CompTIA

INFORMATION SECURITY TRENDS

FULL REPORT

RESEARCH

TENTH ANNUAL • NOVEMBER 2012

www.comptia.org

About this Research

CompTIA's *10th 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.
- Gain insights into the security issues associated with emerging technology.
- Understand the role that the IT channel is playing in cybersecurity.

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: Security in a New Technology Landscape
Section 3: Threats and Defenses
Section 4: Changing Security Mindsets
Section 5: IT Channel Perspectives

This research was conducted in two parts.

Part I
The data for this study was collected via a quantitative online survey conducted September 26 to October 5, 2012 among a sample of 508 IT and business executives directly involved in setting or executing information security policies and processes within their organizations. The margin of sampling error at 95% confidence for aggregate results is +/- 4.4 percentage points. Sampling error is larger for subgroups of the data.

Part II
The data for this study was collected via a quantitative online survey conducted during late September and early October 2012. The sample consisted of 368 executives at U.S IT firms, with most having some level of involvement in the IT channel. The margin of sampling error at 95% confidence for aggregate results is +/- 5.2 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

TENTH ANNUAL • NOVEMBER 2012

www.comptia.org

Key Points

- Given the criticality of information security it is no surprise that four out of five companies in CompTIA's *10th Annual Information Security Trends* study expect to keep security as a high priority. Larger companies place a higher priority on security than small or medium sized businesses. While there is generally confidence in the effectiveness of defenses, some of this confidence may be misplaced if a company simply has not had (or detected) a security breach recently.

- The focus on security has translated to robust sales of security products and services. According to a report from PricewaterhouseCoopers, global cyber-security spending is expected to reach $60 billion in 2011 and is forecast to grow 10% every year during the next three to five years. IDC forecasts small and medium business (SMB) spending on security technology will continue to show strong growth and will exceed $5.6 billion in 2015. According to Gartner, worldwide security software sales reached $17.7 billion in 2011, a 7.5% increase over 2010 revenue.

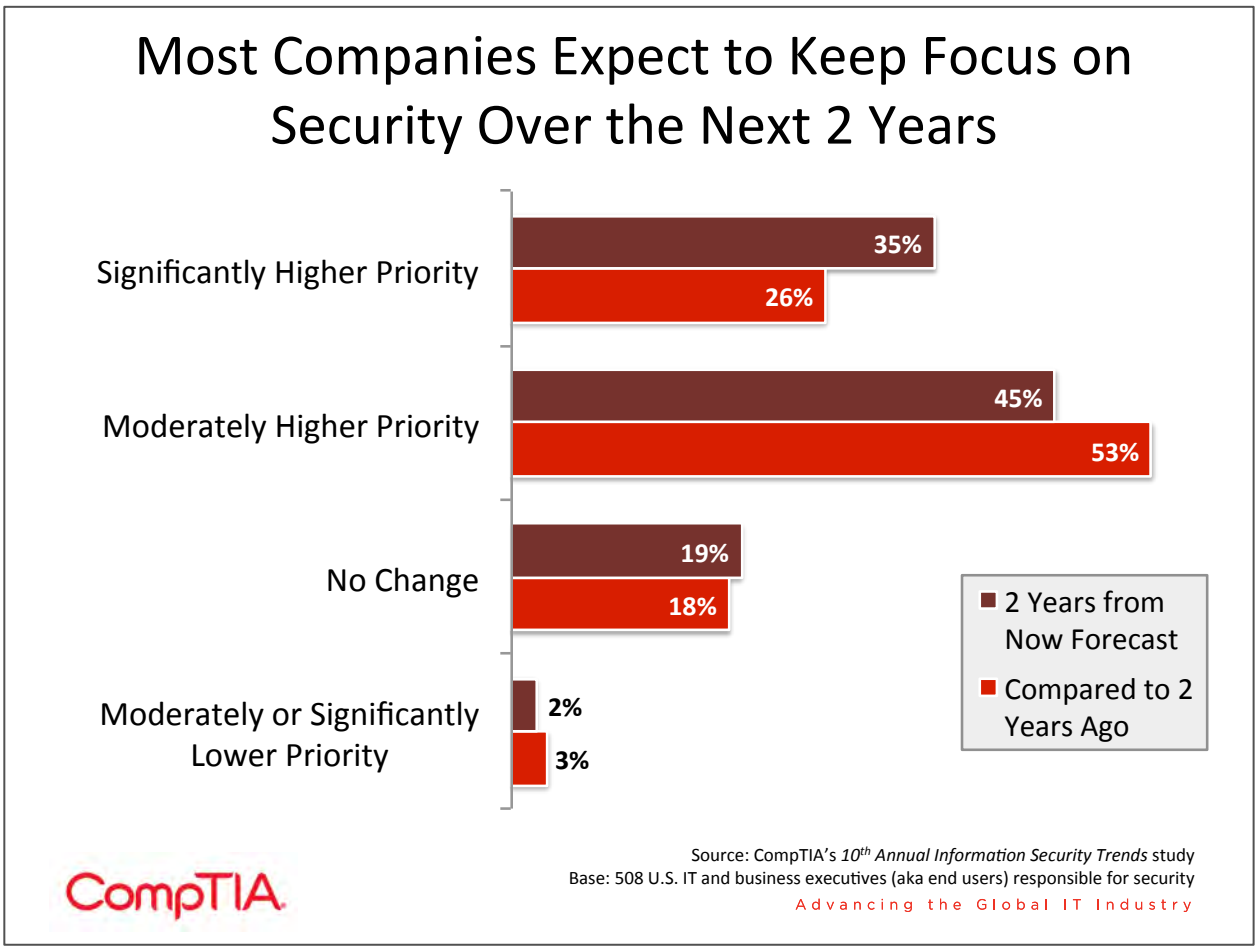
- The continued emphasis on information security has meant that it is one of the unique fields where the demand for qualified professionals exceeds supply. CompTIA's *10th Annual Information Security Trends* study finds that the intent to hire is strong with a net 49% of companies saying that they intend to hire security specialists, including those that also plan on training current staff.

- Regardless of how the information security landscape changes, one constant will always remain – the human factor. The majority of companies attribute human error as the cause of security breaches. According to data from CompTIA's *10th Annual Information Security Trends* study, almost 6 in 10 companies believe that their security team has the appropriate level of expertise. Among those who observe some deficits, the gap is most pronounced in areas relating to emerging areas such as cloud security, mobile security, and data loss prevention.

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, where the stakes are very high. Organizations are faced with ever evolving threats and 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." Given the criticality of information security it is no surprise that four out of five companies in CompTIA's *10th Annual Information Security Trends* study expect to keep the focus on security. Larger companies place a higher priority on security than small or medium sized businesses. This trend is consistent with findings from last year's study.



The data also shows that 3 out of 4 companies are "confident" or "very confident" in their security defenses with medium and large scale companies showing more confidence when compared to smaller companies. This may be a false sense of confidence, though. Companies may feel assured in their

defenses if they believe they have not experienced a security breach recently, but there is evidence that many breaches go undetected. Even if a company has truly been breach-free, it may just be a matter of time until defenses break down if those defenses are not regularly tested and adjusted. Especially as companies explore new technology models, ongoing vigilance is required to maintain a secure posture. Organizations may sense that there is room for improvement—though 75% are "confident" or "very confident," only 19% have enough assurance to rate themselves "very confident."

Spending on Information Security

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

- According to a report from PricewaterhouseCoopers, global cybersecurity spending is expected to reach $60 billion in 2011 and is forecast to grow 10 percent every year during the next three to five years. The report notes that in the US, the growth is fueled equally by private and government spending unlike in other countries where it is mostly driven by private sector spending.

- According to the research firm Gartner, worldwide security software sales reached $17.7 billion in 2011, a 7.5% increase over 2010 revenue. The top 5 players in the space, Symantec, McAfee, Trend Micro, IBM and EMC, accounted for 44% of this market.

- IDC forecasts small and medium business (SMB) spending on security technology will continue to show strong growth and will exceed $5.6 billion in 2015. Overall SMB IT spending is forecast to grow at a rate of 5-6% per year over the forecast period, SMB spending on security products and solutions is expected to grow almost twice as fast.

- Figures from Infonetics expect the network security market to have revenues of $6.7 billion by 2016. The top

InfoSec Spending on Emerging Areas

As a subset of general security spending, spending on emerging areas in the security sphere is growing as evidenced by increased spending in the fields of data loss prevention, and mobile and cloud security.

- Given that so far in 2012, more than 9 million records have been exposed (according to data from the Identity Resource Center), it is no surprise that the data loss prevention market is growing. In 2010, IDC estimated that the market size for data loss prevention in 2009 was $262.3 million and would grow at a rate of 20.2 percent over the next five years to more than $658 million by 2014. In 2011/2012, they estimate the market size to be in the $387 million to $472 million range.
- Data from Vision Gain and Juniper Research point to a growing market for mobile security. Vision Gain has determined that the value of the global mobile security market in 2012 will reach $1.6 billion. Juniper Research forecasts a $3.6 billion opportunity for mobile security software providers by 2016.
- Forrester research forecasts that cloud security is set to grow into a $1.5 billion market by 2015 to make up nearly 5% of IT security technology spending. Data from Tech Navio notes that the cloud security market made up 2% of the global security market in 2010 and this will increase to 4% of the global security market in 2014.
- As enterprises struggle to keep pace with security threats, IDC predicts that the emerging predictive security market is forecast to grow from $198 billion in 2009 to $905 billion in 2014.

three players in 2011 according to Infonetics are Cisco, Checkpoint and Juniper.

- IDC estimates the worldwide managed security services (MSS) reached $14.9 billion in 2011 and is expected to reach $26.1 billion in 2016. The worldwide and U.S. network security services market showed significant improvement in growth from 2011 to 2016, with a CAGR of 19.7%. The 2011–2012 year-over-year growth rate for global managed security services is expected to be 12.6%, resulting in a market that will reach $26.1 billion in 2016.
- From a channel perspective, 66% of channel firms involved with security expect their revenue to grow in the next year, with 16% expecting significant growth (10% or more).

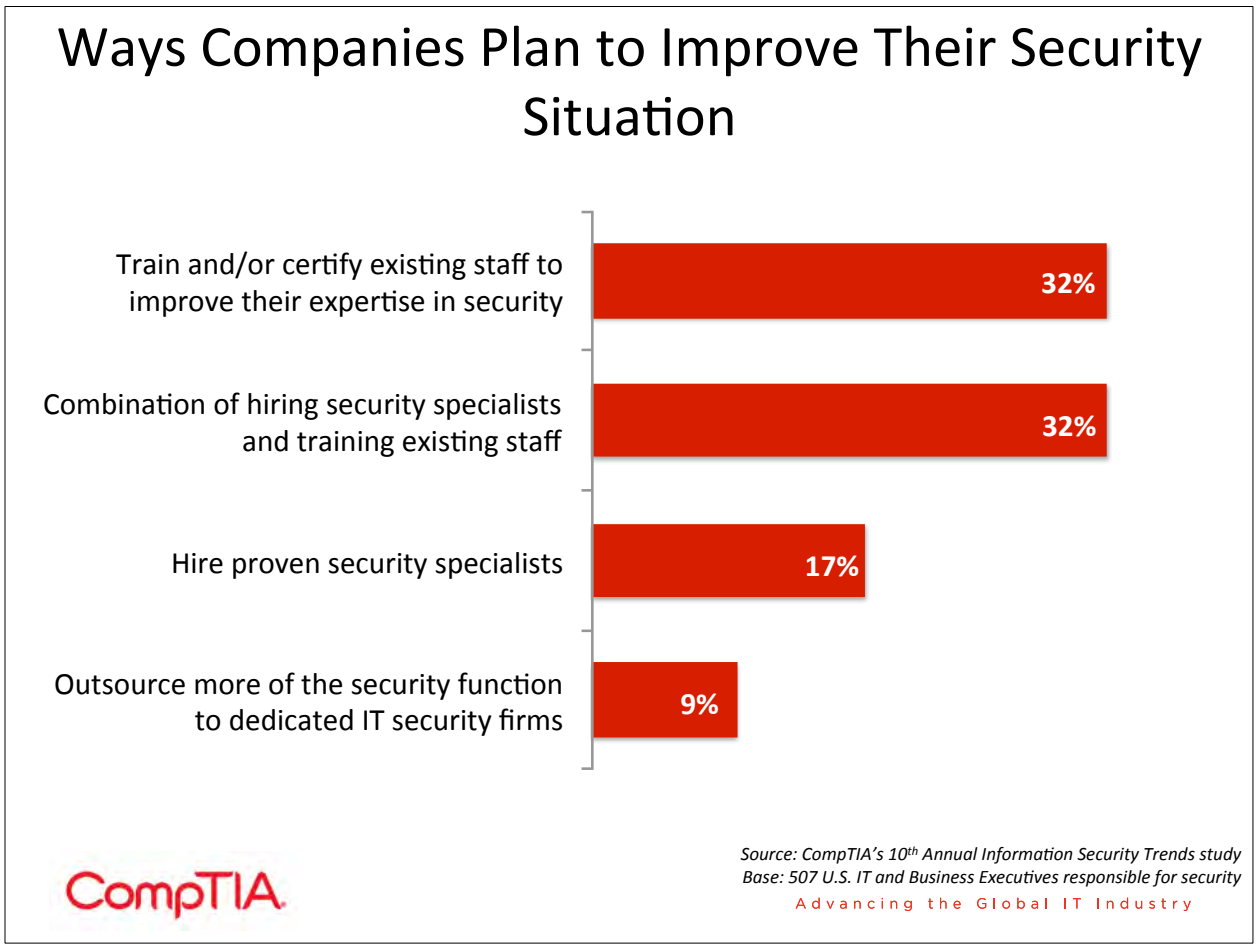
The Strategic Security Survey conducted by InformationWeek Analytics found that similar to previous years approximately 1 in 4 firms spend 10% or more of their IT budget on security. From an ROI perspective, the spending on information security is justified. The 2012 Norton Cybercrime Report estimates the direct cost of consumer cybercrime to be $110 billion worldwide. The average loss per person was $197, and the report found an increase in the incidence of crimes on social and mobile platforms. The Ponemon Institute's 2011 Cost of a Data Breach study found that in the United States the organizational cost and cost per stolen/lost record had declined when compared to previous years but still stood at $5.5 million and $194 respectively.

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. According to the job board aggregator Indeed.com, the number of information security jobs has shown an increasing trend since 2006.

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 2012 Career Impact Study conducted by (ISC)2 found that qualified IT security professionals are hard to find and 96% of the respondents were currently employed. The survey also found that security budgets and hiring were on the rise and that security was a priority staffing need. CompTIA's *10th Annual Information Security Trends* study also finds that the intent to hire is strong with a net 49% of companies saying that they intend to hire security specialists, including those that also plan on training current staff.

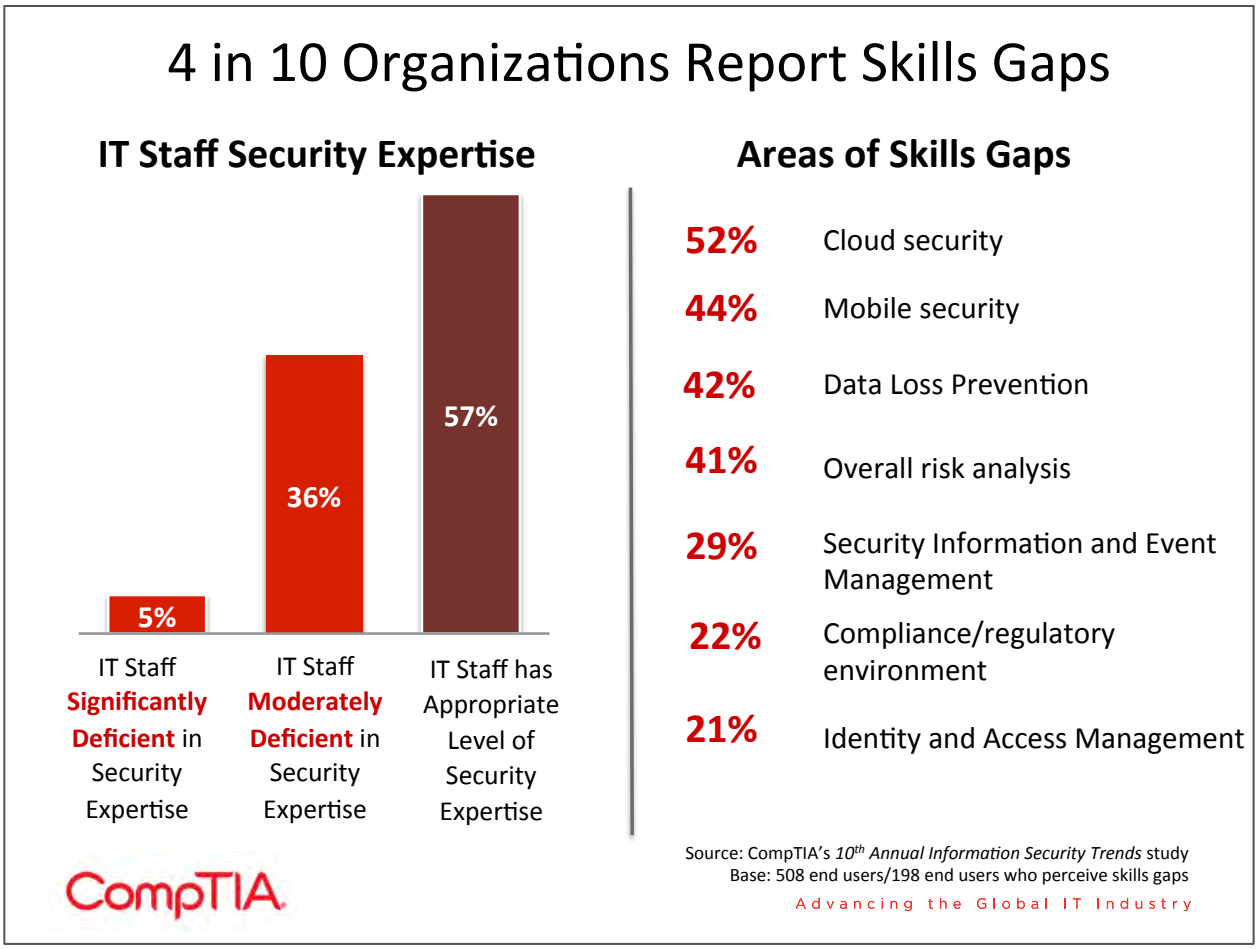


CompTIA's *10th Annual Information Security Trends* study finds that a fifth of firms say that they have experienced challenges in hiring IT security specialists. This is significantly lower than last year when 40% of firms reported experiencing difficulties with hiring. More than anything, this may be a statement that hiring has been frozen over the past year—external data suggests that security professionals are in high demand. Any companies that have had less experience with security incidents may have placed hiring of security experts as a lower priority.

Assessment of the IT Workforce

Regardless of how the information security landscape changes, one constant will always remain – the human factor. The majority of companies attribute human error as the cause of security breaches. According to data from CompTIA's *10th Annual Information Security Trends* study, 41% of companies report that their staff has moderate or significant deficiencies in their security expertise. The deficit is

most pronounced in areas relating to emerging areas such as cloud security, mobile security, and data loss prevention. Organizations say that some areas of impact of these deficiencies are being unaware of areas where the company is exposed (44%), loss of business as a result of security issues with customer data (39%), and costs incurred for training the current workforce (38%). Overall, security skill gaps are among the most serious across all IT skills; CompTIA's *State of IT Skills Gap* report showed that a net 89% of companies place a high importance on security skills, and it is also one of the top concerns for organizations.



This study found that organizations view certified staff as an integral part of their security apparatus, and 84% indicated that there was a positive ROI from security certifications. The value provided by certification to the companies in the survey is evident: many agree that certified staff are more valuable to the organization, have proven expertise, and perform at a higher level than non-certified staff.

CompTIA

INFORMATION SECURITY TRENDS

SECTION 2: SECURITY IN A NEW TECHNOLOGY LANDSCAPE

RESEARCH

TENTH ANNUAL • NOVEMBER 2012

www.comptia.org

Key Points

- Shifts in the technology landscape are driving new security practices. Cloud computing is forcing end users to consider how data is handled outside of their organization. Seventy-eight percent of cloud users perform regular reviews of their cloud providers, covering topics such as business continuity/data recovery, identity and access management, and data integrity. This represents a slight increase from the previous year. A net 80% of cloud users are "confident" or "very confident" in the ability of cloud providers to demonstrate effective security in their environment.

- Mobile devices and applications are also causing concern for security professionals. Lost or stolen devices are the most typical security incident, driving an interest in Mobile Device Management (MDM). However, the top overall concern is the use of unauthorized apps, as malware strains are becoming more prevalent in both Android and iOS marketplaces.

- Over half the sample (51%) identifies the rise of social networking as a factor impacting security. Malware and viruses now have new avenues for distribution, but the larger threat is that of the human element. With human error becoming more of a factor than technology error over the past two years, companies must decide how to regulate users that have access to powerful technology.

Reacting to 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 services 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.

Major Eras of Enterprise Technology

Many types of industrial or mechanical technology have made significant impacts on businesses, but information technology (IT) has been the dominant technology player since the mid-1900's. IBM describes five distinct phases of business technology over this timeframe. This description is not necessarily all-inclusive, but it does provide one baseline for thinking about the changes in technology and security.

- **Mainframe:** The first computers used for business were expensive machines requiring specialized skill, but the companies that could afford them realized a significant competitive advantage.
- **Departmental Computing:** The first stage of moving computing closer to end users, this trend forced the IT department to consider usage that was not fully supervised.
- **PC:** With the introduction of the PC, end users became more tech-savvy and more enabled. Work could even be brought home on physical media, forcing guidelines around removing corporate data.
- **Internet:** High connectivity drove new business models and new security requirements, as making information available to the world also introduced pathways for the world to access corporate systems.
- **Social Business:** Once again, the power of the previous era spread from a command-and-control structure to end users. See below for more details.

CompTIA's *10th Annual Information Security Trends* study highlights the characteristics of the current shifts. End users identified the following items as the top factors impacting security practices:

- **57%:** More reliance on Internet-based applications
- **55%:** Greater interconnectivity of devices, systems, and users
- **51%:** Rise of social networking

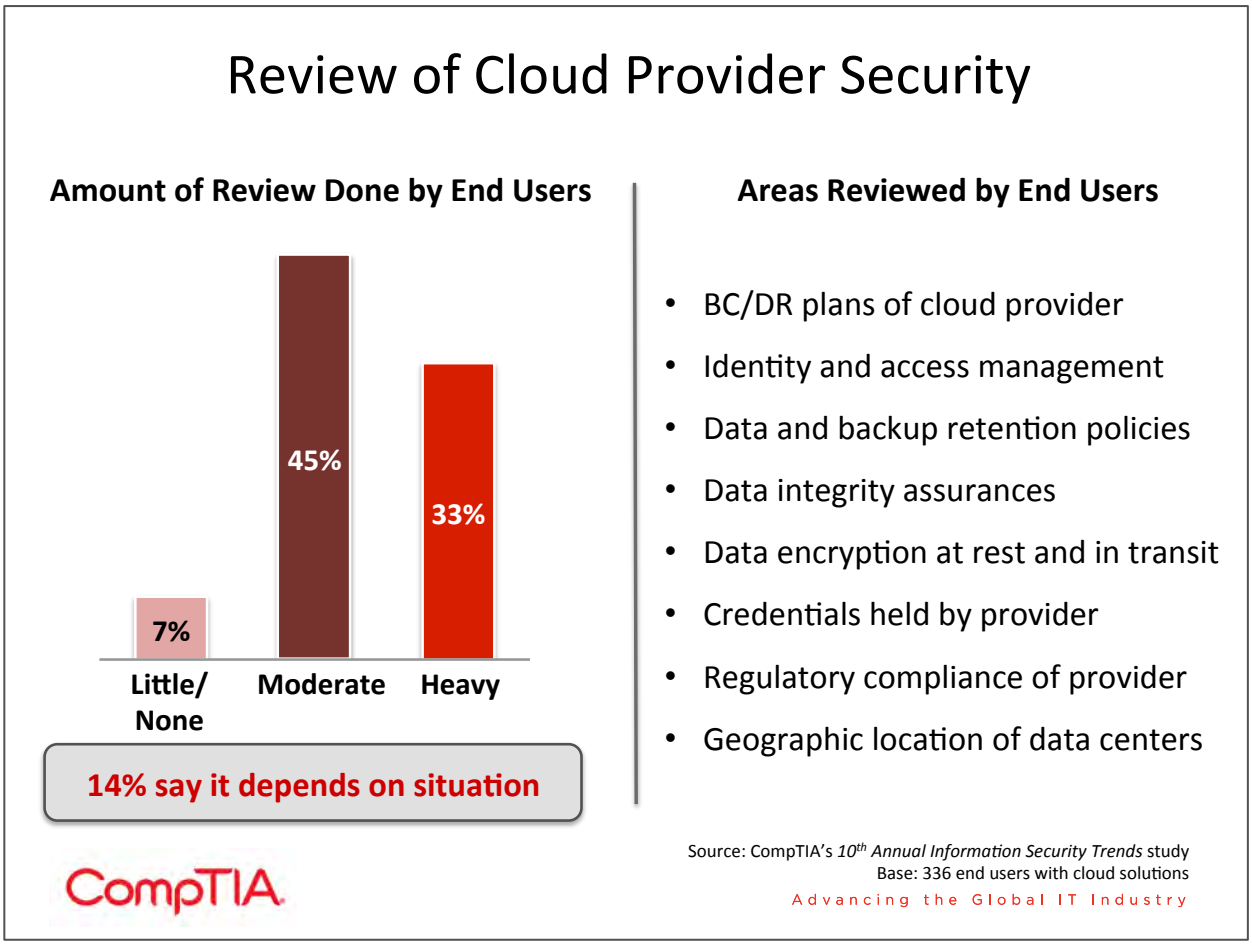
Cloud computing, mobility, and social business are changing the way that technology is used in the enterprise. These elements were all present in the previous version of the study as well, with social networking now moving into the top three and greater numbers identifying these as major factors. As

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.

Security In (and By) the Cloud

Cloud computing has been one of the most dominant IT themes in the past decade, and while the term may be overused by enthusiastic marketing teams, there is certainly great potential to be found through the use of cloud resources. At a high level, IT operations may not change drastically—at least not during a company's initial foray into cloud computing. Data backups will take place and virtual machines will be spun up for use in software development or web applications. The difference, though, is the location of the data. If public cloud solutions are used, the data resides at a provider's facility in a multi-tenant environment.

Nearly 80% of companies in the study were using cloud computing to some degree. This matches adoption rates found in other CompTIA studies. Data from previous studies indicates that one of the most commonly used functions at this point is data storage, so companies will obviously want to feel that their data is just as secure with a cloud provider as it is on-premise.



To achieve this, end users must be willing to review the policies of their provider. CompTIA's *9th Annual Information Security Trends* study examined the topic of cloud security in detail, including incidence of cloud provider reviews along with data on cloud concerns and mitigation strategies. Compared to that

report, there was a slight increase in the number of users that said they performed moderate or heavy reviews of their cloud providers' security policies and practices. Overall, the number of firms that performed no review dropped from 13% to 7%. No one topic stands out among the areas that are frequently reviewed, though it is noteworthy that geographic location of data centers ranks well below other topics for the second straight year. Different states can have different laws pertaining to digital data or regulatory compliance; even if the data being stored is not subject to these laws, it is advisable to be familiar with data locations as there are potential effects on data speed and availability.

Overall, companies must be happy with what they are finding during security reviews—a net 80% of cloud users are "confident" or "very confident" in the ability of cloud providers to demonstrate effective security in their environment. This represents a slight dip from last year's 85%, but it is still a good sign that end users trust the defenses that providers have installed. Fittingly, respondents showed a lower level of concern over issues such as data encryption at rest, physical data center security, or malicious activity by provider employees. The top areas of concern remain data availability and data security in transit. Downtime can certainly affect a business, but on-premise data centers cannot guarantee 100% uptime any more than a cloud provider. Failover procedures are simply a requirement in today's digital world.

Securing data in the cloud is the focus of many cloud security discussions, but many companies are also employing the cloud for security functions. Cloud applications are used for a wide range of functions, including Internet protection (such as anti-virus and web proxy), email protection, and management of PCs or mobile devices. Aside from the standard benefits of cloud software, cloud security applications offer some unique advantages. For example, anti-virus software that looks for suspicious patterns can draw on a much larger sample, and virus definitions can be updated automatically without requiring action from the user.

Getting Control of Mobile Devices

As disruptive as cloud computing is to a company's IT flow and security policies, mobility may be even more disruptive. 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 caused companies to reexamine their approach.

Top Concerns in Mobile Security

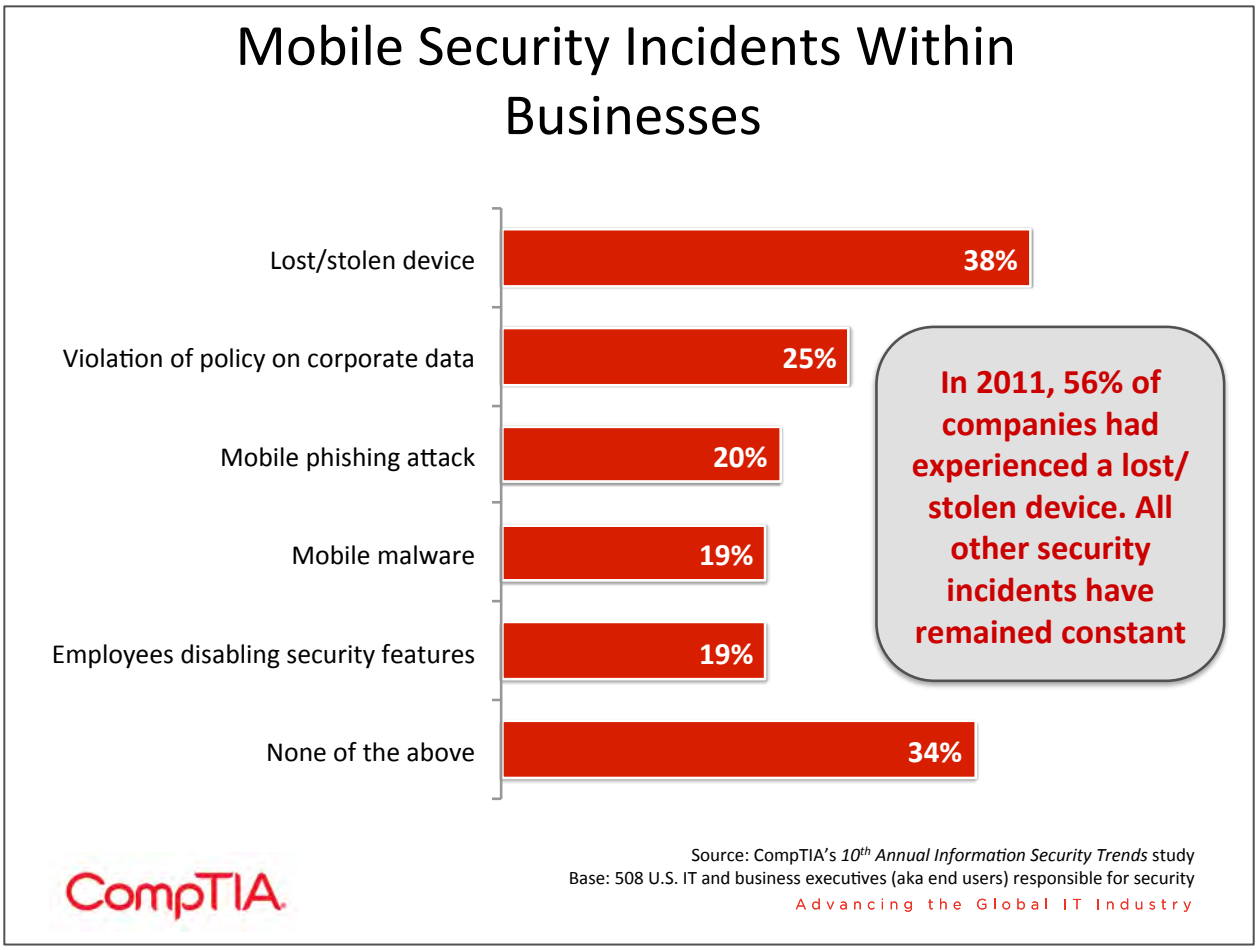
% of respondents rating as serious concern

33%	Employees downloading unauthorized apps
30%	Theft or loss of corporate device
29%	Risks associated with open Wi-Fi networks
29%	Malvertising
28%	Risks associated with social media
28%	Mobile device-specific viruses/malware

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.

The downloading of unauthorized apps continues to be the top mobile security concern among security professionals. Much of this concern stems from the growing amount of malware on the Android ecosystem. The latest data from market intelligence firm comScore (published prior to the iPhone 5 launch) show that Android accounts for 53% of the US smartphone market, and security firm Trend Micro has seen Android malware grow at double the expected rate, leading them to predict 250,000 malware samples in the Android market by the end of 2012. iOS is not immune to malware, though: after being malware-free for five years, the App Store saw its first instance of malware in the Russian language app "Find and Call" in July of 2012.



While mobile malware is an area of future concern, at present it has not been a major issue for businesses. In fact, it ranks at the bottom of a list of mobile incidents that have taken place at companies surveyed. Only the disabling of security features ranks as low, and that number is a function of the number of companies that have actually installed security features on devices (only 67% of companies even require passcodes to unlock mobile devices).

As with last year, a lost or stolen device is the most common mobile security incident—a fact that has driven interest in the field of Mobile Device Management (MDM). Most of the steps that companies have taken following a mobile security incident revolve around attempts to track and secure devices, such as installing tracking software (47%), establishing a lost device procedure (44%), and requiring encryption on mobile devices (43%). These strategies are apparently proving effective in stemming lost or stolen devices, as there was a significant drop in those incidents from one year ago.

Only 37% of the firms that experienced a mobile security incident began building a formal mobility policy as a result. According to CompTIA's *Trends in Enterprise Mobility* study, formal mobility policies are in place at just 22% of all companies, with another 20% in the process of building such a policy. As mobile devices become standard equipment for many workers, companies must consider what activities will be allowed on these devices. Guidelines for mobility may be included in other pre-existing policies, but with mobile devices being used by such a large percentage of the workforce and impacting workflow and liability, it may be more appropriate to build a separate policy explicitly stating corporate regulations.

While smartphones and tablets are the primary considerations for a company as it builds a mobility strategy, the rise of intelligent sensors and machine-to-machine (M2M) systems also falls into the category of mobility and introduces possible security risks. The data being streamed from sensors is being analyzed in new ways for business purposes, and cyber criminals may also find new ways to mine this data for malicious purposes. Strong encryption of data is a good start, and best practices will continue to emerge around security and privacy. See CompTIA's *An Introduction to M2M Systems* whitepaper for a primer on this emerging topic.

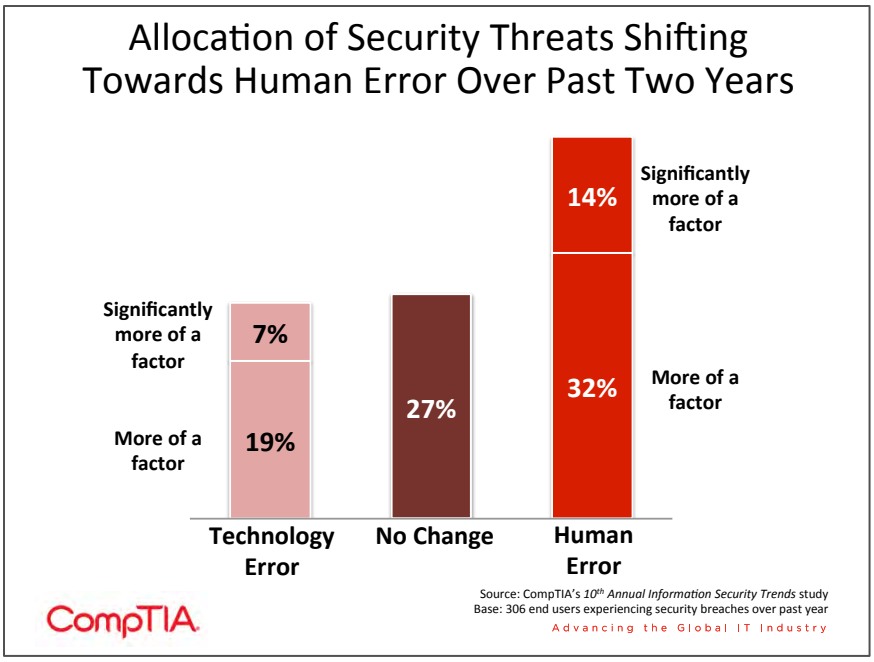
More Power for End Users Means More Responsibility

IBM labels the fifth era in enterprise technology as "social business," and it is true that social networks are a prime example of the ways in which companies are changing their communication and collaboration. Whether a business is performing marketing and customer communications on social media sites (such as Facebook, Twitter, and LinkedIn) or building internal communities and collaboration platforms using social business tools (such as Jive, Telligent, and IBM Connections), social technologies are making an impact in the enterprise.

Along with this impact, there are security considerations. By their nature, social networks depend on the sharing of personal information, and users may tend to view a social site as a safe platform. Spammers and other cyber criminals are taking advantage of these aspects to launch attacks. Malware and viruses are being introduced in new ways: shortened URLs that appear to come from a friend, corrupted applications that operate within social sites, and ads that seem legitimate (aka malvertising). Some of these may bring worms or Trojans onto a system, which can be a serious corporate threat. Others may simply be annoying, such as bots that perform unauthorized recommendations (aka like-jacking).

Another serious security threat in the social space is emblematic of a larger issue. Social engineering schemes are designed to trick a user into divulging personal information, including passwords, to an attacker. An attacker can make a request for such information seem legitimate by using information that the user has shared publicly. The information is then used to gain access to accounts, and if those accounts are business-related, real damage can be done. The identity hacking of Wired senior editor Mat Honan in August 2012 showed how simple it can be to gain access to accounts if they are not protected properly, and it also showed the dangers in linking accounts or using similar credentials for both personal and business accounts.

The larger issue is best categorized as the consumerization of IT. As individuals gain access to powerful computing resources that can be easily used without tech support, there is the potential for much greater productivity. However, there is also the potential for more widespread security risk, as these users do not necessarily have the security background to understand what comprises a breach when using such resources.



Companies that have experienced security incidents can see the impact that consumerization is having. Looking back over the past two years, human error is clearly becoming more of a factor in breaches. The causes of this human error are not malicious; instead, there is a lack of knowledge, expertise, and discipline that leads to many breaches.

Accounting for the human element, as unpredictable as it may be, requires a different approach than protecting from external threats. Technology can assist in the effort, but education, training, and policy enforcement will be key factors as well. Section 4 of this report examines the issue of consumerization more closely and provides insight on ways in which companies can improve their security posture in this area.

CompTIA

INFORMATION SECURITY TRENDS

SECTION 3: THREATS AND DEFENSES

RESEARCH

TENTH ANNUAL • NOVEMBER 2012

www.comptia.org

Key Points

- Cybersecurity threats continue to rise—in addition to the well-known threats (such as spam, malware, and viruses), there are new threats to contend with (such as advanced persistent threats and IPv6 vulnerability). While companies in the survey showed a lower level of concern than in previous studies, IBM's X-Force research team believes that 9,000 new vulnerabilities will be discovered in 2012, surpassing the record set in 2010.

- Data loss is a serious threat for businesses—41% of companies are aware of data loss over the past year. Before robust data protection can be put in place, the data must be centrally organized. Thirty-five percent of companies are at a stage of identifying/organizing data (while another 16% have no current data initiatives).

- Other modern security mechanisms seek to address issues with current technology and provide management capabilities for a complex discipline. Some of the defenses being utilized are identity and access management (adopted by 53% of companies), security information and event management (46%), external vulnerability assessments (36%), and enterprise security intelligence (35%).

The Threat Landscape

In the IT world, large security breaches make headlines on a regular basis. Digital data is playing an increasingly important role in the lives of consumers and businesses, and cloud computing has connected all this data in ways that are sometimes unexpected. These large breaches, then, tend to highlight the ways in which companies must constantly update their security schemes and individuals must be aware of the changing environment.

A large breach involving confidential information can certainly be detrimental to a company's reputation, but even smaller breaches have a financial impact. Section 1 of this report described the costs incurred by security breaches. Revenue is impacted directly and indirectly, as there is time involved to recover data or remove viruses. A series of small breaches can cause the cost to accumulate quickly.

Symantec publishes a monthly intelligence report analyzing the nature and amount of cybersecurity threats. The September 2012 report includes a high-level view on several common areas:

- Spam rate: 75% (3 out of 4 emails being sent worldwide are spam)
- One in 245 emails identified as phishing
- One in 211 emails contain malware
- 780 malicious websites blocked per day

These numbers tend to fluctuate over time, but there are some general trends shown in the report: spam has generally declined since the middle of 2010, phishing and malware have remained relatively constant over the past several years, and the number of malicious websites has returned to previous levels after somewhat of a spike in late 2010 and 2011. Even with the decline in spam, all of these areas remain very active, showing that attackers are still finding success in methods that have been on the security radar for a long time. Baydin, an email management service, estimates that the average email user receives 147 emails a day. That accounts for both personal and corporate email, but that average influx and the phishing/malware rates suggest that emails users could easily see these types of threats on a weekly basis.

In addition to these "tried and true" methods, many new forms of attack are springing up in attempts to take advantage of a changing technology landscape.

- 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 in April 2012 news broke that 600,000 Macs had been infected with the Flashback Trojan. This was likely the leading edge of a wave of new Mac-targeted malware.
- 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.

Attacks from the outside are not the only risks to a company's security posture. Firms must also deal with the threat of internal leaks (whether malicious or unintentional) and a complex regulatory environment.

Companies in CompTIA's *10th Annual Information Security Trends* study are clearly aware of all these risks. The greatest concerns are focused on external threats—malware, hacking, and social engineering. Lower on the list are internal threats, such as malicious insider abuse or unintentional human error.

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.)	35%	60%	44%	57%
Hacking (e.g. DoS attack, APT, etc.)	35%	54%	47%	53%
Social engineering/Phishing	47%	39%	54%	46%
Understanding security risks of emerging areas, i.e. cloud, mobile, social	51%	37%	49%	51%
Data loss/leakage	45%	37%	64%	36%
Physical security threats (e.g. theft of a device)	41%	31%	71%	29%
Intentional abuse by insiders, i.e. staff, contractors	40%	25%	74%	26%
Human error among end-users	59%	24%	71%	29%
Human error among IT staff	49%	22%	78%	22%
Lack/inadequate enforcement of company security policy	48%	21%	72%	23%
Lack of budget/support for investing in security	42%	20%	79%	22%

Source: CompTIA's *10th Annual Information Security Trends* study
Base: 508 U.S. IT and business executives (aka end users) responsible for security

CompTIA
Advancing the Global IT Industry

It is interesting to note that across the board, the level of concern is lower than in the previous study. For example, 37% rate data loss or leakage as a serious concern, but 54% rated this as a serious concern previously.

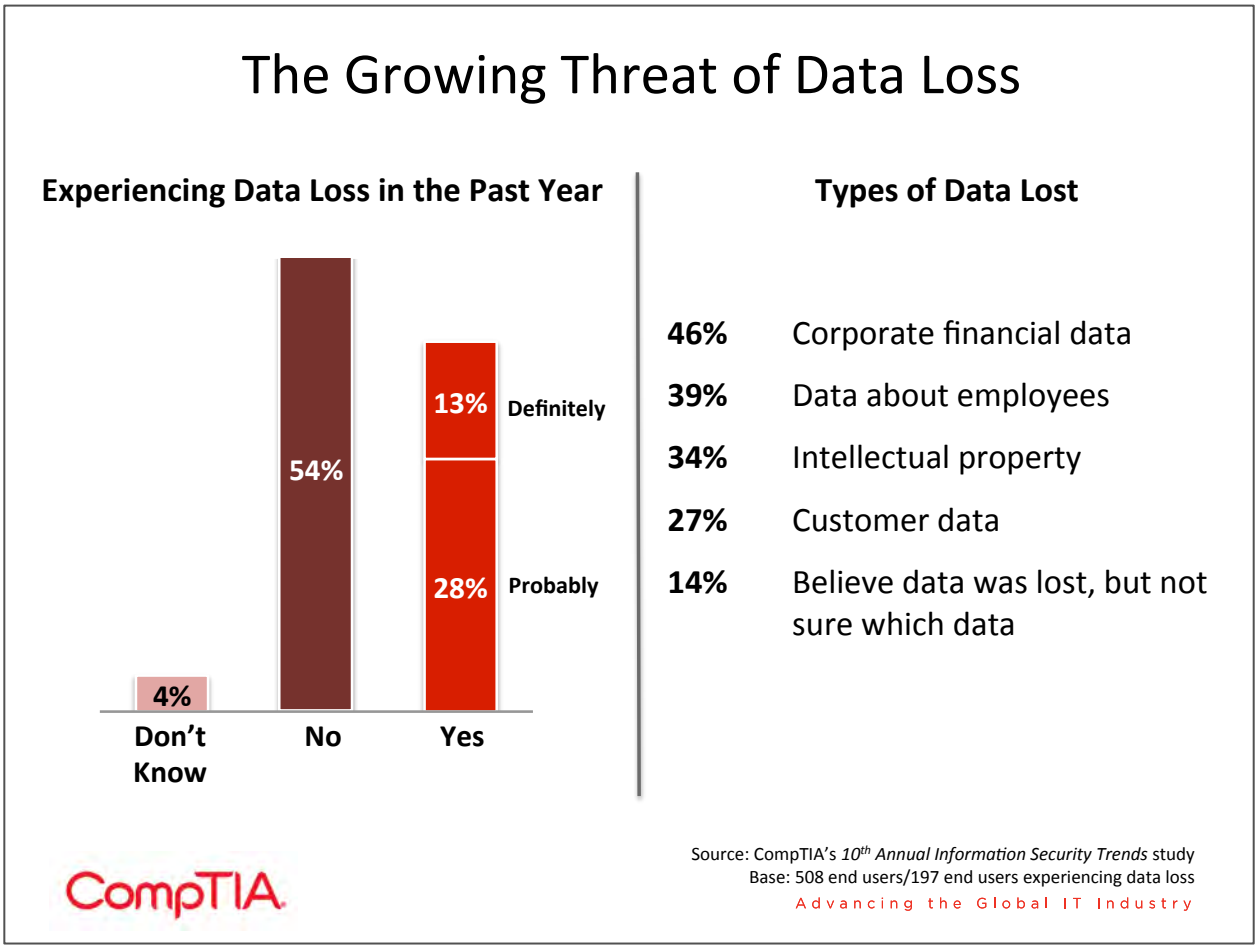
This lower level of concern is likely tied to the sample's perception of the breaches that have occurred at their organizations. In the *9th Annual Information Security Trends* study, 76% of companies reported experiencing a security incident in the past year. In the most recent study, only 61% reported a breach. Subject matter experts in security typically observe that a company is more likely to take security seriously once something bad happens to them.

While it might be nice to imagine that lower levels of concern and lower volumes of reported breaches indicate progress in the war on cybercrime, this is probably not the case. To begin with, perception of breaches is different than actual breaches. A large number of companies will admit that there have probably been breaches that have gone undetected. Small breaches or losses of data may go unnoticed for a long time, but can still be damaging.

Secondly, all indications point to the threat level rising rather than declining. PandaLabs reports that 73,000 out of the 206,000 files received daily are new strains of malware. IBM's X-Force research team, after declaring 2011 the "year of the security breach," believes that 9,000 new vulnerabilities will be discovered in 2012, surpassing the record set in 2010. Hacking and malware are obviously proving to be profitable for cyber criminals, and the changing use of technology is opening up new avenues for internal breaches.

Focusing on Data Security

One of the reasons it is surprising to see a drop in the concern over data loss is that there has been a major focus on data security in recent years. Digital data is becoming the lifeblood of a business—CompTIA's *Big Data Insights and Opportunities* study showed that a net 87% of companies believe data is important to business operations. As mobile devices proliferate and cloud solutions become standard parts of IT architecture, building a secure perimeter is impossible and the data itself must be secured in some way.



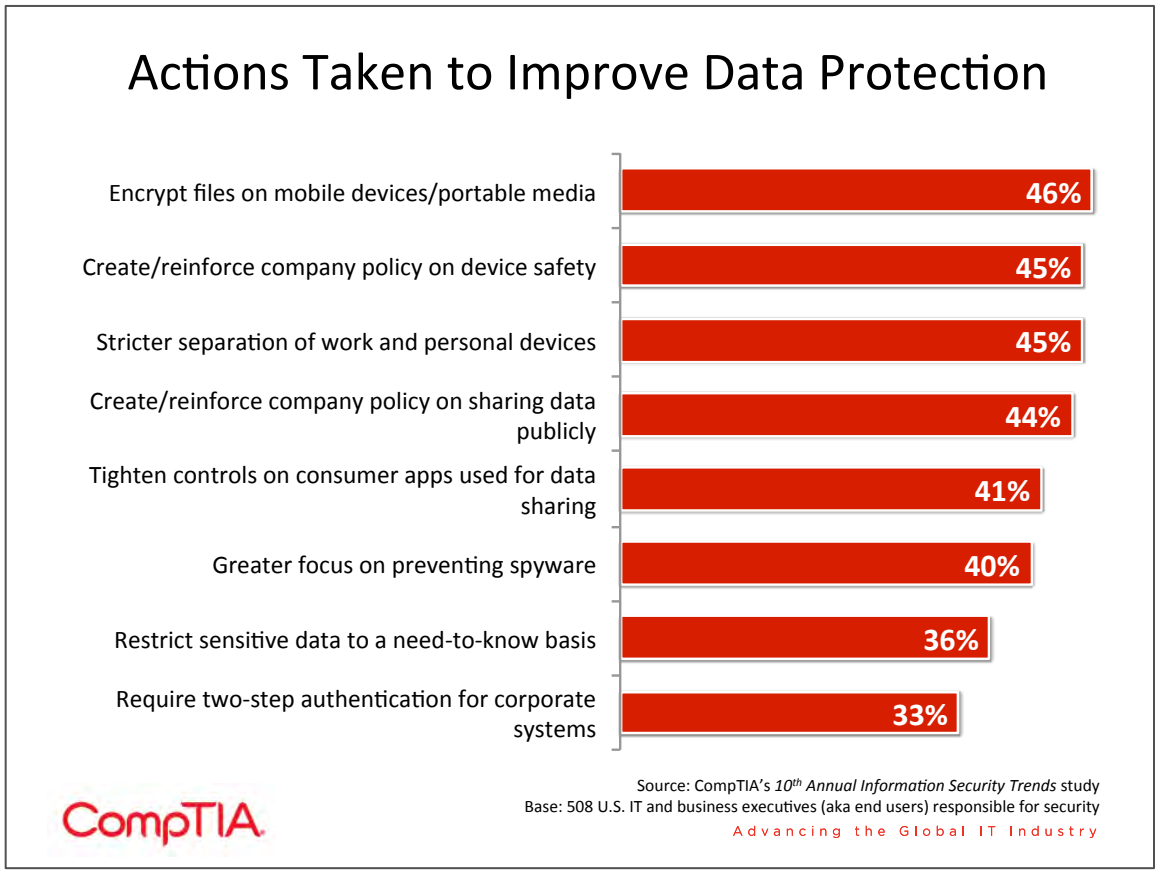
Over half the sample believes there has not been a data loss incident at their company, but it is likely that data loss falls into the category of undetected breaches. Consider the example of an employee mentioning their project on Facebook. If the information stops with the employee's friends simply finding it interesting, it is hard to discover that data has been shared. If a competitor or an analyst

happens to see the comment, though, it may become more apparent that confidential data has leaked outside the company.

Small companies (1-99 employees) are the most likely to say that they have not experienced data loss. Similarly, small companies show a lower level of concern for all types of security threats. Many smaller companies may believe that their data does not appeal to attackers. Data from the June 2012 Symantec Intelligence report suggests otherwise, though. The average number of attacks per day on companies with over 2500 employees is 68.9. This number then drops dramatically—17.4 attacks per day for companies with 1501-2500 employees. The trend continues downward as company size shrinks, up to the smallest companies (1-250 employees). Here, the number of attacks per day spikes back up to 57.7.

Small companies may not have intellectual property or customer data that is terribly interesting for attackers, but any employee data can be used for personal gain or for phishing. Employee data is the second most common type of data lost, and attackers may find that small companies have not properly built defenses, so that market provides an easy target for them. Small firms that have not recently examined their security practices would be wise to do so.

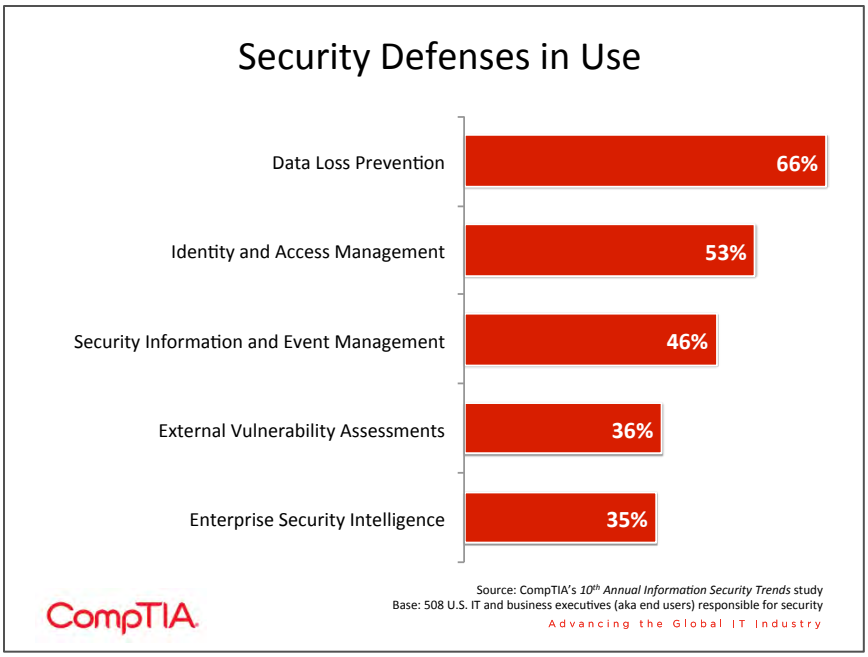
Before a robust data protection plan can be put into place, a company must understand the types and locations of the data it has on hand. Many companies have data siloes, as different departments have built data stores to serve their own needs. This data must be aggregated for analysis, and identification and organization also play a key role in security. Thirty-five percent of companies are at this identification/organization stage (while another 16% have no current data initiatives). From there, companies may move on to examining new sources of data (such as social streams or sensor data) and utilizing new Big Data tools for analysis.



Once data has been organized, a business can take steps towards preventing data loss. There are many actions a company might take, ranging from policy creation/enforcement to Data Loss Prevention (DLP) technology. Two thirds of companies are currently using DLP solutions, with another 22% planning to use them in the near future. Large companies lead current adoption, and small/mid-size companies show more intent to purchase.

Other Security Defenses

Aside from DLP, several other techniques have recently been gaining traction. These tools and methodologies address the changing nature of the security landscape and the growing complexity in managing organizational security.



Identity and Access Management: IAM technology basically turns perimeter security on its head: rather than giving end users the ability to get through the firewall, IAM recognizes a user and then gives them access based on their permissions.

One of the challenges of IAM is establishing the access rights for various groups. Outside of very small organizations (which likely do not have much need for IAM anyway), building individual permissions for every user is unworkable. Users must be placed into the group that best suits them, which will likely leave certain users unable to access specific pieces of data they may need. Beyond that, user needs are very dynamic, and it is difficult to keep up with the changing demands.

Another challenge is the way users are authenticated. IT staff that participated in CompTIA's *Trends in Enterprise Mobility* study identified a need for improved technology in the mobile security space. Identity authentication is certainly an example of an area that could use improvement. The standard user/password method is lacking, as evidenced by the large amount of advice available for choosing better password strategies. Two-factor authentication provides additional security, but it has its own issues and was only adopted by 1 out of 3 companies in this study. In the future, a field such as biometrics may provide much more accurate and secure methods for identifying users and tying them to the device being used. Global Industry Analysts predicts that the worldwide biometrics market will grow to $16.5 billion by 2017, fueled by improving technologies such as iris scans (projected to grow at 25.9% CAGR).

Security Information and Event Management: SIEM is a comprehensive solution that combines the functions of two previously distinct tools. Security Event Management (SEM) capabilities include the monitoring of events throughout a system, the correlation of events with known profiles or with each

other, and the reporting of events. Capturing this activity over time and performing analysis on the data is handled by Security Information Management (SIM). SIEM combines these functions in a single application that gives a security professional the ability to monitor the entire system and react to events as they occur.

SIEM technology has actually been driven by a desire to maintain compliance. Regulatory audits for areas such as HIPAA or FISMA often require logs showing what activity has taken place involving sensitive data. SIEM tools can provide this type of tracking information, so security teams have introduced SIEM as a way of supporting an organization's Governance, Risk management, and Compliance (GRC) policy. Similarly, SIEM functionality can assist with e-discovery or digital forensics. Once the solution is in place supporting these business functions, it can be extended to provide broader security coverage.

The biggest downside to SIEM is the amount of complexity involved in implementing the solution. With each area of a security scheme being relatively complex on its own, it is easy to understand the degree of difficulty in setting up a system that brings everything together. Proper training should be built into the plans, or a third party could be considered for SIEM implementation or operation.

External Vulnerability Assessments: This is a service provided by an outside company. A simulated external attack is performed on a business's public-facing systems through port scanning and attempts to exploit known weaknesses in web applications and operating systems. These weaknesses in public-facing systems can open paths to internal data. The service can be performed remotely and brings the benefits of additional security expertise as well as a new perspective from people who are not biased by legacy details.

Obviously, the assessment does not actually close the loopholes that may exist. A company will have to invest further to address any vulnerability that is found. A vulnerability assessment is also a snapshot of a firm's state of security. In a constantly shifting market, new assessments must be done on a regular basis. Some providers offer contracts for ongoing assessments, but the company requesting the service must carefully assess the value of repeat assessments against the costs incurred.

Enterprise Security Intelligence: ESI is a term originally coined by Gartner to describe the overarching management of many disparate security technologies and procedures. Staying ahead of external threats and maintaining control over internal data is becoming a major effort, especially for smaller firms without individuals that can focus solely on security. Few vendors offer products under an ESI label, though many offer dashboards that can give a view to their suite of tools.

It remains to be seen whether ESI will persist as a viable term, but a holistic approach to security will be important for businesses going forward. Section 4 of this report examines the dynamics taking place within companies as they change their approach, including deeper risk analysis as part of building a security scheme.

CompTIA

INFORMATION SECURITY TRENDS

SECTION 4: CHANGING SECURITY MINDSETS

RESEARCH

TENTH ANNUAL • NOVEMBER 2012

www.comptia.org

Key Points

- The majority of companies in this year's study have seen a moderate or drastic amount of change in their approach to security over the past two years. For the most part, this has been driven by a change in IT operations (such as a move to the cloud or a new mobility strategy). It could also be caused by a security incident, knowledge received through training, or a change in management.

- Many companies are familiar with the concept of risk management, but they may not be fully applying those concepts to security. Just over half (52%) of companies say they heavily use risk analysis within their security management. Without the ability to place all corporate information inside a secure perimeter, companies must consider the amount of investment they will place in securing various systems.

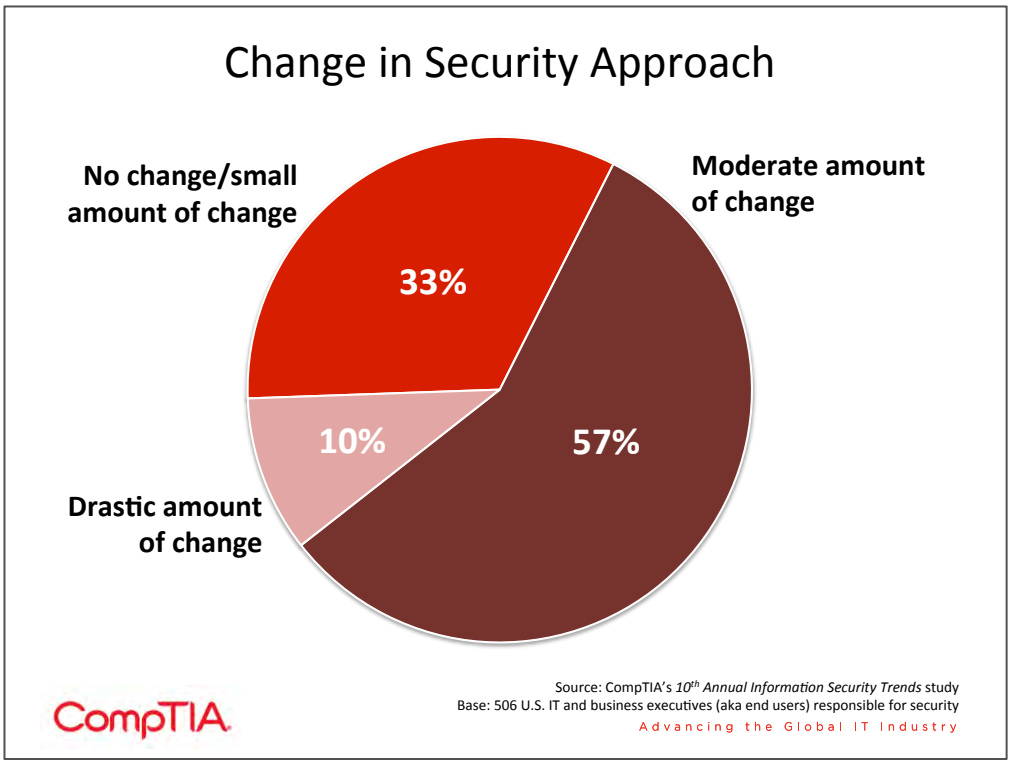
- When businesses consider security breaches they have experienced, they believe that 54% of the root cause is the human element. Security products may help monitor this to some degree, but companies must also consider how to educate their end users. This education should be ongoing and interactive, and companies should establish a baseline to measure against so that progress can be tracked.

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 really 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.

Over the past two years, two thirds of the companies in CompTIA's *10th Annual Information Security Trends* study have seen changes in their firm's approach to security. For a small percentage, there were drastic changes; but for the majority, the changes were moderate. Bearing in mind that survey respondents were all fairly involved in security at their organization, their view of moderate change may have been perceived as more drastic by employees in line-of-business departments.



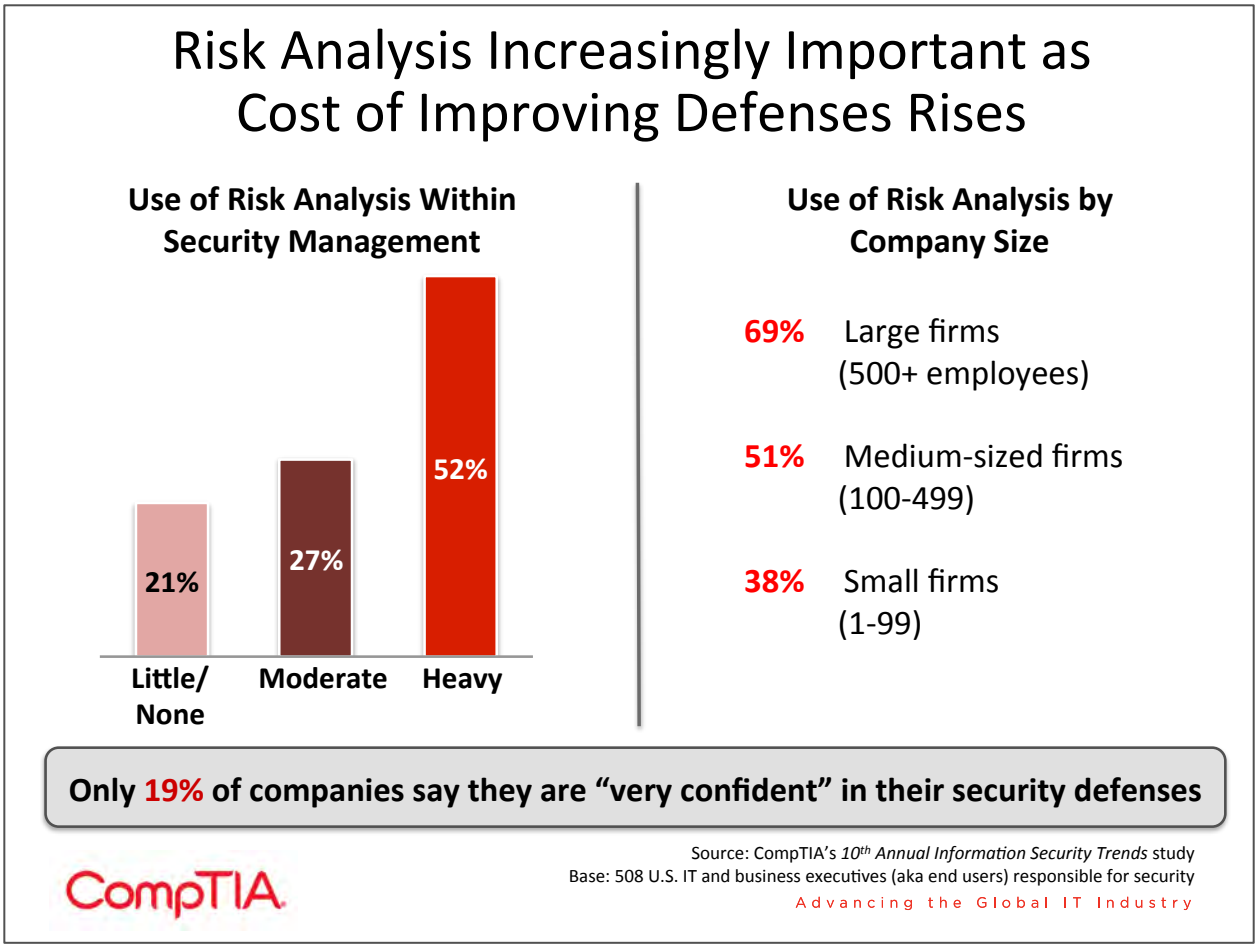
The main driver for new security approaches has been a change in IT operations—51% of the sample report that a move to cloud solutions or a new mobility strategy has been responsible for new security tactics. Reports of breaches at other organizations (44%) and internal security breaches (31%) were also popular drivers, highlighting the tendency of companies to react to security incidents. Other scenarios that influenced a new security approach included training or certification leading to new knowledge, a change in business operations, or a focus on a new vertical.

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 there are no corporate systems 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.

Similar cost structures apply to other aspects of security. Even though just 1 in 5 companies say they are "very confident" in their defenses, organizations are realizing that they cannot afford the investments necessary to become "very confident" in securing all their data in cloud and mobile environments.

As a result, companies are turning to other strategies that mitigate the risk in using certain technologies. A business may decide that certain types of data will not be candidates for cloud solutions. Corporate financial data, credit card data, and intellectual property are commonly kept on premise. Companies may also build private clouds to gain the benefits of the cloud model without the exposure of a public cloud provider.

One important note about risk analysis is that it 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.

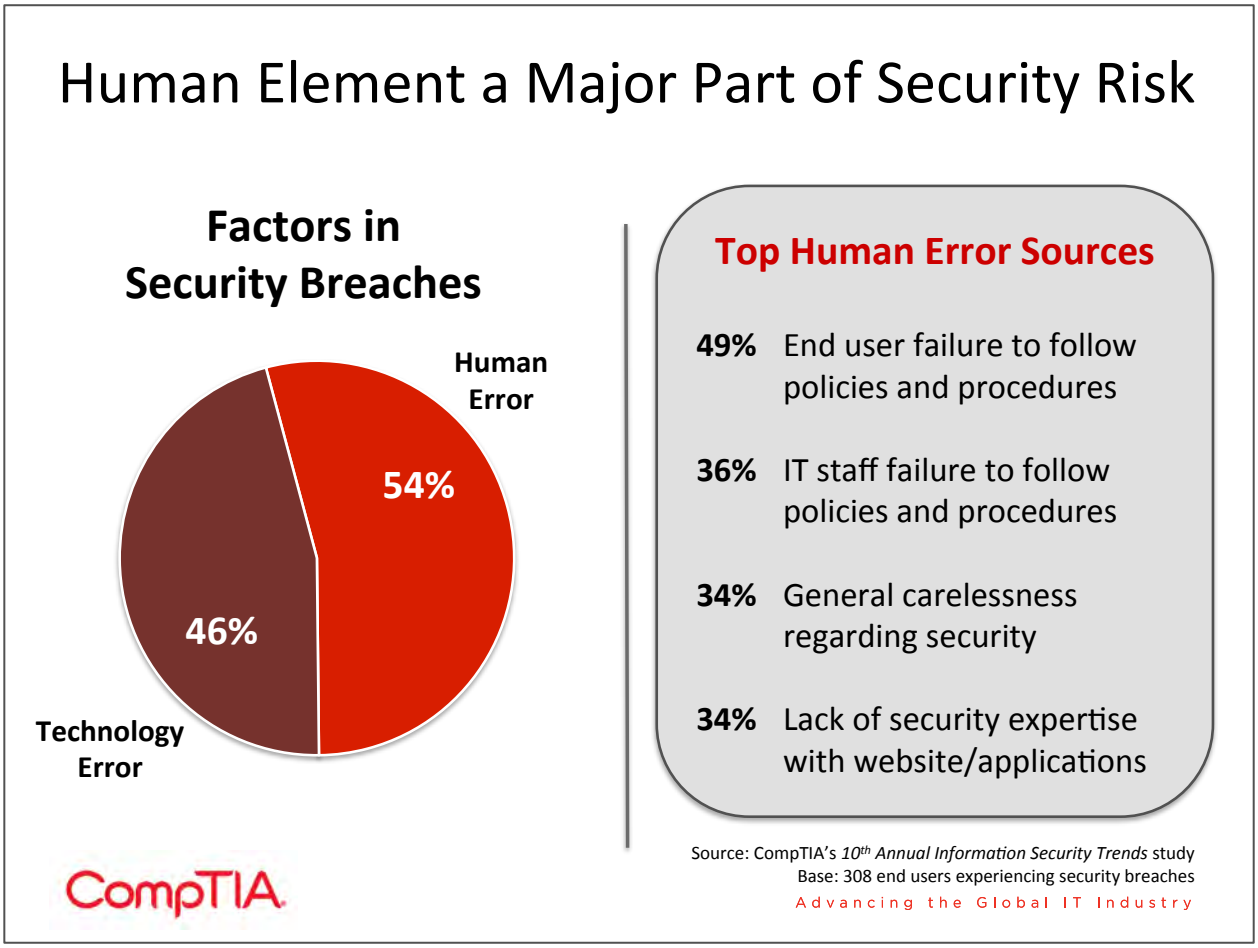
Stepping up End User Education

Cloud computing, mobility, and social media are all emblematic of the "consumerization of IT" trend. Section 2 of this report describes some of the actions that are taking place in the areas of cloud and mobility, but the threats from social media are not as easily addressed through provider reviews or device management.

The human element of security threats is steadily growing. 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.

What makes the human element especially hazardous is the fact that companies seem slow to recognize the magnitude of the risk. When asked about various security threats, respondents showed the highest levels of concern over threats coming from the outside (malware, hacking, and phishing). Concern over human error among end users or IT staff rated much lower. The data on trends over the past two years is even more surprising—over 70% said that human error had not changed or was less critical today.

These numbers are intriguing because they do not match up with the contributing factors to security incidents. As section 2 showed, companies acknowledge that human error has become more of a factor in breaches or data loss. Overall, the human element now accounts for 54% of the problem, up slightly from 52% in the *9th Annual Information Security Trends* study.



In some cases, the human element may be malicious, such as a disgruntled employee who has the access rights necessary to create a problem or steal confidential data. In most cases, though, the human error is unintentional—failure to follow procedure or a general lack of expertise, leading to inadvertent security missteps.

Technology is not able to completely solve this problem. Security tools are most effective in the hands of experts who understand the threats to the environment and the ways in which technology can guard against those threats. The dilemma for businesses today is that each employee needs to raise their level of awareness and expertise in security—not to the level of becoming a certified subject matter expert, but enough to understand some best practices.

End user education and training is the primary method for achieving this goal. This is a change in direction for many companies, who are accustomed to relegating security to their experts and merely providing capital expense budget for the tools that are needed. It is also a change for the IT department or solution provider in charge of security, as they now must find effective ways to distribute their knowledge to a wide user base.

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 will define corporate guidelines, processes will help maintain integrity, products will assist with 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.

Considerations for Security Training

- Training should be ongoing, as the nature of security threats changes regularly. This may be the most difficult aspect to explain to upper management if the typical view on training is that it is one-time or annual.
- Interactive training not only demonstrates concepts more clearly, it keeps training interesting for employees. Simulations of phishing or randomly placed "lost" thumb drives are good examples.
- It is important to establish a baseline and track metrics. For example, an initial phishing simulation may show that 40% of employees click on suspicious links. That number can be tracked through subsequent simulations to show progress.

CompTIA

INFORMATION SECURITY TRENDS

SECTION 5: CHANNEL PERSPECTIVES

RESEARCH

TENTH ANNUAL • NOVEMBER 2012

www.comptia.org

Key Points

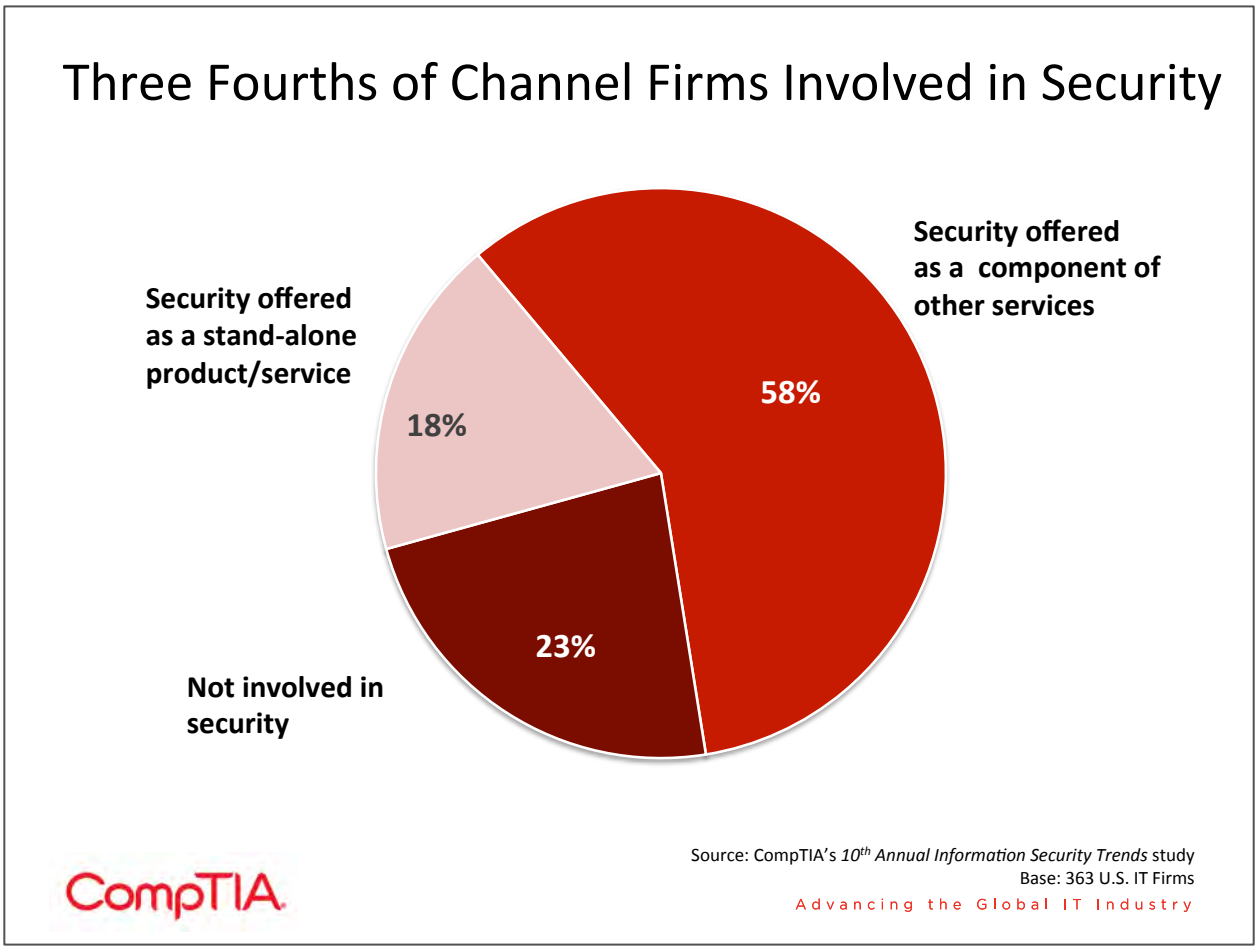
- Whether it is offered as a stand-alone service or integrated into other products or services, security is a stand-alone offering for more than three-fourths of channel firms. Security needs are growing more complex, as new technology trends such as cloud computing and mobility are more widely adopted and end users are taking more technology into their own hands, so there may be more of a need for companies whose exclusive focus is on security.

- Cloud security and mobile security are the areas where channel firms are placing the most focus over the next 12 months. The security topics covered by the most channel firms include network security (74%), business continuity/disaster recovery (71%), and data protection (70%).

- Sixty-six percent of channel firms involved with security expect their revenue to grow in the next year, with 16% expecting significant growth (10% or more). Many channel companies are considering ways to make security a recurring revenue stream, such as offering security products in the cloud or utilizing a managed services model to provide ongoing security or training for end users.

Security in the IT Channel

Previous sections of this report confirm the primary role that IT security plays in an organization. A broad range of CompTIA research shows that cybersecurity tops the list of strategic priorities for organizations year after year. Given the central role security plays, it is no surprise that more than three fourths of IT channel firms have some involvement in the delivery of security products and services to customers.



Among those firms that have an involvement in security, less than one in five consider security their primary business. For the majority, security is embedded – a component of other products/services they offer. The data shows that medium-sized channel firms (100-499 employees) are more likely to have security as a primary function than small or large companies or large companies. This may indicate that a medium-sized firm is the ideal size to tackle security as an exclusive focus. Smaller firms may not have enough staff to cover all the areas within security, and large companies may have a need to diversify beyond security in order to keep their business robust.

On one hand, this shows that security is a critical function that must be baked in to any IT consideration. On the other hand, there is a possible opportunity for channel firms to specialize in security as a way of differentiating themselves. Security, like general technology, is growing sufficiently complex to require overarching management by a party that understands various types of threats, defenses, and risk mitigation strategies.

This complexity can be seen in the list of services and products that IT firms currently offer. The choices range from specific security products to consultative offerings, showing that channel firms can be involved at a high level or down in the details.

Security Services/Products Offered by IT Firms

Security Product/Service	Currently Offering	Plan to Offer in Next Year
Network Security	74%	7%
Business continuity/Disaster recovery	71%	10%
Data protection	70%	8%
Email/web security	67%	6%
Encryption solutions	61%	13%
Risk management	57%	14%
Training/end user awareness	57%	15%
Intrusion prevention/detection	57%	12%
Compliance management	56%	13%
Identity and access management	51%	15%
Security information and event management	45%	16%
Cloud security	43%	**25%**
Mobile security	35%	**24%**

Source: CompTIA's *10th Annual Information Security Trends* study
Base: 275 U.S. IT Firms involved with security

Advancing the Global IT Industry

Cloud computing and mobility are changing the way that technology is used in the enterprise, and companies involved with security are responding to these shifts in technology and the ensuing requests from customers. CompTIA's *3rd Annual Trends in Cloud Computing* study found that security was the most common concern or objection from customers as channel firms pitched cloud services. While cloud security and mobile security represent the lowest currently offered services in the channel—indicating that these areas require a more holistic approach and are not as easily tied into specific products—they also represent the areas that most firms are planning to begin offering over the next year. Section 2 of this report details the security challenges end users face with regard to these trends, and channel firms should be sure to understand the unique challenges presented by these shifts in technology.

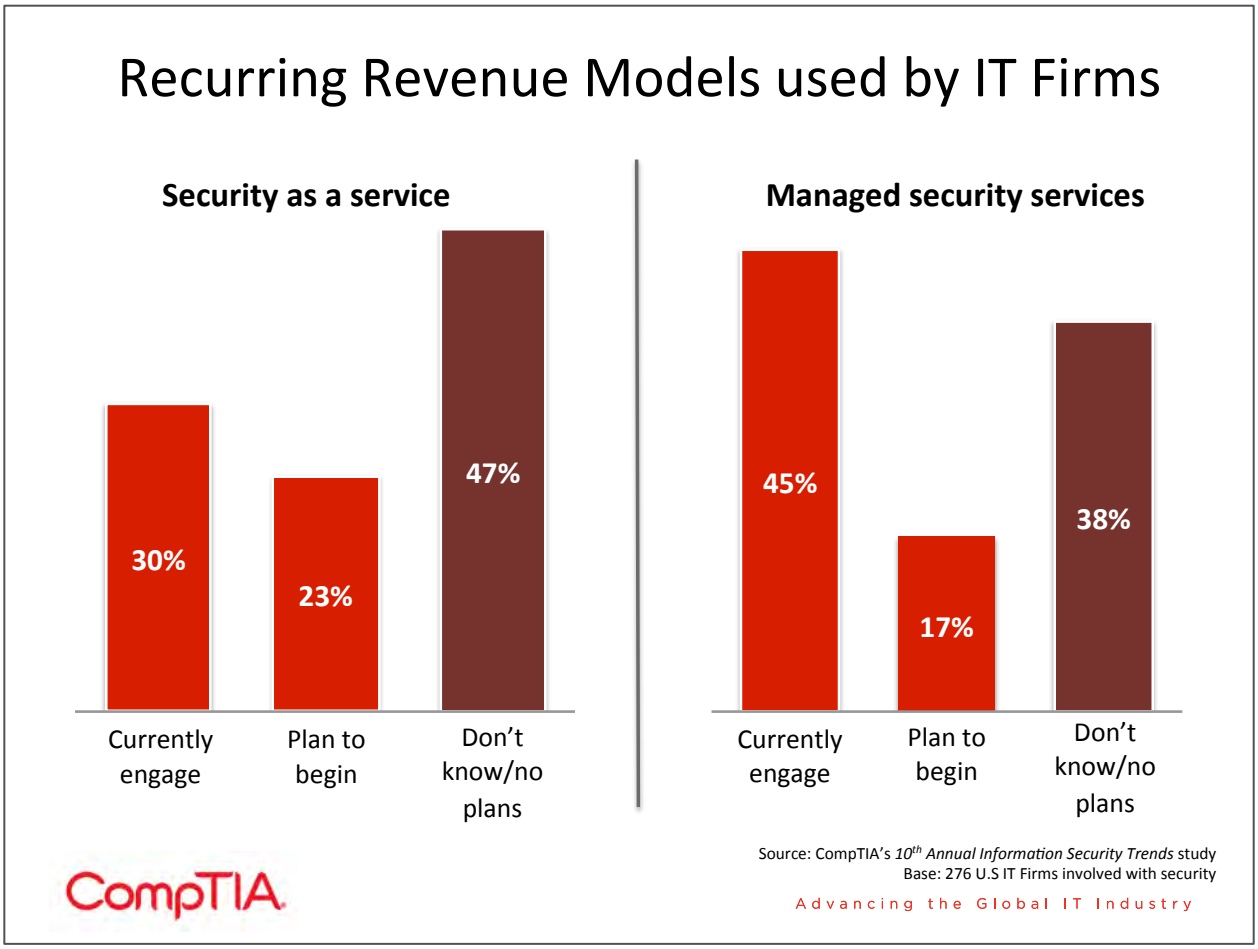
A review of the other offerings provides additional insight into the channel mindset on security. The focus on data loss prevention (DLP) matches up with the importance of data to business operations. CompTIA's *Big Data Insights and Opportunities* study showed that a net 87% of companies believe data is important to business operations. As noted in Section 3 of this report, solution providers have the opportunity to help companies understand the types and locations of the data it has on hand. Many companies have data siloes, as different departments have built data stores to serve their own needs. This data must be aggregated for analysis, and identification and organization also play a key role in

security. Once this data structure is understood, DLP is important for day-to-day operations and business continuity/disaster recovery is important for those times when operations are suddenly interrupted.

Risk management and end user training are fairly common offerings, but these may require channel firms to take a different approach as clients are also adjusting their views on these topics. Section 4 described how these areas are becoming an integral part of an overall security scheme. End user education in particular may undergo drastic changes in the coming years as companies consider the most effective methods for raising employee awareness on security issues such as phishing or social engineering. One-time education sessions may be replaced with ongoing, interactive training. This is an ideal opportunity for an outside firm, as most companies will not necessarily have in-house expertise in providing training to their workforce.

The Financial Side of Security

The continuing significance of security is also reflected in the fact that firms involved with security also expect revenue growth over the next year. Sixty-six percent of channel firms involved with security expect their revenue to grow in the next year, with 16% expecting significant growth (10% or more). Just 5% expect that security-related revenue will shrink over the next 12 months.



As with other trends in technology, channel firms are investigating ways to create recurring revenue streams with security. There are two principal models that channel companies are considering. First is 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 second model is to provide security as a managed service, using the lessons that have been learned from the general transition to managed services over the years. 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