



INTRODUCCIÓN A LA INDUSTRIA DE LA SEGURIDAD INFORMÁTICA

DEVELSECURITY

Developing Security for you.

Ing. Camilo Fernández


Consultor en Seguridad Informática

CISA, CISSP, CEPT, CEH, ISO27001 Lead Auditor, MCSE: Security, CHFI, Security+



Agenda



- Introducción
 - Por que necesitamos seguridad ?
 - Seguridad Informática
 - Seguridad de la Información
 - Historia
 - Estado Actual de la Seguridad
 - Amenazas
 - Servicios
 - Industrias
 - Inversión
 - Áreas de Seguridad de la Información
 - Tipos de Trabajos en la Industria
 - Conclusiones
- 



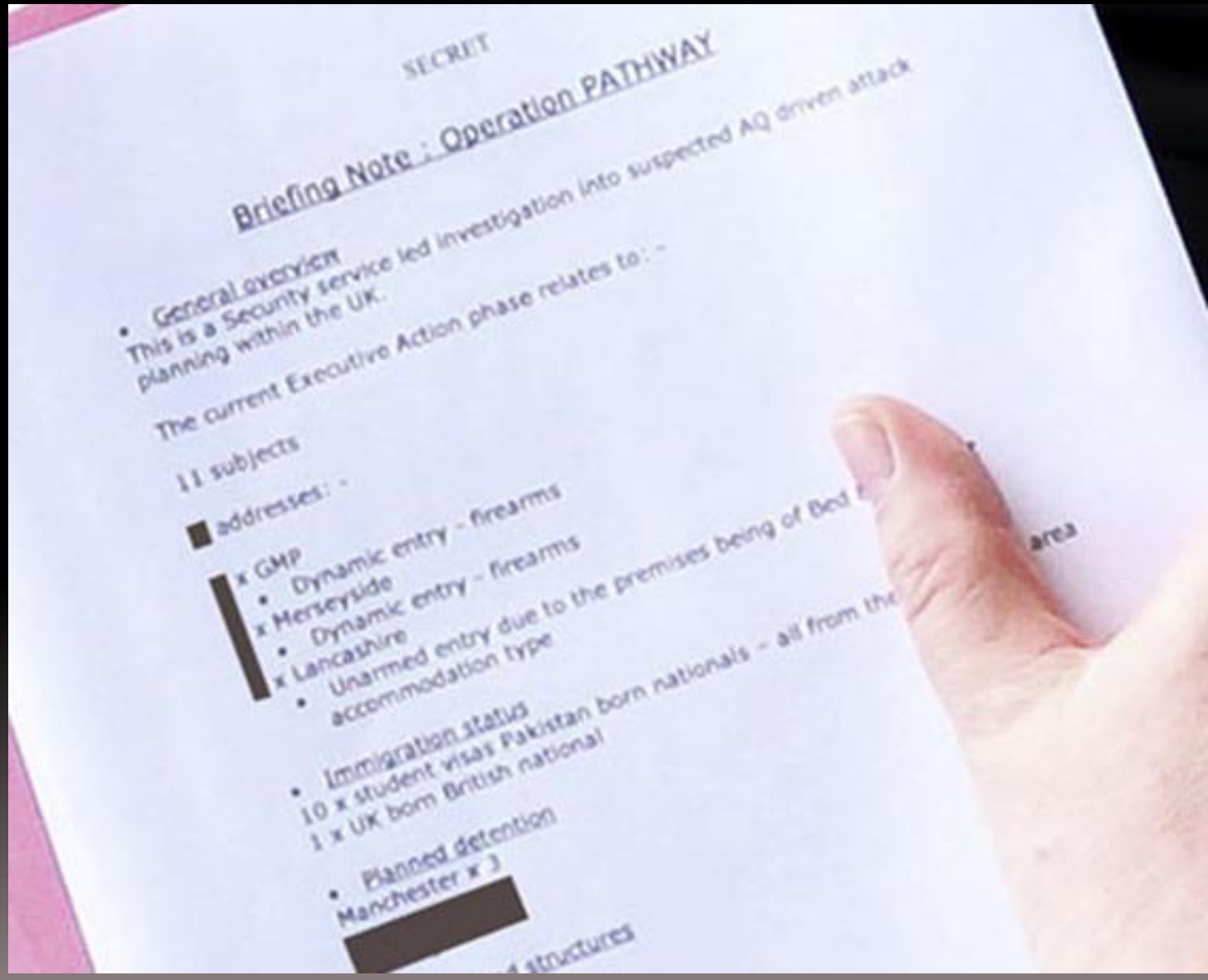
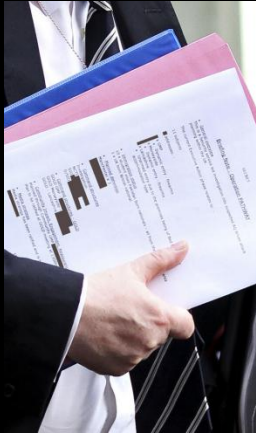
Introduccion

- Por que necesitamos Seguridad?





Introduccion



SECRET

Briefing Note : Operation PATHWAY

- General overview
This is a Security Service led investigation into suspected AQ driven attack planning within the UK.

The current Executive Action phase relates to: -

11 subjects

■ addresses: -

- x GMP
 - Dynamic entry - firearms
- x Merseyside
 - Dynamic entry - firearms
- x Lancashire
 - Unarmed entry due to the premises being of Bed & Breakfast type

• Immigration status

10 x student visas Pakistan born nationals - all from the [redacted] area

1 x UK born British national

• Planned detention
Manchester x 3

[redacted] structures



Introduccion

- Otro vivo Ejemplo ?
 - La guerra de Irak iba a comenzar.
 - USA quería de aliado a UK.
 - USA envía un documento a UK
proveyendo de la existencia de armas
de destrucción masiva en Irak
 - Tony Blair le presenta el documento al
parlamento de UK
 - El parlamento le pregunta a Tony Blair,
quien a modificado el documento?
 - El respondió: **Nadie!**



Introduccion



Microsoft Word bytes Tony Blair in the butt

[Home](#) > [Privacy](#) > Blair's Iraq Dossier

Richard M. Smith (rms@computerbytesman.com)

June 30, 2003

Microsoft Word documents are notorious for containing private information in file headers which people would sometimes rather not share. The hard way.

Back in February 2003, 10 Downing Street published a dossier on Iraq's security and intelligence organizations. This dossier was cited by Colin Dr. Glen Rangwala, a lecturer in politics at Cambridge University, quickly discovered that much of the material in the dossier was actually plagiar

You can read Dr. Rangwala's original analysis of the dossier from Feb. 5, 2003 at this URL:

<http://www.casi.org.uk/discuss/2003/msg00457.html>

Blair's government made one additional mistake: they published the dossier as a Microsoft Word file on their Web site. When I first heard from I had worked on the document. I downloaded the Word file containing the dossier from the 10 Downing Street Web site (<http://www.number-10>).

```
Rev. #1: "cic22" edited file "C:\DOCUME~1\phamill\LOCALS~1\Temp\AutoRecovery save of Iraq - security.asd"
Rev. #2: "cic22" edited file "C:\DOCUME~1\phamill\LOCALS~1\Temp\AutoRecovery save of Iraq - security.asd"
Rev. #3: "cic22" edited file "C:\DOCUME~1\phamill\LOCALS~1\Temp\AutoRecovery save of Iraq - security.asd"
Rev. #4: "JPratt" edited file "C:\TEMP\Iraq - security.doc"
Rev. #5: "JPratt" edited file "A:\Iraq - security.doc"
Rev. #6: "ablackshaw" edited file "C:\ABlackshaw\Iraq - security.doc"
Rev. #7: "ablackshaw" edited file "C:\ABlackshaw\A;Iraq - security.doc"
Rev. #8: "ablackshaw" edited file "A:\Iraq - security.doc"
Rev. #9: "MKhan" edited file "C:\TEMP\Iraq - security.doc"
Rev. #10: "MKhan" edited file "C:\WINNT\Profiles\mkhan\Desktop\Iraq.doc"
```



Introduccion

- Que es la Seguridad de la Información?
- Seguridad de la Información tiene como fin la **protección de la información** y de los sistemas de la información del acceso, uso, divulgación, interrupción o destrucción no autorizada.
- La Seguridad de la Información se refiere a la **Confidencialidad, Integridad y Disponibilidad** de la información y datos, independientemente de la forma los datos pueden tener: **electrónicos, impresos, audio u otras formas**.



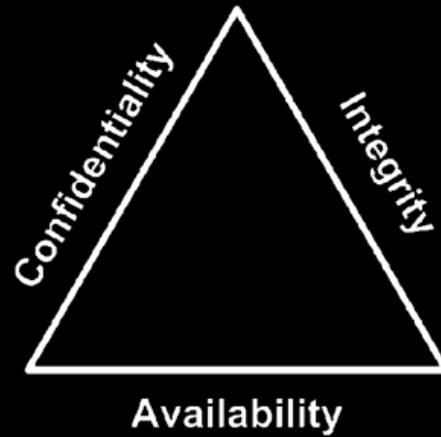
Introduccion

- Que es la Seguridad Informática?
- La seguridad informática consiste en asegurar que los recursos del **sistema de información** (material **informático** o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida así como su modificación sólo sea posible a las **personas** que se encuentren acreditadas y dentro de los límites de su **autorización**.



Introduccion

InfoSec **!=** IT Security

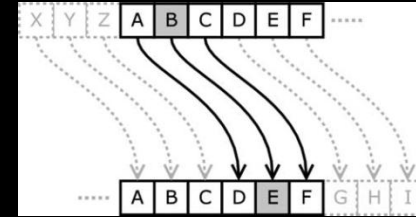


- diferencias radican principalmente:
 - Enfoque.
 - Metodologías utilizadas.
 - Zonas de concentración.



Historia

- Julio Cesar (Algoritmo Cesar)
 - protección de mensajes
- Segunda Guerra Mundial
 - Inicio de la seguridad de la información de manera profesional
- Invención del Computador (*Internet*)
 - Firewall
 - Antivirus
 - Control de Acceso Lógico
 - Troyanos
- Políticas y Metodologías
 - ISO 27001
 - COBIT
 - NSA
 - NIST
 - SDLC





Estado Actual - Ecrime

La evolución de cibercrimen:

Época Romántica (1996-2000)

- Virus destructivos
- Carácter local, sin propagación
- Creación de Virus
- Personas solitarias, muy localizadas

MOTIVACIONES:
Superación personal
Conocimientos técnicos

Origen:
Personas individuales o grupos muy pequeños

A destacar:
Alta calidad técnica
No hay programación

Edad Media (2001-2004)

- Primeros phishing (11S)
- Gusanos
- Botnets 1.0 (IRC)

MOTIVACIONES:
Dinero rápido
Infecciones masivas

Origen:
Personas individuales o grupos muy pequeños

A destacar:
Baja calidad técnica
No hay programación

Fraude (2005-2006)

- Milicias cibernéticas
- Múltiples objetivos
- Control del 50% de los ordenadores

MOTIVACIONES:
Dinero de cualquier forma
Extorsiones

Origen:
Personas individuales o grupos muy medianos

A destacar:
Phishing y malware
100% fraude bancario

e-crime (2007-2009)

- Ataques geopolíticos
- Botnets 2.0
- ISP a prueba de balas
- Infraestructura en venta
- Iframe businesss, pay per install, clickfraud, botnets, DDoS, infection kits, C&C, cyberwarfare, espionaje industrial...

MOTIVACIONES:
Controlar Internet
Dominación total

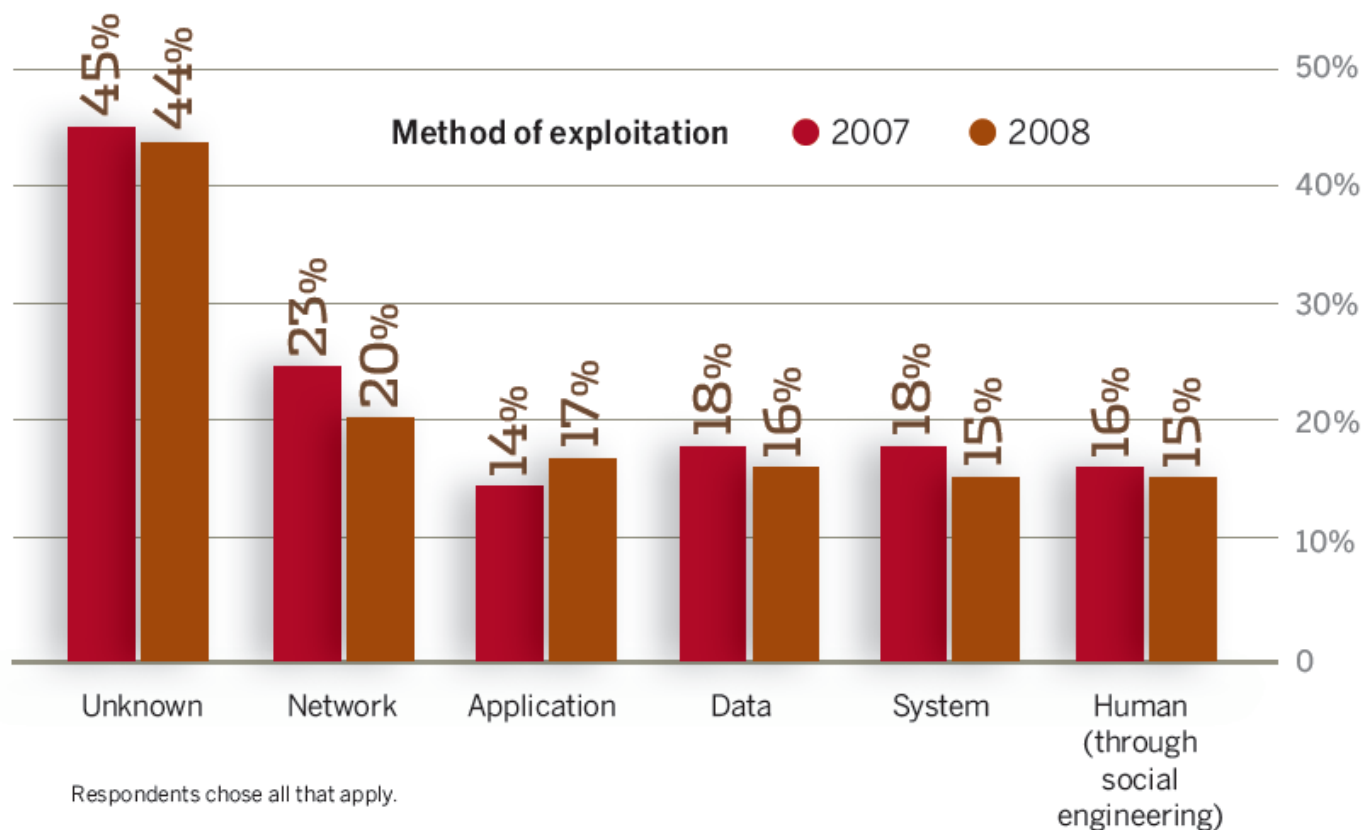
Origen:
Grupos de crimen organizado

A destacar:
Target: gobiernos, empresas
Amenazas políticas

Estado Actual - Explotacion



Nearly half of respondents can't identify vulnerabilities that led to security incidents

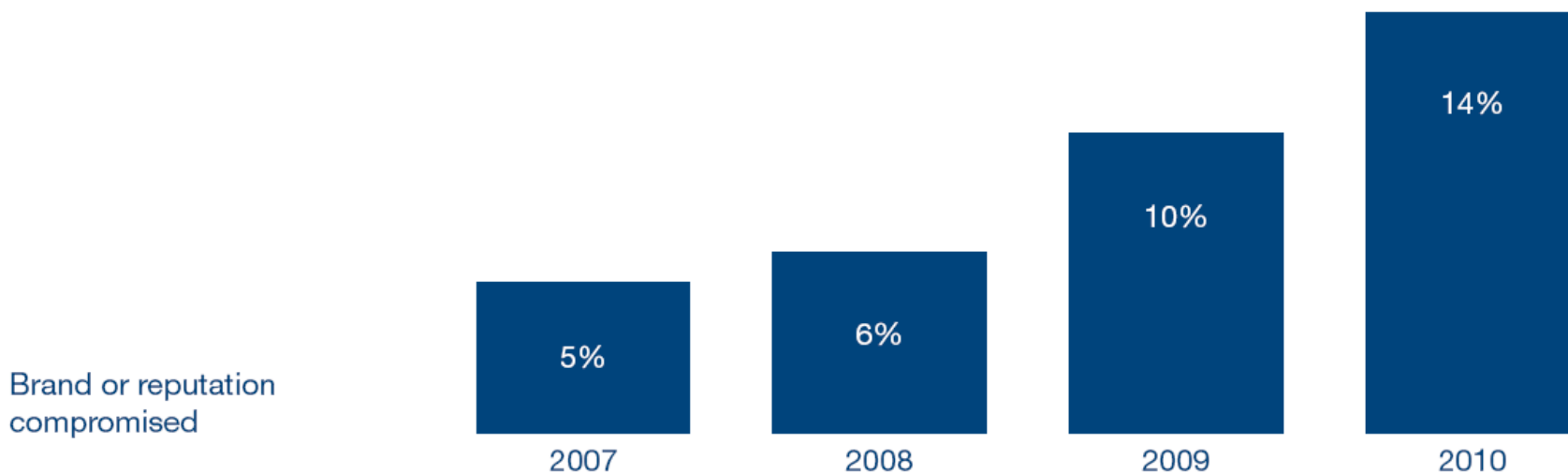


Fuente: Reporte Information Security 2008 por PWC

Estado Actual - Impacto



Figure 12: Percentage of all survey respondents who report the following business impacts to their organization. ⁽¹⁰⁾

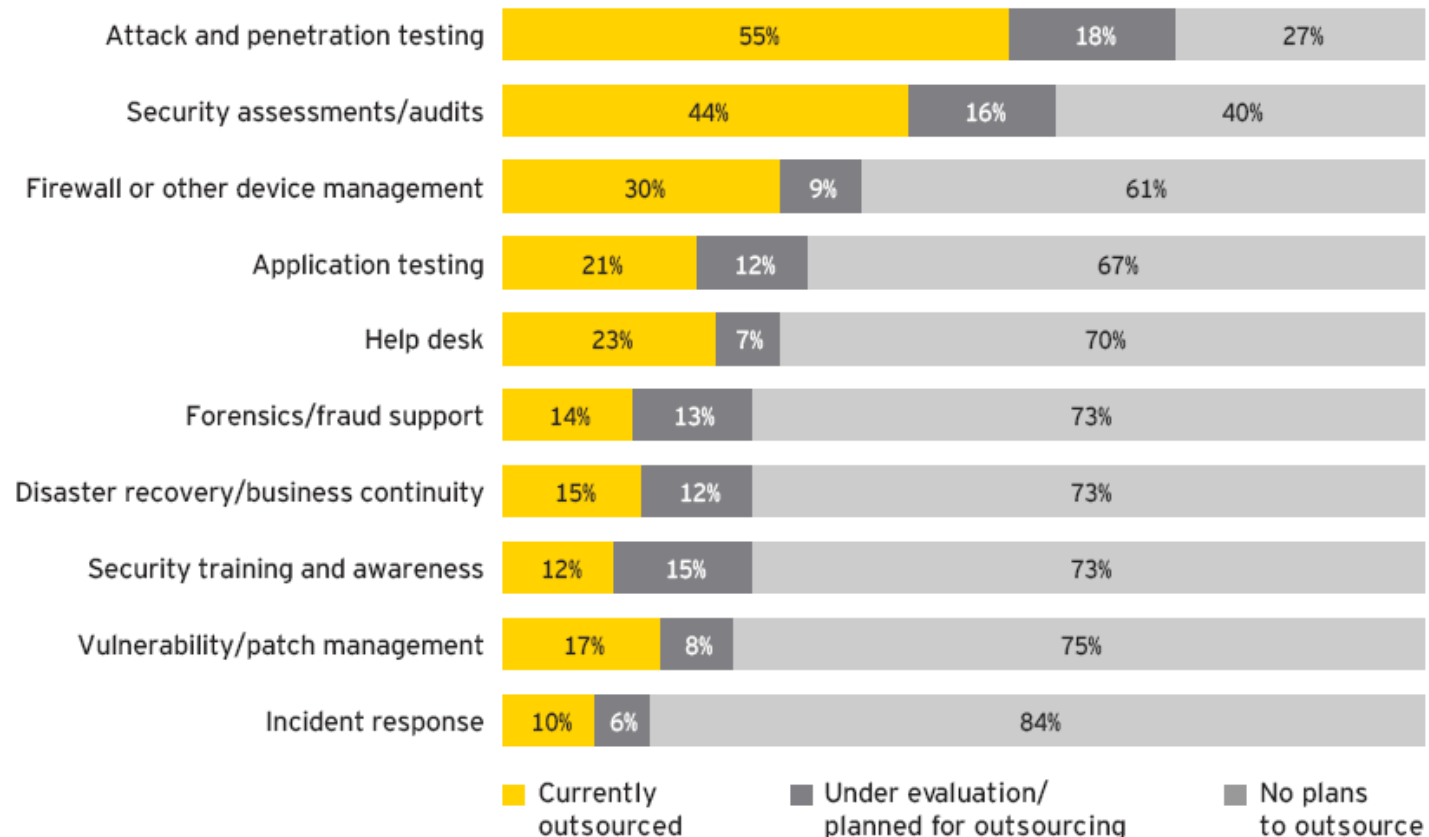


Fuente: Reporte Information Security 2010 por PWC

Estado Actual - Servicios



Which of the following security-specific activities have been outsourced or considered for outsourcing?



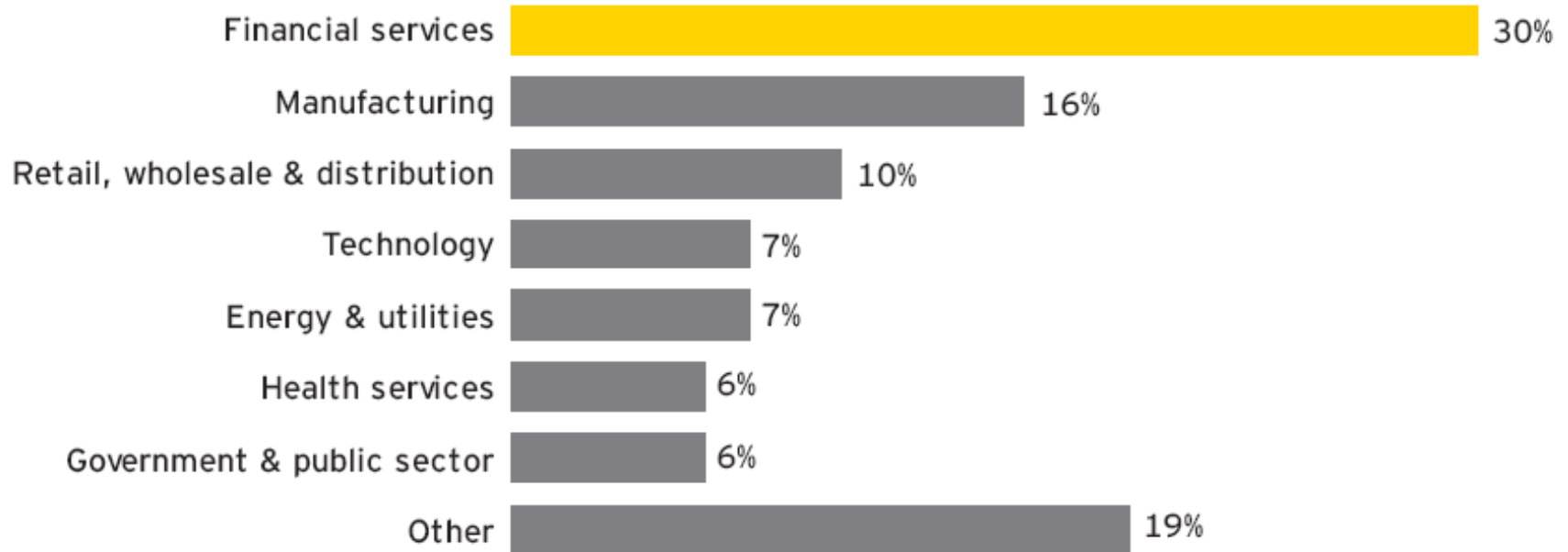
Shown: percentage of respondents

Fuente: Reporte Information Security 2010 por Ernst & Young



Estado Actual - Industria

Survey participants by major industry group



Shown: percentage of respondents

Fuente: Reporte Information Security Survey por Ernst & Young



Areas de InfoSec

- Técnica
 - Análisis de Vulnerabilidades
 - Hardening de Servidores
 - Pruebas de Intrusión
 - Análisis Forenses
 - Diseño de Redes Seguras y Comunicaciones
 - Análisis de Malware
 - Análisis de Aplicaciones y Protocolos
 - Investigación y Desarrollo



Areas de InfoSec

- Funcional
 - ▣ Análisis de Riegos de Procesos de Negocio
 - ▣ Planes de Continuidad de Negocio
 - ▣ Creación de Políticas de Seguridad
 - ▣ Políticas de Buenas Practicas
 - ▣ Procedimientos estandarizados
 - ▣ Establecimiento de Métricas

Trabajos dentro de InfoSec



- #1 Information Security Crime Investigator/Forensics Expert
- #2 System, Network, and/or Web Penetration Tester
- #3 Forensic Analyst
- #4 Incident Responder
- #5 Security Architect
- #6 Malware Analyst
- #7 Network Security Engineer
- #8 Security Analyst
- #9 Computer Crime Investigator
- #10 CISO/ISO or Director of Security
- #11 Application Penetration Tester
- #12 Security Operations Center Analyst
- #13 Prosecutor Specializing in Information Security Crime
- #14 Technical Director and Deputy CISO
- #15 Intrusion Analyst
- #16 Vulnerability Researcher/ Exploit Developer
- #17 Security Auditor
- #18 Security-savvy Software Developer
- #19 Security Maven in an Application Developer Organization
- #20 Disaster Recovery/Business Continuity Analyst/Manager





Penetration Tester

- **Puesto:** Penetration Tester (*Hacker*)
- **Edad:** 20 - 27
- **Bebida Favorita:** Coca-Cola
- **Arma Favorita:** Nmap
- **Habilidades:**
 - Conocimiento de Internet!!
 - Conocimiento de Arquitecturas
 - Conocimiento de Protocolos
 - Conocimiento de Troyanos
- **Lenguajes de Programación:**
 - Scripting: Perl, Python, Ruby
 - C#, Java, PHP, ASPX, ASP
- **Frase:**

You can be a hacker,
but do it legally and get paid a lot of money!
GOT ROOT ?



Forensic Investigator



- **Puesto:** Forensic Analyst (*Forenser*)
- **Edad:** 25 - 30
- **Bebida Favorita:** Red-Bull
- **Arma Favorita:** Encase
- **Habilidades:**
 - Conocimiento de File Systems
 - Conocimiento de memoria (Stacking)
 - Conocimiento de Sistemas Operativos
 - Conocimiento de Protocolos
- **Lenguajes de Programación:**
 - Scripting: Perl, Python, Ruby
 - C, C++
- **Frase:**

The thrill of the hunt!
You never encounter the
same crime twice!"





Malware Analyst

- **Puesto:** Malware Analyst (*Reverser, Bug Hunter*)
- **Edad:** 24 - 30
- **Bebida Favorita:** Te
- **Arma Favorita:** Debugger
- **Habilidades:**
 - Leet Master **Hex** Reader
 - Conocimientos de binarios ELF y PE
 - Prefiere leer el periódico en Hex
 - Buffer Overflow Mastery
 - Introducir `0x41` y `NOP`'s.
 - Fuzzing
- **Lenguajes de Programación:**
 - ASM...ASM...ASM!!!
 - C, C++
- **Frase:**

“\x43\x52\x54\x01\x2A\x42\xD4
\x8A\x57\x53\x3”
ShellCode!”





CISO

- **Puesto:** Chief Information Security Officer (*CISO, CSO*)
- **Edad:** 30 - 45
- **Bebida Favorita:** Café
- **Arma Favorita:** Word, Excel
- **Habilidades:**
 - Reorganización de Procesos de Negocios
 - Conocimiento de Estándares de Seguridad
 - COBIT
 - ISO27001
 - NIST
 - Creación de Políticas de Seguridad
 - Conocimiento de Análisis de Riesgos
- **Lenguajes de Programación:**
 - Excel & Word & PowerPoint Master!
- **Frase:**

“Security starts from Management Responsibility”





Conclusiones

- La seguridad no es simplemente un **Plug & Play**.
- InfoSec **!=** IT Security.
- **Casas, Carros, Sueldos, Puntos** en Seguridad Informática.
- Google it & **RTFM** (Read the Fu.....ll Manual)!



Preguntas ?



Gracias por su atención!



www.develsecurity.com