

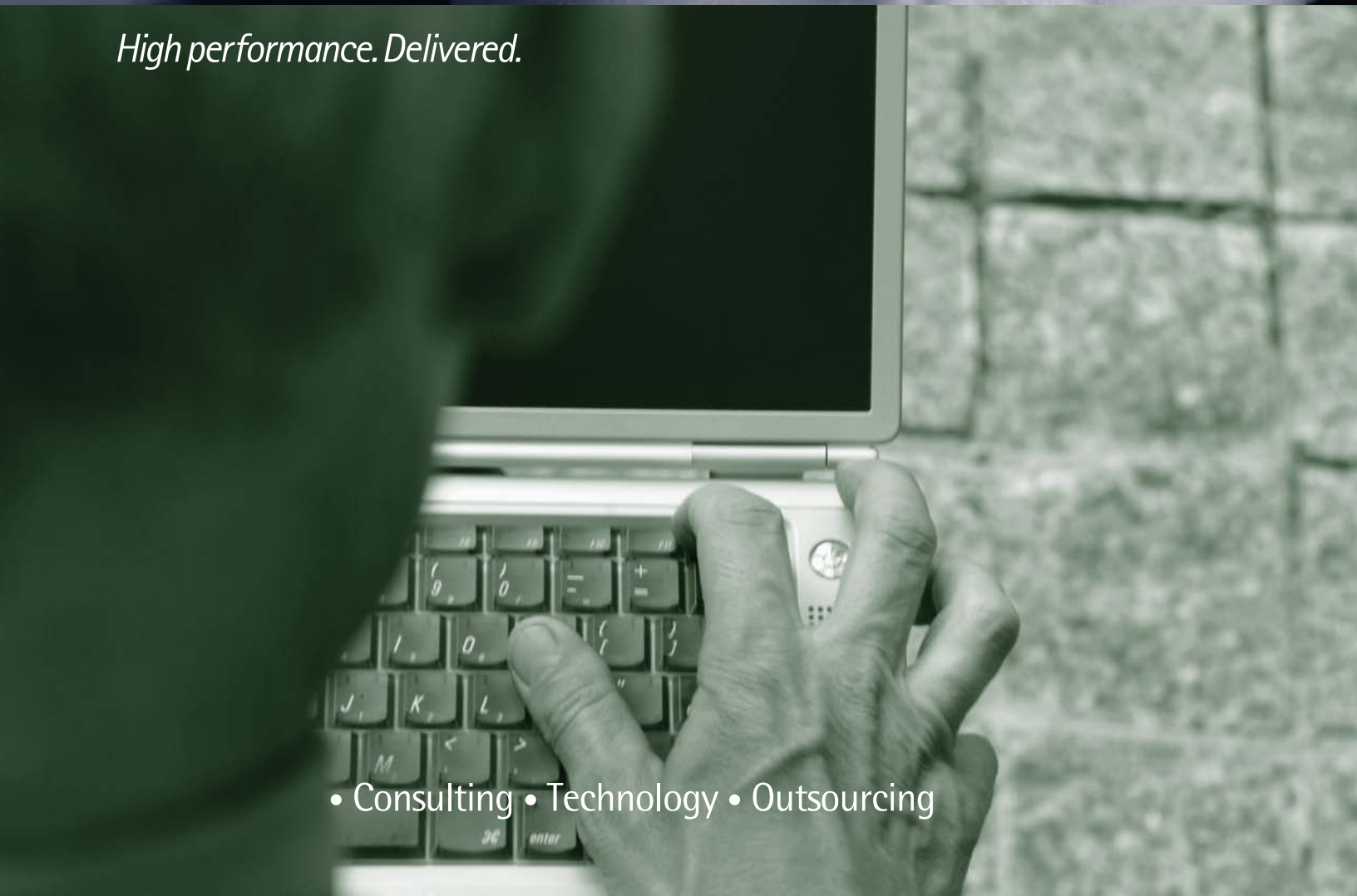


# Mounting a security offensive to counter cyber threats and enable high performance

By Alastair MacWillson and Bill Phelps

**accenture**

*High performance. Delivered.*



• Consulting • Technology • Outsourcing



With almost every transaction now conducted over the Internet, organizations become more vulnerable to cyber intrusion. Automated tools have made it easier for hackers to generate attacks, creating a flood of noise that may distract organizations from discovering the most sophisticated attacks in a timely manner.

This has become a senior management issue, not just a technical problem. Strong security practices are necessary to both defend the enterprise and enable the enterprise to operate innovative new processes without increasing risk. This paper offers five steps to guide a proactive, high-performance approach to cyber security.

# Enemies of every stripe



How many of your teams are using a cloud-based application to share documents with a client? Which of your software developers has recently used his credit card to provision a server on a cloud service? What's your plan for launching backup when a key data center does eventually crash? How do you determine whether a system has crashed because of performance issues or an intrusion?

These questions are not academic. Tremendous benefits can accrue from open, distributed computing systems and the rich services offered by Google, Amazon, and others. New applications can enable enterprises to sell and deliver products more efficiently, as well as to facilitate communications

with customers and employees. But many organizations keen to use such services and applications don't fully consider the new risks that they pose.

Unfortunately, the Internet has become an easy target for malevolent use. Open systems, interfaces, and commonly used document formats can propagate vulnerabilities if appropriate security controls are not applied and enforced. Employees working at home, hotels, or cafes often bypass the standard corporate security controls when connected to unsecure environments. And many IT products and solutions are released without the robust functionality now required for enterprise-wide data protection and privacy, particularly as it relates to

compliance. Additional risks extend from incubating technologies, from the marriage of interoperable technologies that support cloud-based services, and from the new frontier of social media platforms (see sidebar, "Porous perimeters of social networking websites.") In short, the attack surface has gotten much broader, with many more sources at home and abroad.

With greater dependence on web-based applications comes a far more serious consequence of infrastructure compromises and disrupted operations through data breaches, data loss, and non-compliance with government regulations or important industry standards—along with the potential erosion of customer confidence.



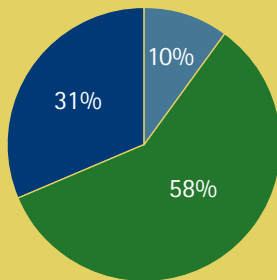
In the United States alone, more than 346 million records containing sensitive personal information have been involved in security breaches since January 2005.<sup>1</sup> Such breaches can have serious implications for the enterprises involved. Publicly held companies experiencing breaches of confidential information typically suffer a 5 percent drop in stock price when such a breach is made public.<sup>2</sup>

Cyber vulnerabilities put at risk critical infrastructure such as power grids, financial markets, emergency services, and air traffic control. Customer information of all kinds is also at risk as online shopping and point-of-sale capture have become widespread. Entire industries are being forced to adjust as a result. Every merchant that accepts credit card payments has already experienced the considerable cost and expense to strengthen protection against identity theft, and health insurers are investing to prevent medical records theft.

# A few heart-stopping data points

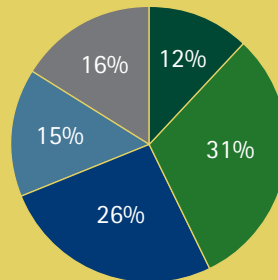
Figure 1: Data breaches

Did your organization ever lose sensitive personal information?



- Yes
- No
- Can't recall

If yes, how often has this occurred in the past 24 months?



- Only once
- 1 or 2 times
- 3 to 5 times
- More than 5 times
- Can't recall

Source: Accenture survey, 2009.

Some 58 percent of executives polled recently by Accenture in 19 countries said they have lost sensitive personal information, and for nearly 60 percent of those who have had a breach, it was not an isolated event. Larger organizations appear to struggle more to prevent breaches than smaller ones—likely because, with more employees and geographically dispersed operations, the opportunities for data to be lost or compromised are greater.<sup>3</sup>

- A May 2009 survey by Actimize found that 81% of financial services organizations expect an increase over the next year in ATM/debit card fraud.<sup>4</sup>
- Computer hackers stole more sensitive records in 2009 than in the previous four years combined, with ATM cards and PIN information growing in popularity, a Verizon study found. Organized criminal groups orchestrated nine in 10 of the most successful attacks, with 93% of the records exposed coming from the financial sector.<sup>5</sup>

- Zeus and Clampi botnets, which steal online account credentials with a focus on bank accounts, have gained in size and strength in recent months. Cheap (\$700), and easy-to-use toolkits that hackers can purchase to control botnets are widely available online.<sup>6</sup>
- In 2008 alone, industry estimates of loss from intellectual property data theft range as high as \$1 trillion.<sup>7</sup>
- McAfee reports nearly one-third of companies it surveyed suffered large-scale distributed-denial-of-service attacks multiple times each month, and nearly two-thirds of those said such attacks impacted operations.<sup>8</sup>

# The industrialization of cyber crime

Make no mistake; the adversaries have become smarter, better organized, and more persistent. The number of cyber threats is proliferating faster than companies can defend against them. Hackers constantly exploit weaknesses in popular products and pioneer new techniques using viruses, rogue antivirus software, keystroke loggers, botnets, and other tools, for immediate targets or time-triggered actions. Stanford University law professor Lawrence Lessig even invokes the prospect of an “i-9/11 event” that spirals out of control and causes significant damage to any operation that depends on Internet access.

Some cyber criminals engage in attacks strictly for the money. Earlier this year, a crew of hackers was sentenced to prison for breaking into systems belonging to a number of U.S. retailers as well as Heartland Payment Systems, a processor of credit card transactions. The crew sold millions of credit card

numbers to Russian criminals and used some of the data to make unauthorized ATM withdrawals. Cyber criminals are also now targeting hotels to steal credit card data from guests. The common weakness at hotels is the security surrounding point-of-sale software, which hotels use to process credit card transactions.<sup>9</sup>

Theft of intellectual property through digital channels, especially across emerging markets, is on the rise. Companies are losing crown jewels such as detailed product designs, trading algorithms, and drug or food formularies.

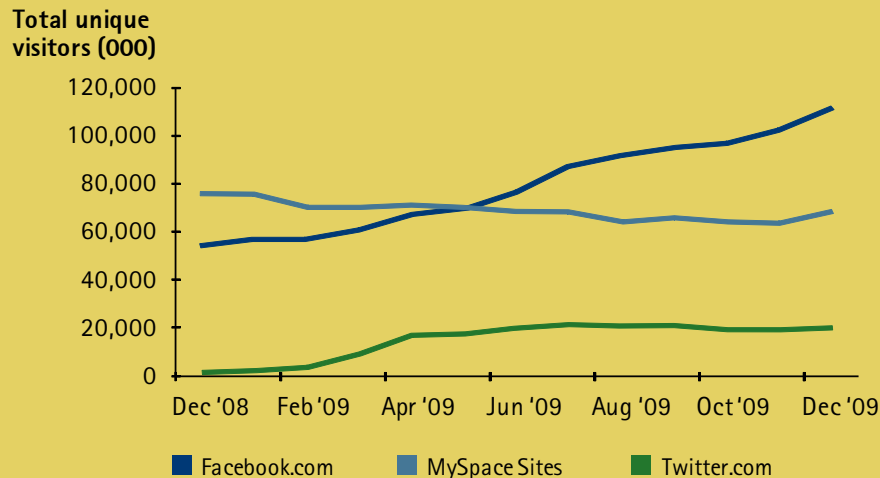
Cyber terrorists, meanwhile, aim to cripple servers and other critical infrastructures to disrupt the operations of governments, utility companies, supply chains, or media outlets. Some are interested in controlling the conversation and silencing those with whom they disagree.

Whatever their goals, intruders don't always fit the image of a lone wolf probing corporate systems just to show that he or she can. Many hackers are part of a well-organized criminal effort, or agents acting on behalf of a nation-state. Recent online attacks on Google and dozens of other American corporations, for instance, were traced to computers at two educational institutions in China, including one with close ties to the Chinese military.

The proliferation of attacks and threats has pushed cyber risk management from primarily a technical problem to a high priority meriting attention at the highest levels of the organization. The increased breadth and depth of government regulation is forcing enterprises to invest more, to remediate legacy weaknesses, and to prepare for the minefields ahead. Companies, government agencies, and non-profit organizations may increasingly be held liable for cyber security failures, either through sanctions or common law remedies.

# Porous perimeters of social networking websites

**Figure 2:** Much of the growing traffic of online social networking...  
2009 visitor trend to Facebook.com, MySpace sites, Twitter.com



Source: comScore Media Metrix (U.S.)

Consider both the astonishing spread and the particular challenges of social networking sites. Nearly four out of five Internet users visited such a site in December 2009, and the activity now accounts for 11 percent of all time spent online in the United States, making it one of the most engaging activities across the Internet, according to comScore.<sup>10</sup>

Since the premise of social networking sites is to more easily and efficiently share personal information, site users tend to lower their guard. These sites thus become attractive locations for illegal data mining and malware insertion. One computer worm, Koobface, has targeted Microsoft Windows users of Facebook, MySpace, Friendster, Twitter, and similar sites to gather sensitive information such as credit card numbers. Although social networking companies have become more conscious of these threats, staying ahead of new attacks is a major challenge.

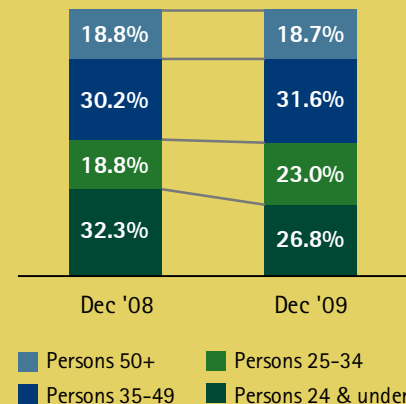
In another recent case, a hacker named Kirillos has been selling Facebook user names and passwords. Researchers at VeriSign estimate Kirillos has sold almost 700,000 of the 1.5 million accounts he or she is offering. The asking price: \$25 to \$45 per 1,000 accounts, depending on the number of contacts each user has.<sup>11</sup>

Other forms of malware tap users' "100 things about me" postings to mine data that is typically used to answer password-reset questions such as "What was your first pet's name?"

Once the security of an employee's laptop is breached through a social networking site, the company's systems and infrastructure become susceptible to cyber attacks. Yet blocking access to sites may not fully address the problem.

...comes from working-age users.

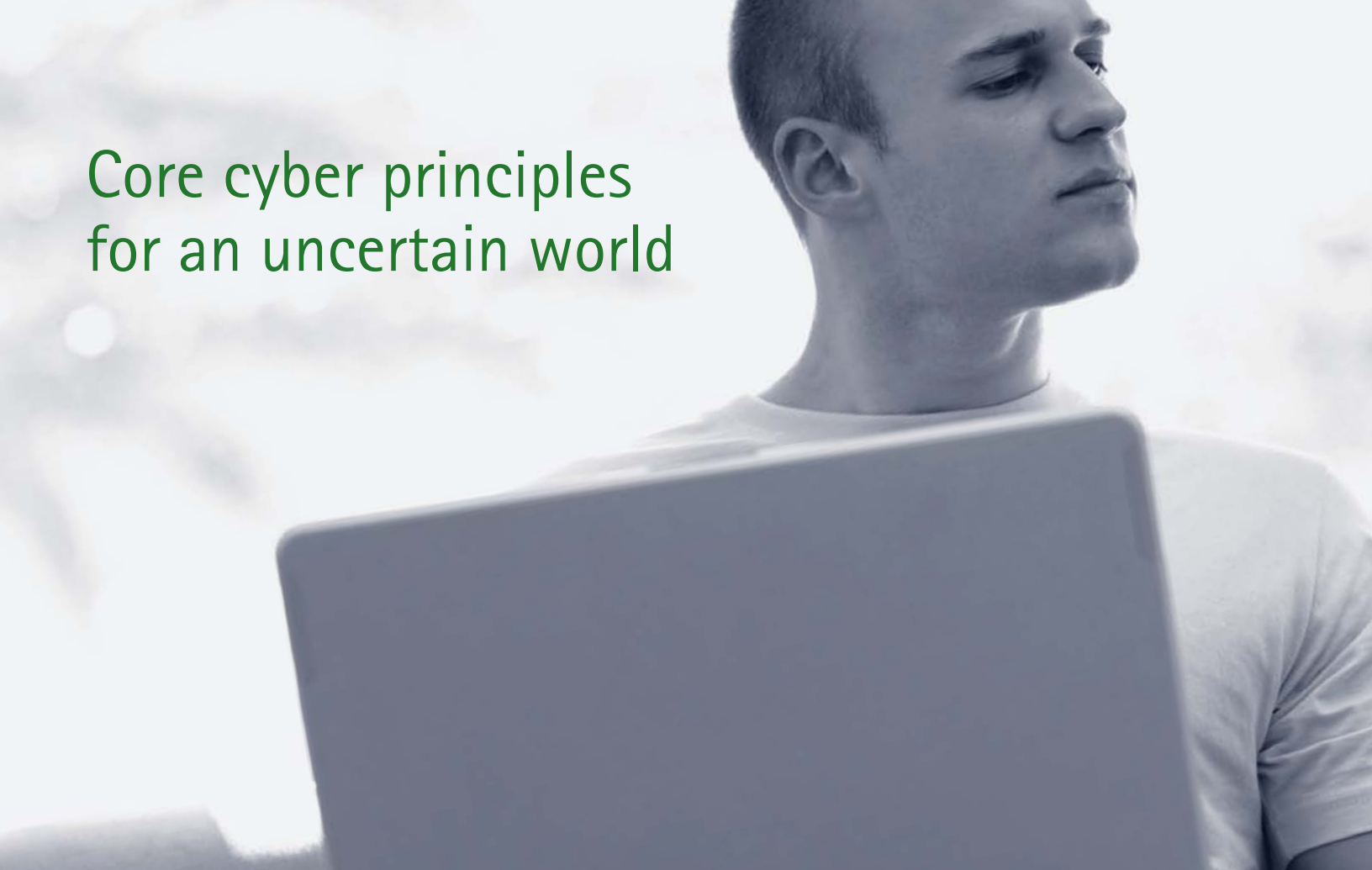
Percent composition of visitors to Facebook.com by demographic segment



Source: comScore Media Metrix (U.S.)

For one thing, employees can often access the sites through their own smart phones—on which they may also check their corporate email. For another, many companies are themselves engaged in marketing and customer contact activities through these sites.

The most effective solution for the near term will consist of several elements: employee education about safe online behavior; security controls such as Policy Enforcement Agents or Network Access Controls on the end user's device; and monitoring techniques that give an early alert on legitimate breaches versus mounds of false positives hiding these attacks.



# Core cyber principles for an uncertain world

As senior executives weigh their next moves in cyber security, we advocate a proactive approach: Anticipate what new threats may challenge the enterprise, and which security elements can help to improve performance; then weave the right security features into the enterprise's infrastructure and digital assets.

Getting ahead of the threats is not easy, to be sure. The measures taken in most industries and government sectors have been largely reactive, designed to defend against a repeat occurrence of an attack that has already occurred. Reactive capabilities are still useful, to reduce response times to and reporting of incidents, but a reactive mode is not sufficient. Few enterprises have sufficiently implemented the controls necessary to protect themselves from cyber attackers.

Effective cyber security should be incorporated into processes throughout an enterprise, not just on the perimeter. As companies and public organizations build, acquire, or source the right combination of capabilities, the experiences of leading organizations offer up a set of five principles that have proven quite effective in guiding this type of initiative.



## The key principles of cyber security

1. Identify and secure the IT assets themselves, not just the perimeter.
2. Build a hard-nosed "culture of security."
3. Pay closer attention to applications.
4. Check and double-check user identity.
5. Develop acute situational awareness.

## 1. Identify and secure the IT assets themselves, not just the perimeter.

Many multinational organizations don't know what all of their valuable assets are or where they're located. Effective cyber security starts by knowing what data and technology are essential to operations and business continuity. There should be a detailed plan to protect these assets and capabilities from being compromised, including a robust test of the plan to make sure that it's viable.

While organizations typically focus on securing the IT perimeter, it's more effective to secure the data or asset itself, wherever it travels and wherever it lives. Organizations should embed cyber resilience and defensive capabilities throughout the organization, not just individual components.

This is not always a straightforward task, as it requires navigating a maze of regulatory, compliance, privacy, and business demands. Current and pending compliance frameworks differ by country, by industry, and by activity within a company. An organization must be agile enough to keep pace with changes in demand and in the nature of cyber threats. Most initiatives will benefit from an end-to-end approach, from the problem analysis to monitoring the controls that follow implementation of the solution.

Analysis of the cyber risk ecosystem will include the relevant compliance requirements and controls that need to be configured to make certain that the network and infrastructure on which it runs are secure and resilient. The right people will need to be granted the right levels of access to enterprise applications.

## 2. Build a hard-nosed "culture of security."

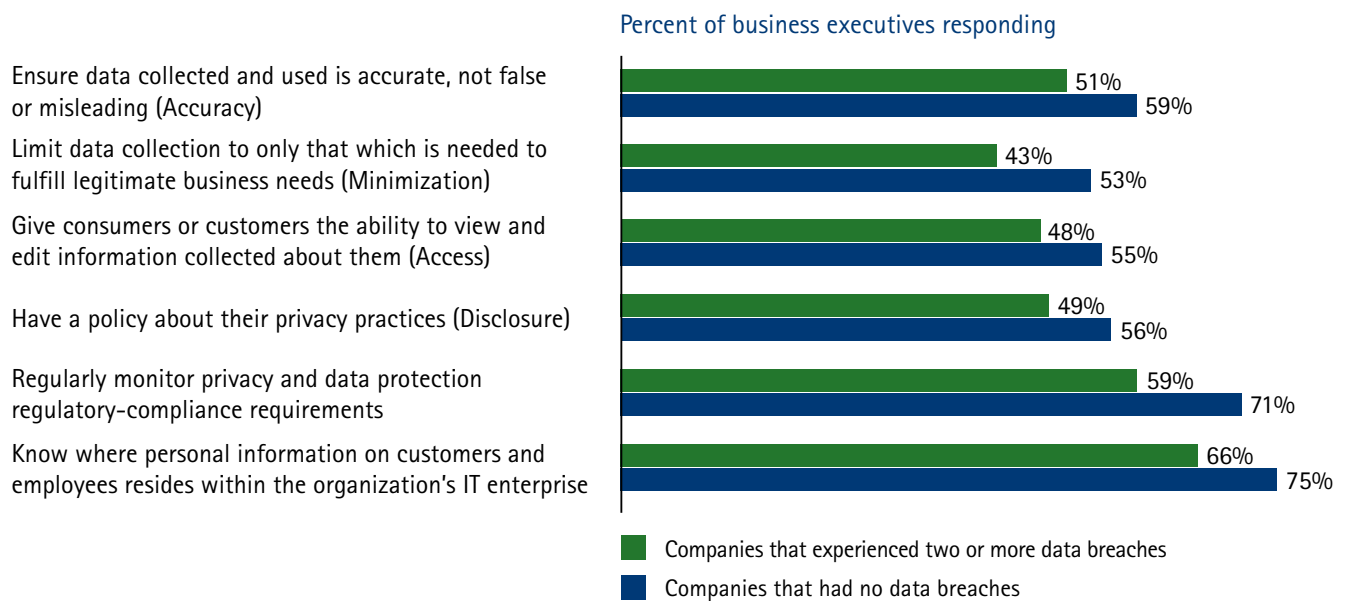
Many organizations do not clearly define where the oversight or accountability for cyber security lies. They may also find that the management responsibility and accountability can be dispersed and fragmented, with the Chief Information Officer, Chief Security Officer, Chief Privacy Officer, or the legal function all having some involvement. For instance, the CIO could be responsible for maintaining IT and data security, the CPO for setting policies and procedures, and the general counsel for ensuring the organization is complying with regulations. As a result, it's not clear where the buck stops on information security.

By contrast, organizations that exhibit a "culture of security" do make responsibilities and accountabilities explicit. For example, General Electric and Intel have formally extended the remit of their privacy officer's role to information governance and/or data security to ensure a holistic approach to information management and protection. Such organizations tend to view themselves as stewards, not owners, of personal data and take actions to protect data entrusted to them. Accenture's recent survey confirms that organizations with clear responsibilities and strong policies are less likely to experience security breaches, as shown in Figure 3.

The first step to building this culture is to put in place an IT governance program that integrates the people, processes, and technology needed to manage data effectively and efficiently. Effective governance programs typically start by defining roles and responsibilities for data owners and stewards. In some cases, it may make sense to establish a privacy and protection council, composed of stakeholders from across the business, which is responsible for overseeing how sensitive data is managed and used, as well as for continuous improvements of the organization's security posture.

Any data protection framework should address protection in a unified manner and avoid addressing regulatory compliance in separate silos of country, business process, or type of data. Organizations should create a common set of data privacy and protection standards that can be applied consistently from country to country to minimize complexity, cost of compliance, and chances for breaches while, at the same time, enabling responsible data sharing and global data flows.

**Figure 3: Data protection policies matter**



Source: Accenture survey, 2009.

### 3. Pay closer attention to applications.

Many serious breaches result from application-level weaknesses. Most applications were not engineered with security in mind, because developers assumed they would sit behind a secure perimeter. As that assumption is no longer valid, legacy applications will eventually have to be reengineered, and new applications need to be developed under a new security paradigm.

This is not just an issue for corporations. Many federal government agencies as well have adopted the benefits of commercial off-the-shelf applications from Oracle, SAP, and other firms to support daily business operations and to enable efficiencies, cost savings and citizen-centric services. Those applications need to be trusted, secure and flexible, and must meet

requirements imposed as a result of the Comprehensive National Cyber Security Initiative and the Presidential Homeland Security Directives.

Requirements include establishing trusted supply chains, complying with Security Technical Implementation Guides, implementing anti-tampering technologies, validating and testing systems, and following standards such as Federal Desktop Core Configuration.

As federal and state agencies link vast numbers of distributed resources (internal and public) through cloud computing technologies, the complexity and reach afforded to an adversary escalates. Protecting the perimeter around applications is no longer enough of a defense, as firewalls or anti-virus solutions may not be comprehensive enough. Most organizations should extend security to the device level as well as to the application layer.

Trusted applications development and delivery thus is a critical component of a security initiative. Organizations need to be able to measure a commercial-off-the-shelf application's strength and ability to process and handle sensitive information throughout its deployment lifecycle. The system should undergo stringent testing to help confirm that mission-critical applications can be run with reduced risk.

## 4. Check and double-check user identity.

Identity management has become a top security priority with the convergence of several trends. In the public sector, organizations are facing border management and illegal immigration issues; an increase in the volume and speed of international commerce, identity, and benefit fraud; the threat of terrorism; and growing taxpayer demand for public service value. In the private sector, organizations are facing sharp increases in identity theft; risks associated with having an extended enterprise of customers, suppliers, and contractors with access to enterprise applications; greater use of mobile devices that adds another interface to secure; and a variety of country-based regulatory frameworks such as the Health Insurance Portability and Accountability Act (HIPAA), the Patriot Act, and Sarbanes-Oxley.

For many digital systems, the traditional paradigm of identity authentication is based on knowing phrases or numbers that once were considered secret or at least protected—your social Security number or your mother's maiden name. Now much of that information may be commonly available or, at least, discoverable, severely undermining the premise of conventional authentication.

Mastering the ability to determine whether customers, citizens, suppliers or employees are who they claim to be when they access enterprise systems and facilities is crucial to enterprise performance. Yet with IT budgets under increased scrutiny, many CIOs are charged with reducing risks and threats while also improving the administrative and cost efficiency of managing user identities and access to information.

Effective identity and access management programs should create value by embedding pervasive security without sacrificing functionality and ease of use. Aspects such as single-sign on, immediate access revocation when needed, self-service functionality, and real-time analysis to support audits are key components that will both support the business needs while also managing risk appropriately. Open-source protocols such as OpenID, which allow users to log on to different services with the same digital identity, are starting to catch on as a means of creating strong authentication combined with ease of use.

Businesses and governments can take advantage of improving price-performance characteristics of other authentication technologies, such as biometrics (fingerprint or retinal scans) and smartcards, to speed the time to value and increase the return on investment of identity management initiatives. These trends are putting cutting-edge solutions in reach, even for organizations operating under fiscal constraints.

To realize value from identity and access management investments, organizations will need to integrate strong authentication technologies with access management technologies. Non-biometric, two-factor authentication is also useful for managing access and is more appropriate for some environments. (Biometric data on every user of a social networking site, for instance, would be too costly to store and would likely run into opposition over privacy concerns.) A user could be required to have two forms to verify identity, such as a smart card in addition to a password.

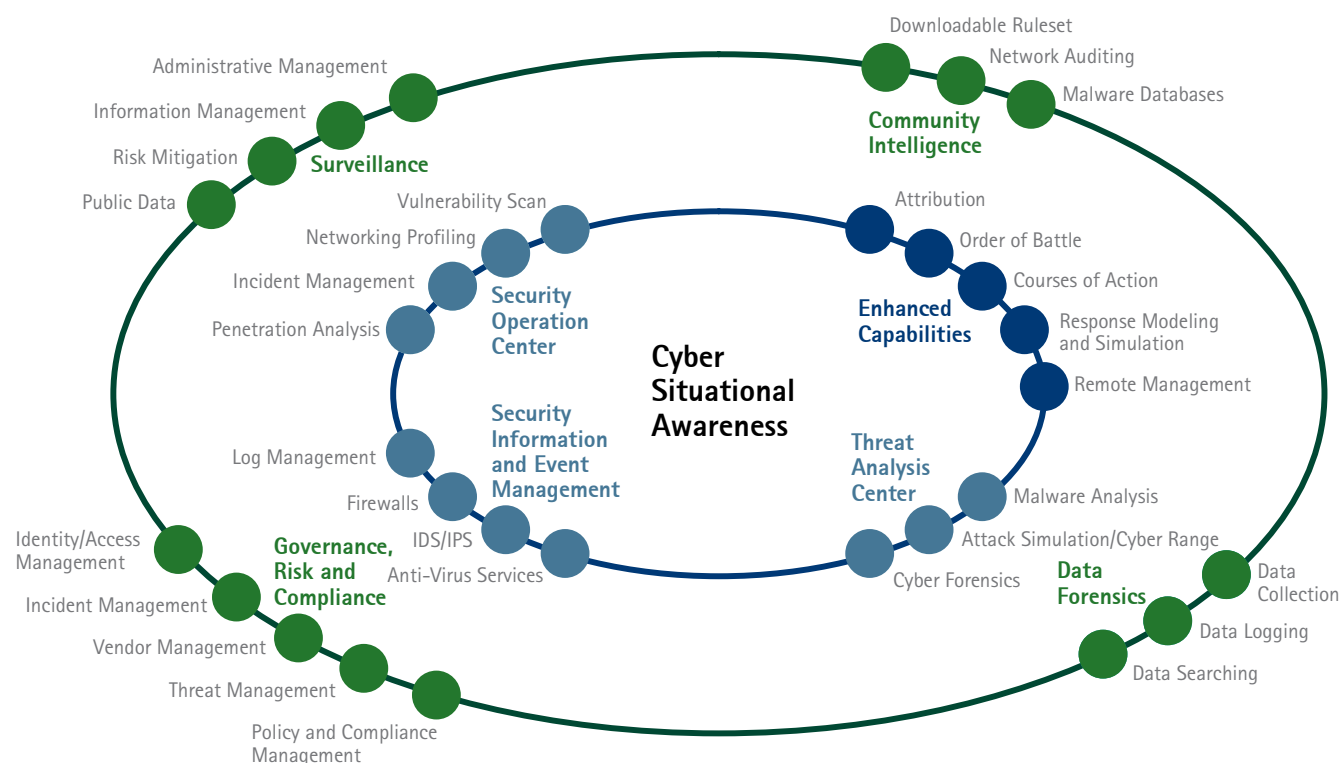
By combining stronger identity management methods with biometric technologies, companies and governments can redefine how they do business. For example, Accenture has worked with U.K. officials to create a biometric gate to speed up registered travelers through customs at Heathrow Airport. Larger retailers are already using "pay by touch" systems to verify the identity of customers who cash checks for payment of items. This helps simplify the check authorization process and significantly reduces fraud.

## 5. Develop acute situational awareness.

Keeping ahead of risks means, first of all, understanding exactly which key risks the organization is facing—across the whole risk landscape, including the supply chain and business partner network, not just compliance status. Be aware of a risk's potential impact on the organization's overall performance, have a clear view of which risks might emerge, and have appropriate measurements in place to manage or mitigate these risks.

Addressing supply chain risk management and business network security is a sensitive and complicated challenge, because of all the players involved, but requires the same diligence as dealing with the internal organization. Organizations should collaborate with business partners that take equal or greater care with data, and rigorously assess partners' knowledge, practices, and experience in managing sensitive data across organizational and national boundaries in accordance with local privacy laws and industry regulations.

**Figure 4: A situational awareness capability map**



Microsoft is one of a number of leading organizations that have developed vendor-management programs to enable them to embed data privacy considerations and requirements in the procurement process and during delivery. Some of these firms have implemented auditing processes to test the providers' security practices.

It is believed that hackers and malicious entities start work quite far out in time and distance from the occurrence of a detectable event. Malicious activity may start by building familiarity with employees to gain a foothold, scanning the network, getting access to a database, escalating privileges, pilfering data, covering tracks, and leaving behind back doors permitting later unauthorized entry.

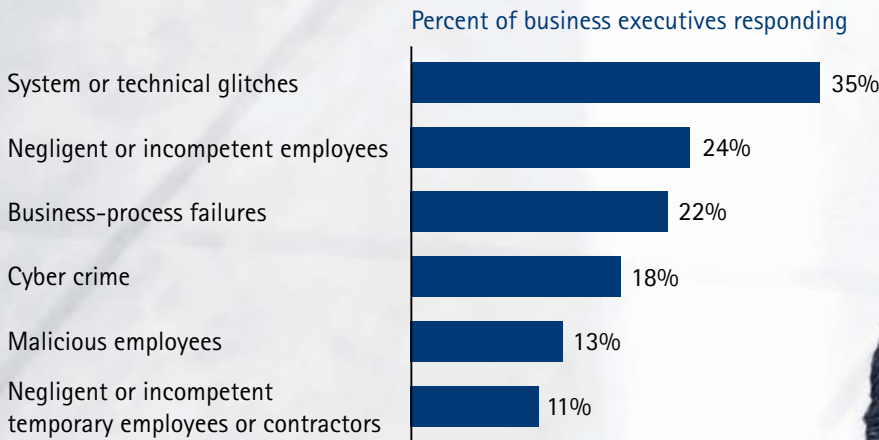
However, if organizations only react to suspicious activity, a recorded incident, onset of an attack, or a malware outbreak, it may be too late. An organization must also actively gather cyber intelligence and watch downstream activities in order to:

- Recognize back doors and vulnerabilities unseen by point compliance and checklist efforts
- Recognize complex and chained patterns that indicate the initiation of an attack
- Expand the scope of vulnerability assessment or penetration tests
- Harness external sources of threat intelligence to understand and train for zero-day exploits
- Detect reconnaissance activity by a terminated employee or a hacker forum

Application vulnerability scanner results, firewall rules, SIEM reports, chatter on blogs and forums as well as software vulnerabilities are readily available sources of threat intelligence. Layering and fusing these multiple sources of information helps to form an operating picture where the sum is greater than its parts (Figure 4).

Staying current with evolving threats will entail keeping staff educated and technology up to date. Cyber security will need to be built into projects and procurement going forward, including pointed training for IT managers. In the recent Accenture survey of business leaders and individuals, internal issues—employees (48 percent) and business or system failure (57 percent) were cited most often as the source of the breaches (Figure 5).

**Figure 5: Internal issues are frequent causes of security breaches**



Source: Accenture survey, 2009.

One of the most common reasons for internal lapses is a lack of adequate policies and training programs. Some training can be as simple as how to choose a secure password (hints: don't use variations of the same password, don't use birthdays, don't use family member names). Cyber security training in general has become more important of late; recent analysis by Verizon of cyber breaches shows that IT managers' mistakes did more damage than careless behavior by rank-and-file employees.

To streamline the time in which the organization is able to sense and respond to threats, it's worth a fast, concentrated effort to get a clear view of readiness within a specific set of IT resources, a specific topic area, or an organizational unit. Ideally, an organization will identify emerging security problems before they increase in severity, and also pinpoint areas that represent potential opportunities to make significant improvements in readiness. Use the findings of this effort to set priorities, adjust plans of action and milestones, outline budgets and identify how to better use and secure existing technology.

## Living with risk when funds are tight



Information and data have become critical to an organization's success, whether they include customer data, financials, or confidential corporate intelligence. With each advance in technology that enhances connectivity and communication, the migration from the traditional office environment, where work happens behind fortified network walls, will continue. The convergence of cloud computing, online collaborative work tools, and handheld computing all accelerate the shift to the borderless enterprise.

The traditional corporate perimeter, with clearly identifiable boundaries, has diminished. In its place, a network with limitless potential is rising—one where companies, their customers, and their partners demand access to

information whenever and wherever they need it. Customers and partners will increasingly consider how the custodian of their data is going to protect sensitive information before embarking on a long-term relationship.

As a result, high-performing organizations are starting to take a more proactive and holistic approach to cyber security. They need a way to gauge the reputation of sources of traffic, and to stop suspect traffic sources before they cause problems. Since attacks can be multipronged—via email, the web, and the network—the ability to view traffic across protocols and networks can improve an organization's ability to detect and block these attacks.

Cost and risk are the trade-offs in any security agenda. At one extreme, IT security can be a choke point to progress; at the other, it is an afterthought or list of to-dos. Neither, of course, is acceptable. As the pace of technology accelerates, an enterprise will have to quantify its tolerance for risk in accordance with business requirements.

Leaders must take bold steps to ensure that security approaches and solutions are agile enough to adapt to rapid business change today, while forging the right risk management program to support growth and high performance. The economic slump adds to the strain on security resources. Yet executives should make sure that in the campaign to cut IT costs, they don't increase cyber risk such that lax security fails to support the needs of the enterprise.



## Questions for executives

Does each manager know what his or her responsibilities are with regard to information security?

Do we assign ownership of and accountability for information security through a data governance program?

Does our information strategy allow us to identify, track, and control how data flows across all our systems and processes?

Have we evaluated our privacy and protection technologies to confirm they are providing the necessary level of protection?

Have we built a consistent level of awareness among employees?

Have we provided them with the appropriate guidance and training for how to handle sensitive data and create secure passwords?

Have we reexamined our data protection investments?

Are we choosing business partners with care regarding their own security posture?

Do we have formal incident response policies, procedures, and teams?

# How Accenture can help in information security

Accenture has more than 20 years of experience helping corporations and governments across the globe use security to both defend the enterprise against malicious threats and enable the enterprise to operate innovative new business processes without increasing risk. By combining our security and technology know-how with industry-specific experience, we help our clients weave cyber resilience into their infrastructure, applications, and core business processes—securing the fabric of their entire organization.

## How we deliver our services

We address clients' information security priorities along the full spectrum of activities from strategy to implementation to management.

Our experienced core practice of security professionals is backed by our broad technology, management consulting, and outsourcing teams from across Accenture. We draw on Accenture experts from the relevant industry or capability, such as systems integration or analytics, when their experience will help to measurably improve the outcome.

Our approach is to identify the holistic set of requirements relevant to the client's business and regulatory environment, in order to define a solution that delivers an appropriate return on investment. We understand the importance of working side by side with clients to build the requisite security capabilities in their own organizations. However we can also partner with clients over extended periods to run key security processes on an outsourced basis.

## The business challenges we address

There is a pressing need to transform the security and risk functions and move beyond pure compliance to value creation. We help clients make better decisions and align risk and reward in the pursuit of business advantage.

Our clients generally want to simultaneously protect existing value and create new value. To address these challenges, we work with clients on several fronts:

- Enhancing security capabilities and embedding a culture of security and risk management throughout the organization
- Proactively positioning the enterprise for potential stress situations and reacting quickly to fast-moving events
- Increasing cost efficiency despite mounting cyber threats and regulatory burdens

## Global capabilities, tailored approaches

- Global delivery network of cyber professionals available around the clock through onshore and offshore models
- Outcome-focused, emphasizing the results of a particular security program relative to its cost and risk
- Able to see the forest for the trees, through an understanding of the business and the technology
- Solutions tailored to the unique needs of each industry and country, building on deep experience in government and more than 20 major industry sectors

## Best-of-breed information security solutions

Accenture offers a full spectrum of security capabilities including these core solutions:

- Security Strategy and Risk Management
- Infrastructure Security
- Enterprise Application Security
- Identity and Access Management
- Business Resilience and Continuity Management
- Data Protection and Privacy
- Security as a Managed Service

# Notes

<sup>1</sup> <http://www.privacyrights.org/ar/ChronDataBreaches.htm>

<sup>2</sup> "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market," Katherine Campbell, Lawrence A. Gordon, Martin P. Loeb, and Lei Zhou, *Journal of Computer Security*, Vol. 11, No.3, 2004, pp. 431-448.

<sup>3</sup> "How Global Organizations Approach the Challenge of Protecting Personal Data," Accenture, 2009.

<sup>4</sup> <http://www.actimize.com/index.aspx?page=news196>

<sup>5</sup> <http://www.verizonbusiness.com/about/news/displaynews.xml?newsid=25282&mode=vzlong>

<sup>6</sup> "Annual Security Report," Cisco, 2009.

<sup>7</sup> "Unsecured Economies Report," McAfee, January 2010.

<sup>8</sup> "In the Crossfire: Critical Infrastructure in the Age of Cyber War," McAfee, 2010.

<sup>9</sup> "Data Breaches Are Heaviest at Hotels," *The Wall Street Journal*, March 18, 2010.

<sup>10</sup> "The 2009 U.S. Digital Year in Review," comScore, February 2010.

<sup>11</sup> <http://www.networkworld.com/news/2010/042310-15-million-stolen-facebook-ids.html>



Copyright © 2010 Accenture  
All rights reserved.

Accenture, its logo, and  
High Performance Delivered  
are trademarks of Accenture.

Accenture is a global management consulting, technology services and outsourcing company, with more than 181,000 people serving clients in more than 120 countries. Combining unparalleled experience, comprehensive capabilities across all industries and business functions, and extensive research on the world's most successful companies, Accenture collaborates with clients to help them become high-performance businesses and governments. The company generated net revenues of US\$21.58 billion for the fiscal year ended Aug. 31, 2009. Its home page is [www.accenture.com](http://www.accenture.com).