High Performers and Foundational Controls: Building a Strategy for Security and Risk Management

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for IBM

December 2009

EMA™ IT MANAGEMENT RESEARCH, INDUSTRY ANALYSIS AND CONSULTING

Table of Contents

Executive Summary

With all the attention given to the increasing sophistication of threats, and the security implications of technology trends such as Virtualization and Cloud Computing, are enterprises ready for tomorrow's security risks?

For many, the answer is a resounding **no**. Many are ill-prepared for dealing with today's most basic issues, let alone what may emerge tomorrow. For example, in a recent ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) survey, nearly half (48%) of 200 global enterprises surveyed indicated that their IT risk management objectives were not adequately implemented or enforced.[1]

This is a contributing factor to successful breaches resulting from low-sophistication exploits of vulnerabilities that remain prevalent, despite their well known risks. Among these chronic exposures are gaps in configuration control and the inconsistent adoption of secure practices. The majority of those studied in the EMA survey fail to achieve all four milestones of defining effective controls, actually implementing them, monitoring the environment to assure control, and enforcing control when issues arise. Gaps in any one of these milestones makes a successful breach just that much easier.

From the attacker's perspective, the rationale is simple: When foundational controls fail or do not exist, why seek a more challenging target? Neglecting the fundamentals makes an organization an easy—and hence preferred—target.

In this paper, EMA examines the broad domains of controls enterprises must consider in order to build a solid foundation for IT security management:

- Countering threats
- Resolving vulnerabilities (in more than just software)
- Managing application risks
- Protecting sensitive information
- Managing and enforcing identity, access and entitlements
- Managing events and responding to incidents
- Stretching the boundaries: Extending to domains such as physical security, and fostering a more secure culture

The security implications of technology trends in relation to these controls are considered, as well as the advantages of security services for helping organizations achieve more effective control. Those responsible for security strategy will want to take note of how thoroughness in all four phases of the "Plan-Do-Check-Act" philosophy characterize high performers in EMA research findings, and how these high performers apply valuable lessons from domains such as Quality Management. Those who work in specific topic areas will want to consider their efforts in light of the examples and guidance offered in each relevant section.

The paper concludes with a look at today's IBM, as an example of an enterprise vendor that combines breadth as well as depth in security expertise as well as primary research and development, giving it a level of confidence among senior executives that only IBM can muster. Together, these capabilities give

1 *IT Governance, Risk and Compliance Management in the Real World*, EMA Research Report, May 2008

IBM a very strong position from which to help their customers take a new and more practical approach to building a strategy for addressing today's risks, as well as for those that are yet to come.

After all, if the enterprise cannot get a handle on today's fundamentals, how will it cope with tomorrow?

Introduction

Few today would argue with the fact that the tide of challenges in IT security is rising. In a few short years, organizations have gone from dealing with simple viruses to complex or blended threats that automate capabilities for vulnerability discovery, exploit, self-propagation, and a range of other behaviors. Exploit vehicles have evolved from noisy worms that served primarily to attract attention, to sophisticated threats that can cause significant damage. Organized criminals as well as national security strategists have recognized the potential that security vulnerabilities offer the attacker for exploiting information having tangible value. A black market for this information has kept this interest high. According to the Privacy Rights Clearinghouse[2], more than 260 million data records of US residents have been exposed due to security breaches since January 2005.[3]

Security is a constantly moving target. As the pace of technology continues to accelerate, so do the vulnerabilities introduced in complex IT systems.

Security is a constantly moving target. As the pace of technology continues to accelerate, so do the vulnerabilities introduced in complex IT systems. The flexibility of modern applications, particularly those centered on Web functionality, has led to an explosion of new development—which, in turn, has led to an equally substantial increase in vulnerabilities. 2008 was the busiest year for chronicling vulnerabilities in the history of IBM Internet Security Systems' X-Force, with a 13.5% increase overall compared to 2007, high and critical vulnerabilities increasing 15.3%, and medium severity vulnerabilities up a sobering 67.5%.[4] At the same time, the emergence of advanced persistent threats has raised the bar substantially on defense.

While the "bad guys" are discovering new opportunities and become more organized every day, many organizations fail already at the basics. According to the Verizon Business 2009 Data Breach Investigations Report[5], 87% of breaches examined in this report were considered avoidable through simple or intermediate controls such as configuration management and adopting well known secure practices. While errors such as misconfiguration play a leading role in these control gaps, taking a more proactive approach to tactics such as patch management may not be enough. For one thing, according to the IBM ISS X-Force 2008 Trend & Risk Report, not all vulnerabilities are "patchable," nor do software and systems vendors always go back to patch a previous year's vulnerabilities.[6] This should motivate enterprises to think in broader terms when it comes to managing security risks in IT—yet the fact that the 83% of attacks investigated in the 2009 Verizon Business report were classified as "not difficult," makes it clear that many still do not.

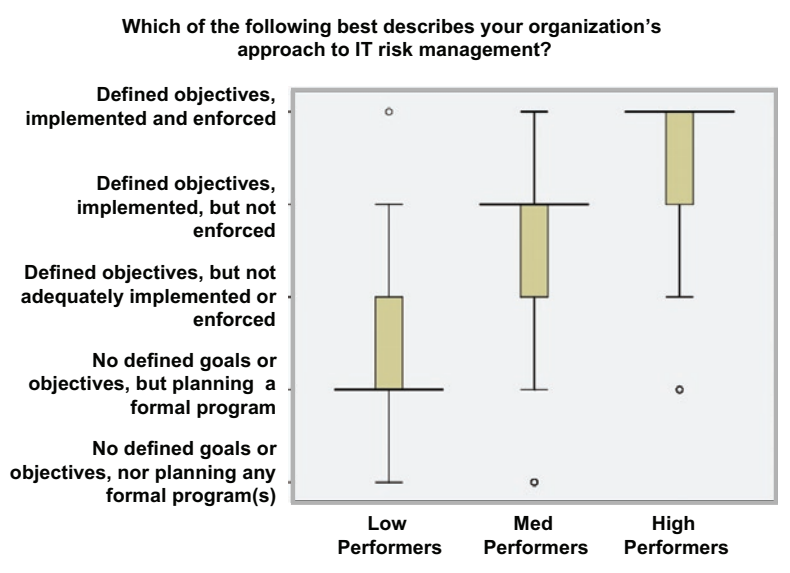
2 http://www.privacyrights.org (as of July 2009)
3 For a graphical depiction of the global distribution of loss incidents, see http://datalossdb.org/statistics
4 *IBM Internet Security Systems X-Force® 2008 Trend & Risk Report,* IBM Global Technology Services, January 2009
5 W. H. Baker et al, *2009 Data Breach Investigations Report,* Verizon Business RISK Team, April 2009
6 *Op. cit.*

What is missing in many cases is a more strategic approach to IT security management. Such an approach recognizes the critical value of establishing a foundation of reliable consistency in IT controls and tactics—but a truly effective approach goes beyond addressing the basics of a disciplined environment. It means a recognition that visibility and insight into the continuous evolution of threats and how to deal with them has become an essential fundamental, and that effective controls must embrace actions, processes, and continuous improvement of the approach, not just static objectives and fixed milestones.

For many, this may require seeing the security management challenge in a new, more comprehensive, and more systematic way—a way that enables the building of a solid foundation for combating today's risks and emerging issues, and gives the enterprise an advantage in preparing for those that are yet to come.

What Sets High Performers Apart?

This implies a decidedly proactive approach—but what defines success? This was the question EMA sought to answer in researching the effectiveness of enterprise security, IT risk management and compliance efforts among more than 200 organizations worldwide.[7] We asked about the criticality of IT to specific business priorities such as reaching new markets or key business processes, and the extent of executive support for security, risk management and compliance initiatives. We asked about outcomes in terms of percentages of disruptive security events and those resulting in lost control of sensitive information. We also examined IT's effectiveness in managing risks such as availability, performance, and project outcomes, which speaks to the IT organization's commitment to serving the business. Grouping respondents according to their level of response in these areas enabled us to categorize high, medium and low performers. What we learned from high performers says a great deal about the perspectives of those who take a strategic approach to security and risk management.



High performers do more than pay lip service to the "Plan–Do–Check–Act" philosophy. In general, they define objectives, actually implement them, monitor the environment for deviations and potential risk events, and respond accordingly. In this and similar "candlestick" diagrams in this report (taken from recent EMA research on IT risk and compliance management among more than 200 enterprises), the wide central tick mark represents the median of all responses within the group. The grey bar represents the middle 50 percent of responses, while the tails at top and bottom represent the top and bottom 25 percent respectively. When a significant number of responses are similar, they may be concentrated at a single point. Other marks within the group represent "outliers."

7 *IT Governance, Risk and Compliance Management in the Real World,* EMA Research Report, May 2008

If there is one thing high performers have in common, it is their commitment to all four phases of the "Plan-Do-Check-Act" ("PDCA") approach.

If there is one thing high performers have in common, it is their commitment to *all four* phases of the "Plan-Do-Check-Act" ("PDCA") approach. This is the essence of guidance such as the ISO 27000 series of information security best practices—but high performers do more than pay lip service to the philosophy. In general, they achieve all four milestones of: 1) defining their objectives; 2) actually implementing them (it is remarkable how often many do not); 3) monitoring for adherence to those objectives, as well as for potential events and other factors that threaten the posture; and 4) responding when events and issues require. Do not be deceived by such a simple four-point summary, however. Achieving such thoroughness requires considerable, consistent and ongoing commitment from the organization, backed by solid support from senior management, beginning at the C-level. *All* these factors characterize high performers in the EMA study.

Compare this to the findings of an earlier Verizon Business data breach study, in which four years of data from over 500 cases was examined.[8] In 59% of the cases in this study, the breach victim had established security policies, but had failed to enact them in actual processes. These organizations had defined their objectives, but failed to implement them. In 82% of cases, evidence was available to victims (in the form of log data, for example), but this information was either not noticed or not acted on. These victims had defined their objectives, actually implemented them, and were monitoring the environment, but failed to achieve the fourth milestone of responding to issues and events as they arose. This last example underscores Enterprise Management Associates' finding that *all four* milestones are vital to the effectiveness of a management strategy.

Note that these are also values prized by those who excel in the disciplines of IT Service Management (ITSM), which targets the responsiveness of IT in serving the business—particularly meaningful in light of the close relationship of ITSM values such as configuration control and vulnerability remediation. These factors also speak to the quality management priorities of high-performing organizations, in the stability, reliability and continuous improvement of ITSM and security alike.

These parallels are more than coincidental. They are reflected in the EMA study's findings that highlight the guidance respondents adopt most often. Considering the risk and compliance focus of this research, one might have expected the most frequently adopted standards, control frameworks or best practices to be the ISO 27000 family, COBIT or COSO, NIST or similar guidance. They were not. What respondents adopted the most was ITIL, the process- and service-centric IT Infrastructure Library that guides IT Service Management initiatives worldwide—and at 55%, the only guidance adopted by a majority.

Just as provocative is the fact that the next most frequently adopted guidance was not specific to security, risk management or compliance, either. It was Quality Management (Six Sigma, Total Quality Management, and ISO 9000 standards, for example); adopted by 36%—6 percentage points ahead of the most commonly adopted security-specific guidance, the ISO 27000 family. These findings emphasize that the management of security is not a silo. It is part of the overall challenge of managing business risk in IT and helping the business to pursue its primary objectives. Opportunity is not without risk, and high performers seek to help their organizations seize opportunity while managing the risks they can. Those who share this view with the business may fare better in winning the support of their organization in pursuing a more effective strategy.

8 W. H. Baker et al, *2008 Data Breach Investigations Report,* Verizon Business, June 2008.

Laying the Foundation: Applying the Lessons of High Performers

Many may look at their own approach and wonder how or where they can best make improvements. Others may consider the investment already made in their approach in the light of the continued evolution of risks and threats, and wonder how they can chart a course through an increasingly challenging future.

Where to Begin?

- **The best—and in fact, the only—place that any organization can begin this journey is to consider the current state of play.**

Most organizations have some range of security management tools and processes in their environment. The current posture may be the accumulation of responses to risks, threats, and compliance requirements that have built up over time. If the organization has not experienced a significant incident—or is not aware of threats that may already be present—it may or may not have undergone any substantial re-evaluation.

Sometimes the organization does have a (relatively) blank slate, as with the adoption of new technologies or in planning the deployment of new IT services. In these cases, high performers in the EMA study recommend integrating a consideration of risk factors as early as possible—from concept forward. When harmonizing such an approach with the interests of the business, organizations should note the consistency of this philosophy with, for example, ITIL version 3 principles regarding the lifecycle of IT services, particularly when integrating security considerations early in Service Strategy and Service Design phases.

Putting this philosophy into practice can be made practical through tools that integrate security into the Software Development Lifecycle (SDLC) of applications developed by the enterprise, such as source code security analysis in development. These tools help developers identify and resolve security issues before resulting functionality is put into production, as part of development processes that integrate security directly into the SDLC. Even earlier in the process, concepts such as Model Driven Security can enable modeling tools to generate security functionality integrated directly into resulting source code, with minimal developer intervention. While the concept of Model Driven Security may as yet be unfamiliar to many developers, tools such as source code analysis are becoming better known. (We will return to the topic of application security later in this report.)

In reality, however, organizations already employ a range of processes, tools and techniques. While a detailed discussion of a thorough assessment of the current posture is outside the scope of this report, enterprises may want to compare themselves to some specific examples of how high performers take a more systematic and proactive approach.

Counter Threats

- **Making the most of today's countermeasures**
- **Leveraging intelligence to enhance capabilities**

Many organizations employ commonly accepted tools of defense, such as firewalls, intrusion detection and prevention, and antivirus systems, at both the network and host levels. These have more recently been supplemented with technologies such as anti-spam and message filtration, and safe Web browsing. As threats continue to evolve, these tools augment defense by capturing activity throughout the environment, which provides important insight into the nature of actual threats. High performers recognize that this information provides data to event management systems for correlating and identifying priority issues, and to security operations and incident response teams for analysis and follow-up. This is one example of not only how the value of existing tools can be extended in the face of emerging threats and new risks, but of how high performers tend to take a more systematic approach to security management. They also recognize that security intelligence provides more than just an awareness of the threat environment.

Security intelligence is one of the most important—yet far too often overlooked—assets a security management program can leverage. Many recognize the need to understand the nature not only of actual threats "in the wild," but of research that reveals vulnerabilities and weaknesses in current environments, new and emerging threats, and the impact of security events on their peers. High performers often take advantage of services that enable them to "tune" their intelligence resources to those issues directly relevant to their environment, to improve the efficiency of intelligence gathering.

Modern countermeasures can directly leverage security intelligence resources to tune their response to emerging threats or other issues that might otherwise go unrecognized without human intervention.

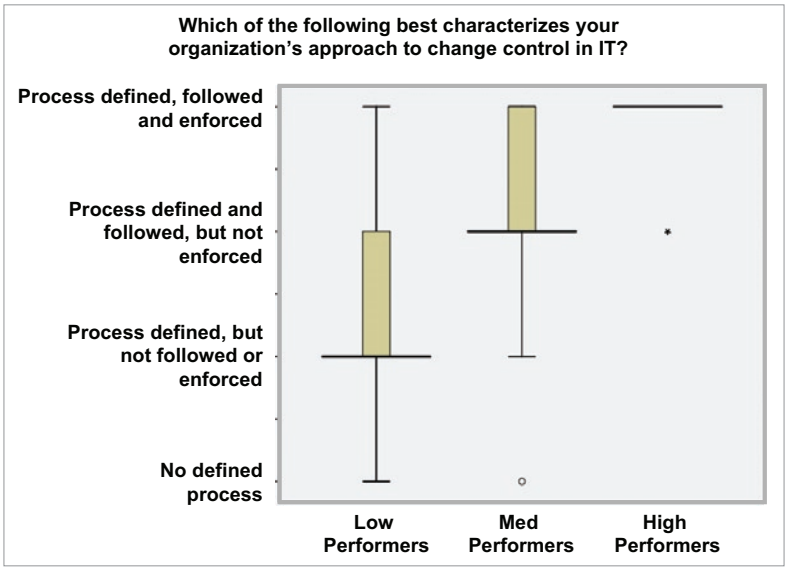
Today, security intelligence can provide even more. Modern countermeasures can directly leverage security intelligence resources to tune their response to emerging threats or other issues that might otherwise go unrecognized without human intervention. When they can do this automatically, they not only help to ease the burdens of security management, they can deliver a more proactive response to emerging threats, reducing risk exposure when second count.

Resolve Vulnerabilities

- **Unfortunately, too many organizations focus on threat defense without considering the adequacy of their approach to managing vulnerabilities.**
- **In the broadest sense, vulnerabilities may include gaps in management processes and dependence on human judgment as well as weaknesses in software and systems, all of which may play a role in exposing risk.**
- **These lapses are a peculiar paradox considering that, while attackers themselves cannot be controlled, many aspects of the enterprise environment can.**

Penetration testing and the assessment of vulnerabilities in software and system configuration have long been considered standard procedures for measuring this aspect of the actual security of the environment. Many organizations rely on service providers for these tasks because of the expertise required,

the need to subject the environment to the same realistic tactics an attacker would use, and the intelligence needed to measure the environment against current real-world threats. Today, the assessment of software and system vulnerabilities extends into entirely new domains, largely due to the proliferation—and increased exposure—of Web applications. Because each Web application environment has its own unique characteristics, the need for specialized expertise in this realm is even greater.



Vulnerability assessment must be complemented by vulnerability remediation, which highlights the central importance of tactics such as configuration and change control to security. Just as important, however, is the significant and positive impact controls such as configuration and change management can have on the quality and performance of IT's service to the business, by improving the stability and reliability of the environment. These are two of the reasons why high performers in EMA research are virtually unanimous in this area. Ninety-four percent of high performers achieve all four PDCA milestones of *defining* configuration and change control processes, actually *implementing* those objectives, *monitoring* the environment for unauthorized change as well as for outcomes of authorized changes, and *responding* to change events as warranted. Response may range from triggering a security incident management process, to enforcing consequences for changes made by enterprise personnel or contractors outside authorized processes. Given these values, it should not be surprising that high performers not only have half the median incidence of disruptive security events, but also tend to have lower incidence of unplanned IT work, more successful IT changes, and better overall achievement of IT Service Level Management (SLM) commitments.

The complementary natures of vulnerability assessment and vulnerability remediation highlight the systematic approach high performers take to a comprehensive security management strategy. As technologies such as antivirus and anti-malware address their current challenges, this systematic approach will be taken even further. Approaches such as "whitelisting" that restrict systems to an approved complement of components can help organizations defend against malware that seeks to modify vulnerable targets, exploit memory management, and implant threats such as keystroke loggers, rootkits and Trojans. Here again, enterprises will want to engage with thought-leading vendors across all these domains to assure the continuous improvement necessary to effective defense.

They will also want to take a broader view of vulnerability control, in areas such as weaknesses in applications developed in-house, controls on sensitive information, the management of identity and access to IT resources, and other interactions of people and process with technology that can reinforce a stronger security foundation. Web-related vulnerabilities in particular have become one of the most fertile fields for attackers—on both the client and server side. The browser and its seemingly endless range of add-on functionality has become an increasingly popular target of attack, while Web applications present an entirely new domain of endeavor, for attackers and security professionals alike.

Manage Application Risks

- **Vulnerability management and configuration and change control have already been recognized as key components of managing risks to system platforms and commercial "off the shelf" applications.**
- **Today, however, thanks largely to the flexibility and extensibility of Web technologies, applications are becoming much more capable and reaching more broadly than ever before.**
- **This raises new risks for vulnerability control, particularly when the enterprise develops and maintains its own applications.**

This reality was underscored by the IBM Internet Security Systems X-Force 2009 Mid-Year Trend and Risk Report, which reported a 508 percent increase in the number of new malicious web links discovered in the first half of 2009. This includes an increase in malicious content on otherwise legitimate and even trusted Web sites, including online publications and mainstream news outlets—an indicator that attackers are leveraging vulnerabilities in legitimate sites in order to exploit user trust in those sites and propagate attacks.[9]

The emerging field of vulnerability assessment for Web applications was touched on in the preceding section, but security for application environments must go much farther, not just for remediation but for proactive prevention of security exposures before they appear in a production application. This means integrating security more effectively throughout the SDLC. It also means recognizing fundamental and systemic weaknesses in Web security, where the interoperability between server-side functionality, browsers and browser plug-ins increases complexity and exposes risk. Taking a systematic approach to managing these risks will be required, if the future of Web security is to be assured.

For security-aware organizations, an approach to more secure application development and deployment begins in the SDLC itself. As introduced earlier, tools such as static source code analysis can help developers identify security issues during development—but more is still needed in order for organizations to build a truly systematic approach. It may not be reasonable to expect developers to also become security experts—but they are directly responsible for integrating security directly into applications, and have primary responsibility for crafting remediation once vulnerabilities become known. This highlights a need not only for developer training, but also for the encouragement of a "culture of security" throughout application development and deployment processes. As with all other applications and systems, a disciplined approach to configuration and change management can help assure more effective control over the application environment, and can alert the organization when changes to critical application dependencies may impact business priorities. When complemented by regular security assessment of Web applications, combined with a layered approach to defense that specifically protects applications, these tactics can help realize a comprehensive application security strategy.

9 *IBM Internet Security Systems X-Force 2009 Mid-Year Trend & Risk Report*, IBM Global Technology Services, August 2009

Protect Sensitive Information

- **Today's security threats increasingly target sensitive information as their primary objective.**
- **Protecting this information is one of the broadest challenges in the enterprise. Information is found literally everywhere in an organization—and beyond.**
- **Strategies must recognize that regulatory requirements change over time, and must therefore be adaptable to new approaches to control.**

From the data center to the endpoint, on both internal and external networks, among partners and contractors as well as its customers and stakeholders, managing the security and privacy of sensitive information has become a primary concern of the enterprise. Responding to the impact of lost control, privacy regulation has become a priority for public as well as industry policy makers in multiple sectors, with much of the burden laid on corporate information security efforts.

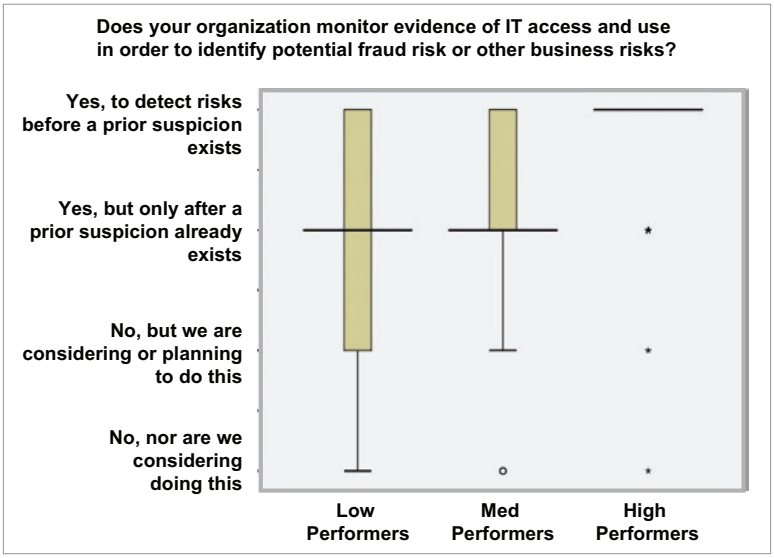
Given the scope of the challenge, it would be hard to imagine anything requiring a more systematic approach. Not surprisingly, *every* high performer in the EMA study reported having a strategy for securing sensitive information, while 11% of medium performers and 27% of low performers did not.

The discovery and classification of sensitive information throughout the enterprise can be one of the most daunting challenges of all—a challenge compounded by the sheer volume of *unstructured* data, largely found in documents, messages, and other places outside more systematic repositories such as databases. Once sensitive information is discovered, privacy controls must be applied consistently in order to assure policy and strategy objectives. These demands require the advantages of automation—a requirement that has spurred investment in technologies such as Data Loss Prevention (DLP) for automating the consistent application of policy controls. They will also recognize that sensitive information is not always found where one might think. The need to protect sensitive data used in application development and testing, for example, has raised new awareness of the need for techniques such as data masking in the SDLC. Data masking can also be used to protect sensitive data from those without a need to know, such as development contractors.

Those who recognize the importance of integrating a data protection strategy across multiple, often diverse resources will value not only the capabilities of today's information management systems, but also technologies such as data masking that can protect the data needed to test and evaluate applications in development, as well as cross-vendor initiatives such as the Key Management Interoperability Protocol (KMIP) that promote comprehensive as well as consistent control. Even when integrated in a strategic approach, however, the adoption of such tactics addresses only part of the challenge. For example, while encryption is a powerful privacy enabler, it may also have the unintended consequence of impairing the visibility essential to more effective security management. Attackers can leverage encrypted network links, for example, just as effectively as legitimate organizations to hide actions and content. High performing organizations that recognize the need to balance these priorities will therefore deploy privacy controls in line with a strategy for maintaining as much visibility throughout the environment as possible. This requires both expertise in designing and deploying such controls, as well as a substantial experience of success in challenging technologies such as encryption.

Strategists must also recognize that regulatory requirements continue to emerge, while existing mandates—particularly the most prescriptive—will change and evolve over time in response to the ongoing evolution of risks and threats. This requires an approach to control that adapts to these changes—and highlights another area where security services may expand this adaptability.

Manage and Enforce Identity, Access and Entitlements



- **Identity and Access Management (IAM) is a front-line IT control, and a primary focus of information protection.**
- **IAM is essential to defining access appropriate to the individual's current role, as well as to enforcing separations of duties (SoD) and other controls on business risks.**
- **Effective access control can also enable higher confidence in information-centric business processes, particularly when complemented by controls on threats that exploit access privileges.**

As anyone experienced in an identity management deployment well knows, however, identity and access management is more than just a set of technologies for managing access to IT. It must also recognize—and implement—the business processes that link users, groups, and their roles with specific resources. High performers recognize not only these human factors, but the practical application of the principle of "least privilege" that constrains access to that required for specific business purposes.

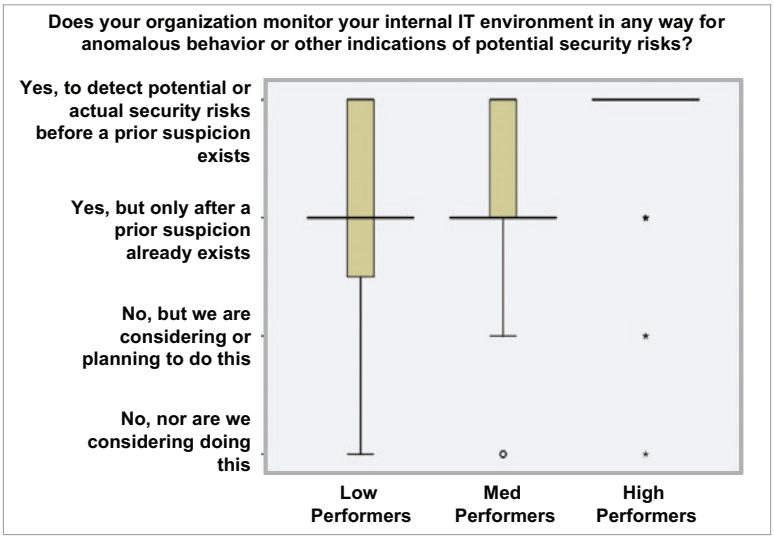
The foundations of identity and access management begin with a thorough approach to IAM governance that meets the requirements of discovering, documenting and analyzing user access; establishing a process for user access governance; ensuring that constraints help manage business conflict; enforcing policies; and continuous monitoring. This provides the basis for the intelligent deployment of tools for provisioning access entitlements for new users and groups, recognizing business roles and accommodating role changes in the organization, and—critical to managing comprehensive risks—*de*-provisioning or terminating access and entitlements when no longer required. These capabilities are just as important, if not more so, for managing the access of external customers and the general public.

Because Web technologies are often used to reach these groups, Web identity has become as significant to strategy as access control within the enterprise, with emerging trends such as "user-centric" and claims- or assertion-based approaches attracting new interest, for their value in protecting *specific* elements of sensitive information in a given use case.

Many organizations recognize that success in this domain has come with experience. Here again, preferred suppliers will demonstrate a substantial track record in developing and deploying the systematic processes and technologies of identity and access control, with a reputation for successfully integrating emerging developments that may have a direct impact on strategy going forward.

Manage Events and Respond to Incidents

- **Once the processes and tools of proactive risk mitigation and threat defense are in place, organizations must consider how they monitor and respond to issues as they arise.**
- **These are the third and fourth milestones respectively of the high performer, and are among the most important domains in which security tactics can have a positive impact on refining and improving risk control.**



This means collecting more than suspicious events. It also means monitoring the consistent observance of policy and process, from the application of privacy controls to change events and outcomes and the access of sensitive resources by users and groups. It requires the ability to recognize activity that may indicate a wide range of risks, from attacks to the unauthorized behavior of personnel, contractors, customers and the public alike. Ideally, a truly comprehensive approach should integrate input from management tools beyond those centered on security or compliance, such as systems, network and application management resources that can help correlate a more complete context of events. Conversely, security event management may provide insight into root cause events that directly impact the business performance and availability of IT.

Security Information and Event Management (SIEM) systems are natural centers for aggregating, correlating and prioritizing this information. Without such tools, the wealth of information collected

can be overwhelming, and important issues may become lost in the noise. They are key enablers of threat awareness and incident response, triggering investigation of suspicious activity, and alerting response teams efficiently. They can also help to reduce the cost and burden of compliance reporting, through automating the generation of reports. Organizations dedicated to continuous improvement will also recognize their capability for capturing information than can later be analyzed for new or as-yet unknown issues, with learnings folded into the continuous improvement of strategies for more effective defense.

Stretching the Boundaries

- **Increasingly, the security mandate in many organizations goes beyond securing IT and information alone.**

Physical security, for example, is increasingly integrated with "digital" security in many enterprises—hardly surprising considering that many physical security controls not only rely heavily on IT for their management, but in fact are often IP-networked systems and devices themselves, and these networks must also be secured. The sheer volume of information generated by physical security controls such as video monitoring also brings this domain together with IT. Physical and logical security also have a common interest in both physical and logical threats to the business in disaster recovery and business continuity planning (DR/BCP), a critical domain of information risk management in its own right which must be factored into a comprehensive security strategy.

Distinctions between physical and logical security are not the only fading boundaries of control. Ultimately, it is the actions of individuals that are behind many if not most threats to sensitive information and IT. This not only includes the malicious, but also the everyday behavior of ordinary individuals in their interactions with technology. It also includes the actions of skilled professionals, as described in the earlier section on the need to better integrate security into application development processes.

Ultimately, it is the actions of individuals that are behind many if not most threats to sensitive information and IT.

Here, addressing human factors such as professional training, awareness programs and business process definition can help organizations foster a more security-aware corporate culture. The importance of such a culture is underscored by the emphasis high performers place on senior management support for their efforts. Programs that enhance security awareness can help play an important role in assuring that this support pervades the organization to the extent possible. They can foster more secure business processes and better understanding of policy, while helping skilled professionals as well as ordinary technology users learn how to better implement security in practice, and to use information tools and technologies with less risk. Just as important, such efforts keep the lines of communication open with security strategists, and can be used for valuable feedback and insight into what works (and what doesn't) when it comes to adapting effectively to human and cultural realities.

Many organizations, however, have more than they can handle in dealing with day-to-day firefighting, let alone taking on these additional aspects. Service providers can help organizations define more secure business practices and processes, and can deliver training and awareness programs tailored to the needs of a specific organization based on experience with approaches that have demonstrated impact.

Toward the Future: Emerging Technologies, Threats and Tactics of Defense

- **The foundations of information security must go beyond the approaches that prevail today.**
- **Technologies continue to evolve, for IT and information management as well as for effective control.**
- **And, just as importantly, so do risks and threats.**

Virtualization is one of the most visible recent examples of the impact technology advances have on security strategy. The technology of virtualization itself has been well known in a mainframe context for years. Today, the scale-out of virtualization on commodity systems and the implications of consolidating multiple virtual machines in such an environment raise new issues for control. The meaning of a "dedicated server"—directly relevant to Payment Card Industry (PCI) compliance, for example—is just one example. More significant are the impact of security threats not only at the level of the hypervisor, but on shared resources such as memory, storage and underlying infrastructure. The challenges of control may be exacerbated when virtual machines can proliferate automatically, should concepts such as live migration fulfill their ultimate potential. Already, uncontrolled or poorly controlled "virtualization sprawl" has become a significant management issue.

The challenges of secure virtualization are also part of the security challenge of cloud computing, another concept that has attracted significant attention in recent months. Cloud computing often depends directly on the values of virtualization for providing "IT as a service" in new and more flexible ways—but defining effective control when that control is put into the hands of a service provider, assuring regulatory compliance when compliance mandates themselves are not yet clear on requirements, and maintaining visibility that satisfies both the customer's and the service provider's requirements, are just a few of the many challenges whose resolution is yet to be defined in a cloud computing context.

This, however, highlights another way in which high performers stand apart. Today's high performers are taking a proactive approach to addressing these concerns. In order to define workable strategies, however, they will need the partnership of service providers and suppliers that are equally proactive.

The emergence of new threats such as obfuscated attacks and complex threats that exploit networks of victim machines numbering into the millions raise the stakes even higher. Together, those who define advanced approaches to control and defense—among technology vendors, service providers, and their customers alike—will help to define what it means to have an effective strategy as these issues transform the nature and meaning of information security.

The Services Advantage

- **Not all organizations are able to deal with these challenges effectively across all domains—even when well informed and willing.**
- **Many would embrace a more comprehensive strategy, but are limited in the range of tactics they can pursue, through budgetary, manpower, or other business constraints—particularly in the current economic climate.**

- **Many more see the value of services as an essential external resource, as with security intelligence.**
- **For these organizations, the alternative of security services may have high appeal**

These have long included managed services such as security point product management (outsourced firewall and intrusion prevention systems management, for example), vulnerability management services such as outsourced assessments and scans, and message filtration. Increasingly, however, organizations are outsourcing broader aspects of security management, from hosted vulnerability assessment, Web and message filtration and the collection, correlation and analysis of events, to incident response, technology integration and deployment, the security implications of configuration and change management, and even strategy development itself.

This highlights the increasing consolidation of security expertise among security service providers, which makes them an attractive resource for helping the enterprise identify how and where it can best make its approach more effective. And this, in turn, brings us back to where we started: where to begin with building a foundation for a more systematic strategy. The experience and expertise of security service providers makes them an excellent resource for assessing risk and charting a course of action. Those whose view is even broader with respect to the business impact of IT and information risk are well positioned to more fully address the wider realities of risk management—something that should go well beyond technology risks and threats alone.

Finding the Right Strategic Partner: The IBM Difference

For many, this journey will lead them to IBM, whose capabilities in both security and business enablement make it a preferred supplier for assessing where the organization is today, and helping it get to where it wants to be tomorrow.

The trajectory of IBM in IT and information security in recent years has paralleled the traits of high performers in many ways. A leading supplier of information technology across the spectrum of business, from solutions for the small- to midsized organization to large-scale data centers and complex global enterprises, IBM knows the security demands of the information-centric enterprise as few others do. This gives the company a unique perspective on how to leverage its capabilities effectively in a comprehensive approach.

IBM is recognized for its commitment to research and intelligence, not just in enterprise IT but across multiple domains of security.

Furthermore, IBM is recognized for its commitment to research and intelligence, not just in enterprise IT but across multiple domains of security. From its longstanding core research organizations to the recognized R&D capabilities of its IBM Security brands, these centers of research give the vendor a distinctive position in the industry: the insight of recognized, security-focused expertise, backed by the capability and credibility of IBM. When coupled with the service delivery capabilities of IBM Global Technology Services, these values give IBM the potential to help organizations develop strategies markedly different from those of the past, with thought-leading security technologies and services complementing preferred business solutions, integrating expertise across the portfolio as customer strategies mature. Such an approach is vital to tackling security and risk management challenges of a complexity and sophistication never seen before.

EMA Perspective

Taking a strategic, comprehensive and systematic approach to security is not something an organization can achieve overnight. It requires cultivating a culture of commitment to security values, embracing new approaches when informed intelligence demands, while making the most of existing assets and making all these tactics work more effectively together. This can only be done in collaboration with trusted partners, armed with the most current and objective knowledge of what works and what doesn't in planning for both today's and tomorrow's risks.

In light of IBM's growing presence in security and compliance, and the weight of its impact on the larger issues of business risk control, these factors should make IBM a primary partner to consider in shaping strategy and evaluating technologies and services that make a difference.

In light of IBM's growing presence in security and compliance, and the weight of its impact on the larger issues of business risk control, these factors should make IBM a primary partner to consider in shaping strategy and evaluating technologies and services that make a difference. Few others have the range of capabilities of today's IBM for addressing the challenge—fewer still have the resources of an IBM for understanding the nature of business risks and emerging threats, and how best to address them going forward. IBM's assets in technologies such as antivirus may not have the visibility or penetration of competitors, but these technologies may be nearing the limits of their legacy capability regardless. Instead, IBM has chosen to take on the future. Though it has thus far chosen to partner rather than acquire in domains such as Data Loss Prevention, the progress IBM has made in its own portfolio in just a few short years suggests how far IBM can go—and may go yet—in leveraging its commanding market presence. Today, no other vendor can match the portfolio of systems, application resources, management technologies and security products and services that IBM can bring to bear on the challenge of managing business risk in IT and information systems.

With a solid and broad spectrum of R&D backed by the capabilities of an IBM, today's IBM is in a very strong position to help enterprises think about the future differently in developing a comprehensive strategy built on the foundations of effective business risk control.

About IBM

IBM offers solutions that are flexible, scalable and secure—bringing all of the elements of securing the enterprise together through products and services. With the IBM Security Framework, organizations gain the advantage of having end-to-end security coverage regardless of organization size, location or industry segment. Through comprehensive security assessments, design, security lifecycle methodologies, and security solutions—all backed by industry-leading security research, development, and expertise—organizations are empowered to manage the risks and compliance mandates associated with technology and a range of business workloads. IBM security can help customers ensure that their dynamic infrastructure is ready to securely support organizational innovation and growth. To learn about IBM's comprehensive suite of IT security solutions, visit ibm.com/security.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that specializes in going "beyond the surface" to provide deep insight across the full spectrum of IT management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help its clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise IT professionals and IT vendors at www.enterprisemanagement.com or follow EMA on Twitter.

Corporate Headquarters:
5777 Central Avenue, Suite 105
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com

1993.121809