Highlights

PwC Perú

Julio 2017

Presentamos los principales hallazgos de nuestro estudio *Doing Business in Peru and the Pacific Alliance 2017/2018*, una guía de negocios para nuestro país y nuestros socios de la región. Adicionalmente, compartimos una entrevista a Alexander García, director de Consultoría de Negocios de PwC, quien detalla los elementos que debe tener un plan de ciberseguridad. Asimismo, brindamos ocho preguntas que permiten a las organizaciones evaluar su nivel de preparación ante una crisis.

Doing Business in Peru and the Pacific Alliance 2017/2018
Guía de negocios en la región

La guía *Doing Business in Peru and the Pacific Alliance 2017/2018* contiene la información más reciente, confiable y detallada para empresarios interesados en el Perú, además de una visión general de las principales consideraciones para invertir o hacer negocios en Chile, Colombia y México.

Para ver la publicación, click aquí:
http://www.pwc.pe/es/publicaciones/assets/DB2017.pdf

Entrevista

Alexander García

Director de Consultoría de Negocios de PwC Perú

"No se puede pretender tener una estrategia de transformación digital sin considerar las variables de ciberseguridad y privacidad"

En un mundo interconectado, los negocios buscan acercarse cada vez más mediante herramientas, canales, procesos y servicios digitales a los consumidores, proveedores, socios estratégicos, entre otros. Sin embargo, es importante acompañar estas iniciativas con una estrategia de ciberseguridad y privacidad antes, durante y después de su implementación. Alexander García, director de Consultoría de Negocios, nos brinda su perspectiva sobre recientes ataques informáticos en el mundo y recomendaciones para proteger a las organizaciones.

Hemos sabido de algunos ataques cibernéticos internacionales en los últimos meses. ¿Qué daños podría causar un ataque de este tipo a una compañía?

Los daños pueden ser de distinta naturaleza dependiendo del impacto del ataque; pueden ir desde la interrupción de las operaciones que dependan intensivamente de recursos tecnológicos hasta pérdidas económicas o daños reputacionales. En el caso de los ataques recientes más conocidos, como *WannaCry* y *Petya*, las empresas afectadas fueron víctimas de un ataque de *ransomware*, un chantaje cibernético por medio del cual los *hackers* –valiéndose de las fallas de seguridad de las organizaciones– ingresan a la red de las compañías y a través de un *malware* denominado *ransomware*, encriptan la información y piden un rescate en *bitcoins* (criptomoneda) para permitir nuevamente acceso a tal información. Solamente en el ataque *WannaCry*, alrededor de 200,000 estaciones de trabajo (servidores y computadoras) en 150 países fueron afectadas

En general, ¿las empresas peruanas están preparadas para hacer frente a un ataque cibernético?

En el ámbito local, cada vez hay más interés de los accionistas y la alta gerencia por entender mejor sus riesgos cibernéticos para poder definir las medidas correctivas necesarias. En compañías de los sectores más regulados, tales como los bancos y empresas de seguros, ya se están implementando acciones que permitan contener estos ataques, como, por ejemplo, creando equipos internos de ciberseguridad o Security Operation Centers (SOC por sus iniciales en inglés). Por el lado de las empresas medianas y pequeñas, se está optando por estrategias de tercerización de la función de ciberseguridad debido a los costos que implica para estas organizaciones contar con equipos dedicados *in house*.

¿Con qué elementos debería contar un plan de ciberseguridad?

Lo primero que una compañía debe considerar en un plan de ciberseguridad es identificar claramente dónde están sus activos digitales más importantes, aquellos que de ser afectados puedan interrumpir la operación o causar daños reputacionales o económicos. Una vez identificados los principales activos, se debe evaluar cuáles son las posibles amenazas que pueden impactar negativamente en esos activos tecnológicos para luego implementar los controles de seguridad y privacidad que impidan que esas amenazas se materialicen. A la par, todo plan de ciberseguridad debe contar no solo con una estrategia de contención, sino también con otra de recuperación (que identifique las acciones necesarias para volver a operar). Finalmente, los accionistas y alta gerencia deben interiorizar que no hay sistema de ciberseguridad perfecto y que la probabilidad de ser atacados cada día que pase es más alta en comparación con años anteriores. Cualquier compañía, por más grande o pequeña que sea, puede sufrir un ataque informático. Lo que deben tener claro las organizaciones es cómo contener, responder y recuperar sus operaciones después del incidente.

¿Qué importancia tiene el factor humano en la implementación de medidas de seguridad cibernética?

El personal juega una pieza clave en el engranaje de ciberseguridad. Se piensa que cuando un atacante informático vulnera una red lo que busca es acceder al servidor con la información más crítica: la cuenta de correo del CEO o del administrador de seguridad, cuando eso es en lo que menos piensa. Lo que suele suceder es que el atacante busca al eslabón más débil de la cadena, que puede ser la persona en recepción que registra la entrada de visitantes con una computadora sin muchas aplicaciones pero con acceso a correo e internet, el asistente contable, el encargado de almacén, etc. Por ello, prevenir ataques implica sensibilizar a los usuarios, a lo que se debe sumar la evaluación del nivel de cultura en seguridad de la información del personal. Muchas veces vemos que las empresas capacitan a los empleados pero no evalúan realmente si han interiorizado el tema de ciberseguridad y privacidad.

> *"Cualquier compañía, por más grande o pequeña que sea, puede sufrir un ataque informático. Lo que deben tener claro las organizaciones es cómo contener, responder y recuperar sus operaciones después del incidente".*

Contacto:
alexander.garcia@pe.pwc.com

CEO Pulse on Crisis

La gestión de crisis como prioridad

La mayoría de empresas ha sido golpeada por crisis externas en los últimos años, y sus CEO prevén que deberán enfrentar nuevas en el futuro cercano. Compartimos ocho preguntas que ayudarán a evaluar si una empresa está preparada para hacer frente a crisis.

Ninguna empresa puede evitar al 100% ser golpeada por crisis externas, ya sean estas económicas, políticas, ambientales o sociales. Es por ello que contar con una estrategia de respuesta a crisis es crucial para los negocios. En atención a esta urgencia, PwC conversó con 164 CEO globales para conocer sus principales preocupaciones relacionadas con la gestión de crisis. Los hallazgos de estas conversaciones fueron presentados en el reporte *CEO Pulse on Crisis*.

A fines de 2016, 65% de los CEO con los que se reunió PwC dijo haber experimentado al menos una crisis en los últimos tres años; más de la mitad reportó haber enfrentado dos o más en ese periodo y el 15% indicó que se vio golpeado por cinco o más crisis en ese lapso. Pensando en el futuro, más del 30% considera que enfrentará más de una crisis en los tres años siguientes.

Pero, ¿cómo pueden las empresas estar preparadas para responder y recuperarse de las crisis? No hay dos crisis iguales, pero sí es posible estar preparado para afrontar todas. Para saber si una empresa está lista para hacer frente a una crisis, es necesario plantearse ocho preguntas:

1. ***¿Cuál es el nivel de riesgo de la empresa?***
Los riesgos existentes y emergentes se identifican, mitigan y supervisan. proactivamente.

2. ***¿El liderazgo comparte una sola visión y sentido de propósito?***
El liderazgo está comprometido con una estructura organizacional que potencia la acción y la toma de decisiones requeridas en una crisis.

3. ***¿Está claro quién es responsable?***
Se ha establecido y comprendido una estructura formal de mando y control de la crisis, además de los roles y responsabilidades relacionados.

4. ***¿Entienden todos el rol que deben cumplir?***
Las prioridades de respuesta a las crisis están claramente definidas y acordadas antes de que se produzca una crisis.

5. ***¿Se cuenta con las habilidades necesarias?***
Se conocen las capacidades y vulnerabilidades del equipo de trabajo en relación con el manejo de crisis y se abordan las deficiencias.

6. ***¿Se cuenta con un toolkit para la crisis?***
Los procesos, tecnologías y recursos necesarios para enfrentar una crisis han sido determinados y son comprendidos.

7. ***¿Se ha llevado a cabo simulacros de crisis?***
Los líderes y las personas que deberán involucrarse en la respuesta a las crisis han sido entrenados y evaluados.

8. ***¿El liderazgo es positivo?***
El liderazgo fomenta la mejora continua de sus capacidades de crisis, especialmente cuando una acaba de ocurrir.

Para ver el estudio, click aquí:
http://www.pwc.com/gx/en/ceo-agenda/pulse/crisis.html

Próximas publicaciones

Repaving the ancient Silk Routes

Reporte del Growth Markets Centre de PwC que detalla y analiza la iniciativa Belt & Road (B&R) de China, que tiene por objetivo conectar al gigante asiático a Europa mediante la reactivación de la histórica ruta de la seda.

Para mayor información visita: ***www.pwc.pe***