Living in a Borderless World

By Chuck Adams, Cisco IBSG Innovations Practice

During the past few years, the walls surrounding enterprise information assets have come tumbling down. The borders of the enterprise have been chipped away by cloud computing, social networking, and a whole new class of mobile consumer devices that enable employees, partners, and even customers to extend the enterprise to almost anywhere, anytime. These new technologies offer the promise of greater productivity, agility, and responsiveness—while presenting complex security threats to organizations' most important asset: their data.

How should CIOs navigate this new borderless world? Should they simply close the door to all external consumer devices in an effort to maintain a walled fortress around their information assets? Or is there a way to provide full protection to the network—*and* full connectivity and productivity for all who need to access it? This paper explores the special challenges CIOs face in this increasingly borderless environment, and offers a strategy for balancing full security with full connectivity.

Blurring the Perimeter: Where Does the Enterprise End?

In the past, data, applications, and users were all housed within an organization's physical campus. The traditional approach to security was to place firewalls around the borders of the enterprise, keeping proprietary data inside and unauthorized intruders outside. That began to change when enterprises started doing business online with customers, partners, and suppliers. This required IT architectures and policies that enabled certain kinds of interaction with outside users, while blocking the rest. In today's workplace, it is not unusual for important business resources—data centers, applications, customers, and partners—to reside outside the traditional enterprise perimeter. Workers may be full-time remote employees, or contractors. Applications might be hosted off-site, or even in the cloud. No longer can these far-flung critical resources be treated in the same way as internal resources. Increasingly, IT leaders are responsible for protecting data, applications, and processes that are outside their realm of control.

The Workforce as Connected Consumers

This new environment also includes devices that are outside IT's ownership and control. The last few years have brought wave upon wave of innovation in consumer technology—from music players, to smartphones, to always-connected tablets. Every enterprise has a workforce of connected consumers who use mobile devices to send text messages and

emails, access the Internet, play games, chat with friends, and share links to websites. They post updates on Facebook, tweet on Twitter, and post blogs, photos, and videos.

Many in this hyper-connected workforce are young people of the "millennial" generation, who have grown up online and expect their work environment to offer the same connectivity freedoms that they enjoy in their personal lives. In an era where work is increasingly global, and workers ever more mobile, business productivity can depend on mobile access to email, applications, and corporate data. Some organizations are also seeing value in having their employees visible on blogs, Twitter, and other social networking media as representatives of the company. Marketing and public relations efforts today are often built around these sorts of new media.

The dilemma for IT professionals is that as workers bring these devices and activities into the virtual workplace—whether they are employer-sanctioned or not—they may be opening a back door to the enterprise, threatening the security of valuable information assets.

Opportunity To Think Differently About Securing the Enterprise

IT and security executives have a wide range of responses to this new borderless environment. On one hand, they may think the safest way to prevent "back-door" access is to block *all* outside access from mobile phones, tablets, and other mobile devices, and to ban access to social networking media from within the organization. This approach may not be realistic, however, given the pervasiveness of new, highly connected consumer devices and technologies. More likely, security organizations will take a defensive approach to these new points of entry, reacting to each security breach as it occurs. This strategy is neither effective nor efficient, and results in a patchwork of expensive, stand-alone security products that may protect some important areas, but leave gaping holes in the organization's overall protective fabric.

The technological environment is evolving too fast for organizations either to block out threats or to react to each one as it happens. With the current dramatic shift toward ubiquitous wireless connectivity, IT managers need a framework to unify wired and wireless access, including security, access control, and performance management across many different device types. They need to evolve their infrastructure to deliver seamless, secure access in a world with many and new shifting borders. They need a pervasive, policy-based, information-centric security architecture that controls the flow of information throughout the environment. In addition to focusing on protecting each piece of corporate data, they also need to manage the flow of that data.

Solution: Borderless Networks for a Borderless World

Securing information resources in a borderless world begins with an overarching network architecture that enables IT to efficiently manage access from multiple locations, from multiple devices, and to applications that can be located anywhere. The key element in providing this sort of scalable, secure network access is a policy-based architecture that allows IT to implement centralized controls with enforcement abilities throughout this network—from server, to infrastructure, to client. Ideally, security is integrated into the very fabric of the architecture, not something that is added on. A networking platform that is optimized to run security services allows you to "turn on" security across the network

infrastructure at all appropriate points of potential attack, providing blanket protection without reducing network performance.

With central policies and consistent management, IT managers can enforce security without micromanaging each security function, user, or resource. A security function that dynamically assigns access and services for users and devices can help ensure that endpoint devices are authorized and healthy, using consistent, network-wide security policy enforcement.

The goal is to provide freedom and flexibility for users, while exercising absolute control over connected resources and everyone who wants to use—or abuse—them.[1]

Benefits: Full Protection, Full Performance

With comprehensive security services integrated into the network infrastructure, IT can unleash the full productivity of the enterprise without compromising system integrity. Mobile workers can have free and easy access to the applications and data they need to do their jobs. Remote or telecommuting workers enjoy the same ubiquitous connectivity as those working on the corporate campus. Vendors have easy access to production schedules and project specifi-cations. And Marketing can post up-to-the minute video coverage of a major product announcement on the web, while monitoring customer reaction in blogs, discussion groups, and social networking sites.

But these examples are only the beginning. A robust and flexible borderless network provides benefits that go beyond the typical province of IT:

- **Broader talent pool:** When employers are not bound by geographical boundaries, they can search far and wide for employees, contractors, partners, and vendors with specific qualifications.
- **Productivity and work-life balance:** Mobile technology offers workers flexibility in when and where they choose to work, enabling parents to stay home with a sick child, or respond to a critical email while watching an after-school soccer game. This flexibility not only contributes to worker productivity—it can also help attract and retain good employees.
- **Business resiliency:** Business operations across the country and around the globe have been disrupted by natural disasters, inclement weather, and potential health threats such as last year's H1N1 virus outbreak. Organizations that can support work from anywhere have the flexibility to keep people home and working productively even in the face of three feet of snow or the fear of infectious disease.
- **Path to the future:** With the convergence of data and voice, IT's responsibilities began to expand beyond its traditional limits. Today, building management systems are being integrated with IP networks, and IT security is coming together with physical security systems. A borderless network architecture will enable seamless network expansion as previously distinct systems continue to converge. [2]
- **Market intelligence:** With converged physical and data security functions embedded in the overall network architecture, organizations can extend security-oriented video analytics capabilities to monitor and study customer behavior in order to gain valuable insights about consumer habits and attitudes, Already, major retailers, hotel chains, and other consumer service organizations are starting to use digital video and

analytics to track customer traffic patterns, improve operational efficiencies, increase promotional effectiveness, and deliver better customer service.

Next Steps

CIOs should begin to evaluate their current information security architecture, and prepare to transform their role and organization. Begin by taking the following steps:

- Work directly with security managers to design a comprehensive and holistic strategy for information security
- Develop a comprehensive policy governing employees' social networking activities and network access from mobile devices, and extend enterprise security to cover each potential point of entry
- Determine the most critical types of information and develop commensurate information security policies and controls to actively protect each
- Transform security-management procurement processes and purchasing criteria to focus on interoperability and alignment with the security and enterprise strategy

As mobile devices and social networking become more ubiquitous, the walls surrounding enterprise information assets will continue to tumble. To protect these assets in an increasingly borderless world, security must be integrated into the very fabric of the network architecture.

For more information, please contact:

Chuck Adams
Business Resiliency Solutions Manager
Cisco Internet Business Solutions Group
cjadams@cisco.com
+1-512-340-3430

Endnotes

1. For more information on Cisco's Borderless Network architecture, see: "Cisco: Leading the Way to Borderless Networks," 2010, and "Cisco Borderless Networks: A Next-Generation Architecture that Delivers the new Workplace Experience," 2010.
2. These and other benefits of a borderless network architecture are cited by Matthias Machowinski in "Eliminating Borders To Enable Any Place, Any Time, Any Device Access: A Win-Win for Business, IT, and Users," February 2010.

Cheri Goodman of Cisco IBSG provided writing and editing assistance for this paper.

More Information

Cisco Internet Business Solutions Group (IBSG), the company's global consultancy, helps CXOs from the world's largest public and private organizations solve critical business challenges. By connecting strategy, process, and technology, Cisco IBSG industry experts enable customers to turn visionary ideas into value.

For further information about IBSG, visit http://www.cisco.com/go/ibsg.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**