CYBER READINESS
INSTITUTE

CYBERREADINESSINSTITUTE.ORG

Hoja de ruta para la preparación cibernética de las pequeñas y medianas empresas (pymes)

Tabla de contenido

Resumen ejecutivo

El Cyber Readiness Institute (CRI) ha convocado con éxito a altos directivos de empresas globales para reunir las prácticas recomendadas para gestionar a las personas, los procesos y la tecnología que son fundamentales para mejorar la ciberseguridad. A partir de esta colaboración, se ha desarrollado contenido y herramientas destinadas a proteger, responder y recuperarse de incidentes que ocurren en toda la comunidad de pequeñas y medianas empresas (pymes) globales.

Los copresidentes y miembros del CRI representan distintos sectores empresariales y tienen presencia en todo el mundo. Estas organizaciones contribuyen positivamente a la protección de las pymes globales de las amenazas cibernéticas con sus recursos, tecnología y liderazgo. Nuestros copresidentes pertenecen a Apple, The Center for Global Enterprise (CGE), Mastercard y Microsoft, y nuestros miembros trabajan en empresas como ExxonMobil, General Motors y Principal.

En la hoja de ruta de CRI para la preparación cibernética de las pequeñas y medianas empresas (pymes) se analizan nuestros cinco primeros años con información obtenida de los datos, testimonios, iniciativas piloto, revisión de contenido y participación de las partes interesadas para evaluar nuestro alcance e impacto. Esta información y los comentarios directos de largas conversaciones con nuestros miembros y otros participantes clave en el programa de CRI proporcionaron directrices para la continuación del trabajo específico requerido para abordar la misión de CRI: permitir a las pymes globales acelerar su preparación para la ciberseguridad y su resiliencia operativa.

Concienciación

Mejorar los conocimientos y la comprensión que tienen las pymes sobre las ciberamenazas relacionadas con la continuidad del negocio y las prácticas recomendadas.

1. Alcance global: garantizar que los recursos de CRI lleguen a las pymes de todo el mundo mediante la asociación con organizaciones de ámbito global
2. Desarrollo e intercambio de datos: recopilar y publicar información única, no específica de ningún proveedor

Implementación

Ayudar a las pymes en la implementación de políticas y procedimientos cibernéticos para crear una cultura de preparación cibernética centrada en el comportamiento humano

1. Estándares de preparación cibernética: desarrollar y ampliar el Programa de preparación de CRI como base para un proceso de certificación estándar para las pymes que sea reconocido y respaldado por los miembros de CRI y las industrias globales
2. Red mundial de formación: establecer una red mundial de instructores de ciberseguridad cualificados

Incentivos

Explorar los mecanismos para incentivar a las pymes para que mejoren su resiliencia empresarial y su preparación cibernética

- Seguro cibernético: reunir información de las pymes para compartirla con la industria convirtiéndonos en la voz autorizada para las pymes
  - Desarrollar directrices para que las pymes seleccionen la cobertura más adecuada para su organización
  - Ayudar a las pymes a proporcionar pruebas de su preparación cibernética para abordar adecuadamente los riesgos
    - Describir los futuros modelos de negocio para los mercados de seguros
  - Proveedor preferido: implementar el Programa de preparación cibernética con proveedores de segundo y tercer nivel a lo largo de las cadenas de suministro globales para que las pymes obtengan una ventaja competitiva con su certificación.
    - Examinar cómo nosotros, con nuestros miembros y socios, podemos utilizar recompensas monetarias

Resumen ejecutivo

(continuación)

Para seguir cumpliendo la misión de CRI establecida hace cinco años, debemos seguir desempeñando un papel de liderazgo para las pymes como su voz e intérprete en cuestiones cibernéticas clave. Aprovechando una vez más la experiencia de nuestros miembros y socios, CRI pretende convertirse en el primer destino para las pymes que quieren mejorar su preparación cibernética centrándose en el comportamiento humano y quieren conocer los procedimientos esenciales para reducir los ciberataques. Dado que muchas organizaciones ya están trabajando para adoptar estos principios, CRI seguirá esforzándose en convertirse en una voz para las pymes a escala mundial en temas cibernéticos clave, representando su punto de vista con responsables de la toma de decisiones clave para garantizar que se consideren sus necesidades.

CRI quiere agradecer a Apple, GM, Mastercard, Microsoft, ExxonMobil, Principal y el Center for Global Enterprise su papel en el desarrollo de esta hoja de ruta. Las ideas obtenidas de las conversaciones con representantes de estas organizaciones han sido esenciales para dar forma a la trayectoria de CRI.

Introducción

Revisión de cinco años

El Cyber Readiness Institute (CRI) ha convocado con éxito a altos directivos de empresas globales para reunir las prácticas recomendadas para gestionar a las personas, los procesos y la tecnología que son fundamentales para mejorar la ciberseguridad. A partir de esta colaboración, se ha desarrollado contenido y herramientas destinadas a proteger, responder y recuperarse de incidentes que ocurren en toda la comunidad de pymes globales. Según una encuesta mundial de CRI realizada en 2021, solo el 18 % de las pymes de los Estados Unidos creen que su organización está preparada para un incidente cibernético.[1]

En la hoja de ruta de CRI para la preparación cibernética de las pequeñas y medianas empresas (pymes) se analizan nuestros cinco primeros años con información obtenida de los datos, testimonios, iniciativas piloto, revisión de contenido y participación de las partes interesadas para evaluar nuestro alcance e impacto. Esta información y los comentarios directos de largas conversaciones con nuestros miembros y otros participantes clave en el programa de CRI proporcionaron directrices para la continuación del trabajo específico requerido para abordar la misión de CRI: permitir a las pymes globales acelerar su preparación para la ciberseguridad y su resiliencia operativa.

Copresidentes y miembros

Los copresidentes de CRI representan distintos sectores empresariales y tienen presencia en todo el mundo. Estas organizaciones contribuyen positivamente a la protección de las pymes globales de las amenazas cibernéticas con sus recursos, tecnología y liderazgo. Sus contribuciones desde el inicio de CRI son innumerables, pero cabe destacar la siguiente labor:

- Apple: Patrocinó un programa piloto de CRI para mejorar la seguridad de los proveedores.
- The Center for Global Enterprise (CGE): Lanzó el Digital Supply Chain Institute (DSCI) para centrarse en la evolución de las cadenas de suministro empresariales y la aplicación práctica de las recomendaciones de gestión de la cadena de suministro.
- Mastercard: Estableció el Centro de confianza para compartir información, herramientas y recursos para ayudar a las empresas a mejorar su ciberseguridad.
- Microsoft: Lanzó Microsoft Defender para Empresas para proporcionar a las pymes funciones de respuesta y detección de puntos de conexión con el fin de protegerlas del ransomware y otras amenazas cibernéticas sofisticadas.

Los miembros de CRI, ExxonMobil y Principal también han desempeñado un papel importante en el avance de la misión de CRI y GM realizó un programa piloto con sus proveedores críticos. Nuestros miembros proporcionan comentarios directos sobre el desarrollo del contenido y las mejoras del programa.

[1] CRI-The-Urgent-Need-to-Strengthen-the-Cyber-Readiness-of-Small-and-Medium-Sized-Businesses (2).pdf

Contenido y recursos

Formación

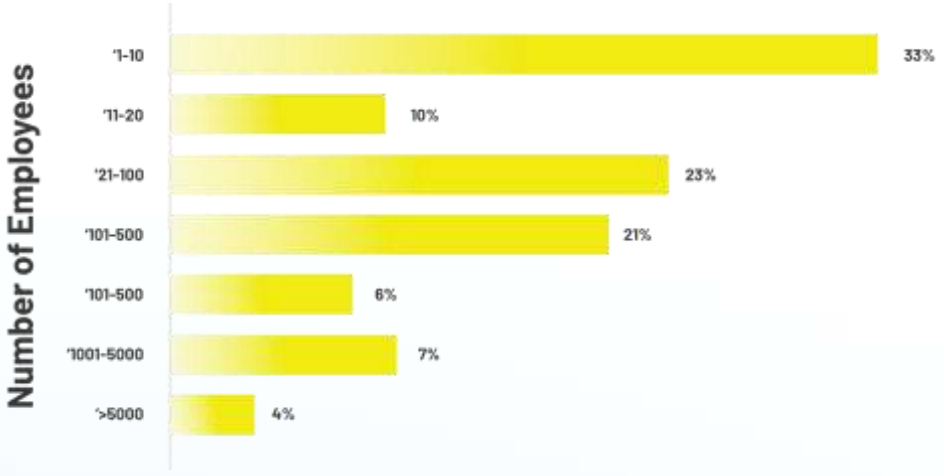
CRI lanzó el Programa de preparación cibernética en 2017 y lo actualizó en 2020. El programa se centra en el comportamiento humano con información sobre cuatro problemas de ciberseguridad clave para ayudar a las pymes a desarrollar políticas y procedimientos, y formar a sus empleados. Estos "cuatro pilares" siguen siendo relevantes para las pymes.

1. Contraseñas: cuatro de cada cinco filtraciones se producen por contraseñas poco seguras o robadas[2]
2. Actualizaciones de software: el 60 % de las víctimas de ataques dijeron que el ataque se produjo por una vulnerabilidad conocida no corregida en la que no se aplicó el parche correspondiente.[3]
3. Suplantación de identidad (phishing): algo más de uno de cada cuatro empleados (el 26 %) admitió haber sido víctima de una estafa de phishing en el trabajo en los últimos 12 meses, una cifra ligeramente superior al 25 % de 2020.[4]
4. Medios extraíbles/USB: las amenazas capaces de propagarse a través de USB o de atacar específicamente medios USB para una infección inicial, aumentaron del 19 % de 2019 al 52 % de 2021.[5]

El Programa de preparación cibernética se ha traducido al español, portugués, francés, árabe, japonés y ruso para facilitar el acceso a las pymes de todo el mundo.

En octubre de 2020, CRI amplió el Programa de preparación cibernética con el Programa de certificación de liderazgo en ciberseguridad. Es un programa de gestión cuyo objetivo es mejorar la capacidad de los empleados de las pymes de crear y mantener una cultura de ciberseguridad en su organización. Este programa más detallado enseña a los usuarios a gestionar a las personas, los procesos y la tecnología fundamentales para proteger su organización.

De estas pymes, el 33 % tiene entre 1 y 10 empleados, el 10 % tiene entre 11 y 20, el 23 % tiene entre 21 y 100, el 21 % tiene entre 101 y 500, el 6 % tiene entre 501 y 1000, el 7 % tiene entre 1001 y 5000 y el 4 % tiene más de 5000.



[2] https://www.verizon.com/business/resources/reports/dbir/
[3] Estudio de Ponemon sobre las brechas en la respuesta a las vulnerabilidades - ServiceNow
[4] **Tessian - Understand The Mistakes That Compromise Your Company's Cybersecurity**
[5] Case Study_SMX_Pulp and Paper 2_Cybersecurity_Honeywell (honeywellforge.ai)

Hasta la fecha, casi 5000 pymes de 178 países se han inscrito en estos programas, con una representación de más de 90 sectores específicos. El mapa de arriba muestra el alcance global de las inscripciones y asociaciones del programa de CRI. La mayoría de las inscripciones correspondientes a pymes son organizaciones con menos de 100 empleados. Está claro que CRI está llegando al público objetivo.

Guías

Desde 2017, CRI ha publicado 25 guías para pymes sobre temas como la autenticación multifactor (MFA), MSP, telemedicina y trabajo híbrido, entre otros muchos. Estas guías son recursos fáciles de utilizar sobre temas en los que se ha demostrado que las pymes tienen lagunas de conocimiento.

Redes sociales

El contenido y los recursos únicos de CRI publicados en Twitter, LinkedIn, Facebook e Instagram han llegado a más de siete millones de personas, generando cerca de 350.000 interacciones y atrayendo a 118.000 personas al sitio web en busca de más información.

Estos logros son solo una parte del trabajo de CRI en los últimos cinco años y han proporcionado ideas claras sobre los pasos siguientes. Por ejemplo, a pesar de las casi 5000 inscripciones, solo 1390 pymes han completado nuestros programas. Está claro que, debido a la poca concienciación, la falta de orientación para la implementación y la ausencia de los incentivos adecuados, las pymes tardan en adoptar las políticas y procedimientos disponibles para mejorar su seguridad.

Hoja de ruta de CRI

CRI contempla la mejora de la resiliencia y la preparación de las pymes globales como una carretera con tres carriles, todos moviéndose a la misma velocidad y en la misma dirección. En cada uno de estos carriles, CRI ha identificado acciones específicas para ayudar a las pymes de todo el mundo. Estas son:

Concienciación

Mejorar los conocimientos y la comprensión que tienen las pymes sobre las ciberamenazas relacionadas con la continuidad del negocio y las prácticas recomendadas.

3. Alcance global: garantizar que los recursos de CRI lleguen a las pymes de todo el mundo mediante la asociación con organizaciones de ámbito global

4. Desarrollo e intercambio de datos: recopilar y publicar información única, no específica de ningún proveedor

Implementación

Ayudar a las pymes en la implementación de políticas y procedimientos cibernéticos para crear una cultura de preparación cibernética centrada en el comportamiento humano

3. Estándares de preparación cibernética: desarrollar y ampliar el Programa de preparación de CRI como base para un proceso de certificación estándar para las pymes que sea reconocido y respaldado por los miembros de CRI y las industrias globales

4. Red mundial de formación: establecer una red mundial de instructores de ciberseguridad cualificados

Incentivos

Explorar los mecanismos para incentivar a las pymes para que mejoren su resiliencia empresarial y su preparación cibernética

- Seguro cibernético: reunir información de las pymes para compartirla con la industria convirtiéndonos en la voz autorizada para las pymes
  - Desarrollar directrices para que las pymes seleccionen la cobertura más adecuada para su organización
  - Ayudar a las pymes a proporcionar pruebas de su preparación cibernética para abordar adecuadamente los riesgos
    - Describir los futuros modelos de negocio para los mercados de seguros
  - Proveedor preferido: implementar el Programa de preparación cibernética con proveedores de segundo y tercer nivel a lo largo de las cadenas de suministro globales para que las pymes obtengan una ventaja competitiva con su certificación.
    - Examinar cómo nosotros, con nuestros miembros y socios, podemos utilizar recompensas monetarias

Dado que las pymes representan aproximadamente el 99 % de empresas en países de la Organización para la Cooperación y el Desarrollo Económicos (OCDE),[1] estas acciones fortalecerán las cadenas de suministro globales desde sus cimientos al abordar las lagunas de conocimientos básicos y recursos para crear una red global de pymes más preparadas para el ciberespacio y más resilientes.

Concienciación

Un problema que surgió una vez más en las conversaciones con las partes interesadas fue la falta general de concienciación sobre el riesgo al que se enfrentan las pymes si no mejoran sus políticas y procedimientos básicos de ciberseguridad. Más de la mitad de los propietarios de pequeñas empresas encuestados por CNBC afirmaron que no les preocupaba que su empresa fuera víctima de un ciberataque. Este punto de vista deja claro que existe un vacío de conocimientos[1]. Es comprensible, ya que la mayoría de las pymes se centran en el trabajo diario necesario para llevar un negocio con recursos limitados y les queda poco tiempo para estar al tanto de las sorprendentes cifras sobre los últimos ataques cibernéticos o para consultar los estándares técnicos. Por lo tanto, CRI tiene la oportunidad y el permiso del mercado para establecerse como la "fuente de referencia" en materia de ciberseguridad para las pymes, con recursos GRATUITOS centrados en temas cibernéticos clave, todo ello en un solo lugar. Para aumentar la concienciación sobre los problemas cibernéticos clave entre las pymes será fundamental centrarse en crear alianzas con las organizaciones globales y proporcionar datos relevantes e imparciales.

Alcance global

Las futuras campañas de concienciación y alcance específico de CRI deben seguir centrándose en las pymes de fuera de Norteamérica. Este enfoque internacional concuerda con la naturaleza global de las cadenas de suministro digitales y proporciona información sobre las realidades de operar en diferentes regiones. Con más recursos de CRI disponibles para más pymes en África y Sudamérica, aumentará la concienciación global sobre cuestiones de preparación y resiliencia cibernética. Para llegar de manera eficaz a estas regiones diferentes, CRI abordará sus esfuerzos de contratación y asociación con las organizaciones y pymes apropiadas que operan en estos países. Esta representación proporcionará nuevas perspectivas a nuestro proceso actual de desarrollo de recursos y ayudará a CRI a enviar un mensaje elocuente a las diferentes culturas. La traducción continua de los programas de formación y otros recursos de CRI es clave para el éxito de este alcance global. Los futuros esfuerzos de traducción vendrán determinados por las necesidades de nuestros miembros y socios para permitir que nuestros recursos den a conocer los problemas de ciberseguridad en todo el mundo.

Desarrollo e intercambio de datos

Una brecha importante que CRI ha identificado en la mejora de la concienciación sobre la ciberseguridad entre las pymes globales es la despreocupación por las consecuencias. Estas pymes a menudo no comprenden las consecuencias que puede tener en sus negocios no mejorar su higiene cibernética básica. Cuando las pymes y otros profesionales del sector de la ciberseguridad buscan datos, a menudo se encuentran con resultados de proveedores que intentan vender un producto. Reforzar las credenciales de CRI como una fuente fiable de datos independiente de cualquier proveedor entre las pymes ayudará a aumentar la adopción de nuestro programa. Al recopilar datos únicos de nuestros programas, realizar encuestas y aprovechar los recursos de nuestros miembros, CRI pretende cuantificar y comunicar mejor el efecto de un suceso relacionado con la ciberseguridad a las pymes.

Implementación

Ofrecer a las pymes recursos para mejorar su preparación cibernética es solo una parte del desafío. Los empleados son cada vez más conscientes del impacto de su comportamiento en la seguridad: el 36 % de los empleados cree que, en los últimos 12 meses, ha cometido un error en el trabajo que ha puesto en peligro la seguridad. Sin embargo, no logran saber cómo evitar el mismo error la próxima vez sin políticas y formación adecuadas. Al comprender los desafíos a los que se enfrentan las pymes, CRI debe crear mecanismos para mejorar la preparación cibernética sin crear confusión o trabajo innecesario ni agotar los recursos. Con la realización de iniciativas piloto con nuestros miembros y socios, arrojamos luz sobre un aspecto clave: un enfoque paso a paso sumamente personalizado es la forma más eficaz de lograr que las pymes completen el Programa de preparación cibernética, que incluye características clave de políticas y procedimientos cibernéticos, y planes de respuesta a incidentes. CRI tiene previsto ampliar esta capacidad, interactuando de cerca con las pymes mientras trabajan para mejorar su seguridad cibernética con un estándar básico y una red global de instructores de ciberseguridad cualificados.

Estándares de preparación cibernética

Los estándares, las regulaciones, las tecnologías y otros aspectos clave de la ciberseguridad avanzan a un ritmo vertiginoso y la mayoría de las pymes no están preparadas para mantenerse al día. Pero ¿de verdad es necesario? En lugar de ello, CRI debe establecer un conjunto básico de políticas y procedimientos que las pymes puedan implementar para demostrar su preparación cibernética. Estas políticas ofrecen a las pymes un punto de partida en su viaje, algo que a menudo les cuesta encontrar. Una vez satisfecho, el estándar de CRI ofrecerá a los clientes, socios de la cadena de suministro, aseguradoras y otras partes interesadas la garantía de que una empresa está preparada para el ciberespacio. El desarrollo de estas políticas y procedimientos requiere una estrecha colaboración pública y privada, así como aportaciones directas de las pymes para garantizar su viabilidad y eficacia. El actual Programa de preparación cibernética de CRI y el proceso de certificación asociado servirán como punto de partida para un proceso escalable en el que las pymes puedan trabajar con instructores de ciberseguridad aprobados por CRI. Conforme el estándar evolucione con el tiempo, ampliaremos nuestros programas y materiales para incluir temas como la gestión de vulnerabilidades y otras cuestiones identificadas como vitales para mejorar la ciberseguridad de las pymes.

Red mundial de formación

Para aumentar los porcentajes de finalización y la eficacia general del programa, CRI tiene la intención de desarrollar una red global de instructores de ciberseguridad cualificados. Usando y ampliando el éxito obtenido de la asociación de CRI con Cyber Hawaii, CRI formará a personas en áreas geográficas locales para ayudar a las pymes a avanzar en su viaje de preparación cibernética y verificar que el programa se ha completado con éxito. Esta red de soporte localizada ayudará a CRI a personalizar las necesidades de las pymes afectadas, lo que permitirá que los socios globales trabajen a través de los programas de CRI a su propio ritmo. Este enfoque tiene dos propósitos: ayudar a las pymes a través del programa y verificar externamente la finalización del programa para que CRI otorgue la certificación. Además, el desarrollo de esta red fortalecerá los equipos de trabajo y ampliará el conjunto de recursos para futuras iniciativas.

Incentivos

Aumentar la concienciación y ofrecer apoyo para la implementación es necesario, pero no suficiente, para ayudar a las pymes a invertir en su preparación y mantener su resiliencia. Los incentivos financieros, y posiblemente los desincentivos, han demostrado ser mecanismos eficaces que tienen un efecto en las prácticas y procedimientos de ciberseguridad. Según una encuesta de 2021 realizada por CRI, solo el 21 % de las pymes cree que el tiempo y el dinero que invierte su organización en ciberseguridad reducirá el riesgo[1]. A medida que buscamos mejorar la preparación cibernética de las pymes, debemos ofrecer más enfoques nuevos para aumentar la seguridad y la protección de la marca. Dos áreas, el seguro cibernético y el estatus de proveedor preferido, surgieron como incentivos favorables en nuestras conversaciones con las partes interesadas clave.

Seguro cibernético

Las pymes generalmente no cuentan con las personas, los procesos y las tecnologías para desarrollar los sólidos programas de seguridad necesarios para optar a un seguro cibernético. Muchas aseguradoras tampoco conocen la realidad de dirigir una pequeña empresa. Esto ha creado una situación cada vez más confusa tanto para las aseguradoras como para las pymes que buscan la póliza adecuada a sus necesidades. Para aclarar esta confusión, CRI debe aprovechar nuestra capacidad de convocar a las partes interesadas para identificar las lagunas de conocimiento y desarrollar material para subsanarlas. Para ello, es necesario que CRI proporcione a las pymes orientación para la selección de pólizas y trabaje con las aseguradoras para crear descuentos u otros incentivos financieros que alienten a las pymes a adoptar prácticas cibernéticas robustas.

Estatus de proveedor preferido

A medida que continuamos estableciendo el Programa de preparación cibernética como estándar para la "higiene cibernética", CRI quiere ofrecer a las pymes la capacidad de demostrar su preparación cibernética a sus socios. CRI aprovechará nuestra capacidad de convocatoria, colaborando con nuestros miembros y socios para ayudar a establecer un estatus de proveedor preferido para proveedores de segundo y tercer nivel, y luego ayudar a las pymes a lograr ese estatus. Además, CRI determinará si ofrecer incentivos monetarios puede aumentar la adopción de este estándar de preparación cibernética.

Mirando hacia el futuro

Para seguir cumpliendo la misión de CRI establecida hace cinco años, debemos seguir desempeñando un papel de liderazgo para las pymes como su voz e intérprete en cuestiones cibernéticas clave. Aprovechando una vez más la experiencia de nuestros miembros y socios, CRI pretende convertirse en el primer destino para las pymes que quieren mejorar su preparación cibernética centrándose en el comportamiento humano y quieren conocer los procedimientos esenciales para reducir los ciberataques.

Esta hoja de ruta que aborda la preparación cibernética de las pymes describe lo que CRI y nuestros socios deben hacer para apoyar a las pymes globales. Al planificar el futuro, es importante reconocer la magnitud de los problemas actuales a los que se enfrentan no solo las pymes, sino también las organizaciones de todos los sectores y tamaños. Por consiguiente, CRI cree que nuestro camino hacia el éxito se basa en los principios de asociaciones estrechas, desarrollo y retención de los empleados y soluciones tecnológicas accesibles.

Asociaciones

Las instituciones públicas y privadas de todo el mundo necesitan abrir las líneas de comunicación centrándose más en la colaboración y no en la competencia. Compartir datos, prácticas recomendadas, políticas eficaces y lecciones aprendidas es clave para mejorar el ecosistema general para las pymes.

Desarrollo y retención de los empleados

El crecimiento de la fuerza laboral global de ciberseguridad proporciona un mayor grupo de talentos, lo que pone a disposición de las pymes empleados más capacitados. Proporcionar el conocimiento adecuado sobre cómo retener esta fuerza laboral garantizará la continuidad y resiliencia en las operaciones comerciales globales.

Soluciones tecnológicas accesibles

Las pymes se benefician enormemente del avance de herramientas y sistemas asequibles y fáciles de usar para gestionar su posición de riesgo. Desarrollar estas tecnologías requerirá inversiones centradas en las necesidades reales de ciberseguridad de las pymes y no simplemente en otra característica más que vender.

Dado que muchas organizaciones ya están trabajando para adoptar estos principios, CRI seguirá esforzándose en convertirse en una voz para las pymes a escala mundial en temas cibernéticos clave, representando su punto de vista con responsables de la toma de decisiones clave para garantizar que se consideren sus necesidades.