



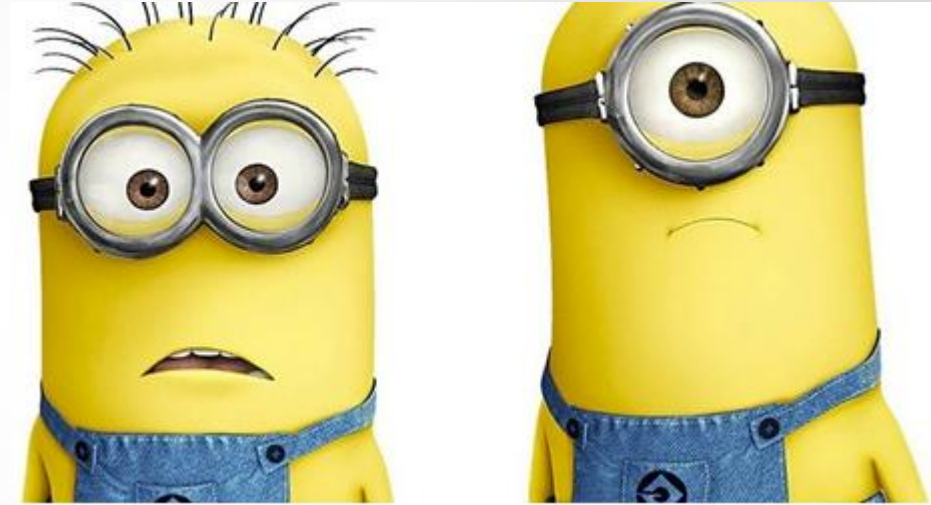
Ciberseguridad & Pymes

Juan Dávila, CISA.CISM,CRISC, ISO 27001 LA, ISO 22301 LA, COBIT 5 Trainer
ISACA Lima Chapter, Presidente

Seminario Miércoles del Exportador - PromPerú
16 de agosto de 2017
Lima, Perú

Reflexiones

- ❖ En serio, ustedes creen que las PYMES están expuestas a los ciberataques?
- ❖ El ser humano es ...



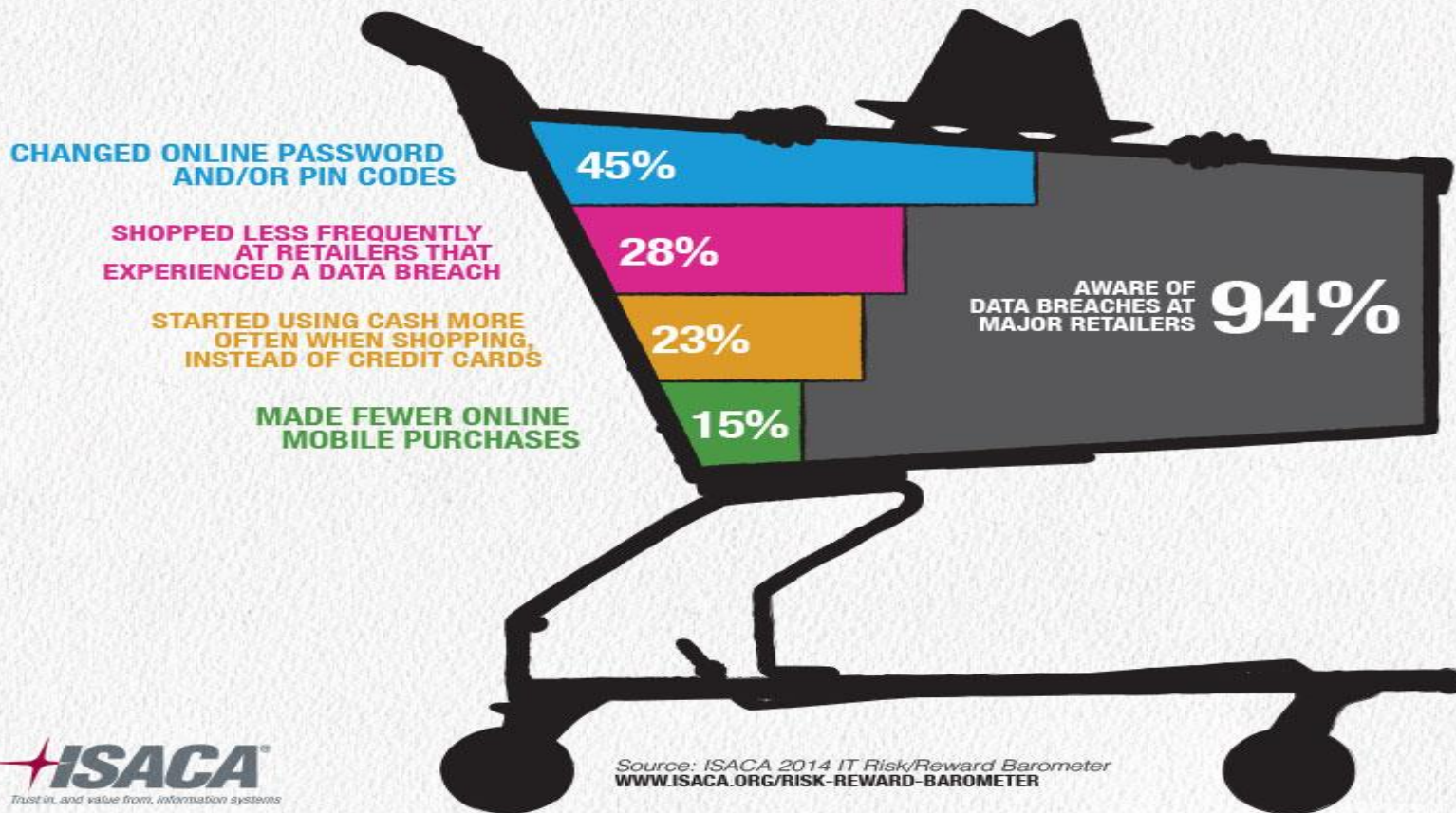
Reflexiones

- ❖ Es increíble cómo nos afectan las tecnologías !!
- ❖ A nivel individual...
- ❖ Organizacional...
- ❖ Nacional...
- ❖ Global?????



DO SHOPPERS CARE ABOUT DATA BREACHES?

Most US consumers are aware of the data breaches at major retailers over the past year. A substantially smaller number changed their shopping behaviors as a result.



El ataque puede venir ...



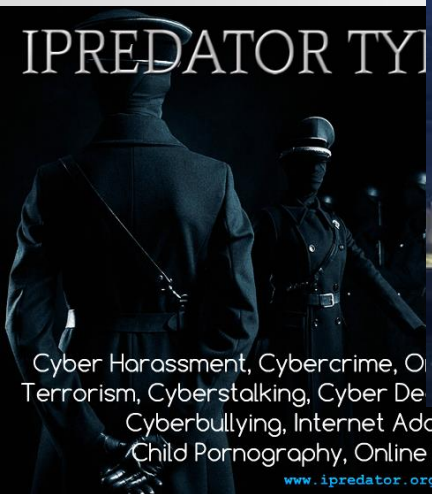
Ciber Ataques – Tendencias

Top 7 Brutal Cyber Attacks

NSA DATA CENTER

300,000,000 Hacking Attempts per Day!

No One is Immune to Hacking



Cyber Harassment, Cybercrime, Online Terrorism, Cyberstalking, Cyber De

Cyberbullying, Internet Addiction, Online Child Pornography, Online Psychopathy

www.ipredator.org

Ciber Incidentes

❖ *“Internet nunca podrá ser seguro”, Vint Cerf.*

Ciberespionaje

Ciberdelincue
ncia

Hacktivismo

Ciberyihadismo

Ciber...

CiberMafia

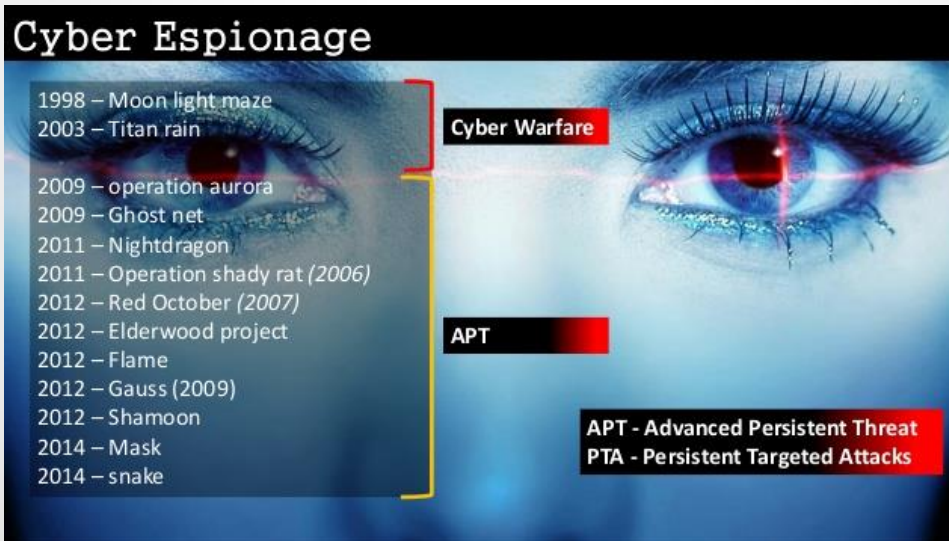
- ❖ Es un modelo de negocio.
- ❖ Cuentan con recursos.
- ❖ Research.
- ❖ La relación costo-beneficio es sideral.



Ciberespionaje

- ❖ Político: Gobiernos, partidos, ciudadanos, ...
- ❖ Industrial: Empresas, gobiernos, investigadores, ...
- ❖ Apuestas: ¿Tendencias?

Cyber Espionage



Cyber Warfare

- 1998 – Moon light maze
- 2003 – Titan rain
- 2009 – operation aurora
- 2009 – Ghost net
- 2011 – Nightdragon
- 2011 – Operation shady rat (2006)
- 2012 – Red October (2007)
- 2012 – Elderwood project
- 2012 – Flame
- 2012 – Gauss (2009)
- 2012 – Shamoon
- 2014 – Mask
- 2014 – snake

APT

APT - Advanced Persistent Threat
PTA - Persistent Targeted Attacks



SUPERVILLAIN

Shamoon:

THE YEAR'S HARBOR OF CYBERATTACKS

The most destructive corporate attack to date. Overwrites boot sectors and renders computers useless to cover its tracks.

Mission: Shatter the equipment company on the ground. Small Android's trace of company, AFRACO.

SECRET AGENT TOOL

ANDROID 3D SPYWARE

Developed by the U.S. military, Android covers an mobile devices and receives sensor data.

Mission: Intercept a 3D virtual model of a target location using the phone's camera and accelerometer sensors.

SECRET AGENT TOOL

From STUXNET, With Love

Developed by the U.S. and Israeli governments, spreads globally causing no harm until it finds and reaches its target.

Mission: Sabotage physical infrastructure.

SECRET AGENT TOOL

FLAME IS FOREVER

The most sophisticated malware ever created, infects computers and searches for intelligence contained in emails, documents, and messages.

Mission: Capture intelligence and intercepts it by intercepting audio and video streams... all under the cover of an encrypted channel.

SECRET AGENT TOOL

CREECH USB DRONE VIRUS

30

of Android's Predator and Rogue devices, require programming over algorithms and other malware.

TOOL

RANSOMCRYPT

Encrypts files on computers and demands payment to recover your files.

Mission: Make money to finance evil plots.

Cibercrimen

- ❖ Herramientas a pedido.
- ❖ Servicio CaaS: Cybercrime As a Service.
- ❖ Servicios de calidad, efectivos y fiables.
- ❖ Incluso atacan a atacantes.
- ❖ Costo promedio Kit/Ataque: US\$1,400.
- ❖ Rentabilidad Promedio Annual: US\$29,000.
- ❖ Otra vez: Tendencias?



Hacktivism

- ❖ Ideologías.
- ❖ Defacement, DDoS, robo de datos, ...
- ❖ Versus Gobiernos, Organizaciones, Iglesias, enfoque de género, de no género, Bueno, de lo que sea !!!!



Ciberyihadismo

- ❖ Ciberterrorismo – Hacktivismo – Ciberguerra.
- ❖ Por ahora, objetivos de propaganda fundamentalist !!
- ❖ Se prevé crecimiento notable.



Insiders

- ❖ Personal de organizaciones que utiliza su acceso a la información para sustraerla o compartirla de forma pública.
- ❖ Escucharon hablar de Mossack-Fonseca, los Wikileaks, ... todos han sido casos de fuga interna de datos !!



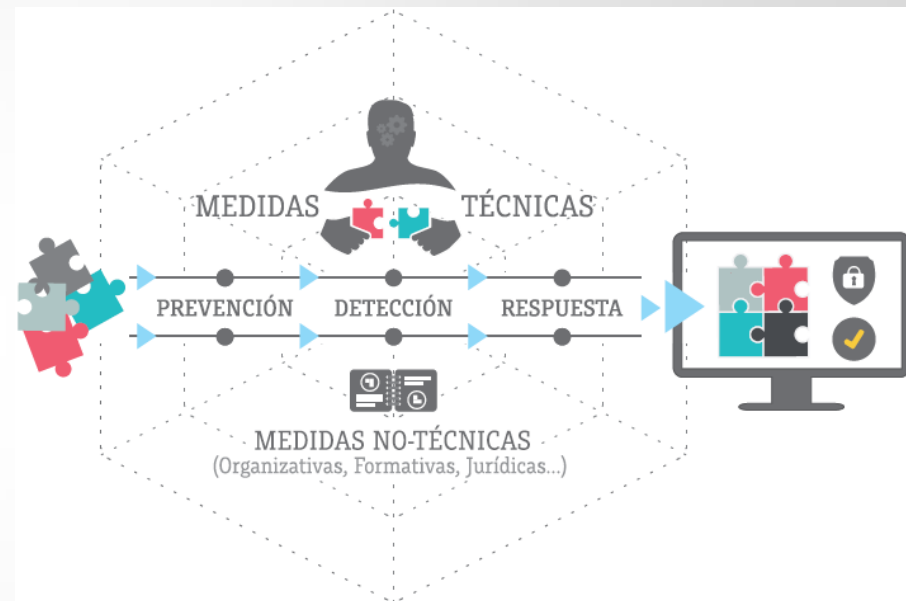
Ciberguerra

- ❖ Estados – Gobiernos – Disidentes – Facciones ...
- ❖ Operaciones militares bajo principios de sistemas de información y/o infraestructuras tecnológicas.
- ❖ Objetivos políticos y/o de defensa nacional, sistemas de comunicación o de información.



Ciberresiliencia

- ❖ Cultura:
 - Usuario – Técnico – Organización.
- ❖ Tecnologías:
 - Cifrado – PDR – Research – Entrenamiento.
- ❖ Estructura:
 - Política – Estrategia – Marco legal – Recursos – CERT – Colaboración ...



¿Cómo vamos a nivel país?

¿Qué pasa si?

- ❖ Gasoducto de Camisea, plantas generadoras de energía, infraestructura de distribución de energía, redes de agua, aeropuertos, bancos, entidades de salud, medios de transporte, telcos, ...
- ❖ Por ahora, infraestructura dependiente de la tecnología e interconectada.
- ❖ Internet no es el objetivo, es el arma.

Objetivos de ciberseguridad

- ❖ Establecer capacidades de ciberdefensa.
- ❖ Habilitar capacidades colaborativas entre stakeholders internos y externos.
- ❖ Desarrollar cultura de seguridad y de gestión de riesgos.
- ❖ Asegurar mercado e infraestructura digital para proporcionar servicios seguros y fiables a los ciudadanos y a las organizaciones.



Estrategia nacional de ciberseguridad

- ❖ Estrategia de desarrollo de capacidades de ciberdefensa y ciberresiliencia.
- ❖ Entidad coordinadora con competencias supra-gobierno.
- ❖ CERT: Infraestructura y recursos.
- ❖ Estrategias y tácticas de cooperación interna y externa.
- ❖ Baselines de ciberseguridad para infraestructuras críticas nacionales.

PRESIDENT OBAMA IS LAUNCHING

THE CYBERSECURITY NATIONAL ACTION PLAN, WHICH WILL INVEST MORE THAN \$19 BILLION TO ENSURE:

- ↗ Americans have the security tools they need to protect their identities online
- ↗ Companies can protect and defend their operations and information from hackers
- ↗ The U.S. government protects the private information citizens provide for federal benefits and services

#Cybersecurity

go.wh.gov/Cybersecurity



Desarrollo de capacidades de ciberseguridad

- ❖ ¿Visión de Estado?
- ❖ ¿De Gobierno?
- ❖ Promoción de la educación en Seguridad y Defensa Nacional:
En elaboración.
- ❖ Política de ciberseguridad: En elaboración (orientado a la seguridad nacional).

PYMES: ¿Qué hacer ante un ciberataque?

Estrategias y tácticas de cooperación

- ❖ Los ciberataques vienen de cualquier lado.
- ❖ Impactos suelen desbordar a una sola organización.
- ❖ Se requiere acción coordinada con fuerte soporte legal y normativo.
- ❖ Ooops... ¿tenemos un marco legal específico?
- ❖ Mecanismos de colaboración con entidades nacionales y de otros países.

PYMES: ¿Qué hacer ante un ciberataque?

¿Qué ofrece ISACA?

- ❖ Contenidos, marcos de referencia,
- ❖ Damos charlas, conferencias, hacemos demos,
- ❖ Vamos a tu PYME.
- ❖ Ahh, si quieren pasar al siguiente nivel:
 - ❖ A nivel infraestructura: Inviertan en fortalecer sus redes.
 - ❖ A nivel soporte: Cursos y certificaciones para su personal.
 - ❖ A nivel organización: Fortalezcan la cultura de riesgos y de seguridad de información.
 - ❖ Obviamente, esto significa \$\$\$\$\$\$



PYM

d

¿Nac

YOU HAVE BEEN

❖ Todo

❖ Hay c

❖ Y pro

❖ Porqu

❖ La implementaci

HACKED !!

YES

TO YOU !!

**Gracias por su paciencia y
buen humor !!**

Juan Dávila, CISA.CISM,CRISC, ISO 27001 LA, ISO 22301 LA, COBIT 5 Trainer
ISACA Lima Chapter, Presidente