Sustento del uso justo de Materiales Protegidos

derechos de autor para fines educativos

UCI
Universidad para la Cooperación Internacional

UCI

Sustento del uso justo de materiales protegidos por Derechos de autor para fines educativos

El siguiente material ha sido reproducido, con fines estrictamente didácticos e ilustrativos de los temas en cuestión, se utilizan en el campus virtual de la Universidad para la Cooperación Internacional – UCI - para ser usados exclusivamente para la función docente y el estudio privado de los estudiantes en el curso Certified Information Security Manager.

La UCI desea dejar constancia de su estricto respeto a las legislaciones relacionadas con la propiedad intelectual. Todo material digital disponible para un curso y sus estudiantes tiene fines educativos y de investigación. No media en el uso de estos materiales fines de lucro, se entiende como casos especiales para fines educativos a distancia y en lugares donde no atenta contra la normal explotación de la obra y no afecta los intereses legítimos de ningún actor .

La UCI hace un USO JUSTO del material, sustentado en las excepciones a las leyes de derechos de autor establecidas en las siguientes normativas:

a- Legislación costarricense: Ley sobre Derechos de Autor y Derechos Conexos, No.6683 de 14 de octubre de 1982 - artículo 73, la Ley sobre Procedimientos de Observancia de los Derechos de Propiedad Intelectual, No. 8039 – artículo 58, permiten el copiado parcial de obras para la ilustración educativa.

b- Legislación Mexicana; Ley Federal de Derechos de Autor; artículo 147.

c- Legislación de Estados Unidos de América: En referencia al uso justo, menciona: "está consagrado en el artículo 106 de la ley de derecho de autor de los Estados Unidos (U.S,Copyright - Act) y establece un uso libre y gratuito de las obras para fines de crítica, comentarios y noticias, reportajes y docencia (lo que incluye la realización de copias para su uso en clase)."

d- Legislación Canadiense: Ley de derechos de autor C-11– Referidos a Excepciones para Educación a Distancia.

e- OMPI: En el marco de la legislación internacional, según la Organización Mundial de Propiedad Intelectual lo previsto por los tratados internacionales sobre esta materia. El artículo 10(2) del Convenio de Berna, permite a los países miembros establecer limitaciones o excepciones respecto a la posibilidad de utilizar lícitamente las obras literarias o artísticas a título de ilustración de la enseñanza, por medio de publicaciones, emisiones de radio o grabaciones sonoras o visuales.

Además y por indicación de la UCI, los estudiantes del campus virtual tienen el deber de cumplir con lo que establezca la legislación correspondiente en materia de derechos de autor, en su país de residencia.

Finalmente, reiteramos que en UCI no lucramos con las obras de terceros, somos estrictos con respecto al plagio, y no restringimos de ninguna manera el que nuestros estudiantes, académicos e investigadores accedan comercialmente o adquieran los documentos disponibles en el mercado editorial, sea directamente los documentos, o por medio de bases de datos científicas, pagando ellos mismos los costos asociados a dichos accesos.

Estudio de Casos

El siguiente estudio de caso sirve para demostrar gráficamente el requerimiento de gobierno de la seguridad explicado en este primer dominio. El caso ilustra cómo los desastres son comúnmente causados por una secuencia de fallas y es un estudio de una estructura y cultura organizacional con problemas de funcionamiento. El no aprender de esta situación (y de otros incidentes significativos) y no tomar las acciones correctivas recomendadas por el equipo externo de expertos en revisión post mórtem indudablemente contribuyó al fracaso definitivo de esta organización financiera de más de 45000 empleados durante la recesión económica de 2008-2009.

En una importante institución financiera de EUA, el personal de bajo nivel que supervisa el centro de operaciones de red (NOC) notó una actividad de red inusual un domingo en la noche cuando el banco estaba cerrado. Confundidos e inseguros acerca de lo que veían, y sin instrucciones para actuar de manera contraria, decidieron observar el evento en lugar de arriesgarse a molestar a los gerentes un fin de semana. La organización no había desarrollado criterios de severidad, requerimientos de notificación o procesos de escalamiento. El lunes temprano, el tráfico siguió aumentando en la instalación principal y de repente comenzó a crecer significativamente en el sitio espejo, a cientos de millas de ahí. A pesar de haber sido asesorado en relación con el riesgo, el gerente de TI (al ser interrogado por el autor de este caso de estudio) afirmó con un grado de orgullo que la red totalmente plana había sido diseñada para un alto rendimiento y que confiaba en que su experimentado equipo podía manejar cualquier eventualidad.

A las 7:00 a.m. del lunes, el personal del NOC estaba lo suficientemente preocupado como para notificar a los gerentes de TI que había un problema y que los monitores mostraban que la red se estaba saturando. Una hora más tarde, cuando el equipo externo de respuesta a incidentes de computación (CIRT) llegó, la red no estaba operativa y el equipo determinó que la red había sido afectada por el gusano Slammer. El gerente del equipo CIRT informó al gerente de TI que el Slammer residía en la memoria y que el reinicio de toda la red y el sitio espejo resolvía el problema. El gerente afirmó que no estaba autorizado para apagar el sistema y que era necesario que el CIO emitiera la orden. No se pudo ubicar al CIO, y los números actualizados de teléfono de emergencia y localizador estaban guardados en un nuevo sistema de localización de emergencias que requería acceso a la red. Cuando se le preguntó sobre el plan de recuperación en caso de desastre (DRP) y lo que tenía que decir en relación con los criterios de declaración, surgieron tres planes diferentes que habían sido preparados por equipos de diferentes partes de la organización, sin el conocimiento del trabajo del resto. Ninguno contenía criterios de declaración o roles, responsabilidades o autoridad específicos. La resolución final requirió que el CEO, quien estaba viajando al exterior y no estaba disponible de inmediato, diera

instrucciones la mañana siguiente (martes) para apagar la red con falla. Más de treinta mil personas no pudieron realizar su trabajo y la institución no pudo operar durante un día y medio. El equipo post mórtem calculó los costos directos finales en más de cincuenta millones de dólares. El trabajo del equipo post mórtem fue obstaculizado por la indiferencia y falta de cooperación de la mayoría de los empleados, temerosos de ser hallados culpables, en una cultura organizacional orientada a la culpa.

El autor de este caso fue el gerente del equipo post mórtem que encontró literalmente cientos de procesos deficientes, una cultura disfuncional y una serie de métricas inútiles, además de una falta absoluta de gobierno adecuado. Para los que supervisan el NOC, las métricas indicaron un problema, pero no fueron lo suficientemente significativas como para que los empleados tomaran decisiones activas, mucho menos correctas. Mejores métricas o una mayor capacidad del personal pudo haber resuelto el problema rápidamente en las etapas iniciales del incidente antes de que éste se convirtiera en un problema. Un mejor gobierno pudo haber conferido una autoridad adecuada a gerente de red para ejecutar la acción apropiada. Un mejor gobierno pudo haber insistido en que se aplicaran los parches para vulnerabilidad emitidos dos meses antes o que se implementaran controles compensatorios apropiados para enfrentar una amenaza conocida. Incluso una gestión de riesgos marginalmente efectiva habría insistido en que una red plana, sin segmentación, no era aceptable y que DRP/BCP era una actividad integrada y probada.

Las conclusiones que se pueden sacar y que son pertinentes para las métricas y el gobierno sugieren que los datos no son información y que una información incomprensible es simplemente datos y no es útil. Este caso también ilustra que no importa cuán buenas sean las métricas y la supervisión que respaldan las decisiones, no son útiles para los que no tienen el poder de tomar decisiones.

En consecuencia, para desarrollar métricas útiles, debe establecerse claramente quiénes toman cuáles decisiones y qué información es necesaria para tomar tales decisiones. A partir de este análisis, se infiere que las métricas de la gestión requieren una variedad de información de diferentes fuentes que luego debe ser sintetizada con el fin de proveer información significativa, necesaria para tomar decisiones relacionadas con las acciones que se requieren.

Este caso demuestra la necesidad que tienen las organizaciones de desarrollar e implementar un gobierno de seguridad de la información y los requerimientos concomitantes de desarrollar métricas útiles.