



Into the cloud, out of the fog

**Ernst & Young's 2011
Global Information Security Survey**

December 2011

 **ERNST & YOUNG**
Quality In Everything We Do

Ernst & Young's Global Information Security Survey

Contents

The Ernst & Young Global Information Security Survey is one of the longest running, most recognized and respected annual survey of its kind; for fourteen years our survey has helped our clients focus on the most critical risks, identify their strengths and weaknesses, and improve their information security.

This year, we conducted interviews with nearly 1,700 information security and IT leaders in 52 countries and across all industry sectors. Our 2011 results show that information security is still one of the most important issues facing our clients.




Introduction	2
Into the cloud, out of the fog	7
Keeping track of mobile computing	15
Seeing through the cloud	21
Connecting through social media	27
Plugging the data leaks	31
Preparing for the worst	37
Looking into the future	42
Summary of survey findings	52
Transforming your security program	55
Related Insights	60



Introduction

Introduction



More and more businesses are moving into a virtual world, supported by new technologies and driven by a need to reduce costs. It is a fascinating journey into the “cloud” that these organizations have undertaken – one that we expect many more organizations will follow.

Our survey identifies three distinct trends that together have had and will continue to have a significant impact on the role and importance of information security.

First, a company’s physical boundaries are disappearing as more of its data is transmitted over the internet. Last year’s survey we already noted this development, and it continues to be a key area of concern.

Secondly, the pace of change continue to accelerate and have witnessed technology transform entire industries – from automotive to publishing to retail. The theme here is the move of business models that are increasingly “digital.”

Lastly, companies are moving from the more traditional outsourcing contracts to cloud service providers. As organizations realize the benefits of bringing their business into the cloud and confidence in the cloud business model continues to rise, they will move more critical capabilities and sometimes their entire IT infrastructure and applications platform into the cloud – thereby forever altering their business model and their IT functions.

Ernst & Young’s 2011 Global information Security Survey outlines these three trends, -- as well as other smaller ones impacting the role and importance of information security.

In Zimbabwe, we have also analysed our data with specific emphasis on issues pertaining to our environment.

Information Security and IT Risk Management

Information Security is one of the most important measures that an organization can take to potentially reduce IT Risks. However there are other areas that can be considered in reducing IT Risks.

IT risk has historically been dismissed as the sole responsibility of the IT Department and has not been considered as a strategic business risk requiring an enterprise-wide focus.

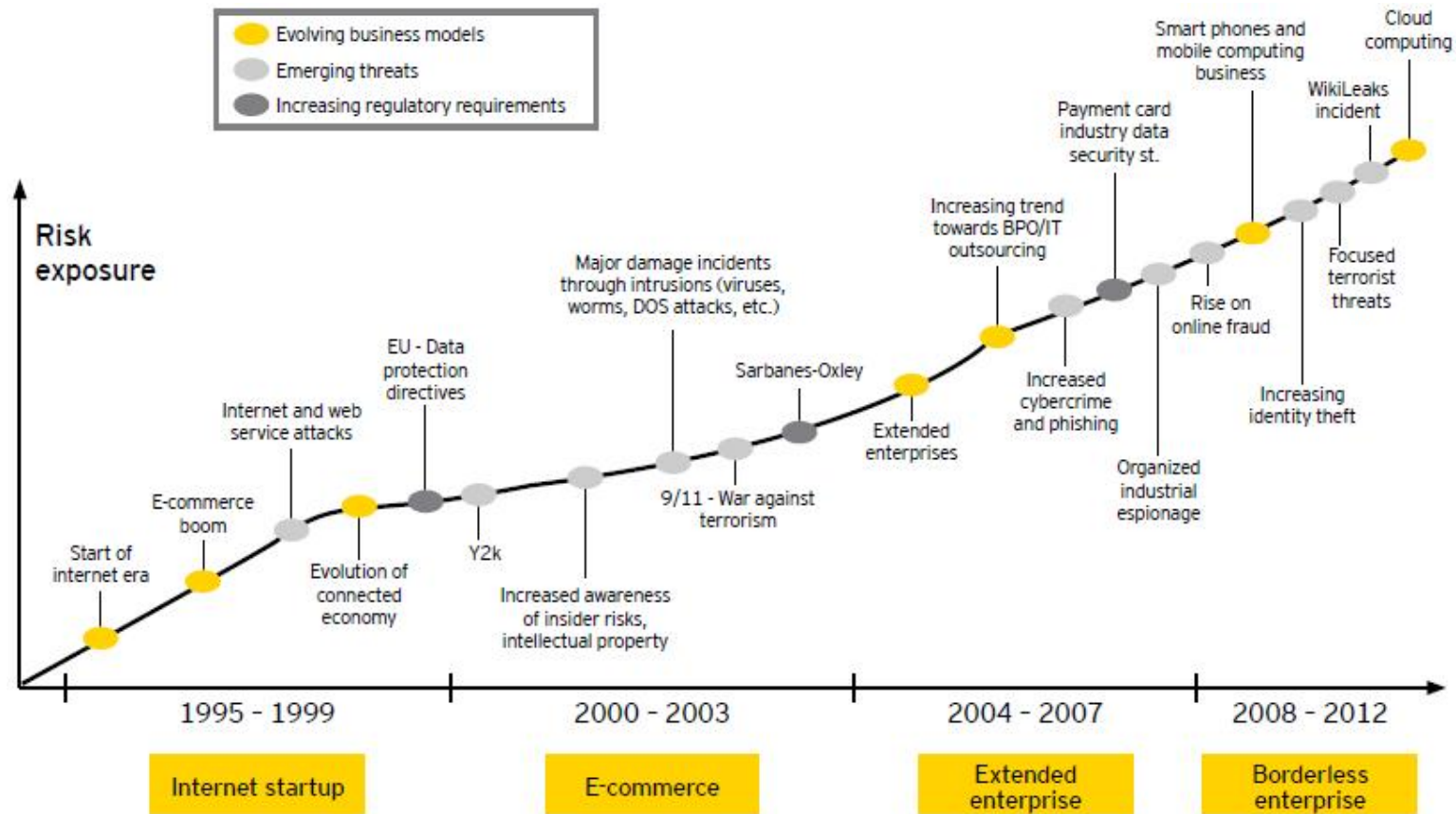
However as the pervasive use of IT tools and technology continues to grow , impacting virtually every aspect of the business function , it is becoming increasingly clear that managing IT risk is less about IT and more about managing risk for the whole business.

Organizations must now include IT Risk Management within their overall enterprise wide risk management approach .

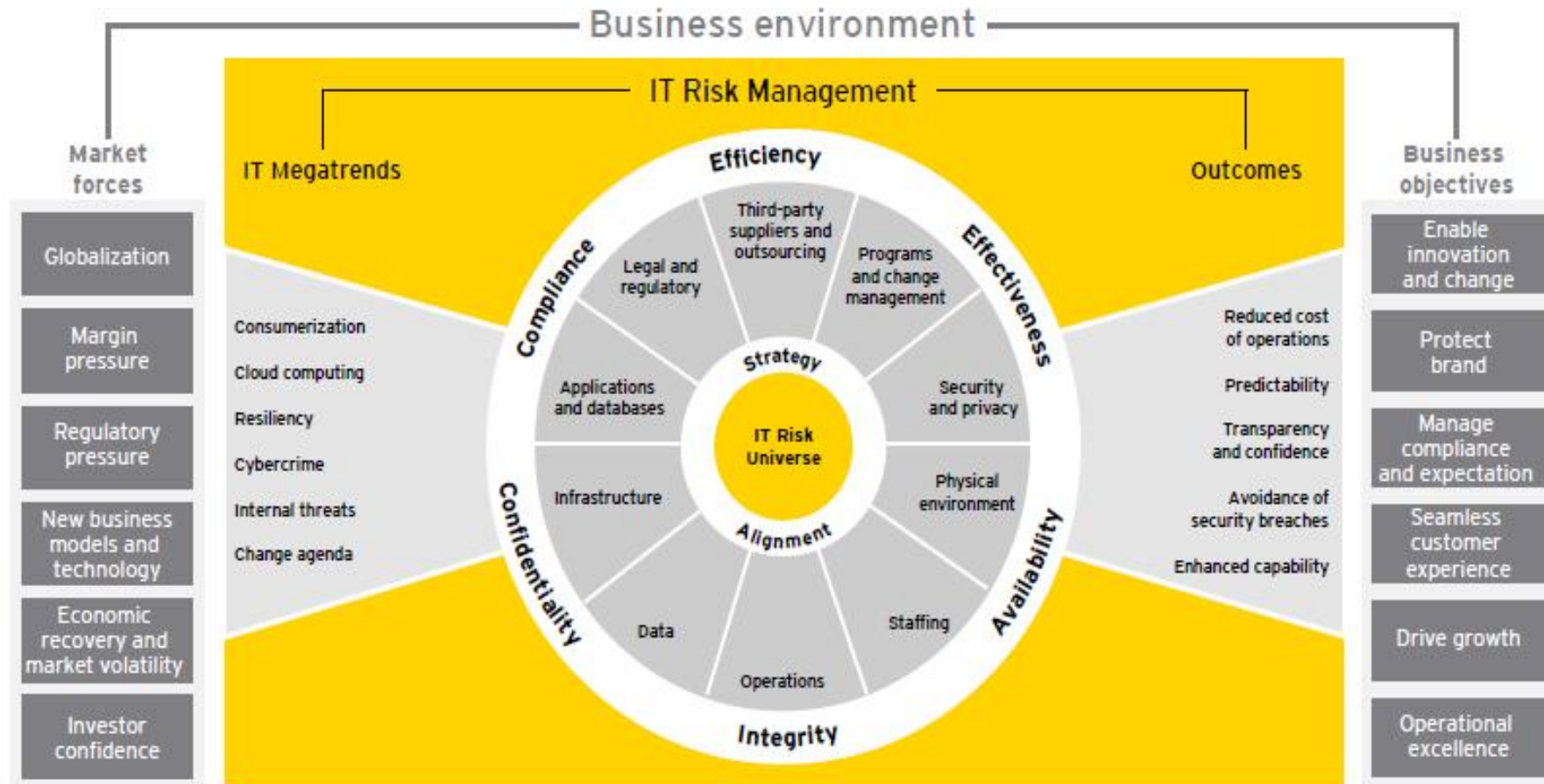
The next slide shows the link between the business and IT risk management.

Evolution of IT Risks over the years

The IT risk paradigm has always been subjected to changes but the complexity and types of risks have expanded significantly over the years and will continue to do so.



The Business Environment and IT Risk Management



The Business Environment and IT Risk Management (ITRM)

IT Risk Management remains an important enabler to achieving overall business objective. Organisations need to manage their "IT Risk Universe" to ensure that IT contributes positively to the business objective. ITRM provides the overall risk and control framework that enables the most important control framework for IT effectiveness, efficiency, compliance, confidentiality, integrity and availability.

It is clear that – with the exception of concerns about issues related to the start of the new millennium – IT risks are only increasing. The breadth and depth of the risks and the need for effective counter measures is expanding rapidly, and will likely to continue to accelerate. Many businesses are recognizing this: in our recent IT Risk Agenda Survey2, two-thirds agreed that managing IT risk has become more challenging over the past few years

The growth of technologies such as mobile computing, cloud computing and virtualization, and the rapid adoption of social media platforms and online commerce/payments shows little sign of slowing. Newer technologies will continue to be created, each for these fast-moving companies, reliance on effective ITRM is considerable. They understand that an IT risk incident imperilling data and undermining consumer confidence could threaten their very existence. Cybercrime is a highly unpredictable risk and has inevitably drawn increasing governmental regulation and oversight scrutiny.

Survey Results on IT Megatrends

To address the evolving trends in IT risk and any critical categories within the IT Risk Universe, many organizations may need to do some significant re-evaluation or readjustment of their ITRM approach. IT should take into account not just the current state, but also factor in the future business response to the megatrends. In our survey, we asked executives in which categories of the IT Risk Universe they had experienced the most negative IT related incidents. Our results show that the three most commonly experienced incidents were in the categories of (1) security and privacy, (2) infrastructure and (3) data. It is not a surprise that all three categories also relate to most of the IT megatrends. We then also asked the participating executives if they planned to spend more or less on the different IT Risk Universe categories. Their response (see below) shows that:

- ▶ security and privacy and infrastructure are recognized as high risk areas and organizations are planning to spend more to mitigate these risks
- ▶ although applications and databases are not immediately a high risk category, organizations plan to spend more (with the potential risk of overspending)
- ▶ the risks around data are not yet very high on the corporate agenda (implying a potential risk of under spending).



Into the cloud, out of the fog

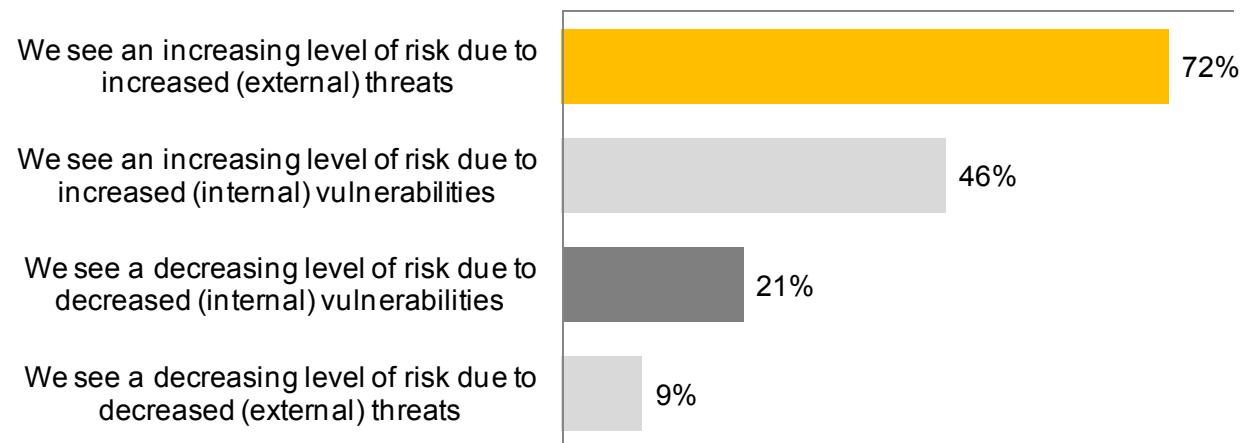
Survey results

Into the cloud, out of the fog- Global

Threat levels remains high as companies scramble to refine strategies to adjust to an ever-changing environment and the resulting security risks

72% of respondents see an increasing level of risk due to increased external threats.

In what way has the risk environment in which you operate changed in the last 12 months?

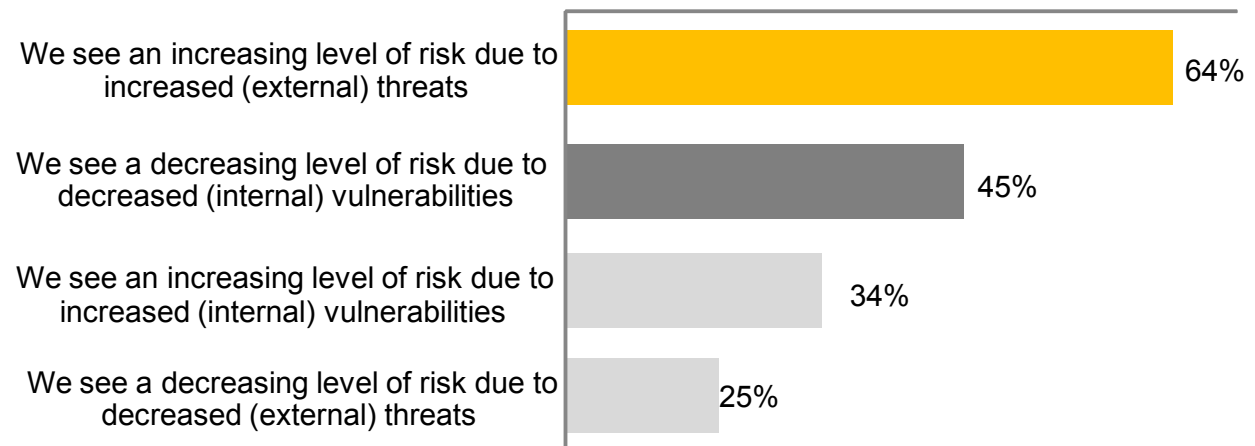


Into the cloud, out of the fog -Zimbabwe

Threat levels remains high as companies scramble to refine strategies to adjust to an ever-changing environment and the resulting security risks

64% of respondents see an increasing level of risk due to increased external threats.

In what way has the risk environment in which you operate changed in the last 12 months?

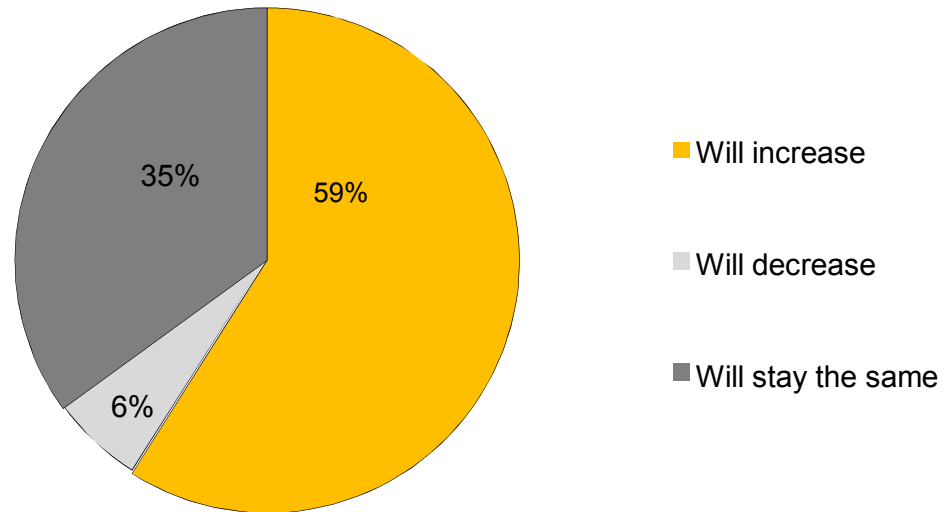


Into the cloud, out of the fog -Global

Resources are flowing into information security programs

59% of respondents expect their information security budget to increase over the next year.

In absolute terms, which of the following describes your organization's total planned information security budget in the coming 12 months?

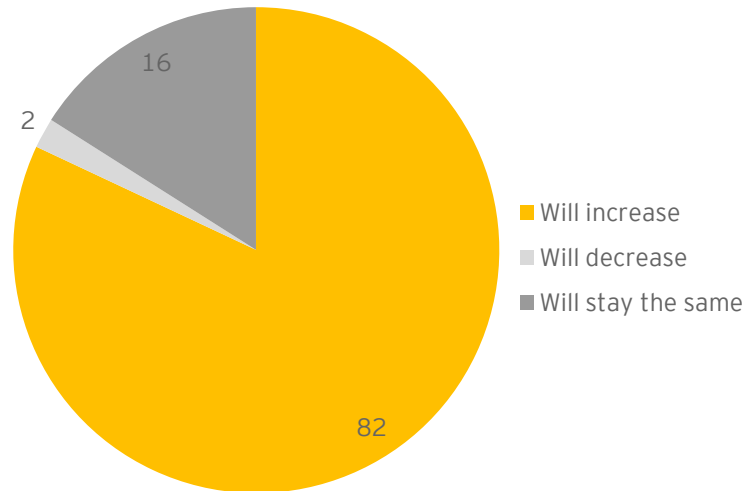


Into the cloud, out of the fog - Zimbabwe

Resources are flowing into information security programs

82 % of respondents expect their information security budget to increase over the next year. Zimbabwe is playing catch up in this area hence the proposed increases security budget.

In absolute terms, which of the following describes your organization's total planned information security budget in the coming 12 months?

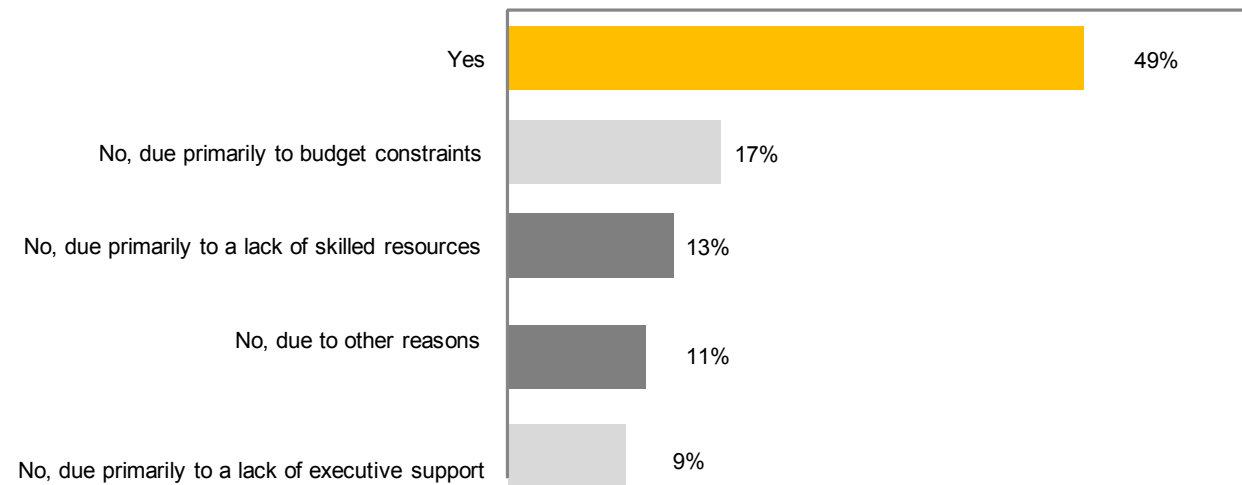


Into the cloud, out of the fog - Global

Despite efforts to grow the strength and capability of information security, a gap remains

While 49% of respondents stated that their information security function is meeting the needs of the organization, 51% said otherwise.

Do you believe the Information Security function is meeting the needs of your organization?

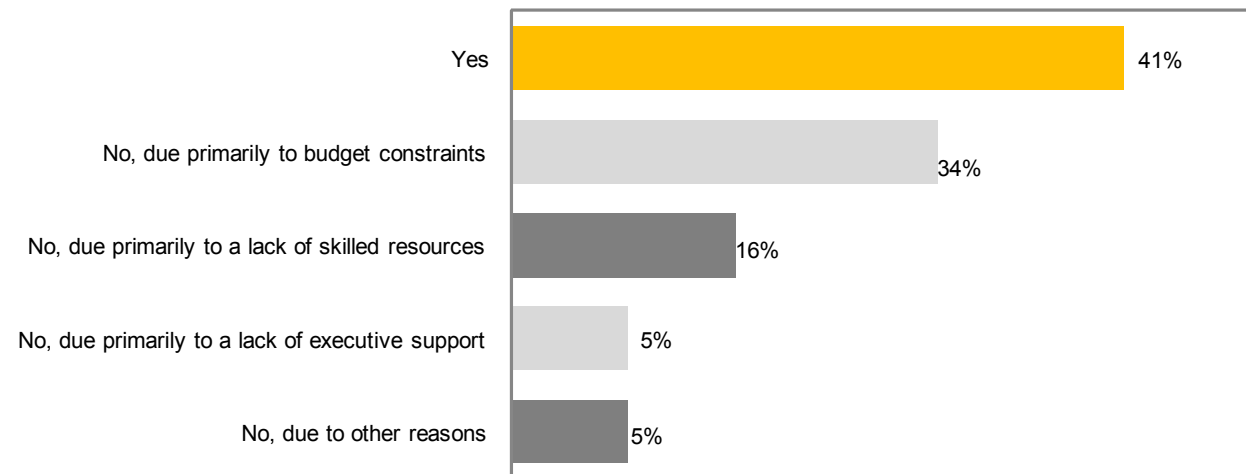


Into the cloud, out of the fog - Zimbabwe

Despite efforts to grow the strength and capability of information security, a gap remains

While 41% of respondents stated that their information security function is meeting the needs of the organization, 59% said otherwise.

Do you believe the Information Security function is meeting the needs of your organization?



Into the cloud, out of the fog

Our perspective

- ▶ Bring information security into the boardroom, making it more visible with a clearly defined strategy that will protect the business while also adding more value through tighter alignment with business needs.
- ▶ Make information security an integral part of service and product delivery and everyone's day-to-day thinking.
- ▶ Focus information security on protecting what matters most, such as customer information and intellectual property. If information security is not adequate and not an enhancement to your brand, why should customers trust you as a business?



Keeping track of mobile computing

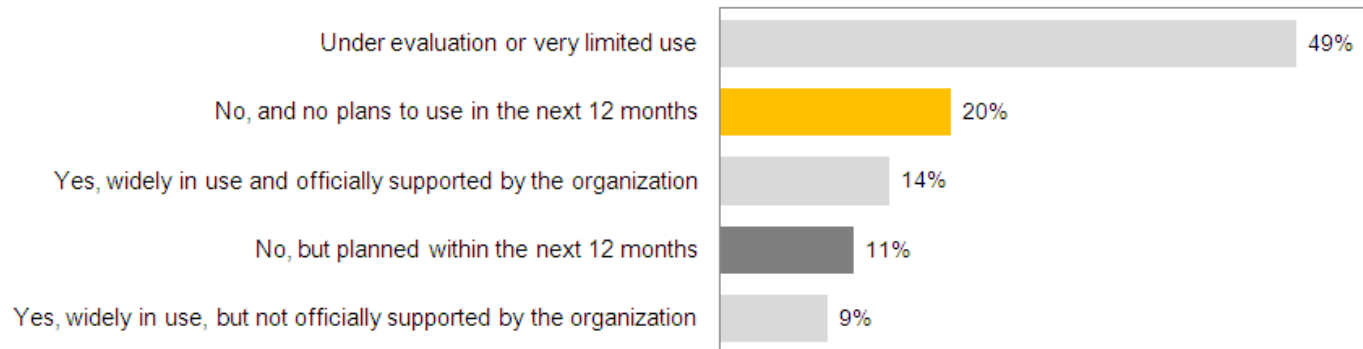
Survey results

Keeping track of mobile computing - Global

While personal adaptation rises, business use lags

20% of respondents indicated that their organization does not currently permit the use of tablets for business use, and has no plans to change that over the next year.

Does your organization currently permit the use of tablet computers for business use?

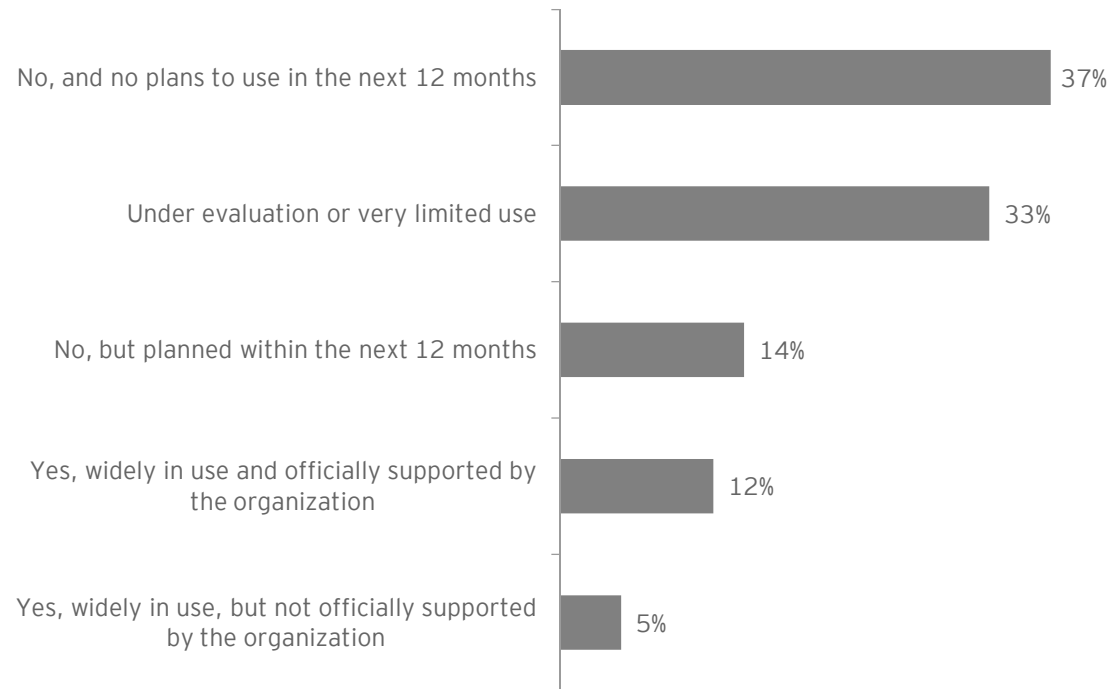


Keeping track of mobile computing - Zimbabwe

While personal adaptation rises, business use lags

37% of respondents indicated that their organization does not currently permit the use of tablets for business use, and has no plans to change that over the next year.

Does your organization currently permit the use of tablet computers for business use?

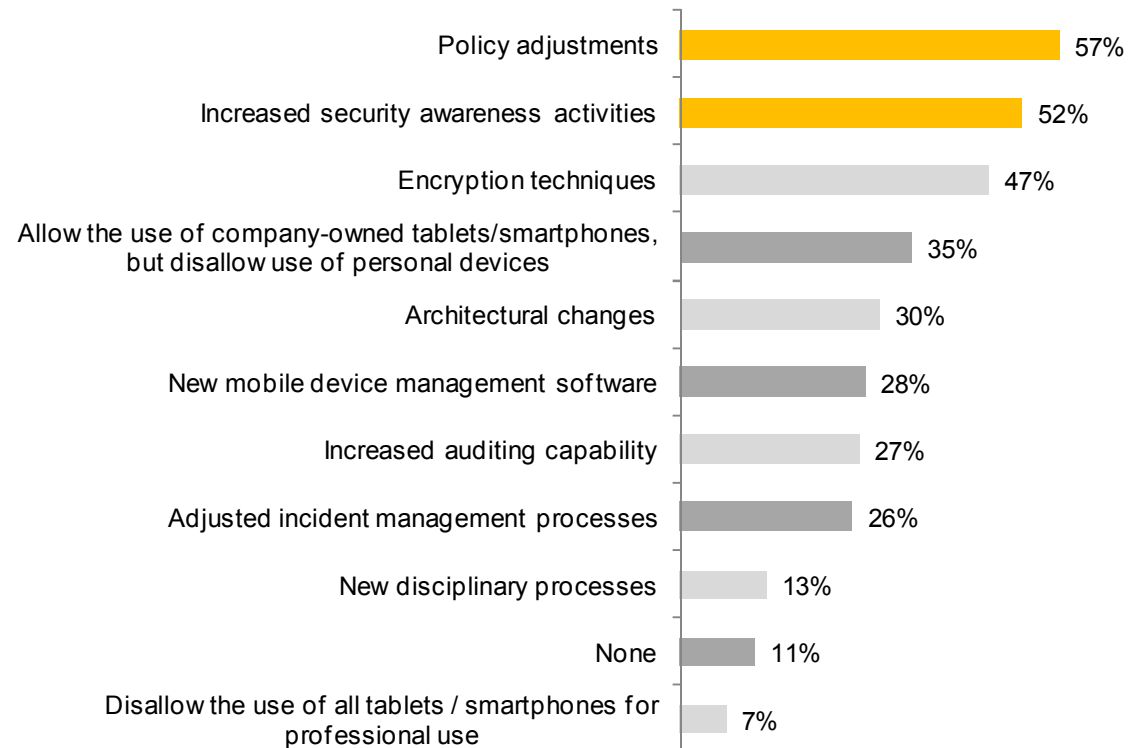


Keeping track of mobile computing -Global

As the use of tablets continues to rise, companies struggle to find ways to keep pace with the security concerns that come with them

57% of respondents have made policy adjustments to mitigate the risks related to mobile computing risks.

Which of the following controls have you implemented to mitigate the new or increased risks related to the use of mobile computing?

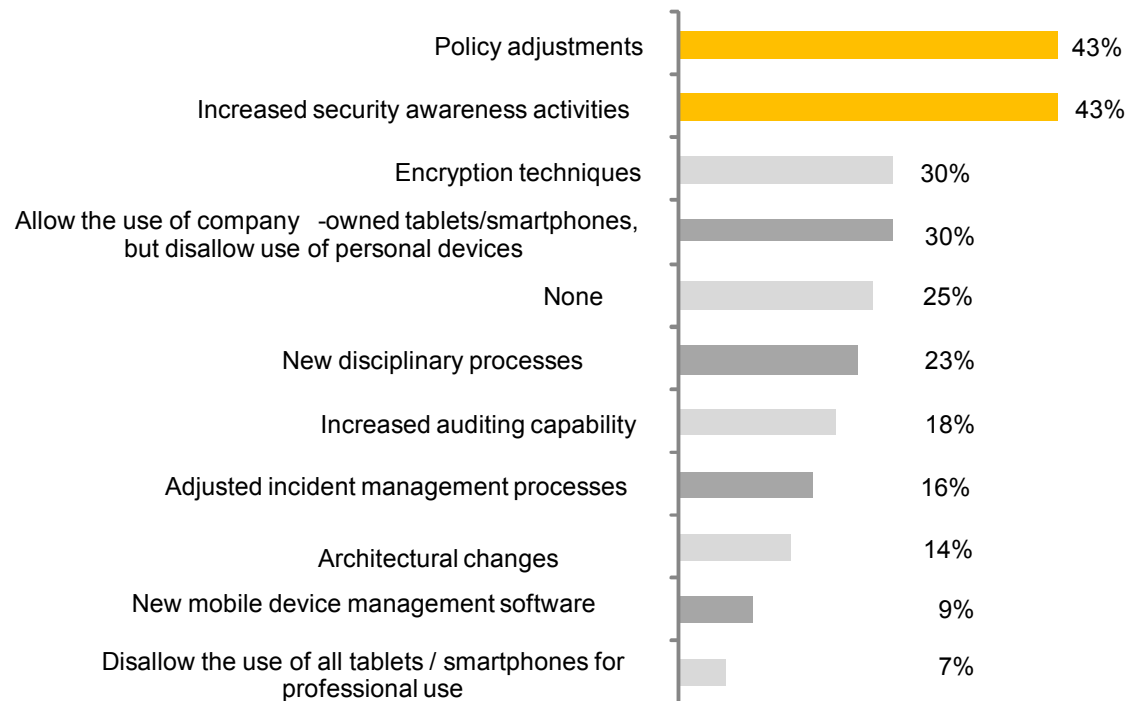


Keeping track of mobile computing -Zimbabwe

As the use of tablets continues to rise, companies struggle to find ways to keep pace with the security concerns that come with them

43% of respondents have made policy adjustments to mitigate the risks related to mobile computing risks.

Which of the following controls have you implemented to mitigate the new or increased risks related to the use of mobile computing?



Keeping track of mobile computing

Our perspective

- ▶ Establish governance and guidance for the use of both mobile devices and their associated security software products.
- ▶ Use encryption as a fundamental control. Because fewer than half of the respondents are using it, organizations should consider embracing encryption.
- ▶ Perform attack and penetration testing on mobile apps before deployment to help reduce the organization's risk exposure.



Seeing through the cloud

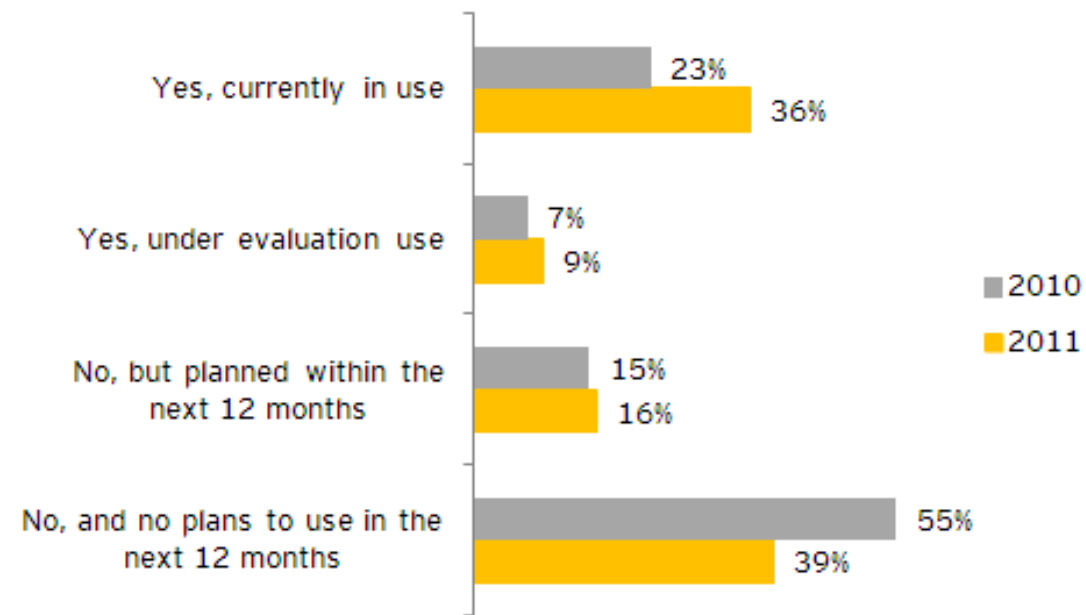
Survey results

Seeing through the cloud - Global

Even as cloud adoption rates and interest continue to climb, lack of clarity persists around security implications and measures

61% of respondents are currently using, evaluating or planning to use cloud computing-based services within the next year.

Does your organization currently use cloud computing-based services?

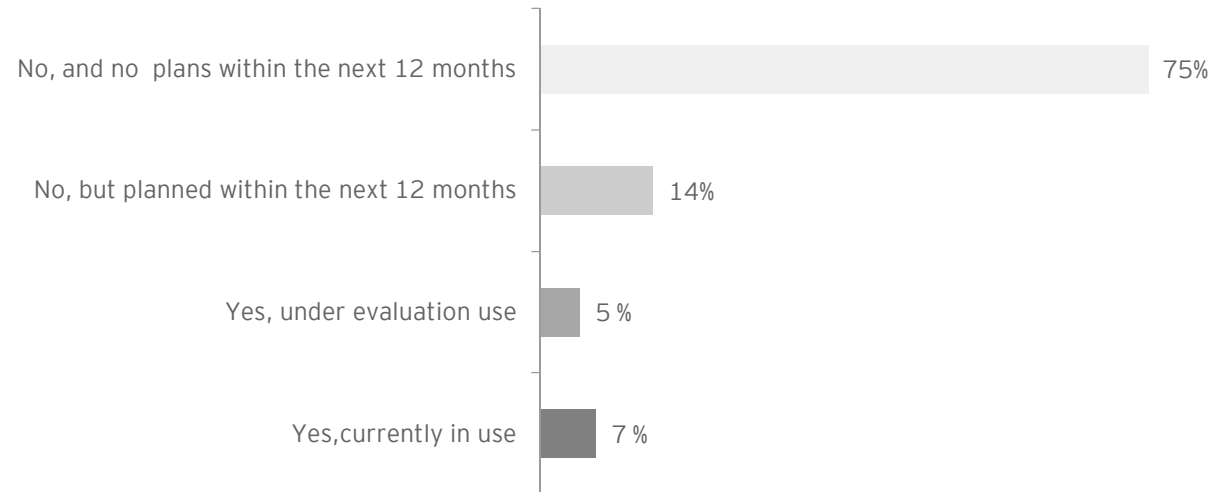


Seeing through the cloud - Zimbabwe

Even as cloud adoption rates and interest continue to climb, lack of clarity persists around security implications and measures

25% of respondents are currently using, evaluating or planning to use cloud computing-based services within the next year.

Does your organization currently use cloud computing-based services?

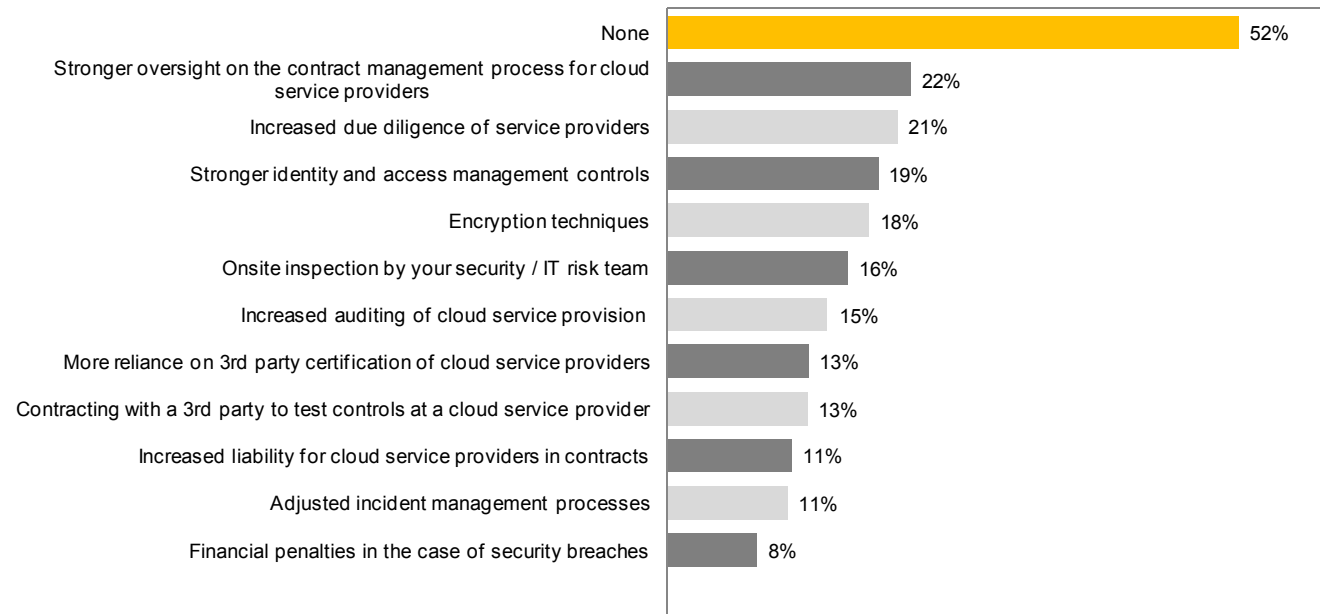


Seeing through the cloud - Global

While cloud adoption rates and interest continue to climb, organizations' information security efforts have not kept pace

More than half of the respondents have done almost nothing to mitigate new or increased risks related to the use of cloud computing

Which of the following controls have you implemented to mitigate the new or increased risks related to the use of cloud computing?

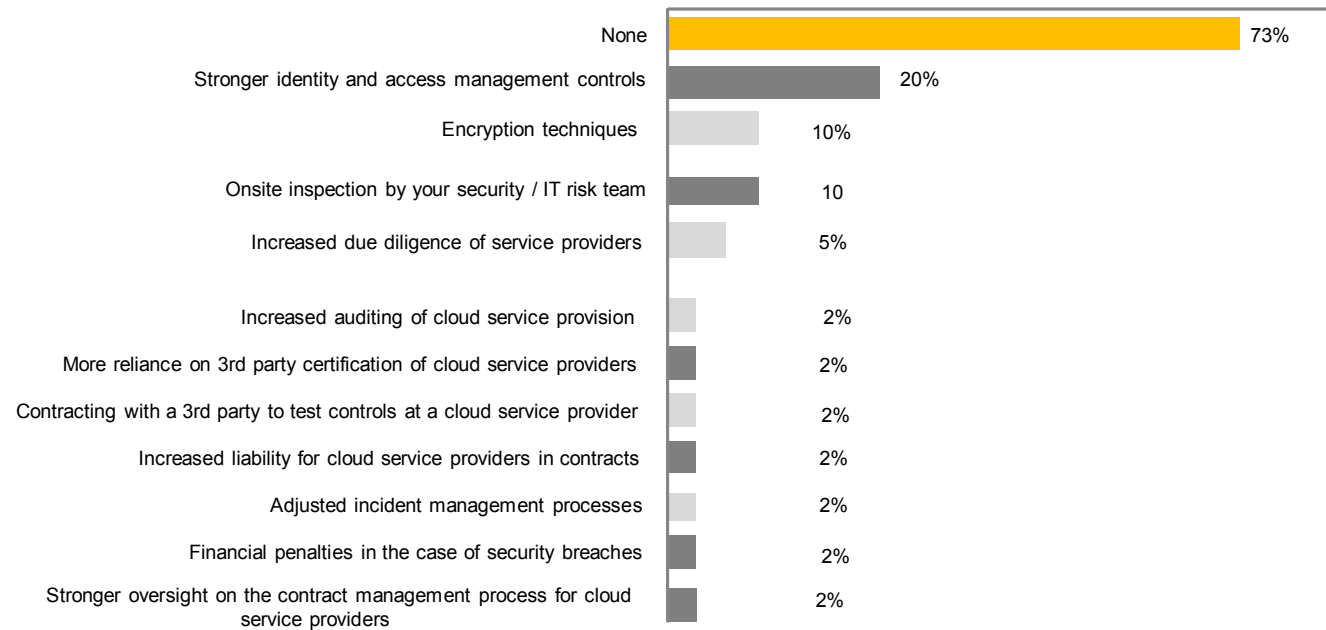


Seeing through the cloud - Zimbabwe

While cloud adoption rates and interest continue to climb, organizations' information security efforts have not kept pace

Almost three quarters of the respondents have done almost nothing to mitigate new or increased risks related to the use of cloud computing

Which of the following controls have you implemented to mitigate the new or increased risks related to the use of cloud computing?



Seeing through the cloud

Our perspective

- ▶ Choose verification above trust.
- ▶ Understand who owns the risks before entering a cloud agreement.
- ▶ Plan for continuity and select providers that are transparent about resiliency build backups and test recoverability.
- ▶ Proceed in using the standard security processes and techniques that have worked effectively on other technologies in the past.
- ▶ Align your business and information security strategy, and continuously assess risks to comply with regulations and industry standards.



Connecting with social media

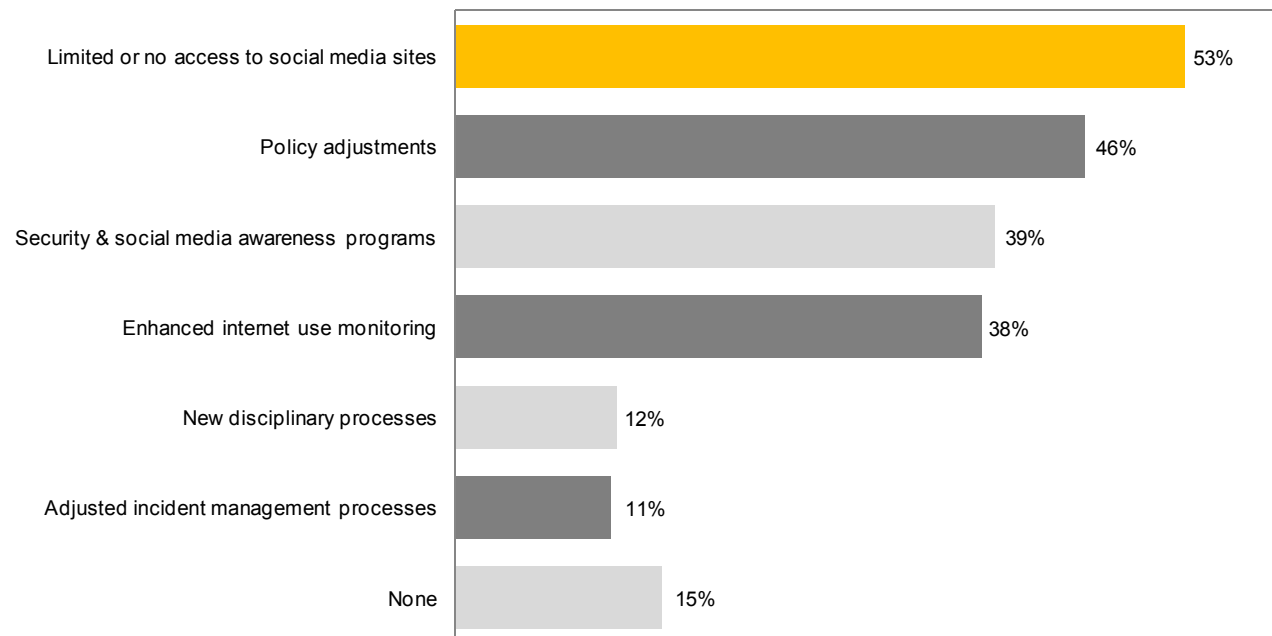
Survey results

Connecting with social media - Global

Organizations are trying to figure out the best way forward to help address security threats in an open, dynamic and nascent industry that is impacting almost every facet of business

53% of respondents have implemented limited or no access to social media sites as a control to mitigate risks related to social media.

Which of the following controls have you implemented to mitigate the new or increased risks related to the use of social media?

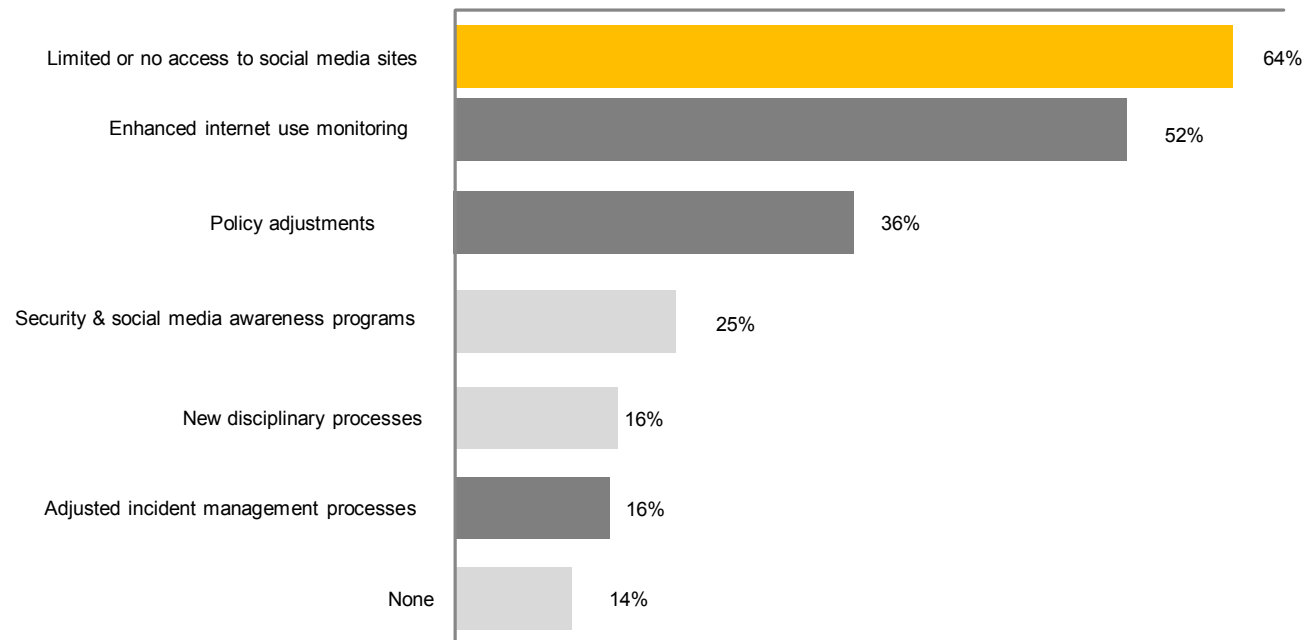


Connecting with social media - Zimbabwe

Organizations are trying to figure out the best way forward to help address security threats in an open, dynamic and nascent industry that is impacting almost every facet of business

64% of respondents have implemented limited or no access to social media sites as a control to mitigate risks related to social media.

Which of the following controls have you implemented to mitigate the new or increased risks related to the use of social media?



Connecting with social media

Our perspective

- ▶ Consider using hard-and-fast “no access/no use” policies for social media sites. This response, while perhaps addressing external threats to internal hardware and software, does not completely address the widespread global personal adoption of social media usage and indirect integration into business use via other channels such as mobile devices. Organizations may consider monitoring their employees’ usage of these sites, without restricting access.
- ▶ Embrace the full advantages of social media. The lack of an integrated information security policy for both access to and use of social media is preventing companies from keeping pace with competitors and may be creating a sense of mistrust with employees.
- ▶ Perform your own reconnaissance to better understand what potential attackers can find on social media.



Plugging the data leaks

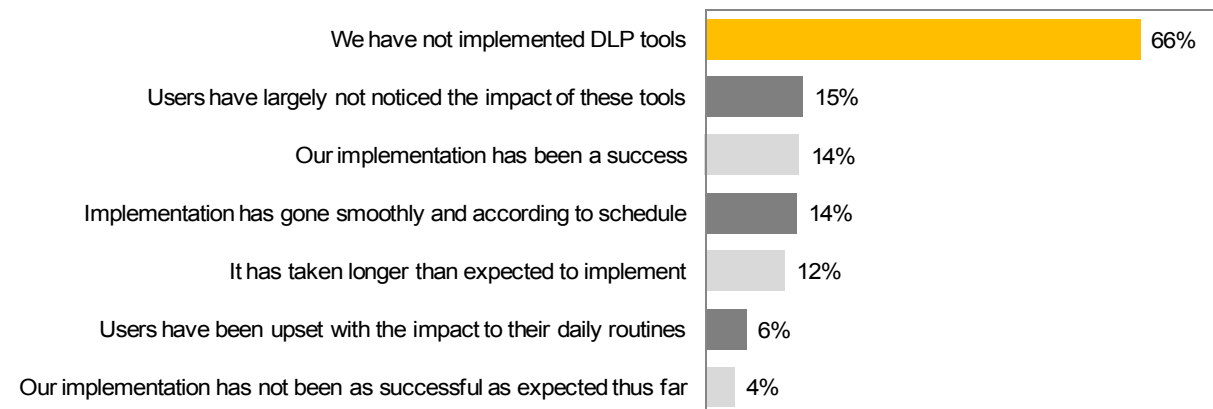
Survey results

Plugging the data leaks - Global

Organizations are moving ahead with policies, procedures and awareness campaigns to help identify holes through which data can pour, but whether it's enough is unclear

66% of respondents have not implemented data loss prevention (DLP) tools. These are systems that identify, monitor, and protect **data in use** (e.g. endpoint actions), **data in motion** (e.g. network actions), and **data at rest** (e.g. data storage) through deep content inspection, contextual security analysis of transaction (attributes of originator, data object, medium, timing, recipient/destination and so on) and with a centralized management framework.

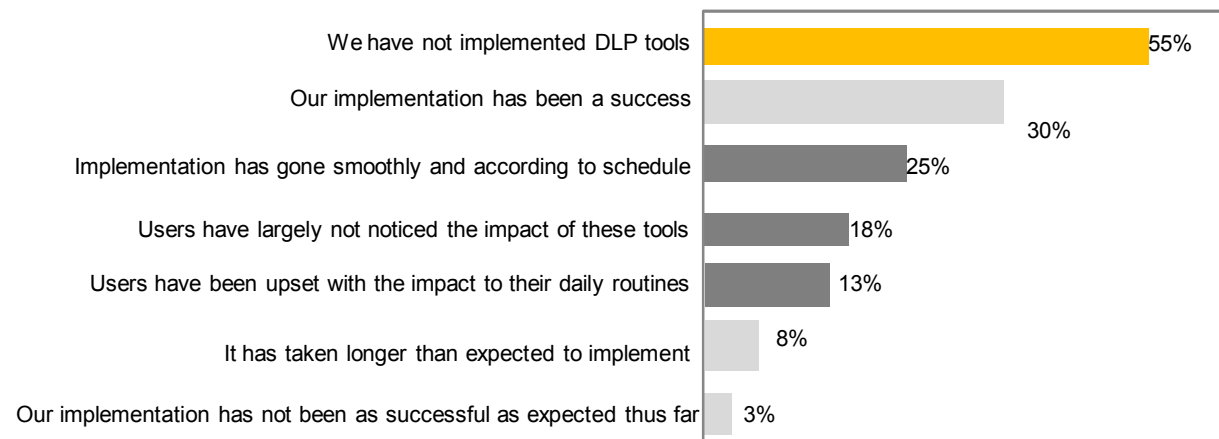
Regarding DLP tools implementation, how would you describe that deployment?



Plugging the data leaks - Zimbabwe

55% of respondents have not implemented data loss prevention (DLP) tools.

Regarding DLP tools implementation, how would you describe that deployment?

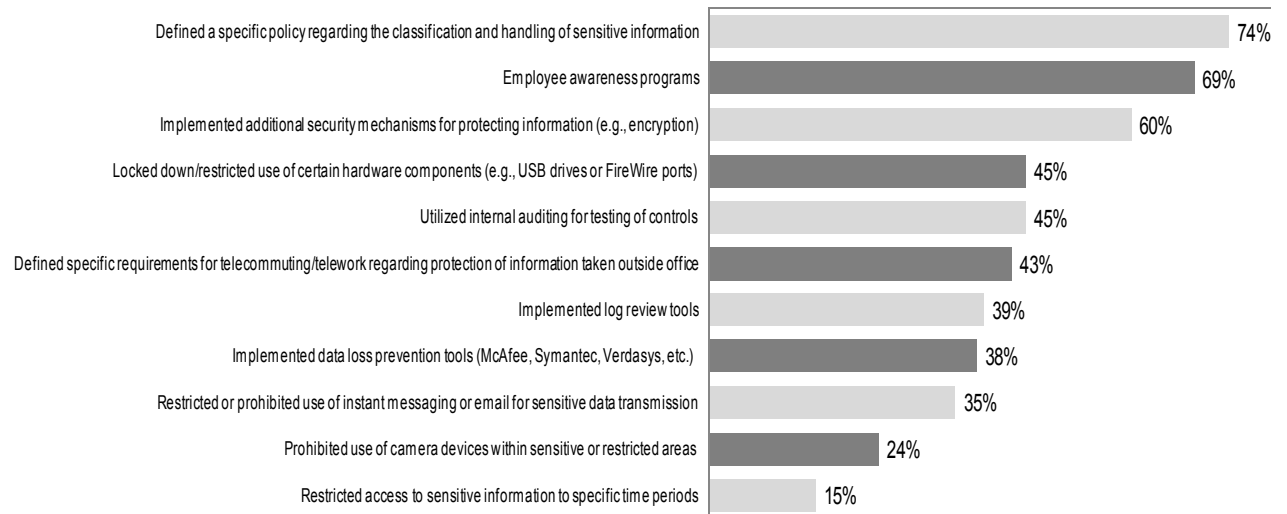


Plugging the data leaks - Global

Organizations are relying mostly on policies and programs as their first line of defense against data loss and leakage

74% of respondents have defined a policy for classification and handling sensitive data as control for data leakage risk.

Which of the following actions has your organization taken to control data leakage of sensitive information?

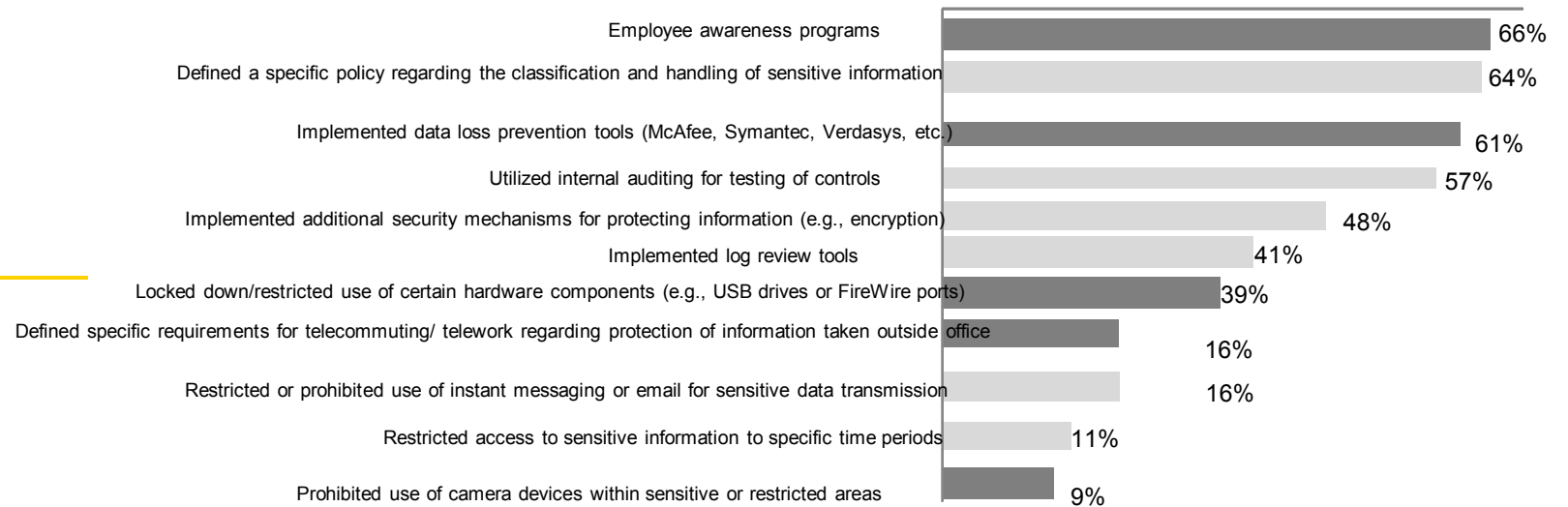


Plugging the data leaks - Zimbabwe

Organizations are relying mostly on policies and programs as their first line of defense against data loss and leakage

64% of respondents have defined a policy for classification and handling sensitive data as control for data leakage risk.

Which of the following actions has your organization taken to control data leakage of sensitive information?



Plugging the data leaks

Our perspective

- ▶ Assess, understand and appreciate the many potential risks and areas of data loss, specifically relating to the data loss channels that exist within the organization.
- ▶ Identify, assess and classify sensitive data so that DLP controls can be focused to provide protection for the most sensitive data.
- ▶ Take a holistic view of data loss prevention by identifying key DLP controls and measuring their effectiveness. All key controls, such as asset management and physical security controls, should provide accurate reporting of data loss risks and controls.
- ▶ Cover data in motion, data at rest and data in use within the organization's DLP controls.
- ▶ Implement incident investigation, enlist a strong team to carry out the program and seek the support of key stakeholders.
- ▶ Pay special attention to third parties with access to sensitive company data.
- ▶ Understand what data is sent to third parties, how it is sent and if the transmission mechanisms are secure.



Preparing for the worst

Survey results

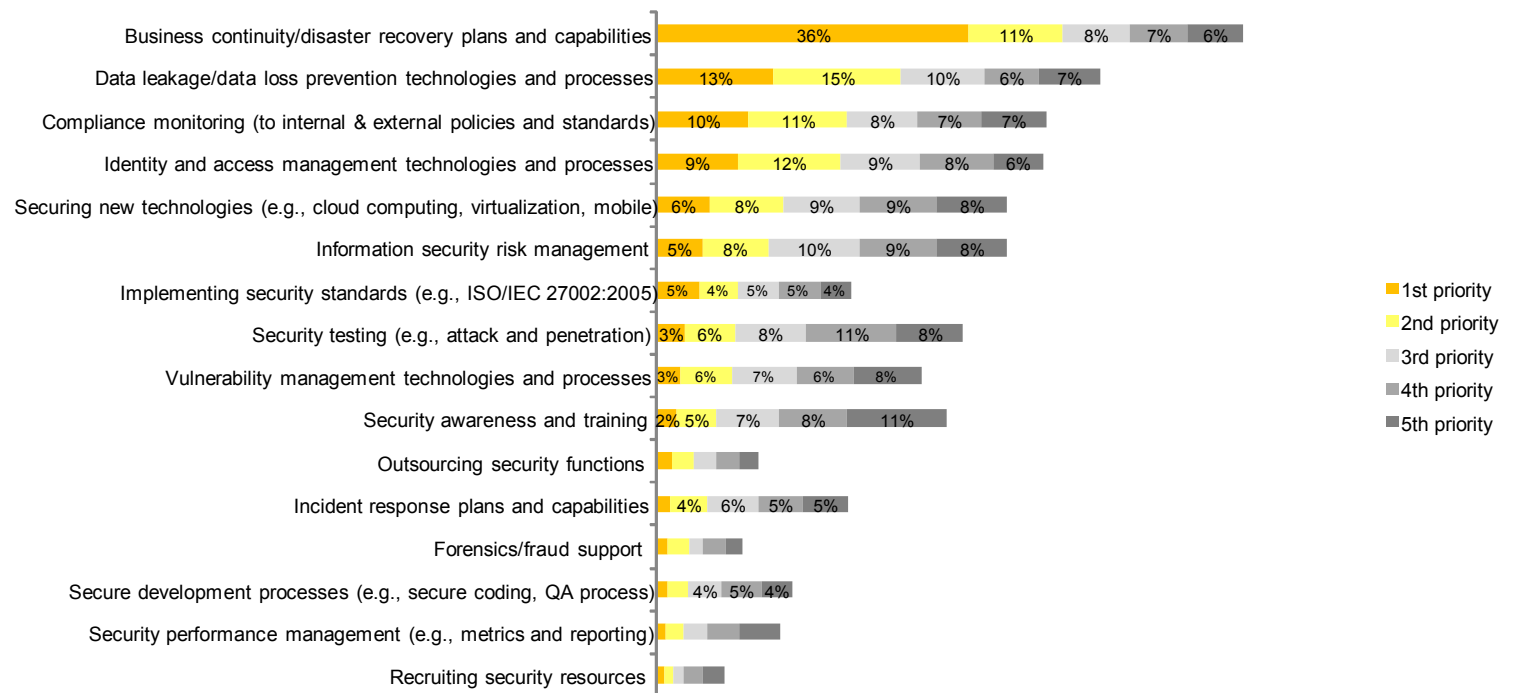
Preparing for the worst

Business continuity continues to be a top funding priority

A1

Nearly three times the number of respondents rated BCM a higher funding priority than their second-ranked priority.

Which of the following information security areas will receive the most funding over the coming 12 months?



Slide 40

A1

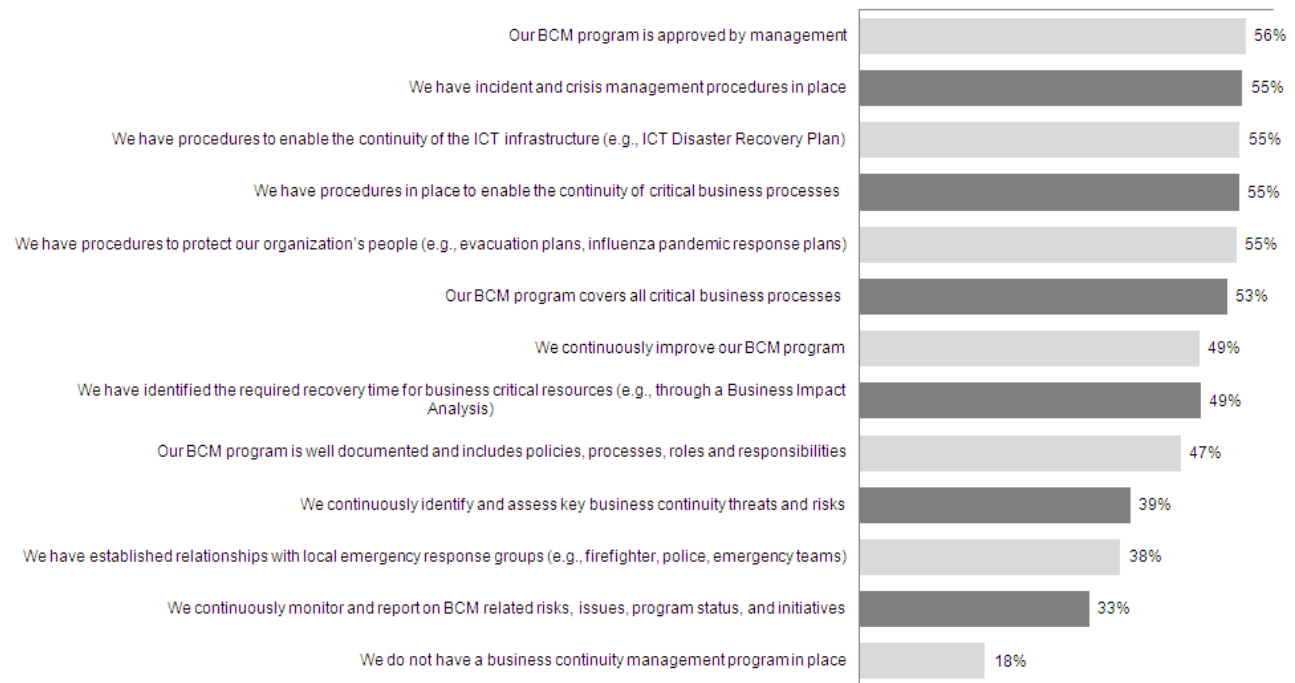
This key hangs way out over the edge. Can we redo this graphic or use the one used in the report?
Author, 2011/10/24

Preparing for the worst - Global

While the focus on business continuity - and the resources to support it - continues to be a top priority, most companies are still unprepared for catastrophic occurrence

For the second consecutive year, respondents have indicated that business continuity is their top funding priority.

Which of the following statements apply to your organization's Business Continuity Management (BCM) strategy and program?

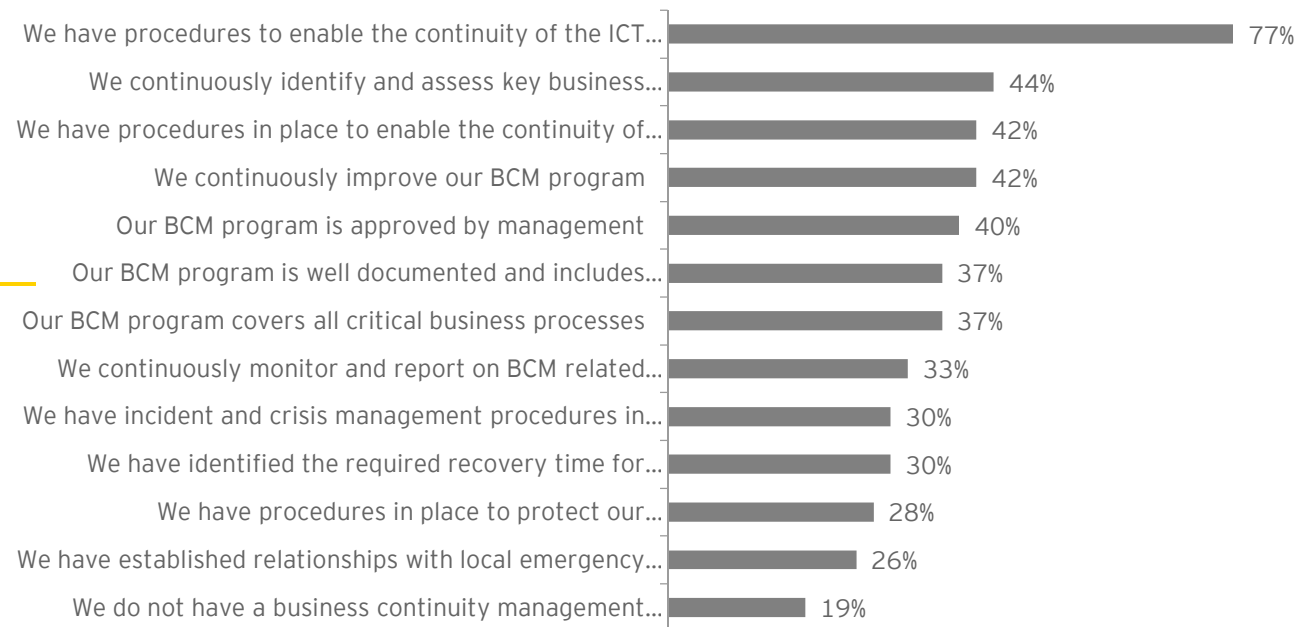


Preparing for the worst - Zimbabwe

While the focus on business continuity - and the resources to support it - continues to be a top priority, most companies are still unprepared for catastrophic occurrence

Respondents have indicated that business continuity is their top funding priority.

Which of the following statements apply to your organization's Business Continuity Management (BCM) strategy and program?



Preparing for the worst

Our perspective

- ▶ Prepare for and secure business continuity plans that anticipate high- impact, low-frequency events, and determine which are integrated into a broader risk management framework that focuses on protecting the organization from catastrophic loss.
- ▶ Assess whether the business continuity plan has the right level of maturity in light of the emerging trends and new technologies.
- ▶ Test the organization's business continuity plan frequently to help validate your business resiliency in practice. The more complex the scenarios that are tested, the better the coverage of the test.
- ▶ Solicit the support of the board and the audit committee for their business continuity programs.
- ▶ There is need for Zimbabwe to consider elevating business continuity management to executives and boards.
- ▶ We lag in incident and skills management



Looking into the future

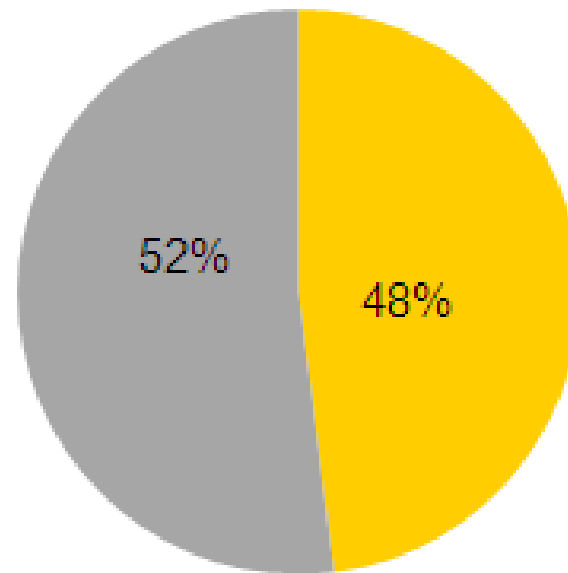
Survey results

Looking into the future - Global

Many companies are approaching information security without a plan

Nearly half of the responding organizations do not have an information security strategy.

Does your organization have a documented information security strategy for the next one to three years?

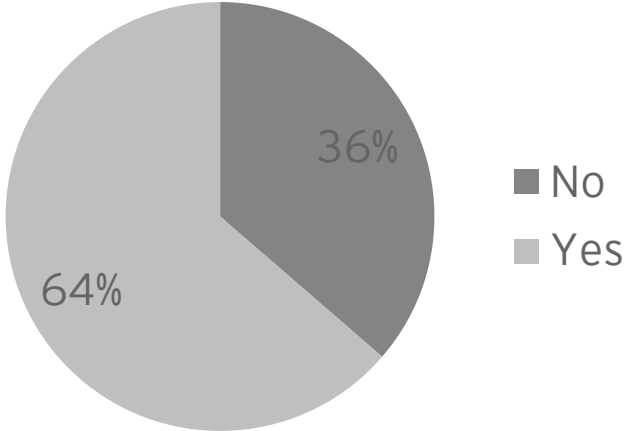


■ No ■ Yes

Looking into the future - Zimbabwe

Many companies are approaching information security without a plan

Does your organization have a documented information security strategy for the next one to three years?

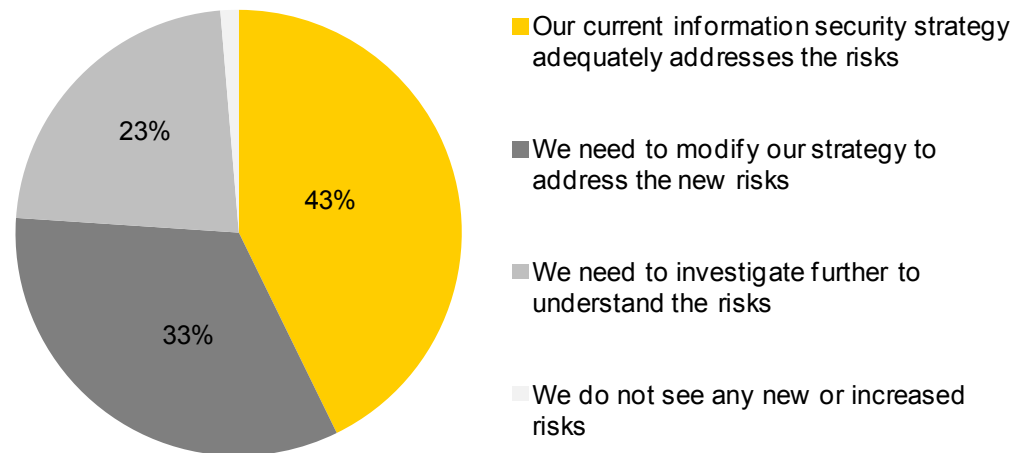


Looking into the future - Global

Just over a third of organizations do not have a information security strategy, and for the rest, plans continue to evolve despite a sense they may not be effective

56% of respondents indicated that their current information security strategy needs to be modified or needs further investigation.

Which of the following statements best describes your organization's information security strategy in relation to today's threat landscape?

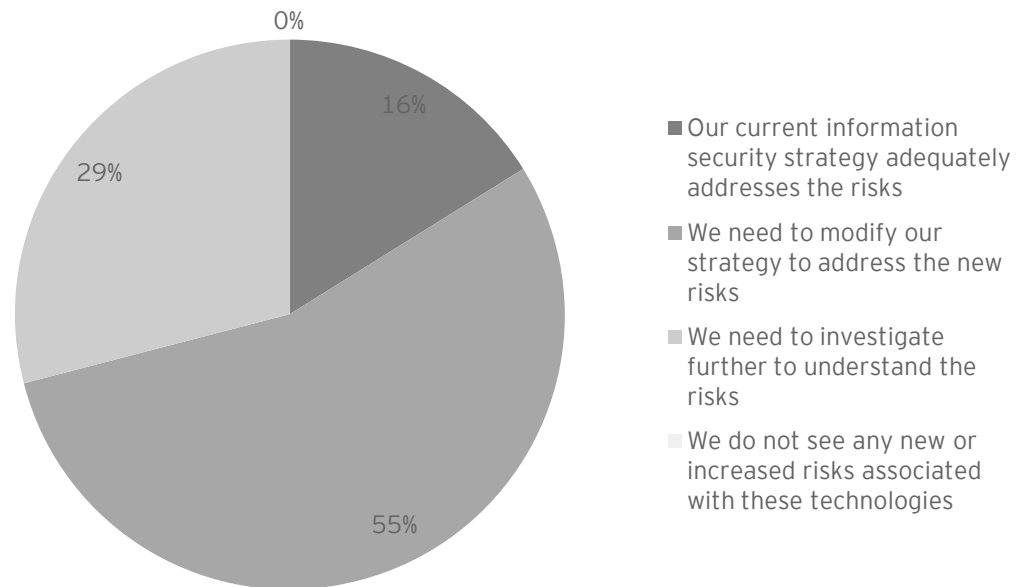


Looking into the future - Zimbabwe

Nearly half of organizations do not have a information security strategy, and for the rest, plans continue to evolve despite a sense they may not be effective

84% of respondents indicated that their current information security strategy needs to be modified or needs further investigation.

Which of the following statements best describes your organization's information security strategy in relation to today's threat landscape?

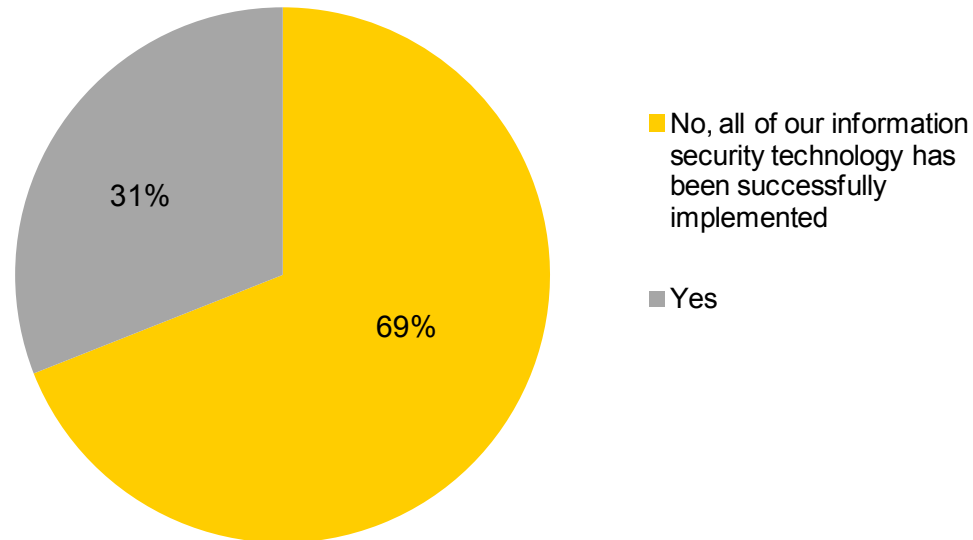


Looking into the future - Global

Nearly a third of respondents indicate that they have bought solutions which they later felt failed or under-performed

31% of respondents indicated that their organization has recently purchased information security solutions that are perceived as having failed or under-delivered.

Has your organization purchased software and/or hardware to support information security initiatives in the past 18 months which is perceived as having failed or under-delivered?

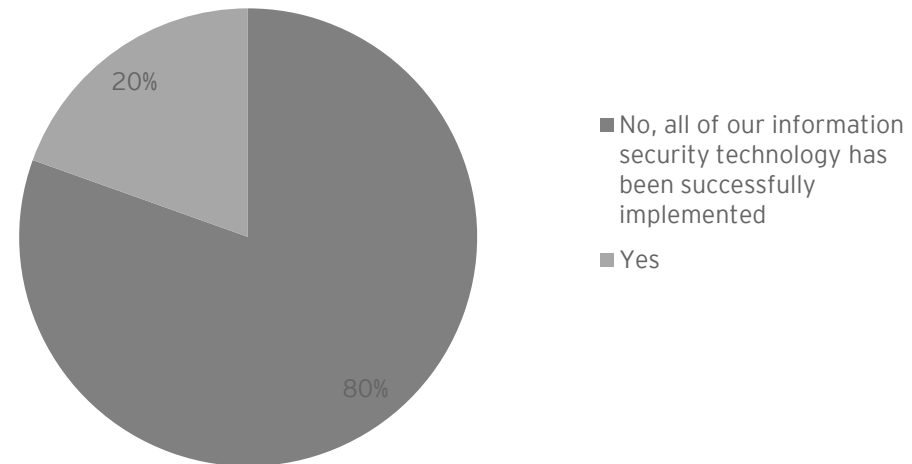


Looking into the future - Zimbabwe

Nearly one fifth of respondents indicate that they have bought solutions which they later felt failed or under-performed

20% of respondents indicated that their organization has recently purchased information security solutions that are perceived as having failed or under-delivered.

Has your organization purchased software and/or hardware to support information security initiatives in the past 18 months which is perceived as having failed or under-delivered?

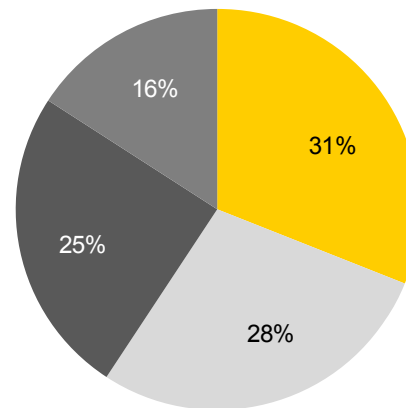


Looking into the future - Global

Most companies recognize the importance of having an IT risk management plan

84% of respondents indicated that they have an IT risk management program in place or are considering it within the coming year.

Do you have a formalized IT risk management program in place at your organization?



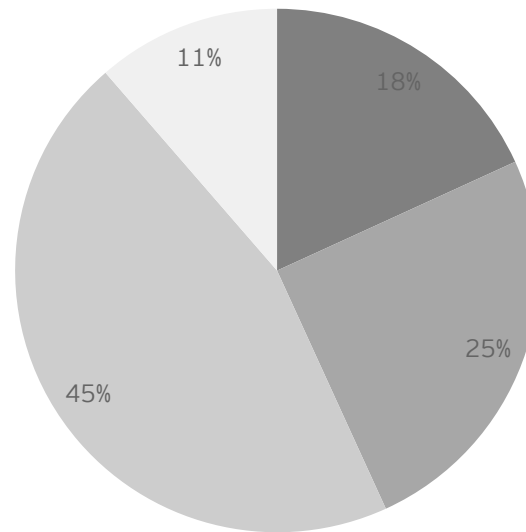
- Yes, we have an IT risk management program that has existed for less than three years
- No, but considering it within the coming 12 months
- Yes, we have had a well-established IT risk management program in place for more than three years
- No, and not considering it

Looking into the future - Zimbabwe

Most companies recognize the importance of having a IT risk management plan

89% of respondents indicated that they have an IT risk management program in place or are considering it within the coming year.

Do you have a formalized IT risk management program in place at your organization?



- Yes, we have had a well-established IT risk management program in place for more than three years
- Yes, we have an IT risk management program that has existed for less than three years
- No, but considering it within the coming 12 months
- No, and not considering it

Looking into the future

Our perspective

- ▶ Revisit your information security strategy to conform to the current risk landscape.
- ▶ Instead of acquiring the latest tools, focus on the fundamentals.
- ▶ Implement a structured, pragmatic approach to managing IT risk to make sure it focuses on the risks that matter. We see an IT risk management or governance risk and compliance (GRC) approach as a key future investment for many organizations.
- ▶ Address the entire IT risk universe in your IT risk or GRC program, which is broader than just information security.



Summary of survey findings

Key survey findings - Global

Introduction	<ul style="list-style-type: none">72% of respondents see an increasing level of risk due to increased external threats.49% of respondents stated that their information security function is meeting the needs of the organization.
Cloud computing	<ul style="list-style-type: none">61% of respondents are currently using, evaluating or planning to use cloud computing-based services within the next year.Almost 90% of respondents believe that external certification would increase their trust in cloud computing.
Mobile computing	<ul style="list-style-type: none">80% of respondents are either planning, evaluating or actually using tablet computers.57% of respondents have made policy adjustments to mitigate the risks related to mobile computing risks.
Social media	<ul style="list-style-type: none">Nearly 40% of respondents rated social media-related risks issues as challenging.53% of respondents have implemented limited or no access to social media sites as a control to mitigate risks related to social media.
Data loss prevention	<ul style="list-style-type: none">66% of respondents have not implemented data loss prevention tools.74% of respondents have defined a policy for classification and handling of sensitive data as a control for data leakage risk.
Business continuity management	<ul style="list-style-type: none">For the second consecutive year, respondents have indicated that business continuity is their top funding priority.
IT risk management	<ul style="list-style-type: none">56% of respondents indicated that their current information security strategy needs to be modified or needs further investigation.31% of respondents indicated that their organization has recently purchased information security solutions that are perceived as having failed or under-delivered.

Key survey findings - Zimbabwe

Introduction	<ul style="list-style-type: none">▪ 64% of respondents see an increasing level of risk due to increased external threats.▪ 41% of respondents stated that their information security function is meeting the needs of the organization.
Cloud computing	<ul style="list-style-type: none">▪ 25% of respondents are currently using, evaluating or planning to use cloud computing-based services within the next year.▪ Almost 20% of respondents believe that external certification would increase their trust in cloud computing.
Mobile computing	<ul style="list-style-type: none">▪ 76% of respondents are either planning, evaluating or actually using tablet computers.▪ 43% of respondents have made policy adjustments to mitigate the risks related to mobile computing risks.
Social media	<ul style="list-style-type: none">▪ Nearly 45% of respondents rated social media-related risks issues as challenging.▪ 64% of respondents have implemented limited or no access to social media sites as a control to mitigate risks related to social media.
Data loss prevention	<ul style="list-style-type: none">▪ 55% of respondents have not implemented data loss prevention tools.▪ 64% of respondents have defined a policy for classification and handling of sensitive data as a control for data leakage risk.
Business continuity management	<ul style="list-style-type: none">▪ 66% Most respondents have indicated that business continuity is their top funding priority.▪ 84% of respondents indicated that their current information security strategy needs to be modified or needs further investigation.
IT risk management	<ul style="list-style-type: none">▪ 20% of respondents indicated that their organization has recently purchased information security solutions that are perceived as having failed or under-delivered.

Other survey findings - Zimbabwe

Areas where are ahead of other firms - globally

- ▶ We are spending more (23%) on information security compared to other firms globally. This is because we are playing catch up for the period where there was little investments in IT and related risks. This figure is 10% higher than what companies spend last year.
- ▶ Globally firms top priority is spending on BCM and this is consistent with Zimbabwe although Zimbabwe is ahead on this metric by about 10%.
- ▶ Also 75% of Zimbabwe companies will spend more on data loss prevention technologies for the same reason mentioned above.
- ▶ The area likely to get least funding is forensics, likely because of the specialist skills required and that this service will be bought outside.
- ▶ More companies will spend on the implementation of standards. Areas likely to get the most funding are CoBIT, ISO 27002 and ITIL.
- ▶ 92% of companies have planned to carry out security testing in the coming 12 months (e.g. Attack & penetration exercise).
- ▶ 93% of companies indicated they will take time to look at emerging trends in IT and adopt based on relevance with 74% perceiving a challenge with the adoption of new technologies.
- ▶ 80% of respondents indicate the budget is one of their greatest challenges with regards to the implementation of IT risk management solutions.
- ▶ 66% see a challenge in the uncertainty of the business environment.
- ▶ Increased used of tablet computers, smart-phones and other mobile services is perceived to be posing a challenge to 67% of the respondents.
- ▶ 95% of respondent plan to implement data loss prevention tools.

Other survey findings - Zimbabwe

Areas where we are lagging other firms - globally

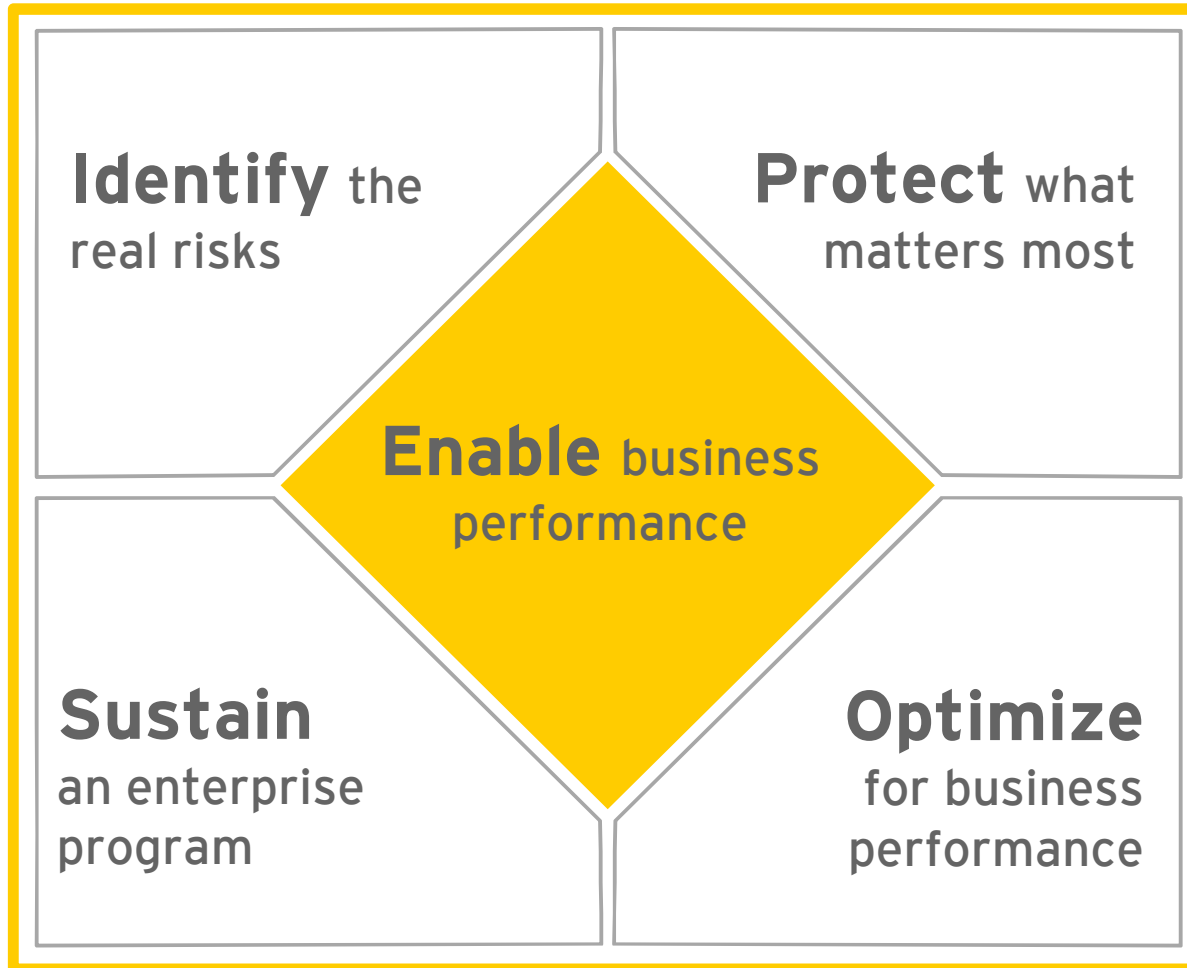
- ▶ Zimbabwean companies under estimate the internal threat compared with other companies globally (45% vs. 21%)
- ▶ We also lag in the following best practices in terms of controlling data losses due to mobile computing:
 - ▶ Encryption techniques (30% usage for Zim vs. 46% globally)
 - ▶ Architectural changes (14% usage for Zim vs. 30% globally)
 - ▶ Adjusted incident management processes (26% usage for Zim vs. 16% globally)
 - ▶ Mobile device management software (28% usage for Zim vs. 9% globally)
 - ▶ Policy adjustments (57% usage for Zim vs. 43% globally)
- ▶ We also lag on our security and awareness programs as it relates to social media (by 14%)
- ▶ We lag in the following with regards to data loss:
 - ▶ Defining policies regarding information that is taken outside the office (lagging by 27%)
 - ▶ Restricted the transmission of sensitive information through email / instant messaging (lagging by 19%)
 - ▶ Defining security policies for protection of information (lagging by 12%)
 - ▶ Laptop and desktop encryption (lagging by 33% and 14% respectively)
- ▶ In terms of testing of the networks, we lag in the following:
 - ▶ External networking vulnerability scanning and penetration testing lagging by 21%)
 - ▶ Application layer security testing (lagging by 10%)
- ▶ We are lagging the rest of the world in establishing ITRM functions by about 12%.
- ▶ Our BCM lags in the following areas: protecting our people (27% lagging); incident and crisis management procedures (25%); Recovery Time Objectives (19%) and inclusion of all business processes (16%).



Transforming your security program

Our services

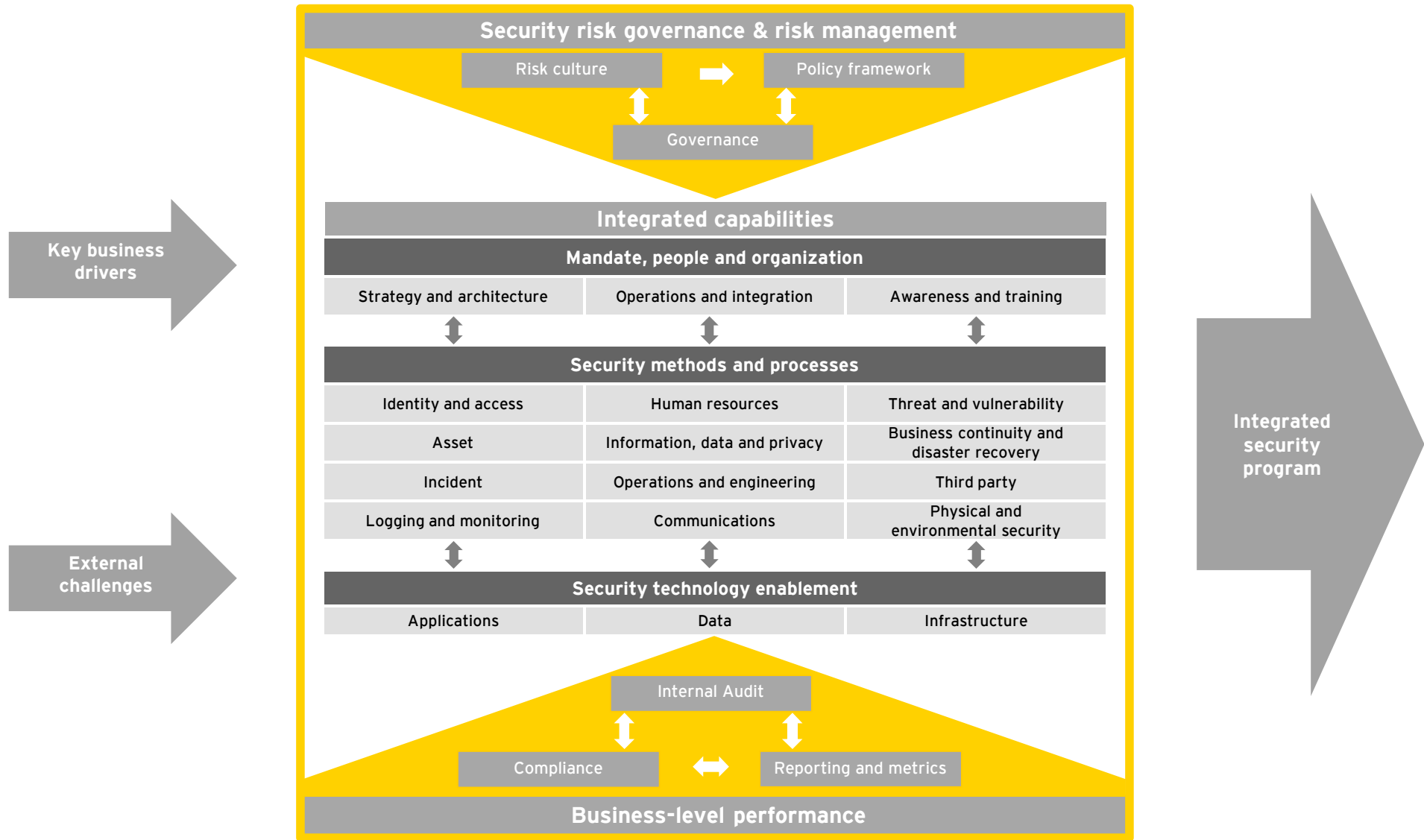
Transform your security program to improve business performance



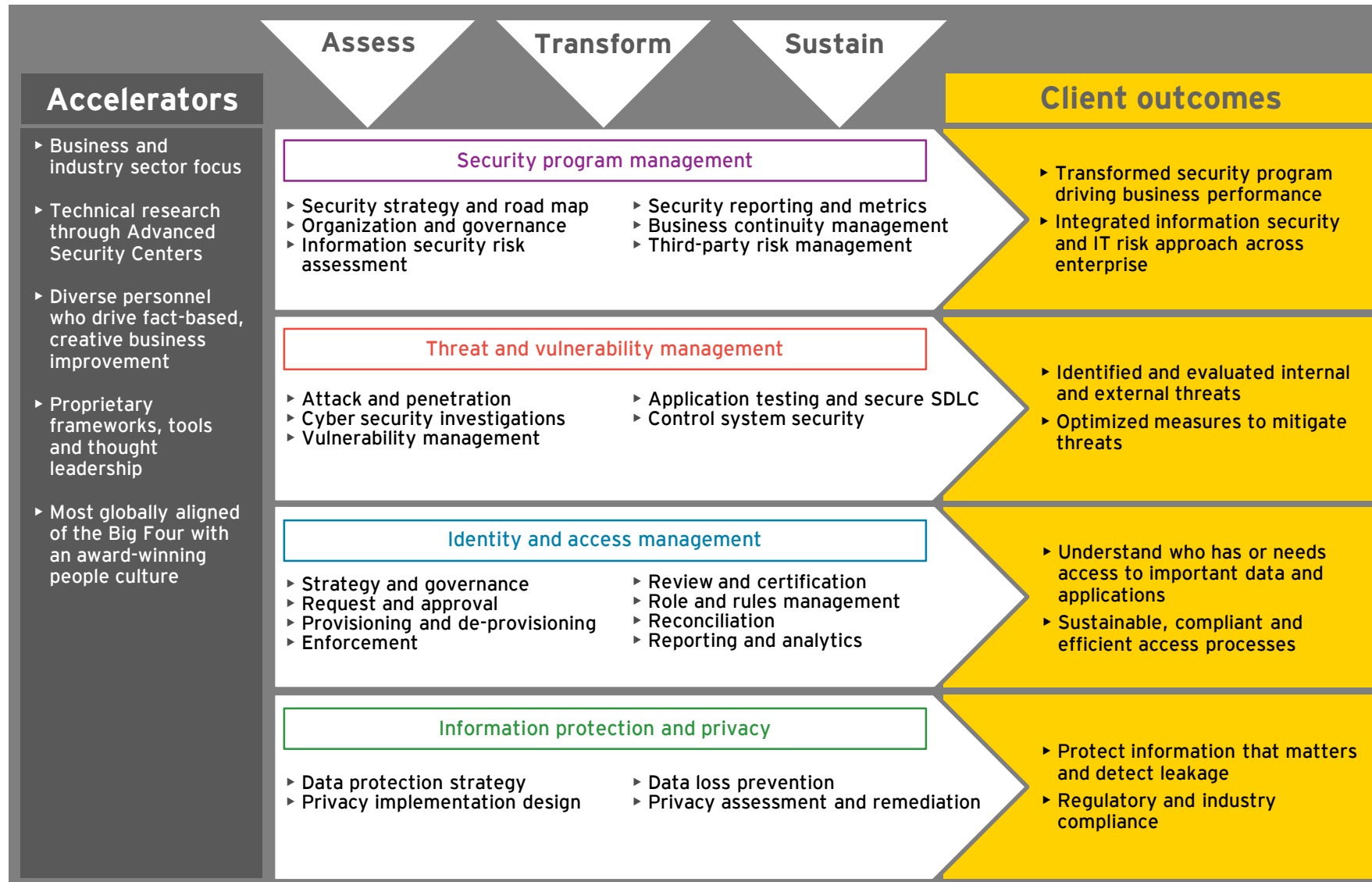
Five questions for the C-suite

- ▶ Do you know how much damage a security breach can do to your reputation or brand?
- ▶ Are internal and external threats considered when aligning your security strategy to your risk management efforts?
- ▶ How do you align key risk priorities in relation to your spending?
- ▶ Do you understand your risk appetite and how it allows you to take controlled risks?
- ▶ How does your IT risk management strategy support your overall business strategy?

Framework to enable your security program to address business needs



Ernst & Young information security services are focused on sustainable business improvement solutions





Related Insights

To see these and more, visit www.ey.com

Related Insights



Business continuity management

Only about half of companies have taken steps to address these potential disruptions and disasters. Organizations need to develop, maintain and sustain effective business continuity management programs.



Information security in a borderless world

Traditional security models that focus primarily on keeping the bad guys out no longer work. It's time to radically rethink how organizations can keep their most valuable assets safe.



The evolving IT risk landscape

A strategic IT risk management program helps address IT risks consistent with strategic corporate objectives and help set risk culture by providing management with a holistic, enterprise-wide perspective.



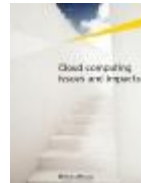
Mobile device security

New mobile technologies come with new risks that are specific to the various device platforms and technologies. These risks may be mitigated through technical device controls, third-party software, and organizational policy.



Countering cyber attacks

Given the continuous and persistent threat posed by new waves of attack channels and malicious entities, leading companies recognize the need to instill a new mind-set and approach toward the organization's security strategy.



Cloud computing: Issues and impacts

Cloud computing alters the technology industry power structure, and can improve business agility and access to computing, storage and communications power.



Data loss prevention: Keeping your data safe

Advances in technology and how users apply that technology, has increased the risk of data leakage. The blurry line between work and personal use of - and access to - data can result in unintentional leaks, as well as malicious ones.



Building confidence in IT programs

About two out of three large IT programs go over budget, are completed too late or do not deliver the expected benefits. Having the right information at the right time can help build confidence throughout the program lifecycle.



Contact Information

For any information on the survey and our services, please contact the following people:

Contact Details

Ernst & Young

Angwa City, Cnr Julius Nyerere Way/
Kwame Nkrumah Ave, Harare, Zimbabwe
Office: +263 4 750979/83 ,750905/14
Fax : +263 4 773842

Leonard Bore

IT Risk & Assurance (ITRA) Partner

Email Address: leonard.bore@zw.ey.com

Prosper Mugare

Email Address: prosper.mugare@zw.ey.com

Tafadzwa Mavhunga

Email Address: tafadzwa.mavhunga@zw.ey.com

Carol Mucherahowa

Email Address: carol.mucherahowa@zw.ey.com

Andrew T Zigora

Email Address: andrew.zigora@zw.ey.com

Farisayi Kusangaya

Email Address: farisayi.kusangaya@zw.ey.com