CompTIA

INFORMATION SECURITY TRENDS

FULL REPORT

RESEARCH

NINTH ANNUAL • FEBRUARY 2012

www.comptia.org

About this Research

CompTIA's *9th Annual Information Security Trends* 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.
- Compare security practices, policies, threats, breaches, etc. between key developed and emerging markets.
- Gain insights into the security issues associated with emerging technology.
- Understand the role of security training and education.

The study consists of five sections, which can be viewed independently or together as chapters of a comprehensive report.

Section 1: Market Overview
Section 2: The Security Landscape – Threats and Challenges
Section 3: Emerging Trends
Section 4: Security Processes and Procedures
Section 5: The Role of Security Training and Certification

The data for this study was collected via a quantitative online survey conducted November 10 to December 19, 2011 to a sample of 1,183 IT and business executives directly involved in setting or executing information security policies and processes within their organizations. The countries covered in this study include: Brazil, India, Japan, South Africa, United Kingdom and the United States.

The enclosed material covers the U.S. portion of the results ONLY. The international results are presented in a separate report.

The margin of sampling error at 95% confidence for aggregate results is +/- 2.9 percentage points. For the U.S. segment of the survey, margin of sampling error is +/- 4.5 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 Ethics and Standards.

CompTIA

INFORMATION SECURITY TRENDS

SECTION 1: MARKET OVERVIEW

RESEARCH

NINTH ANNUAL • FEBRUARY 2012

Key Points

- As technology permeates every functional area of a business and more staff members assume the role of knowledge worker, organizations must contend with new security threats and vulnerabilities. As such, organizations continue to rate security a top strategic priority. CompTIA's *9th Annual Information Security* study found 7 in 10 organizations rating security as a high/upper level priority, compared to 49% in 2010.

- Reflecting concern over emerging threats, Investments in security products remains strong. Gartner forecasts global security services spending to reach $35.1 billion in 2011 and at least $49.1 billion in 2015. IDC forecasts are even higher, with a projection of worldwide security services market growth of 15% (CAGR) over the 2010 – 2015 time period. Revenues are expected to exceed $39.5 billion in 2011, growing to almost $63 billion by 2015.

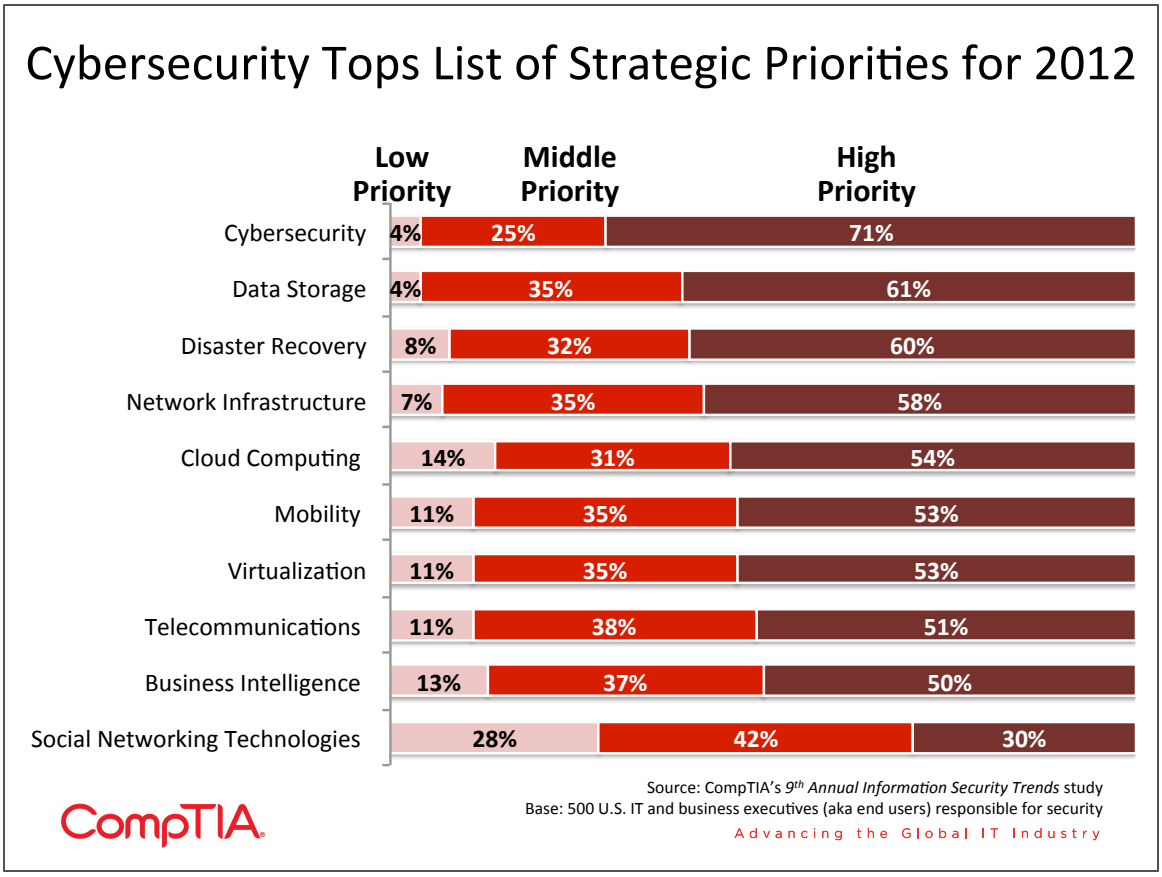
- The continued focus on information security has meant that it is one of the unique fields where demand for skilled workers exceeds supply. Surveys predict that security jobs will be in demand in 2012 and that there will be a lack of skilled personnel with specialized skills to staff these openings. CompTIA's *9th Annual Information Security Trends* study reinforces the difficulty faced in hiring skilled security personnel, finding 40% of organizations report facing challenges in hiring IT security specialists.

Prioritization of Information Security

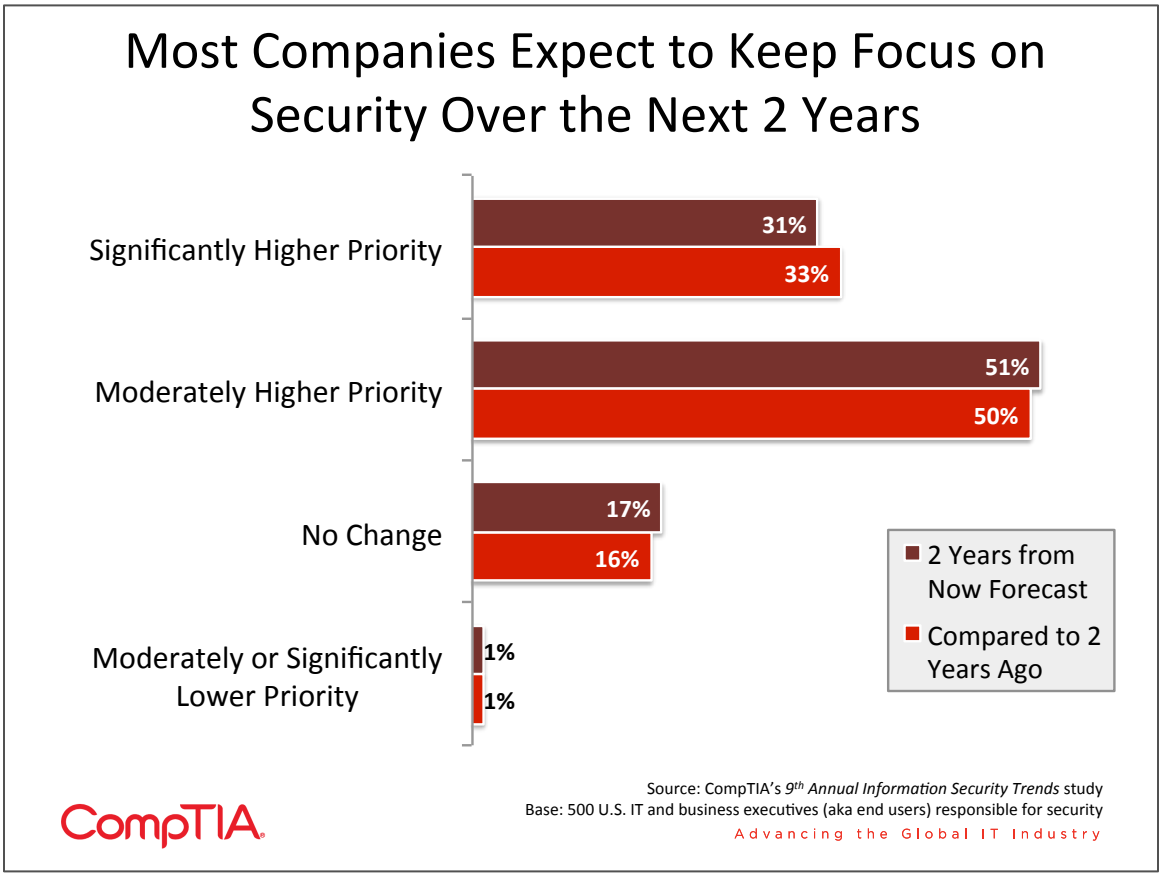
In an increasingly digital, interconnected world, cybersecurity affects more organizations on more levels than ever before. As technology permeates every functional area of a business and more staff members assume the role of knowledge worker, organizations must contend with an ever-shifting information security landscape.

At the same time, organizations must balance the need to allow workers the freedom to leverage the most powerful aspects of technology, such as mobility, information sharing and collaboration.

While much progress has been made over the years in securing networks and information, headline-grabbing stories of malicious viruses, data breaches, crime syndicate cyber attacks or lost laptops with thousands of sensitive customer records serve as a reminder that the next security breach is not a matter of "if" but "when."



The data indicates the prioritization of security is trending upwards when compared to findings from the previous iteration of the study (2010) where 49% rated information security as a high /upper level priority compared to the 71% who rate it as a high priority today. Similar to previous years, larger firms place a higher priority on security when compared to small or medium sized firms as they may have more access points or more sensitive data to protect. Information security is likely to continue to be a top tier area of interest as indicated by the chart below.



Spending on Information Security

The ongoing focus on security has translated to robust sales of security products and services. Consider the following:

- According to the research firm Gartner, worldwide security software sales reached about $16.5 billion in 2010, a 12% increase over 2009 revenue. The top 5 players in the space, Symantec, McAfee, Trend Micro, IBM and EMC, accounted for 44% of this market.
- Additionally, Gartner forecasts global security services spending to reach $35.1 billion in 2011 and at least $49.1 billion by 2015. The North American region is the largest market and is estimated to reach $19 billion by 2015.

- IDC forecasts are slightly higher, showing worldwide security services at 15% rate (CAGR) during the 2010 – 2015 time period. Revenues are expected to exceed $39.5 billion in 2011, growing to almost $63 billion by 2015.
- For the network component of the security market, consisting of hardware and software with functionality that includes firewalls, VPNs, intrusion prevention and detection, and multi-purpose security, IDC reported revenue totals of $8.2 billion in 2011, up over 8% from the previous year. The forecast anticipates software growing at a faster rate than hardware, with software-based solutions making up over 26% of the market by 2014.
- Infonetics expects the managed security services market to grow about 13% in 2011, and forecasts revenues to reach $16.8 billion in 2015, with the strongest growth coming from the SaaS (security-as-a-service) segment. Infonetics also expects the SaaS segment of the market to more than double between 2011 and 2015.
- Other emerging growth areas include security for cloud computing and virtualized environments, mobile devices, remote worker security and social networking security.

CompTIA's *9th Annual Information Security Trends* Study found that four out of five companies expect to increase their budgets for information technology. Gartner estimates that businesses spend on average 5% of their IT budget on security. The Strategic Security Survey conducted by Information Week Analytics found that similar to the previous year approximately 1 in 4 firms spend 10% or more of their IT budget on security.

Financial Cost of Cybersecurity Crime

From an ROI perspective, the resources devoted to security seem justified. A 2011 Norton Cybercrime Report put the cost of cybercrime at $114 billion annually. If lost time is factored in, the total cost is estimated to be $388 billion. Another study by HP, the Second Annual Cost of Cyber Crime Study, estimated that the median annualized cost of cybercrime incurred by a benchmark sample of organizations was $5.9 million per year, with a range of $1.5 million to $36.5 million each year per organization, an increase of 56% from data published in July 2010.

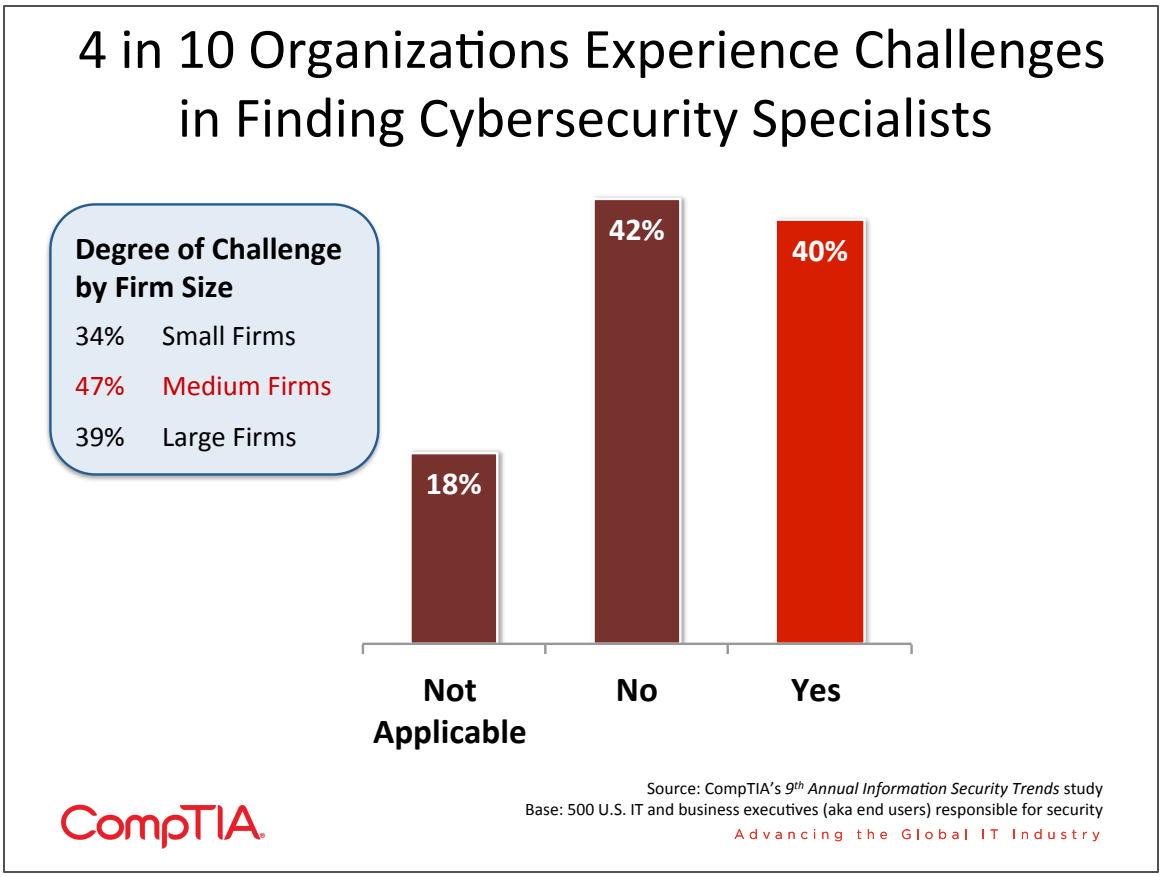
Cybersecurity and the IT Workforce

The continued focus on information security has meant that it is one of the unique fields where demand exceeds supply. The job board Dice.com shows a 79% increase in the total number of information security jobs posted on the site from September 2009 to September 2011. The Bureau of Labor Statistics instituted the category of information security analyst in 2011 and the number of those who consider themselves information security analysts stood at 43,000 for the period April-June 2011. This represents an increase of 16% over the previous quarter. Data from the BLS also noted that the unemployment rate was 0% for those employed in this category.

To put the very low unemployment among information security analysts in perspective, BLS data puts the unemployment rate for the overall IT occupation category at slightly under 4%, and the overall economy at 8.5%.

A survey conducted by the staffing agency Robert Half Technology predicted that security jobs would be in demand in 2012. The survey also noted the lack of skilled personnel with specialized skills to staff these openings. The importance of verifiable knowledge is highlighted by the increasing demand for certifications such as CISSP and CompTIA Security+.

CompTIA's *9th Annual Information Security Trends* study confirms the difficulty faced in hiring skilled security personnel. Forty percent of organizations report facing challenges in hiring IT security specialists.



CompTIA

INFORMATION SECURITY TRENDS

SECTION 2: THE SECURITY LANDSCAPE-THREATS AND CHALLENGES

RESEARCH

NINTH ANNUAL • FEBRUARY 2012

Key Points

- In 2011, 3 in 4 organizations reported firsthand experience with a security incident, a slight increase over the 2010 rate, according to CompTIA data. On average, organizations reported 7 incidents, with about half being classified as serious. It's not just the known incidents which concern companies though, but increasingly the "unknowns" – the undetected breaches or vulnerabilities that will inevitably cause harm. Seventy-three percent of organizations reported definitely or probably experiencing an undetected security breach.

- The all encompassing cybersecurity threat known as malware tops the list of concerns among IT and business executives involved with security. Malware disseminators continue to rely on a variety of tactics to bait their victims, such as emails, websites or texts with promises of celebrity photos or video. Spam filters, antivirus software and end user training goes a long way towards minimizing this risk, but unfortunately, these seemingly obvious ploys snare enough victims to keep them in use. In addition to malware, organizations expressed concern with hacking (e.g. DoS attack), data loss or leakage, social engineering (e.g. phishing) and vulnerabilities in emerging areas (e.g. cloud computing).

- Human error continues to be a significant factor in security breakdowns. A net 53% of IT and business executives say human error is more of a factor today compared to two years ago vs. 24% that say technology shortcomings are more of a contributing factor today. Respondents in this study pin the most blame on end users' failure to comply with the corporate security policy. Other factors though fall more on the shoulders of the IT staff responsible for safeguarding the organization – nearly half of respondents cite lack of expertise in securing websites and applications as a human error induced sourced of breaches.

Overview of Security Threats and Concerns

As noted in *Section 1* of this paper, cybersecurity rates as a top priority for organizations of all sizes. It is not hard to understand why – security incidents cost companies real money.

In 2011, 3 in 4 organizations reported firsthand experience with a security incident, a slight increase over the 2010 rate, according to CompTIA data. While few incidents rival the scale of a Sony breach (77 million compromised customer records), even a relatively minor security breach may lead to sizable costs, especially if it means repairing a damaged brand and having to win back customers.

It's not just the known incidents which concern companies though, but increasingly the "unknowns" – the undetected breaches or vulnerabilities that inevitably cause harm. Businesses detest uncertainty and security represents a variable that can be managed, but never fully controlled. Consequently, IT and business executives face tough decisions in determining the optimal allocation of resources to invest in security defenses. Similar to purchasing fire insurance, too little can be catastrophic, while too much can be a poor use of resources. For some organizations, it may be completely rational to invest in security defenses at one level, and yet, inappropriate for other organizations with a different risk profile.

Despite Best Efforts, Security Incidents Regularly Occur at Most Organizations

Organizations Catch Many Security Incidents, But Not All…

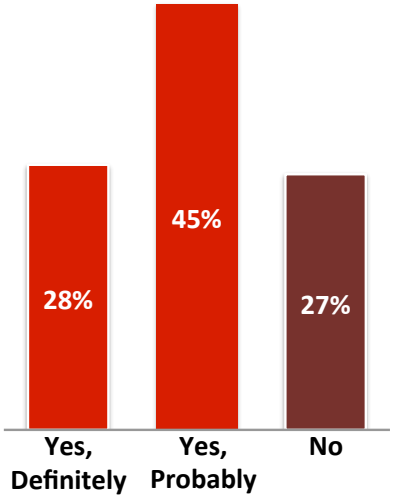
76% % of organizations that report experiencing a security incident in 2011

7 Mean # of incidents experienced

3 Median # of incidents experienced

Among organizations experiencing a security incident in 2011, on average, ***3.6*** of the incidents, or about half of the incidents experienced, were classified as ***serious***.

Likelihood of Experiencing an Undetected Security Incident

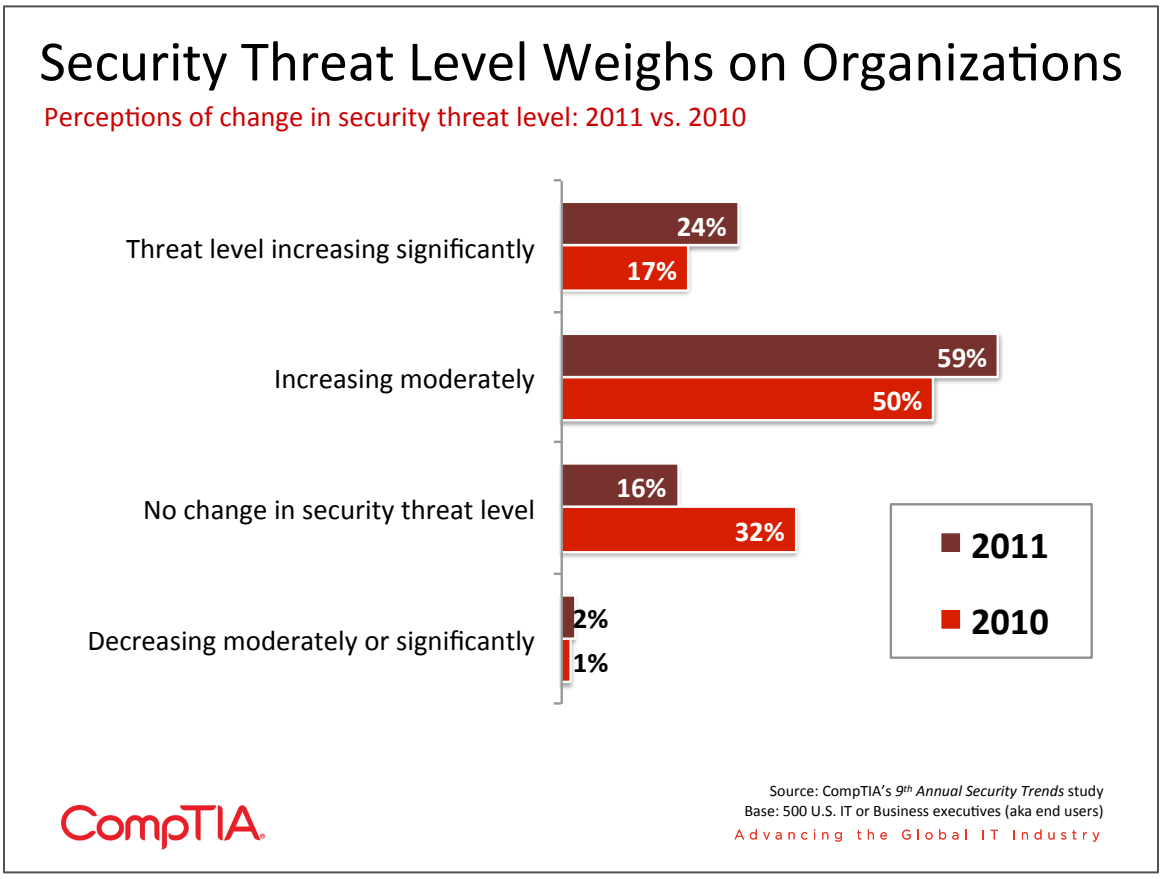


Source: CompTIA's *9th Annual Security Trends* study
Base: 500 U.S. IT or Business executives (aka end users)

Advancing the Global IT Industry

While security concerns keep many executives up at night, it's worth keeping in mind that it is not all bad news. Improvements in technology, policy and training have led to fewer vulnerabilities and better security defenses. The security vendor Symantec recently reported that it expects to see a 30% drop in the total number of software vulnerabilities disclosed to the public during 2011. Greater emphasis on security among a number of operating systems and platforms, such as Microsoft and Adobe, along with better cyber enforcement has contributed to this improvement.

Even with these incremental improvements, the security arms race continues. As a result, the vast majority of IT and business executives (83%) believe the security threat level is on the rise. CompTIA data suggests there is no single overriding factor, but rather a combination of elements that each chip away at information safety and security defenses in some way.



The all-encompassing security threat known as malware tops the list of concerns among organizations (see chart below). Given the sheer volume of known malware, such as viruses, Trojans, spyware, adware, worms and botnets, estimated by PandaLabs to exceed 73,000 new strains created daily in 2011, the number of security breaches could certainly be a lot worse. The economics still favor this "mass market" approach. With relatively low costs to create malware, combined with low distribution costs, it only takes a few victims to make a malware venture profitable. Nearly half of respondents in this study voice concern over accessible, easy to use malware and hacking tools that open the door to criminal behavior among a much larger pool of individuals.

According to PandaLabs, 75% of new malware strains in 2011 were Trojans – code designed to hide on a user's computer or mobile device and transmit information, such as a credit card number, back to its originators. Following Trojans in terms of frequency were viruses, worms, adware and then a few other minor categories.

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.)	33%	65%	40%	60%
Hacking (e.g. DoS attack, APT, etc.)	35%	57%	42%	58%
Data loss/leakage	34%	54%	53%	47%
Understanding security risks of emerging areas, i.e. cloud, mobile, social	42%	51%	45%	55%
Social engineering/Phishing	41%	46%	49%	51%
Intentional abuse by insiders, i.e. staff, contractors	38%	42%	62%	39%
Physical security threats (e.g. theft of a device)	41%	39%	64%	36%
Lack / inadequate enforcement of company security policy	45%	35%	68%	32%
Lack of budget/support for investing in security	42%	33%	63%	37%
Human error among end-users	55%	32%	68%	32%
Human error among IT staff	41%	31%	72%	28%

Source: CompTIA's *9th Annual Security Trends* study
Base: 500 U.S. IT or Business executives (aka end users)

CompTIA
Advancing the Global IT Industry

Malware disseminators continue to rely on a variety of tactics to bait their victims, such as emails, websites or texts with promises of celebrity photos or video. According to McAfee, the former model Heidi Klum ranked as the most dangerous celebrity in 2011. Searches for Klum resulted in a 1 in 10 chance of landing on a malicious site. Other notable events in 2011, such as Osama Bin Laden's death, the Royal wedding and the Japanese earthquake tragedy were also used to lure users to unwittingly infect their computer or mobile device with malware.

Spam filters, antivirus software and end user training goes a long way towards minimizing this risk, but unfortunately, these seemingly obvious ploys do snare enough victims to keep them in use. For CIOs and IT security firms, highlighting McAfee's *Most Dangerous Celebrities* list is a good way to bring attention to an often dry topic.

Top Level Domains with Highest Security Risk (Source: McAfee)

1. .Com
2. .Info
3. .VN (Vietnam)
4. .CM (Cameroon)
5. .AM (Armenia)

While malware represents the most pervasive threat, in some ways, malware attacks are less feared than the highly targeted distributed denial of service attacks (DDoS), advanced persistent threats (APT) and other types of malicious hacking attacks. Whereas malware originators typically release a virus, Trojan or drive-by web exploit without a specific target in mind, highly targeted hacking may entail a concerted effort to exploit a predetermined mark. This makes CIOs especially nervous.

Hacking groups such as Anonymous or LulzSec have unleashed cyberattacks against Sony, the CIA, News Corp., Visa and MasterCard, the Church of Scientology, the Egyptian government, just to mention a few. Moreover, evidence of state-sponsored cyberwarfare or cyberespionage is on the rise. Recently, hackers with ties to the Chinese military were fingered for using spear-phishing tactics to break into the computer systems of the U.S. Chamber of Commerce to steal information.

These philosophical, political, espionage or revenge-inspired activities have increasingly been categorized as hactivism. Fifty-eight percent of respondents in the CompTIA study believe hacking is a more critical threat today compared to two years ago. Concern is greatest among large companies (67% vs. 48% for small firms). It's not uncommon for small medium-size businesses (SMBs) to have the "we're too small to be a worthy target" mentality. While there may be some truth to this thinking, anticipating the motivations and capabilities of every hacker is an exercise in futility. Hackers may pass on larger targets, despite the potential for a score, in favor of easier hunting among SMBs with lower levels of security sophistication.

On the physical security front, skimming remains a dominant concern. It's beyond the realm of possibilities for many consumers to believe bank ATMs or POS payment systems could be vulnerable, which is exactly what cybercrimals count on.

In addition to malware and hacking, three other top tier security concerns of organizations include: data loss/leakage, social engineering and related threats, and emerging areas such as mobility or cloud computing. See *Section 3* of this report for detailed coverage of these topics.

Contributing Factors

Several macro trends provide context to the current and developing security landscape. Cisco estimates that by 2020 there will be 50 billion "things" connected via the Internet. IBM blows this forecast away by projecting 1 trillion Internet connected devices by 2015. These prognosticators expect an explosion of connectivity among the waves of "things" such as vehicles, appliances, machinery, buildings and other structures, materials, and even people that will eventually contain microchips and IP addresses. With each touch point comes the potential for new security vulnerabilities. Compared to the 2010 CompTIA study, respondents this year express more concern over the growing interconnectivity of devices and systems.

Another macro trend that continues to accelerate is the deepening reliance on the web. Software-as-a-service (SaaS), an element of cloud computing, is now the de facto standard for many applications. CompTIA's 2011 *Cloud Computing* study shows ever greater numbers of organizations moving on-premise IT infrastructure to the cloud. With smartphone adoption rates approaching 50%, along with the explosive growth of tablets, the mobile web has become pervasive. Combined, this reliance on the web requires different security strategies than the on premise models of old.

For SMBs especially, using outdated software is a big issue. For example, despite Microsoft's best efforts there are still users that cling to the 10-year-old IE6 web browser. Because of lack of IT sophistication, SMBs may also allow software licenses to lapse with the intent of saving a few dollars. Any minor short term gains could be quickly offset by a security incident due to not having access to patches and other software updates.

Factors Driving Cybersecurity Concerns

%	Concerns
51%	Greater interconnectivity of devices, systems, users
50%	More reliance on Internet-based applications, i.e. cloud computing, software-as-a-service
49%	Growing criminalization and organization of hackers motivated by financial gain
48%	Greater availability of easy-to-use hacking tools, allowing easier entre into hacking
46%	Rise of social networking
46%	Sophistication of security threats exceeding IT staff's expertise to thwart them
37%	Volume of security threats exceeding capacity to thwart them
37%	Consumerization of IT – greater use of consumer-oriented devices or applications
36%	Challenges in finding or training employees with security expertise
33%	Continued use of legacy operating systems, web browsers, etc.

Source: CompTIA's *9th Annual Security Trends* study
Base: 500 U.S. IT or Business executives (aka end users)

Advancing the Global IT Industry

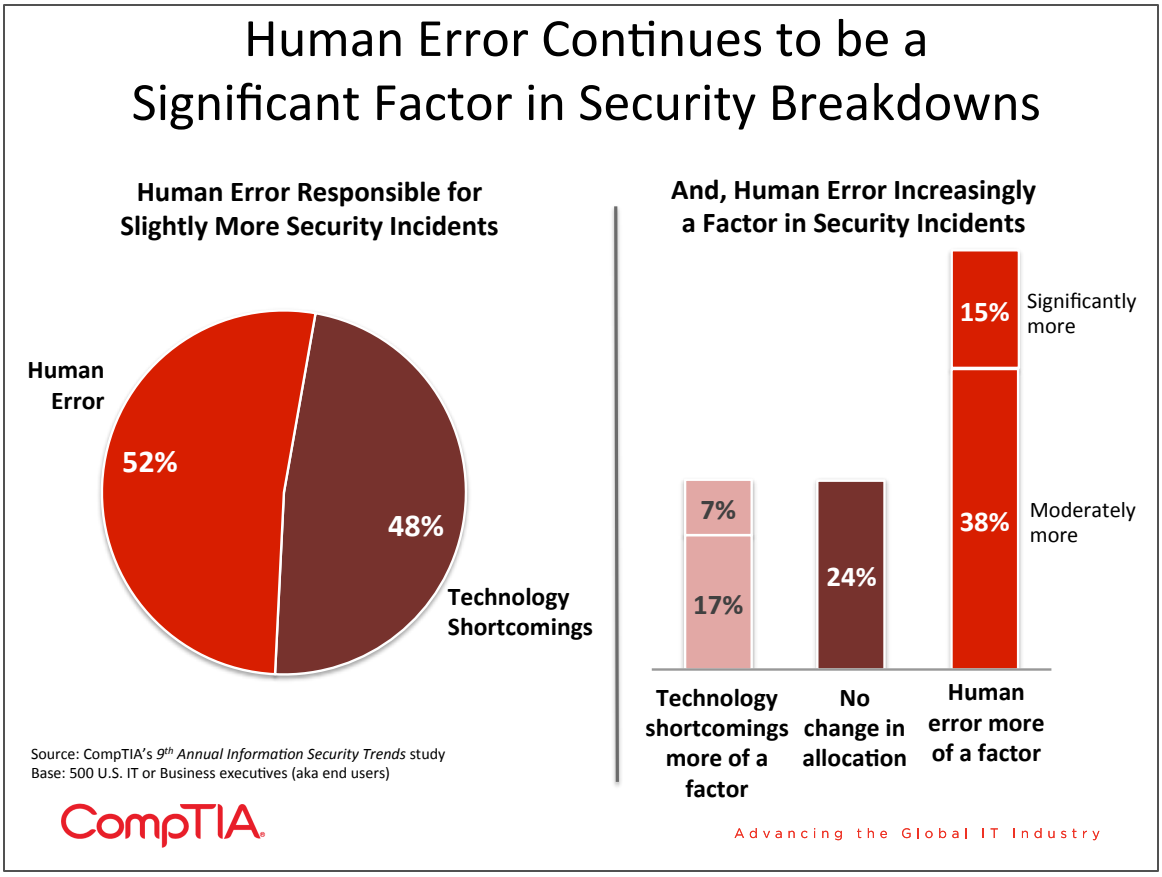
Human Error and Its Impact on Information Security

When asked to assign responsibility for recent security incidents, 52% of respondents in this study allocated blame to human error (down slightly from 59% in 2010) and 48% allocated blame to a technology shortcoming. Obviously, there is a murky middle area where human error and technology error intersect, making it difficult to accurately assign blame. For example, if a security application or appliance proves difficult to use, is it the fault of the technology vendor for an overly complex design or the fault of IT staff for not devoting enough time to figuring out how to use it properly? Probably some of both.

A net 53% of IT and business executives say human error is more of a factor today compared to two years ago vs. 24% that say technology shortcomings are more of a contributing factor today.

Relative to other security concerns (see chart on page 10), human error ranks as a lesser concern. About 1 in 3 rate end user error as a serious concern compared to 65% rating malware a serious concern. Reading between the lines though reveals an element of human error in just about every threat. Concern over social engineering, increasingly sophisticated cyberattacks, and keeping up with emerging areas such as the cloud or mobility, all involve employees and the decisions they make.

IT solution providers and security vendors selling only technology do customers a disservice. Without truly factoring in the human component, security defenses will always be inadequate.



Human error can typically be divided into two primary categories: 1) Failure to follow the rules, either intentionally or unintentionally, and 2) Failure to understand the rules and/or best practices. Both are a function of training and expertise – for more on this topic, see *Section 5* of this report.

Respondents in this study pin the most blame on end users' failure to comply with the corporate security policy. This may entail seemingly harmless activities such as spending time on Facebook, streaming music or video files or trying to catch up on work by transporting corporate files to a home computer via a flash drive to finish over the weekend. More serious violations of company policy may include intentionally circumnavigating safeguards, installing non-approved software or using non-approved devices.

As expected, organizations that experienced a high level of security incidents in 2011 report greater concern in areas such as lack of IT expertise with applications and networks. These types of organizations appear to be under invested in IT staffing, making them potentially ideal candidates for a managed security services relationship.

Sources of Human Error that Contributes to Security Breaches/Incidents

Human-Error Driven Security Concerns	Small Firms	Medium Firms	Large Firms	Few Security Incidents (<5)	Many Security Incidents (>11)
Failure of end-users to follow security procedures and policies	50%	55%	46%	53%	41%
Lack of security expertise with websites and applications	47%	50%	48%	38%	60%
Failure of IT staff to follow security procedures and policies	38%	35%	44%	33%	55%
Inadequate resources - not enough IT staff time to manage security threats	35%	32%	40%	33%	35%
Lack of security expertise with networks, servers and other infrastructure	35%	36%	33%	26%	51%
Failure of staff to get up to speed with new threats (e.g. mobility, social media, cloud, etc.)	30%	31%	40%	32%	37%
General negligence / carelessness towards security	39%	25%	35%	39%	24%
Intentional disabling of security (e.g. to download a non-approved application)	14%	14%	13%	15%	16%

Source: CompTIA's *9th Annual Information Security Trends* study
Base: 500 U.S. IT or Business executives (aka end users)

Advancing the Global IT Industry

CompTIA

INFORMATION SECURITY TRENDS

SECTION 3: EMERGING TRENDS

RESEARCH

NINTH ANNUAL • FEBRUARY 2012

www.comptia.org

Key Points

- With organizations producing more data than ever before, the threat of loss and leakage has increased as well. CompTIA research indicates slightly more than half of organizations knowingly experienced data loss/leakage. Among those experiencing a loss, sensitive corporate financial data was cited at the highest rate (65%). Data in motion (e.g. unencrypted email) generated the greatest concern, followed by data at rest.

- Social technologies have grown at a startling rate. Arguably, the security threat level hasn't been as severe as might be expected. That may change though. A net 87% of IT and business executives rate social engineering and phishing/spear phishing a serious or moderate security concern. A nearly equal number believe risks associated with social networking are on the rise.

- As organizations transition from low-risk, "test the waters" use of cloud computing to mission critical use, security will likely become a much bigger issue. CompTIA research reveals the strongest concerns around system downtime of cloud providers, data exposure during transfers between on-premise and cloud systems, the physical security of cloud data centers and data segregation in a multi-tenant environment. Despite the security concerns, only 29% of organizations report conducting a heavy review of their cloud service provider's security policies, procedures and capabilities.

- The numbers speak for themselves: 2011 was the first year where worldwide unit sales of mobile devices (wireless phones + tablets) eclipsed sales of PCs (desktops + laptops). And yet, few organizations have implemented what would be considered a comprehensive mobile security strategy. The most common safeguard is the use of passcodes – 76% of organizations require their use for corporate mobile devices. Other tactics, such as data encryption and remote data wiping capabilities, are employed by less than half of organizations.

Innovation: New Benefits, New Risks

The past few years have been an incredible period in innovation thanks to increasingly powerful and cheap computing, inexpensive mass storage, reasonably fast and reliable broadband speeds, new UIs such as touchscreens, new coding options such as HTML5, abundant APIs and greater know-how to put it all together.

Today, a lot of the technology used at the enterprise level mostly "just works."

On the whole, technology has never been more important to the success of the organization. Underlying any initiative involving the adoption of new technology is the need to strike the right balance between maximizing efficiency and effectiveness, and minimizing risks such as interoperability issues, cost over-runs and security breakdowns. As noted previously, 8 in 10 executives with security responsibility believe the security landscape is becoming more dangerous due to the increasing sophistication of attacks, new vulnerabilities and the rapid pace of innovation.

If organizations haven't already, they will soon be forced to contend with several disruptive information technology trends:

- Big data
- Social solutions
- Cloud computing
- Mobility

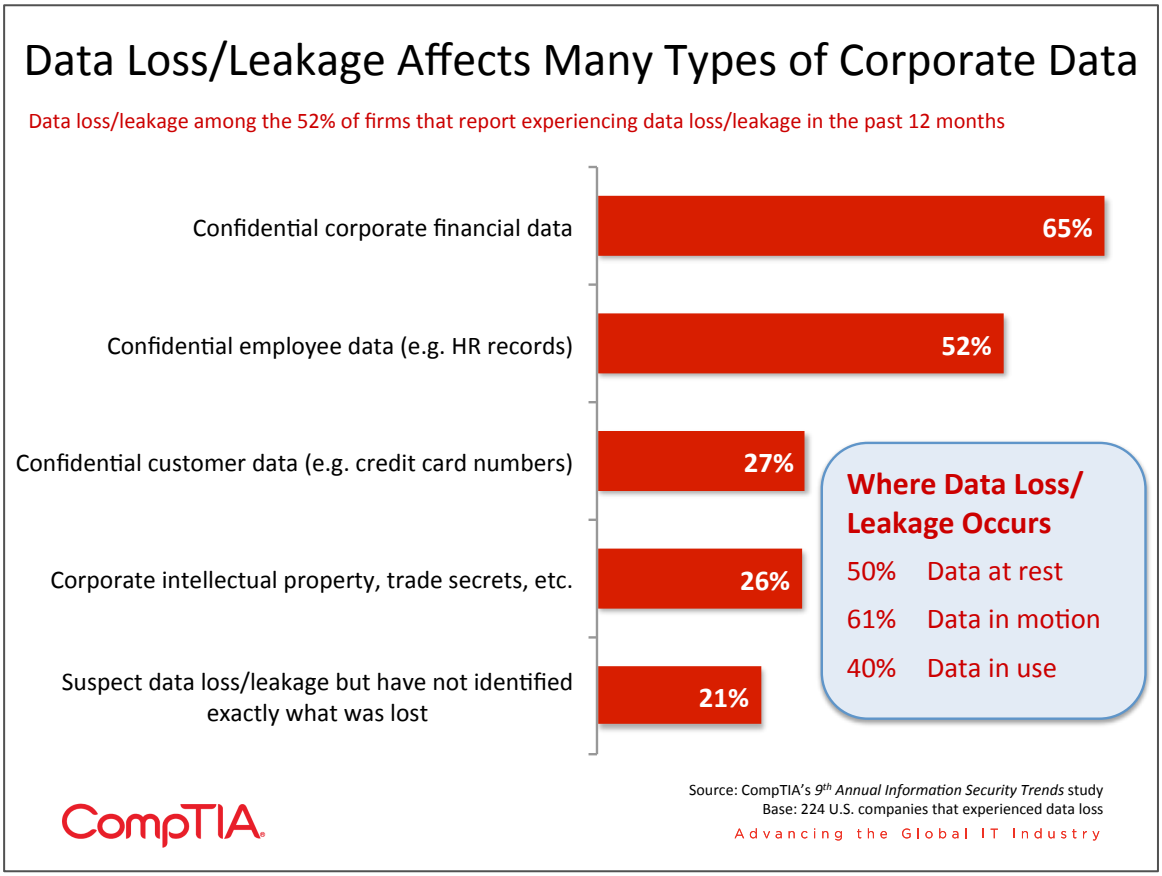
While each holds great promise for businesses of all types, the security risks cannot be overlooked.

Data, Data Everywhere

The barriers to creating, capturing and storing data have fallen to such low levels that many organizations are now swimming in structured and unstructured data. IDC estimates the global volume of data now doubles every two years and will total 1.8 zettabytes (1.8 trillion gigabytes) created and replicated in 2011. It wasn't that long ago when large data volumes were measured in terabytes and petabytes – those figures now seem almost quaint.

With more data being produced and touched by more people, the potential for data loss or leakage grows accordingly. CompTIA research found 1 in 5 organizations reported definitely experiencing sensitive data loss in the past 12 months, while 32% reported likely data loss. The remaining 48% of firms claim a perfect record of data protection, but do they really know for sure? Of course not, which is one of the most disconcerting aspects of data loss/leakage – companies may never know the extent to which they've been harmed by sensitive data falling into the wrong hands.

Among organizations experiencing data loss/leakage, the leading culprit appears to be data in motion. For example, sending information via unencrypted email, downloading or uploading unencrypted data to a website, transporting files via a USB Flash drive, or accessing the Internet via an unsecured WiFi network. Organizations feel slightly more confident in protecting data at rest and data in use, but the numbers still point to high levels of risk.



Organizations face a number of headwinds in addressing data loss/leakage. The rise of social networking has quickly instilled a mentality of "share first, ask questions later" among large segments of the population. It's unrealistic to think employees accustomed to freely sharing their life on Facebook and Twitter will refrain from mentioning work activities. Consider the recent example of the Microsoft employee who tweeted about an unreleased Nokia Windows phone. The employee thought the phone was cool and wanted to share the news, not thinking of the broad consequences or impact to the product release. The data leakage associated with this mental lapse was enough to cause the employee's dismissal.

Along those same lines, the blurring of work and home life has spurred the intermingling of company and personal devices and applications. Knowledge workers are under increasing pressure to be available 24/7, making it easy for them to justify using company property to catch up on personal tasks, or even allowing a spouse or children to use the faster work laptop over the weekend. Conversely, employees at some organizations have been ahead of the curve in adopting certain technologies (think adoption of a smartphone, while the rest of the enterprise uses basic BlackBerrys). This "bring you own device" (BYOD) trend has been another landmine for organizations seeking to balance operating performance, employee satisfaction and information security.

Lastly, the "consumerization of IT" has produced many benefits, such as a greater focus on the user experience and the freemium model. The downside, it may have taught some users to push back against anything perceived as unfriendly. For example, reluctance to embrace corporate policies governing passwords and login/logout procedures. Or, the unwillingness to forego the instant gratification associated with a quick and easy app download.

When data loss/leakage does occur, organizations respond in a number of ways. According to the CompTIA research, the top five responses include:

1. Implement encryption policies for data stored on mobile devices or portable media
2. Create a stricter separation of work and personal devices or communications
3. Reinforce or create acceptable use policies for mobile device
4. Reinforce or create corporate policies governing the sharing of proprietary information on blogs, forums, or social networks
5. Further compartmentalize sensitive corporate data to ensure only need-to-know employees have access

This study did not go into detail on the use of data loss protection (DLP) tools, but for IT solution providers offering security services, it should be a consideration. DLP tools, along with data activity monitoring (DAM), can help organizations discover, monitor and protect sensitive data. Realistically, a comprehensive DLP offering will be beyond the needs and reach of many small and medium-size businesses. A better starting point may be to help customers simply map the location of their data across all devices, databases and any other repositories. Inevitably, organizations will learn of data stored in a location where it shouldn't be – a good first step to framing the data loss protection discussion.

Social Networking Goes Corporate

After trailing the consumer market for some time, many businesses have finally embraced social technologies. Adding a "social" component has become de rigueur for just about any strategic, marketing or PR plan these days. The enormous user bases of the most prominent social networks, Facebook, LinkedIn and Twitter (800 million+, 100 million+ and 100 million+, respectively) could not be ignored. Tools with an enterprise focus, such as Yammer or Salesforce.com Chatter, positioned to enable and encourage cross-employee communication and collaboration, continue to gain momentum.

Despite the staggering growth in the use of social networking, one could make the case that the security risks associated with social have been relatively low. That will likely change though. There are two primary components of the risk: 1) Malware distributed via social networking platforms and 2) Social engineering facilitated by social engagement.

A few examples of the first category include:

- Viruses that infect users with luring messages such as "make money on Twitter," "get 1,000 Twitter followers," "someone commented on your Facebook post," or "someone posted your photo all over the Internet"
- Spam/Solicitations made via Skype or SMS
- Malware hidden in shortened URLs or corrupted apps
- Bots making unauthorized recommendations (aka like-jacking)

One of the biggest security issues related to social networking entails the high level of assumed trust among users. When an individual receives a message from someone in their network the default assumption is one of legitimacy. A scam that made the rounds awhile back involved a malware-induced posting to Facebook along the lines of "Help, I'm traveling abroad and lost my wallet. Please wire money." Seeing a post from a friend, however seemingly unbelievable, will cause most users to at least consider the possibility of it being true. "Social authentication" processes have yet to reliably address these situations.

Beyond obvious scams, the more insidious threat comes from the mining of data from social networks. Publicly available information in profiles, postings or Tweets may help hackers or identity thieves to discover all they need to know to inflict harm. Consider an example of an employee getting a call from someone pretending to be a co-worker in a satellite office. This person may try to build rapport by using information shared via social networking, such as mentioning the mutual attendance at a recent conference. Disarmed, the unsuspecting employee may share sensitive corporate information, or even worse, access credentials.

CompTIA research confirms this concern. Forty-six percent of respondents rated social engineering and phishing/spear phishing a serious security concern, while 41% rated it as a moderate concern. Additionally, 51% said they believe this threat is more critical today compared to 12 months ago.

For IT solution providers and vendors, the direct business opportunities associated with security and social networking are probably still minor since much of the risk is behavior related. Plenty of indirect opportunities exist though in helping organizations develop social media acceptable use policies or providing end user training, offered as part of a unified threat management (UTM) solution.

Security in the Cloud

Amazon, Dropbox and Epsilon all made the news in 2011 for security incidents involving their cloud services. CIOs contemplating "what if" scenarios got to see firsthand the results of a significant cloud outage, a password snafu leaving data exposed and the malicious hacking of a cloud service provider.

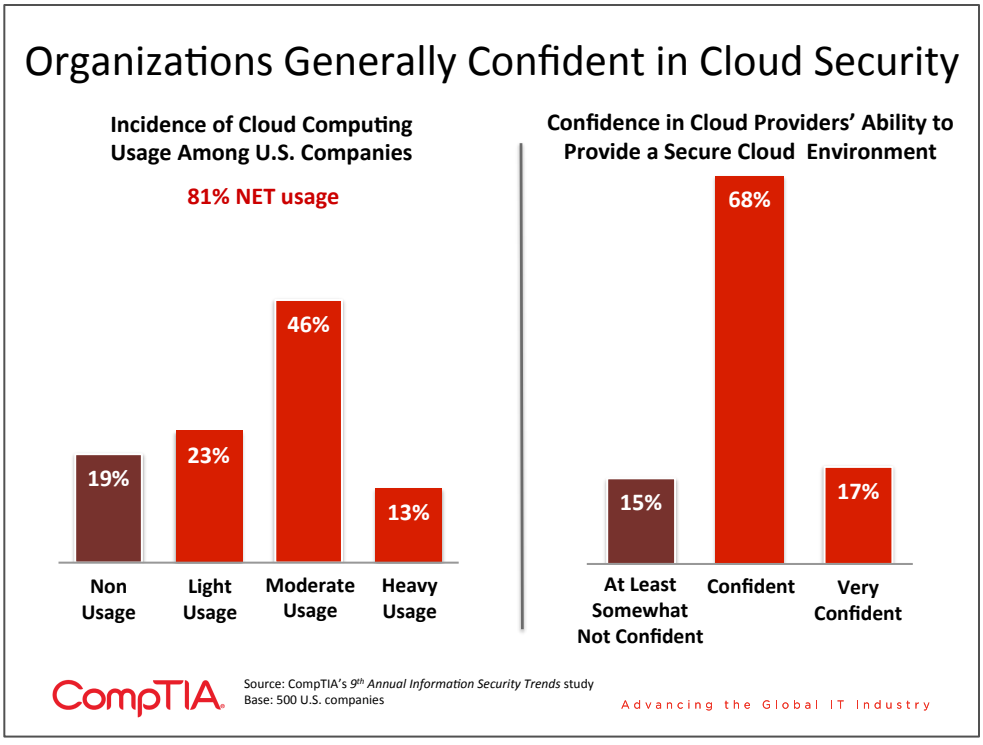
Not surprisingly, top of mind security concerns related to cloud computing tend to revolve around system outages and data loss. It's worth keeping mind that many organizations are still in the experimental stage with cloud computing and may not yet have considered certain risks.

Top 10 End User Concerns Related to Cloud Security

43% System downtime/business interruptions
40% Exposure or loss of data during file transfers to the cloud
39% Concerns over encryption of data (either transactional or at rest)
39% Physical security of cloud service provider data centers
36% Shared technology vulnerabilities (e.g. segregation of data in a multi-tenant environment)
35% Malicious activity from insiders or privileged administrators at cloud providers
32% Identifying/authenticating users
31% Difficulty in assessing and comparing the security of cloud service providers
28% Complying with legal/regulatory requirements

Other concerns mentioned include: ability to conduct audits/review logs, loss of control, vendor lock-in, lack of transparency with location of cloud data centers, and insecure APIs.

According to IDC, the combined public/private cloud security market will more than double over the next few years, accounting for nearly 14% of all security products sold worldwide by 2015, up from about 5.7% of the total market in 2010.



Despite the security concerns, most organizations report being confident or very confident (net 85%) in their cloud service provider. A few notable incidents not withstanding, this should be viewed as a testament to the quality of service offered by the major cloud providers and the support provided by IT solution providers.

All signs point to even greater levels of cloud adoption in 2012, but it could be some time before organizations use the cloud for the majority of their systems. According to the CompTIA research, large numbers of organizations have no intention of putting certain types of data or applications into the cloud. Topping the list includes things such as confidential financial data, credit card data and sensitive IP. For firms especially concerned about security, possibly due to the industry vertical they operate in, the likelihood to withhold certain types of data or applications is even more pronounced.

For IT solution providers and cloud service providers, this should serve as a reality check. Yes, the cloud is an important trend and will affect their business (see CompTIA *Channel Partner Trends* study for more details on this topic), but there will still be a need for robust on-premise and hybrid solutions for many years to come.

Even with High Confidence in Cloud Security, Many Firms Still Unwilling to Store Certain Types of Data There

Data companies are NOT yet willing to put in the cloud	Small Firms	Medium Firms	Large Firms	Security Rated a High Priority	Security Rated a Medium or Low Priority
Confidential company financial data	49%	55%	56%	58%	42%
Credit card data	50%	50%	53%	56%	37%
Employee HR files	45%	43%	44%	43%	47%
Confidential intellectual property / company trade secrets	41%	42%	44%	48%	30%
Customer contact information	30%	35%	25%	30%	28%
Data covered by regulations (e.g. HIPPA, PCI, Sarbanes-Oxley, etc.)	25%	26%	25%	26%	24%

Source: CompTIA's *9th Annual Information Security Trends* study
Base: 500 U.S companies

Advancing the Global IT Industry

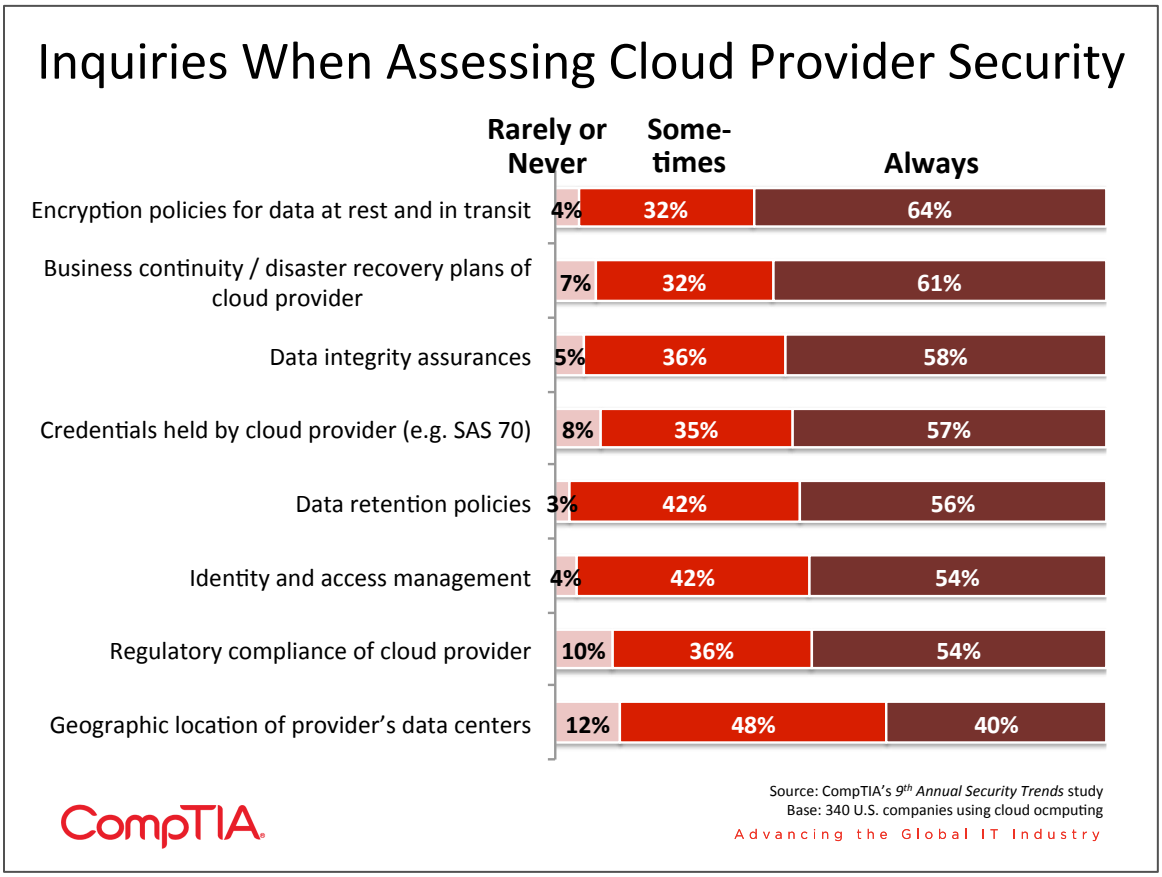
Taking a step back, organizations using the cloud are faced with a range of decisions: the model (public, private or hybrid cloud), service level (IaaS, PaaS or SaaS), the vendors or IT solution providers to hire and possibly the degree of cloud/on-premise integration. In addition to the basic evaluation metrics such as cost and performance, the data suggests most organizations include a review of the cloud service provider's security policies, procedures and capabilities.

Level of Review Conducted by End Users of Cloud Service Provider's Security Policies, Procedures and Capabilities

29% Heavy review
44% Moderate review
13% Little or no review
14% Depends – in some cases heavy review and in others light or moderate review

Security mavens probably view this as a "cup half full, half empty" situation. On the one hand, given the cloud model is still relatively new to many organizations, it's encouraging to see solid numbers of users evaluating their cloud provider in areas such as encryption policies and disaster recovery plans. On the other hand, many critical elements of the cloud security equation appear to be routinely overlooked, such as regulatory compliance, geolocation of data and the credentials of the provider.

SMBs in particular, with often lower levels of IT sophistication, may make the assumption that all aspects of security will be sufficiently handled by their cloud service provider, which may or may not be the case. This is confirmed by the data, where only 22% of small firms report engaging in a heavy review of their cloud service provider's security practices, compared to 41% for large firms.



Recently, the City of Los Angeles and Google learned the hard way what happens when an uncertain regulatory variable is introduced into a cloud deployment. LA had to alter its plan to shift 30,000 city employees to Google Apps when it was discovered Google Apps was not fully compliant with the FBI's security requirements for connecting to the Criminal Justice Information System (CJIS), a clearinghouse of law enforcement data administered by the Department of Justice.

This is one notable example of what is sure to be a more regular occurrence – organizations making the transition to the cloud only to discover a security related element that forces a change of plans. As the cloud model matures, some of these issues may naturally work themselves out, but in the shorter-term, IT solution providers and cloud vendors can provide a valuable service in reducing the likelihood of these types of situations. Longer term, third party assessments of cloud service provider security policies, procedures and capabilities may become standard.

A good resource for the types of security questions that should be considered when evaluating cloud service providers comes from the Cloud Security Alliance (CSA). This not-for-profit organization provides a useful list of over 200 questions covering data integrity, security architecture, audits, regulatory compliance, governance physical security, legal and more. The document can be accessed here: https://cloudsecurityalliance.org/research/cai/

Additionally, CSA publishes a top-level security roadmap for cloud operations, which can be found here: https://cloudsecurityalliance.org/research/security-guidance/

Mobility Continues to Disrupt

The numbers speak for themselves: 2011 was the first year where worldwide unit sales of mobile devices (wireless phones + tablets) eclipsed sales of PCs (desktops + laptops). By 2015, Gartner expects sales of mobile products to exceed 1.3 billion units (~1 billion smartphones + 326 million tablets).

The number of annual mobile app downloads is expected to hit 183 billion by 2015, up from only 10.7 billion in 2010 (source: IDC). While downloads tend to cluster around hits (think Angry Birds or the Facebook app), uses have a lot to choose from. The mobile app tracker, Mobilewalla, estimates there are currently about 1 million apps available across the Apple, Android, Blackberry and Windows platforms.

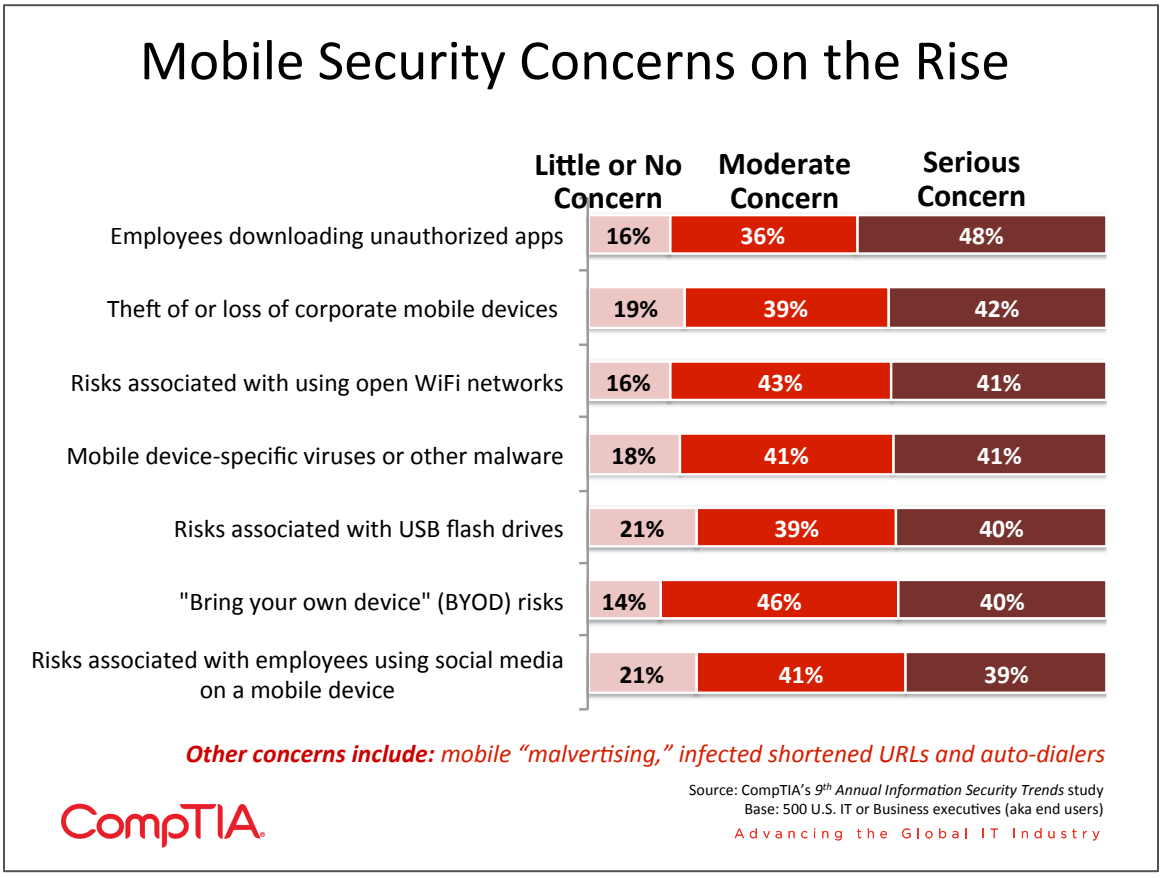
What does this all mean? From a security perspective, the bigger the target, the bigger the potential threat. The bad guys will go "where the money is." Similar to social media though, the numbers of mobile security incidents have been relatively small compared to size and staggering growth rates of mobile adoption. While there have been mobile viruses (e.g. the Geinimi botnet that targeted Android devices), malicious mobile apps (e.g. DroidDream) and plenty of social engineering scams that target mobile users, there hasn't yet been a singular event big enough and destructive enough to get everyone's attention.

That will likely change though. The odds seem to tilt towards a notable mobile security incident happening sooner rather than later.

CompTIA research has found that while organizations may not have specific security initiatives planned, security is still a top concern that must be addressed as other projects take place. As the critical nature of IT drives projects forward at a rapid pace, there are many strategies that are desirable for meeting business objectives but require modification of existing security practices or completely new security technologies.

Mobility is one of these areas that require an innovative approach to security. Global Industry Analysts predicts that the global market for mobile security will reach $14.4 billion by 2017. Results from the CompTIA mobility survey also indicate this to be a growing prospect: 70% of respondents who work in IT departments say that security of mobile devices is the largest risk to deal with when building a mobility strategy.

This concern over security would appear to be well founded. As employees are bringing their own smartphones and tablets into the workplace and driving IT departments away from the ability to mandate a single, approved device, the security of these consumer devices needs to be brought up to enterprise standards.



At this point, mobile malware is not one of the top security incidents experienced by IT departments, which seems about consistent with the threat level to date. The most common security incident is a lost device, which has been experienced by 56% of organizations in the survey. The next most common incident was a violation of company policy regarding corporate data (25%), an emerging factor in data loss as noted earlier in this report.

While device theft or loss is still a major concern, downloading unauthorized applications rates as the top mobile security concern. A few factors contribute to this concern. One, many organizations allow end users free reign to download and manage apps on their mobile device. In a "bring your own device" (BYOD) environment, this practice is often the norm. In terms of user perceptions of apps, the default position for many is one of "if it's in the app store, it must be safe."

Secondly, while each of the major mobile OS platforms have procedures in place to screen apps, the process is not 100% fail safe. Google reportedly removed more than 60 malicious apps from its Android app store in 2011. Situations that are especially dangerous involve approved safe apps that are then hijacked and made to inflict harm.

In response to these threats, IT departments take a number of actions. CompTIA research found 76% of organizations with staff using mobile devices mandate passcodes to unlock the phone or tablet. This is a good first step as long as users avoid being too obvious. Researcher Daniel Amitay of Big Brother Camera Security analyzed over 250,000 passcodes and found that 14.4% of passcodes involve 10 combinations, with '1234,' '0000,' '2580,' and '1111' the most common pin choices.

Mobile Security Strategies in Use

76% Passcodes
40% Encryption of data on the device
33% Requiring the OS and apps are up to date with patches, etc.
26% Disallowing "jailbreaking" of the OS
25% Use of a service for tracking and/or wiping a lost device

Outside of passcodes, few organizations have implemented what would be considered a comprehensive mobile security strategy.

As IT departments strive to secure corporate data and end users push for strategies that help increase productivity and convenience, it will be challenging to find solutions that please all parties. Many businesses feel that they are currently striking a good balance (44%), but clearly this is an issue that requires collaboration between those trying to set security policy and those trying to get the most use out of mobile devices.

Position of Organizations on Balancing Mobile Security Needs vs. Worker Needs

44% Strike the right balance between mobile security and the needs of workers
39% Lean towards managing mobile security risks at the expense of worker needs
14% Lean towards worker mobility needs at the expense of managing security risks
3% Don't know

For IT solution providers and vendors, mobility represents a significant business opportunity, but it is not without challenges. Clearly there is a need among end users to better understand best practices in mobile device management. The data suggests end users have a reasonably solid grasp of mobile security threats, but unfortunately, that alone is often not enough to spur firms to automatically increase their investment in products or services to bolster their defenses.

Along with mobility, many customers are also working to grasp the implications of cloud computing, big data, social networking, unified communications, business process automation and a host of other technology-driven changes that may affect them. IT solution providers and vendors most willing to embrace the Trusted Advisor role, which may mean sacrificing short-term gains in favor of a long-term relationship, will be best positioned to succeed.

For mobile security, this translates to helping customers understand their current and future needs in the areas of:

- Mobile Device Management (MDM)
- Mobile Security Software
- Cloud Syncing Services
- Mobile Virtualization
- Curated App Stores

CompTIA

INFORMATION SECURITY TRENDS

SECTION 4: SECURITY PROCESSES AND PROCEDURES

RESEARCH

NINTH ANNUAL • FEBRUARY 2012

www.comptia.org

Key Points

- Three quarters of organizations report having a written security policy in place. This is significantly more than the 55% who reported having a written policy in place in 2010, a positive sign more organizations have embraced a multi-pronged security strategy. Organizations that place a high priority on security are more likely to have a written policy in place than those where security is a medium or low priority (80% vs. 63%). Additionally, organizations that have confidence in their defenses are more likely to have a written policy in place.

- Companies need to train employees and enforce the implementation of security policies. Data from this study indicates that the main reason for a security breach attributed to human error was the failure of end-users to follow security procedures and policies, with 50% of the respondents rating it as a contributing factor. Formalizing security policies that address threats resulting from the increasing mix of personal and business technologies (i.e. smartphones and social networks) and adequately training employees to follow these policies can significantly reduce the likelihood of security breaches.

- Multi-department involvement in formulating security policies is especially true for larger organizations with 82% of large companies noting that security policy formulation is a joint effort, compared to 65% of small companies who said it was a joint effort. In companies where security is a high priority, business and IT teams work together to formulate a policy.

- Most firms report tracking security effectiveness in some way. Fifty -five percent say that they use security metrics aligned with business objectives and 13% say their metrics are technical in nature.

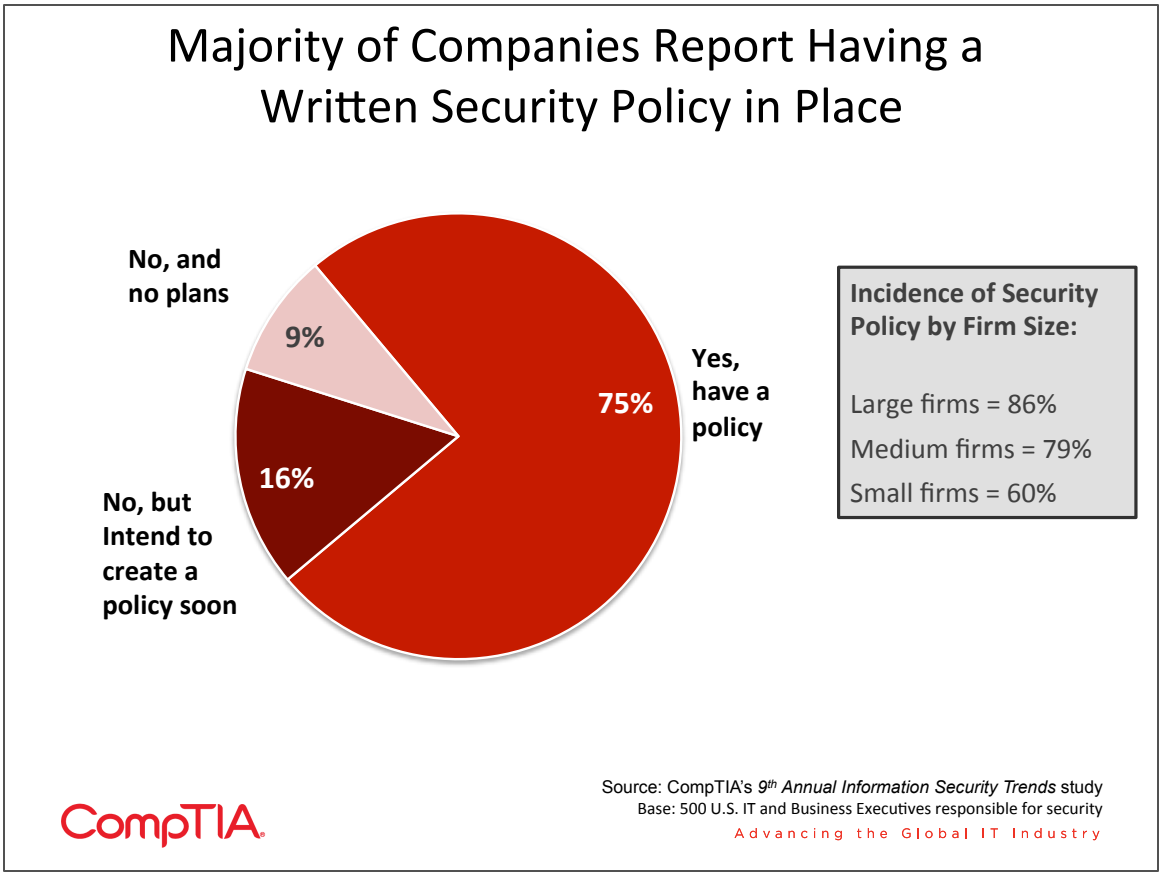
The Role of Corporate Security Policies

In response to widespread cybersecurity threats, as detailed in *Sections 2 and 3* of this report, organizations employ a number of safeguards. The standard second pillar of defenses is the corporate security policy. In addition to the direct benefits to the organization, security policies provide indirect benefits in demonstrating due diligence to customers, shareholders, regulators and other stakeholders. Well thought out and executed policies and procedures convey to outsiders a structured and proactive approach to security – an important element of damage control should a breach occur.

Data from CompTIA's *9th Annual Information Security Trends* study shows that three quarters of organizations report having a written security policy in place. This is significantly more than the 55% who reported having a written policy in place in 2010, a positive sign more organizations have embraced a multi-pronged security strategy.

This study did not go into detail on the specifics of those with policies, but it's assumed they range from basic to extensive. Some respondents likely see the employee manual, which may contain an acceptable use policy covering company property, doubling as a security policy. This may explain some of the variance in security policy rates, such as the lower incidence reported by Symantec among SMBs.

Not surprisingly, organizations that place a high priority on security are more likely to have a written policy in place than those where security is a medium or low priority (80% vs. 63%). Additionally, organizations that have confidence in their defenses are more likely to have a written policy in place.



Companies do not just need to proactively develop policies to secure information and those dealing with it but also need to train employees and enforce the implementation of security policies. Data from this study indicates that the main reason for a security breach attributed to human error was the failure of end-users to follow security procedures and policies, with 50% of the respondents rating it as a contributing factor. Thirty-nine percent of respondents point to the failure of IT staff to follow established security protocols as the reason for a security breach caused by human error.

A survey of 990 end users conducted by the security firm Avira reiterated this concern and showed that 35% do not consider it important to follow security policies and 26% believe that security is the IT department/system administrator's concern. Despite the publicity that security breaches get, many employees are often too engrossed in their jobs and deadlines to remember policies.

There is also the fact that most companies provide an overview of policies when an employee is hired and is deluged by a lot of information on policies and procedures and is unlikely to retain the information on a specific policy for later use.

Moreover, formalizing security policies that address threats resulting from the increasing mix of personal and business technologies (i.e. smartphones and social networks) and adequately training employees to follow these policies can significantly reduce the likelihood of security breaches. A corporate information security policy ensures confidentiality, integrity and availability of data in an environment where physical boundaries hardly matter and information is increasingly digitized. Given that the data from this study shows that human error is a significant contributor to security breaches, the importance of a policy framework cannot be underestimated.

IT solution providers and vendors that overlook the policy and training/education element of their security offerings run the risk of stopping short of a fully satisfied customer. Not to mention, the missed business opportunities and loyalty associated with a long-term trusted advisor relationship.

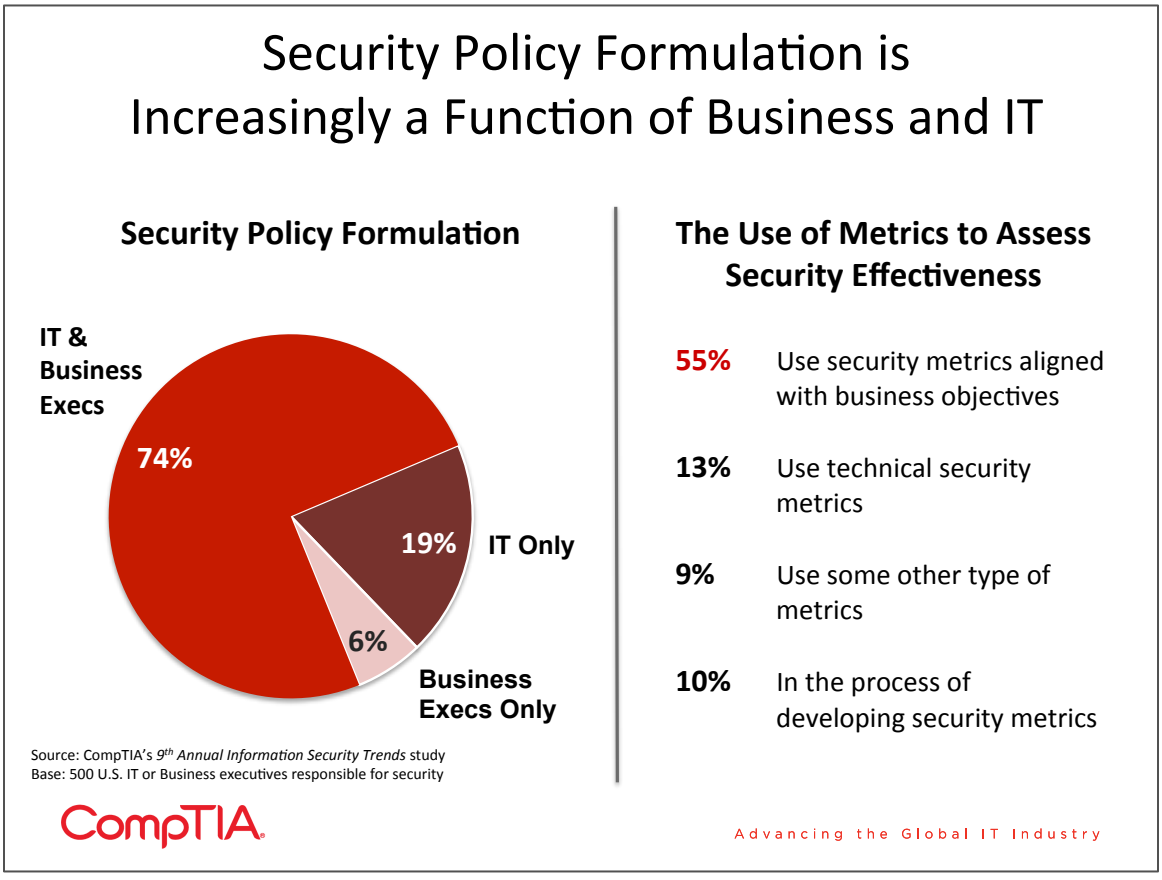
Security Policy Elements

Increasingly, information security is viewed as more than just an IT issue, but rather a business issue, requiring alignment with the strategic direction of the company. This approach can be seen in how corporate security policies are now formulated. The data indicates significant collaboration between IT and business executives in developing corporate security policies.

Multi-department involvement is especially true for larger organizations with 82% of large companies noting that security policy formulation is a joint effort, compared to 65% of small companies who said it was a joint effort. It stands to reason that in a greater proportion of companies where security is a high priority, business and IT teams work together to formulate a policy. The 2011 Strategic Security Survey conducted by Information Week also found growing involvement of business executives in the formulation of security policy.

Business executive involvement in security policy formulation is especially critical in the areas of regulatory compliance and establishing a clear disciplinary pathway for policy violations.

To be effective a security policy needs to be understandable, realistic, consistent, enforceable, communicated effectively, reviewed at regular intervals and flexible. CompTIA data shows that companies try to strike the balance between managing risks and meeting the needs of workers. For example, for mobile devices, 44% of companies believe they have struck the right balance when it comes to mobility needs of employees and the security requirements of the enterprise.



The SANS Institute, a cooperative research and education organization, provides a number of useful security policy templates and examples:
http://www.sans.org/security-resources/policies/

Including emerging areas, such as:
Mobile Security Policy: http://www.sans.org/security-resources/policies/mobile.php

Assessing the Effectiveness of Security Safeguards and Strategies

The adage, "If you can not measure it, you can not improve it," is a concept the savviest of organizations take to heart. As noted in the previous chart, most firms report tracking security effectiveness in some way. From an IT department perspective, metrics may help make the case for additional investments in security when competing for scarce budget dollars. From the perspective of business executives, metrics may help to provide insight into the risk profile of the organization and better enable leaders to fulfill their governance duties. On the ROI front, metrics guide decisions in how to allocate resources in the areas of security technology, policy and training.

At the most basic level, security metrics may start with reporting from anti-virus software, such as the number of malware threats caught, quarantined or cleaned. This type of data is technical in nature and according to CompTIA research, 13% of organizations rely primarily on this assessment of security effectiveness.

Because security has become much more complex than simply defending the perimeter via anti-virus software, many organizations require a broader set of measures. Some examples include:

- IT staff response time to security incidents
- System downtime due to security incidents
- Monetary value of loss of staff time or productivity due to security incidents
- Time between release of patches and installation
- Number of helpdesk tickets that are security related
- Number of IT staff and end users that have completed security training
- Number of holes or vulnerabilities identified by penetration testing
- Number of phishing emails that get through anti-spam efforts
- Count of number of sensitive data files found on computers or servers where they shouldn't be
- Number of data loss incidents occurring from staff sharing via social media

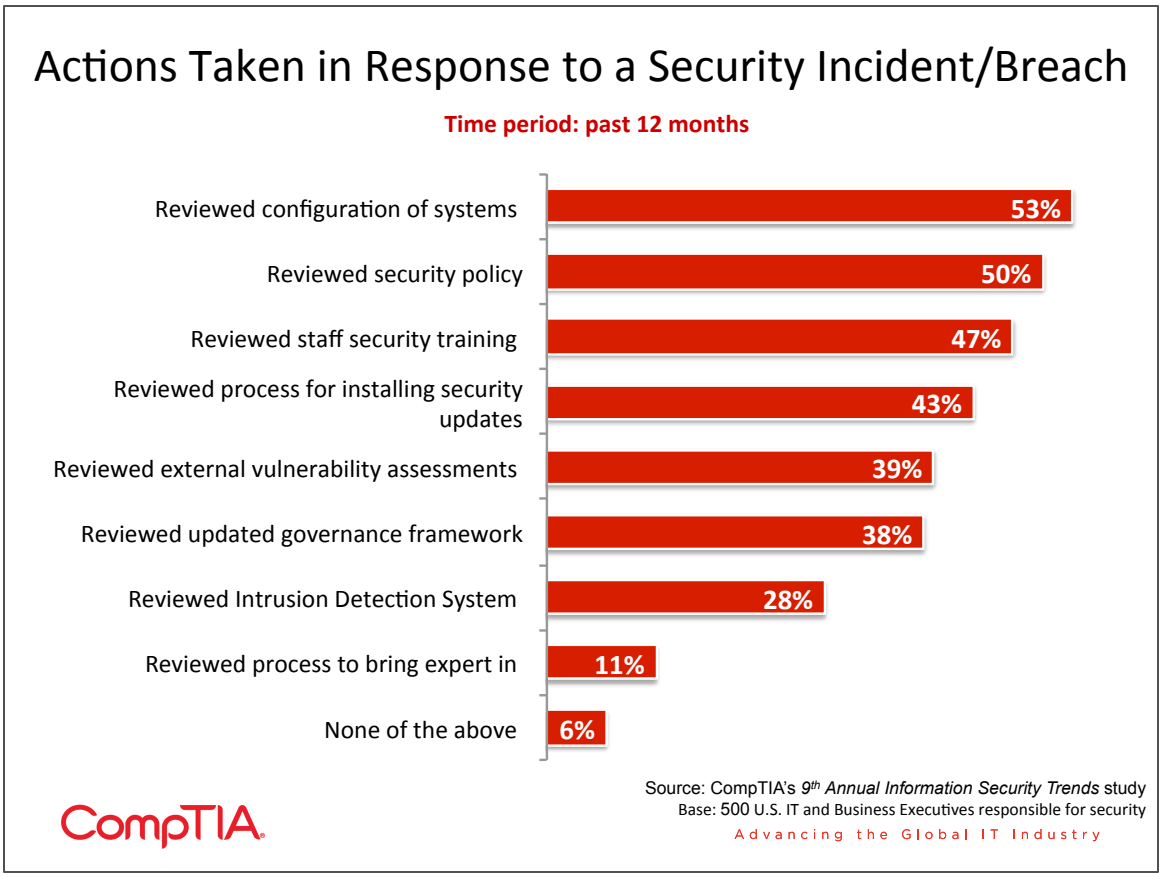
Among the 55% of organizations with security metrics aligned with business objectives, only 28% report the metrics on a regular basis, such as quarterly or annually. This implies that while many organizations claim to have a system in place for tracking security metrics, a portion of these firms are doing so on an ad hoc basis, which limits the value of being able to connect security metrics to business objectives and/or acting on the metrics.

Data from the 9th Annual Information Security Trends Study also shows that organizations with a formal, written security policy are more likely to value training and follow more formal processes of certification when compared to those that don't have a formal policy.

Drivers of Corporate Security Policy Changes

Improvements to a security policy are largely reactive and are often a response to a breach experienced internally (30%), because of an incident that has happened elsewhere (41%) or to comply with regulations (37%). Other reasons that motivate changes are recommendations from a security consultant (40%) and vulnerabilities discovered by outside parties (29%). The input of security consultants is more of a factor in large and medium sized organizations.

Some of the actions taken in response to incidents or proactively are listed in the chart below. Large organizations are more likely to have undertaken reviews of systems, servers and firewalls and updated staff training when compared to small and medium sized enterprises. Not surprisingly organizations where security is a priority have taken more of these actions when compared to those who rate security as a medium/low priority.



One example of organizations refining their security policy in response to risks stems from the protracted and deep recession. According to CompTIA data from 2010, 34% of U.S. businesses believed the internal security threat at their organization increased as a result of the difficult economic times. Layoffs, low morale and desperation may lead otherwise honest employees to cross the line. The greatest concern came from departing employees having knowledge of logins, access points and other vulnerabilities (35%), followed by the risk to proprietary data, code or other intellectual property (29%). More than half of organizations updated (29%) or planned to update (30%) to their security policy in response to that issue. Even though the data was collected in 2010, the risk is just as prevalent today.

CompTIA

INFORMATION SECURITY TRENDS

SECTION 5: THE ROLE OF SECURITY TRAINING AND CERTIFICATION

RESEARCH

NINTH ANNUAL • FEBRUARY 2012

Key Points

- Regardless of how the information security landscape changes, the human factor remains the one constant factor. CompTIA's data found that 41% of organizations report moderate or significant deficiencies in security expertise among their IT staff. Concern is especially high with insufficient security expertise as it relates to websites and applications. Networks, servers and other infrastructure are mentioned as well, but at a slightly lower rate.

- CompTIA's research indicates about 40% of professionals developed their skills primarily through experience, while 23% relied heavily on formal training/education. The middle 36% cited both equally. Among those with deficiencies in some area of security, the greatest number of respondents believe more training/education is needed to address the shortcomings. Smaller firms appear to have a stronger need for formal training/education than larger firms (58% vs. 39%).

- On average, organizations report being about 30% short of headcount devoted to security. Unfortunately, in the real world of "do more with less," most companies are forced to operate at less than optimal staffing levels. Hiring intent for security professionals is on the rise, as 46% of organizations signal their intent to hire security specialists over the next two years. This could be challenging though given the experience of those that have already attempted to hire security specialists.

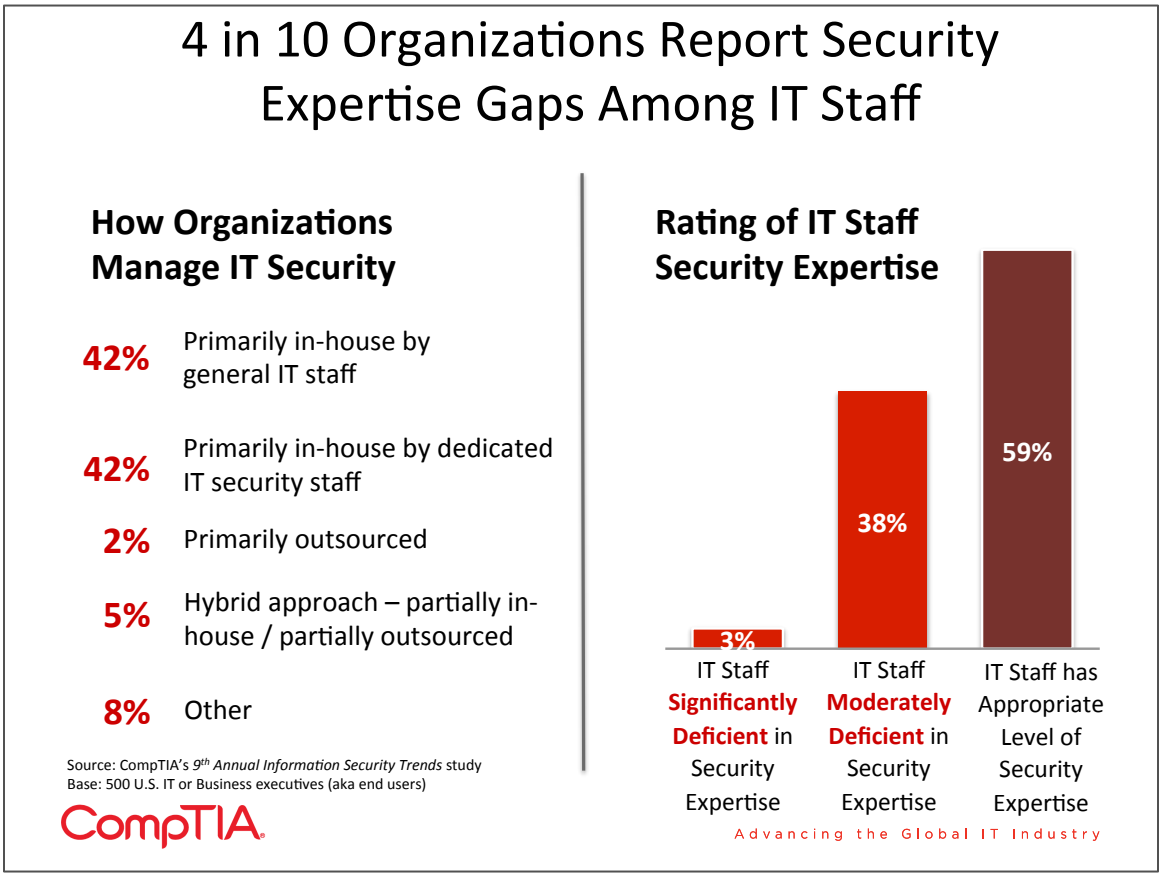
- More than 8 in 10 organizations formally or informally use security certifications as a means to validate expertise. Organizations view certified staff as an integral part of their security apparatus. The validation provided by certification is evident by the high level of agreement to certified staff being more valuable to the organization, having proven expertise and the belief that the organization is more secure because of the presence of certified staff

Assessment of IT Staff

Regardless of how the information security landscape changes, one constant will always remain – the human factor. As covered in *Section 2* of this report, organizations cite poor decisions by staff as a contributing factor in many security incidents. Some of these poor decisions stem from the failure to follow company security policies, but others are a direct result of insufficient training.

According to the CompTIA data, 41% of organizations report moderate or significant deficiencies in security expertise among their IT staff. Concern is especially high with insufficient security expertise as it relates to websites and applications. Networks, servers and other infrastructure are mentioned as well, but at a slightly lower rate.

Interestingly, smaller firms rate their IT staffs' level of expertise with security at about the same rates as larger firms (64% of large firms rate their IT staff as having the appropriate level of expertise vs. 55% for small firms).

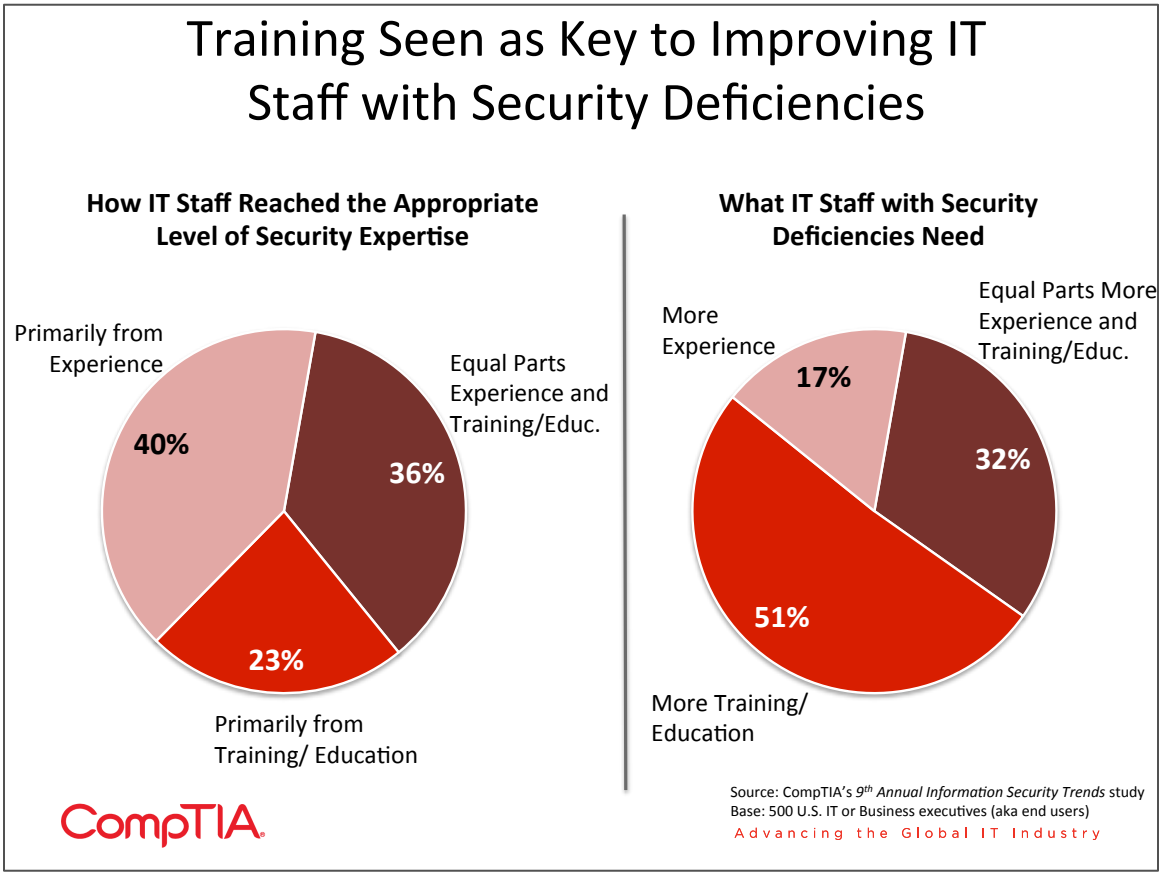


Improving Security Expertise

The debate between the role of experience and the role of education in short and long-term performance is probably as old as the workplace and schools themselves. Clearly, both "learning by doing" and formal training/education contribute to success, and yet, their weightings can vary significantly. Some occupations have high educational barriers to entry (think the legal or medical profession). Technology, on the other hand, is a notable example of where different combinations of on-the-job training, formal education and IT-specific credentials can be leveraged for career success. Few sectors can rival technology in the number of college drop-outs that went on to do amazing things (Steve Jobs, Bill Gates and Mark Zuckerberg just to name a few).

In the case of security, the research indicates about 40% of professionals developed their skills primarily through experience, while 23% relied heavily on formal training/education. The middle 36% cited both equally. It's beyond the scope of this study to assess which approach is best, although indirect evidence suggests a need for more formal training/education.

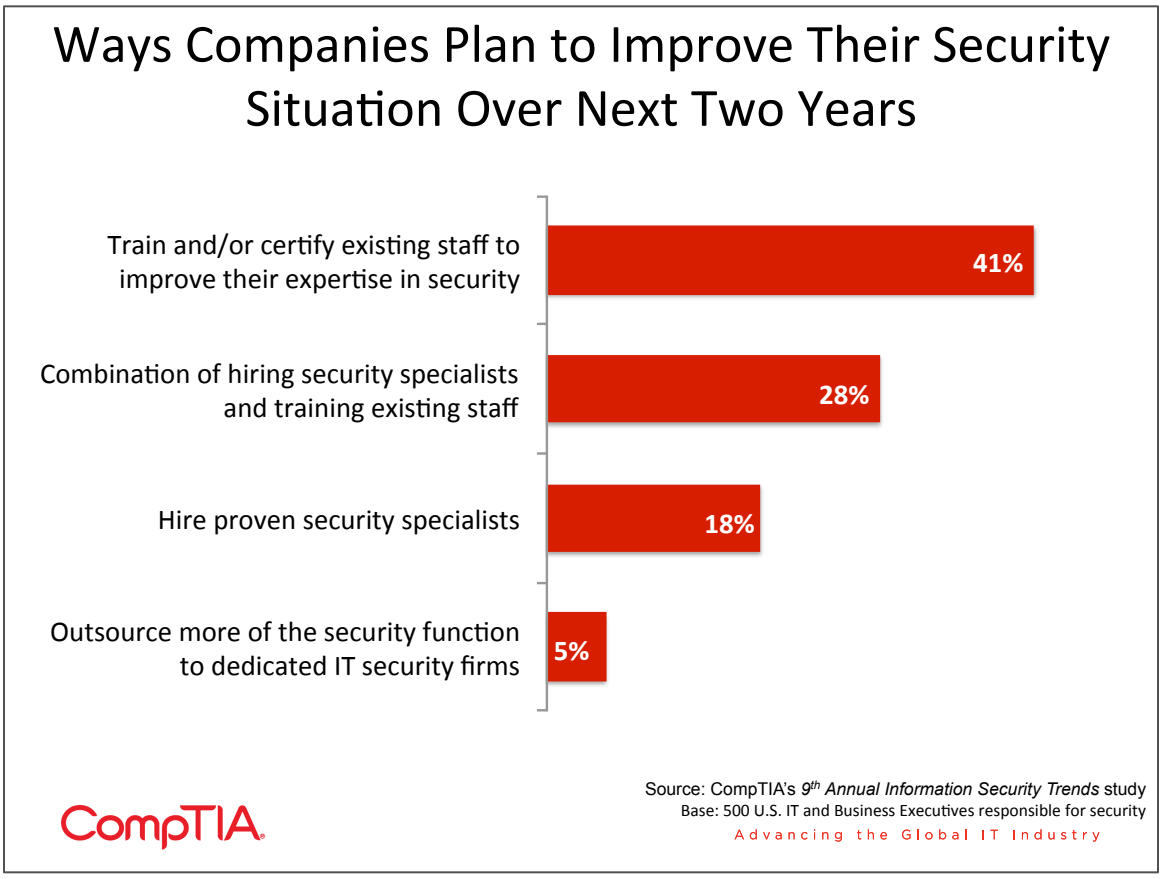
Among those with deficiencies in some area of security, the greatest number of respondents believe more training/education is needed to address the shortcomings. Smaller firms appear to have a stronger need for formal training/education than larger firms (58% vs. 39%).



On average, organizations report being about 30% short of headcount devoted to security. For example, a company with 10 IT staff focused on information security, would ideally like to have 13 staff for optimal performance. Unfortunately, in the real world of "do more with less," most companies are forced to operate at less than optimal staffing levels.

Nonetheless, hiring intent for security professionals is on the rise, as 46% of organizations signal their intent to hire security specialists over the next two years.

This could be challenging though given the experience of those that have already attempted to hire security specialists. Forty percent of firms in this situation reported difficulty in finding security specialists with the right mix of expertise and experience, not surprising given the many hats security professionals must wear. Reflecting this shortage, Robert Half Technology projects salaries for data security analysts will increase 6% in 2012, netting compensation of $89,000 - $121,500.



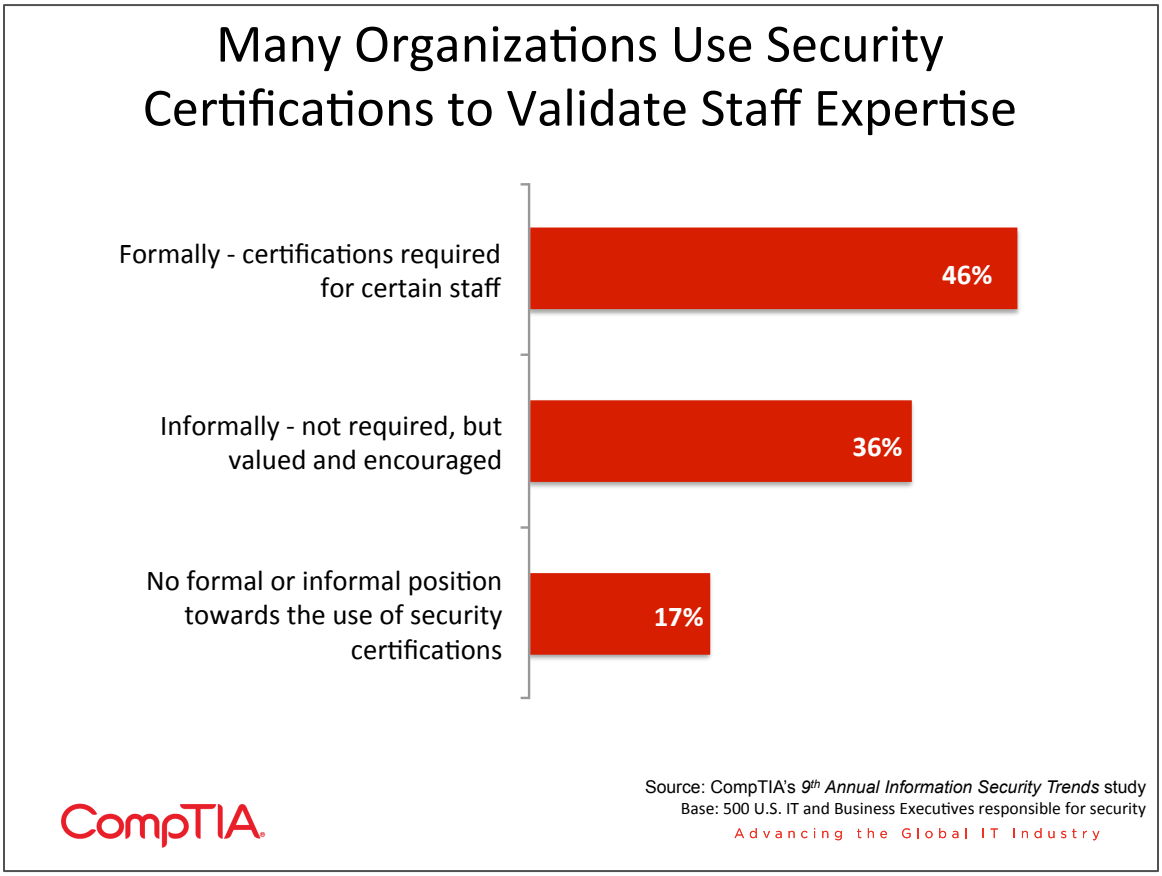
The longer-term outlook for security employment tracks closely with the overall security trend. A 2011 (ISC)^2 Global Information Security Workforce Study conducted by Frost & Sullivan estimated that the number of security professionals worldwide will grow at a compound annual growth rate of 13.2%, reaching 4.24 million professionals by 2015. This study identified three areas where shortages of expertise could be especially pronounced: information risk management, applications and systems development security and digital forensics.

The Role of Certifications

More than 8 in 10 organizations formally or informally use security certifications as a means to validate expertise. A prior CompTIA study, *Employer Perceptions of IT Training and Certifications*, confirms that both hiring managers and HR personnel factor certifications into the assessment process of job candidates.

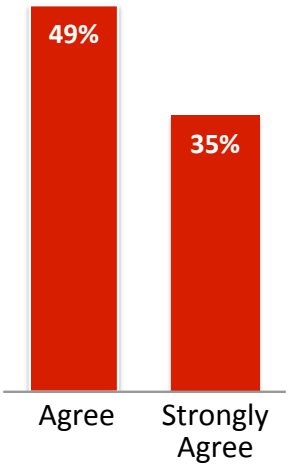
Organizations view certified staff as an integral part of their security apparatus. The validation provided by certification is evident by the high level of agreement to certified staff being more valuable to the organization, having proven expertise and the belief that the organization is more secure because of the presence of certified staff (see chart on following page).

As expected, there is a correlation between organizations that have a formal policy towards the use of certification and the value assigned to certifications. Also, those who have been the target of a greater number of security breaches find greater value in having certified employees.

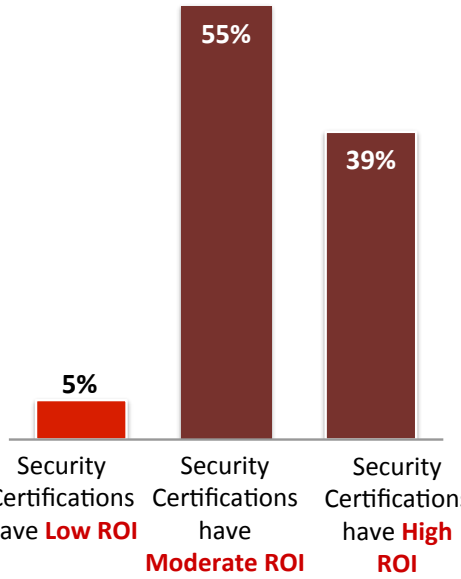


Organizations Recognize the Value of Testing After Training to Confirm Knowledge Gains

A net **84%** of organizations agree that it's important to **test after training** to confirm knowledge gains



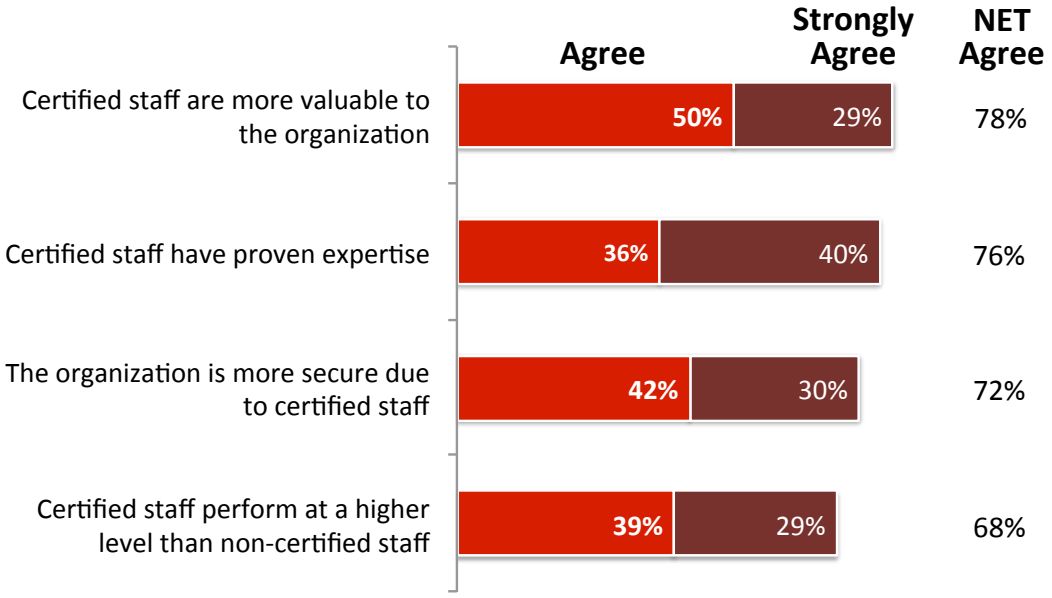
A net **94%** of organizations* believe security certifications **positive ROI**



Source: CompTIA's *9th Annual Information Security Trends* study
Base: 350 U.S. organizations with a formal or informal policy towards the use of IT certifications

CompTIA
Advancing the Global IT Industry

Staff with Security Certifications Viewed as More Valuable to the Organization



Source: CompTIA's *9th Annual Information Security Trends* study
Base: 500 U.S. IT and Business Executives responsible for security

CompTIA
Advancing the Global IT Industry

Because security is broad field, with technical, legal, strategic and managerial aspects, no single certification can possibly satisfy all necessary skill sets. Below is a sampling of the many security related certifications available today:

- Certified Ethical Hacker (CEH)
- Certified Information Security Manager (CISM)
- Certified Information Systems Security Professional (CISSP)
- Certificate of Cloud Security Knowledge (CCSK)
- CompTIA Security+
- CompTIA Advanced Security Practitioner (CASP)
- CyberSecurity Forensic Analyst (CSFA)
- Global Information Assurance Certification (GIAC)
- Vendor certifications such as Cisco's Certified Network Associate Certification (CCNA), Microsoft's Certified Systems Engineer (MCSE) that have a security component

Mapping security job roles and career paths to certifications has been a goal of certifying bodies, the private sector and government agencies for some time. One recent effort from the National Initiative for Cybersecurity Education (NICE), an extension of the U.S. government National Institute of Standards & Technology, is the Cybersecurity Workforce Framework.

The framework identifies seven high-level categories of cybersecurity, along with definitions, key job roles, skills and sample occupation titles.
http://csrc.nist.gov/nice/framework/documents/NICE-Cybersecurity-Workforce-Framework-printable.pdf

1. **Securely Provision**
   - Conceptualizes, designs and builds secure IT systems, with responsibilities for some aspects of the systems' department.
2. **Operate and Maintain**
   - Provides support, administration and maintenance necessary to ensure effective and efficient IT systems performance and security.
3. **Protect and Defend**
   - Furnishes identification, analysis and mitigation of threats to internal IT systems and networks.
4. **Investigate**
   - Responsible for the investigation of cyber events and/or crimes of IT systems, networks and digital evidence.
5. **Operate and Collect**
   - Accountable for the highly specialized collection of cybersecurity information that may be used to develop intelligence.
6. **Analyze**
   - Responsible for highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.
7. **Support**
   - Provides support so that others may effectively conduct their cybersecurity work.

www.comptia.org