RESEARCH REPORT

MARCH 2015

Trends in IT Security

CompTIA

About this Research

CompTIA's *Trends in Information Security* study provides insights into the behaviors, techniques, and opportunities associated with IT security as businesses use new technology. 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: Challenges
Section 3: Usage Patterns
Section 4: Workforce Perspectives
Section 5: Channel Dynamics

This study was conducted in three parts:

Part 1: Online survey focused on general security issues fielded to business executives and technology professionals during January 2015. A total of 400 companies based in the United States participated in the survey, yielding an overall margin of sampling error at 95% confidence of +/- 5.0 percentage points. Sampling error is larger for subgroups of the data.

Part 2: Online survey focused on security training issues fielded to business executives and technology professionals during January 2015. A total of 300 companies based in the United States participated in the survey, yielding an overall margin of sampling error at 95% confidence of +/- 5.8 percentage points. Sampling error is larger for subgroups of the data.

Part 3: Online survey focused on security offerings fielded to IT channel executives and professionals during October 2014. A total of 291 IT companies based in the United States participated in the survey, yielding an overall margin of sampling error at 95% confidence of +/- 5.9 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 and analysis. Any questions regarding the study should be directed to CompTIA Research and Market Intelligence 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.

SECTION 1:

Market Overview

CompTIA

Key Points

- While it has always been an important field, IT security is growing even more critical as businesses place more reliance on digital processes. The field is also showing healthy growth, with Gartner expecting final 2014 revenue for global security to hit $71.1 billion.

- The level of concern shown over various threats reflects both the historical mindset and the need for new action in the future. Malware and hacking are still the top threats causing concern, with nearly half of all companies citing these as serious concerns. Other areas such as social engineering or human error are growing as concerns but may still require education to understand the true impact and mitigation strategies.

- Pushing the importance of security is not the best avenue for security discussions as most firms agree that security is important. Instead, there should be a focus on other actions that have triggered security changes at various organizations, such as new IT operations (47%) or knowledge gained from training (34%).

The IT Security Market

The IT landscape has shifted dramatically in the past five years. Not only are businesses exploring new models for technology, such as cloud computing and mobility, but they are also viewing technology more as a strategic endeavor that can directly accelerate growth. These two drives are somewhat complementary to each other, but the dual pursuit definitely creates a more complicated picture for businesses as they consider their IT strategy.

In this environment, IT security is gaining even more prominence than it has held in the past. The two technology pursuits create a perfect storm for security: with new models, there are new loopholes to exploit; and with greater technology reliance, there is a greater potential for disruption. Add in escalating privacy concerns and critical regulatory concerns, and it is easy to see how IT security is becoming much broader than firewalls and anti-virus software.

In fact, there is a good argument for security becoming its own discipline within a business rather than an embedded function of IT. This is already happening in part at large enterprises that have someone in a role of chief security officer (CSO) or chief information security officer (CISO), and the movement towards a fully contained discipline can be seen in IDC's prediction that 75% of these roles will report directly to the CEO by 2018. This thinking will gradually work its way into medium-sized and small businesses, who will be looking to bring in dedicated security expertise or work with a third party focused completely in this area.

Businesses are certainly bringing in the skills to form these self-contained teams: data from job aggregator Burning Glass shows that the number of postings for information security analysts grew 73% between Q4 2013 and Q4 2014. Although the base number of jobs is not as high as other technical fields, this is by far the greatest growth across all of Burning Glass's categories. Looking forward, the Bureau of Labor Statistics predicts that information security analysts will be the fastest growing job category,

Changes to the CIA of Security

IT security has always been a complex field, as shown by the three distinct areas that have traditionally defined an organization's approach. A quick overview of concerns in each of these areas shows how the complexity is rising.

- **Confidentiality:** In the past, keeping data confidential involved placing all sensitive data behind a secure perimeter and ensuring the strength of that perimeter. Now, mobile devices are making a secure perimeter impossible, and companies must consider protection of the data itself at a much more granular level.

- **Integrity:** Keeping consistent data sets is important for efficiency and advanced analytics. As businesses explore big data opportunities, they are finding that many data silos exists and must be consolidated even as new streams of data are rapidly being introduced.

- **Availability:** With in-house systems, companies have a greater degree of control over establishing redundancy and responding to outages. Moving systems to cloud providers requires a complete rethinking of redundancy, and companies must also deal with elevated expectations for system uptime.

with 37% overall growth between 2012 and 2022.

Worldwide spending forecasts are another signal that security is more of a growth area than some might imagine. Gartner expected global security spending to hit $71.1 billion in 2014, a 7.9% increase over 2013. Compare that to overall IT spending, which Gartner projects to grow at 2.4% in 2015, and it is apparent that security is not a commoditized part of the IT equation. Forecasts of individual parts of the security ecosystem provided by MarketsandMarkets illustrate how much activity is taking place across a wide range of security efforts:

- **Identity and Access Management (IAM):** $18.3 billion by 2019
- **Physical Access Control:** $10.4 billion by 2020
- **Enterprise Firewall Market:** $8.4 billion by 2019
- **Mobile Security Market:** $5.8 billion by 2019
- **Encryption Software:** $4.8 billion by 2019
- **Data Center Logical Security:** $3.2 billion by 2019

The complexity that businesses must consider for their security approach is directly related to the complexity of attacks that are occurring. Thanks to new technology models, new behaviors, and new motivations, attackers are employing many new methods for stealing data and disrupting operations.

Level of Concern over Security Threats

	Level of Concern		Change in Concern	
	Moderate	Serious	No change/less critical today	More critical today
Malware	37%	50%	51%	49%
Hacking	38%	49%	54%	46%
Privacy	36%	45%	62%	38%
Data loss/leakage	42%	40%	66%	34%
Social engineering/phishing	41%	38%	58%	42%
Understanding risks of emerging areas	43%	36%	61%	39%
Lack of budget/support	34%	34%	72%	28%
Physical security	42%	33%	71%	29%
Regulatory compliance	37%	32%	75%	25%
Insider abuse	35%	31%	75%	25%
Human error among general staff	52%	30%	74%	26%
Policy enforcement	38%	29%	74%	26%
Formal risk assessment	46%	28%	73%	27%
Human error among IT staff	41%	27%	80%	20%

Source: CompTIA's Trends in Information Security study | Base: 400 U.S. end users

The level of concern shown over various threats reflects both the historical mindset and the need for new action in the future. Malware and hacking are the top areas of concern. These are very traditional

focus areas, both are certainly happening today at high volume. The most recent quarterly overview report from security firm PandaLabs estimated that 20 million new strains of malware were created in the third quarter of 2014 alone.

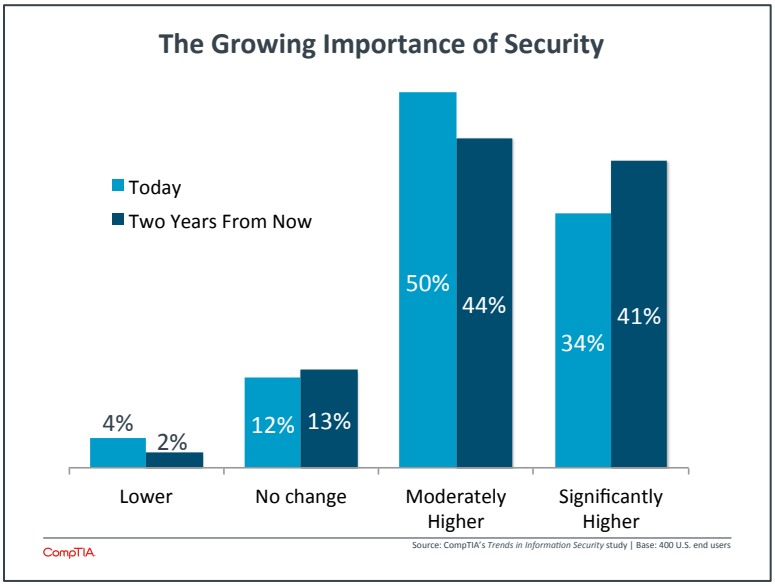
Beyond these two areas, though, there are a great many threats that should raise nearly the same level of concern. Physical security is becoming more critical as mobile devices become bigger targets for theft. Regulatory compliance plays an important role for more and more companies as more business is done via the Internet. Human error ranks low as a serious concern, but companies report that it is the largest factor behind security breaches (see Section 4 for more detail).

There is a silver lining in all the chaos. Compared to 2013 data, the percentage of companies rating an item as causing serious concern rose across the board for all categories except malware, which still commands the top spot. Companies are beginning to realize the broad difficulties in building a strong security posture. The big question now is what action they will take.

Getting Motivated to Change

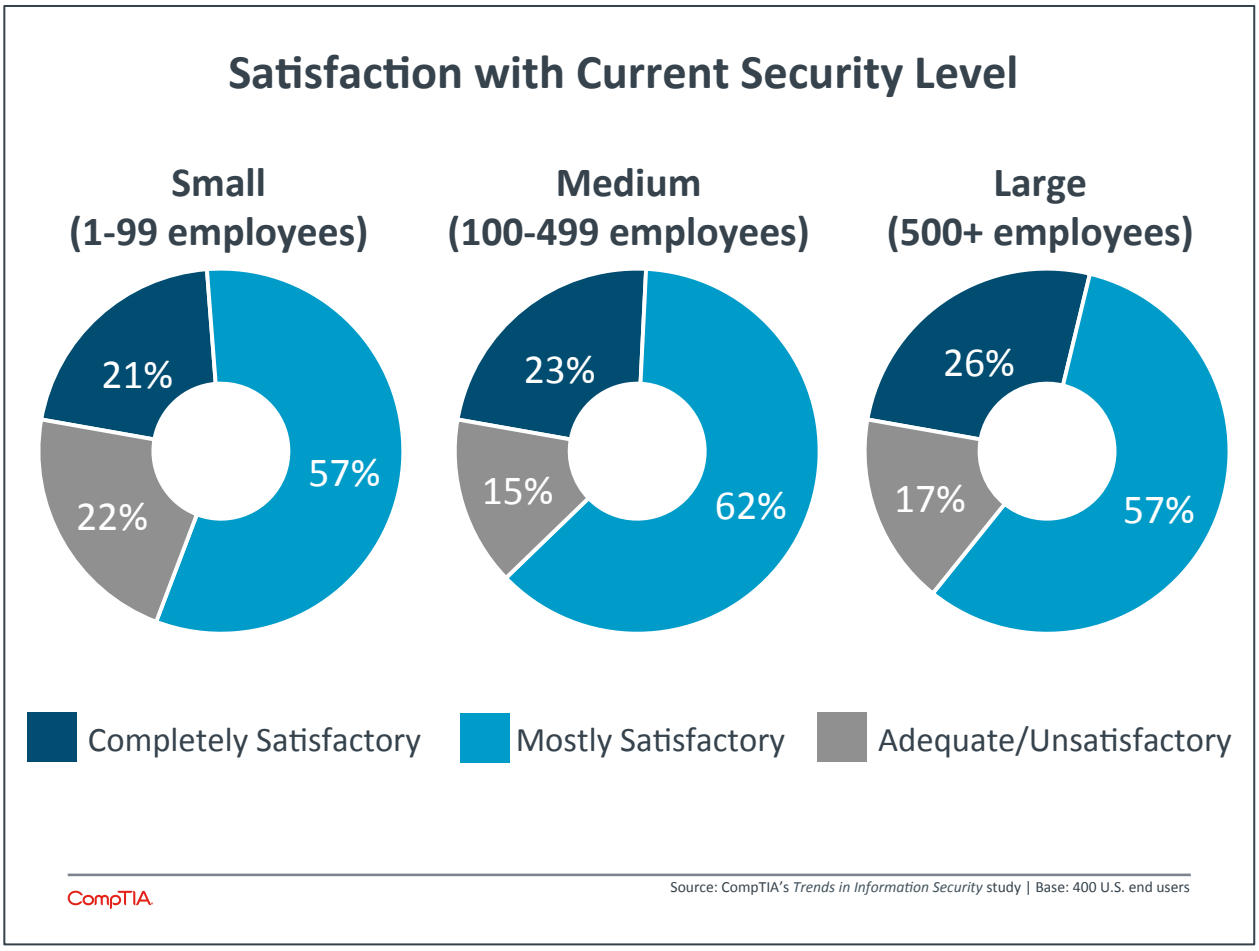
To say that security is a top business concern seems unnecessary. IT security has existed for as long as there has been an IT function, and most companies understand that it is not something to be taken lightly. Indeed, 74% of firms in CompTIA's survey say that security has a higher priority today than it did two years ago, and 85% say that it will have an even higher priority two years from now. These results are fairly consistent across different sized companies; medium-sized companies are actually most likely to indicate security as a higher priority, likely due to growing operations requiring revamped security.

The problem in discussing security as a top priority is that there is a difference between stating a priority and knowing which action to take. Consider the big security breaches that have happened over the past two years. Target, Home Depot, eBay, JP Morgan Chase, and Anthem all likely placed a high priority on security, but there were still faults that led to the theft of more than 50 million records for each company. Furthermore, these faults were not the result of a move into new technology. Instead, they were often routine mistakes in areas that are well-known security danger zones.



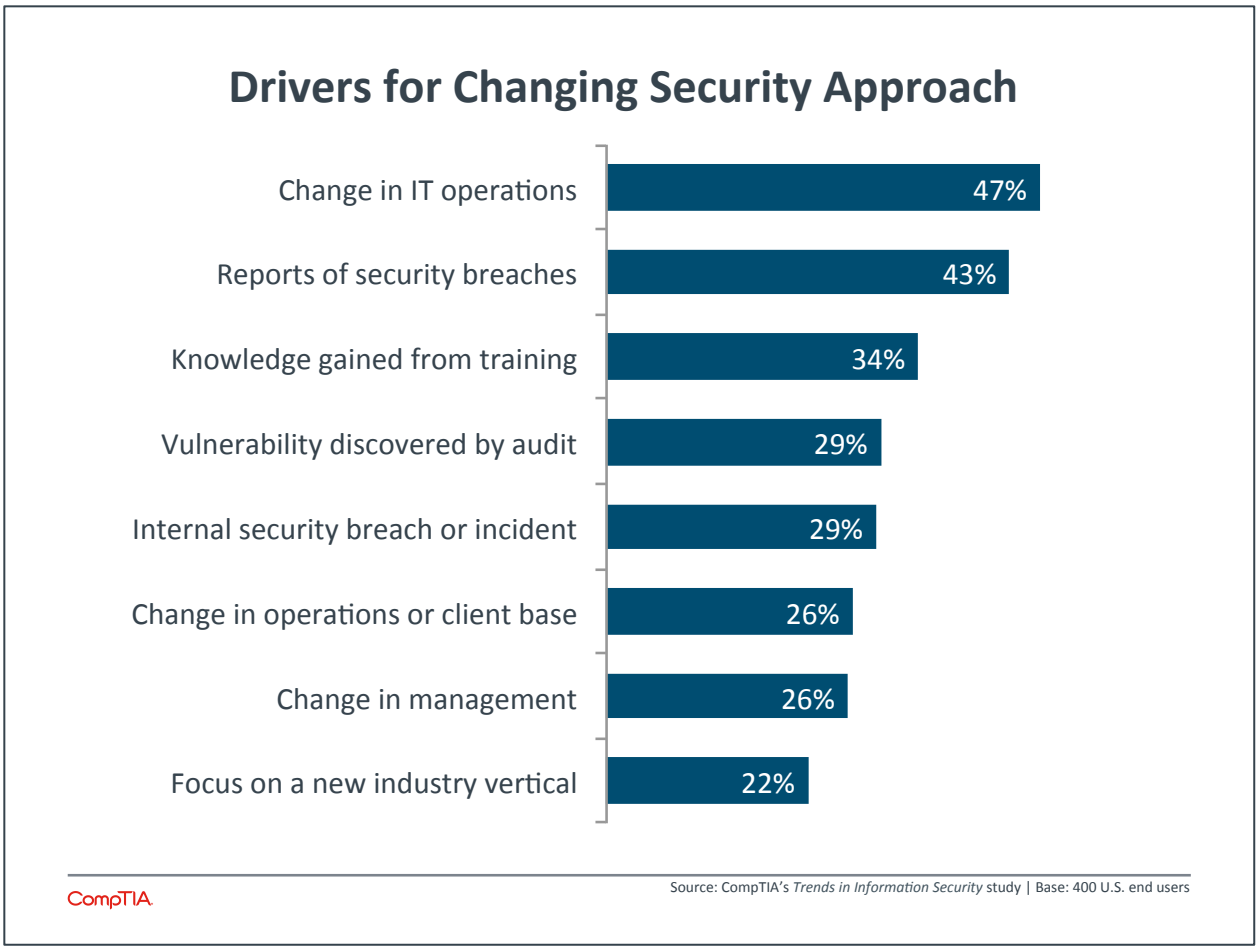
The first step in knowing what action to take is acknowledging the need for such action. While companies strongly rate security as a top priority, they also have a strong sense that their current security is sufficient. Across company size, the sentiments are fairly consistent, with a minority of firms feeling that their current security is simply adequate or unsatisfactory in some way.

Medium-sized companies are the most confident in their current level of security. In some cases, these firms have taken the necessary precautions to improve their security. In many cases, though, these firms may be relying on a belief that their security is satisfactory because the threat level is low based on the relative importance of their data compared to large enterprises. In reality, attacks in the SMB space are occurring at the same frequency as the enterprise space, not because the data is valuable but because the defenses are low.



The situation, then, is not that businesses need to be convinced that security is important. Instead, they need to be convinced of the ways that their current security approach may be putting them at risk. One of the most common triggers for improving security is having a security breach occur within the organization. However, there are other triggers that may act as a good checklist for firms that believe they are in a good position.

It is not surprising to see that a change in IT operations is the most common trigger, since cloud and mobility create such drastic changes to process and IT architecture. It is more of a surprise to see that less than half the sample reports this as a driver, though. Adoption of cloud and mobile solutions is much higher than this, so there should be many more companies considering how a new IT strategy creates new security issues.



Security training is becoming a major initiative for many businesses for two reasons: keeping the technical team up to speed with the dynamic environment and keeping general staff from creating unnecessary risk as they use technology more in their day to day jobs. One third of companies are seeing an additional benefit—the training they are pursuing leads to new knowledge that changes the organizational mindset.

A final trigger to highlight is any vulnerability discovered by an external audit. Having an audit done is a move that many companies may not be considering, but there is good reason to believe that this could become a best practice for all businesses in the near future. An external firm will bring specialized expertise and unbiased scrutiny, and an audit can provide a baseline for measuring security readiness—a metric that most firms base on whether or not they have had a security incident.

With the IT function entering a new phase following the introduction and adoption of cloud and mobility, IT security sits at a critical juncture. Many IT observers and analysts (including CompTIA) have predicted that 2015 will be a year when IT security is transformed. From the technical methods to internal process to organizational training, there are many ways in which this change could take place and many areas of opportunity for IT firms looking for new ways to serve their clients.

SECTION 2:

Challenges

CompTIA

Key Points

- There are many factors contributing to growing complexity in the security space. These factors are both external (e.g. the growing organization of hackers) and internal (e.g. greater interconnectivity of systems and devices). Businesses must begin considering new approaches, as old approaches will not address this complexity.

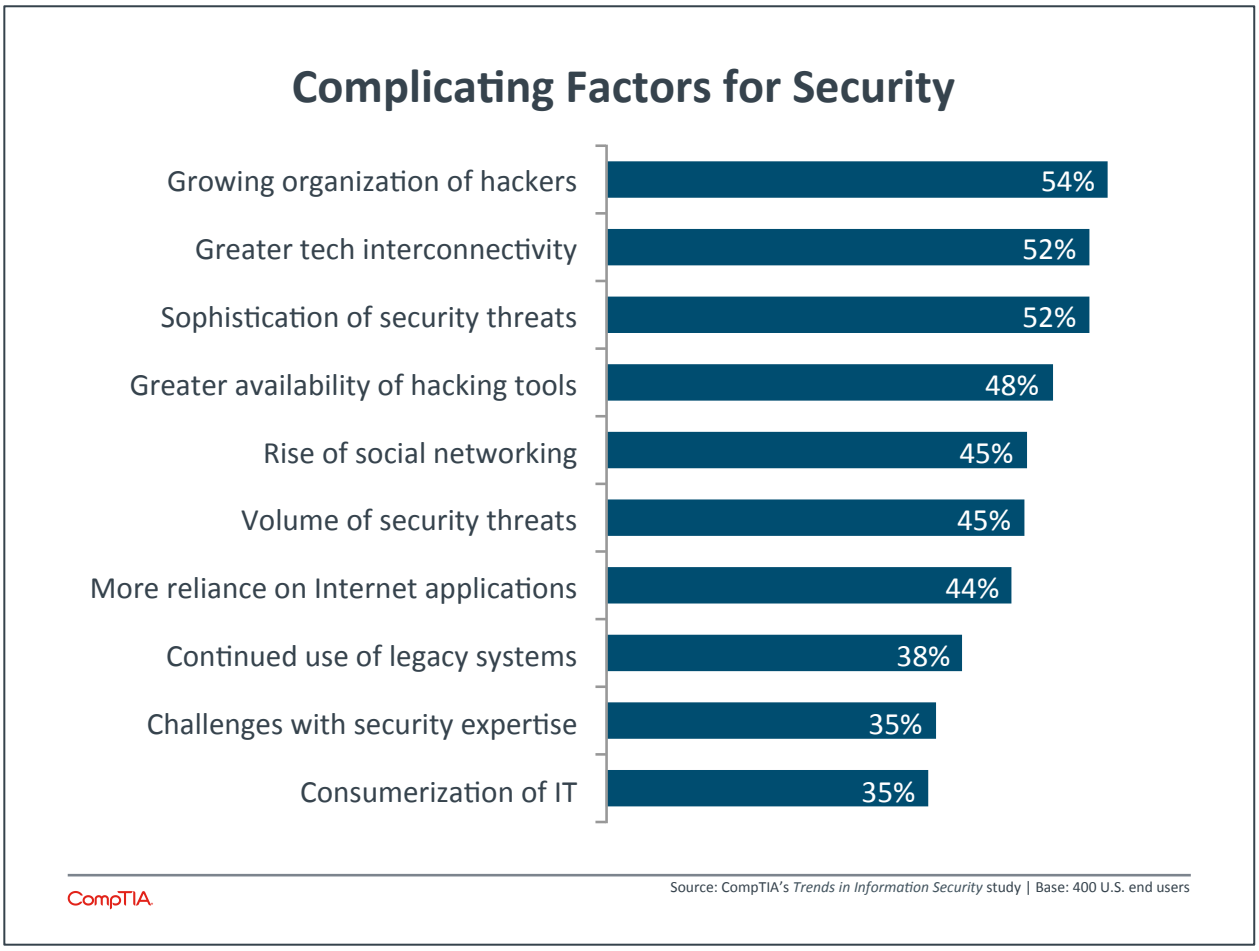
- Data is perhaps the prime area where a shift in security mindset must occur, as data now routinely travels outside a company's secure perimeter. Twenty-nine percent of companies say that they have definitely had a data loss incident in the past year, up from 19% in 2013.

- As more companies move to cloud computing, there continues to be a need for more thorough reviews with cloud providers. Many companies may not fully understand their own security baseline, which is a requirement before understanding what a cloud provider offers for security.

- Lost devices are no longer the sole mobile security incident companies are guarding against. In the past year, companies have also seen employees disable security features on mobile devices (31%) and experienced mobile malware (30%).

A Complex Security Situation

In considering how to alter their approach to security, businesses have a great many factors that they must take into account. There are new influences shaping security as businesses consider new technology usage and attackers employ new methods. Overall, no single factor stands out as the primary complication, showing how important it is to broadly consider the entire landscape when creating new tactics.



The growing organization of hackers and the greater availability of hacking tools carry two implications that create concern for businesses. First, attacks can be more dynamic, changing rapidly and targeting with greater efficiency thanks to pooled resources. Second, attacks have new motivations, as political groups or random troublemakers can create havoc without necessarily having to build expansive technical skill. Both of these concerns weigh heavier on SMBs, who have fewer resources of their own to apply to the problem and who now find themselves increasingly being targeted thanks to weaker defenses.

Moving forward with defenses can be hampered by existing infrastructure and skills. Legacy systems may rely on a notion of perimeter security and not be good candidates for moving to a cloud environment. Security skills also may be geared more towards a company's current setup, and those skills are likely concentrated within an IT function rather than being spread throughout the organization.

Lines of business feel these constraints most keenly, as they are anxious to explore new technology but do not yet have the right set of skills within the department to ensure safety.

Beyond the changes in attacker capability and concerns over changing the existing configuration, the complications for security are due to the new technology that businesses are exploring. Interconnectivity of devices and users is a result of mobility initiatives. The rise of social networking creates both a new platform for potential breaches as well as a new mindset for information sharing that can lead to unintentional leaks. A greater reliance on Internet applications is a direct result of moving systems to cloud providers in the quest for greater agility. These new technologies certainly contain a great deal of potential, but they also create problems that must be solved quickly before they are exploited.

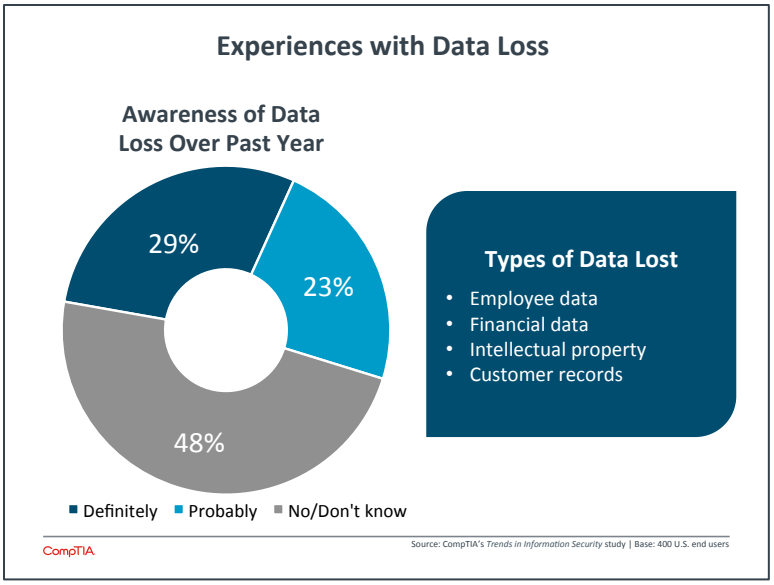
It would appear that companies are rapidly bringing in new security technologies to go along with the new business technologies they are using. Data Loss Prevention (DLP) is still one of the most common new tools, currently in use by 58% of companies. Identity and Access Management (IAM) and Security Information and Event Management (SIEM) both took substantial leaps since 2013, with IAM going from 47% adoption to 57% adoption and SIEM going from 37% adoption to 49% adoption.

Keeping an Eye on Data

Perhaps the biggest shift in mindset that needs to occur for improved security is the way in which data is viewed and handled. In the simplest comparison, a company that maintained all of their own systems and applications behind their own corporate firewall would view data simply as a byproduct of those systems, and if the systems were kept safe through maintaining a strong perimeter, then the data was safe.

Data now travels easily outside the physical and virtual borders of a company. Migrating systems to cloud providers obviously moves the data under external control, and mobile devices can potentially carry data even if the backend system is in-house. This drives a need to secure the data itself, a task that is more complicated as data goes through different phases (at rest, in transit, or in use).

As companies move towards a data-centric mindset, they often find that their data practices require improvement. CompTIA research has found that companies have a high incidence of data silos, and this incidence is actually rising as companies take a closer look at how their data is being stored and managed. These silos make it difficult to perform comprehensive analysis, and they also make it difficult to fully grasp which data exists or to generate a single customer view.



Compared to 2013, more companies are admitting to data loss incidents. Two years ago, 56% of firms claimed

that data had not been lost or that they did not know whether or not data had been lost. In addition, just 19% of companies at the time said that they definitely knew of data loss or leakage over the previous year. Just as a closer concentration on data leads to more awareness of data silos, it is also creating greater awareness of when data has been compromised. By a fairly wide margin, small companies are the least likely to believe that data has been lost, indicating a lower level of focus. As with any data-based initiative, data audits are a good place to start when working with small companies to reduce their exposure to data loss.

The fact that employee data is the most likely type of data to be lost is a further signal that hacker motivations have changed. Attacks on larger companies tend to be more focused on financial data, intellectual property, or customer records, all of which can have direct monetization potential for attackers. Employee data, though, is more likely to be a means to an end, such as using the data gathered for a phishing attack on a bank or some other larger target. Companies of all sizes experience the loss of employee data at high rates, with medium-sized businesses leading the pack.

To better protect data, companies are considering a wide range of actions. The top anticipated action is a stricter separation of work and personal devices. This flies in the face of the notion that most companies will be forced into a BYOD model, and other data points and anecdotes throughout the business world further support the idea of business maintaining majority control over devices used for work purposes. Other potential actions to stem data loss include creating or reinforcing company policy regarding social networks (49%), creating or reinforcing company policy around device safety (47%), and encryption of files on mobile devices and portable media (47%).

Got DLP?

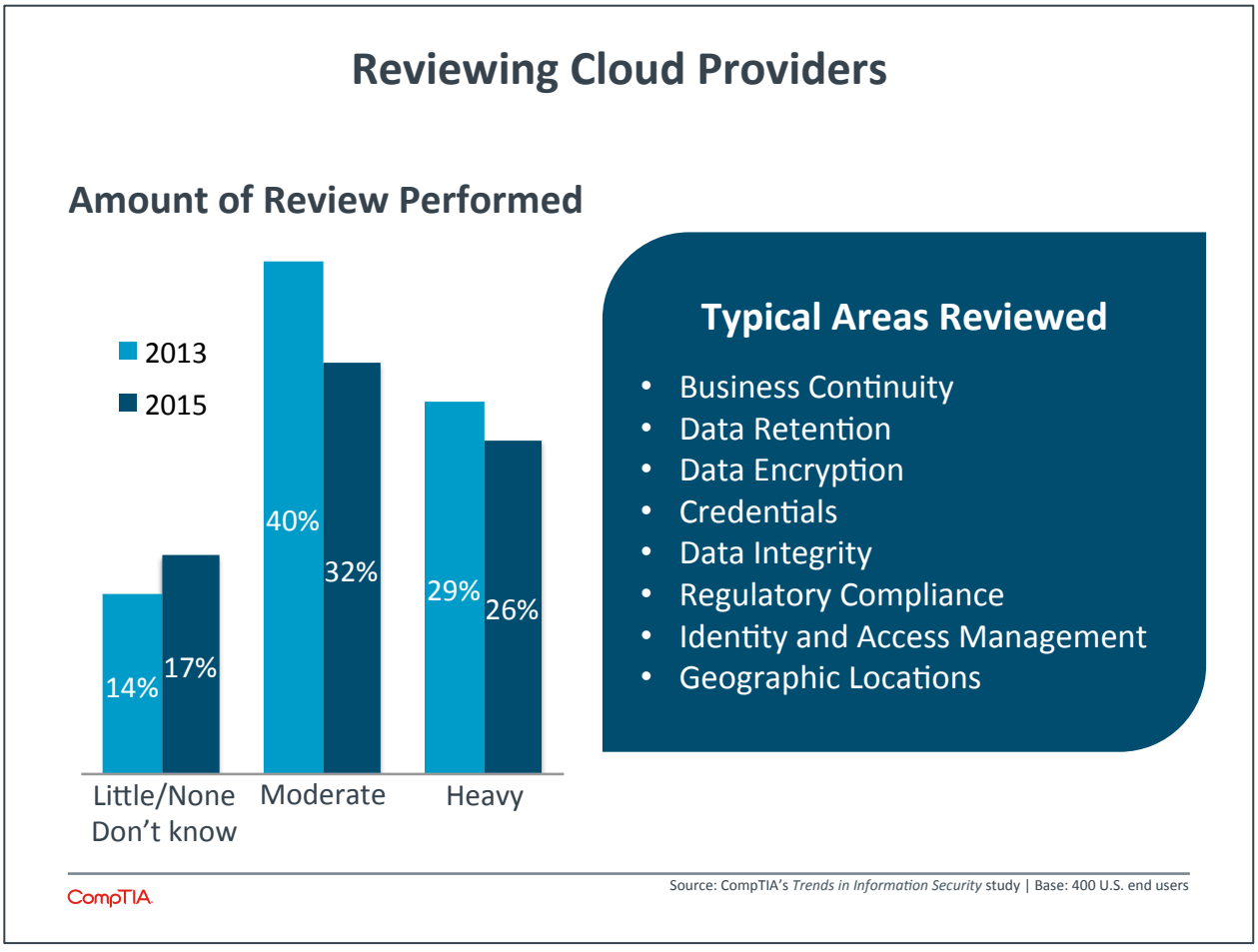
Although 58% of companies claim to have a DLP solution in place, this is probably not a true representation of robust data protection. Espo Systems is a security solutions provider in Illinois that is seeing a growing demand for these tools. “Our vendors are throwing all their weight behind DLP solutions” says Nick Stricker, VP of ESPO Systems Websense business unit. “Fields like firewall or antivirus are saturated, but data is a greenfield opportunity.” For all the demand, though, many companies may be fooled into thinking they have full data protection by a tool liberally using the DLP label. Brian Gardner , director of ESPO Systems Proofpoint business unit, notes that “some tools claim DLP capabilities, but they only look for basic information like credit card numbers or social security numbers.” A more robust DLP solution can track whatever data a company might choose to identify, and a staged installation will help firms realize what that data should be and just how much is leaving the company walls. A typical DLP setup will start with monitoring, where the tool will simply observe network traffic to understand how data is moving. The next phase is detection, where users can be notified if they are about to send suspicious data and choose whether to continue or abort. Finally, the tool can be configured to block any sensitive data that should not be shared by email or copied to external memory. This is a far more robust approach than many tools’ so-called DLP features, and it is worthwhile to dig into data protection strategies to understand the true extent of a company’s defenses. Of course, no solution can completely prevent data loss. “There’s nothing out there yet that knows when people are taking pictures on their cell phones” says Gardner.

Understanding Implications of Moving to the Cloud

Aside from data concerns, the migration of systems into the cloud creates several issues for companies, especially if they have not carefully considered their security requirements before engaging with a cloud provider. In the early days of cloud adoption, security was often cited as the primary reason that companies were not using cloud systems. Today, the vast majority of companies have cleared that hurdle, either by thoroughly examining security in a cloud environment or by assuming that mass adoption of cloud systems indicates adequate security.

That assumption is obviously not the best way to move to the cloud, as companies will find that security concerns, while solvable, still exist. Following an initial cloud migration, many companies have made some sort of secondary move for security-related reasons. This could be moving from a public cloud to a private cloud (36%), moving from a public cloud to an on-premise system (31%), or moving from one public cloud provider to another (30%).

Secondary migrations imply that there are some lessons being learned following a migration that could have been avoided with a proper review of a cloud provider's policies. Again, this review requires that a company understand its own security requirements up front, but once that understanding is in place, a thorough review of potential providers can help avoid confusion or additional work.



The reason it is so important for companies to understand their own security requirements before engaging with a cloud provider is that there are so many different areas involved to ensure safety and reliability. Across the board, the percentage of companies saying they always review each of the items listed in the chart above has risen over the past two years. The distribution is also fairly tight, with 40%-60% of companies saying they always review each area. Businesses are recognizing the importance of conducting reviews and the breadth of issues that a review should cover.

Going through the process of understanding security requirements and reviewing cloud providers can drive internal changes as well. Forty-eight percent of companies say that they have changed company policy as a result of changing views on cloud security, and 41% have built additional security features into cloud-hosted applications. Moving to the cloud does not just require additional security measures to close gaps that exist in the cloud provider, it also requires changes to application architecture and business workflow, and these changes often prove more challenging to implement than system migration.

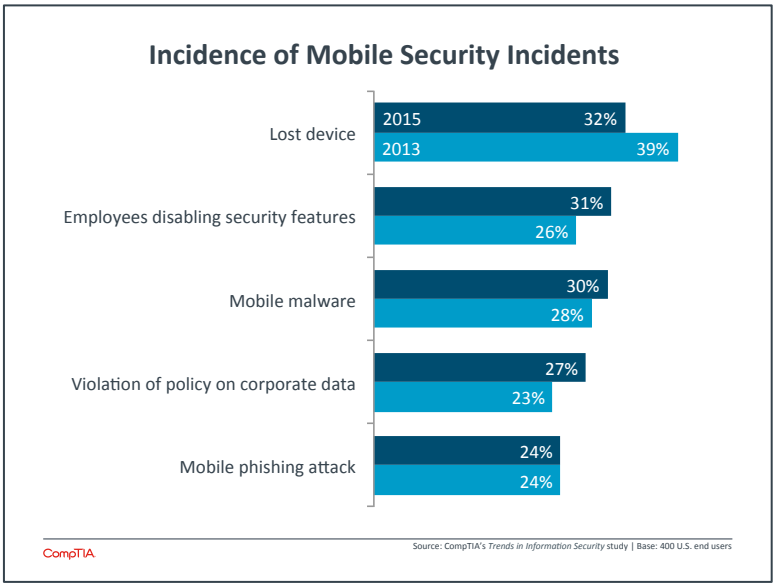
Taking Mobility Security Beyond the Device

As recently as three years ago, the primary mobile security incident that companies were worried about was a lost device. With smartphones and tablets more portable and more desirable than laptops, losing a device was at the very least annoying because of the time and energy for replacement. At worst, it could have represented a serious security breach if there was confidential corporate data stored on the device.

BYOD made matters more complicated. As employees were either pushing IT to allow their personal devices to be used for work or simply finding a way to make it happen, the ability to place any type of corporate tracking software or anti-virus protection seemed to be up in the air. Businesses wanted the productivity that mobile devices offered, and consumer technology was pushing the technical envelope, widely available, and moving very fast.

Now, the mobile security picture is beginning to resemble a typical enterprise security mindset. Even in 2013, the types of mobile security incidents that companies were seeing had more balance. The most recent data shows that mobile malware continues to rise and end user issues are also occurring more frequently.

Medium-sized companies are the most likely to report any type of mobile security incident, and this ties into the latest shifts in the BYOD space. There is a growing sense that companies are finding ways to pursue mobility strategies without opening themselves up to the dangers that come through BYOD. Mobile devices and mobile operating systems are becoming more enterprise-friendly, and businesses are able to provide desirable devices while still maintaining control. This is happening most often at large



companies, explaining the dip that they are reporting in mobile security incidents.

For small companies, the range of mobile security threats pushes the complexity beyond the capabilities that exist. Even being aware of the different range of threats demands bandwidth that may not be available (see Appendix). The same resource constraints that prevent a good understanding of the mobile threat landscape prevent strong policies on device management, so BYOD proliferates the most among small companies. The risks are high, and there is real opportunity among these firms for education, products, and services.

Getting started with mobile security does not have to be a costly endeavor. While the most common action that businesses take as a result of a mobile security incident is to purchase and install tracking or wiping software for mobile devices, the next four actions cost nothing and simply require an understanding of best practices.

The data also shows that mobile security still has a long way to go. As with cloud migrations, the companies on the leading edge are finding that deeper changes are needed to fully implement a secure environment that includes mobile devices. For example, companies may use new methods such as virtual desktops for accessing company data. However, only 33% of companies are exploring this type of option. As businesses continue their pursuit of cloud- and mobile-based technology to drive revenue and growth, they will find that proper security goes far beyond patching the existing strategy and stretches into a complete re-imagining of security practices.

Actions Taken to Increase Mobile Security

45% Install tracking/wiping software

44% Require passcode on mobile devices

41% Establish procedure for lost devices

39% Require encryption on mobile devices

35% Begin building formal mobility policy

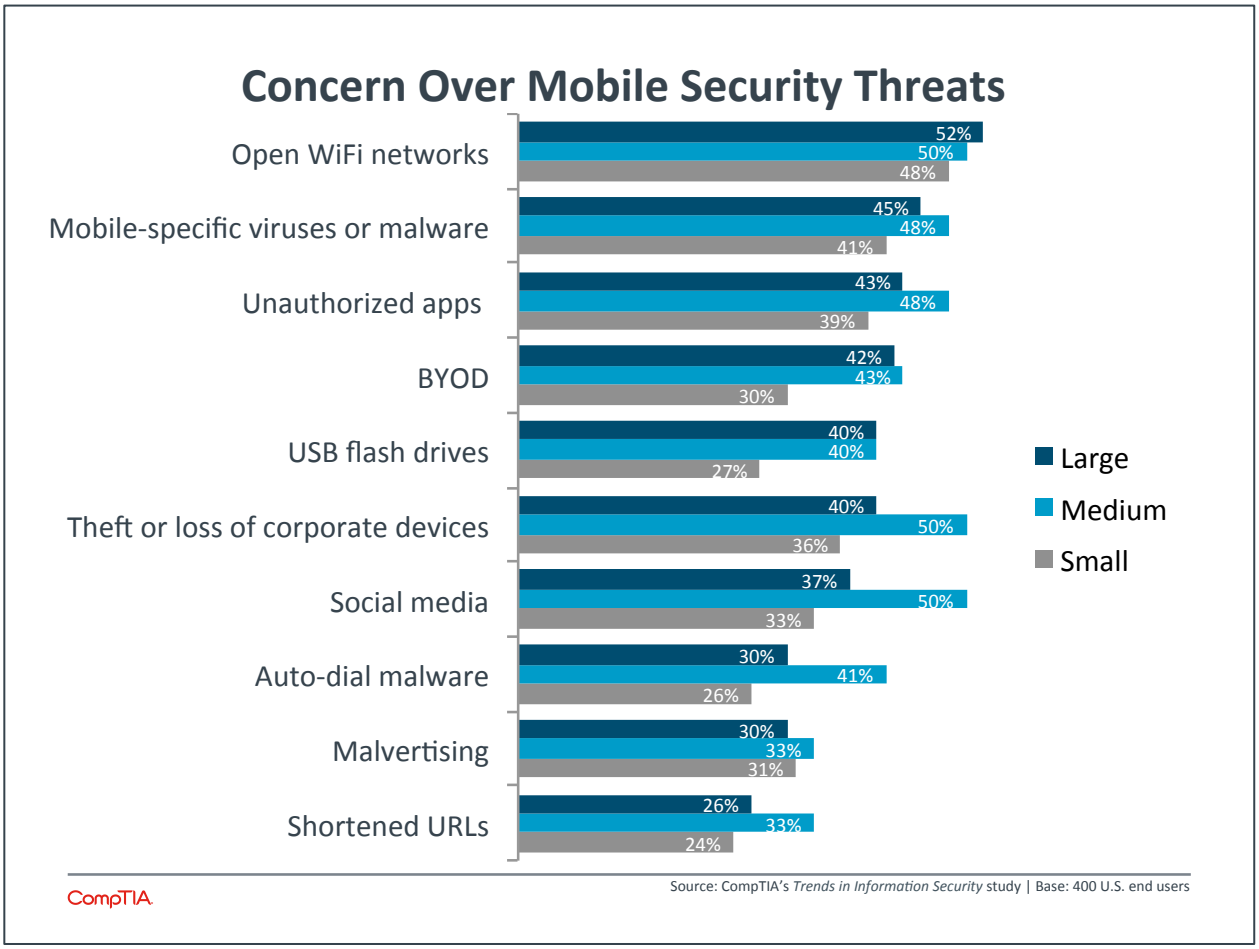
33% New methods for accessing company data

32% Additional training on mobile security

30% Engage third party for mobile security

26% Build approval process for apps

Appendix


Concern Over Mobile Security Threats
Open WiFi networks
52%
50%
48%
Mobile-specific viruses or malware
45%
48%
41%
Unauthorized apps
43%
48%
39%
BYOD
42%
43%
30%
USB flash drives
40%
40%
27%
Theft or loss of corporate devices
40%
50%
36%
Social media
37%
50%
33%
Auto-dial malware
30%
41%
26%
Malvertising
30%
33%
31%
Shortened URLs
26%
33%
24%
Large
Medium
Small
CompTIA
Source: CompTIA's Trends in Information Security study | Base: 400 U.S. end users

SECTION 3:

Usage Patterns

CompTIA

Key Points

- Technology is only one piece of a new security approach. Processes must also be considered, and the best place to document process decisions is in a security policy. Only half of all companies believe they have a comprehensive security policy, with 18% of small businesses not even planning to build a policy in the next year.

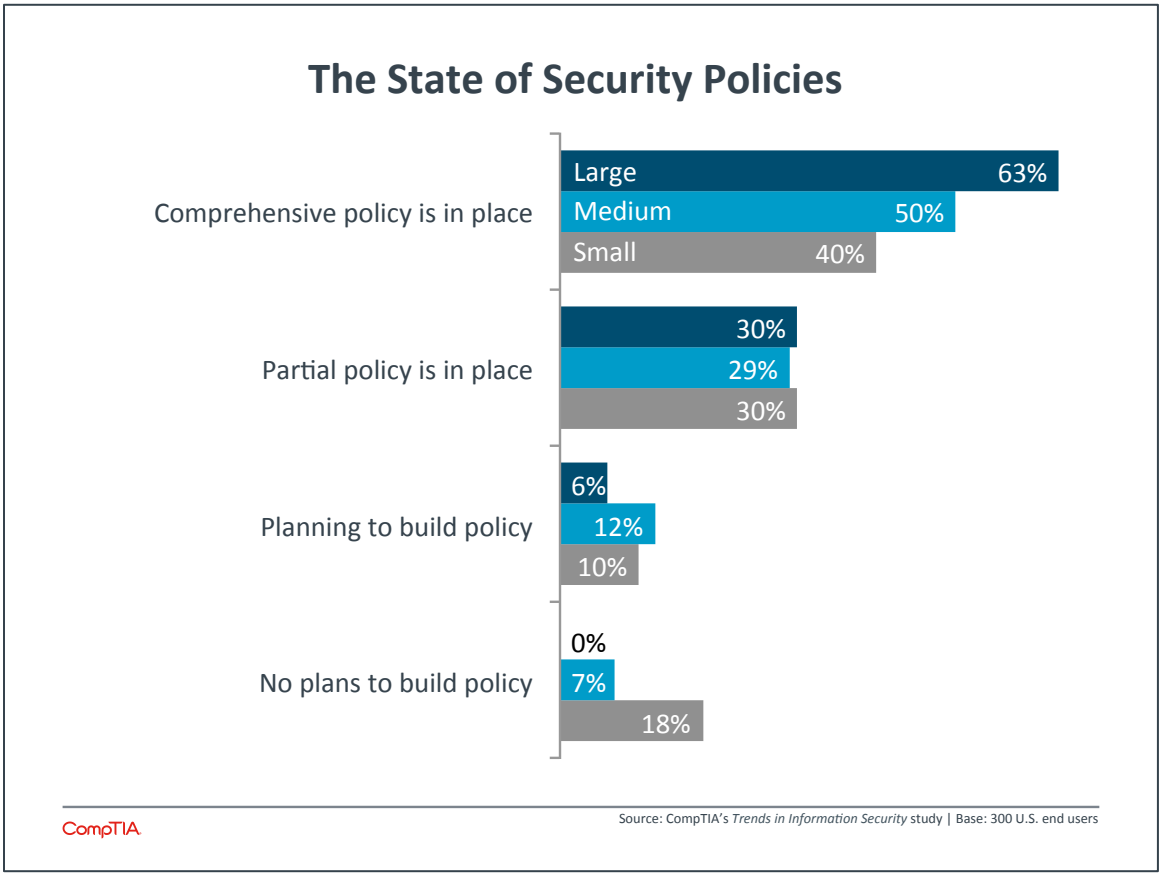
- Formal risk analysis is one process that more companies need to focus on. Compared to 2013, fewer companies feel that they have an appropriate balance of security and risk, indicating that companies are starting to think closely about this area. Thirty-four percent of businesses now feel they have too much risk and must consider tighter security.

- Another process that is rapidly rising in importance is compliance, with companies increasingly exposed to a wide range of regulations. Fifty-four percent of companies say that maintaining compliance requires a high level of effort, signaling a possible desire to outsource the work since it may not be a core competency.

Process and Policy

The true mark of disruptive technology is that it does not simply replace existing models but drives deeper transformation to corporate processes and workflows. This is what companies are seeing with cloud and mobility. These two foundational trends are forcing businesses to examine their IT architecture, their business operations, and their policies.

As businesses take the next steps in their ongoing evolution, security is an area that will require special consideration. As section 1 described, the rapid digitization of business has raised the potential impact of cybercrime. Security breaches can severely impact operations, and the cost of recovery can be substantial. Those costs typically include the costs of reputation repair, especially in the case of data breaches in a time when privacy has become critical for most customers. Attackers are fully aware of these possibilities and have broadened their attack patterns, looking for any weak defenses that could allow them to meet their goals, regardless of company size.



As they shift the mindset and the approach to IT security, companies will need to pay attention to their security policies. In many cases, these policies may not be very robust if the previous view of security was simply a secure perimeter for on-premise devices and information. In other cases, no policy exists at all. Whatever the reason, half of all companies state that they do not have a policy or that their policy needs some work.

The existence of policies among different-sized companies breaks down as expected. Sixty-three percent of large companies feel that their policy is comprehensive, compared to 50% of medium-sized

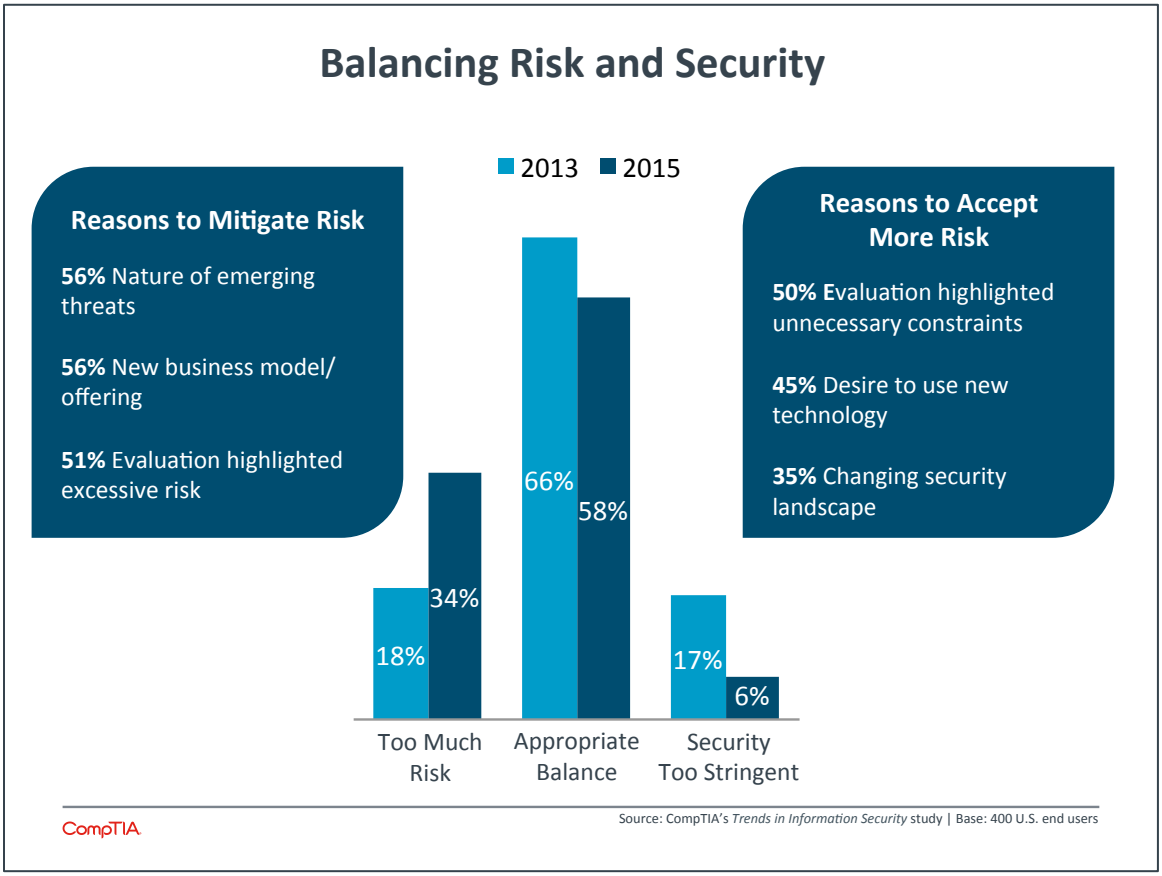
companies and 40% of small companies. The ratios are fairly even when considering policies that need adjustments or plans to build policies in the next 12 months, and small companies dominate the segment that has no policy and no plans to build one. These firms may feel that a formal security policy is overkill, but it presents the opportunity to agree on security matters, and the only cost involved is the time required for discussion.

Comprehensive security policies are directly correlated to satisfaction with security. When a company has taken the time to thoroughly review all areas of security, they feel more comfortable that their decisions are placing them in the best position. Seven out of ten companies that feel completely satisfied with their security also have a comprehensive security policy in place.

Starting with Risk Analysis

In deciding on revamped security policies, businesses will likely encounter some internal processes that should be established or overhauled. These processes are somewhat separate from the security technology described in Section 2, which covers day-to-day monitoring and management. While those technical operations are mostly the purview of the IT team, these other internal processes will involve all the departments within an organization.

The first of these processes is formal risk analysis, an area that many companies may believe they already understand. The practice of risk analysis in project management is well established, with various risks being assigned probability and impact, then mitigation strategies being put in place based on those assignments. However, applying this discipline in the area of overall security is not practiced as widely.



Formal risk assessment ranked near the bottom of businesses' list of security threats, with just 28% citing it as a serious concern. This follows a pattern seen throughout CompTIA research of companies placing a low emphasis on areas that are not well understood. Typically, levels of concern and adoption will rise as a new trend becomes more of a fixture.

There are already some signs that risk analysis is getting more attention. Compared to 2013 data, there are fewer firms that feel that they have an appropriate balance between risk and security. This viewpoint is shared very evenly across all company sizes, with some slight differences appearing on either end of the risk/security spectrum. Large companies are more likely to say that they currently have overly stringent security, and medium-sized companies are more likely to say that they are accepting too much risk.

There are greater differences when considering job function. Executives are the most likely to feel that the balance is correct, with 64% placing their company in this category. IT employees do not fall far behind, with 59% believing that the balance is appropriate.

The biggest difference—and the biggest surprise—comes from employees in a business role. Just 43% feel that the current balance is ideal. By itself, this number may not be surprising, but line of business employees are not pushing for less restrictions. On the contrary, 45% of these employees feel that there is too much risk in the current environment and that more investment, policies, or training could improve the situation.

This finding goes against much of the common thinking around the topic of rogue IT. In most scenarios, rogue IT is described as lines of business circumventing the IT department to procure and use technology on their own. With cloud computing and mobility making technology so easy to access and configure, rogue IT has been perceived as a threat that will be difficult to contain. However, recent data indicates that business departments are experiencing difficulties as they strike out on their own. Integration is certainly one issue for which many departments will not have the right skills, and the data on risk suggests that they are also either directly experiencing security incidents or somehow understanding that rogue IT has created a weak security situation.

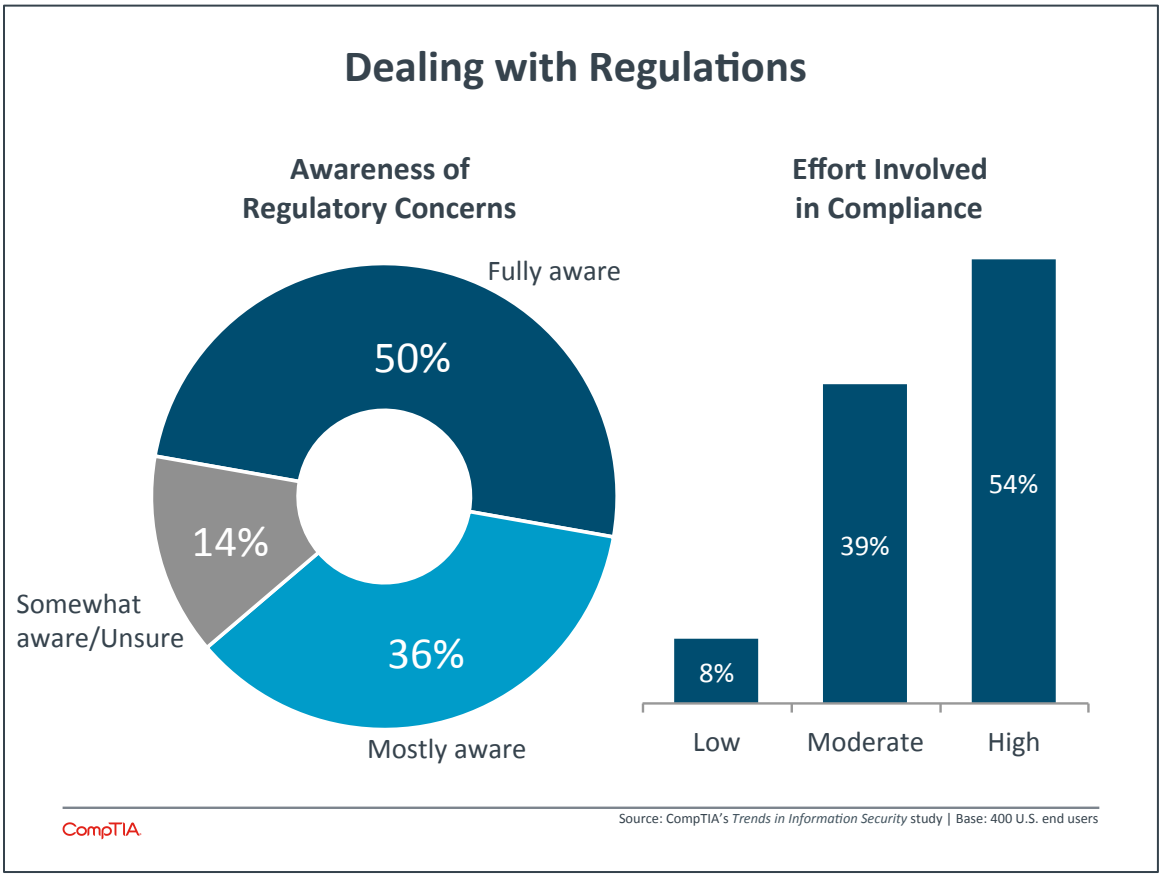
As companies move towards formal risk analysis and seek better ways to educate their entire workforce, they may start by understanding how everyday behavior translates to a security position. For a basic framework in performing a security self-assessment, see the Appendix. Further information can be found in CompTIA's *Buying Guide for IT Security.*

The Growing Field of Compliance

One of the biggest concerns facing companies today is the changing regulatory environment and the need to comply with various laws. The concept is nothing new; modern compliance practices can trace their origins to the Securities Exchange Act of 1934. The new part is the whirlwind of differing laws speeding into existence. Thanks to the way that business is conducted in a digital environment across state or national lines, many companies are finding that they have reason for concern where none existed before.

Sarbanes-Oxley, PCI DSS, and HIPAA are high-profile examples of recent regulations driving a new level of compliance awareness and verification activities. Even when certain regulations are directed towards specific verticals (as HIPAA is with the health care industry), there can be ripple effects as companies interact with each other and receive goods or services that must also remain in compliance. Data privacy

threatens to be the next major topic that will drive additional regulations that will have far-reaching impact.

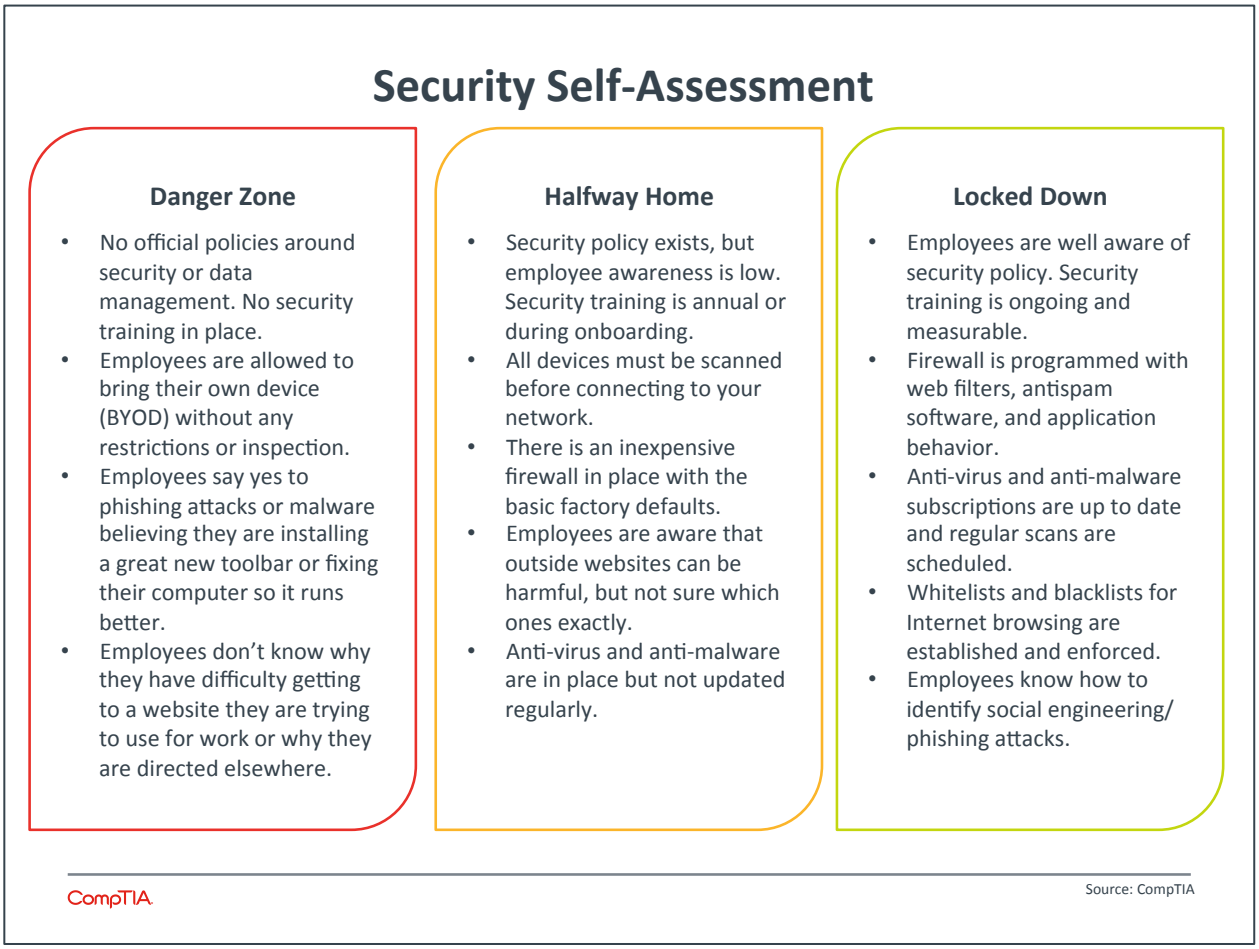


The first order of business when dealing with compliance issues is simply being aware of which regulations apply to an individual business. Given the potential consequences of non-compliance, it is somewhat sobering to see that only half of all companies rate themselves as being fully aware of the regulatory concerns that could affect them. As expected, small companies are the least aware (41%), but large companies do not exhibit the level of confidence that one might expect (54%).

Keeping track of the various regulations and maintaining the proper records for clean audits is a sizable effort. Here, large companies take a wider lead, with 61% claiming that they expend a high level of effort (compared to 56% of medium-sized companies and 46% of small companies). There is not much difference in the way that different job functions perceive the level of effort, so compliance is a good candidate for a topic that can engage a representative cross-section of a company.

Maintaining compliance is not just a good idea for staying out of trouble with the government; it is also a good business practice as consumers and business clients want to protect themselves and their data. More than four out of ten businesses (44%) say that they have achieved higher customer satisfaction as a result of maintaining regulatory compliance, likely thanks to more efficient internal processes and improved organization of corporate data. Thirty-six percent say that maintaining compliance has helped attract new clients, and 27% say that compliance helps create differentiation. Just 21% feel that compliance holds no additional benefit and is simply a cost of doing business.

Appendix


Security Self-Assessment
Danger Zone
No official policies around security or data management. No security training in place.
Employees are allowed to bring their own device (BYOD) without any restrictions or inspection.
Employees say yes to phishing attacks or malware believing they are installing a great new toolbar or fixing their computer so it runs better.
Employees don't know why they have difficulty getting to a website they are trying to use for work or why they are directed elsewhere.
Halfway Home
Security policy exists, but employee awareness is low. Security training is annual or during onboarding.
All devices must be scanned before connecting to your network.
There is an inexpensive firewall in place with the basic factory defaults.
Employees are aware that outside websites can be harmful, but not sure which ones exactly.
Anti-virus and anti-malware are in place but not updated regularly.
Locked Down
Employees are well aware of security policy. Security training is ongoing and measurable.
Firewall is programmed with web filters, antispam software, and application behavior.
Anti-virus and anti-malware subscriptions are up to date and regular scans are scheduled.
Whitelists and blacklists for Internet browsing are established and enforced.
Employees know how to identify social engineering/ phishing attacks.
CompTIA
Source: CompTIA

SECTION 4:

Workforce Perspectives

CompTIA

Key Points

- The final element in a new security approach is considering the human element. While only 30% of companies rate this as a serious concern, they also report that the human element accounts for 52% of the root cause of security breaches. More than in years past, companies are citing specific areas where human error is contributing to a security incident.

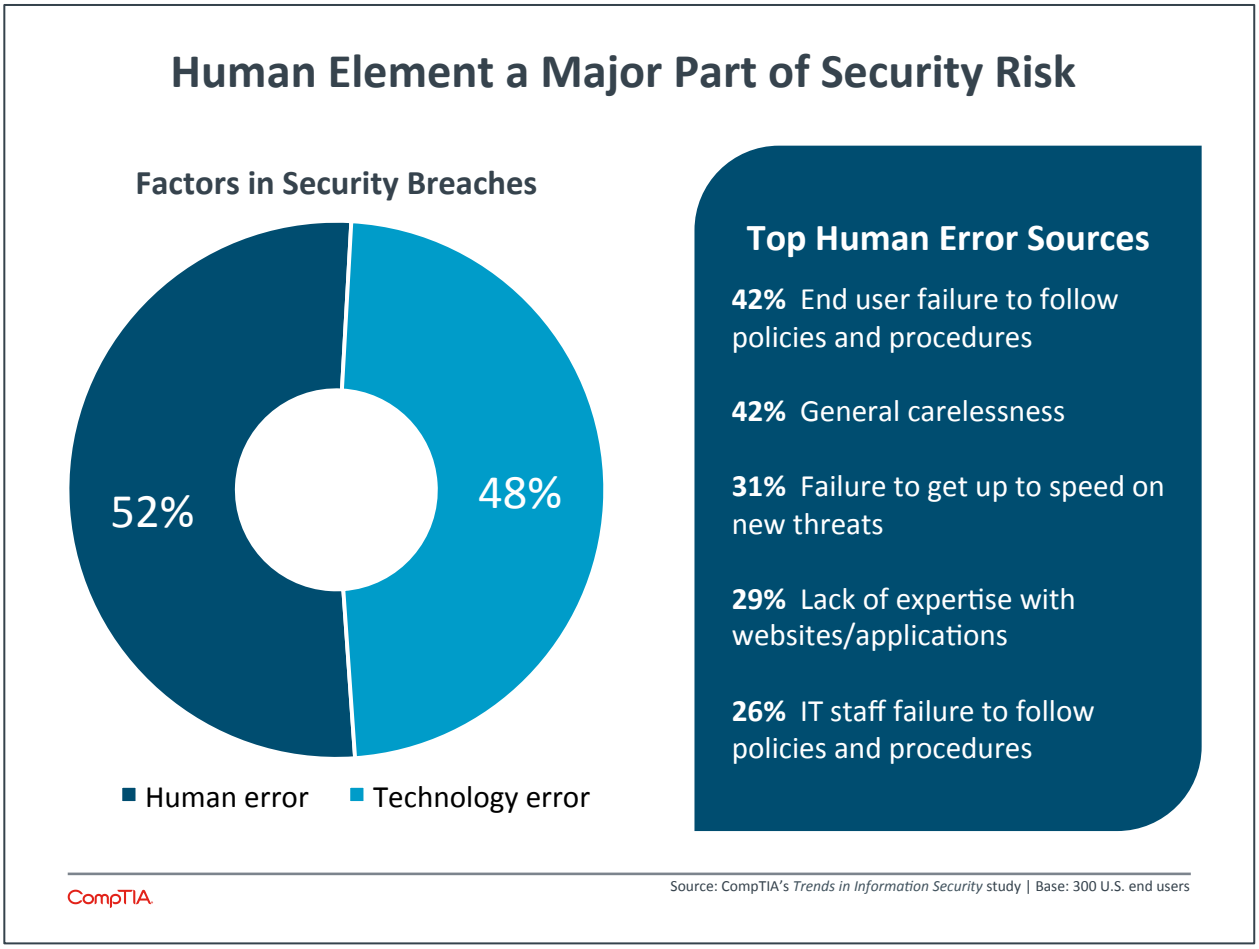
- Training is the clear answer for mitigating human error, but companies struggle with understanding how to make an investment in training. Only 54% of companies offer some form of cybersecurity training, with the format most often being new employee orientation or some kind of annual refresher course.

- Although 86% of companies that offer security training feel that it is effective, this is analogous to a large percentage of companies feeling that their current security is sufficient. There are rarely metrics in this area, and businesses readily acknowledge that they would like to see better content in their security training.

The Weakest Link

Section 1 of this report described the many types of security threats that exist and the level of concern that businesses have for each threat. One of the threats driving the lowest level of concern was human error, whether that error came from general staff (only 30% of companies rated as a serious concern) or from IT staff (27% of companies rated as a serious concern).

The reason this level of concern is so shocking is that businesses consistently rate human error as the leading contributor to security breaches. Of course, it can be difficult to separate human error from technology error; for example, is incorrect firewall configuration a technology error or a human error because of lack of knowledge for proper settings? There is some room for interpretation, but consistent examples throughout various CompTIA surveys have established a general baseline for the type of behavior classified as human error.



The 2015 data show that companies are starting to see more and more examples of human error in day-to-day operations. In 2013, the top human error sources were "end user failure to follow policies and procedures" and "IT staff failure to follow policies and procedures." Two years later, businesses cite more specific examples along with these two generalizations.

General carelessness now rates as the second leading example of human error. This behavior is the primary outcome when security and convenience collide. End users often know what best practices in

security are, but they often choose a more convenient solution in the pursuit of efficiency. Passwords are a perfect illustration of this; most people are fully aware of what makes a strong password, but SplashData's worst password list is still headed by "123456" and "password" (the list is made up of the most common strings found in lists of leaked passwords).

Failure to get up to speed on new threats is also a contributor to human error, and companies are seeing this in greater numbers as their employees push for technology solutions but do not fully understand the security implications. Although rogue IT may be faltering somewhat (see Section 3), it is still a potential source for this type of behavior.

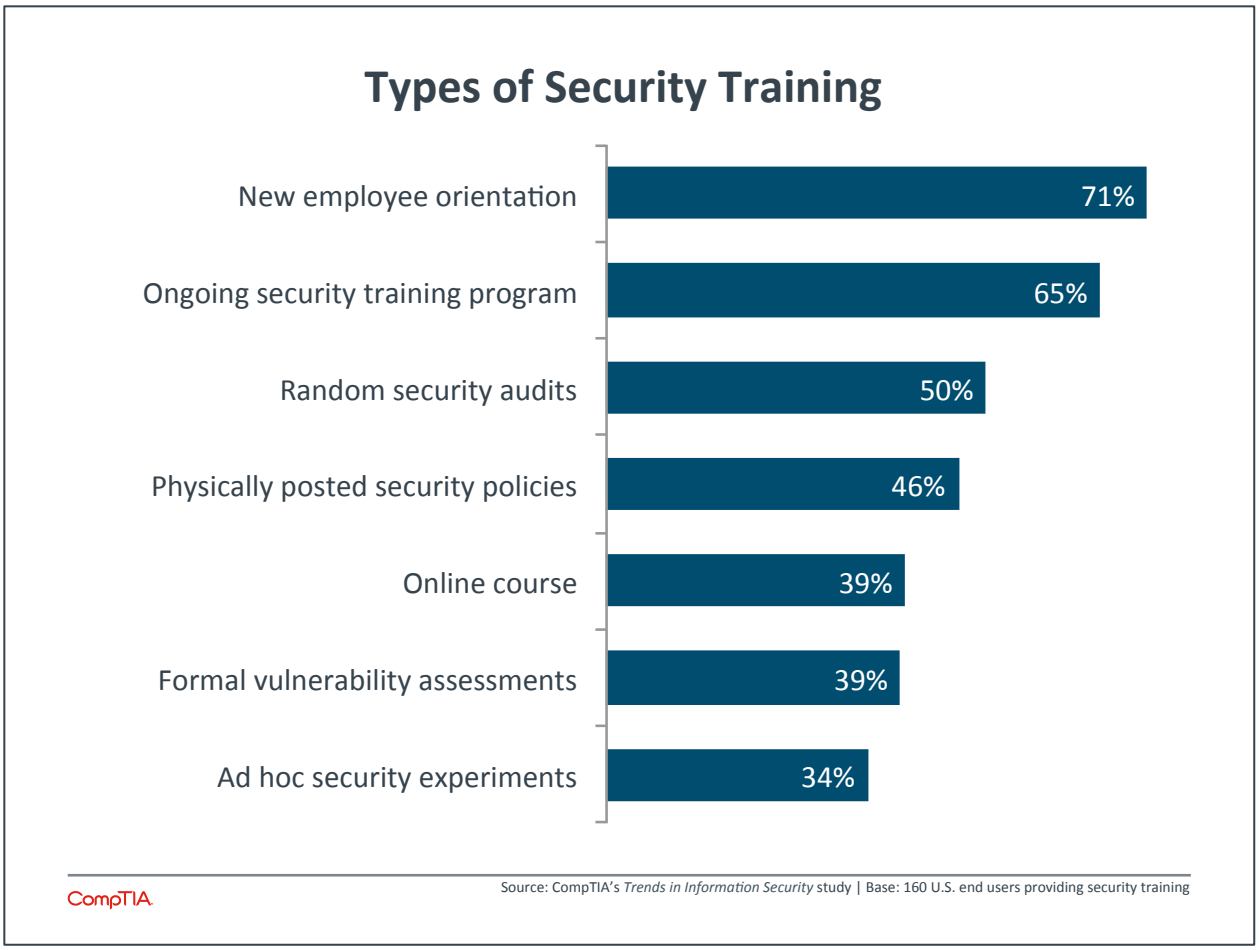
While the overall mix of human error vs. technology error is not changing much year over year, there are other indications that human error should be a greater cause for concern. Among those companies that indicated human error played some role in security incidents, 39% felt that human error was more of a factor over the past two years. This sentiment is slightly stronger at large companies, where security breaches are more closely examined to determine root cause. As small- and medium-sized businesses become more sensitive to security issues, they will also see some of the problems caused by inexperience and carelessness among the workforce.

Exploring Training Options

The main reason that companies exhibit a low level of concern over human error is that it is a problem without an obvious solution. A high level of concern over malware or hacking can be addressed with an investment in technology. A high level of concern about employee error can possibly be addressed with an investment in training, but there are complications involved.

Most businesses struggle with the thought of providing education. It is not their forte, and the effects are very difficult to measure. Few training programs offer direct correlation to business results, and this is especially complicated for an area like security where the desired effect is the absence of any incident.

Still, most businesses have some notion of providing foundational training, whether that is job-related, compliance-driven, or HR-mandated. Security training is one of the most common offerings, but that does not mean it is widespread. Only 54% of companies offer some form of cybersecurity training, a number that is likely to increase as companies battle the issue of human error.



This provides a baseline of sorts as companies consider how to create a more secure workforce. The gap between the current state training and the ideal state can be glimpsed when considering the top form of training. If security is discussed only at new employee orientation, then there is no mechanism for pushing out new information once the employee is onboard.

Based on anecdotal evidence, companies that claim to have an ongoing security training program are likely referring to some form of annual refresher that is pushed out to the workforce. A smaller number of companies actively manage a program that has multiple touch points throughout the year. These touch points might include ad hoc security experiments such as simulated phishing attacks or "dropped" USB sticks that can alert the security team when they are plugged into a computer.

Whatever the methods, companies feel that their current security training is working. More than 8 in 10 companies (86%) that offer security training believe that it is "extremely effective" or "mostly effective." At first glance, this does not offer much room for improvement. However, only 36% of firms use the "extremely effective" rating, indicating at least some potential for enhancement.

Furthermore, it would be worthwhile to dig deeper with these companies and ask how exactly they are measuring effectiveness. Without a well-established metric, it may be more of a general feel. There is some proof of this when examining how respondents in different job roles rate their security training. More than half of executives—those furthest from potential security issues outside of a major breach—

rate their training as “extremely effective.” Only 32% of IT workers and 26% of business workers feel the same way.

A final reason to believe that companies may be overstating the effectiveness of their security training is that they are quick to give examples of what could be done to enhance the approach. Especially considering the fact that the top example is better content within the security training, it seems that companies are aware of areas that are not being adequately covered.

Other potential improvements point to the need to ensure that training has an impact. Making training more engaging or dynamic will help with retention and ultimately improve security awareness. If companies are able to establish methods for measuring that awareness, then these factors will be definite differentiators among various training offerings.

What about the segment that is not currently providing security training? With nearly half of all companies in this segment, it seems like a field full of opportunity. As expected, one of the main reasons that these companies do not offer training is that they do not have sufficient budget (26%). Knowledge gaps also exist, whether companies are not sure how to find the proper security training (20%) or they are not sure which security training is the most effective (19%).

However, the biggest reason offered for not providing security training is that there is no reason. Nearly 1 in 3 companies (29%) say that there is no specific hurdle to security training, but they simply haven’t

done it. The field is indeed full of opportunity for IT firms that can offer the best training or the best overall security package for mitigating human error and improving a business's security posture.

SECTION 5:

Channel Dynamics

CompTIA

Key Points

- Most channel firms that offer security do so as a part of other offerings, rather than having security as a standalone product or service. As security becomes more critical and more specialized, there is the potential to offer security in new ways or partner to create a more robust security posture for clients.

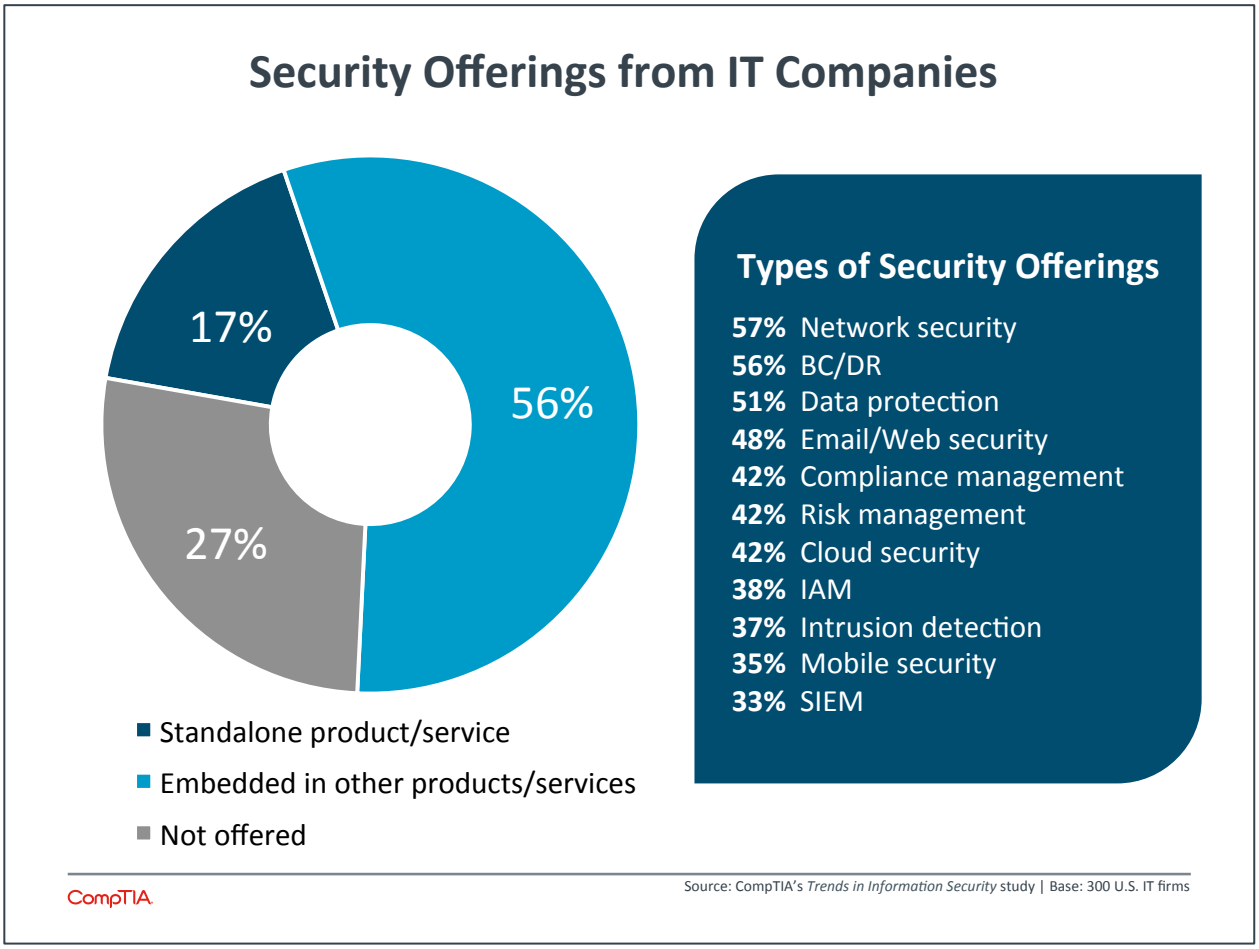
- At least 1 in 3 channel firms claim to offer either security as a service or managed security services, with incidence rates higher among leaf channel firms like solution providers and MSPs. These may be broad interpretations and still not convey comprehensive security offerings, but they are good starting points for building more capability.

- Nearly half of all channel firms (48%) say that they experience no inquiries and take no action as a result of major security breaches. There is ample opportunity here to take a proactive approach to security discussions and highlight areas where clients might be exposed.

Channel Involvement with Security

At the very least, channel firms need to ensure that they have a strong and thorough understanding of the security landscape. As the regulatory field is growing, it is creating a halo effect where partners and suppliers can be held liable for breaches. The massive Target breach in 2013 is a perfect example of the ways that third parties can create exposure: the hackers were able to access Target's network thanks to credentials stolen during an attack on one of Target's HVAC contractors.

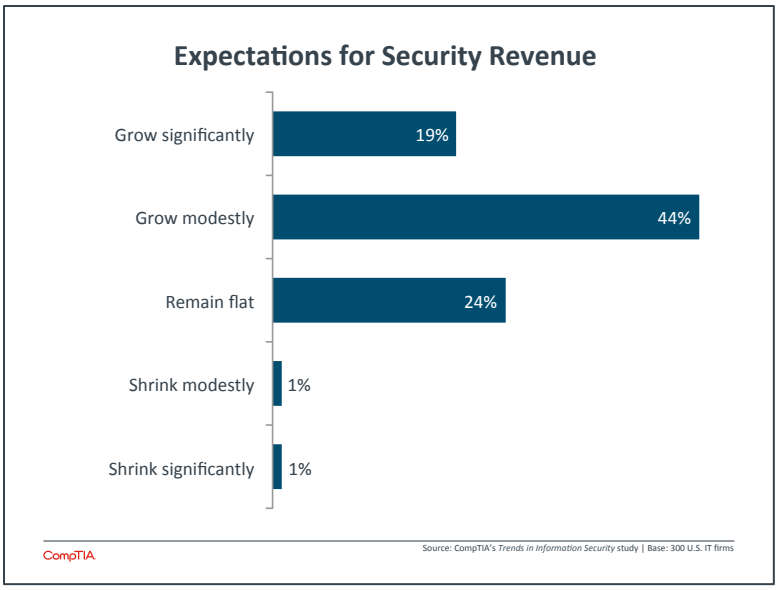
With a topic so long-standing and important, it makes sense that most IT firms are addressing security at some level. Nearly 3 out of 4 channel firms have security as part of their portfolio in some way, with a slightly higher incidence rate (81%) among firms identifying as a solution provider, VAR, or managed services provider.



The products and services offered by channel firms are very much in line with the way that customers have been approaching security. Network security, business continuity, and email security are all foundation pieces of a security strategy, and companies have had these in place for years. Data protection is also widely offered, but as section 3 described, there are many flavors of data protection. The services currently offered might not all be as comprehensive as possible.

In addition to possibly expanding data protection services, there is strong potential to expand in other areas as well. The demand for network security and email security will not drop, but compliance

management, risk management, cloud security, IAM, mobile security, and SIEM could all easily become components in a new security baseline.

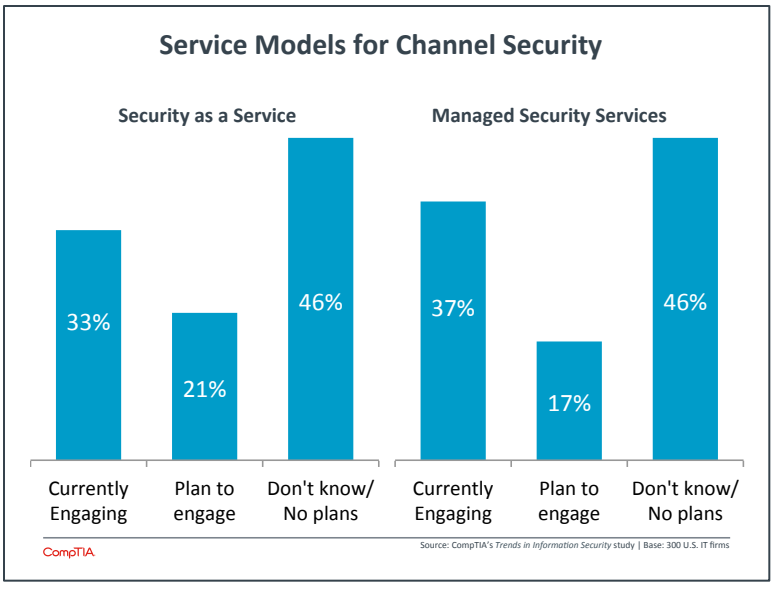


Just as this situation creates new degrees of complexity for end users, it creates complexity for the firms working with these solutions. For resellers, new products mean changes to the sales structure, whether that means training for the new areas or adding new salespeople. For service providers, a wider range of options requires understand how everything fits together to provide the best service possible. As security grows more complex, end users will lose the capability and the bandwidth to provide integration themselves and will increasingly look for a cohesive solution that makes life simple.

One way to procure that type of solution is to outsource, and this driver is one of the reasons that channel firms expect to see growth in security revenue moving forward. Revenue expectations are fairly consistent regardless of company size, but there is a more positive outlook among solution providers/VARs/MSPs. These firms are the mostly likely to provide the types of comprehensive solutions customers are looking for, so it makes sense that they are seeing greater potential than vendors of specific products.

Becoming a Security Provider

Larger companies are seeing security become more of a separate focus area, and there is a similar opportunity for channel firms to start considering security as its own discipline. There will always be a place for individual product installation and support, but there will increasingly be a need for a "soup to nuts" approach that encompasses products, processes, and people.



When discussing two of the delivery models that might apply to this type of security approach, it appears that the channel is well positioned to make this evolution. At least 1 in 3 channel firms claim to offer either security as a service or managed security services, with incidence rates higher among leaf channel firms like solution providers and MSPs.

Another group is planning bring one of these offerings to their customers in the next 12 months, indicating that more than half of all channel firms will have some form of recurring security revenue in the near future.

However, there is also some discrepancy between the number of firms with these types of service models and the number of firms that offer security as a standalone service. For the most part, that discrepancy can be tied to broad interpretations of "security as a service" and "managed security services." To some channel firms, this can mean that they simply offer a single security product that is cloud-based or that security is one piece of a larger managed services engagement. Even among leaf channel firms that are most likely to offer security services, only 23% have security as a standalone offering, implying that the focus of most discussions is on other products and services with security as more of an adjacent conversation.

Bringing security into greater focus and treating it as a distinct topic begins with starting the conversation around security in the right way. Section 1 showed that emphasizing the importance of security is not the best conversation starter since most firms understand that security is important, and using internal changes to IT or shifts in business operations might be a more effective way of highlighting specific security actions that need to be taken.

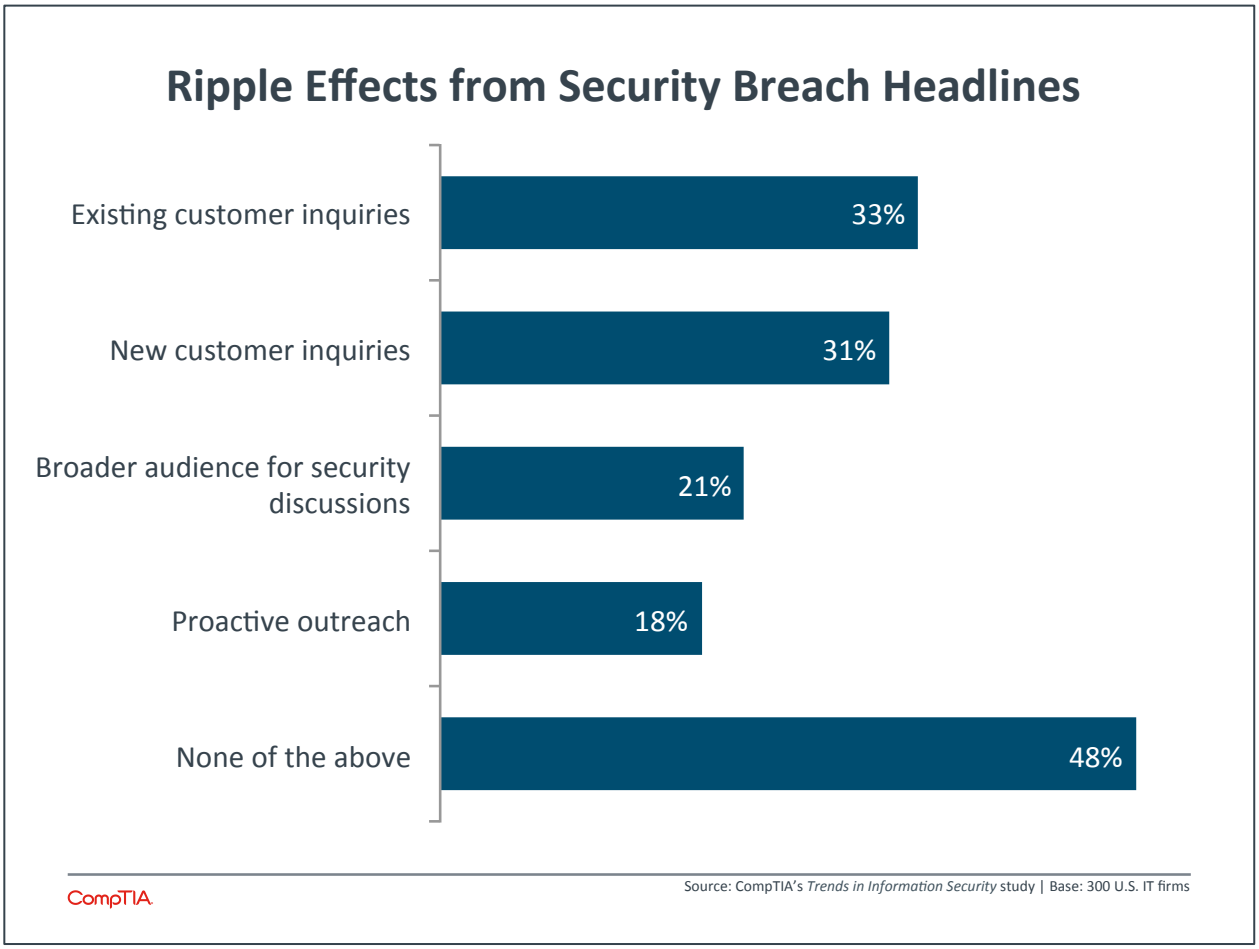
A Place for Everyone

As the director of partner communities at LogicNow, Dave Sobel has a front row seat to the changes taking place in the channel. Sobel and his team work with the companies that subscribe to LogicNow's MAXfocus MSP platform—over 12,000 firms across 100 countries. As things get more complex for IT in general and security in particular, there are many ways in which a channel firm might transform to meet growing demand. "The channel hasn't quite figured out the nomenclature for all the different models that are emerging," says Sobel. "You might be a reseller of a single security product or an MSP that gets recurring revenue out of a single product. Beyond that, you might be a managed security services provider (MSSP), tying multiple security pieces together to form a more comprehensive solution. Then there are firms acting as a virtual CIO, deeply understanding business implications and building the right processes as a starting point before getting to the technical solution." What's interesting is that all of these models appear to be viable in the foreseeable future. Every end user has different needs, different budgets, and different technology appetites, so a number of models or combinations could work depending on the circumstances. "Just like we haven't figured out all the nomenclature, we haven't figured out all the relationships either," Sobel notes. "There's a great opportunity for many different types of business to come together and figure out what the future looks like."

Another entry point for channel firms can be the security incidents that are regularly making headlines. From Target to Sony Pictures to Heartbleed, security breaches and loopholes are making their way more and more into the mainstream news and highlighting the many different methods and motivations of attackers.

Many channel firms see new inquires as a result of these incidents, whether those inquiries are coming from existing customers or new customers. Some firms reach out proactively and may find broader interest for security discussions among business executives. Many firms, however, are not seeing new activity and are also not taking any type of action. Building a comprehensive practice around security

can start by being more aware of the landscape and bringing attention to common mistakes, then presenting a plan to mitigate those mistakes and help customers truly be confident in their security.



CompTIA.org