Capgemini Press Contact:
Florence Lièvre
Tel.: +33 1 47 54 50 71
Email: florence.lievre@capgemini.com

RSA Press Contact:
Alison Raymond Walsh
Tel.: +1 781-420-6337
Email: Alison.RaymondWalsh@emc.com

Only one in five organizations set up to securely manage user identities

Capgemini and RSA survey finds that most businesses are ill-prepared for the digital services transition, causing a shortfall in identity and access management security

Paris and San Francisco, 29 February 2016 – A survey conducted by Capgemini, one of the world's foremost providers of consulting, technology and outsourcing services, and RSA, The Security Division of EMC (NYSE:EMC), revealed that as organizations seek to capitalize on digital opportunities through rapidly developing and hosting new services online, they frequently under-invest in adequate cybersecurity measures creating significant risks, in particular governing user access.

"Identity Crisis: How to Balance Digital Transformation and User Security?", a survey of more than 800 C-level executives in the US, UK, Germany, France, Benelux and the Nordics[1] revealed that 62 percent believe it is very important or critical for their organizations to enable or extend access for users to digital services securely, yet only 26 percent have the technology in place to do so. However, it is clear from the findings that organizations recognize the need to do more to improve the user experience, with 84 percent acknowledging the need to offer more flexible, adaptive authentication methods and IDs.

Jim Ducharme, Vice President of Identity Products at RSA, said "*As organizations extend to the cloud they must ensure they have solutions in place that address the risk and threats associated with assuring user identities. These solutions must understand who is accessing what; manage that access effectively; and control access across the various cloud services. These elements are absolutely essential to giving the organization the assurance that users are who they say they are in a cloud environment."*

The findings show that companies are moving to bridge the divide and bolster their existing security practices. In the wake of high profile, extremely damaging online breaches, IAM[2] is seeing a noticeable increase in investment. Nearly seven in ten companies (68 percent) report a rise in their IAM budgets, with 28 percent noting a 'strong' increase.

The survey also revealed a shift in the way IAM is being viewed and implemented, prompted by maturing and emerging technologies and anticipated user demand. The results suggest that allowing users to bring their own identity, where visitors use their existing social identities to log in, is viewed as many companies' ultimate goal

[1] Denmark, Sweden, Norway and Finland.
[2] IAM: Identity and Access Management

as long as it can be implemented securely. Interestingly it is apparent that this ambition is being balanced with widespread uncertainty surrounding data privacy, security regulations and transparency regarding where services are hosted. The report highlights:

- Adaptive Authentication[3] is set to define the future of device and service access for users. 84 percent of organizations consider the ability to deploy such authentication and offer access via an increasing number of methods and devices a high or very high priority;
- For most companies (85 percent), it is critical or very critical to onboard new services underpinned by cloud technology – which are only expected to increase – quickly and efficiently, and that these are supported by IAM;
- Organizations from both the United States and Europe are very sensitive to where security services are hosted, with close to 90 percent of respondents preferring or mandating data centers that deliver identity management services be located within their country or region.

"*It is clear that the days of logging into a company's system with a username and password specific to that organization are numbered. Users aspire to log in from anywhere in a variety of ways, including with social media profiles and existing email account*" said Mike Turner, Global Cybersecurity COO at Capgemini Group. "*The ownership of online identities is moving away from the organization to more flexible and secure services maintained by the user, addressing access management needs. While it is extremely positive to see increasing recognition and investment from senior leadership, a considerable gap between the task at hand and the current capabilities of many organizations remains. The extent of this security challenge should not be underestimated.*"

"Identity Crisis: How to Balance Digital Transformation and User Security?" findings are drawn from a survey of 831 C-level decision makers, with a majority of respondents from IT departments (47% IT services and 29% IT security), and other participants from departments such as Sales & Marketing, HR or Finance. Conducted by KuppingerCole on behalf of RSA and Capgemini, those surveyed were based in the US, UK, Germany, France, Benelux and the Nordics[4] represent organizations with more than 500 managed identities, of both employees and consumers. One third of the organizations covered are in the range of 5,000 to 50,000 managed identities, while 40% have more than 50,000 identities under management and 7% are managing more than 1 million users.

For more information on the survey, its findings and Capgemini's Identity as a Service (IDaaS), please visit: www.capgemini.com/identitysurvey

[3] Adaptive Authentication, or risk-based authentication, is a system that determines the necessary level of complexity a login process should hold for a user based on their risk profile, where users deemed 'higher risks' are set an enhanced authentication challenge
[4] Denmark, Sweden, Norway and Finland.

About Capgemini
With more than 180,000 people in over 40 countries, Capgemini is one of the world's foremost providers of consulting, technology and outsourcing services. The Group reported 2015 global revenues of EUR 11.9 billion. Together with its clients, Capgemini creates and delivers business, technology and digital solutions that fit their needs, enabling them to achieve innovation and competitiveness. A deeply multicultural organization, Capgemini has developed its own way of working, the Collaborative Business Experience™, and draws on Rightshore®, its worldwide delivery model.
Learn more about us at www.capgemini.com.

Rightshore® is a trademark belonging to Capgemini