

# Análisis de Riesgos

## Curso 2024-2025

# ÍNDICE

1. Conceptos generales
2. Análisis de Riesgos

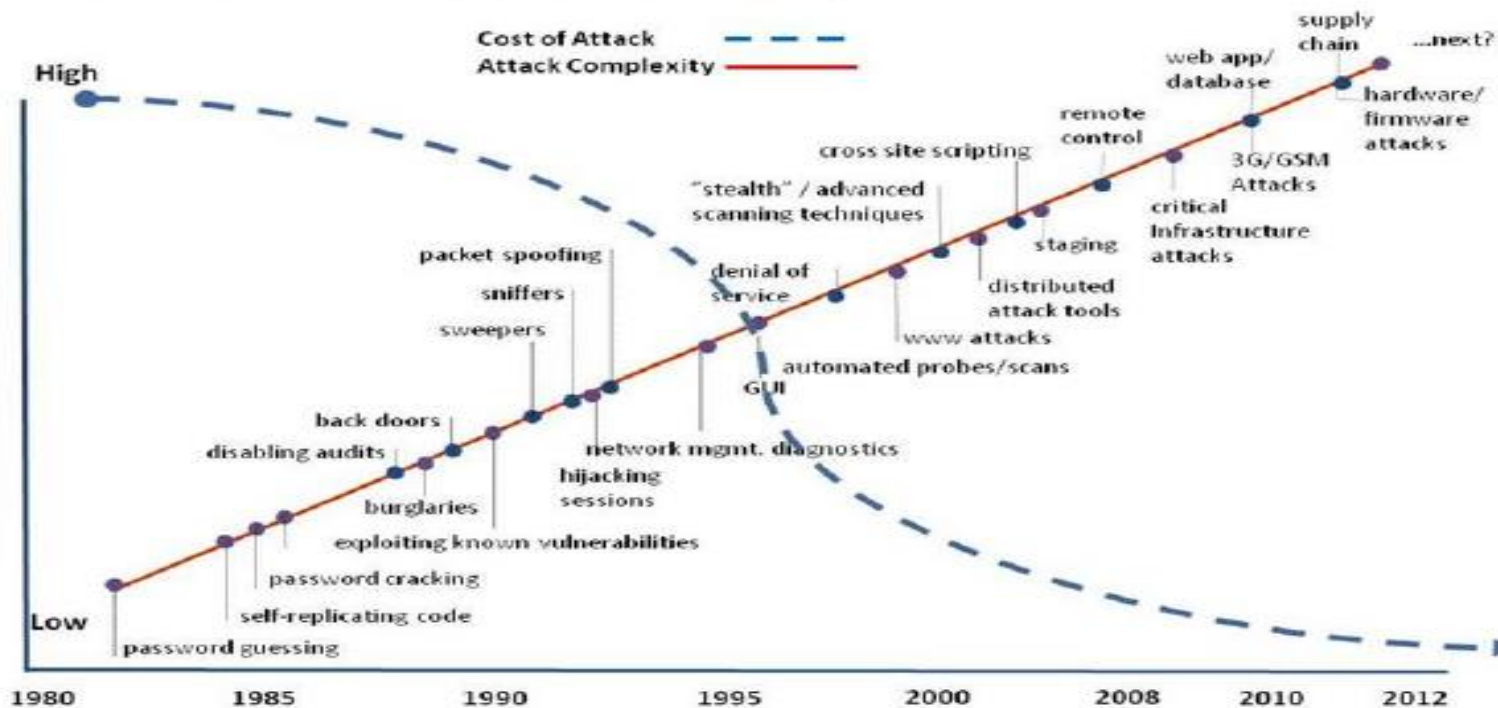


# Conceptos generales

- Mayor **disponibilidad** de herramientas más **avanzadas**

## Diminishing Attack Costs & Increasing Complexity

*Increased network complexity & dependence means more attacks succeed with high payoffs  
Technology advances mean lower cost for a successful attack*



## Conceptos generales

- Cualquier atacante puede comprometer seriamente un sistema seguro



# Conceptos generales

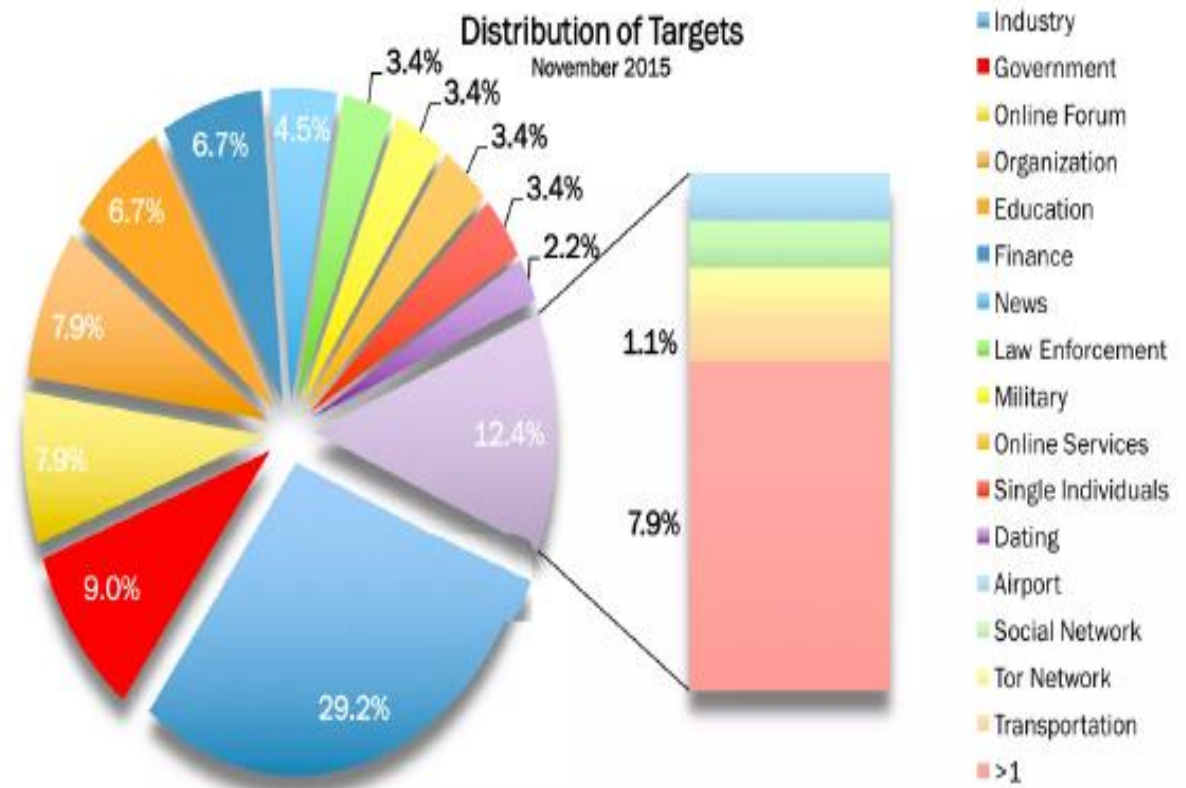
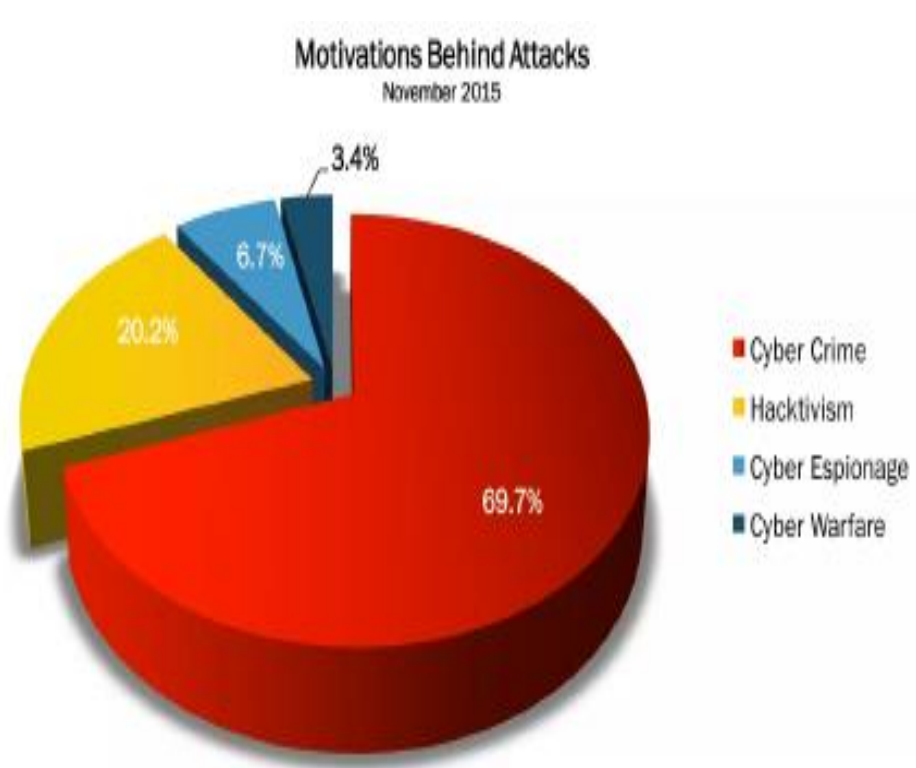
- “Empresas” especializadas





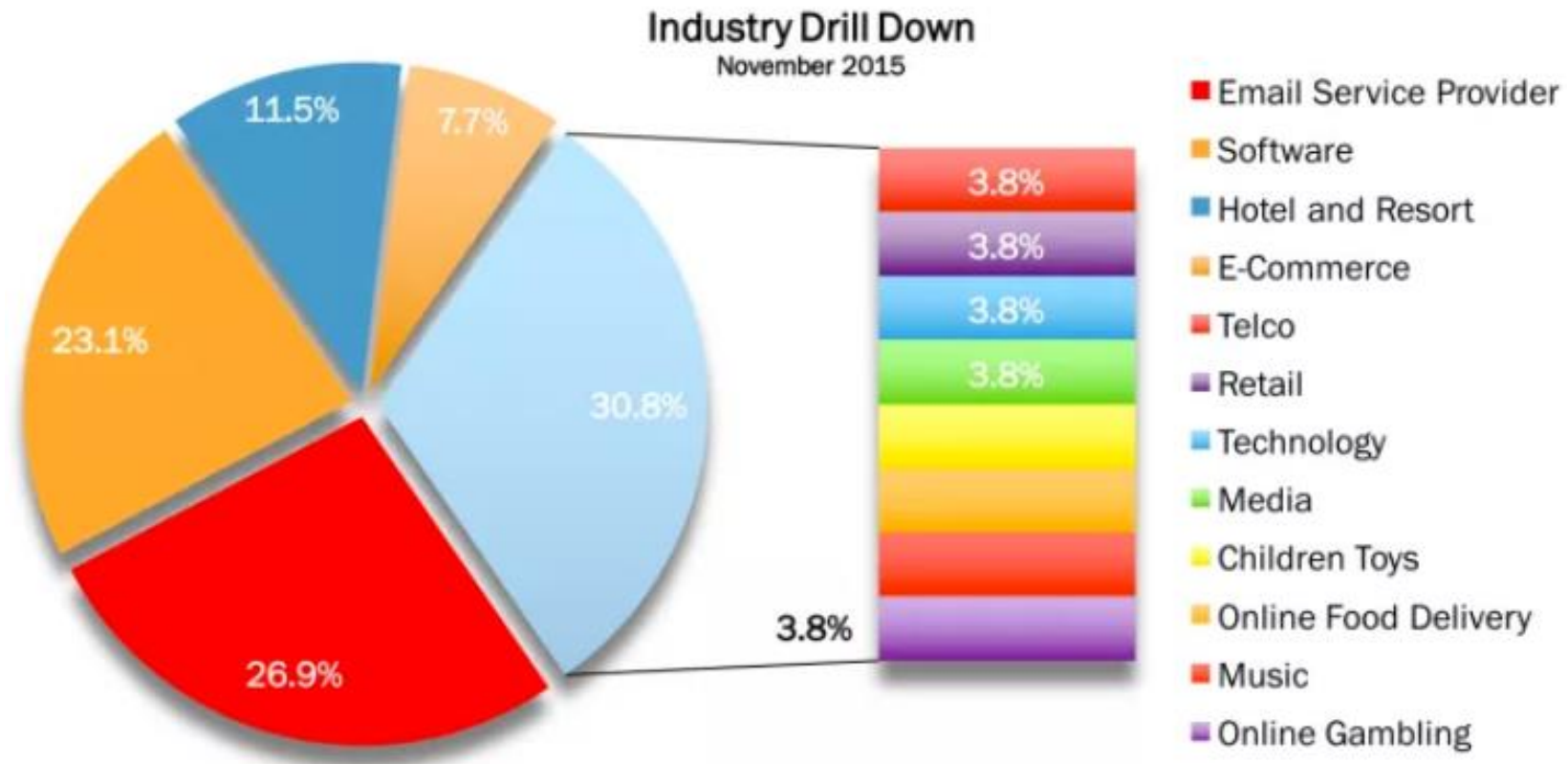
# Conceptos generales

- Perfil profesional del atacante



# Conceptos generales

**Desafío.** ¿En qué se fijaron los atacantes?



## Conceptos generales

- “Existe algo detrás del trono aún mayor que el propio Rey” (Sir William Pitt, Primer Ministro Jorge III, 1770)





# Conceptos generales

- Servicios de Inteligencia → Seguridad Nacional
  - ¿Cuáles son los límites de la “Seguridad Nacional”?
  - Lucha contra el Terrorismo
  - Espionaje gubernamental para empresas nacionales



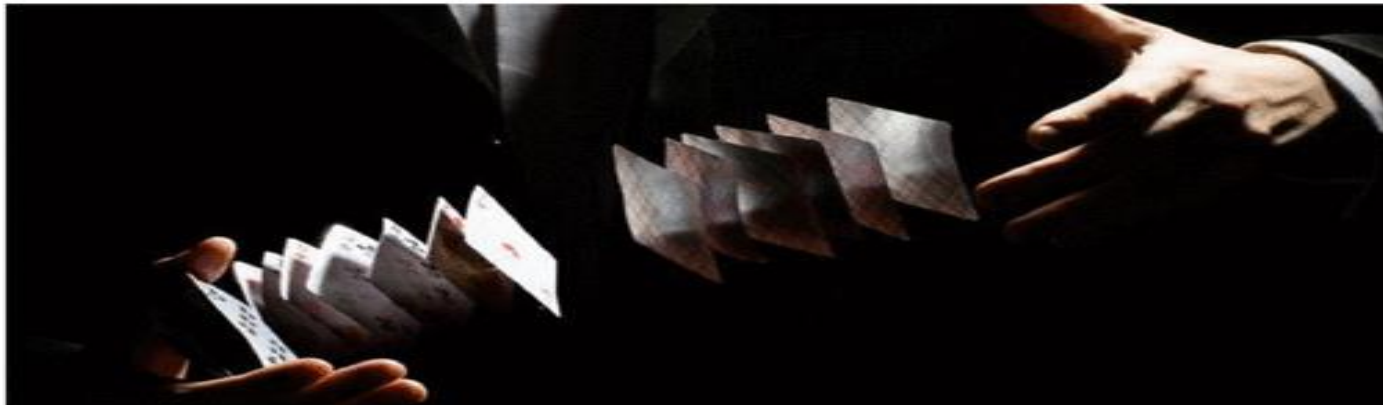
## Conceptos generales

- Inteligencia Económica → Relación Corporación & Estado
  - Estrategias conjuntas para dominar tecnologías clave y/o hacerse con segmentos del mercado mundial
  - Minimizar el riesgo en la toma de decisiones
  - Ayuda para explotar un mercado extranjero
  - Relación de quid pro quo
  - Círculos sociales: ejecutivos en los mismos entornos y con un idéntico “destino”
  - Corporaciones Nacionales = GRANDES Ciudadanos

## Conceptos generales

- Ataques contra la inteligencia de las organizaciones
- “Realidad fabricada” mediante la manipulación/falsificación de la Inteligencia

SECRET//SI//REL TO USA, FVEY



We want to build *Cyber Magicians*.

## Conceptos generales

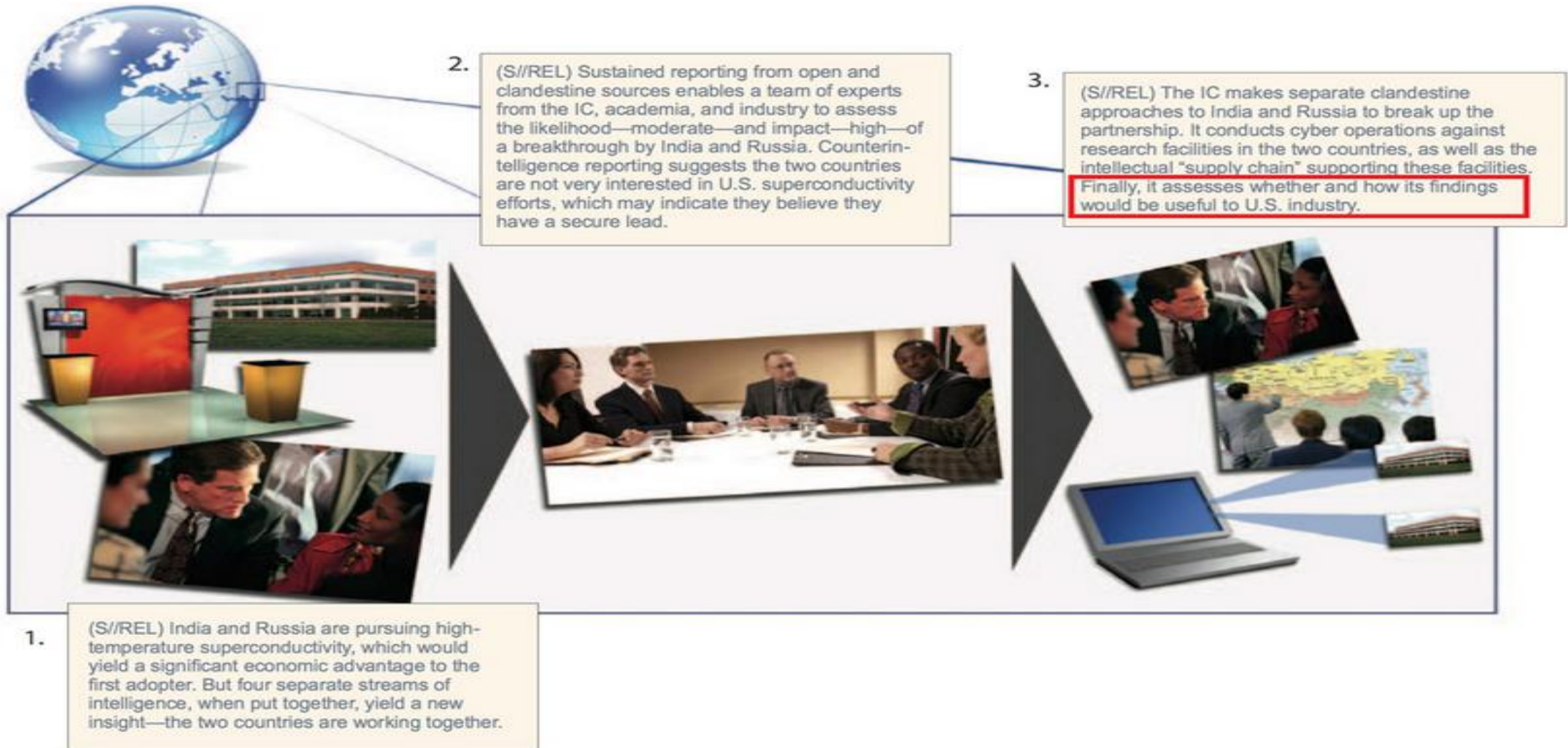


### *Discredit a company*



- Leak confidential information to companies / the press via blogs etc
- Post negative information on appropriate forums
- Stop deals / ruin business relationships

# Conceptos generales





# Conceptos generales

- Impacto reputacional

FIGURE 4. COMMON THREATS RANKED IN TERMS OF REPUTATIONAL IMPACT

Data breach/data theft

5.5

Natural or manmade disasters

5.2

IT system failure

4.3

Data loss (backup/restore failure)

4.0

Cyber security breach/advanced persistent threats

3.8

Human error

2.6

Third-party partner security breach or IT system failure

1.2



# Conceptos generales

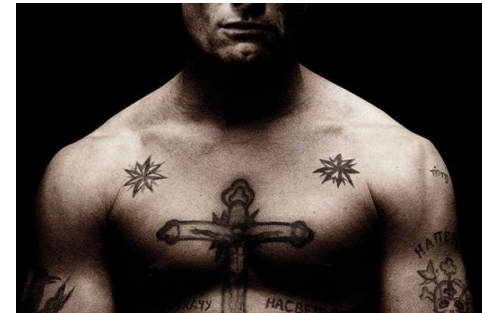
- Daño reputacional
  - Altas expectativas de los clientes sobre sus datos y la ética corporativa
  - Publicidad viral negativa
  - Antes eran noticia los grandes escándalos, ahora cualquier incidente tiene un impacto

FIGURE 6. ESTIMATED REPUTATION-RELATED COSTS RESULTING FROM DISRUPTION TO BUSINESS OR IT OPERATIONS OVER THE NEXT 24 MONTHS

| Minor    | Moderate  | Substantial |
|----------|-----------|-------------|
| \$20,929 | \$468,309 | \$5,274,523 |

# Conceptos generales

- Hacktivistas
- Crimen organizado
- Servicios de Inteligencia



# Conceptos generales

- Usuarios



## Conceptos generales

- Falta de concienciación interna → HUMINT (Int. Humana)
  - Ingeniería Social
  - Concienciación Directiva
  - Dispositivos portátiles
  - Viajes, reuniones, congresos,
  - actividades sociales, encuentros
  - “casuales” ..
  - Filtraciones internas
  - Honey Traps



*“Utiliza a tu enemigo para derrotar a tu enemigo. Si utilizas al enemigo para derrotar al enemigo, serás poderoso en cualquier lugar a donde vayas”*



## Conceptos generales

- Riesgos operativos de gran importancia (por ej. fraude interno)
- Empresas que cuentan con un programa de prevención de fraudes → 30% - 35%
  - Menos personas realizan labores de monitorización
  - Reducción o anulación de las auditorías de control
  - Relajación de los controles de entrada y salida de mercancías
  - Pocas personas concentran funciones vitales de control (autorizar pagos, emitir cheques, etc)
  - Reducción de los programas de formación en materia ética

# Conceptos generales

- Triángulo del Fraude



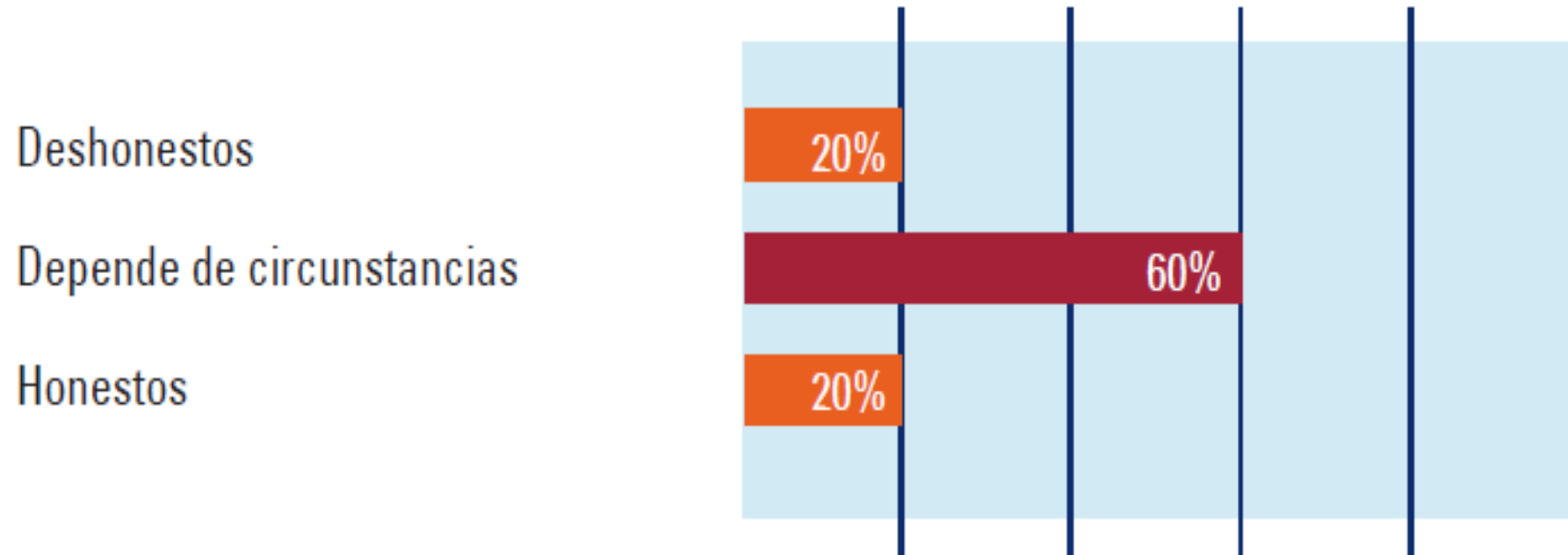
# Conceptos generales

- Mecanismos de detección

| País      | Incidencia | Principal mecanismo |
|-----------|------------|---------------------|
| Argentina | 30%        | Accidentalmente     |
| Brasil    | 68%        | Denuncia            |
| Chile     | 26%        | Controles internos  |
| México    | 50%        | Denuncia            |
| Uruguay   | 81%        | Controles internos  |

## Conceptos generales

- Comportamiento ético de los empleados



## Conceptos generales

- Perfil del defraudador
  - Hombre entre 36 y 45 años
  - Nivel de antigüedad en la empresa => 10 años
  - Relacionado con el área financiera
  - Cargo gerencial o superior



# Conceptos generales

- Perfil del defraudador
  - Evita tomar vacaciones
  - Rechaza injustificadamente ascensos o rotaciones
  - Disfruta de una vida ostentosa
  - Goza de inusuales atribuciones
  - Entrega discrepantes informes financieros
  - Excesivo secretismo sobre su función y operaciones

## Conceptos generales

**Desafío.** Diseñar controles para detectar comportamientos anómalos en un entorno de alta incidencia de fraude interno

# Conceptos generales

- Cisnes Negros



## Conceptos generales

**Desafío.** Analizar posibles Cisnes Negros desarrollados por atacantes contra todo tipo de organizaciones

# Conceptos generales

- Cisnes Negros intencionados

INTERNACIONAL

**Francia: ¿El vuelo de drones sobre siete centrales nucleares prefigura un atentado?**



1

 Share


0

 Tweet

0

 Google +

0

 Reddit

0

 Email



# Conceptos generales

- Las amenazas son diversas
  - Spam
  - Phishing
  - Spear phishing
  - Malware
  - Ransomware
  - DDoS
  - Vulnerabilidades 0-day
  - ..

# Conceptos generales

**Desafío.** Según lo comentado, ¿qué prácticas podrían conseguir tener un riesgo controlado?

- ¿Defensa en profundidad?
- ¿Monitorización y alertas de vulnerabilidades?
- ¿Control de dispositivos extraíbles?
- ¿Control de aplicaciones para evitar la descarga de contenido malicioso?
- ¿Protección en la navegación?
- ¿Encriptación de datos sensibles?

# Conceptos generales

## Percentage of Spam in Email by Industry

► Some industry sectors receive more spam than others, but the range is only approximately 5 percent.



| Industry Detail                   | Percentage of Email as Spam |
|-----------------------------------|-----------------------------|
| Mining                            | 56.3%                       |
| Manufacturing                     | 54.2%                       |
| Construction                      | 53.7%                       |
| Services                          | 53.0%                       |
| Agriculture, Forestry, & Fishing  | 52.9%                       |
| Retail Trade                      | 52.7%                       |
| Nonclassifiable Establishments    | 52.6%                       |
| Wholesale Trade                   | 52.5%                       |
| Public Administration             | 52.2%                       |
| Finance, Insurance, & Real Estate | 52.1%                       |
| Transportation & Public Utilities | 51.8%                       |
| Non SIC Related Industries        |                             |
| Healthcare                        | 54.1%                       |
| Energy                            | 53.0%                       |

# Conceptos generales

*Phishing Ratio in Email by Industry*

► Retail was the industry sector most heavily exposed to phishing attacks in 2015.

| Industry Detail                   | Phish Email Ratio |
|-----------------------------------|-------------------|
| Retail Trade                      | 1 in 690          |
| Public Administration             | 1 in 1,198        |
| Agriculture, Forestry, & Fishing  | 1 in 1,229        |
| Nonclassifiable Establishments    | 1 in 1,708        |
| Services                          | 1 in 1,717        |
| Manufacturing                     | 1 in 1,999        |
| Finance, Insurance, & Real Estate | 1 in 2,200        |
| Mining                            | 1 in 2,225        |
| Wholesale Trade                   | 1 in 2,226        |
| Construction                      | 1 in 2,349        |
| Transportation & Public Utilities | 1 in 2,948        |

## Non SIC Related Industries

|            |            |
|------------|------------|
| Energy     | 1 in 2,525 |
| Healthcare | 1 in 2,711 |

# Conceptos generales

| Industry Detail                   | Distribution | Attacks per Org | % Risk in Group* |
|-----------------------------------|--------------|-----------------|------------------|
| Finance, Insurance, & Real Estate | 35%          | 4.1             | 8.7%             |
| Services                          | 22%          | 2.1             | 2.5%             |
| Manufacturing                     | 14%          | 1.8             | 8.0%             |
| Transportation & Public Utilities | 13%          | 2.7             | 10.7%            |
| Wholesale Trade                   | 9%           | 1.9             | 6.9%             |
| Retail Trade                      | 3%           | 2.1             | 2.4%             |
| Public Administration             | 2%           | 4.7             | 3.2%             |
| Non-Classifiable Establishments   | 2%           | 1.7             | 3.4%             |
| Mining                            | 1%           | 3.0             | 10.3%            |
| Construction                      | <1%          | 1.7             | 1.1%             |
| Agriculture, Forestry, & Fishing  | <1%          | 1.4             | 2.0%             |

| Non SIC Related Industries |     |     |      |
|----------------------------|-----|-----|------|
| Energy                     | 2%  | 2.0 | 8.4% |
| Healthcare                 | <1% | 2.0 | 1.1% |

# Conceptos generales

## *Top 10 Sectors Breached by Number of Incidents*

- *Health Services is denoted as a sub-sector within the Services industry, and 120 of the 200 breaches that occurred within the Services sector were attributed to Healthcare.*

|   | Sector                            | Number of Incidents | % of Incidents |
|---|-----------------------------------|---------------------|----------------|
| 1 | Services                          | 200                 | 65.6%          |
| 2 | Finance, Insurance, & Real Estate | 33                  | 10.8%          |
| 3 | Retail Trade                      | 30                  | 9.8%           |
| 4 | Public Administration             | 17                  | 5.6%           |
| 5 | Wholesale Trade                   | 11                  | 3.6%           |
| 6 | Manufacturing                     | 7                   | 2.3%           |
| 7 | Transportation & Public Utilities | 6                   | 2.0%           |
| 8 | Construction                      | 1                   | <1%            |

# Conceptos generales

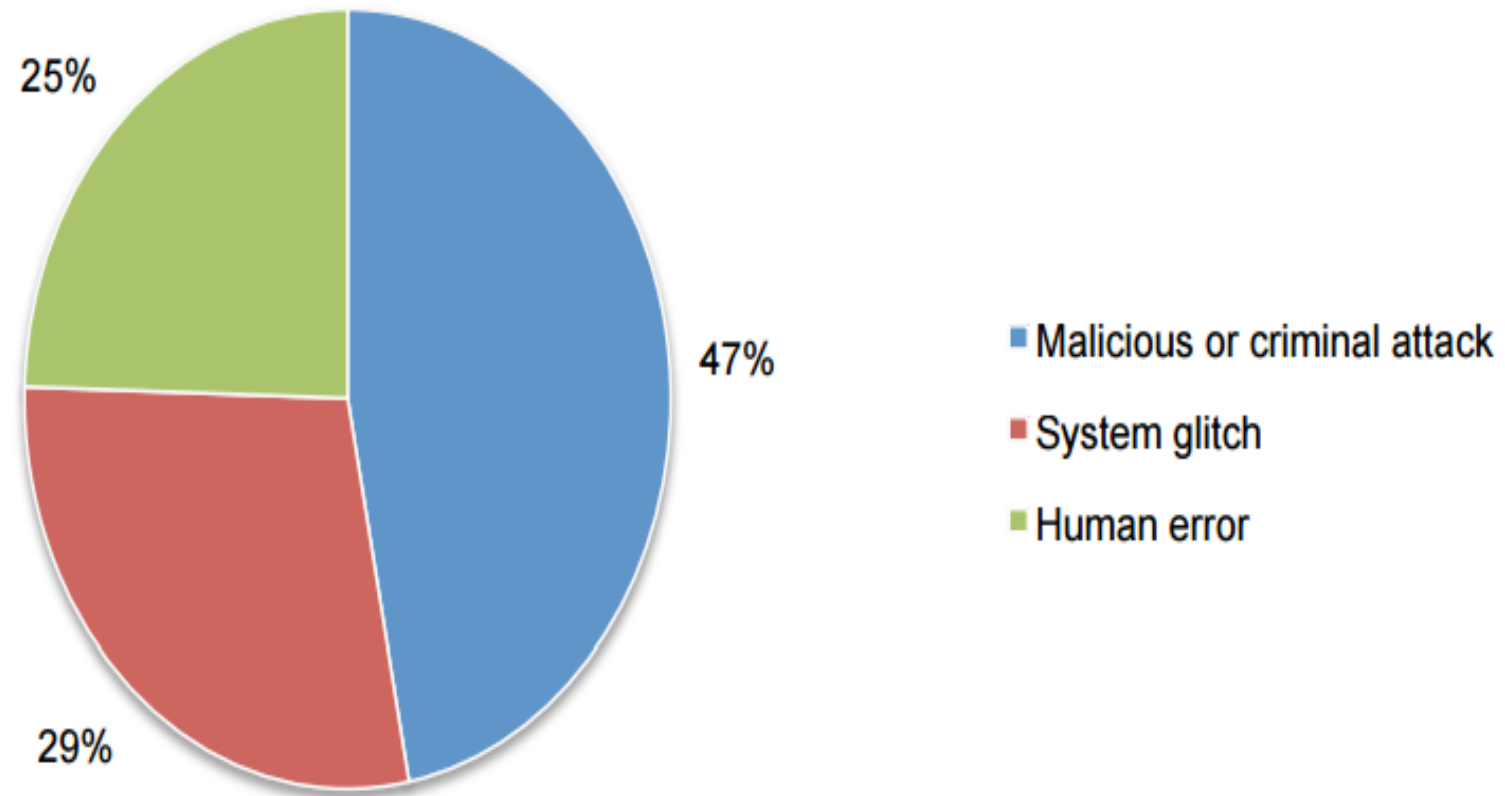
*Top 10 Sub-Sectors Breached  
by Number of Incidents*

|    | Sector                            | Number of Incidents | % of Incidents |
|----|-----------------------------------|---------------------|----------------|
| 1  | Health Services                   | 120                 | 39.3%          |
| 2  | Business Services                 | 20                  | 6.6%           |
| 3  | Educational Services              | 20                  | 6.6%           |
| 4  | Insurance Carriers                | 17                  | 5.6%           |
| 5  | Hotels & Other Lodging Places     | 14                  | 4.6%           |
| 6  | Wholesale Trade - Durable Goods   | 10                  | 3.3%           |
| 7  | Eating & Drinking Places          | 9                   | 3.0%           |
| 8  | Executive, Legislative, & General | 9                   | 3.0%           |
| 9  | Depository Institutions           | 8                   | 2.6%           |
| 10 | Social Services                   | 6                   | 2.0%           |



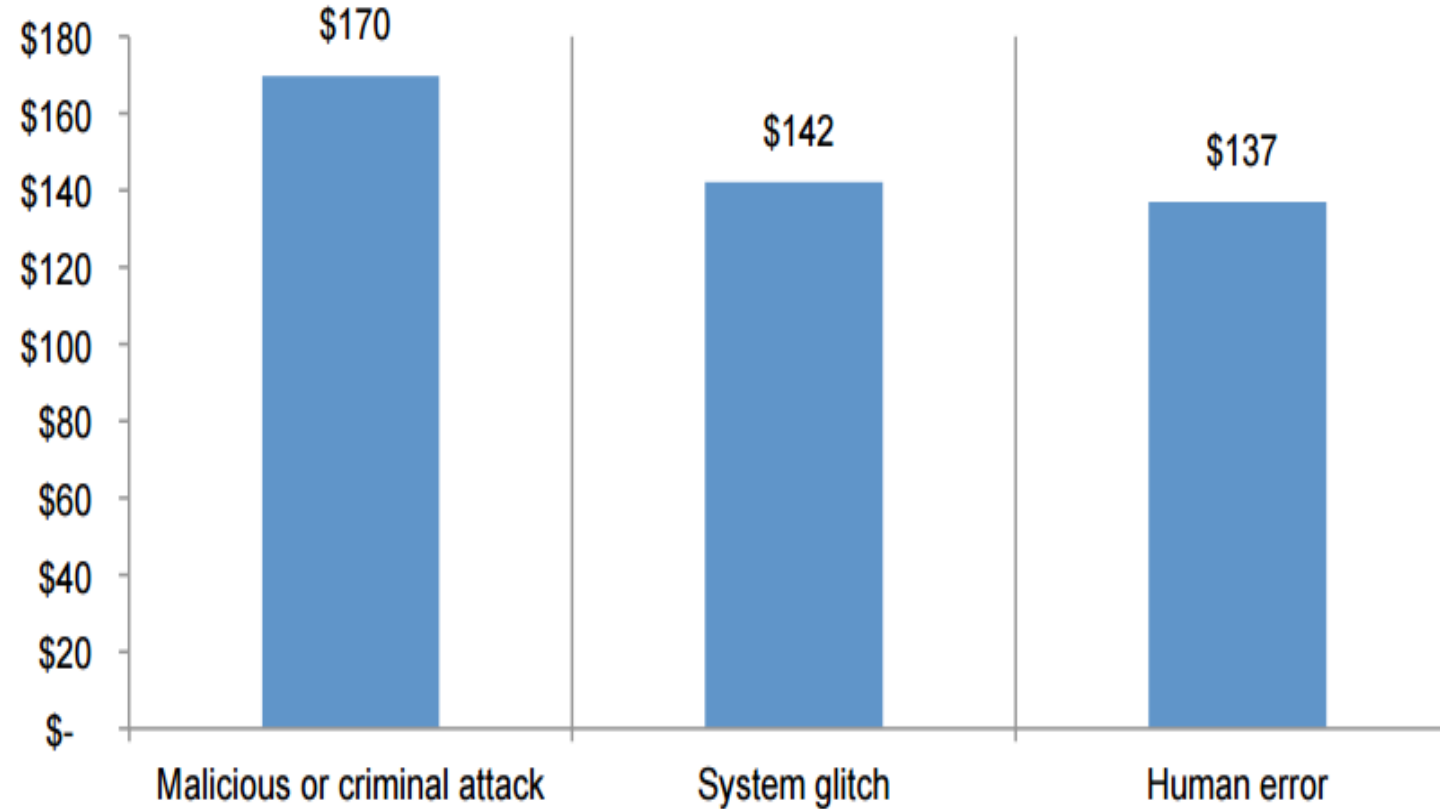
# Conceptos generales

**Pie Chart 2. Distribution of the benchmark sample by root cause of the data breach**  
Consolidated view (n=350)



# Conceptos generales

**Figure 5. Per capita cost for three root causes of the data breach**  
Consolidated view (n=350), measured in US\$



# Conceptos generales

- Coste de las brechas de seguridad
  - Incremento en la frecuencia de los ciberataques
  - Incremento de los costes de remediación
  - Incremento de las consecuencias en pérdida de negocio
  - Incremento en los costes de la detección y el escalado (forensic, auditoría, equipo de crisis, comunicación, etc)

## Conceptos generales

**Desafío.** ¿Qué actividades lanzaría para la identificación y la respuesta inmediata a una brecha de datos? ¿Y después de dicha fase?

## Conceptos generales

- Conducting investigations and forensics to determine the root cause of the data breach
- Determining the probable victims of the data breach
- Organizing the incident response team
- Conducting communication and public relations outreach
- Preparing notice documents and other required disclosures to data breach victims and regulators
- Implementing call center procedures and specialized training

## Conceptos generales

- Audit and consulting services
- Legal services for defense
- Legal services for compliance
- Free or discounted services to victims of the breach
- Identity protection services
- Lost customer business based on calculating customer churn or turnover
- Customer acquisition and loyalty program costs

# Conceptos generales

- ¡Las brechas de seguridad tienen múltiples costes derivados!
- Los controles tecnológicos como salvaguarda del negocio





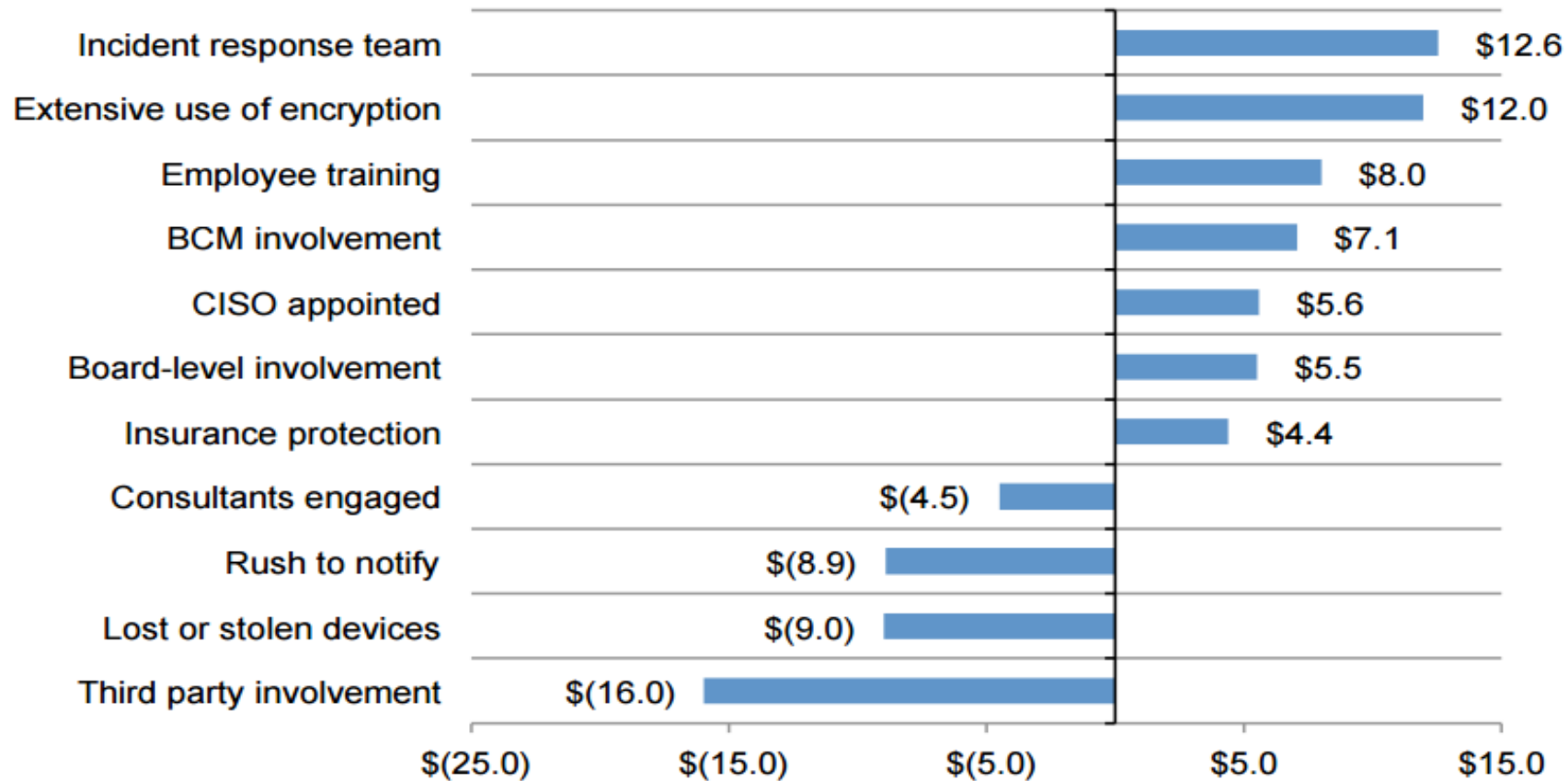
## Conceptos generales

Table 2 provides a list 11 factors that accelerate or moderate the per capita cost of data breach.

| Table 2. Factors that impact the per capita cost of data breach |                         |
|---|-------------------------|
| Factors   | Percentage of companies |
| Employee training   | 51%                     |
| BCM involvement   | 50%                     |
| Incident response team  | 48%                     |
| CISO appointed  | 45%                     |
| Extensive use of encryption                                     | 44%                     |
| Third party involvement   | 36%                     |
| Consultants engaged   | 35%                     |
| Lost or stolen devices  | 33%                     |
| Insurance protection  | 32%                     |
| Board-level involvement   | 31%                     |
| Rush to notify  | 29%                     |

# Conceptos generales

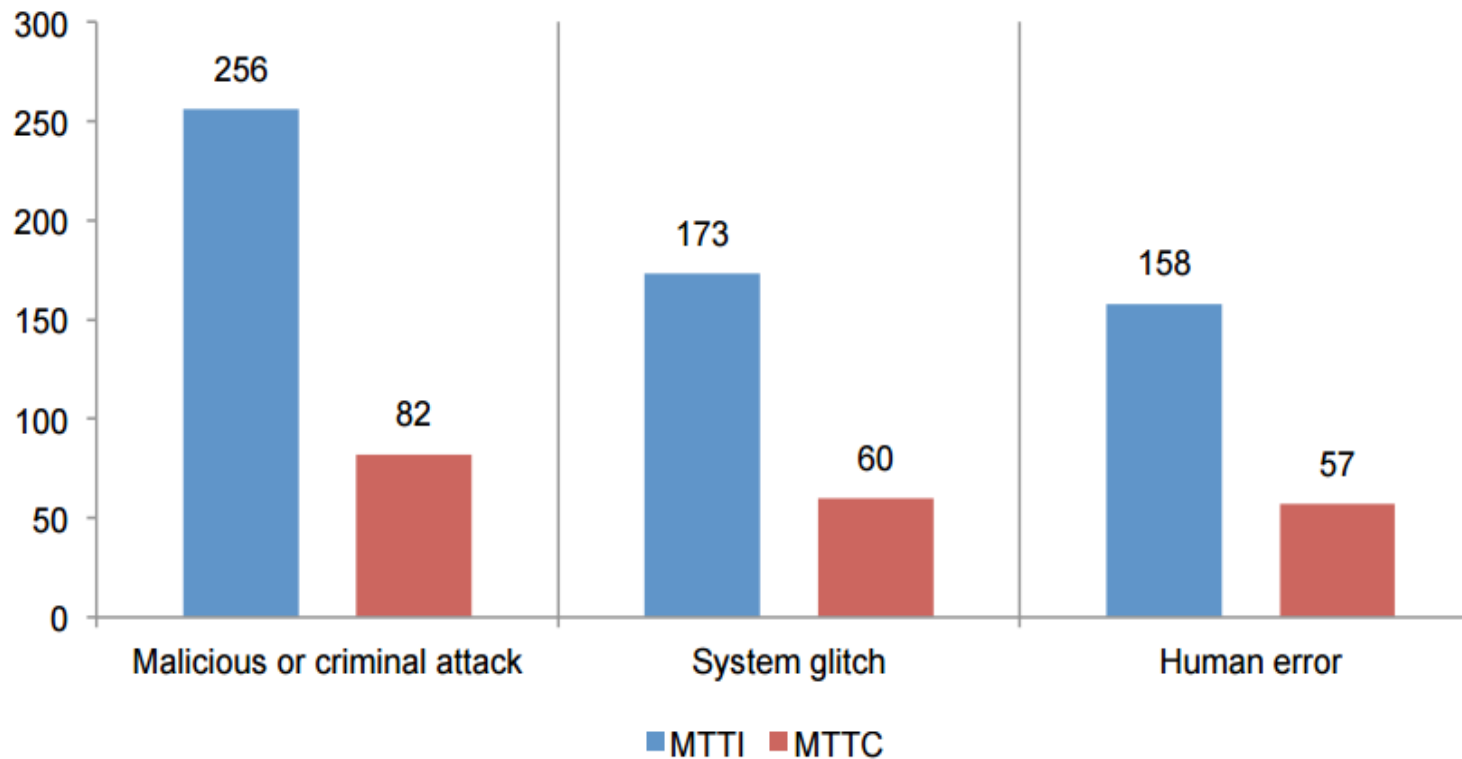
**Figure 8. Impact of 11 factors on the per capita cost of data breach**  
Consolidated view (n=350), measured in US\$



# Conceptos generales

- Tiempo de identificación y contención

**Figure 18. Mean time to identify and contain data breach incidents by root cause (in days)**  
Consolidated view (n = 350)



# Análisis de Riesgos

- Riesgos sobre nuestro puesto profesional
- Comunicar sin cesar



# Análisis de Riesgos

- ¿Sobre qué alcance haremos el análisis de riesgos?
- Alcance del SGSI – Proceso de Ciberseguridad
- Grave fallo: Errar en el alcance, objetivo general y objetivos específicos del SGSI
- Recordar que los activos raíz son los servicios/información

**Desafío.** Alcance, objetivo general y objetivos específicos para implantar un SGSI en una organización

# Análisis de Riesgos

- No existen catálogos completos de amenazas
- En función del ámbito y la metodología puede variar el enfoque
- Clasificaciones tradicionales
  - Origen natural
  - Origen industrial
  - Origen humano
- Los catálogos deben considerarse como un punto de partida y no como el total de las posibilidades

# Análisis de Riesgos

- Catálogo MAGERIT
  - Desastres naturales
    - Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta
    - Fuego, daños por agua, desastres naturales
  - Origen industrial
    - Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Pueden ocurrir de forma accidental o deliberada
    - Fuego, daños por agua, averías, cortes de electricidad
  - Errores y fallos no intencionados
    - Fallos no intencionados causados por las personas
    - Errores de usuarios, errores de administración, ..
  - Ataques intencionados
    - Fallos deliberados causados por las personas
    - Análisis de tráfico, extorsión, uso indebido



# Análisis de Riesgos

**Desafío.** Identificar posibles amenazas en cada una de las siguientes categorías

- Desastres naturales
- Errores y fallos no intencionados
- Ataques intencionados

# Análisis de Riesgos

- Las amenazas sobre los activos afectados tienen dos parámetros de estudio
  - Probabilidad de ocurrencia: cómo de probable o improbable es que se materialice una amenaza
  - Degradación en caso de ocurrencia: cómo de perjudicado resulta el valor del activo
- No todas las amenazas afectan de igual forma a las diferentes dimensiones de cada activo
- Cada metodología de AR empleará uno u otro enfoque

**100** → muy frecuente—a diario

5% → Degradación Baja

**10** → frecuente—mensualmente

30% → Degradación Media

**1** → normal—una vez al año

50% → Degradación Alta

**1/10** → poco frecuente – cada varios años

80% → Degradación Muy Alta

**1/100** → muy infrecuente—cada varias décadas

100% → Completa

# Análisis de Riesgos

- **Desafío.** Identificar amenazas que se den contra una organización determinada con cada una de las probabilidades indicadas
  - Muy frecuente – a diario
  - Frecuente – mensualmente
  - Normal – una vez al año
  - Poco frecuente – cada varios años
  - Muy infrecuente – cada varias décadas

# Análisis de Riesgos

- **Desafío.** Crear tablas de valoración de impactos para cada uno de los siguientes tipos de impactos
  - Daño medioambiental
  - Pérdidas económicas
  - Daño reputacional
  - Responsabilidades administrativas
  - Imposibilidad de operar o contratar
  - Pérdida de oportunidades de negocio

# Gracias

José Antonio Rubio

[jose.rubio.linkedin@gmail.com](mailto:jose.rubio.linkedin@gmail.com)





Somos  
#**UAX**makers