Insights on IT risk

April 2011

Information security in a borderless world

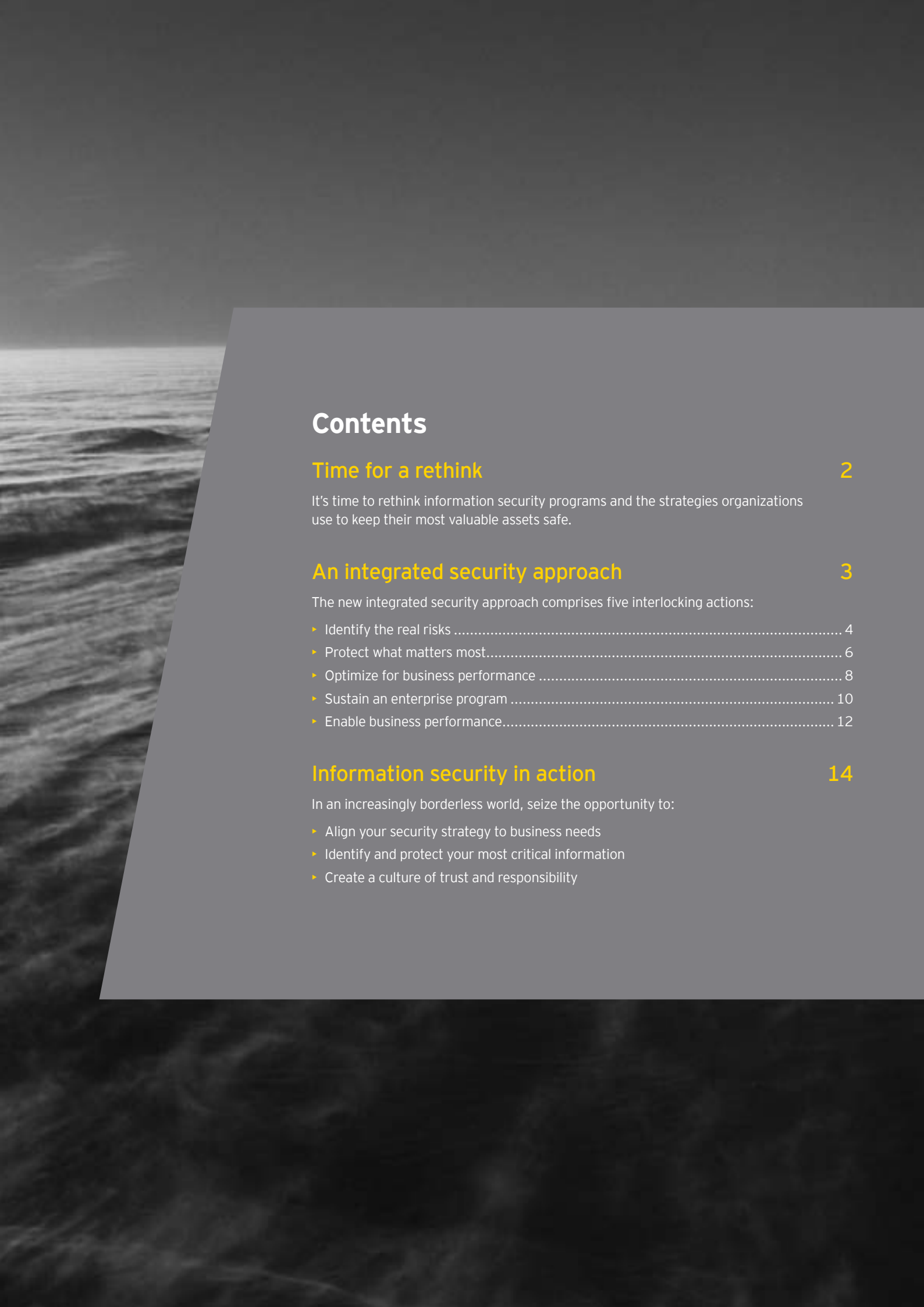
Time for a rethink

Ernst & Young

Quality In Everything We Do

Information security is a balancing act between the level of security and cost that poses two important questions:

- **What are the measures companies should take in today's hyper-connected, borderless world?**
- **When are companies secure enough?**



Contents

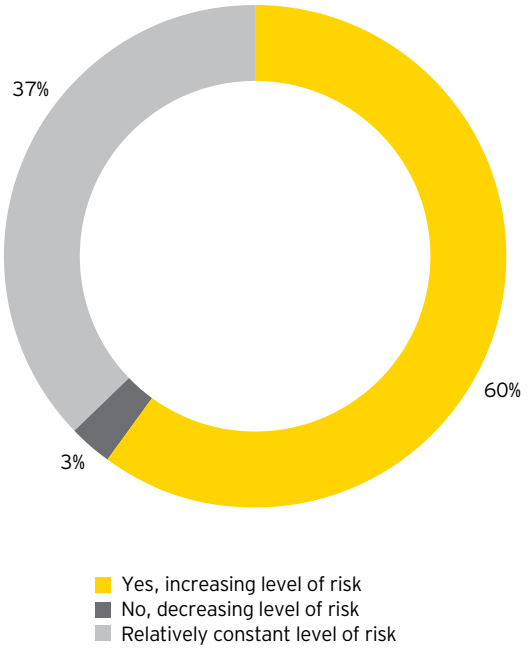
> If your organization is looking only to the past for ways to protect the future, your information security program is already out of date.

Introduction

Time for a rethink

Traditional security models focus on keeping external attackers out. The reality is that there are as many threats inside an organization as outside. Mobile technology, cloud computing, social media, employee sabotage — these are only a few of the internal threats organizations face. Externally, it's not just about the lone hacker who strikes for kicks. Overall, the risk environment is changing. As we learned in *Borderless security: Ernst & Young's 2010 Global Information Security Survey*:

Given current trends towards the use of such things as social networking, cloud computing and personal devices in the enterprise, have you seen or perceived a change in the risk environment facing your organization?



Shown: Percentage of respondents

Source: *Borderless security: Ernst & Young's 2010 Global Information Security Survey.*

It's time to rethink information security programs and the strategies organizations should use to keep their most valuable assets safe. Information security should be strategically aligned with the broader business agenda and based on an organization's risk tolerance. What constitutes an acceptable level of information security risk in an environment when intellectual property, personal customer information and the brand are at stake? It's a tough decision, but one that should be made to form the foundation of a transformational information security program.

Advancing technology has created access to information that is far too big for barricades. Instead, companies need to learn how to securely embrace change. Our integrated security approach can help your organization build a program that enhances trust with your customers, vendors, business partners and employees — in a way that is cost-effective and sustainable.

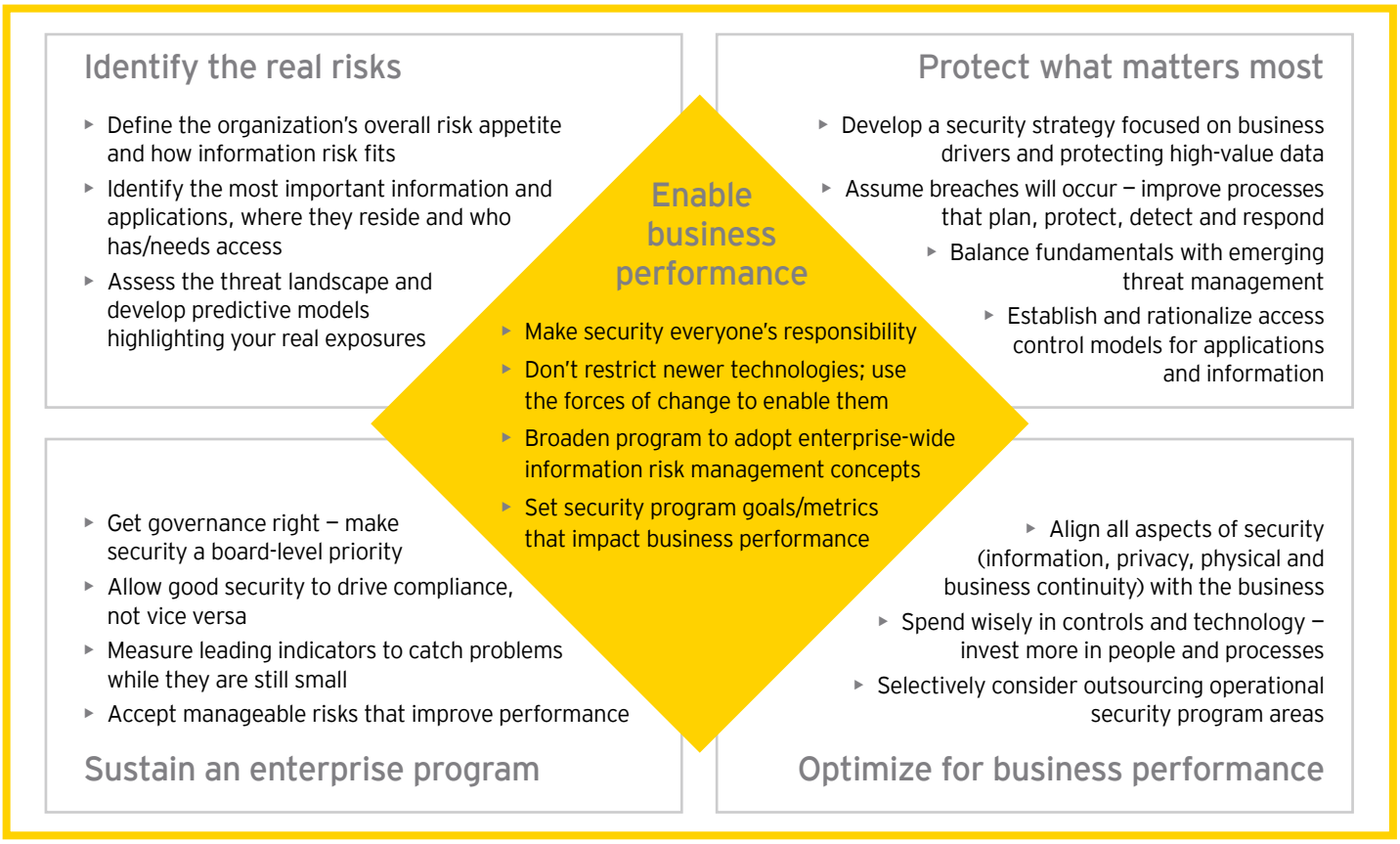
Topics to rethink

- Traditional security models that primarily focus on keeping external threats out of the organization are no longer effective. The new security model is predictive and enterprise-wide.
- To protect your organization's information, business owners and security teams need to identify the most important information and applications, where they reside and who has or needs access to it.
- Attacks are inevitable. Focus on solutions that plan, protect, and detect and respond to threats. Use the right protections for the information most at risk.
- The fundamentals are as important as ever, but they need to be balanced with emerging threat management.
- Spend wisely in controls and technology to improve performance. Consider selectively outsourcing some pieces of your program.
- Get governance right — make security a board-level priority.
- Increase security measures by enabling the appropriate use of new technology rather than banning it.

An integrated security approach

Predictive and enterprise-wide

It's time to shift perspective. Information security is not a "check the box" compliance exercise. No one solution can inoculate a network from attack, and protecting information is not solely IT's responsibility. Instead, the new integrated security approach is predictive and enterprise-wide. It proactively protects while anticipating the worst. It embraces rather than bans. It focuses on trust, not paranoia. Here are the elements of a transformational information security strategy that your organization can use to build trust in a borderless world.



> If you don't think you have any real risks, you haven't looked.

Identify the real risks

Identify the real risks

- Define the organization's overall risk appetite and how information risk fits
- Identify the most important information and applications, where they reside, and who has/needs access
- Assess the threat landscape and develop predictive models highlighting your real exposures

Often, security professionals complain that they are too busy reacting to immediate issues and have no time to anticipate what may be lurking around the corner. To have any hope of protecting your organization's critical assets, both the business and security teams need to understand where your information lives, inside or outside. Identifying what your organization classifies as its most important information and applications, where they reside and who has or may need access to them will enable the business to understand which areas of the security program are most vulnerable to attack.

After understanding where information resides, assess the threat landscape and develop predictive models that can highlight your real exposures. The following represent some of the more relevant threats that organizations face:

- **Internal threats.** The recent WikiLeaks release of classified U.S. State Department diplomatic cables is an excellent example of malicious attacks from within. In this case, a low-ranking U.S. Army intelligence specialist has been accused of disseminating classified information, which was ineffectively controlled. But the threat doesn't stop there. Insider threats are even more prevalent than outsider threats, either accidentally or intentionally. Organizations have failed to understand the importance of internal threats for far too long – this risk will only increase if it isn't addressed now.
- **Cloud computing.** Increasingly, organizations are turning to cloud computing providers because of several potential advantages, including significantly less initial investment, fewer skilled internal IT resources and lower operating costs. However, for all the intended benefits, cloud services raise security risks and regulatory challenges as personal information and intellectual property potentially cross borders. Since not every country places a premium on information security and privacy, the ability to adhere to many of the regulations is daunting. Additionally, concerns are raised regarding the core security practices the cloud providers follow. Even in jurisdictions that have a high regard for privacy, there may be exceptions. For example, certain US regulations would allow authorities to access personal information (in specific circumstances) residing with a third-party cloud provider without first notifying the information owner or subject.
- **Mobile devices.** The proliferation of consumer-oriented mobile devices in recent years has dramatically altered the flow of information in and out of organizations. Employees commonly use media-enabled smartphones and tablets – often owned by the individuals – to access company information anywhere and anytime. While increasing employee productivity, it comes with a number of threats and risks. Many organizations think that banning many of these devices is the answer to reducing risk, but in reality, such restrictions may only increase their use. The real answer is to enable them with the right security protections.

Case in point

Many successful compromises of information security start by exploiting a small weakness to achieve a much larger goal. For example, during a recent security assessment, our security team was able to compromise an individual account simply by using the client's standard reset password process and by doing a small amount of research for publicly available information. By discovering some of the key answers to the questions ("What was the name of your first pet?" and "What is your mother's maiden name?"), the team was able to successfully reset the user's password and then log on as that person, resulting in a compromise of the HR system for which that user was authorized. Based on these results, the organization adjusted its policy, process and control for identity and access management.

- **Cyber attacks.** Although organizations have been dealing with opportunistic cyber attacks for years, many now find themselves the target of more sophisticated and persistent efforts. These attacks are focused on a single objective, often lasting over a long period of time and until the desired target is obtained. They leave few signs of disturbance, because they are designed to remain hidden to acquire as much sensitive information as possible. In our experience, those at the greatest risk are information-intensive entities or organizations with intellectual property that is most attractive in emerging economies. Unfortunately, many organizations have no idea they are compromised until it is too late.
- **Social media.** Now more than ever, people are driven to use social media. As the technology evolves, the lines between personal and professional interactions increasingly blur. Employees need to understand how their use of social media — at home or at work — could jeopardize the organization's security and success. Unfortunately, information loss is often an unintended consequence of an employee's behavior. Organizations need to implement enterprise-wide awareness programs for employees on their personal responsibility for protecting the organization's intellectual property. Organizations need to ensure that information security is everyone's responsibility.

Getting ahead of the threats

In today's security world, the term "threat" is about much more than keeping the bad guys out. Traditional information security solutions that focus on external threats can expose organizations to other forms of attack, especially from within.

Know your program's weaknesses and get ahead of both the internal and external threats to your organization's network, information and brand:

- **Define the organization's risk appetite.** An organization's risk appetite depends on its risk culture. By effectively understanding an organization's culture, you can align its potential exposure to the risk it is willing to take.
- **Identify the most important information.** It's not good enough to make an educated guess. Identify, inventory and prioritize the information's value. Placing a value on information based on the organization's broader business strategy will enable you to prioritize the assets that matter most.
- **Assess the threat landscape.** Today's security assessments need to focus on knowing where the information resides, who has or needs access to it and how it could be compromised. Understanding how information is used helps to identify the threats against it. For example, a national health care organization recently sent people into the field to determine how employees and third-party suppliers were using information. By actually seeing how information was shared, the organization could identify areas of security risk and take appropriate action.
- **Develop predictive threat models.** Once your security team identifies the areas of risk, it is useful to run through threat scenarios. These exercises help you understand and quantify the probability of a breach occurring in each specific risk area, the size of the vulnerabilities and the level of damage a security breach could cause.
- **Determine appropriate protection mechanisms.** Use the threat model that has been developed to apply controls commensurate with the level of risk.

Three key questions

- What is your organization's risk culture?
- Are you detecting and monitoring threats inside and outside the organization?
- Have you anticipated new technology risks, such as mobile devices, social media and cloud computing?

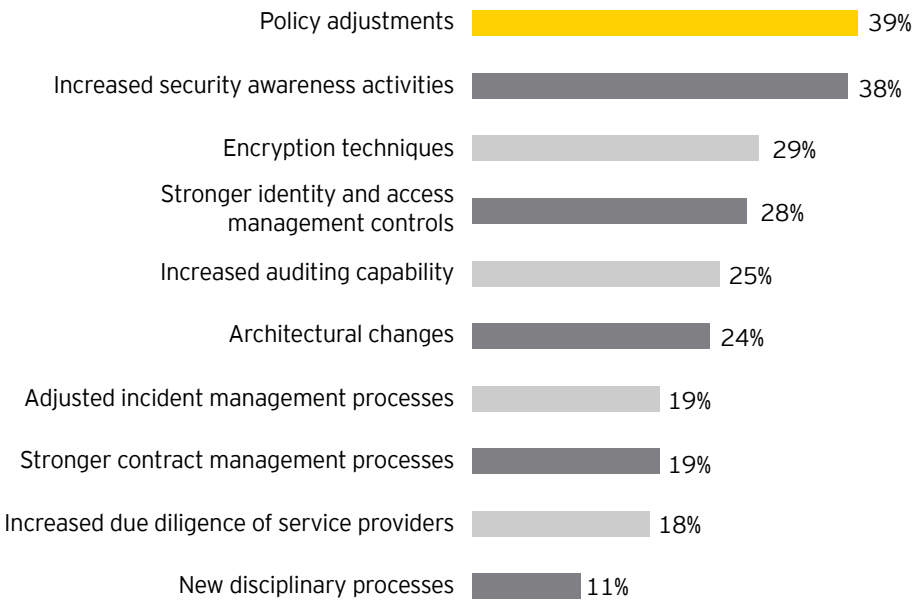
Protect the information that matters most

Protect what matters most

- Develop a security strategy focused on business drivers and protecting high-value data
- Assume breaches will occur — improve processes that plan, protect, detect and respond
- Balance fundamentals with emerging threat management
- Establish and rationalize access control models for applications and information

There is no such thing as being 100% secure anymore. Instead, organizations need to develop a focused strategy that protects the information that matters most and responds quickly when a breach occurs. In *Borderless security: Ernst & Young's 2010 Global Information Security Survey*, we took a look at the steps organizations are taking to address new or increasing risks. Among respondents, the top three controls their organizations are implementing are: policy adjustments (39%); increased security awareness activities (38%); and encryption techniques (29%) .

Which of the following controls have you implemented to mitigate the new or increased risks?



Shown: Percentage of respondents

Source: *Borderless security: Ernst & Young's 2010 Global Information Security Survey*

Case in point

An oil and gas company didn't believe it had any data leakage issues. However, based on an attack a peer experienced, the company decided to hire an outside provider to ensure that its information was secure.

On day two of Ernst & Young's assessment, our team discovered that a foreign jurisdiction was stealing sensitive information about proprietary intellectual property and sending it overseas. Our client had no customers in that jurisdiction and no good business reason for the information to be flowing in that direction.

Based on the results, which surprised the board and the audit committee, the organization completely rethought its approach to handling information — how to protect information, yet enable its use.

> Smart companies are shifting their focus toward building effective predictive detection and response capabilities.

Detect and monitor

Smart companies are shifting their focus toward building effective predictive detection and response capabilities. This means capturing new information sources, storing the information longer and analyzing it to detect signs of intrusion or abnormal activity that indicates compromise. Since today's threats operate stealthily, simply running an intrusion detection system to flag known malicious behavior is not enough. Your security teams should be able to use predictive indicators to analyze network activity that may seem legitimate — but is in fact harmful.

Effective threat management only starts with detection. After that, it is critical to have the capacity to respond to attacks when they are detected. Benchmarking reveals that incident response teams are an increasingly important part of today's information security team. While incident response used to be limited to battling viruses or worms, today's incident responders must be not only technically deep, but also able to forge relationships with peer organizations for information sharing, collaborate with government agencies for intelligence and lead large global teams.

Data loss prevention

Data loss prevention tools (DLP) are known for their ability to stop insiders from copying information to a removable drive or emailing files to a competitor. In this context, it is important to build strong cross-functional teams and set clear policy before turning on a tool.

Even so, keep expectations real; the best-implemented DLP help identify broader areas of risk — and in many cases prevent data loss — but DLP cannot prevent an insider who is determined to steal information or a sophisticated attacker tasked with collecting intellectual property. Understanding these limitations means your organization can realize value by stopping inadvertent, non-malicious data loss and using the tools to raise awareness among users.

DLP can also be effective as an aid for detection and response. Even in organizations that are reluctant to enable DLP blocking — for fear of disrupting a business process — DLP can be an outstanding input for a broader detection effort. Its alerts can point to coordinated attempts at insider information theft, and its inventory capabilities can inform incident responders of the criticality of a compromised asset.

Optimize controls

Today's IT risk organization is often at the nexus of privacy, information protection and IT compliance efforts. In fact, in *Borderless security: Ernst & Young's 2010 Global Information Security Survey,* 36% of organizations said that regulatory compliance is one of their top five areas of IT risk. Yet many still take a siloed approach to compliance. Leading organizations are taking a more holistic, consolidated approach to risk. Collapsing multiple sets of controls into a single governance framework removes duplication and simplifies compliance — sometimes reducing the effort by half. More efficient compliance means more time to focus on emerging threats and better security.

Three key questions

- Have you considered automating security controls?
- Are your security teams using predictive indicators to analyze seemingly legitimate network activity?
- Are your resources focused on emerging threats?

Balance the fundamentals

Optimize for business performance

- Align all aspects of security (information, privacy, physical and business continuity) with the business
- Spend wisely in controls and technology — invest more in people and processes
- Selectively consider outsourcing operational security program areas

The smartest companies are aligning all aspects of security (information, privacy, physical and business continuity) with the business. They are also taking the following actions to stretch their spending, focusing on the right investments, optimizing spending on mature fundamental security mechanisms and diverting spending to emerging threats.

Balance priorities and investments

Sound information security still emphasizes security fundamentals. However, many organizations are spending so much time and money on basic operations that they have neglected the emerging threats.

There is no question that the building blocks of a security program — configuration and patch management, simple policies with measured compliance, basic access control validation and strong asset inventories — are crucial.

It may also be time to tip the balance back in favor of people over technology. When it comes to information security fundamentals, technology alone is not the best investment. Hardware and software depreciate and become obsolete. People, on the other hand, learn and adapt. It may seem easy to look at information security as a problem solved by hardware and software, but as threats begin to evolve faster than technology can cope, a well-trained, technically deep security staff can be your best line of defense. Recognize the importance of investing in people across the organization who understand information security — centralized and decentralized. Stress a culture of "the information security team includes all employees." Educate everyone on their role, align the security team with key business leaders and seek sponsors in the business units. However, it is important to maximize the investment organizations already have in their people by enterprise-wide emphasis that information security is everyone's responsibility.

Case in point

During the integration process following a recent acquisition, a global organization took a hard look at the overall effectiveness of its security organization, its processes and its technology. Ernst & Young's analysis uncovered many areas for optimization, including:

- Streamlining its various compliance frameworks and controls by consolidating them into a more thorough governance framework addressing multiple compliance needs at once
- Significantly reducing its spend on vulnerability management by outsourcing desktop and PC management
- Enhancing the tools it had deployed for identity and access management by enabling new self-service features that eliminate a significant number of help desk calls

> Drive value from the investments you are already making. And spend more in the areas with the most risk.

Spend wisely

Borderless security: Ernst & Young's 2010 Global Information Security Survey found that nearly half of all information security budgets were increasing in 2011, a pattern that we have seen for several years. Yet 97% of respondents indicated that their risk posture was the same or worse than in prior years. New technology is needed to stay ahead of an evolving threats, but you can do more to increase efficiency by providing more resources to stay ahead of the threats and by optimizing what exists now before seeking new technology.

Outsource selectively

Selectively outsourcing the most highly operationalized portions of your information security program can free up resources for tasks with higher value. Outsourcing such standardized processes as security operations, patch and configuration management, device management and first-tier alert handling can leave internal staff to manage more critical issues.

Use technology appropriately

The information security industry has been accused of being driven by fear, uncertainty and doubt. Too many organizations use technology as the answer to their security problems but often fail without the surrounding processes. Additionally, companies often acquire but under-deploy large quantities of "shelfware." Many would acknowledge that their existing tools produce huge quantities of information that goes without being analyzed, contain features that have not been enabled or are outdated. To get the most from your technology, build use cases first, before even looking at the new technical features of the latest tool. Then ask how your organization can meet those use cases by first mining existing information, using latent functionality or re-engineering existing processes.

Three key questions

- Are you balancing spending among key risk priorities?
- Have you investigated the latent functionality of your existing tools?
- Are you outsourcing any of your information security?

> You will make mistakes. Catch them early, and keep them small.

Reach beyond compliance for sustainable security

Sustain an enterprise program

- Get governance right — make security a board-level priority
- Accept manageable risks that improve performance
- Allow good security to drive compliance, not vice versa
- Measure leading indicators to catch problems while they are still small

Get board-level attention for governance and setting risk tolerance

Leading organizations are making information security a board-level priority. Two key issues for the board are establishing a solid security governance foundation and setting a process for determining acceptable levels of risk tolerance for the organization. Leading organizations have a board-level committee for IT governance and oversight, including security, as well as enterprise-wide IT risk councils. We recommend a periodic update to the board of directors at least annually that includes results from compliance audits, significant incidents and the status of key initiatives.

The board is also involved in determining that information security is strategically aligned with the organization's broader business agenda, based on its acknowledged risk tolerance. An alignment issue is determining a level of security investment that is aligned with risk tolerance levels. The real cost of security is the total investment in the security program plus the cost of any security incidents, when they occur. Lower security program investment creates a risk of higher costs related to security incidents. Conversely, by increasing the investments in the security program the total cost of incidents should drop, resulting in falling total security costs. The 'balancing' act is aligning the accepted risk tolerance of the organization to the total security costs. There is a baseline cost of security programs, as many organizations find additional investments in security measures have a decreasing level of effectiveness and will not result in a correlated drop in security incidents.

Case in point

For five years, a financial institution had been investing in a program to identify and develop treatments to remediate 10 years of known extreme information security risks. With Ernst & Young's help, the company undertook efforts to embed a sustainable risk management practice into the program within an accelerated three-year time frame. The project was launched in one division of the organization, with the intention of expanding it to other divisions depending on its success.

Within the three-year commitment, the organization was able to:

- Improve its information security risk audit rating
- Reduce more than a dozen business risks
- Free up audit capital
- Reduce extreme risks by a double-digit percentage

The program was so successful that the company began a scaled deployment of a similar program across the Asia-Pacific region.

"There's been amazing change in the past few years in the regulatory environment around information protection. We are only going to see more laws and regulations in the years ahead. Responsible companies are looking to get ahead of these regulations to avoid disruption to business processes and to work toward global, seamless standards and processes that enable, and in fact accelerate, growth."

Nuala O'Connor Kelly, Senior Counsel, Information Governance & Chief Privacy Officer, General Electric

Let security drive compliance

Organizations that focus their security programs on just being compliant fall short in being secure. Recent cases of information loss showed that organizations were "compliant to the standard" but they were not secure enough. Breaches occurred because of insecure practices rather than non-compliance to the regulatory standard. Regulators globally do not agree on exactly what information or how much of it needs to be protected. As such, regulations do not define in detail how to protect an organization's information. They are behind in addressing developments such as social networking and mobile devices, as well as the privacy of personally identifiable information. In an effort to catch up, lawmakers are trying to understand how to protect information in the public realm and in the corporate domain. Regulators are also beginning to demand that organizations not only demonstrate that they have implemented a compliance program, but also provide proof that it works.

Obviously, regulatory compliance has to be a critical element of any information security strategy. However, it shouldn't be the only driver, particularly since it doesn't guarantee safety against existing or emerging threats. Being in compliance is not the same as being secure. International information security standards are a helpful guide in driving security initiatives, but the real success comes in the implementation. Standards and regulations do not guarantee security across the enterprise.

Measure leading indicators

Traditional security metrics tend to look backward — vulnerability counts, compliance with policy, missing patches, percent completion on initiatives — or they focus on seemingly relevant security statistics that have little bearing on the actual security of the information that organizations are trying to protect. For example, traditional security dashboards might report the number of alerts generated by intrusion detection systems, scans seen on perimeter devices and the number of times malware has been blocked. But these metrics may not be relevant or they may not be sufficient. In congressional hearings about the effectiveness of the Federal Information Security Management Act (FISMA), the congressional committee members acknowledged the ineffectiveness of compliance-based metrics.[1]

Numerous federal CIOs and security experts acknowledged that despite billions of dollars spent on compliance-based measurement for FISMA, it has done little to improve security in the US Government. Sadly, many US companies still follow the same approach.

Instead, focus on output-based metrics. While traditional metrics should still be tracked, the focus should be on the critical few metrics that really matter:

- The number of actual information security compromises
- The number of business records lost through an attack
- The time it takes for the organization to recover from a breach

These metrics align directly with business objectives of competitiveness and data integrity, as opposed to other measurements, such as patching effectiveness or compliance with security policies.

These leading indicators will enable you to catch problems while they are still small. The small mistakes will alert you to the unintended consequences of security decisions or actions. As a result, your organization will be able to make smarter risk-based security decisions, spend wisely on information risk management and act more effectively on security areas that pose the most risk.

Three key questions

- Are you taking controlled risks rather than eliminating risks altogether?
- Are your key indicators trailing or leading?
- Is information security a board-level priority?

[1] David Perera, "FISMA blasted at House hearing," FierceGovernmentIT, 24 March 2010.

> Don't ban new technologies. Use the forces of change to enable them.

Don't ban – embrace change

Enable business performance

- Make security everyone's responsibility
- Don't restrict newer technologies; use the forces of change to enable them
- Broaden the program to adopt enterprise-wide information risk management concepts
- Set security program goals/metrics that impact business performance

In the face of rapid change, your organization has two choices: resist it or embrace it. We firmly believe in the latter, as embodied in our integrated security approach. In fact, you can use the forces of change to develop smarter security policies that enable the use of new technologies rather than banning them.

Make security everyone's responsibility

The key to a more secure environment is to make employees understand their personal responsibilities when using newer technologies or accessing corporate information. The awareness goes beyond high-level policies to pragmatic examples of activities that are permitted and prohibited when using social networks, laptops, tablets or smartphones. A concrete "dos and don'ts" list is the most effective means of communicating the policies and enabling responsible use.

Enable newer technologies

Users increasingly want to bring personal mobile devices into the workplace. Rather than implementing ineffective policies in an attempt to keep them out, examine the controls that can protect, optimize and enable access. Such solutions as moving critical information to a secured data center can facilitate real-time access to information on mobile devices without compromising the information itself. A large multinational organization recently deployed a security solution that not only enabled the use of personal devices, but enjoyed substantial savings related to the support and acquisition of corporate-owned devices.

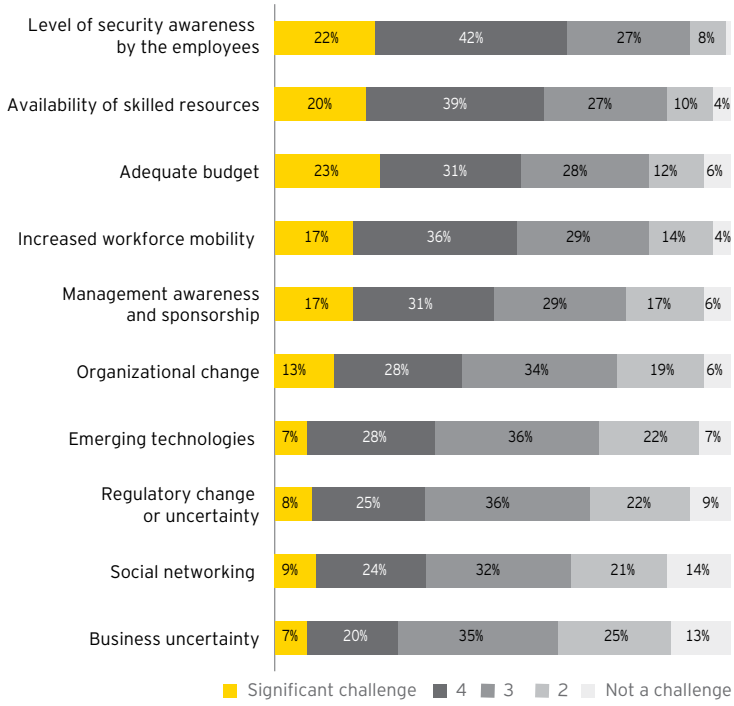
Similarly, many organizations block employee use of social networking sites on corporate devices. However, this doesn't stop employees from accessing social networks either directly or on their personal mobile devices during work hours. In fact, many young recruiting prospects expect unfettered access to their social networks, and organizations that can meet those demands will gain a competitive advantage in hiring and retaining the best talent.

However, our 2010 survey results show that social networking is not high on the list of challenges for most of the participants. Only 33% of respondents indicated that social networking is a considerable challenge to effectively delivering information security initiatives. This is an indication that, although most companies recognize the fact that there are risks and information security issues related to social media, only a few have developed an approach that will balance the business opportunity with the risk exposure.

Three key questions

- Do all the organization's stakeholders understand the importance of information security?
- Is your organization up to date with the new technologies hitting the work force?
- Does your organization have the right measures to create a scorecard on information security at the enterprise level?

What is the level of challenge related to effectively delivering your organization's information security initiatives for each of the following?



Shown: Percentage of respondents

Source: *Borderless security: Ernst & Young's 2010 Global Information Security Survey*

The fact that only 9% of respondents indicated the examination of social networking as a critically important function is further evidence that few organizations have assessed this impact.

Of course, embracing change may require a substantive culture shift within your organization. You will need a good change management program and an executive champion to lead it. Begin with tone-from-the-top support and executives who lead by example. Follow with a relentless focus on the people – communicate openly and honestly, address their fears and focus on the benefits change will bring.

Extend security programs across the enterprise

Information security should be a foundational element of your organization's enterprise-wide risk management strategy. This will create greater transparency of potential risks and enable security teams to work collaboratively with the broader risk teams to plan, protect, and detect and respond to existing and emerging threats. Security teams will also have to work with business units to:

- Align information security functions to those risks that matter most to the business
- Coordinate infrastructure and people by continually evaluating capability levels and gaps as well as investment in skills development
- Employ consistent methods and practices that apply a structured approach to information security management enterprise-wide
- Ensure common information and technology, which promotes consistent sharing of information about key information security and business risks throughout the organization

Set security program metrics that impact business performance

Any new information security program will need to focus on value, measurement and accountability. As such, you will want to develop security program metrics that measure the program's impact on business performance. These metrics need to align directly with your organization's broader business objectives.

A value scorecard to report on your progress and contributions can help you achieve your performance goals. Defined in collaboration with stakeholders, this will serve as a qualitative measure of information security performance and the value delivered to the organization. Topics that a value scorecard should cover include:

- How managing the number of incidents that gave the company negative external exposure has helped to manage the brand value and limit the reputation risk
- How proper security measures helped limit the amount of redone work and as such added to the bottom line
- How communication about security and privacy measures (on websites, in articles, based on certificates) helped to grow the e-business and as such added to the top line

Conclusion

Information security in action

By rethinking your information security strategy and using our integrated security approach, your organization can proactively protect while anticipating the worst; it can embrace change instead of resisting it; it can focus on trust rather than paranoia.

In doing so, your organization can manage the right risks and drive value by:

- Understanding your security maturity today and tomorrow; knowing where you are and where you want to be guides the strategy
- Having a risk-based information security strategy that aligns with business needs, enables compliance and maintains the integrity and confidentiality of critical information
- Gaining an in-depth understanding of what constitutes the critical information of the organization, where it resides, and who has or needs access to it
- Devising a means to measure, monitor and report on the effectiveness of the security program and controls
- Emphasizing better governance of information security
- Optimizing security programs to gain efficiencies and achieve cost savings
- Creating a culture of trust and responsibility among customers, consumers, suppliers and employees in an increasingly borderless world

About Ernst & Young

At Ernst & Young, our services focus on our individual clients' specific business needs and issues because we recognize that each is unique to that business.

IT is a key to allowing modern organizations to compete. It offers the opportunity to become closer to customers and more focused and faster in responses and can redefine both the effectiveness and efficiency of operations. But as opportunity grows, so does risk. Effective IT risk management helps you to improve the competitive advantage of your IT operations by making these operations more cost-efficient and managing down the risks related to running your systems. Our 6,000 IT risk professionals draw on extensive personal experience to give you fresh perspectives and open, objective advice – wherever you are in the world. We work with you to develop an integrated, holistic approach to your IT risk or to deal with a specific risk and information security issue. We understand that to achieve your potential you need tailored services as much as consistent methodologies. We work to give you the benefit of our broad sector experience, our deep subject matter knowledge and the latest insights from our work worldwide. It's how Ernst & Young makes a difference.

For more information on how we can make a difference in your organization, contact your local Ernst & Young professional or a member of our team listed below.

Contacts

Global		
Norman Lonergan (Advisory Services Leader, London)	+44 20 7980 0596	norman.lonergan@uk.ey.com
Paul van Kessel (IT Risk and Assurance Services Leader, Amsterdam)	+31 88 40 71271	paul.van.kessel@nl.ey.com
Advisory Services		
Robert Patton (Americas Leader, Atlanta)	+1 404 817 5579	robert.patton@ey.com
Andrew Embury (Europe, Middle East, India and Africa Leader, London)	+44 20 7951 1802	aembury@uk.ey.com
Doug Simpson (Asia-Pacific Leader, Sydney)	+61 2 9248 4923	doug.simpson@au.ey.com
Naoki Matsumura (Japan Leader, Tokyo)	+81 3 3503 1100	matsumura-nk@shinnihon.or.jp
IT Risk and Assurance Services		
Bernie Wedge (Americas Leader, Atlanta)	+1 404 817 5120	bernard.wedge@ey.com
Paul van Kessel (Europe, Middle East, India and Africa Leader, Amsterdam)	+31 88 40 71271	paul.van.kessel@nl.ey.com
Troy Kelly (Asia-Pacific Leader, Hong Kong)	+85 2 2629 3238	troy.kelly@hk.ey.com
Giovanni Stagno (Japan Leader, Chiyoda-ku)	+81 3 3506 2411	stagno-gvnn@shinnihon.or.jp

Related thought leadership

Thought leadership at ey.com/informationsecurity

Privacy trends 2011: challenges to privacy programs in a borderless world

Executives are investing more money to protect the privacy of personal information. But are they spending it in the right places? Read this year's report to find out which privacy issues you need to be thinking about in an increasingly borderless world.

Borderless security: Ernst & Young's 2010 Global Information Security Survey

In our 2010 Global Information Security Survey, more than 1,600 participants from 56 countries share their greatest strengths and most critical risks in today's information security environment.

Countering cyber attacks

Traditional information security solutions are not enough to protect against persistent threats and attacks. This updated report discusses the measures organizations should consider to detect and react to successful cyber attacks.

A risk-based approach to segregation of duties

Segregation of Duties (SoD) is top of mind for many professionals, due in part to control-driven regulations worldwide and the executive-level accountability for their successful implementation. This document outlines a practical, risk-based approach to SoD compliance.

Cloud computing issues and impacts

As mainstream adoption of cloud computing services begins in earnest, there are a multitude of factors that cloud service providers and cloud users must carefully consider. This Ernst & Young report explores critical aspects of cloud computing for all companies (users and providers of cloud services) and consumers.

Plugging the leaks: managing threats to confidential data

Over the last five years, organizations have experienced a rise in the volume of intentional and unintentional data leakage. This new whitepaper explains how a program that includes both behavior and technical controls can give responsible employees an outlet for escalating concerns while protecting confidential data from being leaked by those with malicious intent.

Ernst & Young

Assurance | Tax | Transactions | Advisory

About Ernst & Young
Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 141,000 people are united by our shared values and an unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve their potential.

Ernst & Young refers to the global organization of member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit www.ey.com.

About Ernst & Young's Advisory Services
The relationship between risk and performance improvement is an increasingly complex and central business challenge, with business performance directly connected to the recognition and effective management of risk. Whether your focus is on business transformation or sustaining achievement, having the right advisors on your side can make all the difference. Our 20,000 advisory professionals form one of the broadest global advisory networks of any professional organization, delivering seasoned multidisciplinary teams that work with our clients to deliver a powerful and superior client experience. We use proven, integrated methodologies to help you achieve your strategic priorities and make improvements that are sustainable for the longer term. We understand that to achieve your potential as an organization you require services that respond to your specific issues, so we bring our broad sector experience and deep subject matter knowledge to bear in a proactive and objective way. Above all, we are committed to measuring the gains and identifying where the strategy is delivering the value your business needs. It's how Ernst & Young makes a difference.

EYG no. BT0097
(Supersedes EYG no. BT0094)

In line with Ernst & Young's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

www.ey.com/informationsecurity