

As Hyper-Extended Enterprises Grow, So Do Security Risks

As more enterprises embrace new web and communications technologies, they need to shift their security strategies to accommodate extreme levels of data sharing while protecting business assets.

Businesses are rapidly embracing new tools and technologies including cloud computing, social networking, virtualization, and mobile communications, accelerating the breakdown of the traditional boundaries that surround organizations and protect their data assets. The result is the “hyper-extended enterprise.” Although this evolution is helping companies achieve strategic goals such as cutting costs, boosting innovation, and improving internal and external communications, it’s also potentially exposing them to information security risks.

A recent survey by IDG Research Services examines these risks and suggests how companies can assess and address them. Key research findings include the following:

- **Although nearly half of respondents say they have adopted Web 2.0 technologies or plan to do so in the next year, a significant number have no strategies to assess the risks involved, and some have even deployed the technologies without informing corporate IT security.**
- **More than 8 of 10 respondents are concerned that pressure to cut costs and generate revenue has increased their exposure to security risks. More than 7 of 10 say they have experienced a security issue in the last 18 months.**
- **Only 44% have created employee “acceptable use” policies for social networking tools and sites.**
- **The majority of respondents agree that they need to improve their approach to enterprise security strategy to accommodate the realities of the hyper-extended enterprise.**

exchange more information with more constituencies in more ways and in more places than ever before. Hyper-extended enterprises typically use these technologies internally across their global enterprises and externally to integrate customers, partners, suppliers, and other third parties into their operations. Nearly 3 out of 4 respondents believe that their organizations meet this definition or will soon.

However, the survey results suggest the accelerating trend toward hyper-extension is causing many company leaders to act in one of two extremes: either overly eager or overly cautious.

Some companies are so excited about the potential of these new technologies that they are leaping into adoption without doing the due diligence needed to ensure their critical processes and data will be secure. Cloud computing provides a dramatic example. Among all survey respondents, 31% have already moved at least some enterprise-wide or departmental applications to the cloud, and another 16% say they plan to do so in the next year. More than half of this group says they are unsure how they will ensure data integrity and compliance as they use shared infrastructure services. A majority do not clearly understand how potential cloud computing vendors will protect their data or how their enterprise security team will meet compliance obligations once data moves to the cloud. More than 40% say they worry about not being able to trace the geographic location of their data. Most surprisingly, more than a quarter (29%) say business units have used cloud computing services without involving or informing corporate IT.

LEAPING BEFORE THEY LOOK

The “hyper-extended enterprise” is defined as one that uses new web and communications technologies to



The Security Division of EMC



And yet, even though only 17% of this group have actually established a cloud computing security strategy, 70% of them feel “very confident” or “somewhat confident” that they’re ready for widespread adoption of enterprise cloud computing from a security perspective.

This disconnect holds true across the web and communications technologies that define the hyper-extended enterprise: Only 43% of survey respondents say their IT security team works with business in all cases to develop a risk assessment and mediation process, while 35% report gaps, and 16% say security only gets involved after a problem arises. What’s more, some respondents admit their organizations are adopting these technologies without security’s awareness.

On the other hand, other respondents are actively avoiding these technologies, thus passing up opportunities to reduce costs and improve business flexibility, productivity, and ability to innovate.

The sensible way to enable the hyper-extended enterprise without excessive exposure to risk is to aim for the middle ground. This means shifting the focus of the enterprise security strategy to policies and practices that accommodate data sharing while still protecting its confidentiality, integrity, and availability. This new approach must be more proactive and more collaborative, starting with a focus on safeguarding data regardless of where it’s stored or who accesses it.

PROTECT THE DATA, NOT THE CONTAINER

With the proliferation of mobile devices and the growing

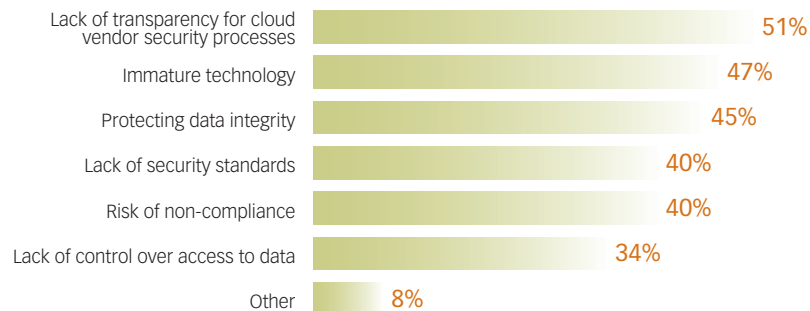
popularity of virtualization, enterprise data is increasingly processed and stored in places and ways that are much more difficult to secure. Survey respondents realize this, and the vast majority (87%) agree that security needs to shift its focus toward protecting data rather than the device or server containing it. However, this requires companies to become more aware of where data might be — a complicated task when 83% of respondents say they’ve increased their use of virtualization technology in the last 12 to 24 months, 65% say they’re seeing increased use of consumer mobile devices such as iPhones, and enterprise security teams support an average of six different types of end user devices.

The issue of protecting data becomes even murkier when companies start to move critical information and processes into the cloud. Survey respondents’ top concerns for cloud computing in particular include these issues:

- **Lack of transparency for vendor security processes (51%)**
- **Immature technology (47%)**
- **Protecting data integrity (45%)**
- **Lack of security standards (40%)**
- **Risk of non-compliance (40%)**

Identifying risk after the fact or only in the event of a security breach is, frankly, a gamble few organizations can afford. Yet organizations are still racing to adopt new technologies without full attention to the security issues they create. Given this disconnect, organizations clearly

Biggest Security Issues Concerning Cloud Computing



Source: IDG Research, April 2009

need to prioritize and increase their ability to assess and mitigate risk before adoption.

“Adopting these technologies is often a cost-based decision, an appetizing way to reduce operational line items,” says Roland Cloutier, vice president and Chief Security Officer at EMC Corp. of Hopkinton, Mass. “Businesses don’t necessarily understand that the data involved may be as valuable as intellectual property as a finished product is.”

Cloutier says businesses must clearly understand the resources, information, and technology they plan to use, share, or extend so they can make an educated decision about the risks they might be taking on. For example, he says, he’s heard the phrase “cloud computing” used to refer to a processing environment, a platform environment, software as a service, and a location outside the enterprise where code is being developed. If companies don’t define precisely what they’re outsourcing or co-sourcing as well as their desired and actual end result, they can’t fairly assess the basic threats and risks involved.

Since the hyper-extended enterprise shares data with vendors and partners, it must also include them in security risk assessment. Although 47% of survey respondents say their vendor and partner agreements require any subcontractors to meet their specific security requirements, 12% say their agreements do not hold subcontractors to their security standards, and 5% say they do not even know whether their vendors and partners use subcontractors — a surprising oversight, especially for companies using outsourcing or offshoring.

ACCEPTABLE USE POLICY DEVELOPMENT

As the traditional boundaries surrounding assets and information dissolve, companies need strong policies governing the acceptable use of technologies that are increasingly under employee control. This is especially important with social networking sites and tools (which easily blur the lines between personal and professional information) and laptops and other mobile devices (which if lost or stolen can expose any critical data they contain).

Respondents to the survey are particularly concerned about social networking web sites. Only 17% say they

allow unhindered access. Nearly a third, or 30%, simply block access completely. However, 44% report they have created acceptable use policies outlining the risks and governing how employees can use these sites. These companies understand that having a presence on social networks can enable employees and customers to communicate at minimal cost, but they also recognize the critical importance of minimizing the risk that users will accidentally or maliciously disclose confidential information.

Acceptable use policies must ensure that employees understand how to use the tools of the hyper-extended enterprise as securely as possible. Policies must also include procedures for monitoring and managing the data employees create and access. Most critically, Cloutier says, they should be consistent across every type of technology and be supported with tools for user awareness.

USER EDUCATION AND TRAINING

User education in security policies goes far beyond telling employees what they may or may not post to a social networking site. It can, and should, also be an opportunity to train them in proven ways to leverage the tools of the hyper-extended enterprise for maximum productivity and strategic benefit.

However, many organizations are clearly failing to do either one. More than 70% of survey respondents report experiencing a security issue in the last 18 months, most commonly malware infection (52%), data breach (22%), or identity theft (22%) — all issues that can be significantly mitigated by educating users about the importance of protecting data and consistently adhering to security policies. These policies are, after all, only useful when users are aware of them, understand why they’re important, and observe best practices.

“The reality is that this is how the world communicates today,” Cloutier notes. “The challenge for businesses is how to embrace Web 2.0 tools and integrate them into the workflow seamlessly and securely.”

A BALANCED APPROACH

One company giving careful thought to these issues is Inteva Products LLC, which manufactures components for car interiors and doors. The international company,

based in Troy, Mich., has already moved its email, payroll and benefits, and ERP systems to the cloud, with a long-range strategy of focusing its IT organization on support rather than technology, says CIO Dennis Hodges.

“We ask our cloud vendors for a lot of documentation about how they secure our data,” Hodges says. “So far, we’ve found that because their business depends on it, they’re much better at security than we could ever be — but that’s because we look for vendors that are recognized for their technology.”

Inteva has acceptable use policies that, while not technology-specific, require employees not to damage the company’s reputation or disclose corporate secrets, as defined in Inteva’s employment code of ethics and employment agreement. It also conducts regular user trainings for its cloud-based applications, although Hodges notes that these applications are almost entirely on the back end. When employees use Microsoft Outlook, he says, they can’t tell that their email is going out to a cloud-based service provider.

Hodges’ advice to other businesses as they develop a new information security model for the hyper-extended enterprise is simple and basic: Perform due diligence first, not later or only when something goes wrong. Choose vendors that have proven track records and references from major customers. Follow the same

security strategy that you would in deploying an internal system. And above all, he says, “If you think you’re giving something up by adopting one of these technologies, don’t do it.”

CONCLUSION

The need to be increasingly flexible and responsive to changing market conditions means the hyper-extended enterprise is here to stay. As enterprises adopt these technologies for competitive advantage, capitalizing on new opportunities while minimizing risk requires them to formulate a new approach to information security.

To do so, Cloutier suggests, consider these three steps:

1. Ask the business side how they expect to use a given technology and why, and then make decisions based on actual business needs rather than potential benefits and presumed threats.
2. Test the technology and make decisions based on its actual performance.
3. Ask vendors for their opinions. As vendors learn to support products beyond the traditional boundaries of the enterprise, they can increasingly share customer stories, both successful and otherwise.

For more information, visit www.RSA.com/innovation

Social Media, Virtualization, Mobile Devices on the Upswing

| How has usage of the following web and communications technologies (for business purposes) changed at your company over the past 12-24 months? | Increase in usage | No change in usage | Decrease in usage |
|--|-------------------|--------------------|-------------------|
| Virtualization technology | 83% | 13% | — |
| Personal consumer mobile devices such as iPhones | 65% | 25% | 3% |
| Social networking platforms/media | 51% | 34% | — |
| Cloud computing | 34% | 44% | — |
| Consumer VoIP services such as Skype | 25% | 48% | 4% |

Source: IDG Research, April 2009