New COBIT 5 Guide Identifies Top Three Cybersecurity Game Changers

ISACA Forms Cybersecurity Task Force Featuring Leading Industry CSOs

Sydney, Australia, (20 June 2013)—Cybercrime is on the rise, but will grow even faster if organisations ignore an emerging group of cybersecurity game changers: always-on connectivity, an increasingly IT-centric society, and a new class system that separates people by technology skills. ISACA's latest guide, *Transforming Cybersecurity Using COBIT 5,* examines the impact of these game changers and how to manage and transform security by using COBIT 5, a business framework for the governance and management of enterprise information and technology. Along with publication of the guide, IT association ISACA also announced today the formation of a global cybersecurity task force.

The three game changers named in the guide provide both motive and opportunity for cybersecurity breaches and criminal activities—especially the advanced persistent threat (APT) —if ignored:

GAME CHANGER		IMPACT
Always-on Connectivity	• Critical data and information are clustered in clouds. • Wi-Fi hotspots are growing. • Work systems are easily accessible at home or on the go.	→ Increases window of opportunity for attack
IT-centric Business and Society	• Online systems are the new critical infrastructures. • Society's reliance on "always-on" creates wider windows of attack time. • There is no paper fallback in emergencies.	→ Increases number of business processes that can be targeted
New Class System by Technology Skills	• Mobile device features remain a mystery to many. • Fewer digital natives have deep IT skills. • New apps and operating systems favor convenience over user control.	→ Increases role of human error in enabling cybercrime

“In just the past three years, the number of threats and vulnerabilities has grown almost exponentially. By using COBIT 5, security professionals have a systematic approach for overcoming some of their biggest internal barriers—especially inadequate budget and lack of senior management support,” said Rolf von Roessing, CISA, CISM, CGEIT, CISSP, FBCI, lead developer of the guide and president of FORFA AG.

This latest addition to ISACA’s cybersecurity series is designed for information security managers, corporate security managers, end users, service providers, IT administrators and IT auditors. It includes guidance on using the COBIT 5 framework to integrate cybersecurity with an overall approach to security governance, risk management and compliance, as well as eight principles for transforming security.

“The enormous opportunities inherent with cloud, mobility, social networking and big data also create significant security risks, and most organisations are ill-prepared to respond effectively. If we want to defend ourselves from sophisticated and targeted cyberattacks, it’s time to shift the industry’s thinking from a focus on compliance and perimeter security to a more proactive posture that is all about protecting the crown jewels,” said Eddie Schwartz, CISA, CISM, chair of ISACA’s Cybersecurity Task Force and chief information security officer (CISO) at RSA, the Security Division of EMC.

A recent ISACA cybersecurity survey of more than 1,500 security professionals worldwide found that 94 percent of respondents believe that the APT represents a credible threat to national security and economic stability. Top risks were seen as loss of enterprise intellectual property (26 percent), loss of customer or employee personally identifiable information (24 percent) and damage to corporate reputation (21 percent).

ISACA Global Cybersecurity Task Force
As part of its ongoing commitment to helping business and IT leaders maximise value and manage risk related to information and technology, ISACA also announced the formation of a cybersecurity task force to drive research, guidance and advocacy. Eight information security professionals from locations around the world were named to the Cybersecurity Task Force:

- Eddie Schwartz, CISO at RSA, the Security Division of EMC (USA) (chair)
- Brent Conran, Chief Security Officer, McAfee (USA)
- Marcus Sachs, Vice President for National Security Policy, Verizon (USA)
- Neil Barlow, Head of Information Security Governance, Risk & Compliance (GRC), Euronext, NYSE (UK)
- Samuel Linares, Director and Founder, Industrial Cybersecurity Center (Spain)
- John Lyons, Chief Executive, International Cyber Security Protection Alliance (UK)
- Manuel Aceves, Director General, Cerberian Consulting (Mexico)
- Derek Grocke, Security & Infrastructure Manager, Internode (Australia)

Commenting on the new Global Cybersecurity Task Force Jo Stewart-Rattray, CISA, CISM, CGEIT, CRISC, FACS CP, International director of ISACA and

director of information security and IT assurance at BRM Holdich, said: “ISACA’s new Global Cybersecurity Task Force is an important milestone and will provide pragmatic guidance for organisations in an emerging area. I am delighted that my colleague Derek Grocke has been appointed to this taskforce as he has significant experience in this field of practice and will bring an Oceania perspective to the group’s offerings. ”

Transforming Cybersecurity Using COBIT 5 is the third installment in a cybersecurity series from ISACA, a global association of 110,000 information security, assurance, risk and governance professionals. The first two installments, *Advanced Persistent Threat Awareness Study Results* and *Responding to Targeted Cyberattacks*, are available at *www.isaca.org/cyber*.

The guide is available at no charge to members of ISACA; non-members can purchase a print or electronic version at *www.isaca.org/cybersecurity-cobit*.

About ISACA
With more than 110,000 constituents in 180 countries, ISACA® (*www.isaca.org*) helps business and IT leaders maximize value and manage risk related to information and technology. Founded in 1969, the nonprofit, independent ISACA is an advocate for professionals involved in information security, assurance, risk management and governance. These professionals rely on ISACA as the trusted source for information and technology knowledge, community, standards and certification. The association, which has 200 chapters worldwide, advances and validates business-critical skills and knowledge through the globally respected Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in Risk and Information Systems Control™ (CRISC™) credentials. ISACA also developed and continually updates COBIT®, a business framework that helps enterprises in all industries and geographies govern and manage their information and technology.

Participate in the ISACA Knowledge Center: *www.isaca.org/knowledge-center*
Follow ISACA on Twitter: *https://twitter.com/ISACANews*
Join ISACA on LinkedIn: ISACA (Official), *http://linkd.in/ISACAOfficial*
Like ISACA on Facebook: *www.facebook.com/ISACAHQ*