CLAIN 2016

Asunción, Paraguay 19 y 20 de mayo. Hotel Excélsior

"Gobierno Corporativo, Gestión de Riesgos y Auditoría, un enlace que asegura el éxito organizacional"

ASOCIACIÓN DE BANCOS DEL PARAGUAY

Riesgos emergentes en el Sistema Financiero

Jorge Dávalos Campos Cervera

Intendente de Riesgo Operacional
Superintendencia de Bancos
Banco Central del Paraguay

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

JORGE D. DÁVALOS CAMPOS CERVERA

- Intendente de Riesgo Operacional y Tecnológico de la Superintendencia de Bancos del Banco Central del Paraguay.
- Jefaturas en la Gerencia de Tecnología del Banco Central de Paraguay.
- Profesor Titular de Auditoría Informática de la carrera Ingeniería Informática de la Facultad Politécnica de la Universidad Nacional de Asunción desde el año 2015 hasta la fecha. Docente desde al año 1993 hasta la fecha.
- Profesor en la Universidad Americana varios años.
- Asistencia permanente a Congresos y Seminarios tanto a nivel nacional como internacional.
- Entrenamiento permanente en la Reserva Federal de los EEUU, ASBA, FDIC, CEMLA, etc.

Introducción

Conferencia dedicada a:

- Ejecutivos,
- Directores,
- Gerentes de Riesgos,
- Auditores,
- Oficiales de Seguridad,
- Gerentes de Tecnología.

Introducción o antecedentes

- *¿Porqué ésta conferencia podría interesarle a estas personas?*

A los Directores, Ejecutivos, Gerentes Generales, porque deben comprender que los profesionales responsables de las áreas operativas conocen de lo que hablan y que se espera que ellos sean los que avalen los proyectos y medidas propuestos por aquellos.

Deben involucrarse en los proyectos de la compañía, comprenderlos lo mejor que puedan y acompañar de cerca el desarrollo e implementación de los mismos.

Introducción o antecedentes

- *¿Porqué ésta conferencia podría interesarle a estas personas?*

Los Gerentes de Riesgos deberán gestionar con mucha energía y responsabilidad los riesgos conocidos y los residuales.

Deberán generar las sinergias con las distintas áreas de negocio a fin de recabar toda la información necesaria sobre eventos de pérdidas que se produzcan en la compañía.

Deberán requerir los recursos necesarios para desarrollar su actividad de manera a aportar valor a la compañía y no ser un mero elemento de cumplimiento regulatorio.

Introducción o antecedentes

- *¿Porqué ésta conferencia podría interesarle a estas personas?*

Los Auditores deben convencerse que sus controles son cruciales para la compañía, además de ser un apoyo invalorable para las demás áreas de la empresa.

Además de sus tareas de control interno, deben ser sponsors de los reclamos de RRHH y recursos tecnológicos de las demás áreas que lo reclaman.

Deben involucrase tempranamente en el análisis de nuevos proyectos de modo a aportar valor a la compañía.

Introducción

- *¿Porqué ésta conferencia podría interesarle a estas personas?*

A los Oficiales de Seguridad porque son responsables por el aseguramiento físico y lógico (en muchos casos) y deben comprender que sus funciones no están supeditadas a controles rutinarios de perfiles de acceso de usuarios o control de rondas de guardias de seguridad.

Sus actividades pueden abarcar tanto como sus recursos tecnológicos y humanos se lo permitan.

Su tarea es de tiempo completo y para aportar valor a la compañía deben establecer alianzas internas y externas a la organización.

Introducción o antecedentes

- *¿Porqué ésta conferencia podría interesarle a estas personas?*

Les motivará a desarrollar el conocimiento necesario para gestionar la seguridad de su compañía de manera integral.

Les obligará a capacitarse respecto a la tecnología sujeta a su control.

Les impulsará a tomar mayor protagonismo en las decisiones que involucren cuestiones de seguridad.

Finalmente se obtendrá el "seniority" que se espera que todo responsable de área tenga para defender sus posiciones ante los ejecutivos de la compañía.

Introducción o antecedentes

- *¿Porqué ésta conferencia podría interesarle a estas personas?*

A los Gerentes de Tecnología porque comprenderán que deben tomar protagonismo en las decisiones que se tomen en la compañía.

Deben formar parte activa de los Comités de Tecnología, los que deben estar formados por personas con poder de decisión.

Defenderán su posición en el organigrama de la compañía, posición que deberá reflejar independencia respecto de las demás áreas operativas.

Entenderán que deben contar con conocimiento acabado de las múltiples operativas de la compañía para las que presta o prestará servicios.

Introducción o antecedentes

- *¿Porqué ésta conferencia podría interesarle a estas personas?*

Comprenderán que no es conveniente ser considerado amos y señores de la tecnología, datos e información de la compañía.

Que la segregación de funciones, por mas que "retrase" la solución de muchas situaciones, es saludable y necesaria.

Comprenderán que la segregación de funciones no es sinónimo de pérdida de poder en la organización.

Finalmente se obtendrá el "seniority" que se espera que todo responsable de área tenga para defender sus posiciones ante los ejecutivos de la compañía.

Introducción o antecedentes

- *¿Cuáles* son los beneficios que obtendrá la gente de escucharlo a Ud.?

Si bien hablar de beneficios suena un tanto pretencioso, estimo que nuestra comunidad se ve fortalecida con este tipo de eventos donde cada participante aporta la experiencia obtenida en su campo laboral.

En mi caso particular, dado mi carácter de regulador, tengo la ventaja adicional de conocer distintos tipos de administración, en las que se pueden ver desde las mejores prácticas de los cuadros de trabajo hasta los más notorios ejemplos de intentos de implementación de los requerimientos normativos con el único objetivo de cumplir con la norma.

Agenda

1. Riesgos emergentes en el ecosistema tecnológico.
2. Administración basada en riesgos.
3. Conclusiones.

Riesgos emergentes en el ecosistema tecnológico

Las Entidades Financieras se encuentran permanentemente expuestas a una variedad de escenarios globales, los cuales están gobernados por sus entornos ambientales, socio políticos, tecnológicos, geopolíticos, económicos en los que operan.

Estos escenarios variados sirven para exponer a las organizaciones a una acumulación de riesgos rápidamente cambiantes que deben ser administrados a fin de mitigar las amenazas al funcionamiento de las empresas.

Riesgos emergentes en el ecosistema tecnológico

Contar con las herramientas y capacidades para estar preparados y responder apropiadamente a nuevos desarrollos de estas dimensiones evolutivas y siempre cambiantes, es crucial para todos los sectores de la industria, pero especialmente para el sector financiero.

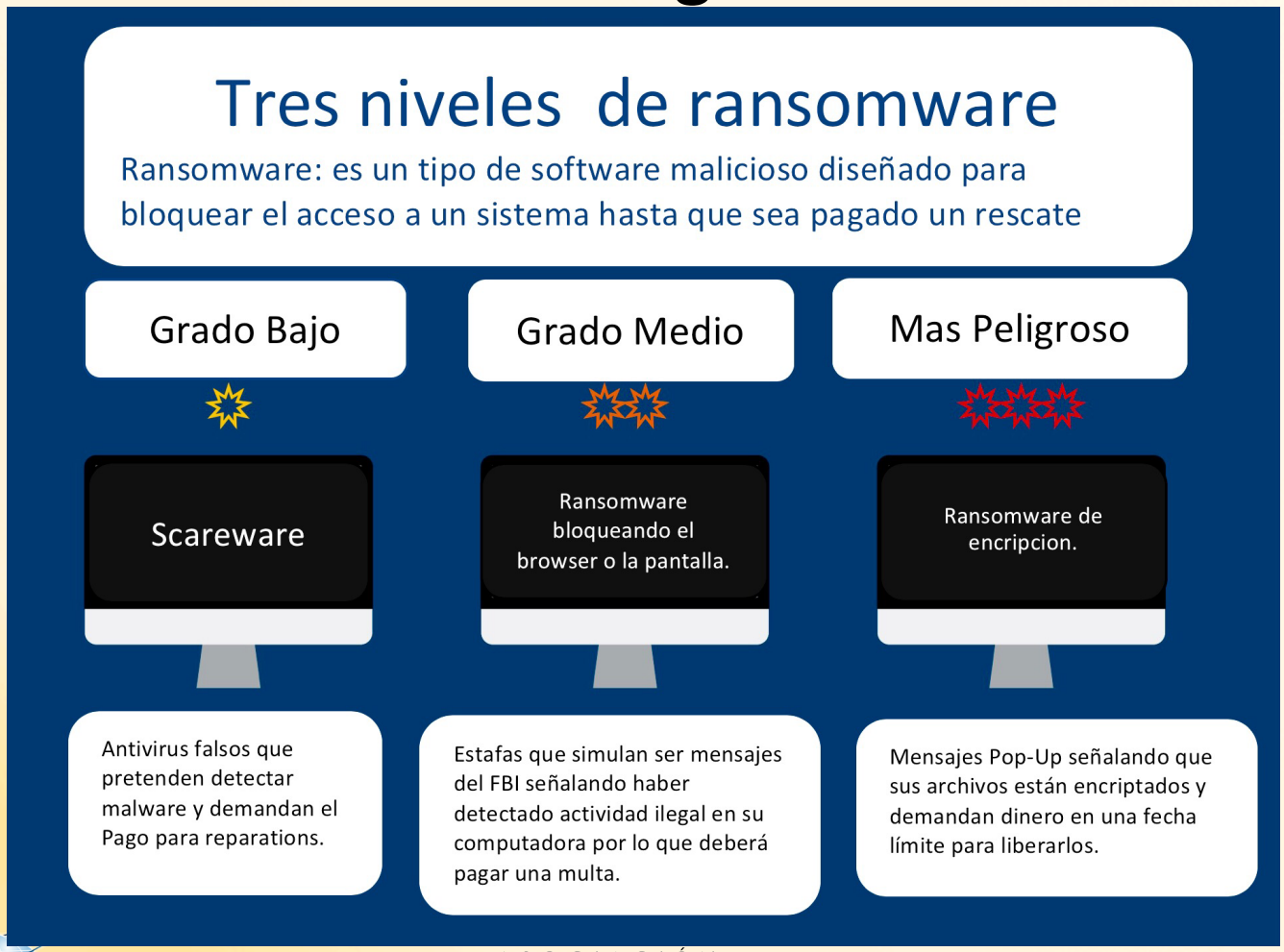
Riesgos emergentes en el ecosistema tecnológico

Según el analista de fraudes del grupo de investigación de Gartner, **Avivah Titán**, "La **ciber extorsión** y los **insiders** en las compañías, actuando como agentes libres, son las mayores amenazas de seguridad de TI enfrentadas por las Entidades Financieras en el 2015."

Sin embargo no sólo, las Entidades Financieras están siendo atacadas por la **ciber extorsión** y **ciberataques de ransomware**, muchas empresas minoristas, empresas de salud e instituciones del gobierno están bajo la misma amenaza

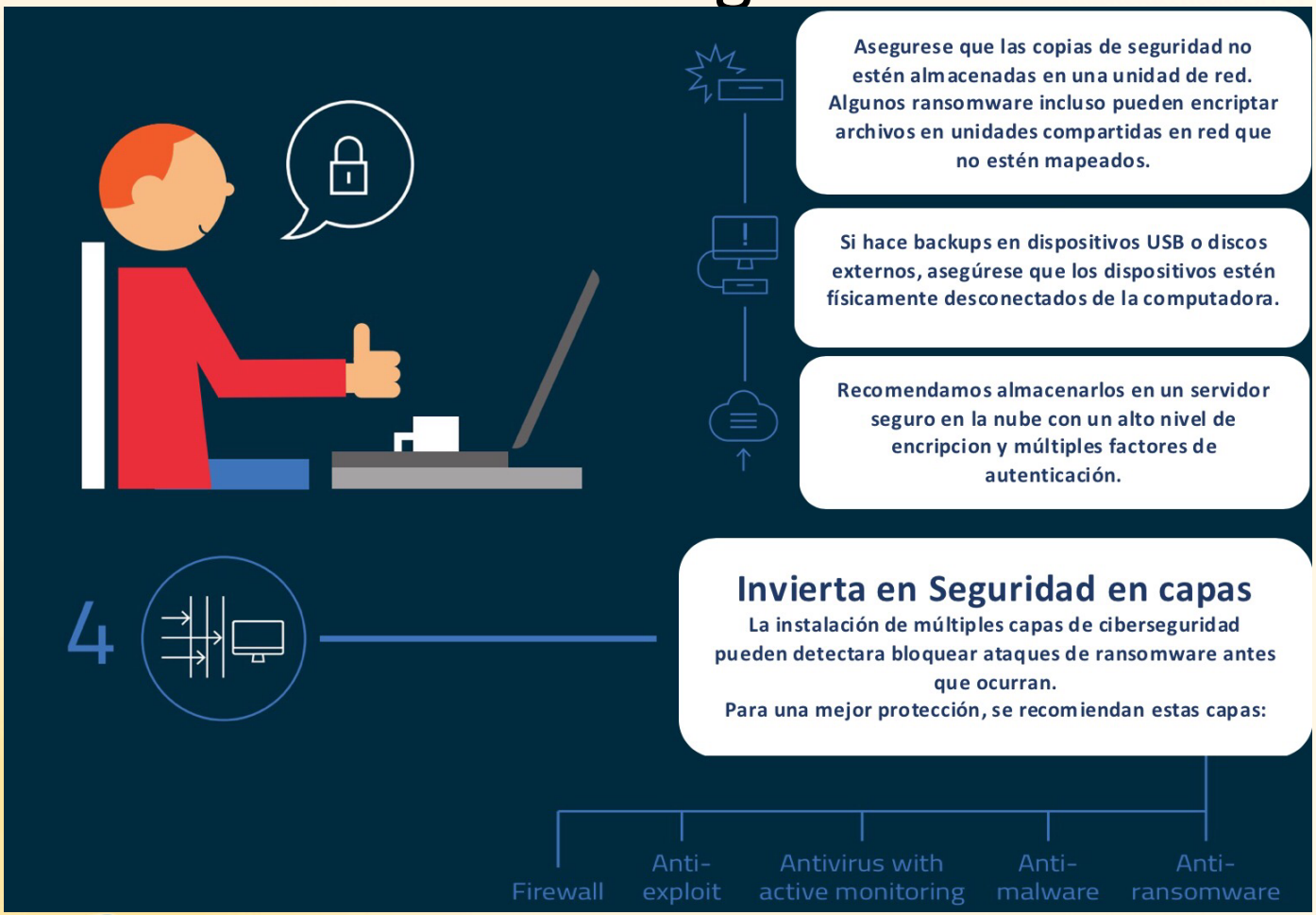
Riesgos emergentes en el ecosistema tecnológico

Riesgos emergentes en el ecosistema tecnológico



Riesgos emergentes en el ecosistema tecnológico

Riesgos emergentes en el ecosistema tecnológico



Riesgos emergentes en el ecosistema tecnológico

- **Ciber extorsión en aumento.**

El grupo ciber criminal **DD4BC** ha estado usando una mezcla de esquemas de ransomware con denegación de servicio distribuido (DDoS) contra números Instituciones Financieras.

Según el reporte de amenazas DDoS de **NSFOCUS** del 2014 el 90% de los ataques DDoS duraron menos de 30 min., un ataque duró 70 horas.

Estas estrategias de ataques más cortos están siendo empleadas para mejorar la eficiencia, así como distraer la atención del personal de TI de la intención real del ataque, que es desplegar malware y robar datos.

Riesgos emergentes en el ecosistema tecnológico

- **Como funcionan los ataques de ciber extorsión en el sistema financiero.**

El esquema de ciber extorsión de **DD4BC** ha causado costosos daños a las instituciones financieras.

Estos ciber criminales plantan malwares en las redes corporativas, extraen información financiera de los clientes y luego amenazan a las instituciones con hacerlas públicas.

Puesto que estos grupos de extorsión, como **DD4BC**, típicamente demandan el pago en Bitcoins, se ha vuelto cada vez más difícil para los organismos de seguridad rastrear y procesar a este tipo de criminales.

Riesgos emergentes en el ecosistema tecnológico

- **Ashley Madison – Violación de datos privados.**

Riesgos emergentes en el ecosistema tecnológico

- **Ashley Madison – Violación de datos privados.**

Este es otro ejemplo reciente de ciberataque ransomware donde el autodenominado grupo cibercriminal "**Impact Team**" hacker el sistema informático del grupo "**Avid Life Media**".

El ataque no fue detectado y los cibercriminales pudieron descargar 300 GB de información financiera y personal de sus 37 millones de usuarios.

La brecha de seguridad también les costó la exposición de más de 30 millones de direcciones de emails, 200.000 correos de la cuenta de gmail del CEO y muchas contraseñas de sus clientes y los últimos 4 dígitos de sus tarjetas de crédito.

Riesgos emergentes en el ecosistema tecnológico

- **Ashley Madison – Violación de datos privados.**

Con la amenaza de exposición 30 días atrás, Avid Life Media escogió continuar normalmente con sus negocios y no bajó los tres sitios mencionados en la amenaza.

Hoy día la violación de datos ha sido catastrófica puesto que ha arruinado la reputación de la compañía e impactado muchas vidas.

Riesgos emergentes en el ecosistema tecnológico

- **Insiders deshonestos**

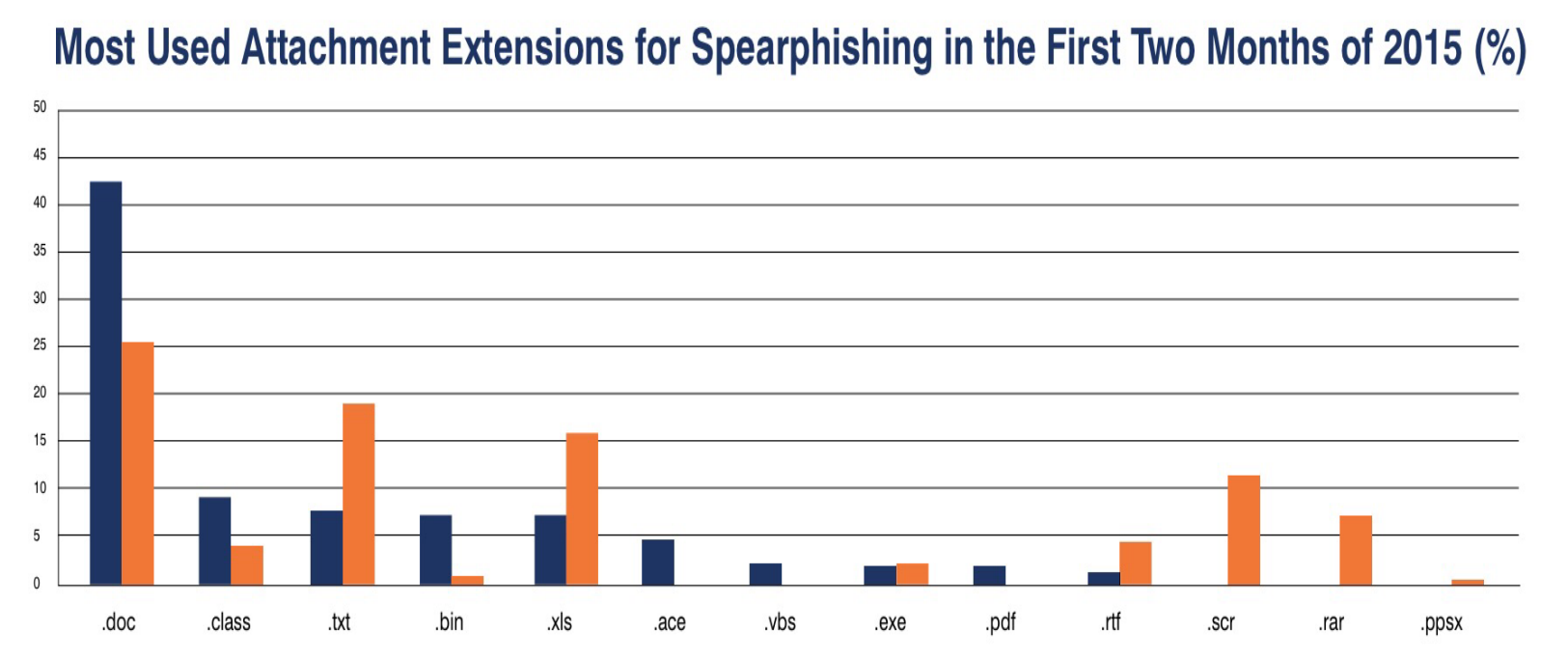
Una tendencia creciente en brechas de seguridad de TI es el incremento de insiders de la compañía operando como agentes libres de los cibercriminales.

Estos son individuos, ya sea empleados actuales o ex empleados, quienes son entrenados para robar y beneficiarse de la venta de datos de clientes en la "Dark Web".

Profesionales de seguridad como John McAfee y el CEO de Avid Life Media tienen la fuerte sospecha que la brecha de seguridad de Ashley Madison fue el resultado de un ex empleado disconforme o uno tercerizado.

Riesgos emergentes en el ecosistema tecnológico

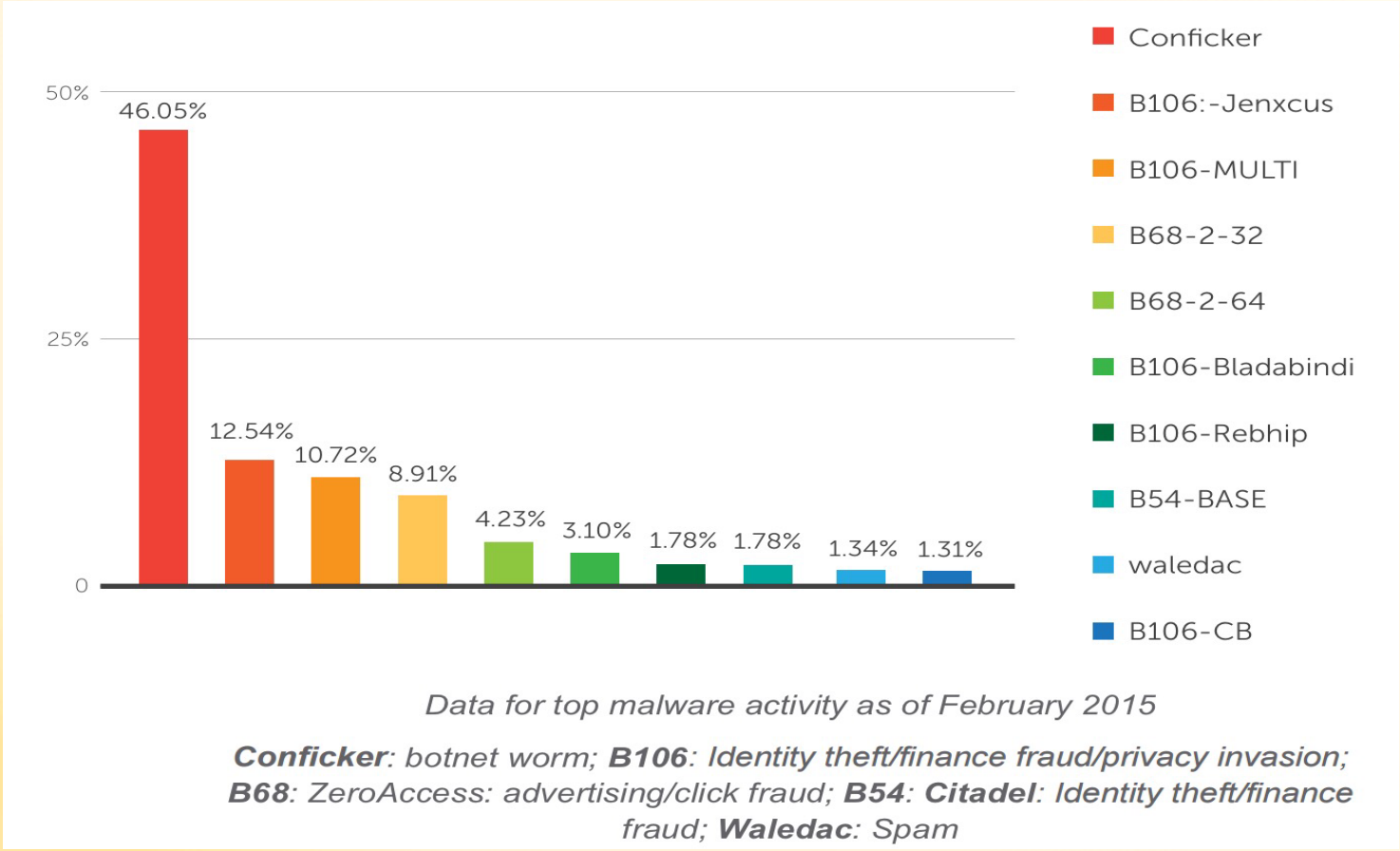
Spear Phishing



Fuente: Proofpoint, Security as a Service provider

Riesgos emergentes en el ecosistema tecnológico

Malwares



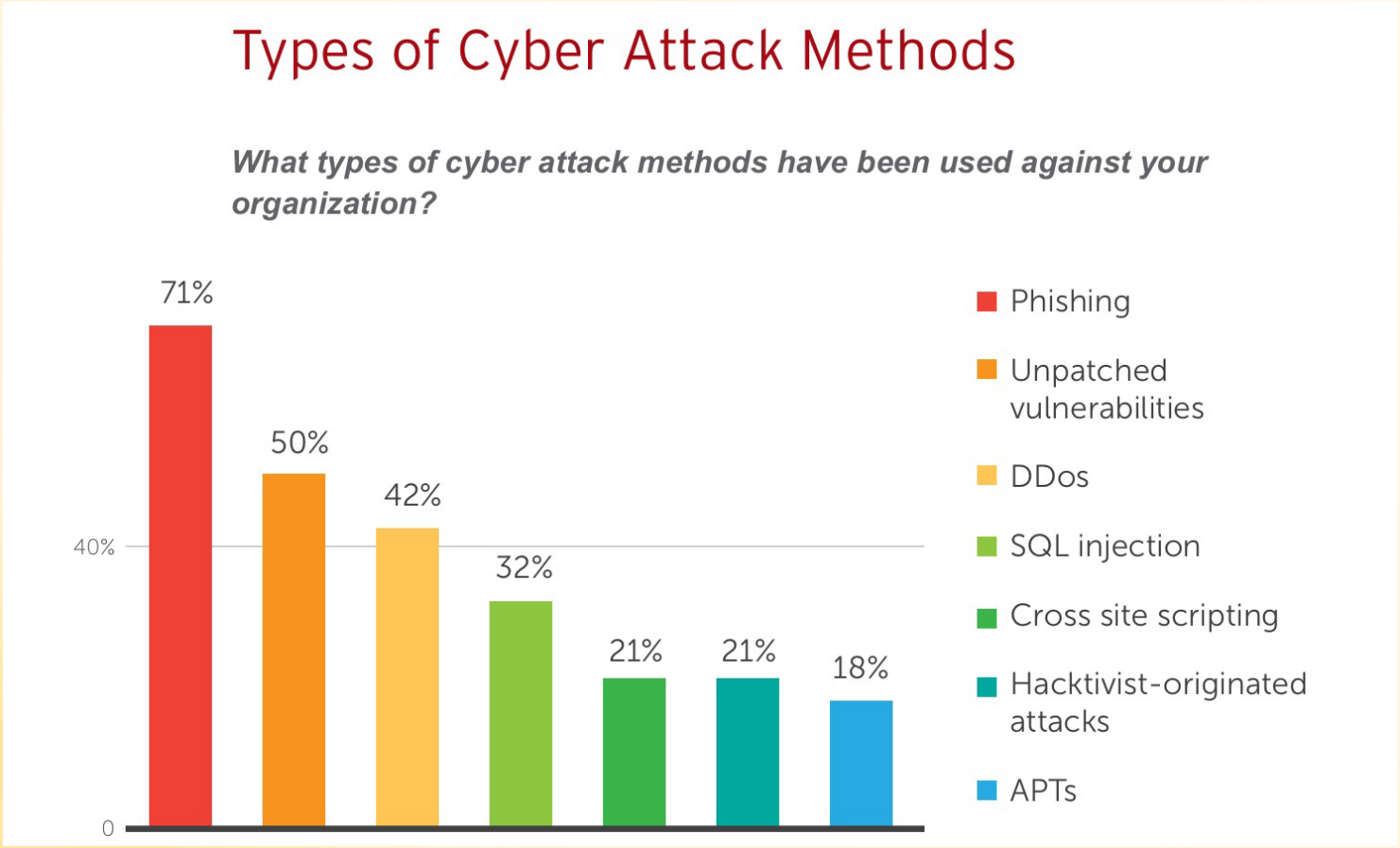
Data for top malware activity as of February 2015

***Conficker**: botnet worm; **B106**: Identity theft/finance fraud/privacy invasion; **B68**: ZeroAccess: advertising/click fraud; **B54**: **Citadel**: Identity theft/finance fraud; **Waledac**: Spam*

Fuente: 2015 Trend Micro Incorporated

Riesgos emergentes en el ecosistema tecnológico

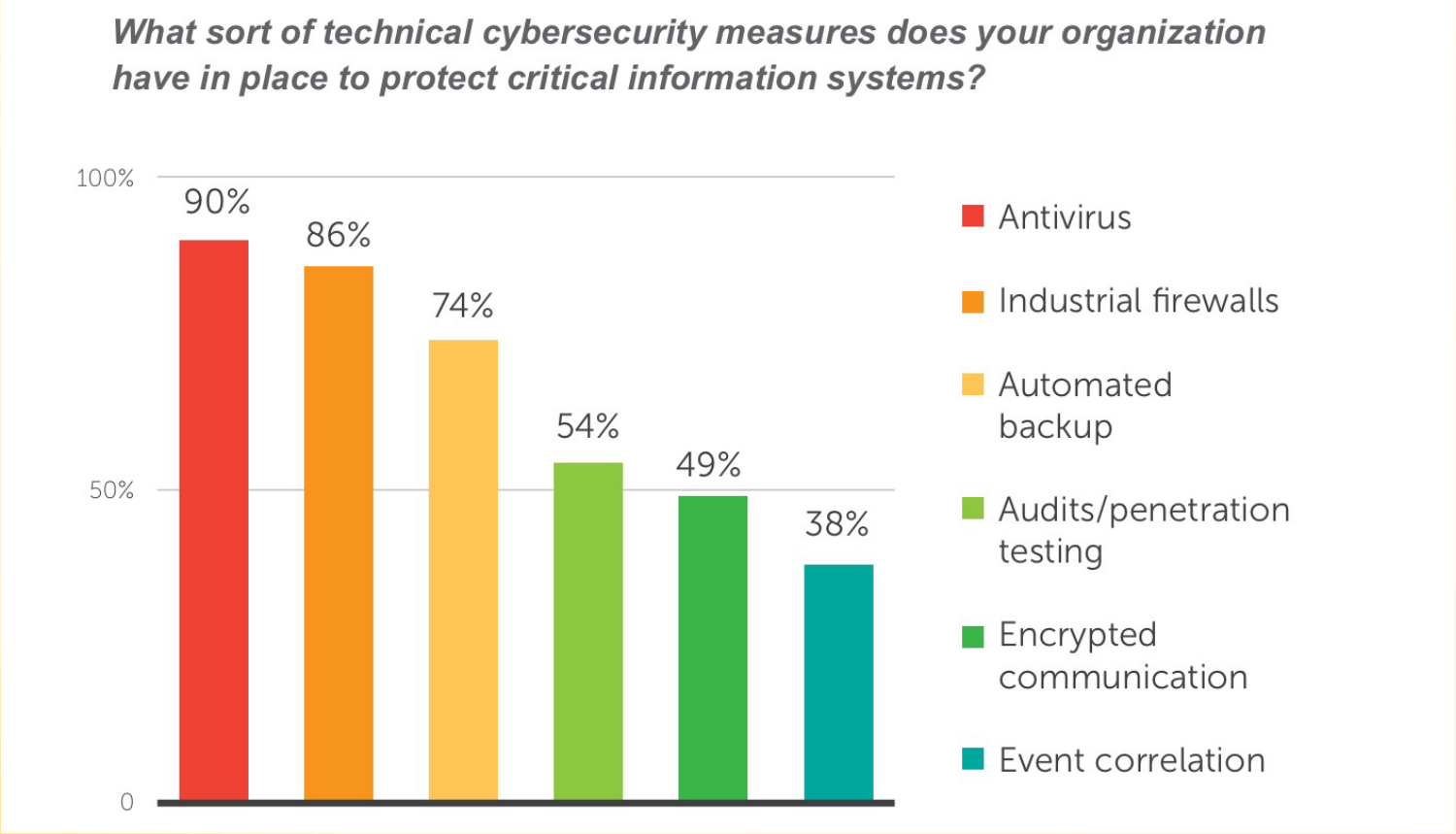
Métodos de ataques



Fuente: 2015 Trend Micro Incorporated

Riesgos emergentes en el ecosistema tecnológico

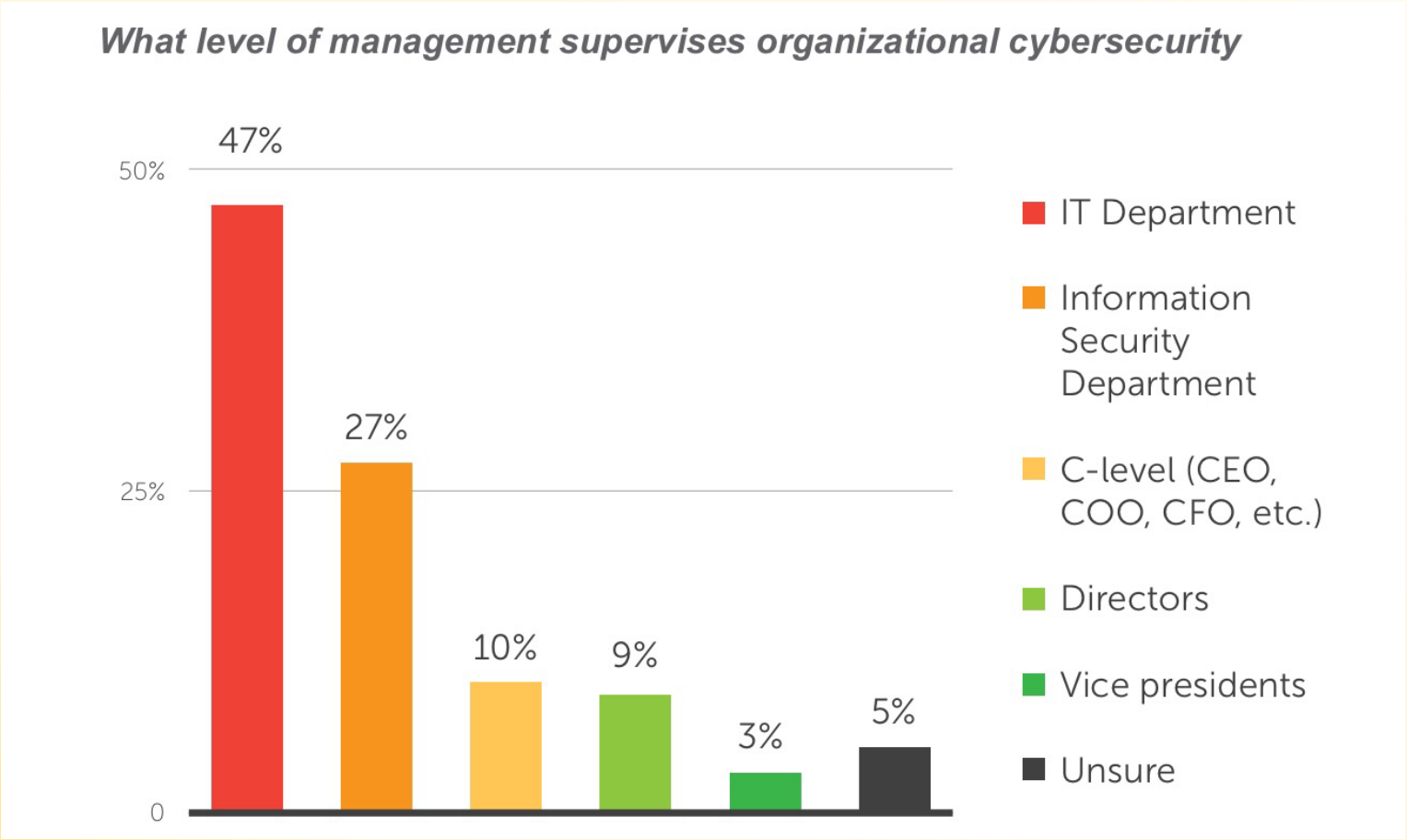
Medidas de ciberseguridad



Fuente: 2015 Trend Micro Incorporated

Resp. de la ciberseguridad

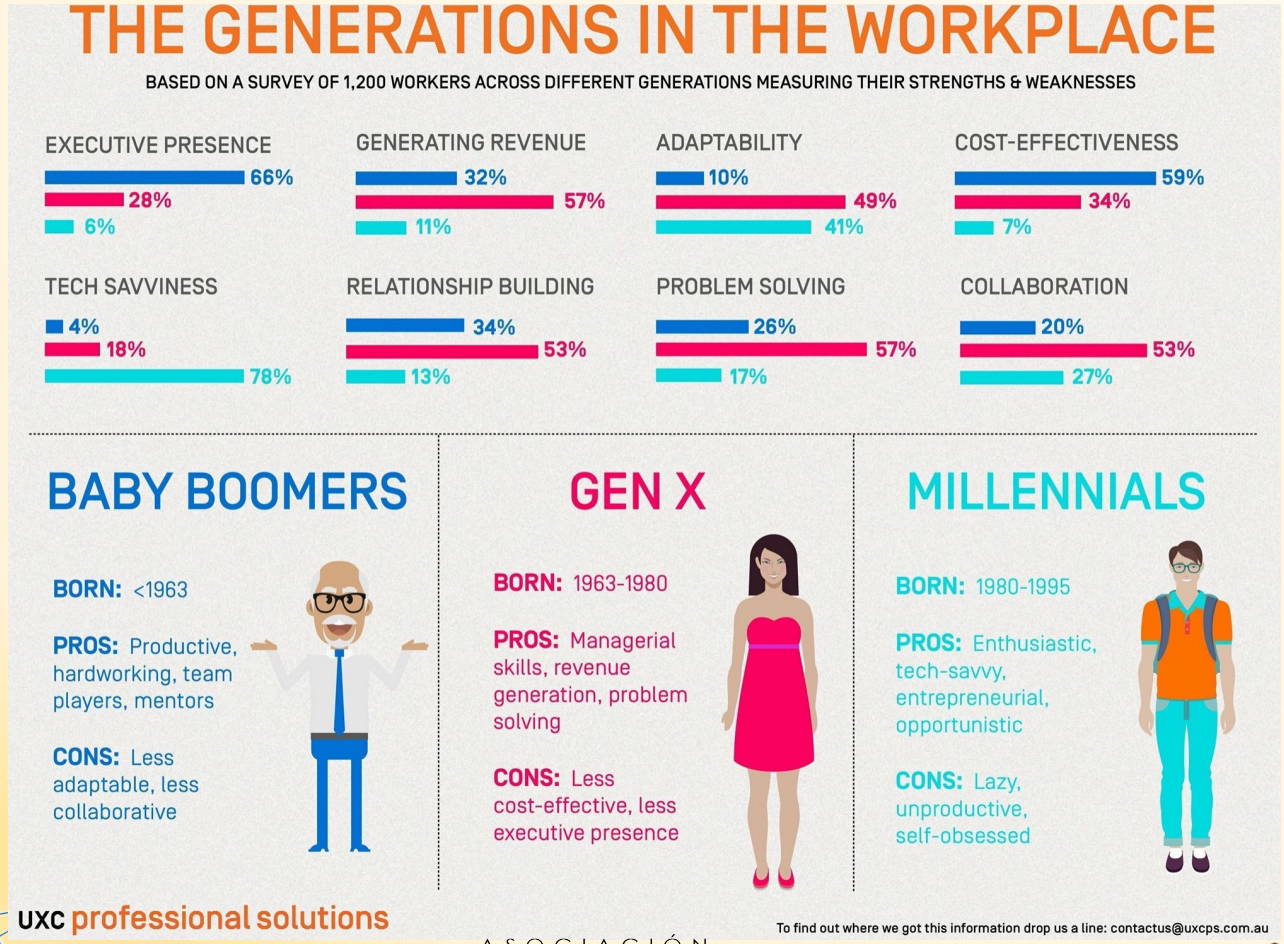
Riesgos emergentes en el ecosistema tecnológico



Fuente: 2015 Trend Micro Incorporated

Riesgos emergentes en el ecosistema tecnológico

Millennials, una bomba de tiempo.



Riesgos emergentes en el ecosistema tecnológico

Millennials, una bomba de tiempo.

http://youtu.be/opRMrEfAIiI

Riesgos emergentes en el ecosistema tecnológico

Millennials, una bomba de tiempo.

Administración basada en Riesgos

Gobierno Corporativo

Seguridad Lógica/Física

Comité de Auditoría

Auditoría Interna

Auditoría Informática

Administración basada en Riesgos

Gobierno Corporativo

Comité de Riesgos

Gerencia de Riesgos

Riesgo Financiero

Riesgo de Crédito

Riesgo Reputacional

Riesgo de Lavado de Dinero

Riesgo Operacional

Riesgo Sistémico

Riesgo Legal

Riesgo Tecnológico

Administración basada en Riesgos

MAPA DE PROCESOS

MATRIZ DE RIESGOS

Conclusiones

- Involucramiento de Ejecutivos
- Rutina de actualizaciones
- Uso de herramientas de seguridad
- Correlación de eventos
- Educación de usuarios/clientes
- Trabajo en equipo – contacto con pares – organizaciones gubernamentales, etc.
- Segregación de funciones (TI, Seguridad, Auditoría, Riesgos)
- Mapa de procesos
- Matriz de riesgos

Información de Contacto

jdavalos@bcp.gov.py
+595-21-6192490
Federación Rusa y Augusto Roa Bastos
www.bcp.gov.py

Muchas Gracias

Por su Atención!