White Paper

Securing Enterprise Information with COBIT 5

WP0167 | November 2014

Michael Lane

Mike is a respected technology professional with nearly 20 years experience, having held senior manager positions in Information Technology, Communications and Consulting.

Over his career he has managed a vast number of Telecoms, IT, Business and Consulting projects and programmes, and the associated global cross functional teams, with a strong track record of results. Mike is a specialist in many aspects of information technology, including infrastructure, architecture, systems development, business processes, service management, policies and standards, leadership, governance and management.

In our modern, technology-centric world, information is everywhere, Enterprises and consumers alike demand it, at any time 24x7x365, from anywhere – location or device, and it is expected to be there, when it's needed, without comprise. Information is arguably, one of the most valuable assets in any Enterprise, essential to its functioning, and not surprisingly it is commonly referred to as the lifeblood of an organization. But unlike other more tangible assets, like land and buildings, or motor vehicles, information is not as easily secured.

Information continues to become increasingly pervasive in every aspect of Enterprise life, and with the emergence of concepts like Big Data driving the demand for informational intelligence through the roof, the value of information is growing exponentially. Becoming so intrinsically and extrinsically valuable to the Enterprise, a critical commodity per se, information brings with it a whole new set of risks for its safeguarding by the organization.

On a par with any other valuable Enterprise asset, internal and external threats to information are ever present. From the disgruntled employee user come hacker, to the national cybercrime syndicate, information can very quickly transition to becoming a liability to any organization. The information challenge for the Enterprise in the 21st century is being able to strike a balance between securing its vast volumes of information, making it available to all relevant stakeholders, when, where and how they need it, and complying with relevant regulations and legislation.

It was this common challenge faced by Enterprises around the world, along with a number of major drivers that lead ISACA to develop COBIT 5 for Information Security, and help organizations in their never ending battle to keep information safe!

COBIT 5: Information Security and Value for your Enterprise

From COBIT 5 we know that delivering enterprise stakeholder value requires good governance and management of information and technology (IT) assets – not least of all, Information. Furthermore, increasing external legal and regulatory requirements related to the Enterprise's use of information and technology, threaten this value, if breached. It goes to say then that information security should be of paramount importance to the Enterprise, and if information is not adequately controlled and secured, it poses a material risk to the organization. Yet for many Enterprises out there, there is a perception of information chaos rather than a clear focus on information security, and it's easy to see why…

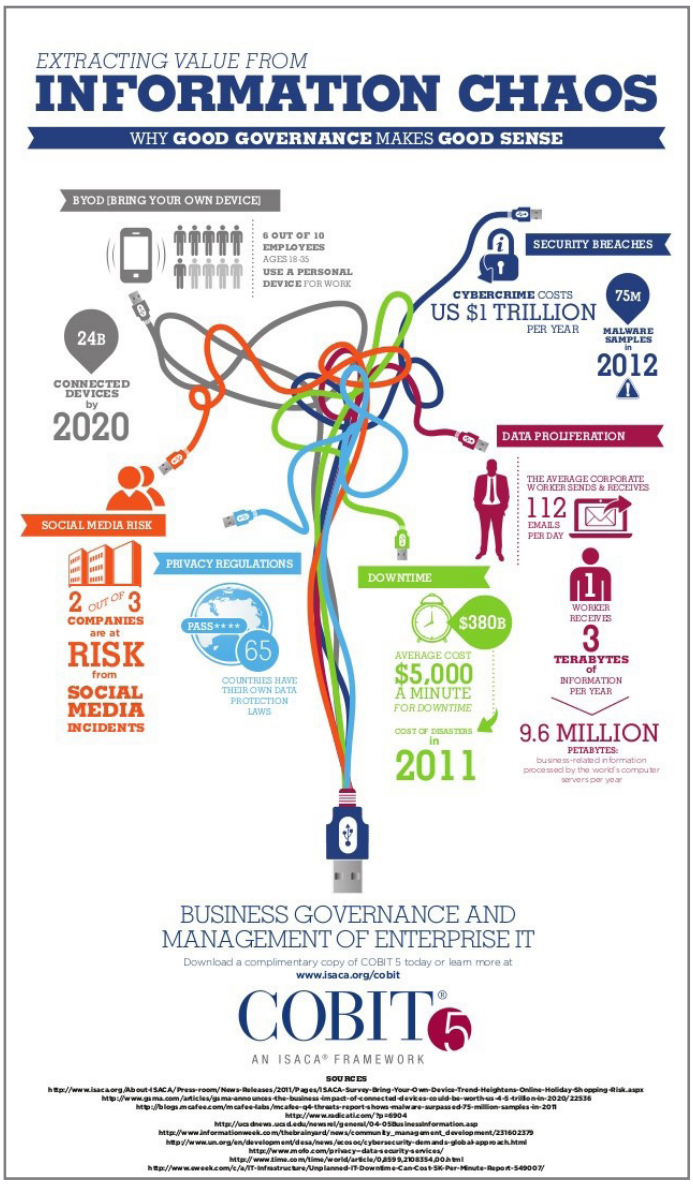

Figure 1 (COBIT® 5, © 2012 ISACA® All rights reserved)

Cybercrime costs the US 1$ trillion per year; 2 out of 3 companies at risk from social media incidents; 24 Billion connected devices expected to be active by 2020; 1 worker receives 3 terabytes of information per year… with facts like these, it's no surprise that many Enterprises see it as information chaos.

Extracting value from this information (chaos) requires more than just good governance and management of Enterprise IT, it requires effective information security to be in place within the Enterprise. And if the past is anything to go by, the sooner the better. Gartner predicts that about one third of Fortune 100 Organizations will face an Information Crisis by 2017 due to their inability to effectively value, govern and trust their enterprise information. This, is according to Gartner, against a backdrop of rising big data, social networking and mobile interactions, and an accelerating increase in the amount of structured and unstructured information enabled and empowered by a new breed of technologies, spearheaded by the cloud. Enterprise Information Management is firmly in the spotlight, and never before has the need to secure information in the organization been more important.

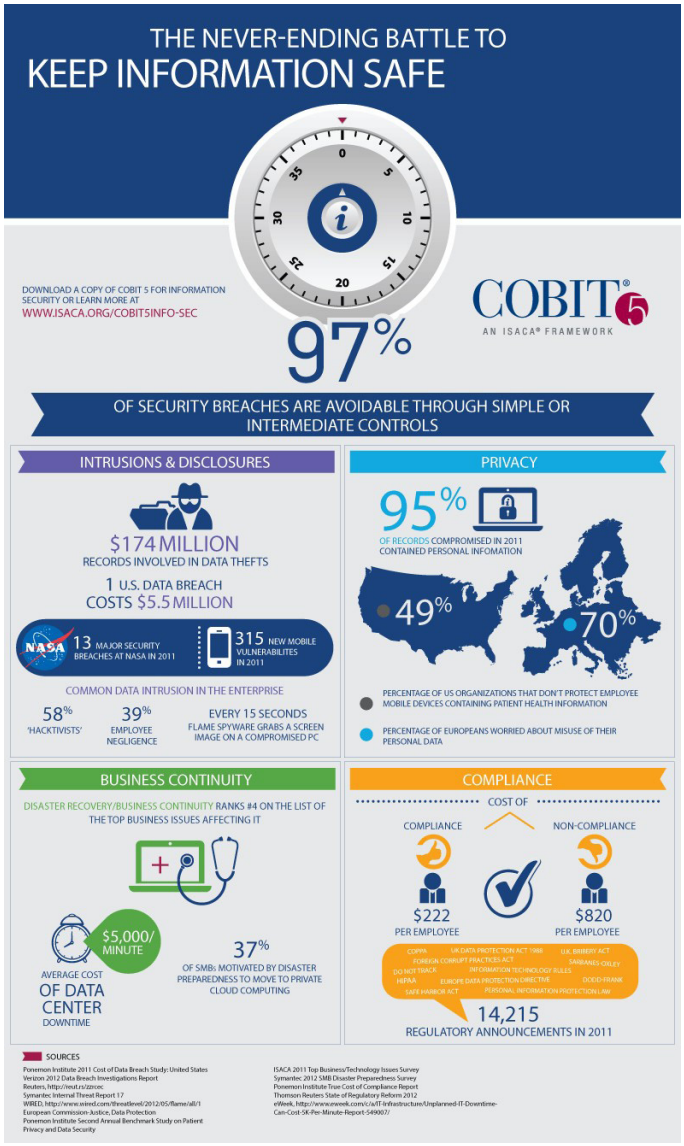

Figure 2 (COBIT® 5, © 2012 ISACA® All rights reserved)

In the Never Ending Battle to Keep Information Safe laminate, published by ISACA, the extent of information security breaches was highlighted:

- **Intrusions and Detections:** $174million records involved in data theft
- **Privacy:** 95% of records compromised contained personal information
- **Business Continuity:** the average cost of data center downtime $5000/minute
- **Compliance:** 14215 regulatory announcements, and a cost of non-compliance per employee of $820

These facts tell us that there is no denying the critical information security challenge faced by every Enterprise around the globe, but perhaps the most important fact of all is this one - 97% of information security breaches are avoidable through simple or intermediate controls… The only question then, is "How?" Fortunately, there is COBIT 5 and COBIT 5 for Information Security… but what is it exactly, why should you choose it and how will it help?

ISACA defines COBIT 5 as:

> *"A Business Framework for the Governance and Management of Enterprise IT." (ISACA 2012)*

And COBIT 5 for Information Security as the means which:

> *"Ensures that within the enterprise, information is protected against disclosure to unauthorized users (confidentiality), improper modification (integrity) and non-access when required (availability)." (ISACA 2012)*

Within the context of COBIT 5 for Information Security, the following supporting definitions apply:

- **Confidentiality** means preserving authorized restrictions on access and disclosure, including means for protecting privacy and proprietary information.
- **Integrity** means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
- **Availability** means ensuring timely and reliable access to and use of information.

The so called CIA triad or concept – Confidentiality Integrity Availability (CIA) – is universal, and not one founded or in sole use by COBIT 5. COBIT 5 for Information Security simply expands on these definitions, describing how information security can be applied within the Enterprise, taking into account the five principles at the heart of COBIT 5:

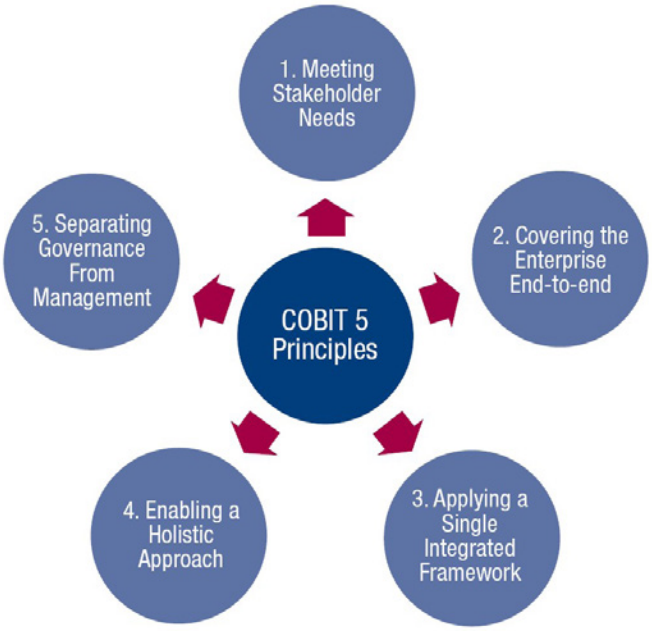

Figure 3 (COBIT® 5, © 2012 ISACA® All rights reserved)

But the generic challenge of keeping information safe, aside, what were these other major drivers for the development of COBIT 5 for Information Security? In summary, the drivers were the following:

1. The need to describe information security in an enterprise context
    a. End-to-end business and IT functional responsibilities of information security
    b. All aspects that lead to effective governance and management of information security
    c. The relationship and link of information security to enterprise objectives
2. The need for enterprises to:
    a. Keep risk at acceptable levels (control risk)
    b. Maintain availability to systems and service (control availability)
    c. Comply with relevant laws and regulation (control compliance)
    d. Contain IT services and technology protection costs (control costs)
3. The need to connect to and align with other major standards and frameworks like ISO 27000
4. The need to link together all major ISACA research, frameworks and guidance

Essentially, COBIT 5 for Information Security was developed to provide guidance to help IT and security professionals understand, utilize, implement and direct important information security-related activities, and make more informed decisions while maintaining awareness about emerging technologies and the accompanying threats. Put another way, COBIT 5 for Information Security can help your Enterprise prevent security breaches before they happen!

A major strength of COBIT 5 for Information Security is that it is not an isolated, standalone information security framework. On the contrary, it's a contemporary evolution of the COBIT 5 framework, offering an extended view of COBIT 5, examining and explaining COBIT 5 'components' from an information security perspective. COBIT 5 for Information Security provides useful, practical guidance for information security professionals, interested parties and stakeholders throughout and outside of the Enterprise. Collectively, COBIT 5 and COBIT 5 for Information Security reflect thought leadership in enterprise governance and management techniques, with globally accepted principles, practices, analytical tools and models to help increase the trust in, and value from, information systems for the Enterprise.

It's not to say that COBIT 5, in its own right, doesn't include any semblance of security at all. Within the COBIT 5 Management area (domain), processes for Manage security, Manage continuity and Manage security services exist, but these provide only foundational and basic guidance on how to define, operate and monitor a system for general security management. However, in COBIT 5 for Information Security the assertion is that information security is pervasive throughout the entire enterprise, with information security aspects relevant in every process and activity performed. Therefore, COBIT 5 for Information Security is truly the next generation of ISACA's guidance on the enterprise governance and management of information security.

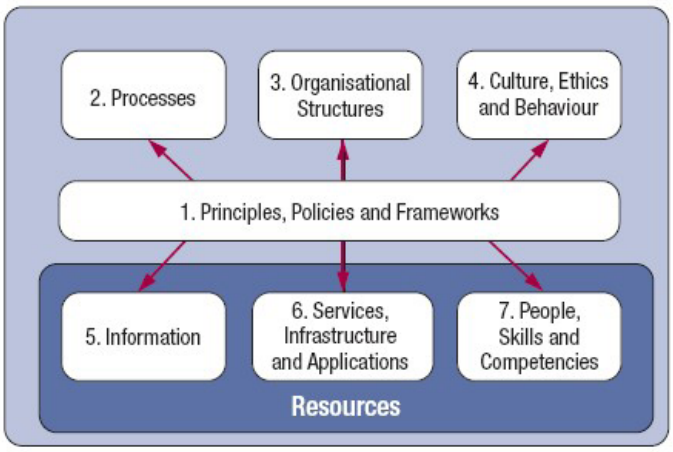

Figure 4 (COBIT® 5, © 2012 ISACA® All rights reserved)

COBIT 5 for Information Security provides detailed and specific guidance related to each of the seven COBIT 5 enablers:

1. Information security policies, principles, and frameworks

Example:

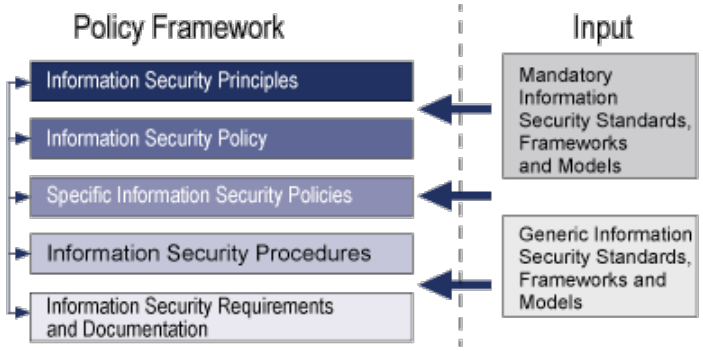

Figure 5 (COBIT® 5 for Information Security, © 2012 ISACA® All rights reserved)

2. Processes, including information security-specific details and activities
3. Information security-specific organisational structures
4. In terms of culture, ethics and behaviour, factors determining the success of information security governance and management
5. Information security-specific information types
6. Service capabilities required to provide information security functions to an enterprise
7. People, skills and competencies specific for information

COBIT 5 for Information Security supports Enterprises in their primary governance objective of value creation. This focus on stakeholder value, and the end-to-end view of the business and IT, ensures that information security is the remit and responsibility of all Enterprise stakeholders – internal and external, inclusive of the CEO and the Board of Directors, and not only the information security officers, managers and professionals within the organization.

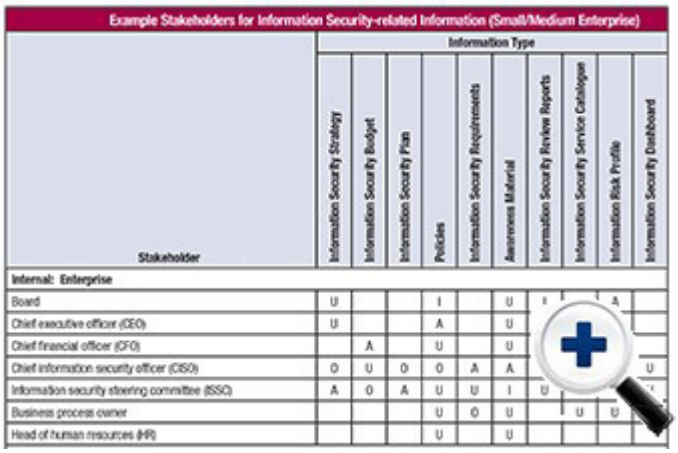

Figure 6 (COBIT® 5 for Information Security, © 2012 ISACA® All rights reserved)

By implementing and using COBIT 5 for Information Security in the Enterprise, organizations can realize a number of significant benefits including:

- ✓ Prevented breaches in information security
- ✓ Real Value extracted from Information Chaos
- ✓ An Information Security framework integrated with other Major frameworks and standards
- ✓ Reduced complexity and increased cost-effectiveness due to improved and easier integration of information security standards
- ✓ Increased user satisfaction with information security arrangements and outcomes
- ✓ Improved integration of information security in the enterprise
- ✓ Informed risk decisions and risk awareness
- ✓ Improved prevention, detection and recovery
- ✓ Reduced impact of security incidents
- ✓ Enhanced support for innovation and competitiveness
- ✓ Improved management of costs related to the information security function
- ✓ Better understanding of information security
- ✓ Addressing of all Stakeholders Needs and Maximized Value of Corporate Information
- ✓ Protection and Driving of Enterprise Value

Conclusions

Whatever the industry or organization type, local or global, Enterprises around the globe are faced with a common challenge in this new age of information chaos – and that is information security. In our time we have seen the unprecedented pace at which information and technology is proliferating and pervading our working and personal space. So too, in a world of continuous change, exists the constant and dynamic threat to the very information on which our lives have become so dependent. And the regulation revolution, driven by the evolving prescripts of corporate governance and legislation, ensures that it is not only in the back-offices of buildings that information is talked about, but instead that in every boardroom the critical need for information security in the Enterprise has a voice.

From the second a new piece of information is planned, through the entire information lifecycle until it is ultimately archived or destroyed, Enterprises bear the responsibility for its confidentiality, integrity and availability.

In COBIT 5 for Information Security, Enterprises find comprehensive guidance and an end-to-end security view of COBIT 5, specifically targeted at helping them manage risk and ensure compliance, continuity, availability, security and privacy in terms of information.

In collaboration with COBIT 5, the business framework for the Governance and Management of Enterprise IT, COBIT 5 for Information Security supports IT assets and Enterprise goals to help ensure that information systems comply with necessary risk controls. What is particularly important for Enterprises to bear in mind when considering their approach to information security is that according to ISACA, 97% of all information security breaches are preventable through controls implemented within the organization.

Information security is fundamental to the day-to-day operation of any modern Enterprise, and in fact their sustainability. Organizations are increasingly unwilling to accept the risk of information security breaches, and would rather invest in preventable measures and controls, to avoid or at worst mitigate potentially devastating financial consequences. More and more Enterprises today are seeking to reduce exposure to information security risk, be it reputational, legal or financial, and focusing on securing their valuable information through COBIT 5 and COBIT 5 for Information Security.

COBIT 5 for Information Security is an extension of COBIT 5, and together they offer an integrated solution for any and every Enterprise seeking to derive maximum value from their investment in IT and the use of information by the organization, whilst minimizing risk and costs. Make the smart choice, and start securing your information today, with COBIT 5 for Information Security, and COBIT 5!

From ISACA:

> *COBIT 5 for Information Security provides the most up-to-date view on information security governance and management through alignment with COBIT 5, International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 38500 and other IT governance initiatives. During the development of COBIT 5 for Information Security, the most important guidance and standards were analysed. COBIT 5 for Information Security aligns with other major frameworks, standards and models in the marketplace, such as the ISO/IEC 27000 series, the Information Security Forum (ISF) Standard of Good Practice, and BMIS. Additionally, ISACA's information security governance offerings, Information Security Governance: Guidance for Information Security Managers and Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition were analysed during the development of COBIT 5 for Information Security.*

Additional Reading:

Securing Mobile Devices Using COBIT 5 for Information Security

Transforming Cybersecurity: Using COBIT 5

Securing Sensitive Personal Data or Information Under India's IT Act Using COBIT 5

References

ISACA (2012). A Business Framework for the Governance and Management of Enterprise IT [PDF] Available from: www.isaca.org/COBIT/Documents/COBIT5-Ver2-FrameWork.pdf *[Accessed September 2014]*

ISACA (2012). COBIT 5 Introduction [PDF] Available from: www.isaca.org/COBIT/Documents/An-Introduction.pdf *[Accessed September 2014]*

ISACA (2012) COBIT 5 for Information Security Introduction [PDF] Available from: www.isaca.org/COBIT/Documents/COBIT-5-for-Information-Security-Introduction.pdf *[Accessed September 2014]*

ISACA (2012) COBIT 5 for Information Security [PPT] Available from: www.isaca.org/COBIT/Pages/Information-Security-Product-Page.aspx *[Accessed September 2014]*

www.isaca.org/cobit/pages/info-sec.aspx

www.techrepublic.com/blog/it-security/cobit-5-for-information-security-the-underlying-principles/

www.slideshare.net/elkanouni/cobit-5-for-information-security

Orbus Software
3rd Floor
111 Buckingham Palace Road
London
SW1W 0SR
United Kingdom

+44 (0) 870 991 1851
enquiries@orbussoftware.com
www.orbussoftware.com

orbus software