Intelligent Security: Defending the Digital Business
“When an opponent comes forward, move in and greet him; if he wants to pull back, send him on his way.”

Morihei Ueshiba, creator of the Aikido martial art
Companies need to move their cyber security efforts away from traditional defensive approaches toward a proactive stance aligned with the organization's business objectives.

Just as an Aikido master blends with and redirects the motions of attackers instead of confronting their force directly, many companies need to adopt a new and more active stance to deal effectively with increasingly sophisticated cyber security threats and burgeoning digital opportunities.

Despite all the effort and resources that organizations invest in traditional information security approaches, many still fall prey to cyber threats, or find they are unprepared to deal with rapidly blurring enterprise boundaries.

A new active security stance will help enterprises address the changing demands of a global and mobile work force, provide proactive data protection, and help organizations to understand potential threats and attack vectors. The new approach will readily integrate with a firm's phalanx of cloud services, suppliers, identity, and access management technologies, and mesh effectively with the information security fundamentals currently in place. In essence, companies need to move their cyber security efforts away from traditional control-focused defensive approaches, toward a proactive stance aligned with the organization's business objectives.

While the list of issues companies will have to juggle to achieve this new stance can be formidable, the five most common are explored on the following pages.
1. Missing the link between business and security

Protecting the business should be the first and foremost goal of any security program, but many enterprises do not make it a core competency. Despite this limitation, organizations need to tie their security programs to overall business goals and imperatives and actively engage business stakeholders in the security conversation, because untethered programs can drift and become largely ineffective. Unfortunately, many firms struggle to achieve this crucial alignment. The potential undesirable outcomes range from a lack of funding and direction to significant losses caused by security breaches or regulatory fines.

Aligning the security program with an enterprise’s commercial objectives requires a strong understanding of technical domains (how the various computing technologies are deployed across the enterprise) and their business relevance (how specific safeguards support specific business strategy objectives). Asked by an enterprise’s CEO how a specific security function supports the organization’s business objectives, some security executives might struggle to draw a clear line between the protection provided and its impact on the company’s customer satisfaction, loyalty and revenue. Similarly, security functions in many organizations are uncoordinated and lack true business performance indicators. Security executives often lack formal security strategies that are readily understood by business leaders. As a result, the security team may lack a logical road map for changing the organization’s view of the security function as simply an inhibitor or cost center.

2. Thinking outside the compliance (check) box

How many executives, on contemplating the latest breach of their company’s digital defenses, have wondered how it could have happened? After all, the organization was compliant with all of the industry’s cyber security regulations. Unfortunately, compliance does not ensure security. Instead, enterprises should view compliance as the minimum acceptable cyber security “bar” they need to clear. What’s more, most security programs that focus exclusively on control- or audit-centered approaches will probably fail because they do not align with two key elements: the business itself and the nature of the threats the enterprise faces.

Today, a sizable distance separates compliance from security, and many organizations have experienced significant losses because they relied too much on a mandated program’s expected ability to protect the organization (Figure 1). Often conceived as audit-centered exercises, compliance programs usually follow a common, limited-scope methodology, that focuses on adhering to regulatory requirements. Once this is established, auditors evaluate the company’s compliance on a quarterly or annual basis. Meanwhile, new threats arrive by the day or even by the hour.

On the surface, these differences may seem subtle and clearly, security and compliance share similarities. With a new security stance however, firms will not measure success in terms of audit findings, but instead by loss events and business impact. What’s more, audit findings are not really risks: they are risk indicators or contributors. Organizations that implement the appropriate security approaches are likely to achieve high degrees of compliance and explicit risk acceptance as byproducts (Figure 2).
3. Governing the extended enterprise despite blurring boundaries

Cloud, mobile and social networking solutions have earned their places in countless enterprise implementations by successfully creating business value, and are the “new normal” bedrock components of many mission-critical business systems. These extensions to the enterprise have changed the game from the traditional IT ownership and responsibility model, to one emphasizing pay-as-you-go for a standard service set with promises of overall reduced total cost of ownership. While business adoption has been widespread and rapid, many security organizations have lagged in establishing the appropriate frameworks, policies and controls to protect the expansions and contractions now common in extended IT environments. Moreover, businesses today demand ubiquitous access to systems and applications, and often allow employees to use their own smartphones and tablets in addition to enterprise-supplied ones. As a consequence, many security organizations face the dizzying prospect of governing and protecting a growing, but only partially owned, inventory of access points and externally hosted services.

A typical day in many organizations’ extended enterprises might include:

- Real-time provisioning of a dozen servers to support testing of a cloud CRM system.
- Granting mobile access to new capabilities for field representatives.
- Rollout of a business social network for sales, product and marketing collaboration.

Such innovations, while Eureka moments for the business units seeking them, represent precisely the types of situations security executives work to avoid: explosions of enterprise risk exposure due to lack of governance and insufficient data protection.

Figure 2: Enterprises unknowingly accept significant risk

<table>
<thead>
<tr>
<th>Compliance-driven or audit-driven security scope can cause organizations to implicitly and unknowingly accept a significant amount of cybersecurity risk.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implicitly Accepted Risk</td>
</tr>
<tr>
<td>Enterprise Security Risk</td>
</tr>
<tr>
<td>Compliance Risk</td>
</tr>
<tr>
<td>Specific Regulatory Risk</td>
</tr>
<tr>
<td>Perceived Risk</td>
</tr>
<tr>
<td>Actual Risk</td>
</tr>
</tbody>
</table>

4. Keeping pace with persistent threats

Cyber security threats have no regard for compliance objectives, regulatory requirements or entities in charge of running the enterprise, cloud services or mobile and social platforms. Instead, threats have a specific intent and target and no organization is completely immune. Annual threat reports paint a clear, quantitative picture of the motives and techniques used by attackers. Increasingly, sophisticated attacks come from multiple, coordinated entities seeking profit, notoriety, market advantage and intellectual property. Unfortunately, as the threats become more persistent, they become harder to identify.

External cyber attackers include national governments, activist groups and common criminals, and each type of attacker has different motivations and targets. Attackers target not only technical systems, but also company employees to gain a willing or unknowing internal accomplice. Given the increasing sophistication of attackers, companies rarely experience the assaults on their known and highly fortified “front doors.” Instead, an attack could begin at a less secure third-tier supplier and expand.

As more companies work to address the basic threats, they can expect increasingly sophisticated attacks and incursions. As a result, companies need to develop a dynamic approach including intelligence, analytics and response to deal with the widening variety of attacks. As Aikido master Morihei Ueshiba counseled students: “The best strategy relies upon an intelligent set of responses.”
5. Addressing the security supply/demand imbalance

According to recent research\(^1\), most organizations lack sufficient security talent to address their current needs. This shortage of skilled staff is contributing to the current rise in security breaches, which could ultimately affect a company’s customers and reduce its ability to grow profitably. Organizations of all sizes face major security expertise attraction and retention challenges including:

- **Skill shortages:** Most organizations lack the appropriate mix and amount of resources required to implement their security programs, and are shocked by hiring premiums. Listings for cyber security positions rose 73 percent in the five years through 2012.\(^2\)

- **Career development:** Security professionals, eager to keep their skills sharp, seek constant exposure to a broad array of new technologies, hands-on experiences and challenges. Supporting this variety of work is challenging for many organizations.

- **Firefighting:** Organizations that fail to align security programs to strategic business objectives, may face degraded morale and practitioner burn-out due to constant security fire-fighting.

**Preparing for a new approach**

As organizations shift from a compliance-centered security mindset to an active cyber security stance, security teams need to adapt to keep pace with evolving business objectives. Organizations must integrate many disparate and partially owned elements into a coherent framework to manage active threats to the company and, inevitably, to the extended enterprise. This is a daunting task; however, Figure 3 illustrates how the components of this holistic, threat-centered security approach could fit together.

Core business assets are protected in the center by robust enterprise security controls. Layered on top are extended enterprise safeguards focused on enabling cloud, mobile and social network adoption.

Advance analytics incorporate cyber threat intelligence to enable proactive, accelerated action. Security metrics are crafted to determine quantitative enablement of business outcomes.

Increasingly, security and business leaders recognize the need to move to an operating model with new governance strategies, technology partners, skills and integrated architectures. While many companies have assembled discrete tools and techniques that fall into these categories, the full value of extensive visibility begins with integration of the elements.

---


Intelligent security for the digital business

Leading companies develop effective cyber security measures to handle vulnerabilities, and, like an Aikido master, mount an active defense, calculated to meet and deflect attacker advances. Leaders proactively manage threats and focus their analytic security defenses on identifying and forecasting threats to the enterprise.

To improve the way they secure the digital enterprise and establish an effective security program, companies should follow five steps:

1. Assess the security program’s capability and identify leap-ahead opportunities

Before leaders can adopt a business-centered cyber security stance, they need to determine where their organizations currently stand and the level of resources required to support meaningful transformation. By assessing the security program’s maturity and adopting a strategy and roadmap, leaders can quickly understand the steps needed to advance (Figure 4).

Leaders can use the assessment to gauge the maturity of security operations, technologies and underlying processes. Companies typically evolve through three maturity phases:

**Phase 1—Understand threats**

Security organizations tend to be reactive and seek to standardize their operational processes and rationalize security tools. They largely use the company’s IT infrastructure for security purposes and strive to move toward a threat-centered approach. Enterprises in this situation need to establish processes for defining asset criticality and rationalized security capabilities, including asset valuation and tool rationalization, actively manage vulnerabilities and monitor threat intelligence.

**Phase 2—Understand your security posture, defenses and gaps**

Rather than simply piggybacking on their IT infrastructure, companies align, harmonize, and rationalize security processes and aggregated data into security intelligence. They use advanced analytics to uncover compromised defenses and outright attacks. They also automate technology and IT/security processes to drive better insight and agility.

**Phase 3—Detect and respond**

At the most sophisticated cyber security maturity level, companies target and research the activities of threat actors, use security intelligence to anticipate and adapt defenses and, when attacked, initiate coordinated, proactive responses. Like an Aikido master, they find ways to redirect an attacker’s advance and if possible use it against him or her.

Figure 4: An active defense road map can help companies assess their maturity and develop a path to their goal
A global energy company moved from simply understanding threats to assuming an adaptive defense posture in level III. Instead of reacting to attacks, it proactively sought to identify and contain them before damage occurred. Success in phase 3 required the company’s teams to gain a complete view of the threat landscape and how it affected the business. Organizations with effective security programs understand the tactics used by threatening actors and the myriad of attack vectors available to them, and have defenses in place to proactively respond.

2. Manage complexity and integrate the enterprise

Leading companies establish an end-to-end enterprise security program and integrate it with existing enterprise architecture processes to reduce complexity levels and produce outcomes valued by the business. In practical terms, they accomplish this by establishing a new vision of how security integrates and works with IT and the business, effectively creating a security operating model.

Through a collection of roles, processes, metrics and governance policies, a security operating model establishes a basic security operation across multiple organizational functions. It becomes part of the organization’s overall IT operating model, providing a holistic view of an organization’s security function and business touch points. It also informs the development of an organization’s security technology process model and forms the basis for security investment based on business attributes.

Ultimately, the model integrates into the overall enterprise architecture, technology and processes. For example, a multinational financial services company transformed its reactive security function into a highly effective global organization responsible for proactively protecting information assets. Focusing on business and security drivers, the new security organization initiated a number of prioritized programs to successfully build essential security skills including:

- Mobile and remote identity and access management
- Infrastructure and application security
- Data protection

The company was able to rapidly deploy a large number of core services relying on foundational methodology, pre-integrated technology and industry-leading services. Quick deployment reduced risk exposure and facilitated realization of business benefits.

Figure 5: Hallmarks of an effective security program

A large financial services company demonstrated successful implementation of the new approach by:

- Meeting business and enterprise risk goals as well as compliance objectives
- Understanding potential threats and vulnerability posture
- Protecting mobile and cloud-delivered business, IT and security services
- Incorporating identity and data protection as core capabilities
- Gleaning security intelligence through advanced analytics and responding effectively
3. Become agile

Leaders embrace the cloud to boost their IT agility and reach customers faster. They allow employees to use their own mobile devices to access sensitive internal data and social networks to sell products and harvest customer trends. Leaders capitalize on efficiency and cost benefits and do so within risk tolerances. Leading organizations match security to this enterprise sprawl through provider due diligence, proactive governance, standards and third-party security solutions to gain additional insight, control-coverage and peace of mind.

Given the stampede of organizations moving to as-a-service offerings for core business functions, leaders establish a security and technology governance approach to manage complexity and maintain acceptable risk tolerances. They actively address the processing and storage of sensitive business and customer data through integrated access management, encryption, tokenization and data loss prevention techniques.

Additionally, leading organizations create security-as-a-service approaches that help them to deploy cloud security services to meet business demands and simultaneously address regulatory, privacy and security requirements.

Leaders achieve equal or better security posture by employing integrated security capabilities across their cloud, mobile and social networks. Firms can take three key steps to make this approach work:

1. Consistently apply technical controls for and from the cloud to the extended enterprise
2. Craft contractual arrangements to address third-party service provider risk
3. Share responsibilities with cloud, mobile and social providers to improve agility in security operations.

Most critically, leading companies are adopting a bi-focal data-centered and threat-centered security model for the extended enterprise. This model can help them identify and locate sensitive data, understand how people are using it, see where it’s going (for example, to which devices, clouds, IP addresses and recipients) and ultimately decide how and when they should employ the most effective control actions. By focusing on the data instead of on the infrastructure or platform levels, teams can employ consistent control mechanisms that will be more resistant to failures within systems and applications, where enterprise control is limited.
4. Accelerate toward security intelligence

Leaders adapt to handle new threats to the enterprise by developing threat-centered operations — developing a deep understanding of adversaries, their goals and techniques. They assume an active defense stance that increases the level of effort required by an attacker and delivers adaptive, intelligent responses.

Leaders employ advanced analytics to deliver "context awareness." Their security operations teams employ a collection of monitoring and detection tools that can create an overwhelming stream of "actionable" alerts. Highly effective teams have discovered that cultivating a deep contextual awareness regarding these alerts allows them to improve their event triage and response performance.

At a global energy company, active defense manifested itself in several ways. First, it piggybacked on the instrumentation already common in the enterprises, mixing it with numerous other threat intelligence feeds and additional security event data sources. In addition, active defense helped the company to orchestrate responses using advanced analytic capabilities that provided superior cyber security intelligence. For example, advanced security analytics provided graphic tools to help teams analyze large data sets visually, supporting rapid, active defense responses.

This helped the company shift its focus from monitoring results to understanding issues and intelligently and rapidly reacting to threats at hand.

This approach can help leaders predict, prevent, and swiftly respond to threats or events within the extended enterprise. Combining high-value data sets with traditional machine data provides a deeper understanding of the story behind the security alerts. High-value data sets include information related to business processes, known external threats, reputation scores for systems and users, and data describing expected baselines. While these insights can help teams understand the event, an enterprise’s security intelligence capabilities will point it toward solutions that can facilitate new levels of security effectiveness.

5. Develop end-to-end delivery and flexible sourcing strategies

Effective security organizations plan a delivery and operational strategy for each of the security services they offer. Doing so requires them to decide which of the end-to-end security services the organization will pursue in-house, and which it will outsource to external providers. Leaders make a clear-eyed assessment of the enterprise’s internal competencies when it comes to designing, building and deploying elements of a cyber-security program.

Leaders justify sourcing decisions based on the overall risk tolerance, business case and commercial strategy determined during the initial security to business alignment. They also recognize that their security and business outcomes will rely on selecting appropriate partners with the skill depth and pre-integrated solutions to keep pace on their journey. Leaders gain security outsourcing benefits of reduced cost and complexity — and instead focus their energy on active defense, proactive security capabilities and business enablement.

Leaders benefit from around the clock coverage, continuously identifying potential threats and situations. They adopt a core security support team, sized to maintain a pre-determined security and risk posture, and have the ability to rapidly expand and contract to meet demand. This dynamic and flexible sourcing approach helps the necessary security coverage to be available when organizations need it most, but also allows better usage of resources during steady-state periods.

The best sourcing partnerships allow organizations to systematically prepare for tomorrow by understanding their current security performance, take steps to manage complexity and integrate the enterprise via an end-to-end security program. Leaders become more agile, adapt quickly to threats and develop excellent end-to-end security delivery.
In industries worldwide, security leaders seek effective ways to improve their ability to defend against cyber security threats, reduce the risk of inadvertent data disclosures, achieve and maintain regulatory compliance, and ultimately enhance the value they deliver to their business counterparts and shareholders. The challenges can seem overwhelming: blurred extended enterprise boundaries; security issues that outpace compliance mandates; increasingly mobile workforces; the rise of a new generation of “industrial-strength” attackers; major disconnects between business needs and security goals; and the continued war for cyber security talent.

There are effective responses to each of these hurdles that can help companies improve their cyber security performance. The first step is assessing current posture and adopting a business-aligned security strategy. Leaders retain staff experienced with security architecture planning and design, tools and integration to drive successful outcomes.

Establishing an end-to-end delivery capability, underpinned by a pre-integrated security solution set allows organizations to modularly select for their specific threat areas and adoption pace.

These new skills can help organizations transform their security programs from an approach based on static controls to one capable of adaptive responses. They also have the potential to disrupt cyber attackers through a variety of technical means. As part of the new cyber security stance, active defense will play a critical role in any organization’s security program success. To orchestrate active defense effectively, companies need a governance model that helps them to support business rules, lifecycles and opportunities.

Few organizations currently have these types of advanced skills and technologies for security management, due to an inability to tie technical assets to business operations. We believe security organizations should move to extract more value from the data they already collect and analyze. By establishing a core set of data management, security and analytic capabilities, security organizations can effectively build and scale up their security management programs to support the extended enterprise.

Like the Aikido master’s approach, creating a clear and complete picture of defense strategies and synthesized security data can help security leaders to make rapid, intelligent security decisions. Moreover, by linking security events and controls to business outcomes, chief information security officers have a clear line back to the value delivered to the business. The company thus focuses on effectively managing the risk environment instead of concentrating strictly on compliance at the expense of strategically securing business growth, value and innovation.
About Accenture

Accenture is a global management consulting, technology services and outsourcing company, with more than 305,000 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$30.0 billion for the fiscal year ended Aug. 31, 2014. Its home page is www.accenture.com.

For more information

Bill Phelps  
Global Security Services Lead  
bill.phelps@accenture.com

Ryan LaSalle  
Security Strategy Lead  
ryan.m.lasalle@accenture.com

Kevin Richards  
North America Security Lead  
k.richards@accenture.com

Dan Mellen  
Cloud Security Lead  
daniel.w.mellen@accenture.com

Anthony Robinson  
Asia Pacific Security Lead  
anthony.j.robinson@accenture.com

Lisa O’Connor  
Accenture Technology Labs, Cyber Security Lead  
lisaoconnor@accenture.com

Floris van den Dool  
Europe, Africa, Latin America Security Lead  
floris.van.den.dool@accenture.com

Arun Singh  
Managed Security Operations Lead  
arunk.singh@accenture.com

Copyright © 2014 Accenture  
All rights reserved.

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

This document makes descriptive reference to trademarks that may be owned by others. The use of such trademarks herein is not an assertion of ownership of such trademarks by Accenture and is not intended to represent or imply the existence of an association between Accenture and the lawful owners of such trademarks. Information regarding third-party products, services and organizations was obtained from publicly available sources, and Accenture cannot confirm the accuracy or reliability of such sources or information. Its inclusion does not imply an endorsement by or of any third party.

The views and opinions in this article should not be viewed as professional advice with respect to your business.