



WHITE PAPER



>>> RISK AND REWARD:
Business
Opportunities
and the IT
Security
Challenge

SonicWALL and *CIO* magazine's custom solutions group recently conducted a series of facilitated conversations with dozens of CIOs and senior IT executives throughout the United States. The upshot: Most IT leaders are now building their technology infrastructure for growth. Their issue: How to seize new business opportunities while mitigating risk.





THE ECONOMY IS SHOWING STRONG SIGNS OF RECOVERING FROM THE RECESSION

shock of 2008 and 2009. Businesses are starting to place orders, and consumer confidence is (finally) on the rise. And while the jobs outlook could be stronger, many economists and business leaders believe that a growth in private sector payrolls is just around the corner. Most important, this period of growth should hold increased opportunities for companies in the majority of industrial and commercial sectors and geographic regions.

However, after an extended period of cost-cutting and overall consolidation, the issue on many IT leaders' minds is how best to prepare their organizations to compete in an expanding economy. For CIOs, it is about preparing for growth and change, and developing the right foundation with which to innovate, scale and build new products and services. It's about making the right business and technology investments. It's about doing all this while still angling for competitive advantage, reducing time-to-market, and driving down the total cost of ownership.

And while it's vital to embrace the

opportunity, opportunity always comes with risk. There's business risk—making inadequate, rushed decisions, or entering the wrong markets. And there's also technology risk—ensuring the company is investing in the types of technologies that build the business while sufficiently securing the enterprise.

The question CIOs must ask themselves is, how can they best mitigate the risks associated with new technology initiatives while bearing security in mind?

Velocity of Technology Change

In the roundtable discussions, IT executives said that, in some ways, they're lucky. New technology paradigms, such as virtualization, data center consolidation and initial forays into private, public or hybrid cloud computing architectures—including software-as-a-service—have provided efficiencies. These efficiencies include greater productivity, cost savings and scalability. Indeed, while business itself took a collective breather, many in the IT community continued on a path toward application modernization and general infrastructure refreshes (think Microsoft Windows 7). The founda-

tion to scale the enterprise was being built, even during the recession.

Add to the equation the increased freedom employees now enjoy, such as the ability to work from home or on the fly, thanks to mobile devices. Although key technologies like unified communications, including VoIP, had been primarily implemented to save costs, a side benefit is increased productivity since more devices now reside on the network. Mobile devices today are used to access enterprise applications and the Web, and for text messaging—increasingly with the aim of getting work done anywhere at any time. Indeed, 77 percent of enterprise respondents in a Fall 2009 IDG New Media survey said that they use a mobile device with Web capabilities.

However, these emerging technology initiatives also bring challenges. For example, those working from home or on the road have greater access to business resources, but they're often using unsecured mobile devices or personal computers, and unsecured connections. There's the potential that workers, customers and business partners accessing company data might provide an unintended gateway into mission-critical business systems.

So how do you secure these proliferating, unmanaged mobile devices? How do you ensure that access is for business purposes only, especially given the advent of cloud computing and employees' greater ability to work from home? And what about the data sent to and from mobile devices?

And then there's the use, whether sanctioned or not, of social media in the workplace. What was once a leisurely, home-based activity is now spilling into the workplace, as employees increasingly access sites such as Facebook®, Twitter® and YouTube®. According to the Web measurement firm Hitwise Intelligence, Facebook has eclipsed Google as

the globe's most visited site. In last fall's IDG New Media survey, 47 percent of respondents said they had added or maintained a profile on a social networking site in the past month—compared with just 29 percent a year earlier.

And it's not just personal. Social networks such as Twitter and LinkedIn function as the new agents of business networking. Even formal IT vendor-supplied collaboration systems now embrace social media. In addition, public relations and marketing teams are finding value in social networking to promote busi-

ness. YouTube is becoming the platform for companies' public relations efforts. And yet some enterprises are creating policies around access to these sites, curtailing or banning use in some cases.

The problem here, said the CIOs and IT leaders in our discussions, is twofold: Social media may provide the gateway for viruses and malware, and employees may end up discussing sensitive or private information without authorization. Overall, these social media sites, with their network demands and potential vulnerabilities, can be an IT headache.

But social technologies are a force to be reckoned with, and are increasingly becoming a top IT priority. In the 2010 State of the CIO survey conducted by CIO magazine, CIOs cite several technologies that will continue to garner the lion's share of IT dollars: virtualization, infrastructure (especially data center) consolidation, cloud computing and software-as-a-service, mobile technologies, Web 2.0-based applications, and converged communications.

And in each of these cases, IT leaders must address security, including data, applications, systems and process security.

The SonicWALL Approach



IT LEADERS ARE LOOKING FOR AN ANYWHERE, ANYTIME APPROACH to risk mitigation. At a time when traditional IT controls are fading, the security focus must be on users, content, devices and applications—not on ports or protocols.

Guided by its vision of Dynamic Security for the Global Network, SonicWALL® develops advanced intelligent network security and data protection solutions that adapt as both

organizations and threats evolve. Trusted by small to large enterprises worldwide, SonicWALL solutions are designed to detect and control applications as well as to protect networks from intrusions and malware attacks through award-winning hardware, software and virtual appliance-based solutions.

The company provides products in: secure remote access, endpoint security, firewall/VPN, email security, backup and recovery, and centralized management and reporting. SonicWALL solutions focus on enterprise infrastructure, retail, healthcare, education, government, PCI, VoIP, Clean VPN, Clean Wireless, and technology partner sectors and technologies.

SonicWALL technologies and solutions help enterprises and other organizations stay ahead of the curve as they move into a period of economic growth and opportunity. SonicWALL's vision reflects your changing world: Dynamic Security for the Global Network.

Organizational Vulnerabilities

IT executives say they recognize that these fundamental technology shifts will continue, unabated, into the foreseeable future. Indeed, the velocity of this change may increase as IT budgets begin to grow again.

According to CIO magazine's Economic Impact survey in April 2010, nearly half of IT leaders say their overall budget will increase in the coming year. That's up from 40 percent reported in the previous quarter, and only 14 percent nearly a year ago. Interestingly, spending plans remain focused on applications (50 percent) and Web or mobile investments (40 percent). And there's a keen emphasis on new projects and technologies. Some 53 percent of IT executives expect the percent of their total IT budget allocated to new projects to increase, up from 43 percent in the first quarter of 2010 and 23 percent in mid-2009.

With all this new technology and investment, however, comes greater vulnerability. Companies shouldn't increase technology investments without consideration to security breaches. Virtualization and cloud computing bring concerns about hypervisor threats and data

Growth can't be unfettered; it must be encouraged. Each organization must be security-aware. Each technology plan—whether it includes virtualization, cloud computing, mobility features or collaboration technologies—must be made with security in mind.

leakage. And what of data efficacy? If you don't house the applications or data on-site—such as in a private cloud—do you trust the inputs? Where is the control for applications if some applications (or some parts of them) reside in a mobile system, in a home-based PC, within the enterprise (data center or regional office), or within cloud-based systems? And aren't there now more potential threats of malware or viruses affecting systems and applications?

Access itself is under threat because of the increased use of data-rich social networks. Some analysts estimate that 30 percent of corporate bandwidth is consumed by social networking traffic. There's just too much unregulated, unstructured data from such sources as Facebook and YouTube moving through business pipes. And both the growth of the mobile Internet and the explosion in content continue unabated. Do enterprises have the right security technologies in place that can scale with or stay ahead of surging network bandwidth needs?

Vulnerability, say IT leaders, is also pres-

ent in the form of compliance. Any data breach where customer data is exposed garners the ire of regulators and the courts. Privacy is paramount.

Today's customer is king, ultimately shaping how data is organized and stored for many companies. Think of online banking consumers: They're inputting highly sensitive information that must be securely protected in ways that comply with a multitude of regulations. Or consider the healthcare industry and how the Health Insurance Portability and Accountability Act (HIPAA) regulates the privacy of patient data. This issue is an increasing concern as healthcare organizations grow more dependent on the portable, digitized medical record. It's a consumer-to-enterprise interaction, and it's an additional locus of vulnerability that organizations must manage.

How can IT executives both leverage the technologies at their disposal and keep their data, applications and devices secure? Do they have the right intelligence about their applications? Do they have the right controls and visibility in place? In the roundtable conversations, CIOs said that they don't have sufficient visibility into their systems, networks, devices, applications and services.

Risk Versus Reward

But these dangers can't—and shouldn't—engender paralysis. It's critical to embrace them, to understand that

planning with risk in mind is the best way to leverage the new technology paradigms.

It has to be this way. Growth can't be unfettered, yet it must be encouraged. Each organization must be security-aware. Each technology plan—whether it includes virtualization, cloud computing, mobility features or collaboration technologies—must be made with security in mind. Mitigating risk should never be an afterthought.

Planning a safe environment means creating a security strategy on four levels: data, applications and systems, devices, and people. It means implementing the right risk-abatement technologies. And it means ensuring that workers and managers (and in many cases, partners and customers) are not only security-aware, but also trained to follow the right policies and procedures in order to secure the business environment.

Risk abatement—and the ensuing the policies regarding access and risk—must be part of a wide-ranging effort that embraces managers and workers, business partners and customers, and regulators and consumers. With all the issues on the plate of senior IT executives, wouldn't it be nice if the security/performance trade-off wasn't one of them? With so much at stake for businesses as the economy is poised to grow again, now, more than ever, is the time to balance risk and reward.



For more information, go to:
www.sonicwall.com

