RIESGOS CIBERNÉTICOS
SEGURO Y RESPONSABILIDAD CIVIL

Esta es una nueva era. La tecnología e Internet han impactado las operaciones del mundo empresarial de hoy. Con estos cambios, la exposición cibernética ha crecido exponencialmente. Con el objeto de proteger los sistemas de informática de su institución y los datos personales de sus clientes, ARM ha preparado esta hoja informativa sobre algunos de los riesgos cibernéticos a los que usted, su institución y sus clientes pudieran estar expuestos, y las soluciones que ofrecemos para minimizar esos riesgos.

Riesgos Cibernéticos

Las exposiciones a riesgos cibernéticos y sus consecuencias son muy reales y cuantiosas. Entre otras cosas, puede que conlleven ataques de denegación de servicio y costos por interrupción de la actividad empresarial. Como resultado, una organización podría verse imposibilitada de ingresar a sus propios sistemas de TI (tecnología de la información) y perder tiempo en el procesamiento de datos substanciales. Así, datos importantes - quizás imprescindibles para la misión - podrían quedar fuera del alcance de quienes están a cargo de tomar decisiones.

¿CUÁLES SON ALGUNOS DE LOS RIESGOS CIBERNÉTICOS A LOS QUE TAL VEZ USTED Y SU INSTITUCIÓN ESTÉN EXPUESTOS?

- Brecha en la privacidad (Divulgación de información personal identificable. Por ejemplo: número de seguridad social, nombre y apellido, dirección, etc.)
- Extorsión cibernética (Datos retenidos como rehenes, a menos que uno le pague al chantajista)
- Delitos cibernéticos (vandalismo, sabotaje a los sistemas de tecnología de la información, etc.)
- El riesgo de terrorismo (uso de sistemas de TI para sabotear infraestructuras como energía eléctrica, comunicaciones, suministro de agua, etc.
- La responsabilidad civil como resultado de brechas de seguridad en la red (demandas legales, requisitos de conformidad, etc.)
- El uso de medios de comunicación electrónicos (como fotos, música, videos y mensajes de texto en línea)
- Uso de propiedad intelectual ajena (por ejemplo: derechos de autor, marcas registradas, patentes)
- Errores y omisiones de tecnología (diseño, mantenimiento o instalaciones de sistemas de manera deficiente)
- En caso de brechas en los datos causadas por piratas informáticos, las universidades se enfrentan a manipulación de los expedientes y/o de las calificaciones de los estudiantes.
- Los centros médicos siempre enfrentan el riesgo implícito en la integridad de los datos en los expedientes médicos.
- El acceso ilegal o no autorizado a sistemas de tecnología de la información puede resultar en transferencias de dinero fraudulentas usando instrucciones de pago en línea.
- El ataque de un virus, por ejemplo, puede dañar los sistemas de TI, incluso el software (soporte lógico), y también corromper los datos en el sistema.

Solución

IDENTIFICACIÓN Y ANÁLISIS DE SUS RIESGOS CIBERNÉTICOS

El costo de recuperar o restaurar los datos que han sido alterados, destruidos o borrados no es fácil de cuantificar. No obstante, el proceso de gestión de riesgos puede llevar a la identificación de riesgos informáticos específicos a los que su organización está expuesta y además ayudar a analizar el tamaño de los riesgos y su impacto en el ministerio de su organización.

SEGURO DE RESPONSABILIDAD CIVIL POR RIESGOS CIBERNÉTICOS

El seguro de responsabilidad civil por riesgos cibernéticos es un instrumento útil para mitigar las consecuencias financieras de una brecha potencial en los datos de los sistemas de TI. Una cobertura de seguro de responsabilidad civil cibernética para iglesias puede cubrir la iglesia como primera parte (o parte principal). Esto significa proteger la propia infraestructura de TI de la iglesia en caso de que ocurra un daño. La póliza también tiene cobertura a terceros, que se concentra en la responsabilidad civil legal hacia otros, como en casos de pérdida o exposición de la información privada de sus clientes. El resumen a continuación repasa a grandes rasgos las dos secciones cubiertas en la póliza de responsabilidad civil cibernética:

TERCEROS (OTRAS PERSONAS):

COBERTURA DE RESPONSABILIDAD CIVIL CIBERNÉTICA

- Seguridad de la red
- Brecha en la privacidad
- Medios de comunicación en Internet

PRIMERA PARTE O PARTE PRINCIPAL (ASEGURADO(A)/ PERSONA NATURAL O JURÍDICA)

GASTOS POR DELITOS CIBERNÉTICOS

- Proceso reglamentario
- Monitorización del crédito
- Primera pérdida de datos
- Interrupción de la actividad empresarial en la red
- Extorsión en la red

Al considerar los riesgos cibernéticos, su organización debe formularse las siguientes preguntas:

- ¿Qué necesita hacer nuestra organización para cumplir con su ministerio en la era de la tecnología?
- ¿De qué instrumentos o recursos, como por ejemplo: sistemas de TI, depende nuestra organización?
- ¿Cuál sería el costo financiero o de reputación al que nuestra organización se enfrentaría a la luz de una brecha en los datos o de indisponibilidad de los sistemas de TI?

Le animamos a incluir riesgos cibernéticos en su planificación de continuidad y a añadir una póliza de responsabilidad civil cibernética a su cobertura de seguro. Por favor, sírvase comunicarse con su ejecutivo de cuentas, para obtener más detalles y un formulario de solicitud. ■

GLOSARIO:

BRECHAS EN LOS DATOS: Se denomina así a la divulgación intencional o no intencional de información segura a entornos no confiables.
CIBER: Como prefijo se utiliza para formar palabras compuestas relacionadas con «computadoras», «redes de computadoras» o «realidad virtual».
DENEGACIÓN DE SERVICIO: Tipo de ataque a una red, creado para entorpecerla o perjudicarla inundándola de tráfico inútil.
MITIGAR: Moderar o atenuar [algo negativo, especialmente doloroso o molesto]; evitar más daños.
NOTIFICACIÓN: Notificación de brecha en la seguridad requerida por ley en la mayoría de los estados.
PRIMERA PARTE (O PARTE PRINCIPAL): La organización o el individuo asegurados.
RESPONSABILIDAD CIVIL: Obligación exigible por ley.
TERCEROS: Organización o persona que no es ninguna de las partes contratantes, por ejemplo, un cliente cuyos datos han sido vulnerados.
TI: Tecnología de la Información.
VIRUS: Segmento de un código que se autorreplica, introducido ilícitamente en un programa de computadora, a menudo para dañar o apagar un sistema o una red.

Gustanos en Facebook **adventistrisk**

Síganos en Twitter **@adventistrisk**

Véanos en YouTube **AdventistRiskMgmt**

PARA OBTENER MÁS INFORMACIÓN, SUBSCRÍBASE A NUESTRO BOLETÍN INFORMATIVO, SOLUTIONS, EN:

www.adventistrisk.org