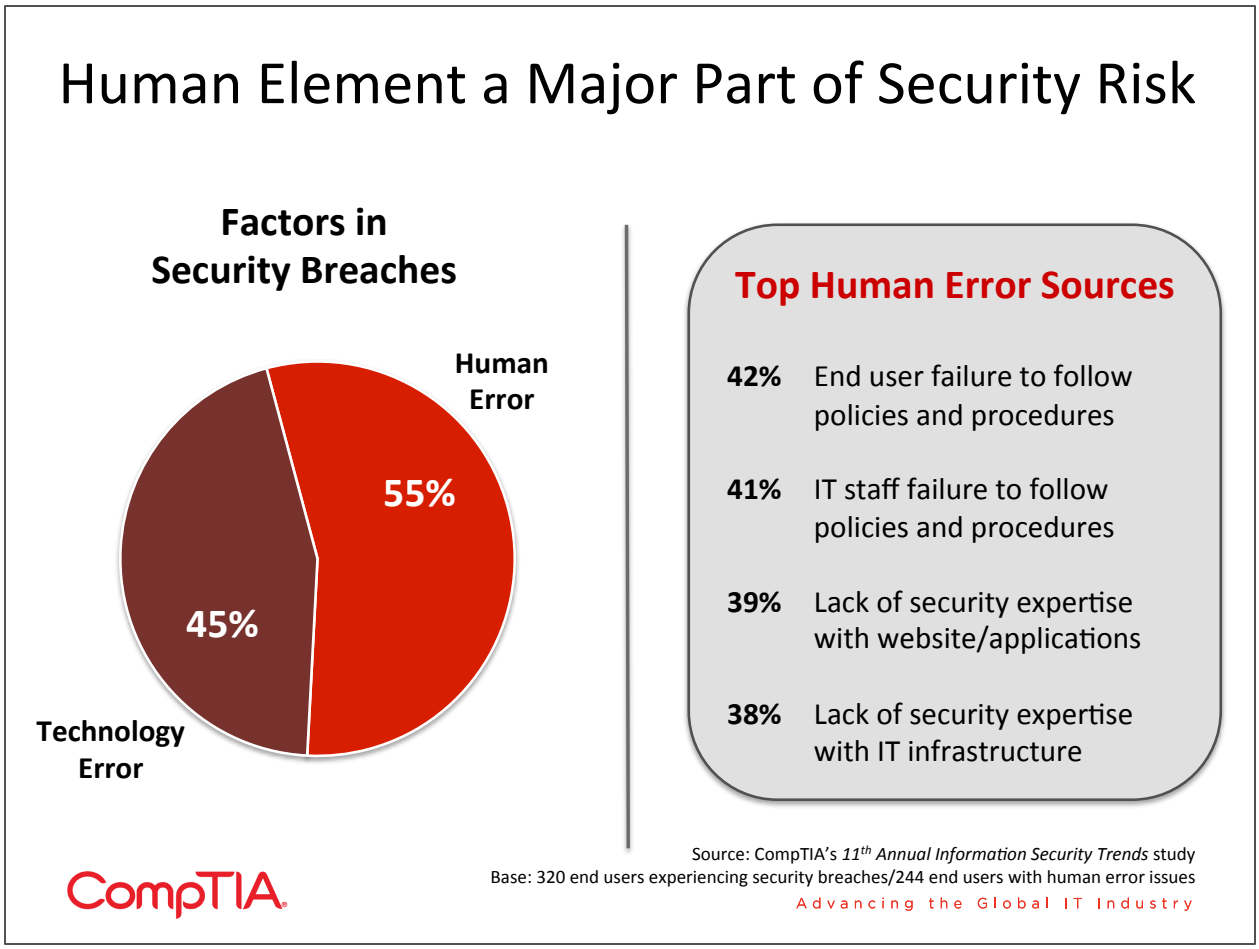


It is interesting to note that an overwhelming majority of companies (82%) view their current level of security as completely satisfactory or mostly satisfactory. In theory, companies may not exhibit concern over threats because they have taken the necessary steps for protection. However, the viewpoints on threats and the usage patterns on defense mechanisms, when taken together, suggest that many companies may be assuming a satisfactory level of security without truly performing due diligence to understand their exposure.

The Human Element of Security

Beyond the technology that may be used to attack or defend, the human element is becoming a more significant factor in security considerations. There are two distinct areas that businesses are dealing with when it comes to managing the human aspect of security: mitigating the risk introduced by users of technology and finding the right personnel for security implementations.

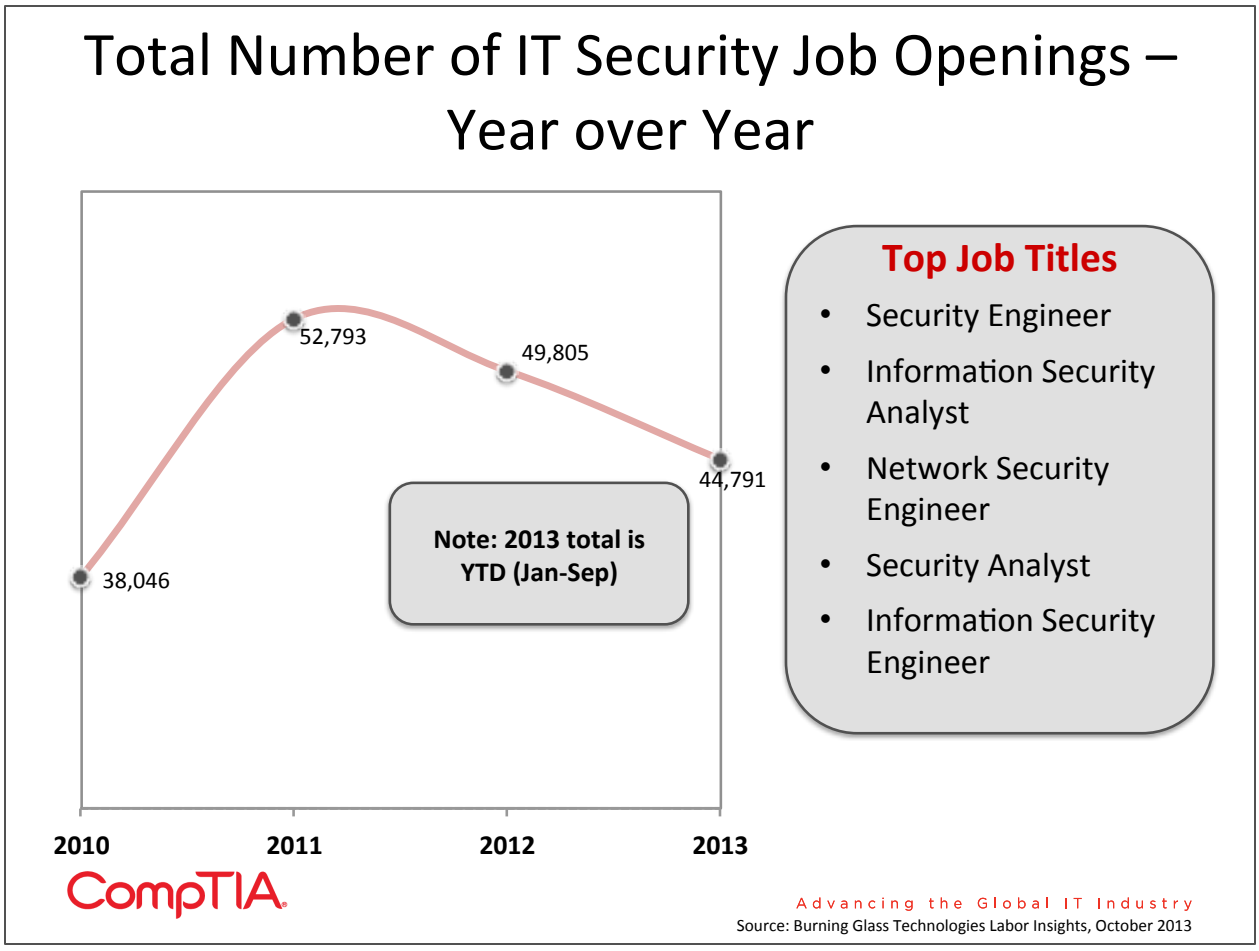
The risk introduced by end users is steadily growing as cloud computing, mobility, and social media all drive further into the enterprise. End users have gained control of powerful devices and business class systems, often without the oversight of the IT team. End users may be able to utilize these systems, but they typically do not have the background knowledge and experience with security that allows them to recognize potential threats.



When it comes to assessing security incidents, companies attribute over half of root cause to human error. In addition, 51% of companies report that human error has become more of a factor in security over the past two years, up slightly from 46% last year. Given these statistics, it is especially striking that so few companies view human error as a serious concern.

The issue may be that companies are unsure how to tackle the problem. With the top sources for human error being a failure to follow policies, the issue is one of education rather than technical improvement. Companies are finding that they must shift their education to be more interactive, ongoing, and measureable in order to raise the level of awareness and expertise in security.

As for finding qualified security personnel, the continued focus on information security has meant that it is one of the unique fields where demand exceeds supply. According to the labor intelligence firm Burning Glass, the number of information security openings has remained high over the past three years, peaking in 2011. The Bureau of Labor Statistics instituted the category of information security analyst in 2011, and the projected rate of change in employment for the 10-year timeframe between 2010 and 2020 is 22%. The average growth rate for all occupations is 14%. The 2013 Global Information Security Workforce Study conducted by (ISC)2 found that even with growth in the security profession, 56% of security professionals believe there is a workforce shortage. The study also found that 70% view certification as a reliable indicator of competency when businesses are seeking to fill gaps. See the appendix for CompTIA's findings on certified security professionals.



CompTIA's survey also shows that companies are at less than optimal levels of staffing when it comes to security. Twelve percent of companies feel that their security team (which could be internal or external) is significantly deficient in skill level, and another 21% feel that their security team is moderately deficient. The effects of these deficiencies are wide-ranging, from being unaware of exposures or trends to incurring additional costs and even losing business.

Top Areas of Security Deficiencies

- **Cloud security (56%).** As mentioned above, the solution to cloud security is more policy-driven than technology driven. Understanding cloud security implies a general understanding of cloud systems and how businesses can best use them.

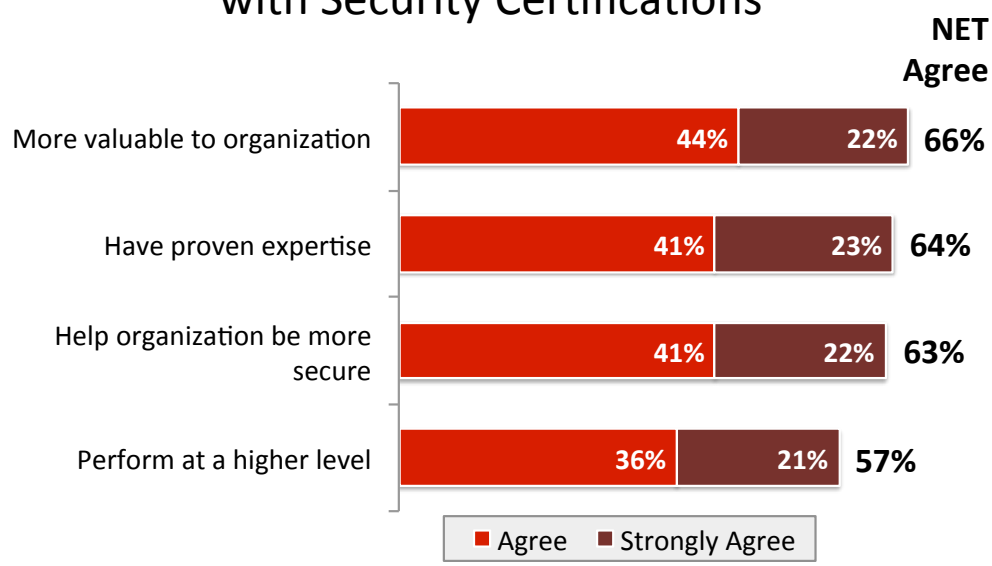
- **Mobile security (48%).** The desire for productivity and flexibility is driving many business to adopt a "use first, secure later" approach to mobile devices. Security professionals have a significant challenge in analyzing and implementing mobile security solutions in the midst of adoption.

- **Data loss prevention (46%).** CompTIA's *2nd Big Data Insights and Opportunities* study found that 93% of companies rate data as important or very important to business success. Data leakage or loss can have a major business impact, and many firms are looking for best practices in this relatively new area.

- **Overall risk analysis (35%).** Since too much data behind the corporate firewall can hinder productivity and too much data in front of the firewall can create a liability, businesses must carefully assess availability decisions. This is an area where knowledge of the business must be matched with technical capabilities.

Appendix

Most Companies See Benefits in IT Professionals with Security Certifications

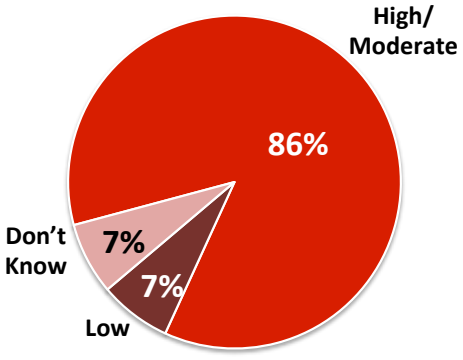


Source: CompTIA's *11th Annual Information Security Trends* study
Base: 500 U.S. IT and business executives (aka end users) responsible for security

Advancing the Global IT Industry

Certified Staff Provide Value to Organizations

View of ROI of Certified Staff



Breakdown of High/ Moderate ROI Viewpoints

81% among executives, indicating strong value for hiring potential

81% among users with a business role, indicating a broad audience for certifications

93% among companies making drastic security changes, indicating importance as companies alter security posture

Source: CompTIA's *11th Annual Information Security Trends* study
Base: 500 U.S. IT and business executives (aka end users) responsible for security

Advancing the Global IT Industry

CompTIA

INFORMATION SECURITY TRENDS

SECTION 2: CHANGING SECURITY MINDSETS

RESEARCH

ELEVENTH ANNUAL • NOVEMBER 2013

www.comptia.org

Key Points

- The use of new technology necessitates a change in security approach. With cloud computing and mobility gaining wide adoption, 64% of companies report a drastic or moderate change to their security approach. Along with technology changes, a new security approach can be driven by reports of other breaches or knowledge gained from training or certification.

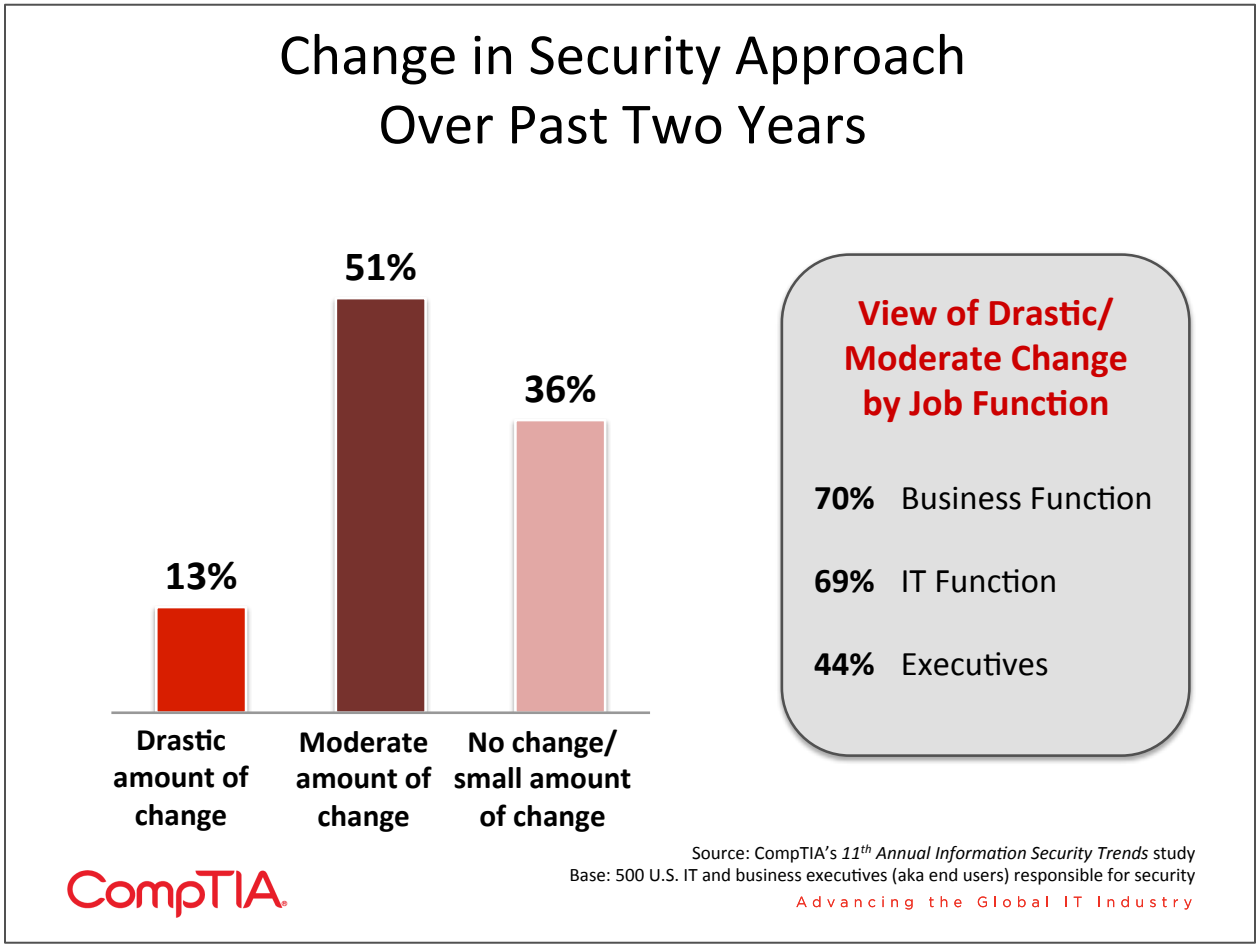
- Risk analysis is becoming a critical activity as companies decide how to handle corporate data, but only 41% of companies are currently performing this in a formal way. While most companies believe that their balance of risk and security is appropriate, those firms that have performed detailed analysis have found reasons to either accept more risk or tighten security, depending on their business objectives.

- More than half of the businesses in the survey view some opportunity to improve the security mindset of their employees and increase their understanding of the corporate policies. In seeking education that is more interactive and ongoing than standard annual security reviews, seven out of ten companies indicate that a tool providing workforce assessment and targeted training would provide relatively high value or very high value.

A Different Approach

Many traditional security technologies are evolving, and many new technologies are springing into place to address new issues. Firewalls are a good example of evolving technology. They initially filtered network traffic based on packet inspection and have advanced to the point of understanding applications and protocols. As for new technologies, Data Loss Prevention (DLP) and Identity Access Management (IAM) are two prime areas where security products are attempting to meet the needs of businesses that are utilizing more cloud solutions and mobile devices.

These technologies, though, are tools in a toolbox that must be used within a larger security framework. It is commonly accepted that companies can no longer build a secure perimeter to protect their assets, but that discussion tends to quickly turn towards the way that technology is progressing beyond a traditional firewall. The reality of the situation is that the overall approach must be re-evaluated from the top levels of a business and down through all departments.



Consistent with last year's findings, nearly two thirds of companies have experienced some amount of change in their approach to security over the past two years. Company size has some impact, with large companies (500+ employees) more likely to have made changes. However, there is a sharper difference when it comes to job function. The fact that executives view change as less significant compared to workers in business or IT functions indicates that executives are unaware of the true cost of security change, including staff time spent implementing changes or adjusting to new workflows.

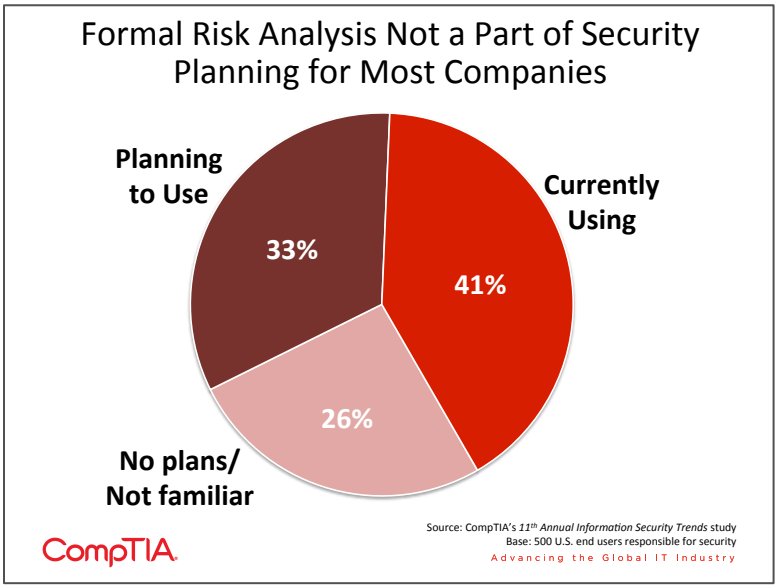
The main driver for new security approaches has been a change in IT operations—56% of the sample report that a move to cloud solutions or a new mobility strategy has been responsible for new security tactics. Reports of breaches at other organizations (40%) and internal security breaches (34%) also tend to drive change, highlighting the tendency of companies to react to security incidents. Four out of ten companies also report that their security approach changed as a result of knowledge gained from training or certification, showing the importance of maintaining up-to-date knowledge and hiring knowledgeable workers.

On the other hand, there are hurdles to pursuing new security initiatives. Forty-seven percent of companies report that a main hurdle is the corporate view that security is adequate—not surprising given that 82% of companies view their security as mostly or completely satisfactory. Other hurdles include prioritization of other technology (42%) and a low understanding of security threats (38%).

A modern approach to security mainly involves changes in two areas: risk analysis and end user awareness. Many companies are familiar with security risk analysis and may be taking steps to properly address different levels of risk, but many others may still be operating from a more traditional mindset. In general, companies seem to be further behind the curve with end users, not fully appreciating the level of effort that must go in to equipping users with knowledge and responsibility in a consumer-driven IT landscape.

Risk Analysis, Mitigation, and Tolerance

Risk analysis is certainly not a new concept for businesses, especially within firms that have a strong project management mindset. Typical analysis activities might include determining the probability of a risk, estimating the potential impact, and determining mitigation strategies. The time and effort involved in building mitigation is directly related to the probability and impact—a high probability/high impact risk requires a more robust mitigation than a low probability/low impact risk.



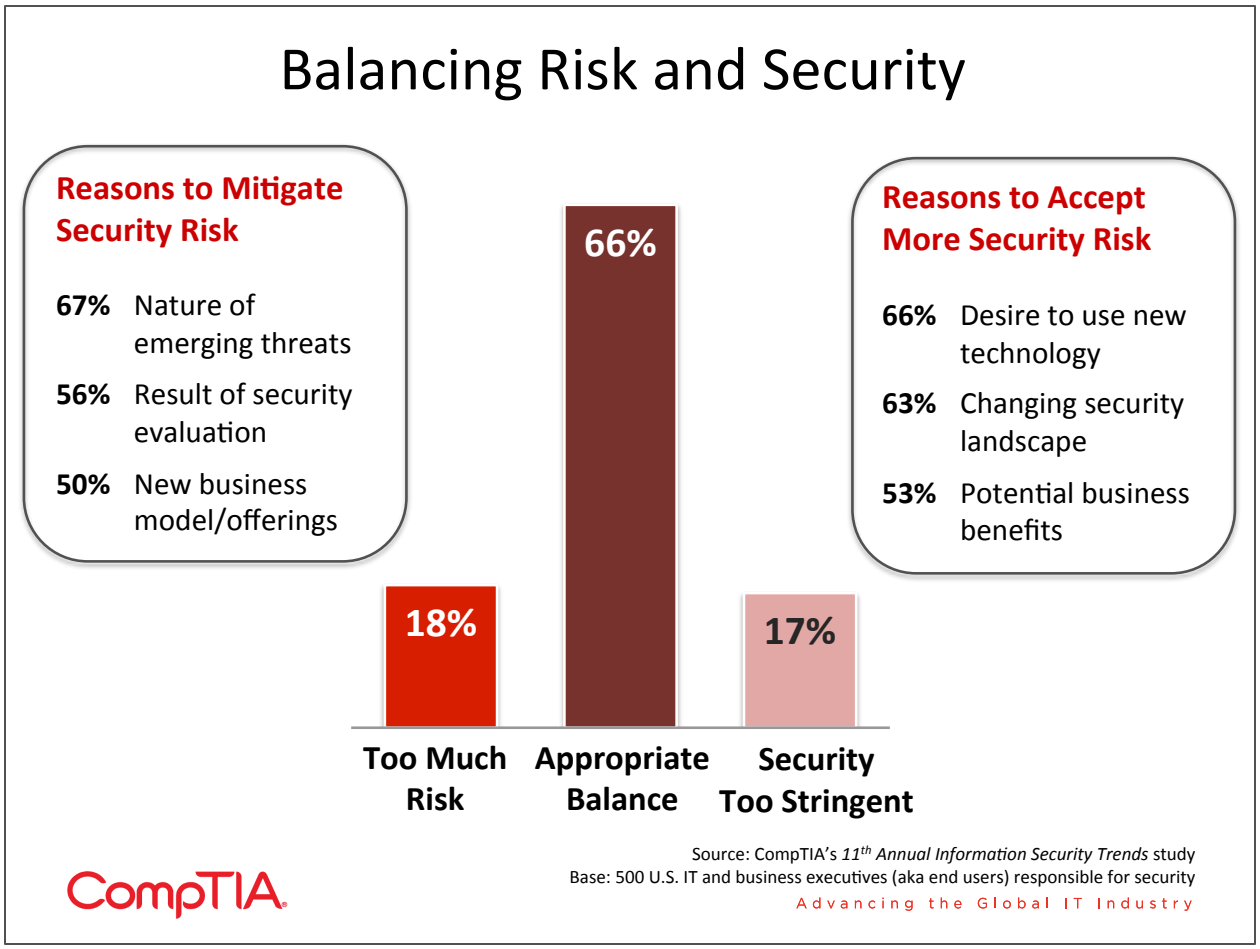
When it was simpler to keep corporate information in a confined area (physical or digital), companies could take a simpler approach to risk analysis. Any information that had any degree of confidentiality could be treated the same and placed inside a secure perimeter. Access to the information could more easily be restricted to corporate devices, either on-premise or through a VPN. The chances of an employee accidentally sharing corporate data to the public were small, though those chances grew as PCs entered homes and laptops became primary work devices.

The trends of cloud computing and mobility have driven those chances much higher in a relatively short amount of time. By definition, public cloud computing requires data to reside outside a company's

control, and productivity on mobile devices is severely limited if corporate systems are not made available. Companies now must evaluate their data and systems to determine which are the most critical to the business and therefore in need of the strongest defenses.

Maintaining very strong defenses for all data and systems is simply too costly. Consider the example of server uptime, a prime factor in the availability component of the security equation. If a system generating $1 million per year in revenue is running on hardware with 99.9% uptime (the uptime defined in the Amazon Web Services SLA), there will be approximately 10 minutes of downtime resulting in just $19 of lost revenue per year. Achieving 99.99% uptime would reduce the downtime to 1 minute and $1.90 of lost revenue—it would be difficult to find a viable backup solution that could improve uptime for less than $20 per year.

Formal risk analysis, then, can provide some balance to the cost equation as companies decide where to place investments. Beyond that, it can give businesses the confidence that they have selected the appropriate level of security for all of their data and systems. Examining companies who felt they had at least a satisfactory level of security, there is a clear correlation to risk awareness. Twenty-four percent of companies in this category were not familiar with risk analysis or had no plans to use it. That number jumps to 34% as companies make plans to use risk analysis and 44% when it is currently implemented.

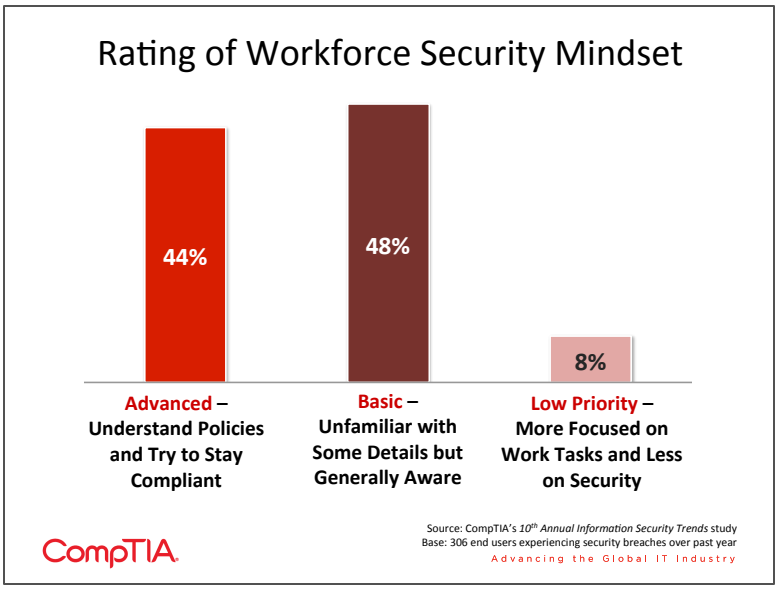


It is not surprising to see that most companies view their balance of risk and security as appropriate. Given the adoption level of formal risk analysis, though, it is also reasonable to assume that many companies have not carefully analyzed this position and simply base their assessment on a gut feel. Predictably, those respondents working in a business function were more likely to feel that security was too stringent, although the view of risk being excessive was shared equally among executives, IT function, and business function.

This highlights the fact that risk analysis is not just the purview of the IT department. It is not reasonable to expect that a CISO or Director of Security will have all the knowledge necessary to properly classify data so that it receives adequate security. Security, like many other areas in technology, is becoming a company-wide exercise, and risk management in particular fits this bill. All executives (or other appropriate stakeholders) must collectively decide what constitutes risk and which areas are the most critical for a business. The CFO, CMO, and other business unit executives can provide input on the nature of their data, and the CIO can advise on the costs and complexity involved in security.

Raising Awareness Levels

As section 1 described, the human element is becoming a great concern for businesses as they determine how best to secure themselves while progressing into new uses of technology. At the most fundamental level, this issue stems from a proper security mindset. Do employees fully understand the reasoning behind security policy and act in the best interest of the company, or are they more interested in getting work accomplished regardless of security implications? In other words, will employees follow the letter of the law (if at all) or truly embrace the spirit of the law?



According to CompTIA's survey, very few employees land at the far end of the spectrum where security is disregarded. However, nearly half the sample indicates that while their employees generally try to stay aware of security concerns, they may not understand all the details of policy, implying that they also may not be able to make the correct judgment call if faced with a new situation.

In such an environment, raising the general level of security literacy becomes part of the investment required for greater corporate protection. As companies pursue education that is more interactive and ongoing than standard annual security reviews, they will also have need of assessments to indicate areas in need of additional training. It would appear that most companies are not currently using such a product—seven out of ten companies indicate that a tool providing assessment and targeted training would provide relatively high value or very high value.

Overemphasizing IT security products can lead to blind spots in three other areas: policy, process, and people. Those companies who are best in class with regard to security will focus on all four areas: policies (with proper risk analysis) will define corporate guidelines, processes will help maintain integrity, products will assist with protection and monitoring, and people will be trained so that they are more aware and responsible. A company-wide emphasis on security will help ensure that the best technology can be used to make the entire workforce productive without placing the company at risk for becoming another cybersecurity statistic.

CompTIA

INFORMATION SECURITY TRENDS

SECTION 3: SECURING EMERGING TECHNOLOGY

RESEARCH

ELEVENTH ANNUAL • NOVEMBER 2013

www.comptia.org

Key Points

- Security concerns are clearly not preventing mass adoption of cloud computing, with 90% of companies in CompTIA's *4th Annual Trends in Cloud Computing* study claiming some form of cloud usage. However, security concerns definitely persist beyond the initial adoption phase, driving more companies to examine cloud provider policies and in a growing number of cases change providers or revert to on-premise systems.

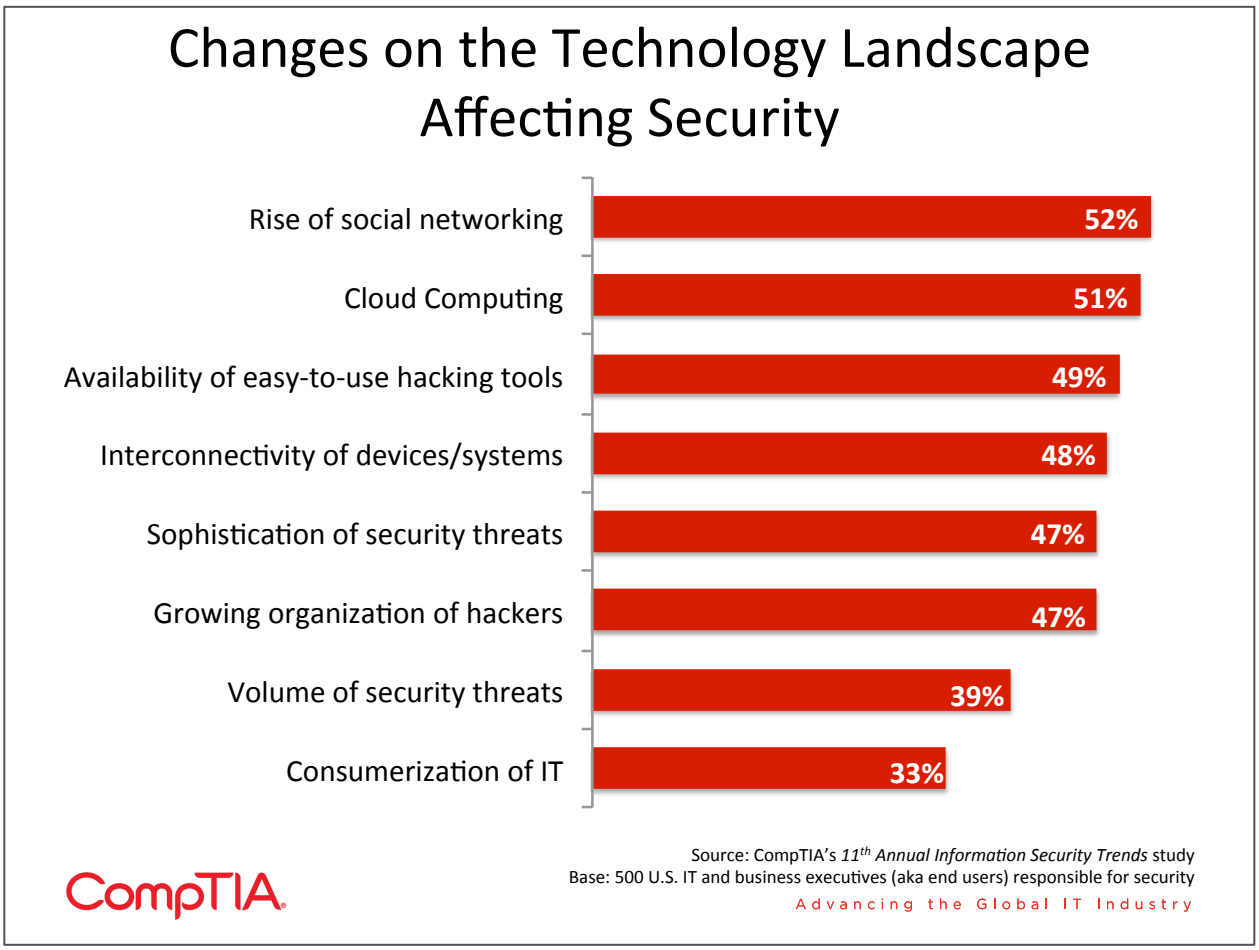
- Lost or stolen devices are still the most common type of mobile security incident. Mobile malware, though, is quickly becoming a concern, with 28% of companies experiencing this attack (up from 19% in 2012). With only 28% of respondents citing mobile malware as a serious concern, companies will need to quickly get up to speed on this growing threat.

- Data loss or data leakage continues to be a major concern for businesses, but 22% of firms indicate that they believe data loss has occurred but are not sure *which* data was lost. This suggests a need not only for data loss prevention technology and policy, but also general data management best practices.

Technology Trends Drive Security Change

The domain of security is tightly tied to the composition and changes of the technology environment. Tools and practices are built around current usage, and shifts in technology open doors for attackers that must be closed. Security by nature tends to be more reactive for many companies: *if* they are going to use technology in a certain way, *then* they must take the steps to secure that technology. Very few organizations will spend resources on security tools that are needed for potential future usage of technology.

From the viewpoint of a security practitioner, there is certainly a need to react quickly to changes in the market. There is also a need to be proactive in thinking about new technology. As a technology passes a tipping point where it becomes clear that there will be wide adoption, security vendors and service providers should take a long view, applying past history and current knowledge to future possibilities. The shifts to networked offices and business on the Internet brought about new methods for security, and the shifts underway in enterprise technology today are no less significant. See the appendix to view some differences in the ways that technology changes are perceived by companies of different sizes.



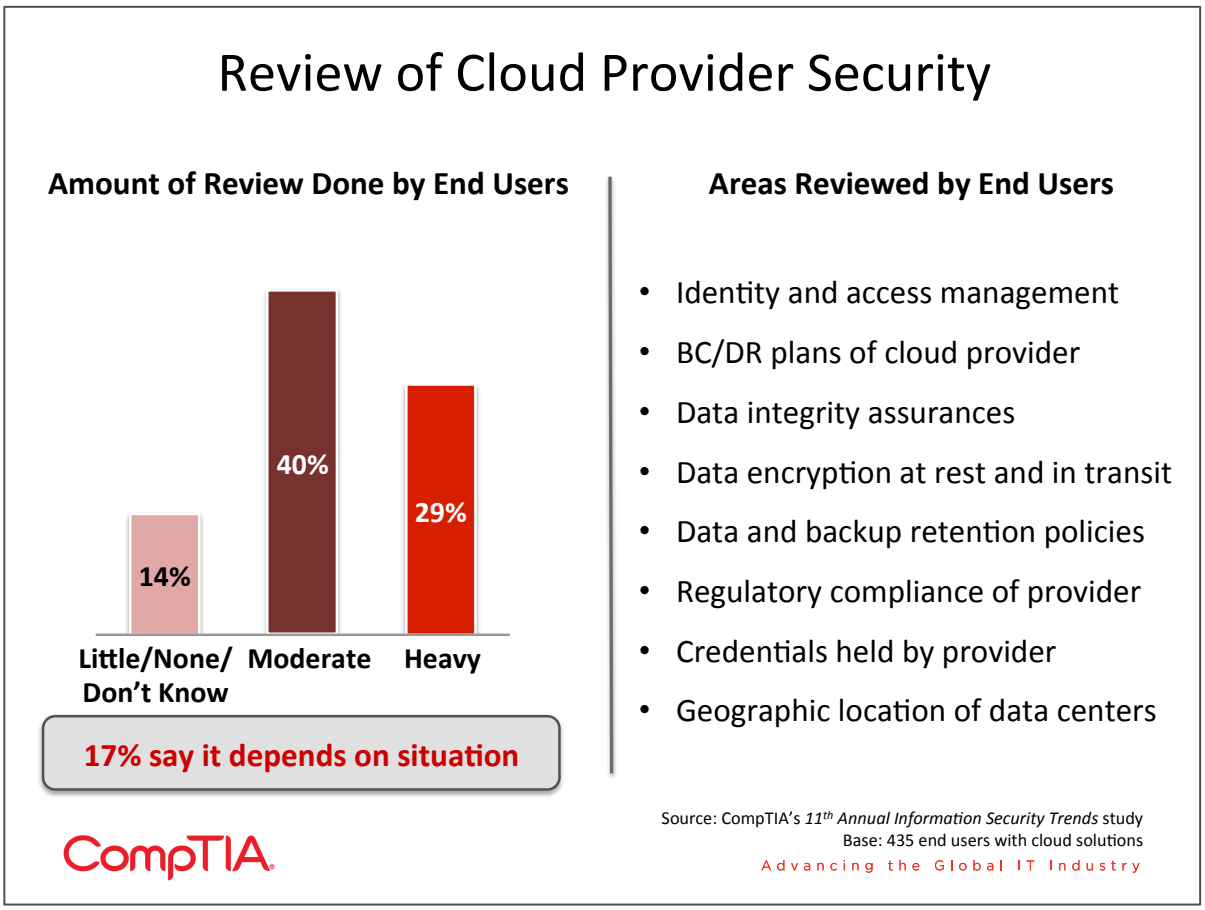
Cloud computing and mobility have ushered in a new era of enterprise technology. It is not only the processes and tools used by the IT department that are changing, but also the general use of technology throughout the entire organization. Similarly, an increasing reliance on technology and rapidly

accelerating creation of digital data have forced businesses to review their data practices as they consider Big Data initiatives. As attackers seek to exploit vulnerabilities exposed through the adoption of these trends, IT departments and solution providers must be aware of the potential threats and be quick to build new defenses.

Cloud Security: From Deal Breaker to Game Changer

Throughout the early stages of cloud adoption, security has consistently been cited as the top factor keeping companies from moving to cloud systems. However, with 90% of companies in CompTIA's *4th Annual Trends in Cloud Computing* study claiming some form of cloud usage, security is clearly not preventing mass adoption.

Still, security remains a major focus area even after companies have performed their first cloud migrations. Anecdotal evidence suggests that many firms placed a higher priority on potential benefits of cloud computing as they moved to the cloud, and with the proof of concept now behind them they are returning to security discussions to ensure that their operations and data are protected.

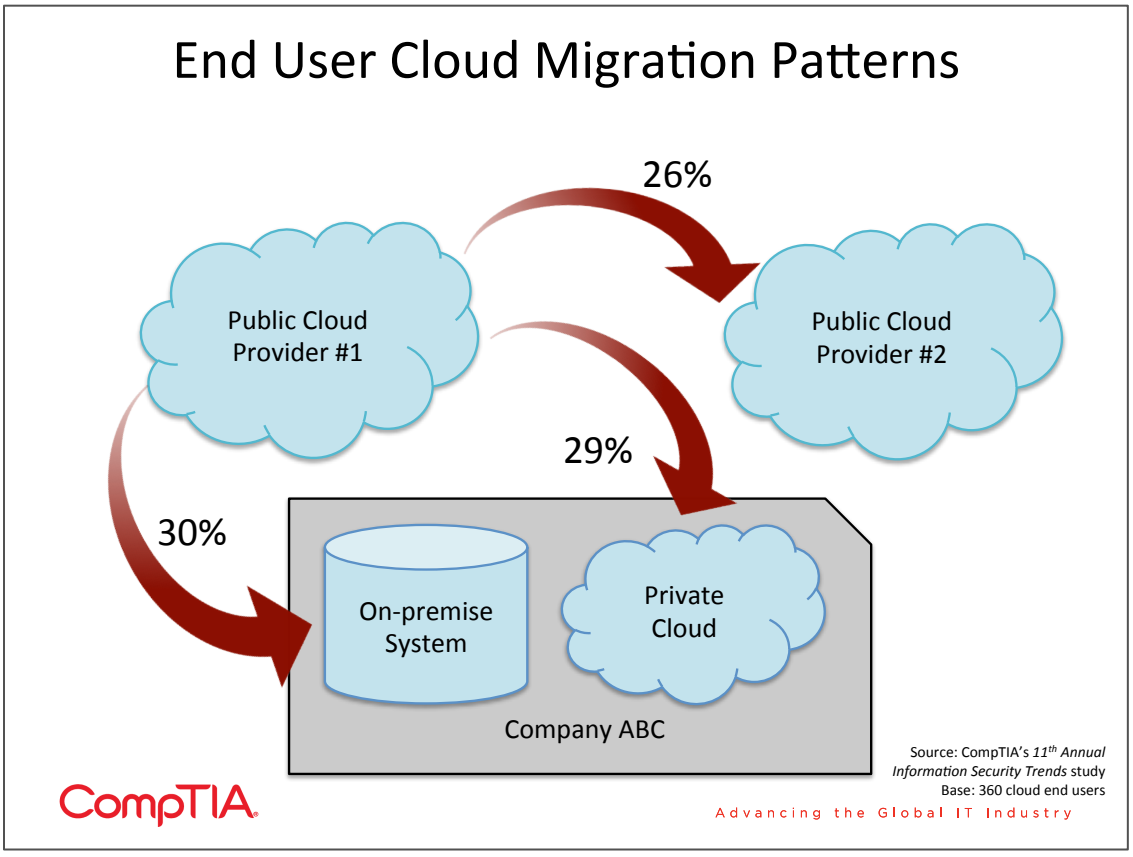


A common concern related to cloud security is that a provider will not match the specific security requirements of an end user, and this concern is valid. A cloud provider by necessity will have a base level of security that serves the needs of all its users, and each user must take steps from there to create their own security posture.

That begins with understanding the practices of the provider. Compared with last year, approximately the same percentage of companies are performing moderate or heavy reviews of their cloud providers. Generally, large companies are more likely to review their providers, though some areas (such as data backup and retention policies) see relatively balanced review from all company sizes.

For a technology trend that has such large disruptive potential, the amount of review is probably on the low side, and companies may not place enough focus on cloud-specific issues, such as geographic location of data centers. End users that are performing little to moderate review may want to examine best practices and typical provider questions, using resources such as CompTIA's End User Buying Guide for Cloud Computing or the Consensus Assessment Initiatives Questionnaire from the Cloud Security Alliance.

Privacy is one aspect of security that is quickly becoming its own concern. Incidents of government data gathering and confusion over ways that data is being used have led to a heightened sensitivity over privacy. Nearly four out of ten companies state that they have a high focus on privacy, handling it separately from more traditional security issues. As businesses gain a better understanding of their cloud providers' data practices, they will also have to be more transparent about data usage with their customers and partners.



The continued focus on privacy and security even after an initial cloud migration has led many firms to explore alternatives to their original provider. The trend of secondary migrations was explored more fully in CompTIA's *4th Annual Trends in Cloud Computing* study, and that trend is confirmed by the rates at which companies in the security study have made secondary moves. Although security concerns are

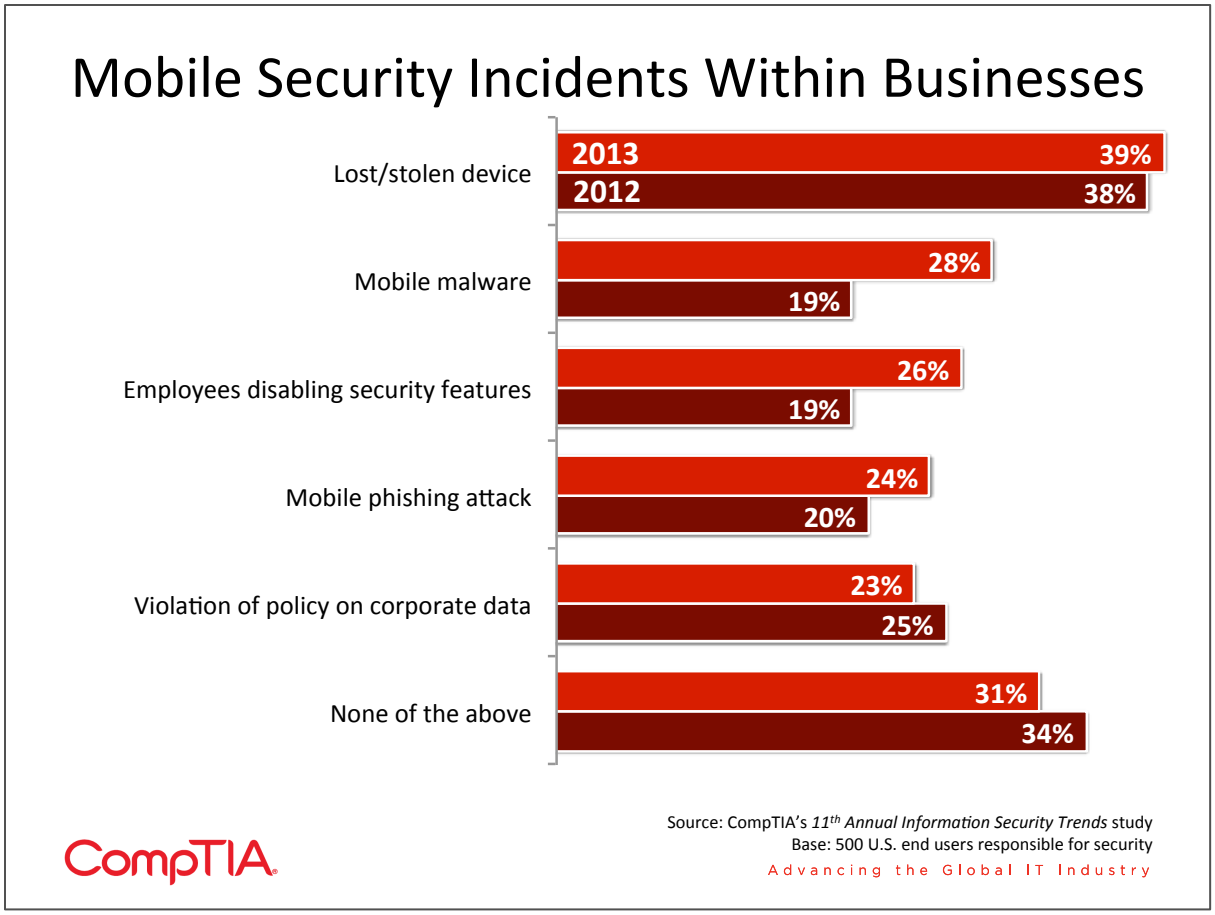
driving some applications back into on-premise systems, some applications are certainly remaining in the cloud, and the use of multiple cloud models implies a significant management and security challenge.

Mobility: A New Platform for Attackers

Just as cloud computing forces businesses to consider data leaving the company and residing with a third party, mobility forces businesses to consider data leaving the company in the hands of its employees. Many IT departments have made the switch to laptops as primary work devices, giving them some experience with devices that may not stay within the secure confines of an office. However, the introduction and rapid adoption of smartphones and tablets in the consumer space has bled over into the corporate world and created a need for new methodologies.

Smartphones and tablets present two main challenges. First, end users are less likely to simply accept whichever device the IT department may choose to provide. There is a much stronger personal connection to these devices, and employees want to use the device of their choice in the way that they want. This is the primary driver behind the Bring Your Own Device (BYOD) movement.

The second challenge is that these devices are more closed than laptops. IT departments are not able to place the same types of safeguards on smartphones and tablets so that they access corporate systems and data in a controlled fashion. Furthermore, any safeguards that are installed have more of an impact on the function of the device, which in turn can impact productivity.



While there have been some substantial changes in the types of mobile security incidents companies are experiencing, the levels of concern surrounding mobile security remain largely unchanged. Theft or loss of a device is still the most common incident, and it is also the most common worry among companies. Mobile malware is definitely a more serious issue this year, though, and those companies not listing this as a concern may be unaware of the gravity of the threat. The discrepancy can be seen in other research as well: McAfee found that 14,000 new mobile malware incidents were discovered in just the first quarter of 2013, and only 42% of companies in a survey they conducted were performing mobile malware scanning.

Top Concerns in Mobile Security

% of respondents rating as serious concern

32%	Theft or loss of corporate device
28%	Mobile device-specific viruses/malware
26%	Risks associated with social media
26%	Employees downloading unauthorized apps
26%	Malvertising
23%	Using personal devices for business purposes

Even if there are gaps in how companies perceive mobile security threats, the uptick in the actions companies are taking to defend mobile devices is an encouraging sign. More companies are encrypting data on mobile devices (56% vs. 51% in 2012), keeping the OS and apps up to date (43% vs. 39%), and preventing jailbreaking (38% vs. 34%). In addition to these technical changes, policy changes are being made, such as ensuring that devices are with the employee or secured at all times (54% vs. 48%).

Device passcodes are still the most common mobile security measure, with two thirds of the sample requiring passcodes on devices that access corporate systems. While passcodes have been shown to have limited security potential, they at least provide a first level of deterrent against amateur attackers. One of the most common challenges in mobile security is the need for improved technology, and the recent introduction of fingerprint authentication on the iPhone 5s presents an intriguing possibility. A small poll of 1,000 random individuals conducted by CompTIA using Google Consumer Surveys showed only a slightly positive view of this technology, with the primary concerns being usability and overall security. However, an effective fingerprint technology may provide at least the same level of security as a passcode while providing greater convenience, acting as a viable substitute for that first level of defense.

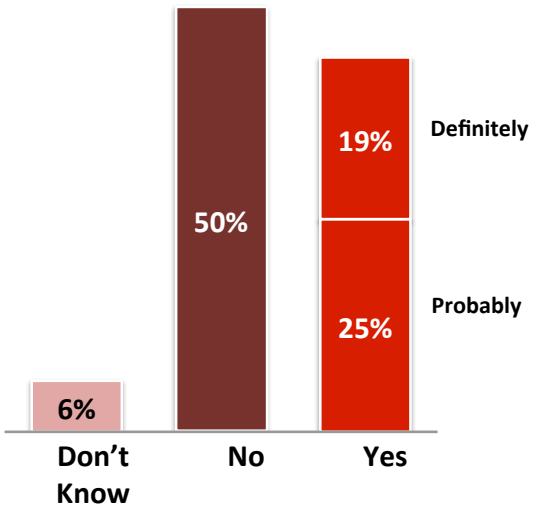
Data: Too Much Leaking Can Bring a Flood of Problems

Digital data is becoming the lifeblood of a business—CompTIA's *2nd Annual Big Data Insights and Opportunities* study showed that a net 87% of companies believe data is important to business operations. As cloud solutions become standard parts of IT architecture and mobile devices proliferate, building a secure perimeter is impossible and the data itself must be secured in some way.

Compared to last year, the incidence of data loss has risen slightly. In 2012, only 13% of companies stated that they had definitely experienced data loss. Similarly, the types of data being lost have risen across the board, indicating that attackers are finding financial gain from a wide range of data, not just customer financial records or intellectual property. It is especially troubling to see an increase in the number of firms stating that data loss has occurred, but they are not sure what types of data have been lost. This shows a pressing need for not only better data protection, but also better data management in general.

The Growing Threat of Data Loss

Experiencing Data Loss in the Past Year



Types of Data Lost

55%	Corporate financial data
43%	Data about employees
42%	Intellectual property
28%	Customer data
22%	Believe data was lost, but not sure which data

CompTIA.

Source: CompTIA's *11th Annual Information Security Trends* study
Base: 500 end users/190 end users experiencing data loss

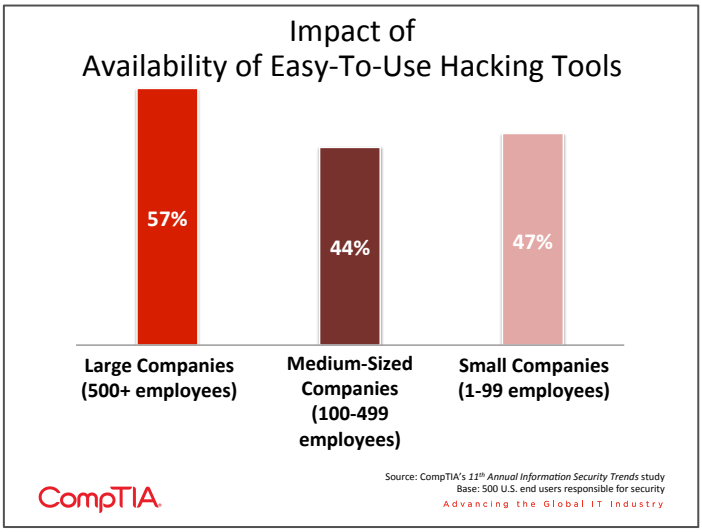
Advancing the Global IT Industry

Along with the use of DLP technologies, companies are planning to take a wide range of steps to help stanch the flow of data outside the organization. The most popular measures fall under the umbrella of mobility, such as stricter separation of business and personal activities (52%), encryption of files on mobile devices (46%), and implementation of two-step authentication (46%). Other common choices include creating or reinforcing company policy regarding social media (46%) and further compartmentalization of sensitive corporate data (33%).

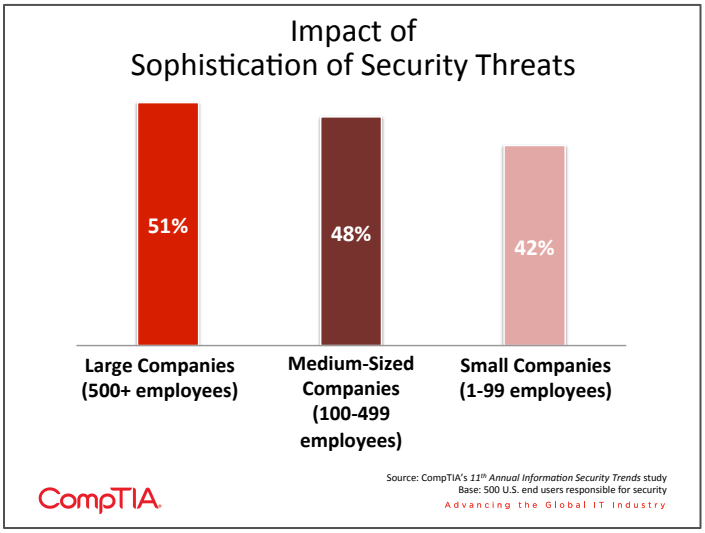
It is encouraging to see that small businesses appear just as likely to take these measures as larger enterprises. Studies have shown that attacks tend to be most concentrated among large businesses, where data has the highest value, and the smallest businesses, where the defenses are likely to be weak. SMBs should certainly not assume that they are unappealing targets, and they may have a major need to upgrade security tools or practices if they have made that assumption in the past.

Appendix

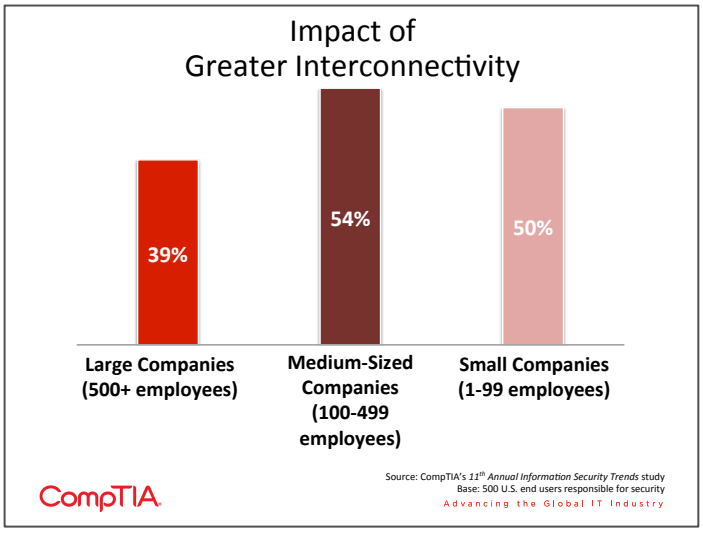
Viewing the impact of technology change across company size gives some insight as to how a solution provider might change their messaging in order to address concerns. For example, a greater share of large companies view the availability of easy-to-use hacking tools as a factor impacting security changes. Smaller companies may believe that these tools enable attackers to go after the bigger targets with more ease, when in fact they enable attackers to go after all targets, especially those with weaker defenses.



Similarly, large companies are more likely to be concerned about the sophistication of security threats. Here, there is a likely correlation to the ability to defend. Smaller companies may understand that threats are becoming more sophisticated but feel helpless to do anything. A solution provider with a broad range of expertise can provide value in this scenario.



Finally, there is a reversal when it comes to the greater interconnectivity of devices and users. Small and medium-sized companies are the ones most concerned here. This may again be a function of capability, or it could be that larger companies are more likely to dictate the devices their employees can use. Along with mobile security tools and techniques, general best practices in the area of mobility can help alleviate these concerns.



CompTIA

INFORMATION SECURITY TRENDS

SECTION 4: IT CHANNEL PERSPECTIVES

RESEARCH

ELEVENTH ANNUAL • NOVEMBER 2013

www.comptia.org

Key Points

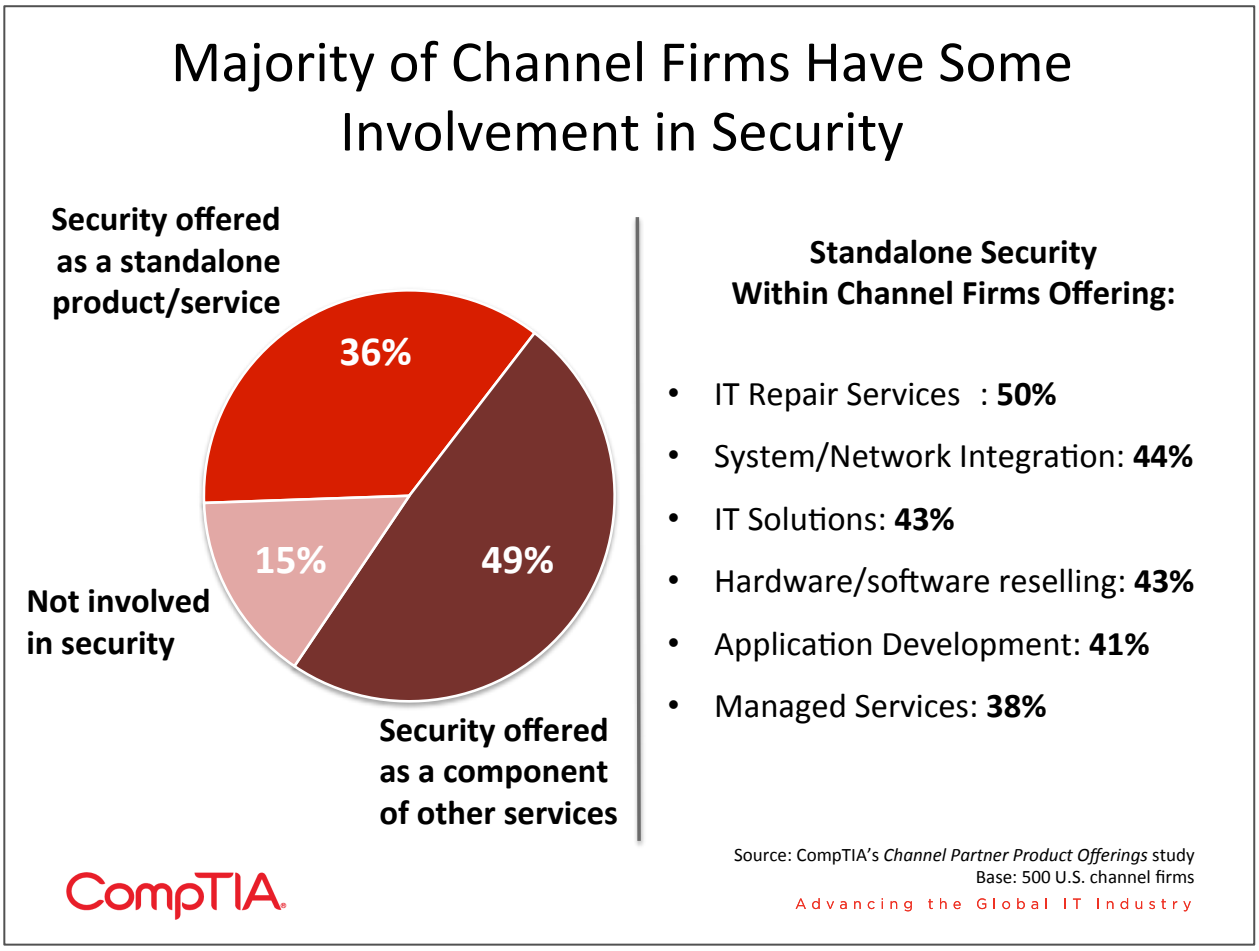
- Eighty-five percent of channel firms claim some involvement in security, but only 36% of all firms claim to offer security as a standalone product or service. With the complexity involved in covering the many facets of IT security, there is opportunity here for some firms to become a one-stop-shop for building robust security policies and postures.

- Although channel firms claim a broad spectrum of security offerings in their portfolios, the data suggests that feature listings by vendors or simple confusion are at play rather than a deep understanding of a range of security topics. Channel firms must ensure a thorough comprehension of the security landscape and may look to areas such as risk analysis or end user education if they are building out expanded security offerings.

- Seventy-eight percent of channel firms involved with security expect their revenue to grow in the next year, with 23% expecting significant growth (10% or more). Security as a service and managed security services have seen dramatic increases in usage over the past year, suggesting that creating recurring streams of revenue for security is not only possible but also profitable.

Security From the Channel Perspective

As with any enterprise technology, the IT channel has a prominent role to play in delivering vendors' security products to a wide audience and assisting end users with their security needs. Given the high priority that companies place on security, it is no surprise that 85% of IT channel firms have some involvement in the delivery of security products and services to customers. As with last year, most of these firms do not consider security a primary business, but instead have security embedded as a component of other offerings.



It is interesting to note that firms offering managed services are the least likely type of firm to have security as a standalone offering. Part of the appeal of managed services is that they are better able to handle the complexity of IT, and security is certainly becoming incredibly complex. On the same note, the smallest channel firms are the most likely to offer security as a standalone service. Without a large pool of resources, these firms are likely offering products or services focused on a specific area of security.

The notion of a one-stop-shop for security might be somewhat novel, but it could well have a place in the technology landscape of the future. CompTIA's previous research in the managed services space has found that 75% of end users contract with more than one firm for technology. Some firms will still choose to work with a single point of contact for all technology needs, but this is becoming a less

common model. Even in the cases where a firm works with a single point of contact, that primary firm may partner with other specialists to produce the overall solution.

While the breakdown by business model and company size indicate that channel firms may not be building themselves into overall security specialists, the range of services and products that are offered seem to tell a different story. Across 13 different security categories, channel firms report having related offerings in six out of ten cases (at a minimum). Such broad adoption would imply that many firms are well positioned to become a source for all security-related issues.

The numbers are somewhat suspect, though. For example, it is surprising to see that fewer firms claim to offer mobile security than security information and event management (SIEM). While mobile security is a somewhat new field, it has been a hot topic for at least the past year, and SIEM is considerably more complex.

Security Services/Products Offered by IT Firms

Security Product/Service	Currently Offering	Plan to Offer in Next Year
Email/web security	79%	12%
Network Security	77%	16%
Encryption solutions	73%	16%
Business continuity/Disaster recovery	72%	21%
Data protection	70%	23%
Security information and event management	68%	22%
Identity and access management	68%	20%
Intrusion prevention/detection	67%	20%
Mobile security	67%	19%
Compliance management	66%	24%
Risk management	66%	21%
Training/end user awareness	65%	22%
Cloud security	61%	28%

Source: CompTIA's *Channel Partner Product Offerings* study
Base: 350 U.S. channel firms involved in security

CompTIA
Advancing the Global IT Industry

The broad claims for security offerings could be based on several factors. For one, channel firms may be reselling or integrating vendor products that have these features, but they may not actually be digging into those features for their clients. This would explain why channel firms believe they are offering certain categories, but end users are not showing that those categories are being used. Another explanation is simple confusion or differences in interpretation. A channel firm may be classifying a

firewall as identity and access management rather than stating that they offer more recent IAM solutions.

Even if the numbers raise some questions, though, there are some takeaways that should prove useful for solution providers. The following areas were ranked the lowest among current offerings, but they are likely among the top issues that end users face as they work towards new security approaches:

- **Risk management:** Like security offerings for channel firms, many end users claim to be using some form of risk management but may not be performing the level of analysis that would lead to useful changes. End users that have performed such a detailed analysis have found that the nature of emerging threats or a move to new business models may create a need to further mitigate risk, while the use of new technology or potential business benefits may be valid reasons to accept more risk in the security strategy.

- **Training/end user awareness:** Human error accounts for 55% of root cause in security breaches, yet it ranks at the bottom of a list of threats that businesses are concerned about. This is partly due to the fact that companies cannot simply purchase technology to address the issue but instead must turn to education that is more interactive and ongoing in order to raise the general level of security awareness among employees.

- **Cloud security:** As discussed earlier in this report, cloud security is also less a matter of technology and more a matter of policy. As businesses change their overall operational model to take advantage of cloud infrastructure, the security practices for storing and using data will also change. Making these policy changes requires an understanding of cloud provider security practices to understand what the end user must do to create an end-to-end solution.

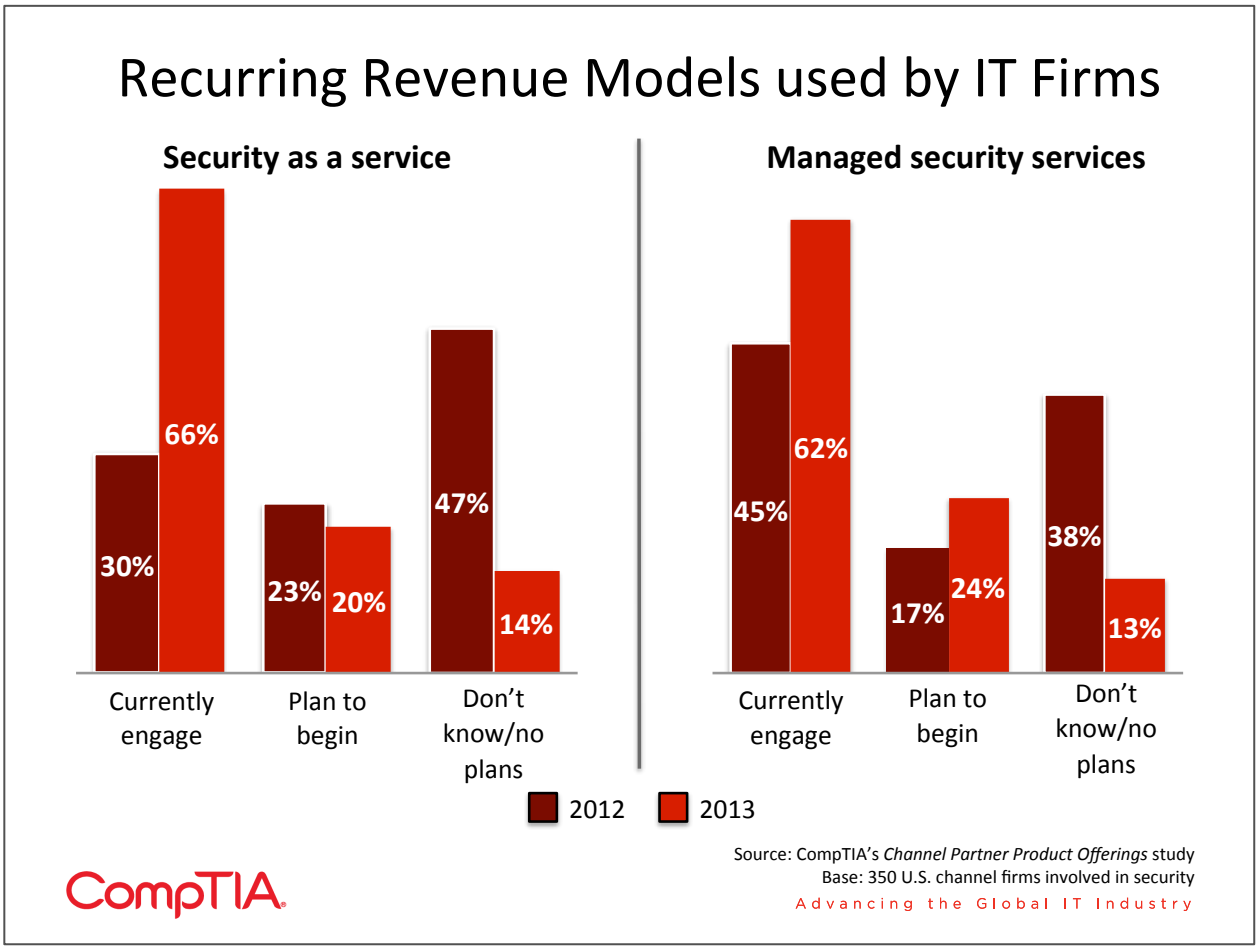
The Financial Side of Security

The continuing significance of security is also reflected in the fact that firms involved with security expect revenue growth over the next year. Seventy-eight percent of channel firms involved with security expect their revenue to grow in the next year, with 23% expecting significant growth (10% or more). Just 2% expect that security-related revenue will shrink over the next 12 months.

One of the goals for many channel firms is to create recurring revenue streams, and many firms are finding success in creating these streams with security offerings. The first way this is being done is through security as a service, or the use of cloud options for providing security functions such as antivirus or web proxies. Many end users are looking at these cloud options as a way of transitioning a security function to a company with more expertise while also getting more robust applications. Cloud security software benefits from a very wide range of patterns to analyze and the ability to update threat definitions without action from the end user.

The success of managed security services further suggests that this can be a viable model for providing value in a complex field. Similar to the cloud model, solution providers can offer greater expertise than a company might have in-house. In addition, a managed services model can address those aspects of security that are not handled by a piece of technology. Ongoing education would be a prime example, and MSPs considering this option should be careful to consider their own investments as they offer services, such as personnel who are well versed in training methodologies.

In general, security may not garner as much buzz as other IT trends such as cloud computing, mobility, and Big Data—but that does not make it less critical. Security is probably seen as table stakes when considering IT purchases, something that must be included for a purchase to be seriously considered. As digital data becomes increasingly important to businesses and the changing technology landscape drives new adoption, security must also be top of mind. As end users deal with new technology and seek improved security, channel firms can rise to the challenge and help manage this complex area.



www.comptia.org