The Infonomics *Letter*
Plain Language about Leadership and (Corporate) Governance of Information Technology
Edición Junio 2011

Una dosis de Realidad

Hola, y bienvenidos a The Infonomics Letter de junio de 2011. Es el fin del ejercicio en Australia, y muchos de nosotros estamos muy enfocados en asegurar que nuestros asuntos financieros y las obligaciones fiscales estén en orden.

Pero mientras el cumplimiento financiero en efecto, se presenta como una dosis de realidad, está lejos de ser la única dosis de la realidad que encontramos en esta era de la información. Para los dueños de algunos de los 4.800 sitios web, la dosis de la realidad entregada durante el mes pasado no puede ser más enfática.

Después de numerosos ejemplos de violaciones de seguridad en los últimos meses, el riesgo de incumplimiento de seguridad de información y el riesgo de la computación en nube se cruzaron cuando los piratas informáticos destruyeron cuatro servidores y todas las copias de seguridad asociados a una empresa australiana conocida como Distribute.IT. En el "Parpadeo de un Ojo" se examinan las cuestiones de gobernabilidad que surgen de este evento.

El caso Distribute.IT es un claro ejemplo de los riesgos de la computación en nube haciéndose realidad. Hemos discutido los riesgos hace dos meses en una historia que se llama "Rocas Escondidas en las Nubes". La historia fue citada en la edición de junio de 2011 de Company Director, como parte del artículo de Stuart Domini "Ver a través de las nubes". Unas palabras más sobre las nubes, añade un poco más de perspectiva.

Una forma diferente de violación de seguridad de la información se reportó en junio por el Instituto Australiano de Directores de Compañía, cuando fue robada una computadora portátil. Los comentarios en la prensa y en foros en línea, plantean algunas cuestiones interesantes. Se discuten algunas de estas en Una vergüenza de pruebas.

Varios gobiernos estatales de Australia han tratado de establecer un enfoque de servicios compartidos de TI. La mayoría han fracasado, adicionando ahora al sur de Australia a la lista, mientras que el nuevo gobierno de Nueva Gales del Sur ha anunciado que va a emprender su propio viaje de servicios compartidos. Se discute el concepto en Observación de Albert Einstein.

ISACA ha publicado un borrador de su próximo marco COBIT 5. Esta es una obra importante, que ha sido influenciada por la norma internacional para la gobernanza de TI. Algunos datos preliminares se analizan en Exposición de COBIT 5.

Mayo y junio vieron mi viaje a Argentina, El Salvador y Malasia para explicar el enfoque del gobierno de TI de la ISO 38500. Afortunadamente, el viaje fue hecho antes que las cenizas del volcán chileno complicaran las cosas. En Historia de Cinco Naciones, se compara la capacidad de gobierno en los cinco países que he visitado hasta ahora en el 2011.

Mark Toomey 30 de junio 2011

Parpadeo de un Ojo

En algún momento a mediados de junio, una o más personas malintencionadas violaron los controles de seguridad de un alojamiento web profesional de Australia conocido como Distribute.IT, accediendo a varios servidores que se utilizan para ejecutar sitios web propiedad de los clientes de Distribute.IT. Estas personas malintencionadas pusieron en práctica programas que efectivamente destruyeron las instalaciones de almacenamiento de datos de los cuatro servidores. Para los no iniciados, esto puede ser comparado con la explosión de una bomba en una biblioteca, la destrucción de todos los catálogos de bibliotecas y trituración de la mayoría de los libros. Dado que las computadoras hacen su trabajo muy rápido, no debe ser ninguna sorpresa que el daño fue causado en un lapso muy corto de tiempo.

Lo que es significativo e inusual en este caso es que los hackers también destruyeron todas las copias de seguridad de los datos almacenados en los servidores. Para ello, los piratas tenían que tener acceso a los dispositivos de almacenamiento separados en los que los datos de los clientes deberían haber sido copiados. Como resultado, todos los datos almacenados en cuatro máquinas probablemente se han perdido permanentemente. Según informes de prensa, esto se ha traducido en la desaparición de 4.800 sitios web.

Algunos de los sitios web pertenecían a empresas. Casi con toda seguridad, algunos eran interactivos, diseñados por lo menos para la captura de información y acerca de las personas que los utilizan. Algunos pueden haber sido sitios de comercio electrónico, procesamiento de transacciones y toma de pedidos. Es muy probable que todos los datos recogidos por estos sitios web se hayan perdido.

Hace apenas dos meses, en la edición de abril 2011, hablamos de los riesgos de la computación en la nube en el artículo "Rocas ocultas en las nubes". Empresas como Distribute.IT son ejemplos de proveedores de la nube - proporcionan la infraestructura para su uso compartido por otras entidades sobre una base comercial. Es probable que muchas de las empresas que utilizan las instalaciones Distribute.IT hubieran considerado a la empresa como una extensión de los brazos del departamento de TI que debe "cuidarnos de todos los problemas de TI". Muchos no han prestado atención a la percepción de "cuestiones técnicas" como la seguridad de los datos.

Ahora que han pagado el precio por no entender que los usuarios de tecnología de la información tienen responsabilidades significativas que están separadas

de las de los proveedores de TI. La aparición de la computación en la nube, en sus diversas formas, ha traído este tema a la superficie.

La posibilidad de un recurso legal sería poco consuelo para aquellos negocios que han sido severamente dañados por la violación de la seguridad de Distribute.IT. A lo sumo, obtener una indemnización será un asunto tedioso. Con toda probabilidad, la compañía no tiene ningún activo realizable significativo, en parte porque el costo de establecer un servicio de alojamiento no es tan grande, con la probabilidad de que la mayoría de los equipos que han sido objeto de financiaciones y en parte debido a la pérdida de clientes y la pérdida de reputación, ha vuelto muy rápidamente el negocio inviable. De hecho, una transacción comercial ya ha sido completada con otro proveedor de hosting para hacerse cargo de los activos de Distribute.IT, dejando la cáscara en el cuidado de sus propietarios y directores para hacer frente a las consecuencias del evento de hacking.

Como con la mayoría de los casos de pérdida o daño, es muy aplicable el viejo proverbio "más vale prevenir que curar". Los que utilizan el servicio Distribute.IT deberían haber tomado medidas para asegurar que su negocio estaba debidamente protegido contra las cosas que podrían haber sido razonablemente identificadas como riesgo. Utilizaremos los seis principios de la norma ISO 38500 como marco para la discusión.

Responsabilidad: ¿Quién fue responsable de los acuerdos comerciales que han existido entre Distribute.IT y sus clientes? Claramente, la empresa proporcionó la infraestructura y debe tener siempre una capa de seguridad adecuadas en torno a esa infraestructura. Tal vez fue requerido como parte de su servicio hacer copias de seguridad de datos de los clientes - pero ¿cuáles eran sus obligaciones a este respecto? Fue también responsable de asegurar que las copias de seguridad se mantienen en los medios de comunicación que son físicamente removidos de la red y con imposibilidad de acceso.

Independientemente de que la responsabilidad fue asignada a Distribute.IT, ¿qué responsabilidad tenían los propietarios de las empresas afectadas para salvaguardar sus datos, y en su caso, los datos de otras personas que estaban usando sus sitios web? ¿No hubiera sido prudente que asuman al menos la responsabilidad de asegurar que los datos estén a salvo de pérdida, daño y exposición? Las mejores prácticas contemporáneas de gestión de la información están fuertemente orientadas a la responsabilidad de los datos de estar primero en los hombros de quienes son sus propietarios y custodios, con una responsabilidad menor que se imponen a aquellos que operan la infraestructura.

Estrategia: De acuerdo con la norma ISO 38500, los planes de TI deben responder a las necesidades del negocio, mientras que los planes para el negocio deben tener en cuenta las capacidades actuales y futuras de TI. En un "contexto de suministro de largo alcance", de los planes de Distribute.IT la tecnología debe haber reunido las necesidades razonables de sus clientes, y debería haber incluido un método eficaz y seguro para las copias de seguridad. Sin embargo, las empresas que utilizan el servicio Distribute.IT también deberían haber sido conscientes de que la mayoría de las formas de computación en la nube son inmaduras, que carecen de normas, disciplinas y controles clave. Deberían haber previsto la posibilidad de que Distribute.IT puede fallar, dejándolos sin servicio de infraestructura y falta de acceso a sus datos.

Adquisición: La decisión de utilizar un proveedor externo para alojar un sitio web es una de las adquisiciones, y tiene la expectativa de que el comprador va a tomar la decisión "por razones válidas, sobre la base de un análisis adecuado y permanente, con la decisión clara y transparente, y con un equilibrio adecuado entre los beneficios, oportunidades, costos y riesgos, tanto a corto como a largo plazo (ISO 38500)". Sin duda, la elección de un proveedor externo es una opción totalmente legítima, en muchos casos hoy en día - siempre y cuando el comprador entiende que el equilibrio entre los beneficios, oportunidades, costos y riesgos será completamente diferente a un acuerdo de suministro interno. La pregunta crucial que surge del caso Distribute.IT es: "¿la mayor flexibilidad y comodidad, combinada con la reducción de costos, compensa el riesgo de un menor control y el riesgo de prácticas inadecuadas por parte del proveedor"?

¿Cuántas organizaciones eligen ciegamente un proveedor externo exclusivamente sobre la base del precio, sin tener en cuenta las demás cuestiones destacadas por el Principio de Adquisición ISO 38500?

Desempeño: ¿Cómo puede un comprador de un producto comercial asegurarse de que funcione bien, siempre que sea necesario? En un contexto de comercio minorista, contamos con amplios marcos legales y regulatorios que aseguran la calidad de los productos y servicios. No podemos comprar coches que no cumplan con las reglas estrictas de diseño, porque a los fabricantes no se les permite vender. Servicios financieros, servicios de telefonía y electricidad, los servicios de salud y muchos más están estrictamente controlados. Muchos servicios modernos sólo pueden ser prestados por personas debidamente capacitadas y con licencia, y muchas ocupaciones profesionales obligarán a ser miembro permanente de una entidad correspondiente.

Cuando hay una ausencia de control jurídico, normativo y profesional, los compradores de productos y servicios toman el riesgo de que el desempeño no pueda medir la altura de las expectativas razonables, y debe manejar el riesgo.

Hasta hace relativamente poco, la mayoría de los usuarios de TI gestionaban el riesgo controlando directamente la infraestructura y el medio

ambiente. Ponen sistemas de gestión con personal especializado, procesos, herramientas, estructura y normas a través del cual deriva la satisfacción razonable de que su TI se realiza según las necesidades. Ahora bien, parte del modelo de negocio de computación en la nube parece ser la prevención de estos gastos. El problema es que la eliminación de la necesidad que el comprador implemente estos sistemas de gestión no es necesariamente acompañada de una obligación por parte del proveedor de la implementación de sistemas de gestión correspondientes. Como hemos visto en el caso de los clientes de Distribute.IT, la ausencia de sistemas de gestión adecuados en ambos lados y los resultados de proveedores con consecuencias trágicas.

Hay un imperativo claro. Para que la computación en la nube pueda alcanzar la madurez, es necesario que se definan un marco adecuado de controles, cualificaciones y garantía independiente que le da a los compradores la garantía de los servicios razonables en la calidad, fiabilidad y rendimiento del producto que han comprado.

Conformidad: Normas claras, sin ambigüedades son una parte esencial de la vida cotidiana, como son los medios de educar a la gente sobre las reglas, y garantizar la conformidad con las reglas. Por supuesto, también es importante que las normas deben ser necesarias y apropiadas, y que las sanciones por la no conformidad deben ser apropiadas.

Como la infraestructura de TI acerca del estado de los productos básicos en todas partes, no tendrán que ser las reglas que se aplican a ese producto. Tales reglas y mecanismos de cumplimiento será una parte integral del régimen a través del cual los compradores de servicios de TI pueden estar seguros de calidad y rendimiento.

Muchas de las reglas de TI ya existentes, a pesar de que la falta de un régimen eficaz en la que la conformidad puede ser razonablemente asegurada. En muchos casos, sin embargo, las reglas no existen como un mandato formal y universal. Sino que existen como las políticas y controles internos de las organizaciones individuales, respaldados por un amplio cuerpo de conocimientos formales e informales. Uno de los temas para los cuales muchas organizaciones con un gran entorno de TI tienen reglas es la protección y conservación de los datos. Las reglas para la retención de almacenamiento y seguridad de los datos son, en muchos casos respaldados por obligaciones legales, sino que también son a menudo dejadas enteramente al departamento de TI, ya que de almacenamiento y seguridad se percibe como "trabajos técnicos".

Hasta que no haya un régimen adecuado de regulación y supervisión de la computación en nube, por lo menos a la par con la electricidad y las telecomunicaciones, y de preferencia con los controles que se aplican a la banca y las finanzas (la información debe ser considerada como y, a veces es dinero), queda en la necesidad de los compradores de servicios verificar que las capacidades, los controles y garantías que requieren están escritos en los contratos exigibles con derecho de verificación proactiva así como los recursos sustanciales en el caso de no conformidad. Si esto no es posible, los compradores tendrán que asegurarse de poner en marcha sus propios arreglos para pagar la protección que necesitan.

Comportamiento Humano: Hay varios aspectos del comportamiento humano que han contribuido a la pérdida experimentada a través de la piratería en Distribute.IT. Los compradores del servicio Distribute.IT fueron sin duda demasiado confiados y complacientes – en no saber cuánto riesgo se adjuntó a su compra, o simplemente esperar que el proveedor gestione por completo este riesgo. Los operadores del negocio Distribute.IT pueden haber carecido de interés y motivación para ofrecer una seguridad eficaz, y puede que no han pensado en el posible riesgo de dejar a los dispositivos de respaldo permanentemente conectados a la red. Pueden haber tenido expectativas irrazonables de sus habilidades y la comprensión de los clientes. Es posible que hayan sido reacios a invertir en lo que pudo haber sido un negocio marginal, o que pueden haber sido reacios a gastar en la esperanza de hacer una matanza en un mercado emergente. Que pudo haber tenido fe suprema en sus propias habilidades, incapaz de reconocer la posibilidad de que sus adversarios ocultos tienen más habilidades.

Pero quizás el mayor problema de conducta humana que debe adjuntar a este incidente es el relacionado con la forma en que se trata el acto criminal que se ha perpetrado. Este incidente nos recuerda una vez más que no todas las personas están comprometidas con el bienestar de los demás. Hay muchos que tienen la experiencia técnica para entrar en las redes de computadoras y dañarlas, y lamentablemente, muchos de ellos carecen de la integridad moral que los dirige para usar sus talentos de una manera perjudicial.

Cuando las personas actúan con mala intención y destruyen, dañan o impiden el acceso o de otra forma inapropiada frente a una propiedad valiosa, nuestro ordenamiento jurídico ofrece para aquellas personas que comparezcan ante la justicia, enfrentar las consecuencias de sus crímenes. Sin embargo, la era de la información trae dos problemas de la conducta humana que tenemos que resolver cuando nos enfrentamos a la creciente prevalencia de los crímenes contra la información. El primero es el problema de la presencia. El segundo es el problema del valor.

El problema de la presencia se debe a que, a diferencia de la mayoría de los casos de daño criminal a una persona o propiedad en que el autor tiene que estar físicamente presente por el delito que se

produzca y no es, pues, la claridad de la jurisdicción, en un crimen contra la información, el autor sólo necesita comunicaciones de red y puede estar físicamente muy lejos - fuera del alcance físico y legal. Es necesario que haya un esfuerzo internacional concertado para desarrollar un marco en el que los autores de delitos contra la información pueden ser llevados ante la justicia, como sería el caso de los crímenes contra personas y propiedades físicas.

El problema de valor se enfoca si tenemos en cuenta la disparidad de consecuencias dictadas por algunos tribunales por crímenes contra la información en comparación con las aplicadas a delitos contra la propiedad. Parece que hay una tendencia de las personas que aprendieron en los tribunales a considerar un delito que daña la información como de menor impacto y las consecuencias de un crimen que podría causar daños. Necesitamos, con gran urgencia, desarrollar un nuevo paradigma en el que los fiscales y los jueces entiendan por completo el impacto financiero que lleva un delito contra la información. [top]

Unas palabras más sobre las nubes

La computación en la nube es un hecho de la vida, y probablemente no va a desaparecer. El término está tan profundamente arraigado que puede llegar a ser una de las pocas frases de moda de la industria de TI que no se marchita. Sin embargo, la computación en la nube es todavía muy nueva, y tenemos mucho que aprender, no sólo por la nueva tecnología (en realidad, la mayor parte de la tecnología de la computación en la nube ha existido por un tiempo), debido a los cambios radicales que implica en la propiedad y el régimen de control. De lo expuesto anteriormente, hay una necesidad de un desarrollo considerable en la regulación y la supervisión antes de que podamos estar realmente cómodos en que la computación en la nube es segura.

Domini Stuart escribe para Company Director, la revista oficial del Instituto Australiano de Directores de Compañía. Ella ha hecho varios artículos útiles sobre los aspectos de la tecnología de la información, y ha sido un placer para mí hacer la introducción a algunos de esos artículos. Su artículo "Ver a través de las nubes" es un ejemplo de ello, donde se teje una discusión muy útil a través de las aportaciones de varios expertos comentaristas, consultores y proveedores.

Sin embargo, hay un par de puntos en el artículo que realmente justifican un debate.

Según el artículo, Aidan Tudehope, co-fundador y director de Macquarie Telecom, describe la nube como una manera de comprar computación y almacenamiento de la misma manera como compra energía - diciendo que "Se paga por lo que se usa como usted lo usa".

El artículo reconoce que, a diferencia de la energía que ingresa, la nube es acerca de datos saliendo y los riesgos asociados son mucho más variados y complejos. Este riesgo se presenta con énfasis en el caso de Distribute.IT.

La analogía con la electricidad puede ser mejorada si nos fijamos en la imagen completa. El sector eléctrico está muy regulado, con énfasis en la continuidad y sostenibilidad de la oferta. Sin embargo, hay poca regulación en la computación en nube e incluso las normas sólo ahora están comenzando a emerger. Incluso con la regulación, las organizaciones que dependen fundamentalmente de la energía eléctrica suelen poner respaldos locales al suministro de energía. ¿Qué se hace cuando los datos están "allá afuera en la nube" y el acceso ha sido cortado?

El artículo también cita a Stuart Bruce McCabe, director de innovación en el grupo de TI de KPMG Consulting, que dice que las pequeñas empresas están aceptando mayores interrupciones de servicio, se comportan como los consumidores.

Eso puede ser cierto. Sin embargo, la pequeña empresa no tiene por qué ser impotente desde el principio, y no debe ser impotente cuando los incidentes aislados se conviertan en errores de rutina. Como con cualquier otro tipo de adquisición, las pequeñas empresas deben tener cuidado en la selección inicial del proveedor de servicios, teniendo en cuenta que el apalancamiento disminuye en gran medida una vez que el servicio es cargado y ejecutado, y que el dolor de la reubicación puede ser mayor que el dolor de soportar un proveedor de servicios fiables. Y a pesar de la atracción en la oferta, la pequeña empresa debe mantener el control lo suficientemente que se puede, ya sea por elección o por fuerza mayor, rápida y eficaz trasladarse a un proveedor alternativo. Esto significa, como mínimo, que debe haber un entendimiento claro de los datos manejados por el proveedor de la nube, y una copia razonablemente actual y útil de los datos que sea accesible, independientemente del estado del proveedor.

Hay una gran tentación para el tratamiento de la computación en nube como un gran salvador que elimina el costo y el dolor de poseer y operar su propia información. Los proveedores de nubes, por supuesto, nos quieren hacer creer que, porque es a través de la creencia de tal manera que hará que su dinero valga. Sin embargo, la computación en la nube implica ventajas y desventajas, y es vital que quienes toman las decisiones acerca de la computación en la nube lo hagan con gran comprensión de la compensación.

Una manera de entender el paradigma de la computación en la nube es considerar la diferencia entre poseer y conducir su propio coche, y el uso de taxis. Cada uno tiene su lugar y para la mayoría, una mezcla de los dos es lo ideal. Pero si uno usa taxis, es el individuo quien decide cuándo y dónde van. En

todos los escenarios de computación en la nube, el usuario del servicio debe permanecer en el control de su propia agenda, y debe asegurarse de que la nube sirve a su propósito de manera efectiva.

En una empresa, la elección de implementar sistemas que utilizan la computación en nube, infraestructura y aplicaciones a demanda son sólo una parte de la historia. Para sacar el máximo rendimiento de cualquier inversión en TI, es esencial que las organizaciones establezcan muy claramente, objetivos cuantificables y luego seguir adelante con el plan cuidadosamente y aplicar el cuadro completo de uso del negocio, incluida la adaptación de procesos de negocio, ajuste de la estructura de organización y control, y preparación de las personas que se ven afectados por el cambio.

La computación en nube, como cualquier avance tecnológico, tiene un valor potencial si se utiliza bien, pero está lejos de la Flecha de Plata que por arte de magia libera al genio de negocios de alto rendimiento sin esfuerzo adicional.

[top]

Una vergüenza de pruebas

Otro incidente de junio 2011 ha captado el interés de un gran número de los miembros de LinkedIn en dos foros de discusión por separado. Este fue el robo de un laptop en el Instituto Australiano de Directores de Compañía. Los detalles del robo fueron notificadas a los miembros de AICD (me incluyo) unos días después del incidente, y posteriormente se informó a través de varios canales de prensa.

La obligación de notificar a los miembros surgió porque la máquina robada contenía un conjunto importante de datos de miembros y contactos, algunos de los cuales miembros de la AICD se consideran como privados, si no sensibles. Se nos dice que aunque los datos no están cifrados, están sujetos a una serie de garantías. También se nos dice que el robo es considerado como un acto oportunista que se produjo durante un corte de fin de semana de la energía que dejo sin funcionar la seguridad de la puerta, y a pesar de la presencia de guardias de seguridad adicionales. El mensaje a los miembros y otros contactos de la AICD está escrito en un tono medido que parece estar diseñadas para minimizar la preocupación que suscita el evento. El texto no niega el riesgo de que los datos sean utilizados, pero no presenta el riesgo de ser relativamente pequeño.

Un punto que no se explica en la carta a los miembros de AICD es la razón por la que un conjunto importante de información de los miembros estaba en el bloc de notas en el primer lugar. Normalmente, se esperaría que estos datos sólo existan en un servidor en un entorno debidamente asegurados, y administrado por una aplicación de negocio adecuada. Sin embargo, uno de los informes de prensa afirma que los datos han sido cargados en la computadora portátil para su uso en la prueba del nuevo CRM de AICD. Tomando este informe a su valor nominal, un número de comentarios posteriores han señalado que el uso de datos en tiempo real para las pruebas, desde hace mucho tiempo se ha considerado como una práctica muy pobre. Algunos han señalado que las buenas prácticas en la administración de datos incluye una política formal que establece el uso legítimo de los datos, así como la responsabilidad de su gestión, la integridad y la seguridad.

Si el informe se toma en sentido literal, se plantea la pregunta de si la AICD ha establecido políticas adecuadas para el uso de los datos. Si tales políticas existen y se observan, sería más probable que los datos no han estado en el computador portátil robado, y si lo hubiera hecho, habría sido objeto de una fuerte encriptación. Sin embargo, si bien ha habido muchos casos a través de muchas organizaciones de la política que lleva a ser ignorados incidentes similares, también existe la posibilidad de que la política no existía, y que nadie había pensado que si esas políticas y controles asociados podrían ser necesarias.

De acuerdo con la carta de la AICD, tomar las medidas incluye la participación de la policía, los expertos forenses y el asesoramiento del Comisionado de Privacidad. Esta es una respuesta significativa a un solo incidente y demuestra que la AICD reconoce la sensibilidad asociada con los datos que han sido robados.

Tomado como un solo incidente, en la mayoría de las organizaciones, la información proporcionada y las medidas adoptadas por la AICD, así puede ser considerado como suficiente. Sin embargo, por lo menos un comentarista ha señalado que un cuerpo que se ocupa principalmente de gobierno debe demostrar la gobernabilidad impecable en todas sus actividades, incluyendo el uso de tecnologías de la información.

Considerarse a la luz de los problemas de seguridad, muchos se informaron durante el año 2011, el incidente AICD puede llegar a ser bastante menor. Sin embargo, también podría presentar una valiosa oportunidad de aprendizaje para la AICD, sus miembros y otras partes interesadas. Aunque hay facciones en la comunidad que siguen negando la necesidad, hay muchos indicadores de la importancia de una supervisión efectiva a nivel de TI. Estos incluyen creciente carga reglamentaria en materia de información, la aparición de una guía específica para directores como en Informe de Sudáfrica III de Gobierno Corporativo, el persistente problema de daño a las organizaciones a través del fracaso evitable de ambas iniciativas de TI y operativos de los sistemas de TI, y la creciente frecuencia y la gravedad de los ataques maliciosos en los sistemas de TI y redes. Para los directores que no están seguros, y para aquellos que ya están convencidos de la necesidad para supervisar el uso de TI, una gran

cantidad de valor pudieran derivarse de la AICD con el incidente como un disparador para una revisión exhaustiva de los arreglos QUE han puesto en marcha para la gobernanza de TI. El aprendizaje a partir de esta revisión debe, además mejorar los puntos débiles identificados en el enfoque utilizado por la AICD, también proporcionan una fuente de conocimiento para los miembros de la AICD.

Esta revisión debería, por supuesto, llevarse a cabo utilizando la norma ISO 38500. Uno se pregunta cómo Podría la AICD ser el ideal de buen gobierno, cuando se mide a través de los seis principios establecidos en la norma. El resultado de una evaluación formal, estructurada ipuede sorprender!
[top]

Observación de Albert Einstein

La definición de estupidez es hacer la misma cosa una y otra vez y esperar resultados diferentes. - Albert Einstein.

El punto de Einstein ha sido demostrado muchas veces cuando organizaciones de todo el mundo han intentado luchar con la tecnología de la información en la sumisión. Un ejemplo de ello han sido los intentos de varios gobiernos estatales de Australia para adoptar un modelo de "servicios compartidos" para el gobierno.

Australia Occidental comenzó su esfuerzo en el año 2003, con el objetivo de estandarizar los servicios de 90 agencias. Que se finalizará en el 2006 a un costo de $ 91 millones, el proyecto fue publicado a finales de 2010 como probable que continúe hasta el año 2013, a un costo de $ 400 millones.

Queensland ha adoptado una estrategia de servicios compartidos de TI en la misma época. La estrategia de manera eficaz se estrelló con el desastroso mayo 2010 con la implementación de un sistema de nómina para la Salud de Queensland, dando lugar a que a muchos funcionarios no le paguen la cantidad correcta en el tiempo (el propósito fundamental de un sistema de nómina es pagar a la gente la cantidad correcta, a tiempo).

Australia del Sur se embarcó en un viaje similar en septiembre de 2006. El informe de prensa del 28 de junio critica el "desastre" de la Coalición de Servicios Compartidos y pone de relieve que no todo está bien con esta iniciativa, con excesos de presupuesto de más de 100% y los beneficios que no están disponibles.

Mientras tanto, Victoria tuvo un enfoque muy diferente a los servicios compartidos en 2005, y se convirtió en la entidad que hoy conocemos como CenITex. El modelo de Victoria se diferencia sustancialmente de las de Australia Occidental, Australia del Sur y Queensland, porque el foco de CenITex ha estado en la infraestructura compartida, en lugar de compartir los sistemas de negocio.

CenITex ha evitado la mayor parte de la complejidad que hace que los cambios a los sistemas de negocio sean muy difíciles - el comportamiento humano, que es una parte fundamental del cambio.

Parte del problema parece ser que el término "servicios compartidos" no cuenta toda la historia. Los modelos de WA, SA y Queensland en realidad van más allá de los servicios compartidos, con el valor que se basa en sistemas de negocios sustancialmente estandarizados - que sólo son posibles cuando las agencias trabajan de la misma manera. Esta normalización es una característica del enfoque utilizado por el gobierno de Singapur, donde la arquitectura del negocio es el elemento principal en materia de normalización, lo que permite la posterior adopción de los sistemas estándar de negocios e infraestructura. La falta de estandarización de negocios, como fue el caso de los proyectos de la nómina en Queensland, significa que el intercambio se limita a una base de elementos de pocos, como el nombre del proveedor del software.

Ahora Nueva Gales del Sur, bajo un nuevo gobierno, también se embarca en un viaje de Servicios Compartidos, con el concepto de ser el centro de una iniciativa para desarrollar una nueva estrategia a nivel estatal para las TI.

Este será un proceso interesante de ver. Modelos de servicios compartidos siguen siendo ampliamente promovidos como "mejores prácticas" a pesar de que a menudo fallan. Uno se pregunta si NSW tendrá como objetivo para la dura rutina de la normalización de los sistemas de negocio a través de lo que puede ser un servicio público del Estado no quiere, o el más sencillo fusión y la estandarización de la infraestructura.
[top]

Exposición de COBIT 5

ISACA ha sido un firme defensor de la buena gobernanza de las tecnologías de la información. A través de su IT Governance Institute, ISACA ha defendido el concepto de responsabilidad de la junta y la participación en la gobernanza de TI. Sin embargo, la orientación práctica sobre los marcos de ISACA y, en particular en COBIT (actualmente en versión 4.1) se ha centrado fundamentalmente en las actividades de gestión, y ha carecido de una clara separación conceptual del gobierno y la gestión. Esta falta de separación conceptual también ha afectado a uno de los títulos insignia de ISACA. La especificación de los conocimientos para CGEIT está dominada por las habilidades de gestión, y no exige grandes conocimientos de gobierno real.

ISACA señaló que esto va a cambiar durante el año 2010 cuando se publicó el borrador de la primera exposición de una importante revisión de COBIT. El proyecto sin rodeos reconoció la falta de separación conceptual, y presagió un cambio importante en el

pensamiento, apoyado en los conceptos de la norma ISO 38500.

Sólo hace unos días, ISACA ha anunciado que el borrador de la nueva edición, COBIT 5, está disponible para su revisión y comentarios. El material de COBIT 5 es de libre acceso y el período de comentarios se mantiene abierto hasta el 31 de julio de 2011. El proyecto consta de dos documentos - un marco de 85 páginas y una guía de 218 páginas de referencia de proceso.

Un examen breve del marco revela una clara influencia de la norma ISO 38500, con el reconocimiento explícito de la norma y las tres principales tareas de gobierno - Evaluar, dirigir y supervisar. Sin embargo, los principios de buena gobernanza establecidos en la norma ISO 38500 no son inmediatamente evidentes. Uno se pregunta si se dará a conocer a través de una inspección más cercana.

Yo sin duda asignaré tiempo para el borrador de COBIT, e incluiré un resumen de mis comentarios en la edición de julio 2011.
[top]

Historia de Cinco Naciones

En la abril de 2011, presenté la evaluación de cómo están en los Emiratos Árabes Unidos y Omán, tras una quincena de visitar esos países. A finales de mayo y principios de junio llevó el conteo de los países cubiertos en 2011 a cinco, con visitas a la Argentina y El Salvador, seguido de una segunda visita a Kuala Lumpur.

La visita argentina fue organizada por mi buen amigo Carlos Francavilla y sus colegas en la compañía BIT Company, y patrocinada por el Instituto Nacional de Administración Pública (INAP). El subsecretario de Gestión de Tecnología, Eduardo Thill organizó una sesión informativa importante en el enfoque de la ISO 38500 para el gobierno de TI para los negocios del gobierno y más de 70 líderes de TI.

Durante la sesión informativa, que se llevó a cabo en el auditorio muy grande de la Secretaría del Gabinete, Eduardo Thill hizo hincapié en el papel de las normas para el gobierno de TI en el reconocimiento de que con la llegada de la banda ancha ubicua de alta velocidad, el usuario de la tecnología de la información es un jugador dominante nuevo, no sólo en la tecnología de la información, sino en todos los aspectos de la sociedad.

Además de la información del gobierno, un breve informe fue proporcionado para los CIOs principales de la ciudad de Buenos Aires, y una clase de Inmersión de la norma ISO 38500 fue completada por 18 directores de TI líderes y consultores.

El Salvador no nos viene a la mente cuando pensamos en las naciones que son líderes en la industria de TI. Por lo tanto, puede sorprender a muchos saber que El Salvador, a través de los esfuerzos de su naciente Cámara de Empresas de la Industria TIC (CasaTIC) y con el apoyo del equipo de la empresa BIT Company, entregó 60 delegados una conferencia de medio día sobre el gobierno de TI, y otros 45 delegados una clase de Inmersión de un día completo.

Mientras que el visitante ocasional puede todavía ver a El Salvador como un país empobrecido, también hay una energía palpable y entusiasmo, con la tecnología de la información que se ve como un campo importante de oportunidades. El entusiasmo y el compromiso en las dos sesiones fueron muy evidentes y se refleja en esta entrada del blog de Lito Ibarra.

Malasia fue uno de los primeros países en comenzar a adoptar la norma ISO 38500 como parte de la agenda de aprendizaje para sus líderes empresariales y de TI. Desde abril de 2009, he trabajado con Expitris para ejecutar cinco clases de Fundación ISO 38500, con más de 60 personas capacitadas hasta la fecha.

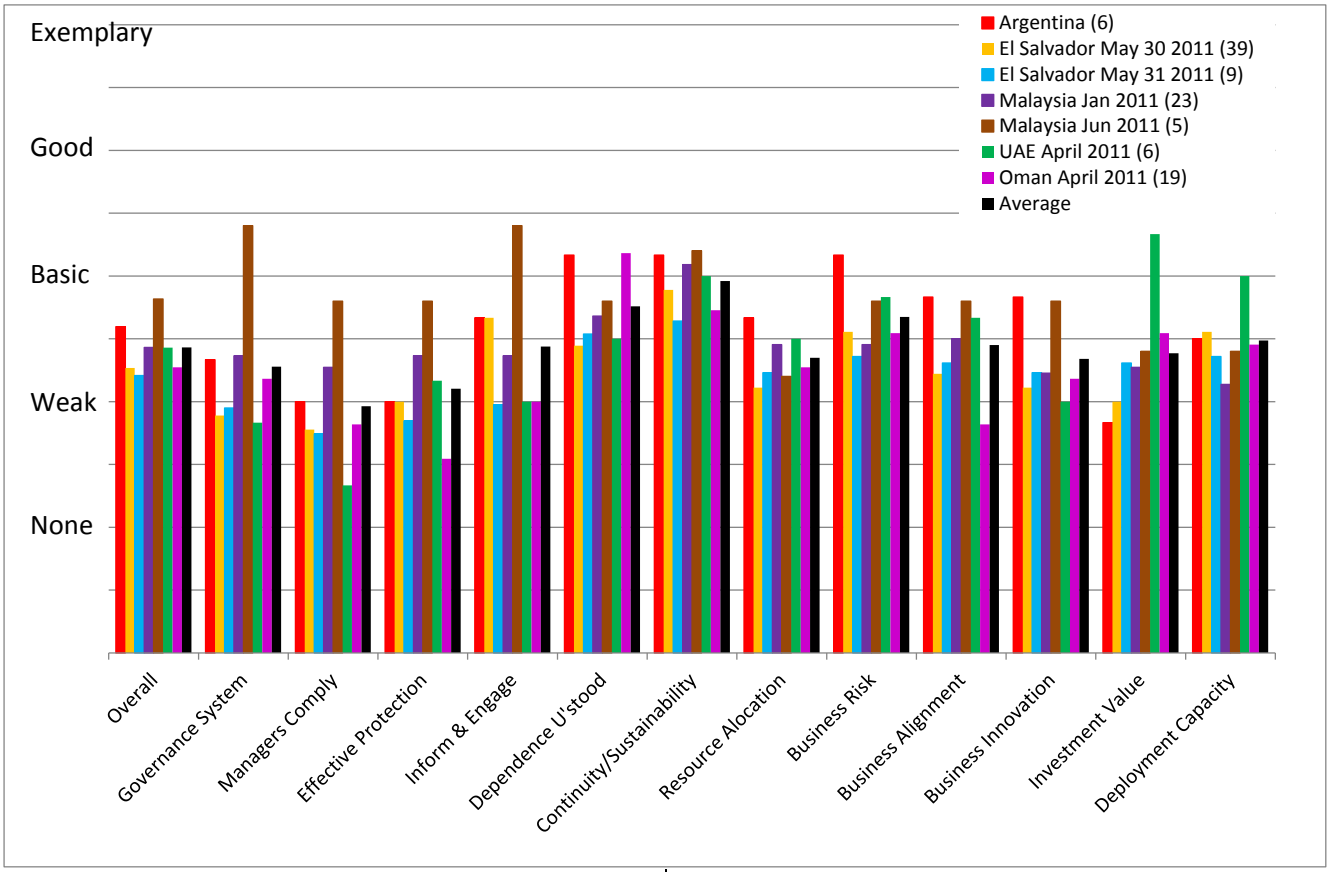
Mientras que los estados árabes claramente disfrutan de los beneficios de la riqueza petrolera importante, son de otra manera las economías en desarrollo - la capacidad de construcción para un futuro sostenible más allá del petróleo. El Salvador, Malasia y Argentina son también los países que se centran en el desarrollo de su futuro económico. Es bastante interesante y agradable ver que estas economías en desarrollo están buscando cada vez más adoptar la orientación de la norma ISO 38500, para mejorar la probabilidad de que sus inversiones en TI entreguen resultados valiosos.

Sin embargo, más que asistir a sesiones informativas y cursos sobre el gobierno de TI es sólo el comienzo de estas naciones. El rendimiento proviene no de aprender acerca de las posibilidades, sino de hacer un cambio real para mejorar el rendimiento. Como siempre, se realizaron evaluaciones en todas las clases en los cinco países como parte de las clases. Estas evaluaciones muestran que la práctica habitual ha entregado a las naciones en desarrollo alrededor del mismo nivel de capacidad en la gestión de las TI como se observa típicamente en el "mundo desarrollado".

La tabla presenta la combinación de "indicadores" resultados de la evaluación de siete clases distintas de cinco países durante el 2011. Los números a la derecha en la leyenda son el tamaño de la muestra, que va de 39 en El Salvador, el 30 de mayo a 5 de Malasia a principios de junio. Los "indicadores" son 12 puntos de rendimiento y capacidad que se puede utilizar para formar una visión aproximada inicial de cómo cada organización rige su uso de TI. En una evaluación completa, los indicadores se complementan con otros 72 puntos relacionados con los principios definidos en la norma ISO 38500.

En la evaluación, a los participantes de la clase se les pide que comparen sus organizaciones, la capacidad y el rendimiento con un conjunto de sentencias ejemplares. El ranking expresa cuán estrechamente las organizaciones se ajustan a las directivas y las expectativas de la norma ISO 38500, y lo bien que gobiernan el uso de TI. El perfil de cada grupo es el promedio de todas las respuestas, y le da un punto de vista inicial sobre la eficacia general de los acuerdos de gobierno en la región a la que pertenece el grupo.

Es raro que un participante clasifique "ejemplar" el estado en cualquier punto específico de la evaluación. La mayoría de las personas que realizan la evaluación son de hecho bastante brutales en su auto-evaluación - y muchos comentarios que, aunque las declaraciones modelo son bastante razonables, existe una oportunidad significativa para mejorar.



Cuando se utiliza en una sola organización, la herramienta de evaluación proporciona una forma rápida de segregación de puntos de vista consistentes e inconsistentes, y establecer un acuerdo sobre dos necesidades y oportunidades para mejorar la gestión del uso de las TI.

En la clase de Malasia de junio, un individuo constantemente calificó el estado de ejemplar, lo que eleva el promedio de la clase. Otras respuestas fueron más consistentes con las respuestas de la clase mucho más grande en enero.

Leyendo de izquierda a derecha, vemos que las cinco naciones, a través de siete encuestas, en general se han debilitado a la gobernabilidad básica de TI. La debilidad se inicia con una tendencia a no tener un sistema de gobierno claramente definido, y la escasa medida en que todos los directores cumplen con las especificaciones del sistema. Sin un sistema de gobierno eficaz, debe ser sorprendente que haya poca protección eficaz contra las cosas que van mal con él. Mientras que algunos gerentes pueden ser muy conscientes de lo que está pasando con él, es probable que un sistema eficaz para un mejor gobierno que informar y comprometer a los gerentes, ejecutivos y miembros del órgano de gobierno que debe garantizar que su utilización es eficaz, eficiente y aceptable.

La omnipresencia de la informática y las consecuencias de TI que va mal, en general contribuyen a un mayor nivel de conciencia del papel que desempeña. Sin embargo, sigue existiendo una brecha significativa entre el grado actual y deseable que se entienda la dependencia de negocio de TI. Los esfuerzos de suministro de TI los equipos tienden a apuntalar un poco de confianza en la medida en que protege el uso de la continuidad y sostenibilidad de la empresa, pero en general sigue habiendo oportunidades significativas de mejora. La diferencia es quizás ejemplificada por el hecho de que la asignación de recursos no responde a las necesidades de las organizaciones representadas en la encuesta, y la percepción de que el riesgo del negocio de fracaso de TI es serio, no se entiende bien.

La alineación del negocio es un problema perenne, frecuentemente discutido en muchos foros. La mala clasificación a través de estos siete estudios quizás se

explica por la clasificación correspondiente bajo el sistema de gobierno, gestión de cumplimiento y el grado en que las personas apropiadas están informadas e involucradas. Un argumento similar puede hacerse con respecto a la innovación empresarial, donde el uso avanzado de TI para apoyar la innovación de negocios depende de un equipo de gestión bien informado y comprometido que bien se puede entender y manejar efectivamente el riesgo empresarial.

Valor de la inversión se realiza cuando las iniciativas de TI producen resultados de negocio y definidos, los beneficios medibles. La entrega de los resultados del negocio depende de un equipo de gestión adecuadamente implicado y mejor informado, que entiende que el valor de la inversión en TI proviene de la atención a toda la gama de cambios en el negocio, y no sólo a los componentes de TI. Esta atención depende en gran medida de la asignación de recursos adecuados, una buena comprensión de cómo asegurar la alineación de TI y la actividad empresarial, y un enfoque eficaz para entender y controlar el riesgo. La debilidad se expresa en estas áreas también puede explicar el grado de oportunidad para mejorar la capacidad de despliegue, a través de lo que el cambio se convierte en un aspecto operativo de la empresa para la cual fue desarrollada.

El reto en cada una de estas naciones, como es el caso también en el "mundo desarrollado", es comprender con mayor profundidad los factores que conducen a la debilidad generalizada en el gobierno de TI, y desarrollar las capacidades y los comportamientos necesarios para reemplazar a esta debilidad con capacidad efectiva robusta que asegure un equilibrio constante entre el costo efectivo, los riesgos y oportunidades de valor.
[top]

Programa de Educación de Infonomics

Después de tres meses de viaje, estamos tomando un breve descanso del programa de educación de Infonomics en julio.

En septiembre, estaré en Londres para una reunión del grupo de trabajo ISO / IEC que gestiona la ISO 38500. Ahora estoy trabajando con socios de negocios de toda Europa para organizar eventos que permitan a las empresas muchos más profesionales de TI y para familiarizarse con las normas y los conceptos que se presentan para una gobernanza eficaz de las TI.

Sugerencias y solicitudes de eventos de educación son siempre bienvenidos - Enviar a mail@infonomics.com.au.