Sign up for other Thought Leaders' e-newsletters/Blog

Thought Leadership Document Outsourcing

John M. Kelly
Executive Vice President,
Major Account Development for ACS,
A Xerox Company
www.xerox.com/thoughtleadership_kelly

Every day, the list of questions about cloud security grows. How do you control access when network end points keep moving further from the core? How do you evaluate the risk of product, business and social information when it changes every minute?

Most of the questions involve fear or doubt. However, after recently speaking with former C.I.A. Director General Michael Hayden, at a Xerox Thought Leadership conference, an intriguing new security question emerged—one with a different perspective:

Is it possible that cloud computing might actually *improve* security?

The answer can be found in a short video of our conversation that you can view here. Or continue reading to find out more.

A Second Chance to Get It Right

General Hayden is one of the country's foremost security experts. A former Air Force general, he served as Director of the National Security Agency and Chief of the Central Security Service before assuming his leadership role at Central Intelligence.

Like many, the General touts the advantages of cloud computing, calling it a "wonderful offering." However, he cautioned that if we are not careful, moving to the cloud would create the same array of problems that emerged when we moved to the Internet.

"We need to make sure as we harvest the cloud's wonderful efficiencies and economies, that we also pay due attention to security," he said. "We didn't do that when we moved to the Net. We're getting a do-over. This is kind of a mulligan for us. So we need to hit this ball really well."

The Origin of Internet Vulnerability

Let's return to the Internet's early days—about half a century ago. During the 1960s, the U.S. Department of Defense developed a network to connect its projects at universities and research labs. Called ARPANET (Advanced Research Projects Agency Network), it was the world's first operational packet-switching network and the foundation for the modern Internet.

ARPANET was designed to quickly and easily move data between a limited number of nodes. Those nodes were well known and trusted. Today, the ARPANET model is still in place, even though the number of nodes has exploded and the "trusted" piece has been shattered to bits. As a result, the Internet is inherently insecure. Contrast that with the cloud, which is evolving with security as a top-of-mind issue.

"The current Net just invites attacks," noted the General. "We stand a good chance that the cloud might actually be a bit more secure."

A Secure Architecture from the Ground Up

Securing the cloud won't be easy. As more people rely on mobile devices, more information is being accessed and generated at the network's edge, rather than within the enterprise. In addition, technologies that lack centralized control or substantial policy management—such as social media—are growing rapidly, jumping from the personal world into the business world.

Because these elements are converging in the cloud, a security breach in one area—e.g., malware on your home PC—can more readily wreak havoc across a wider electronic terrain. When the stakes are so much higher, the controls must be extremely powerful. Simply making the cloud a little bit more secure won't work. Nor will an approach that ignores the need to protect the network's edge *and* core. Clearly, a rethinking of the cloud's security architecture is in order.

Risk Management: A Work in Progress

If we get the security architecture right from the start, the promise of the cloud is more likely to be fulfilled. But much work awaits. Gartner expects that over the next five to 10 years, we'll see maturation in multiple areas of cloud risk management. These include:

- A consensus on the most significant areas of cloud risk, with standards for risk management
- Cloud service certification standards
- Virtual machine governance and control
- Enterprise control over logging and investigation
- Content-based control within SaaS and PaaS offerings
- Multiple forms of proxy security services within the enterprise or in other providers' cloud
- Increasing network access control (NAC) support

With so much yet to come, Gartner concludes that, "For the near future, potential buyers and current users are justified in concerns about placing private or sensitive data within the public cloud, just as they are justified in concerns about any external

service provider."[1] Which brings us to General Hayden's next point: finding the right partner.

Using Security as a Differentiator

The mandate for security can be a valuable tool when evaluating cloud service providers. Rather than choosing companies that simply host data, your organization should seek out service providers with a security mind-set. Find out what they bring to cloud security in terms of original thinking. Ask about the network—is it public, private or a hybrid? Was security an afterthought or a guiding force?

A number of industry questionnaires can help. The Cloud Security Alliance offers a Consensus Assessments Initiative Questionnaire. Shared Assessments, an organization of 60 members (largely financial services firms), has a Standardized Information Gathering questionnaire that includes cloud risks. The U.S. government's Federal Risk and Authorization Management Program (FedRAMP) is expected to release its security risk assessment framework by year-end. And a European initiative, the Common Assurance Maturity Model, is on a similar delivery track.[2]

"You've got to go to the people who provide cloud services and cloud access and use security as a discriminator," suggested General Hayden. "Ease of use, efficiencies, economies of scale—they're all out there. We'll all think they're great. But if we just pause for a moment and say, 'But which of those multiple offerings out there actually is using security to distinguish itself from the other offerings?'—that's a plus."

That plus can easily become a minus if it's ignored. Choose cloud companies that have a security mind-set and your own mind will be more at ease.

In closing, I would like to thank General Hayden for his time and insights. Both were greatly appreciated.

Sincerely,

John M. Kelly

Visit www.xerox.com/thoughtleadership_kelly