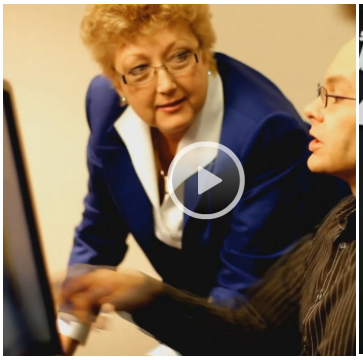
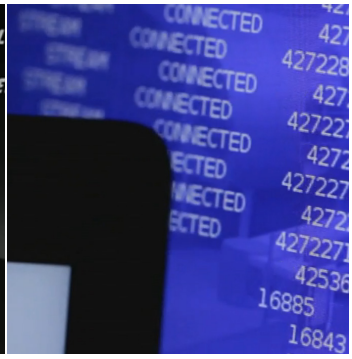
Iniciativas de ciberseguridad de Michigan reducen los riesgos con mejor capacitación de los empleados





RESUMEN EJECUTIVO

Objetivos

- Reducir los riesgos de seguridad con empleados y residentes mejor capacitados.
- Trabajar en coordinación con el sector privado todo lo relacionado con infraestructura crítica y ciberseguridad.
- Crear oportunidades para educación y seguridad continuas.

Estrategia

- Trabajar en coordinación con la Policía Estatal de Michigan y otros organismos gubernamentales responsables del manejo de emergencias en todo el estado.

Soluciones

- Capacitación grupal y en línea de los empleados del estado
- El programa "Cyber Range" permite que el personal especializado en tecnologías practique ejercicios de seguridad de datos.
- En colaboración con entidades públicas y privadas, se elaboró una Estrategia para contrarrestar ciberataques con el objeto de estar preparados ante la posibilidad de un ataque informático a gran escala.

Impacto

- Obtuvo el nivel "A" en los premios Digital States Awards 2012 de la NASCIO (Asociación Nacional de Funcionarios Estatales de Información General de los Estados Unidos); fue uno de los dos estados galardonados.
- Empleados y residentes mejor capacitados; se redujeron los riesgos de seguridad.
- Se evitó más de una docena de amenazas cibernéticas graves; disminuyó el daño por malware y suplantación de identidad.
- Retorno de la inversión estimado del programa: más de 100:1
- Nuevas oportunidades para sesiones constantes de educación y seguridad

Aspectos básicos

En enero de 2014, Cisco publicó los resultados de un profundo análisis de los beneficios económicos de Internet de todo (IdT) para el sector público. El modelo de Cisco reveló que, en los próximos 10 años, podrían generarse aproximadamente USD 4,6 billones de "valor en juego" a partir de la adopción de funcionalidades de IdT en 40 casos de uso clave del sector público, incluidos el agua inteligente, los edificios inteligentes, la energía inteligente, el estacionamiento inteligente y más (http://bit.ly/1aSGlzn).

En una fase posterior del análisis, Cisco contrató a Cicero Group, una importante empresa de investigación y consultoría de estrategias basadas en datos, para que realice un estudio global de las funcionalidades de IdT en esos 40 casos de uso: de qué manera las mejores organizaciones del sector público "conectan lo que estaba desconectado", tal como lo llama Cisco. Para eso, Cicero Group realizó entrevistas con decenas de las principales jurisdicciones del sector público (gobiernos federales, estatales y locales; organizaciones de atención médica; instituciones educativas; y organizaciones no gubernamentales [ONG]) con el objetivo de explorar de qué manera estos líderes mundiales sacan provecho hoy de IdT.

La investigación analizó proyectos reales que se aplican en la actualidad, que se extienden a escala (o a través de pilotos con potencial de escala indudable) y que representan la vanguardia de la preparación y la madurez de IdT en el sector público. El objetivo de la investigación fue comprender cuáles fueron los cambios en cuanto a las personas, los procesos, los datos y los objetos de la jurisdicción. Además, de qué manera las organizaciones del sector público pueden aprender del camino que abrieron estos líderes globales de IdT (e imitarlo). En muchos casos, esas jurisdicciones son clientes de Cisco; en otros, no lo son. Por lo tanto, el enfoque de esos perfiles jurisdiccionales no es promocionar el rol de Cisco en el éxito de esas organizaciones. Más bien se orienta a documentar la excelencia de IdT, a especificar de qué manera las entidades del sector público ponen en práctica hoy IdT, y a informar un plan de cambio que permitirá al sector público abordar los desafíos apremiantes en varios frentes mediante las mejores prácticas que se pueden aprovechar de todo el mundo.

 © 2014 Cisco y/o sus filiales. Todos los derechos reservados.

Acerca del estado de Michigan

El estado de Michigan ha implementado una serie de iniciativas de ciberseguridad que lo ubican entre los mejores estados de EE. UU. en cuanto a conciencia y educación en seguridad de los datos. Estas iniciativas incluyen un programa de capacitación para empleados tan innovador como entretenido, un "Cyber Range" en el que los especialistas técnicos aprenden a contrarrestar amenazas a la seguridad y constante colaboración entre los sectores público y privado para elaborar la Estrategia de respuesta ante ciberataques de Michigan.

Dan Lohrmann se desempeña como director de seguridad, director de seguridad informática y director adjunto de ciberseguridad y protección de la infraestructura (CIP) en el Departamento de Tecnología, Administración y Presupuesto (DTMB) de Michigan. El Sr. Lohrmann ha trabajado en diversos puestos de seguridad y liderazgo del sector público, por ejemplo, en la Administración Nacional de Seguridad (NSA). Fue director de seguridad de la información (CISO) y director de tecnología (CTO) de Michigan antes de asumir su cargo actual.

El estado de Michigan ha implementado una serie de iniciativas de ciberseguridad que lo ubican entre los mejores estados de EE. UU. en cuanto a conciencia y educación en seguridad de los datos.

Andris Ozols es un asesor y analista de políticas de nivel superior que trabaja para el Departamento de Tecnología de la Información del estado de Michigan. Tiene más de 42 años de experiencia como empleado público en Michigan.

Objetivos

El principal objetivo de las iniciativas de ciberseguridad de Michigan fue reducir los riesgos de seguridad mediante empleados y residentes mejor capacitados. El estado también se propuso trabajar en coordinación con el sector privado en todo lo relacionado con infraestructura crítica y ciberseguridad, además de crear oportunidades para educación y seguridad continuas.

Estrategia

El Director de Seguridad del estado de Michigan y el Departamento de Tecnología, Administración y Presupuesto de Michigan (DTMB) son responsables de la administración y el mantenimiento generales del plan y la implementación de las iniciativas de ciberseguridad del estado. Estos esfuerzos están coordinados con la Policía Estatal de Michigan y con otros organismos gubernamentales responsables del manejo de emergencias en todo el estado.

Gran parte de la financiación para las iniciativas de ciberseguridad de Michigan proviene del sector público; se utilizan fondos tanto estatales como federales. Esto incluye subsidios otorgados por el Departamento de Seguridad Nacional y recursos disponibles gracias a la colaboración con entidades de educación superior.

- Las cibercumbres y los eventos de desayunos conferencia se autofinancian mediante patrocinios y derechos de asistencia.
- El programa de capacitación en línea Security Mentor se estableció por menos de USD 200 000, con un costo estimado por empleado de 30 centavos por lección en un período de dos años.
- Se creó el programa Michigan Cyber Range con la ayuda de USD 2 millones en donaciones privadas y subsidios, con un 20% adicional de financiamiento total provisto por fuentes gubernamentales. Se espera que el gobierno del estado ahorre entre un 40% y 50% en costos relacionados con certificaciones, cursos y viajes durante toda la vigencia del programa.

 © 2014 Cisco y/o sus filiales. Todos los derechos reservados.

Solución

En su rol de director de seguridad de Michigan, y trabajando conjuntamente con el gobernador de Michigan, Rick Snyder, el Sr. Lohrmann supervisa el programa de ciberseguridad del estado: La Ciberiniciativa de Michigan. Entre los componentes se incluye capacitación grupal y en línea para los empleados del estado, un "Cyber Range" que permite que el personal especializado en tecnología practique ejercicios de seguridad de los datos y una Estrategia para contrarrestar ciberataques elaborada en colaboración con entidades tanto públicas como privadas (como grandes empleadores, empresas de servicios y agencias federales) con el objetivo de estar preparados ante la posibilidad de un ataque informático a gran escala.

Capacitación pública y de los empleados

El programa bimestral de capacitación en ciberseguridad en línea del estado es el núcleo de su sistema de capacitación para empleados. La organización del Sr. Lohrmann también programa cibercumbres y series de desayunos conferencia, además de publicar un boletín mensual.

Al inicio del programa de capacitación en línea, el Sr. Lohrmann primero sondeó a los empleados para determinar la efectividad del programa existente, que consistía primordialmente en enviar mensajes de correo electrónico con hipervínculos a videos con información sobre seguridad. Los resultados no fueron alentadores.

"Pasamos de una asistencia a la capacitación de aproximadamente el 10% de empleados estatales en los últimos 12 meses a mucho más del 90%. Nos dio mucho placer ver la cantidad de gente que realizó la capacitación".

Dan Lohrmann,

Director de seguridad, director de seguridad informática y director adjunto de ciberseguridad y protección de la infraestructura,

Departamento de Tecnología, Administración y Presupuesto de Michigan

El Sr. Lohrmann recuerda: "En algunos estudios de prueba, el personal iniciaba los videos y luego salía a los pasillos, se tomaba una taza de café, iba al baño, volvía, hablaba sobre el juego de la noche anterior y se quedaba sin hacer nada. Ni siquiera estaban mirando los videos. Eso no era bueno. Queríamos que fuera interactivo. Queríamos que el personal realmente se comprometiera con la capacitación y, lo que es más importante, queríamos cambiar las conductas. No se trataba simplemente de marcar la casilla de verificación y decir: 'Sí, hice el curso de ciberseguridad'".

Para encontrar una mejor manera de captar el interés de los empleados del estado, el Sr. Lohrmann prosiguió con un segundo sondeo. "Conformamos un equipo para determinar lo que el personal quería de la capacitación. Dijeron que querían que fuera breve. No querían una sesión de dos horas (o incluso de una hora) frente al escritorio. Querían que fuera breve pero frecuente. Querían que se renovara periódicamente. Querían que fuera intrigante. Querían que fuera divertida".

El Sr. Lohrmann dijo que el DTMB emitió una Solicitud de propuesta (RFP) para una experiencia de capacitación más interactiva, y desafió a los posibles proveedores con la siguiente pregunta: "¿De qué manera podemos cambiar conductas realmente y tener estadísticas sobre ello?".

El DTMB seleccionó el programa de un proveedor que incluía juegos y actividades interactivas enfocadas en la promoción de conductas seguras en diversos entornos. El programa se aplicó a todos los empleados estatales en el curso de seis meses con una notable respuesta y comentarios positivos. "Pasamos de una asistencia a la capacitación de aproximadamente el 10% de empleados estatales en los últimos 12 meses a mucho más del 90%. Nos dio mucho placer ver la cantidad de gente que realizó la capacitación".

"Lo más sorprendente fue que los comentarios fueron simplemente fantásticos", prosiguió el Sr. Lohrmann. "El personal dijo: 'Nos encanta; es lo mejor que hizo alguna vez el departamento de tecnología,' y también escuchamos comentarios realmente alocados como: 'Esto es increíble. ¿Puedo llevármelo a casa? ¿Puedo mostrárselo a mi familia? ¿Puedo mostrárselo a mis hijos?' Después de cada lección... los empleados la califican de uno a cinco: cinco es genial y uno quiere decir que no les gustó. Con 50 000 empleados estatales, tenemos un promedio de más de cuatro, algo inaudito en este ámbito".

 © 2014 Cisco y/o sus filiales. Todos los derechos reservados.

El Sr. Lohrmann explicó el atractivo de los ejercicios de capacitación típicos: "Uno de los juegos que más me gustaron cubre la importancia de su rol en la oficina, lo que enseña a los empleados a encontrar infracciones a la seguridad, como dejar documentos confidenciales sobre los escritorios. A continuación, se clasifica el motivo por el cual eso es una infracción a las políticas o a la seguridad". Otro juego tiene a un personaje al estilo de Súper Mario que corre por un aeropuerto en busca de 12 computadoras portátiles perdidas o robadas. "Es como una cuenta regresiva: tienes 90 segundos", explicó el Sr. Lohrmann. "La primera vez que lo jugué, creo que encontré siete de las 12".

El Sr. Lohrmann dijo que el aspecto más importante de la capacitación es la facilidad con que puede ser recordada. "La idea es cambiar conductas; ahora, cada vez que estoy en un aeropuerto, no puedo dejar de recordar ese juego similar al Súper Mario", dijo. "Ya sea que uno esté en el mostrador de boletos o en la puerta de seguridad, es inevitable pensar en ello. A los empleados les encanta. Dicen que esperan con ansias cada lección".

"La meta fue convertirlo en una sociedad entre el sector público y el privado: integrar a universidades y a nuestros socios a nivel federal para poder determinar de qué manera tenemos previsto defender nuestras redes y sistemas de los mejores y más brillantes atacantes del mundo".

Dan Lohrmann,

Director de seguridad, director de seguridad informática y director adjunto de ciberseguridad y protección de la infraestructura,

Departamento de Tecnología, Administración y Presupuesto de Michigan

Michigan Cyber Range

En un esfuerzo por ofrecer más capacitación técnica al personal de TI, el Sr. Lohrmann se propuso recrear un entorno de pruebas de ciberseguridad similar a los que se usaban mientras trabajó en la NSA. "La idea fue configurar una organización y una capacitación, lo que llamamos Michigan Cyber Range", explicó. "Cyber Range brinda un espacio para probar, capacitar, aprender y desarrollarse en un entorno no confidencial. La meta fue convertirlo en una sociedad entre el sector público y el privado: integrar a universidades y a nuestros socios a nivel federal para poder determinar de qué manera tenemos previsto defender nuestras redes y sistemas de los mejores y más brillantes atacantes del mundo".

De acuerdo con el Sr. Lohrmann, Cyber Range ofrece capacitación técnica en temas como piratería informática ética y diferentes tipos de técnicas forenses, y cuesta aproximadamente la mitad que enviar a una persona al exterior para que asista a un curso similar.

El Sr. Ozols también enfatiza el amplio enfoque en cuanto a la planificación y dice: "En forma consciente y deliberada, adoptamos una perspectiva a nivel estatal cuando trabajamos con gobiernos y entidades locales. Es tanto parte de nuestra responsabilidad como de nuestra visión y nuestras metas". Ahora, los expertos en ciberseguridad de todo el estado y de toda la Región Central, incluida la Guardia Nacional, consultan periódicamente este sitio.

El Sr. Lohrmann dijo que, como primer paso, llevó su idea de un sitio para pruebas de ciberhabilidades ante el Gobernador Snyder, quien respaldó fuertemente el proyecto. El Sr. Lohrmann luego contrató a una empresa de software para que desarrollara la plataforma para las pruebas: un sistema no confidencial y aislado lógicamente que permitiese a los equipos técnicos aprender técnicas de seguridad de datos a través de una serie de ejercicios.

Los equipos técnicos del Sr. Lohrmann practican sus habilidades con diversas situaciones hipotéticas como "Alphaville", que el Sr. Lohrmann describió como "una ciudad pequeña". Y continuó: "Tiene una biblioteca. Tiene una planta eléctrica. Tiene una planta de agua y municipalidad. Realmente es posible atacarla y defenderla". Los empleados del gobierno que aprueban los cursos tienen derecho a diversas certificaciones.

 © 2014 Cisco y/o sus filiales. Todos los derechos reservados.

Estrategia de respuesta ante ciberataques de Michigan

De acuerdo con el Sr. Lohrmann, el Gobernador Snyder es un excelente defensor de la ciberseguridad. “Realmente enfatizó que los ciberataques son la mayor amenaza a la que Estados Unidos debe hacer frente actualmente... Los peligros nucleares pueden ser la amenaza número uno, pero dice que la amenaza más probable es la cibernética, porque ya está ocurriendo”.

En un esfuerzo por crear una estrategia de seguridad a nivel estatal, el Sr. Lohrmann formó una coalición de planificación integrada por representantes de intereses públicos clave y grandes empleadores de todo el estado. “Nos reunimos una vez al mes y tenemos representantes de las principales compañías del sector privado de Michigan”, explicó el Sr. Lohrmann. “Tenemos a Consumers Energy, a DTE Energy y a algunos bancos. También tenemos a algunos proveedores automotrices y a otras empresas de renombre en Michigan. Trabajamos en conjunto para elaborar la estrategia de respuesta ante ciberataques en torno a cómo compartir información sobre ciberamenazas. ¿Cómo trabajamos juntos en una emergencia? ¿Cómo declaramos una emergencia? ¿A quién vamos a llamar? ¿Cómo nos coordinaremos?”.

En un esfuerzo por crear una estrategia de seguridad a nivel estatal, el Sr. Lohrmann formó una coalición de planificación integrada por representantes de intereses públicos clave y grandes empleadores de todo el estado.

El grupo publica sus conclusiones en línea, en la Estrategia de respuesta ante ciberataques de Michigan, que ha sido denominada como Mejor Práctica Nacional por el Departamento de Seguridad Nacional.

“No se trata solo de la extensión y la capacitación”, dijo el Sr. Lohrmann. “El concepto subyacente es bastante nuevo. Históricamente, los gobiernos estatales responden ante incendios, inundaciones, tornados, emergencias en general. Ahora tenemos ciberemergencias potenciales. Nuestra Estrategia para contrarrestar ciberataques nació a partir de un deseo de estar preparados ante posibles ciberataques que pudieran afectar a todo el estado. ¿Qué sucedería si deja de funcionar la red de distribución eléctrica? ¿Cómo nos comunicamos antes, durante y después de un evento? ¿De qué manera trabajamos en conjunto con el sector privado?”. La estrategia también incluye políticas sobre cómo compartir información acerca de ciberamenazas, cómo definir una emergencia y una lista de contactos en caso de emergencia.

El Sr. Ozols señaló: “Somos uno de los primeros estados que también considera las oportunidades de empleo en industrias o de desarrollo económico vinculadas a la ciberseguridad. Hemos hablado con varios socios potenciales como Canadá e Israel, entre otros. Esto también es parte de la extensión. Es parte de una realidad: tenemos algo más que una perspectiva de vida departamental; tenemos una perspectiva estatal”.

Figura 1. Estado de Michigan: nuevas y mejores conexiones.

Fuente: Cisco Consulting Services, 2014

 © 2014 Cisco y/o sus filiales. Todos los derechos reservados.

Impacto

Las iniciativas de ciberseguridad de Michigan permitieron que el estado obtuviese el nivel "A" en los premios Digital States Awards 2012 del Center for Digital Government; fue uno de los dos estados galardonados. Según el sitio web del premio, Michigan "demostró resultados en todas las categorías de sondeo y los hábiles líderes emplean la modernización para implementar prioridades estratégicas y niveles de eficiencia operativa. [Estos] estados muestran señales inequívocas de colaboración significativa; sus mediciones y estadísticas de rendimiento son adoptadas ampliamente y sus recortes presupuestarios generalmente se basan en estrategias".

Los esfuerzos de capacitación de Michigan también fueron elegidos por la NASCIO en 2013 como el mejor proyecto de ciberseguridad de los 50 estados. Los detalles de este premio se pueden encontrar en www.nascio.org/awards.

El Sr. Ozols señaló que, según el documento de premio de la NASCIO, "gracias a estos esfuerzos, se han evitado más de una docena de ciberamenazas" en relación con el programa.

Cyber Range fue aceptado ampliamente como un espacio de prueba avanzado para capacitar a profesionales especializados en seguridad y la Guardia Nacional utiliza el sitio web para sus propios cursos de capacitación en ciberseguridad.

Las medidas de seguridad de datos de Michigan sirven como modelo para otros estados. El Sr. Lohrmann explicó el impacto del documento de la Estrategia de respuesta ante ciberataques en la comunidad de seguridad nacional: dijo que fue designado como Mejor Práctica Nacional por el Departamento de Seguridad Nacional. "Este marco de ciberseguridad se está utilizando como ejemplo de lo que deberían hacer los estados para coordinarse con el sector privado en torno a la infraestructura crítica y la ciberseguridad", dijo el Sr. Lohrmann.

La mejor capacitación de los empleados y los residentes (y la menor cantidad de riesgos de seguridad que eso genera) son los beneficios más prominentes de las iniciativas de capacitación en ciberseguridad de Michigan. El Sr. Ozols señaló que, según el documento de premio de la NASCIO, "gracias a estos esfuerzos, se han evitado más de una docena de ciberamenazas" en relación con el programa. Los daños debidos a malware y suplantación de identidad se han reducido y, dado el alto costo de las infracciones graves a la seguridad, los funcionarios de Michigan estiman que el retorno de la inversión (ROI) del programa fue de "más de 100 a 1".

Además de los programas de capacitación, las iniciativas también incluyen seguridad reforzada en la forma de una infraestructura de TI mejorada, incluido el cableado, las redes de datos, tecnologías inalámbricas y proyectos de informática móvil.

Las iniciativas también proporcionan un centro de capacitación para empleados no públicos y personas que no viven en Michigan; además, el sitio web del estado contiene información actualizada disponible para cualquier persona con acceso a la red. El programa Cyber Range proporciona un lugar para capacitación tanto estatal como nacional en medidas de seguridad de los datos. Además, las reuniones mensuales que tiene el Sr. Lohrmann con ejecutivos y representantes de las industrias de la infraestructura pública crean un enfoque integral de la seguridad que se está copiando a nivel nacional.

Los programas también crean oportunidades para educación y seguridad continuas. La extensión del alcance a escuelas locales y la creación de iniciativas de ciberseguridad en colaboración con universidades de Michigan ofrecen un incentivo para que los estudiantes procuren perfeccionar sus habilidades y busquen empleo en los campos de la seguridad de los datos. Como señaló el Sr. Lohrmann: "La creación de empleos y el desarrollo económico podrían ser un aspecto complementario positivo de la ciberseguridad".

 © 2014 Cisco y/o sus filiales. Todos los derechos reservados.

Conocimientos adquiridos y próximos pasos

El Sr. Lohrmann explicó que obtener beneficios cuantificables es siempre un desafío al evaluar los beneficios de los programas de seguridad. "En lo que hace a nuestra capacitación, lo difícil es que desconocemos lo que no sabemos", dijo. "Es algo como: '¿Cuántos ataques detuvimos? Cuántas personas no hicieron algo que no debían hacer porque participaron de la capacitación'. Es difícil".

Y prosiguió: "Medimos cuántas personas hicieron la capacitación, cuál fue su reacción. Les preguntamos si cambiaron sus conductas. Por ejemplo: hacemos algunas pruebas para saber si el personal hace clic sobre enlaces. El problema al momento de evaluar el éxito es que podría estar implementando muy bien estos programas, pero eso no necesariamente quiere decir que voy a influir en la cantidad de ataques de los que seamos víctimas. No hay ninguna forma sencilla de medir la seguridad".

"Es más, cuando pensamos en datos, pensamos en el modo en el que la gente interactúa con los datos, en los procesos que tenemos alrededor de los datos y en la tecnología que usamos para proteger los datos. Desde la perspectiva de la ciberseguridad, las personas son un factor importante, es por eso que ponemos tanto énfasis en la capacitación".

Dan Lohrmann,

Director de seguridad, director de seguridad informática y director adjunto de ciberseguridad y protección de la infraestructura,

Departamento de Tecnología, Administración y Presupuesto de Michigan

El Sr. Lohrmann reconoció que el entorno de TI actual fomenta la recopilación de amplias cantidades de datos. Aconsejó a quienes pretenden crear programas similares que recuerden que "no se puede tratar a todos los datos de la misma manera. Hay diferentes clases de datos. Hay gran cantidad de datos no confidenciales y también hay datos confidenciales. Es necesario saber qué clase de datos tienen en sus manos. Sepan bien cuáles son los datos importantes, cómo los están protegiendo y cómo pueden compartirlos. Lleven un inventario, sepan qué son los datos, dónde están y cuáles son sus propósitos. ¿Cuánto tiempo los mantendrán? ¿Cuánto tiempo los almacenarán? ¿Tienen una copia de seguridad? Todos esos detalles son esenciales".

Identificar datos útiles y usarlos correctamente es un punto central que el Sr. Lohrmann pretender perfeccionar. "Tenemos un proyecto más amplio sobre cómo podemos compartir mejor los datos para obtener resultados y descubrir fraudes en el gobierno o descubrir programas para cubrir mejor las necesidades de los ciudadanos, o encontrar la clave para ofrecer mejores servicios a quienes necesitan más ayuda".

El Sr. Lohrmann también describió la importancia de cifrar datos confidenciales, "tanto en reposo como en tránsito". Dijo: "Esa es una política que nos llevó algo de tiempo implementar, pero ya hemos recorrido el 95% del camino. No llegamos al 100%, pero estamos mucho mejor que antes".

El Sr. Lohrmann concluyó: "Es más, cuando pensamos en datos, pensamos en el modo en el que la gente interactúa con los datos, en los procesos que tenemos alrededor de los datos y en la tecnología que usamos para proteger los datos. Desde la perspectiva de la ciberseguridad, las personas son un factor importante, y es por eso que ponemos tanto énfasis en la capacitación. Ni siquiera voy a decir que seremos perfectos, pero sí que tenemos a las personas, los procesos y la tecnología en torno a esos datos, y que tenemos que asegurarnos de pensar profundamente en cómo estamos protegiendo los datos de los ciudadanos".

Más información

Para obtener más información, visite http://www.michigan.gov/cybersecurity

 © 2014 Cisco y/o sus filiales. Todos los derechos reservados.

Sede central en América
Cisco Systems, Inc.
San José. CA

Sede Central en Asia Pacífico
Cisco Systems (EE. UU.) Pte. Ltd.
Singapur

Sede Central en Europa
Cisco Systems International BV Amsterdam.
Países Bajos

Cisco cuenta con más de 200 oficinas en todo el mundo. Las direcciones, los números de teléfono y de fax están disponibles en el sitio web de Cisco: **www.cisco.com/go/offices**.

Cisco y el logotipo de Cisco son marcas registradas o marcas comerciales de Cisco y/o de sus filiales en los Estados Unidos y en otros países. Para ver una lista de las marcas registradas de Cisco, visite la siguiente URL: www.cisco.com/go/trademarks. Las marcas registradas de terceros que se mencionan aquí son de propiedad exclusiva de sus respectivos titulares. El uso de la palabra "partner" no implica que exista una relación de asociación entre Cisco y otra empresa. (1110R)