Seguridad Informática

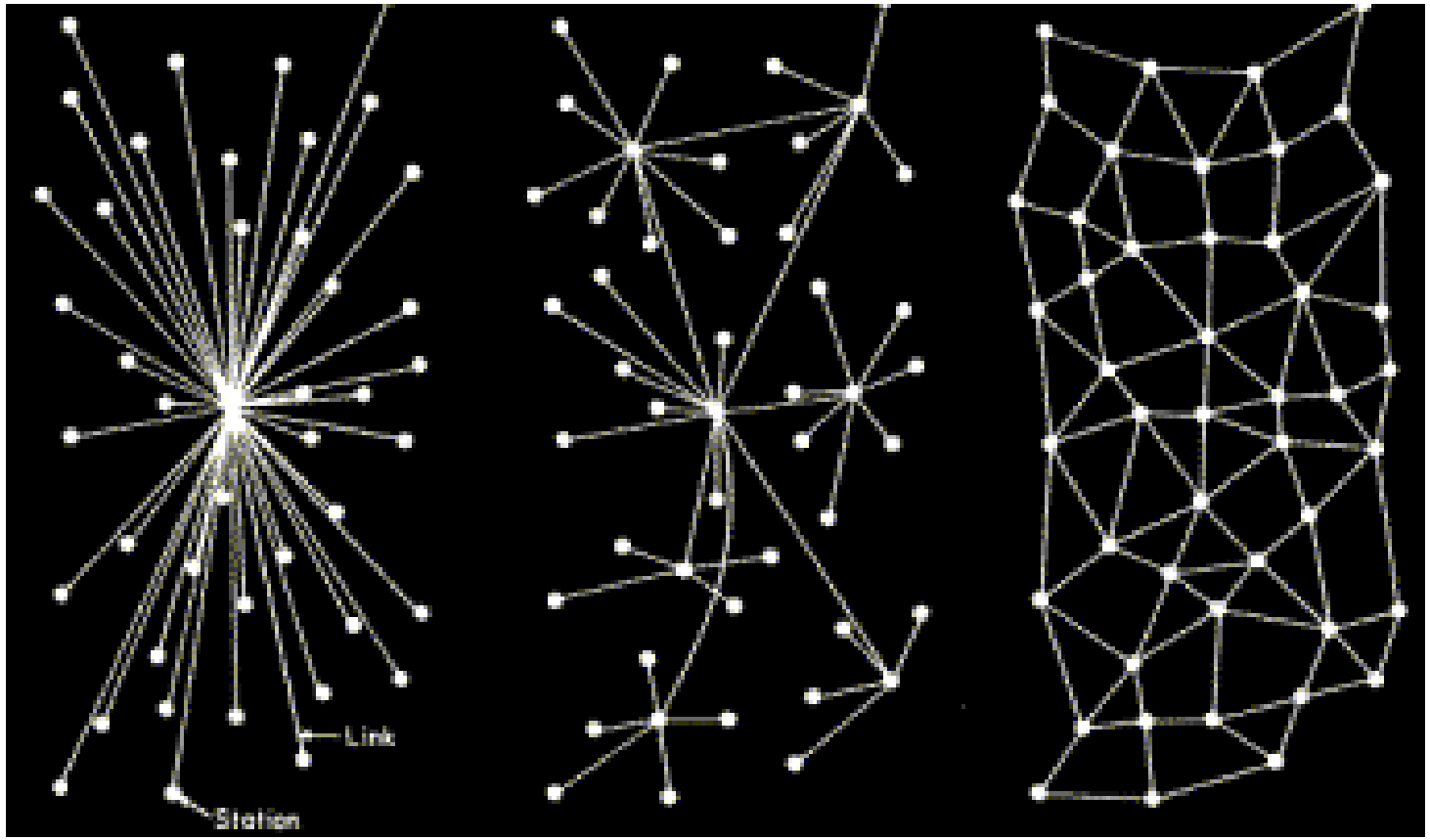
Profesor: Pedro Pinacho Davidson

ppinacho@inf.udec.cl

Contexto

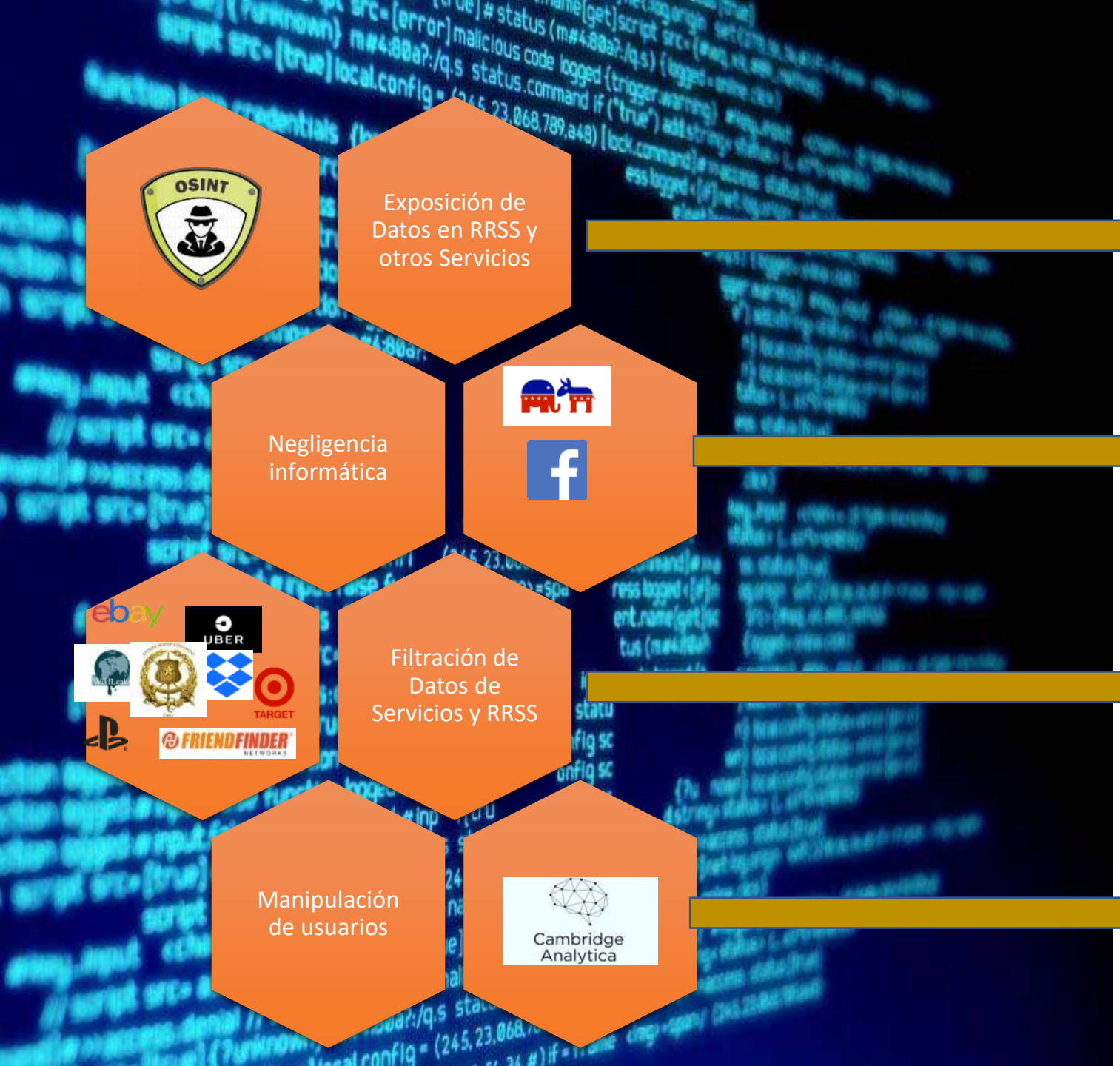
Historia Internet

- Memorando RM-3420-PR Agosto 1964, Paul Baran a Fuerza Aérea de EEUU.



Contexto Actual

Situación Actual



¿Qué tanto puede saber un atacante de nosotros?

¿Qué efecto tiene nuestro uso negligente de las TIC?

¿Puedo confiar ciegamente en la seguridad de servicios TI?

¿Sabemos a que nos exponemos en RRSS?

Sin considerar el riesgo asociado a Modelos IA Generativos

CIBERSEGURIDAD

- La ciberseguridad es la **práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos**. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica.

- La Seguridad de la Información es **preservación de la confidencialidad, integridad y disponibilidad de la información**.
    - NCh2777, NCh-ISO27002:2013

Definición de data breach

- Incidentes desde donde se **roba información** de organización afectada
- Datos:
    - Sensibles
    - Propietarios
    - Confidenciales
    - Datos de clientes
    - Secretos comerciales
    - Seguridad Nacional.

USD 4.45M

Average total cost of a breach
The average cost of a data breach reached an all-time high in 2023 of USD 4.45 million. This represents a 2.3% increase from the 2022 cost of USD 4.35 million. Taking a long-term view, the average cost has increased 15.3% from USD 3.86 million in the 2020 report.

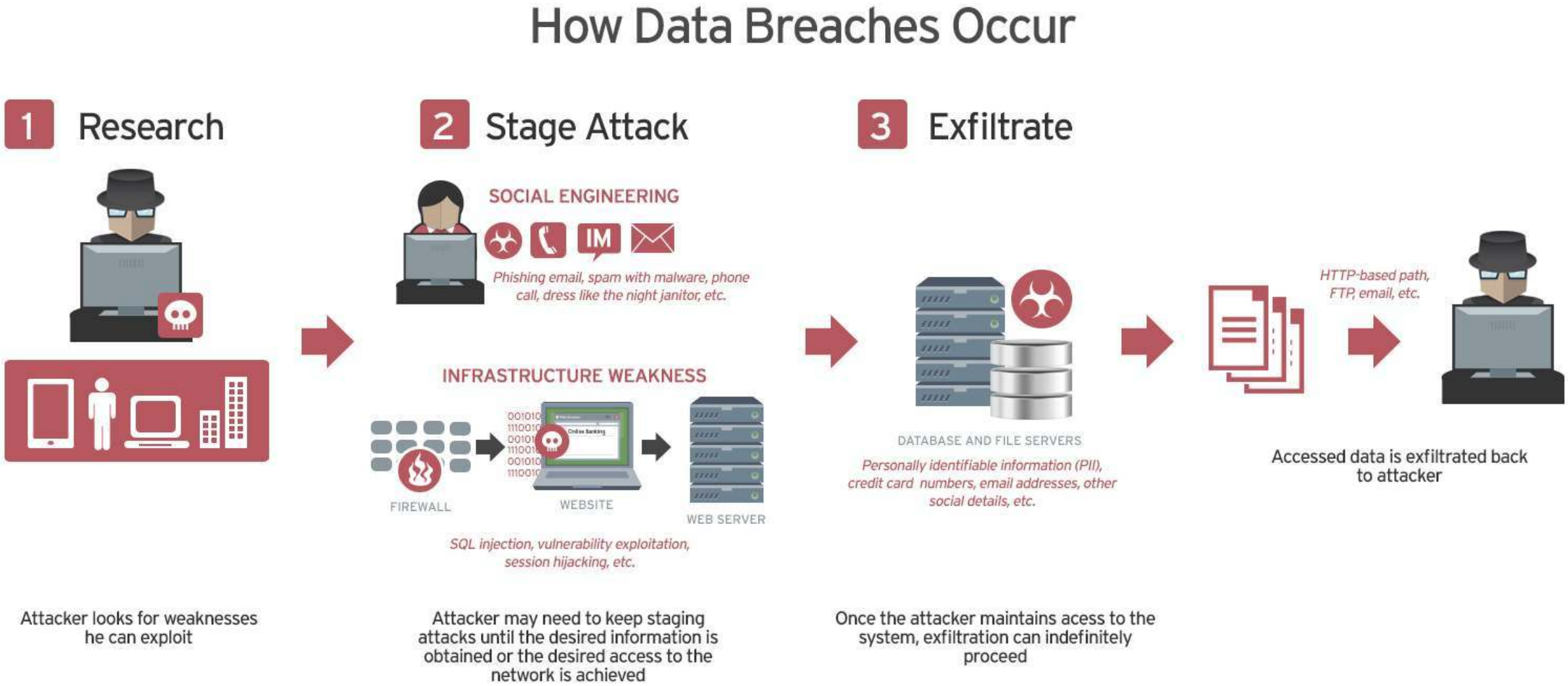
51%

Percentage of organizations planning to increase security investments as a result of a breach
While data breach costs continued to rise, report participants were almost equally split on whether they plan to increase security investments because of a data breach. The top areas identified for additional investments included incident response (IR) planning and testing, employee training, and threat detection and response technologies.

USD 1.76M

The effect of extensive security AI and automation on the financial impact of a breach
Security AI and automation were shown to be important investments for reducing costs and minimizing time to identify and contain breaches. Organizations that used these capabilities extensively within their approach experienced, on average, a 108-day shorter time to identify and contain the breach. They also reported USD 1.76 million lower data breach costs compared to organizations that didn't use security AI and automation capabilities.

¿Cómo ocurre un brecha de datos?



1 in 3

Number of breaches identified by an organization's own security teams or tools
Only one-third of companies discovered the data breach through their own security teams, highlighting a need for better threat detection. 67% of breaches were reported by a benign third party or by the attackers themselves. When attackers disclosed a breach, it cost organizations nearly USD 1 million more compared to internal detection.

USD 1.49M

Cost savings achieved by organizations with high levels of IR planning and testing
In addition to being a priority investment for organizations, IR planning and testing emerged as a highly effective tactic for containing the cost of a data breach. Organizations with high levels of IR planning and testing saved USD 1.49 million compared to those with low levels.

USD 1.68M

Cost savings from high levels of DevSecOps adoption
Integrated security testing in the software development process (DevSecOps) showed sizable ROI in 2023. Organizations with high DevSecOps adoption saved USD 1.68 million compared to those with low or no adoption. Compared to other cost-mitigating factors, DevSecOps demonstrated the largest cost savings.

82%

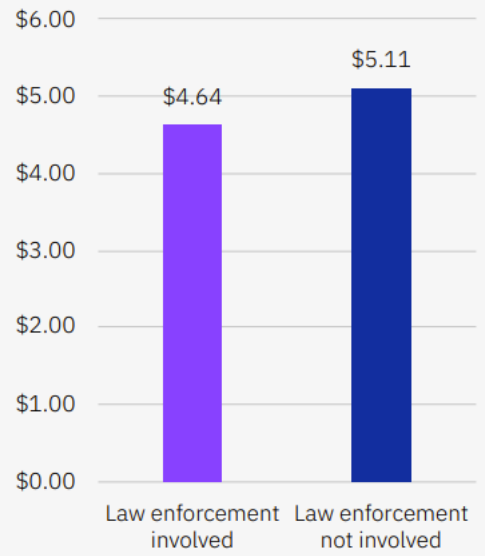
The percentage of breaches that involved data stored in the cloud—public, private or multiple environments
Cloud environments were frequent targets for cyberattackers in 2023. Attackers often gained access to multiple environments, with 39% of breaches spanning multiple environments and incurring a higher-than-average cost of USD 4.75 million.

$4.62m

Average
total cost of a
ransomware breach

Ransomware and destructive attacks were costlier than other types of breaches.

Cost of a ransomware attack by law enforcement involvement



Costo Promedio de Data Breach

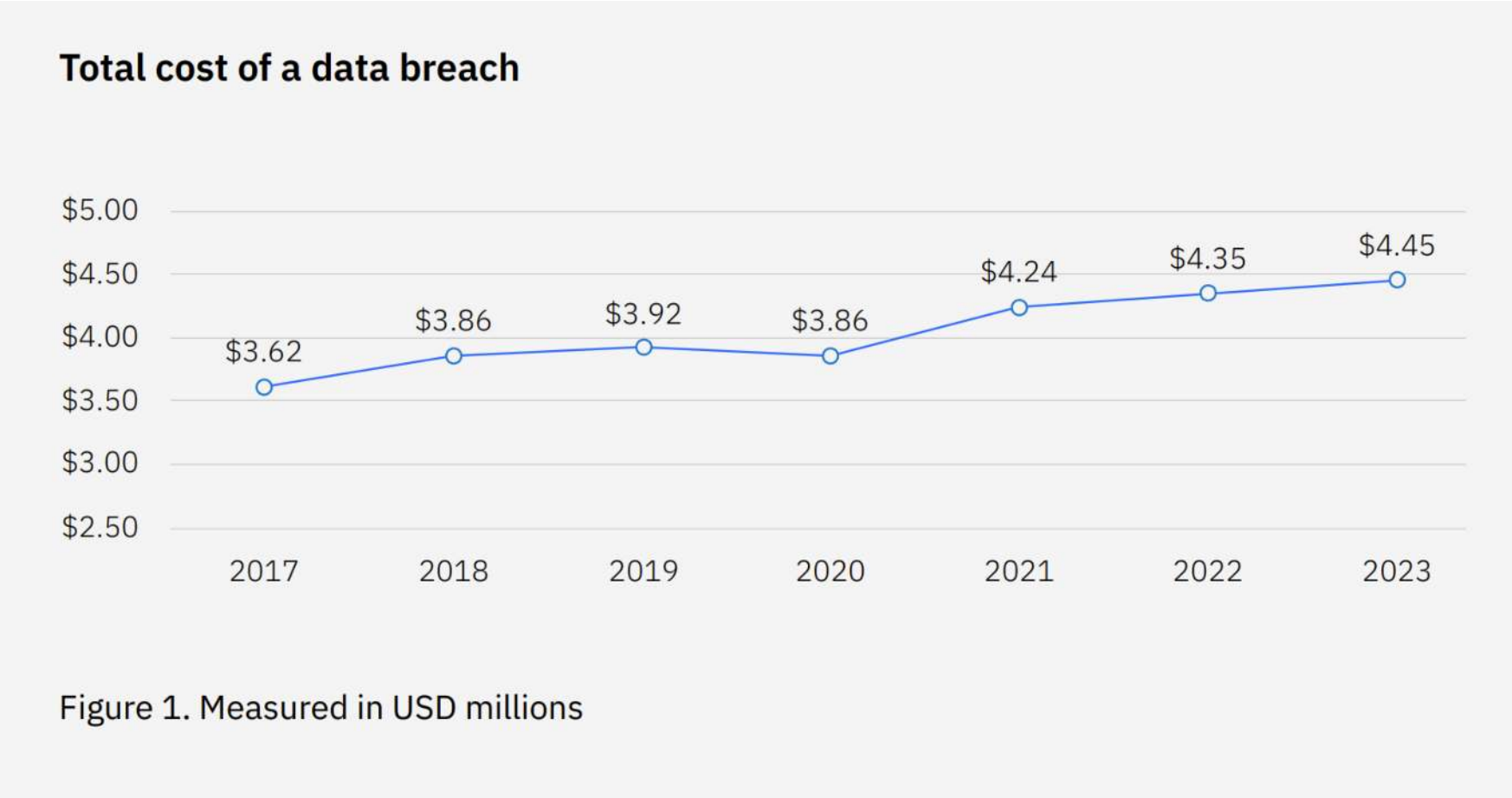


Figure 1. Measured in USD millions

Costo por registro de Data Breach

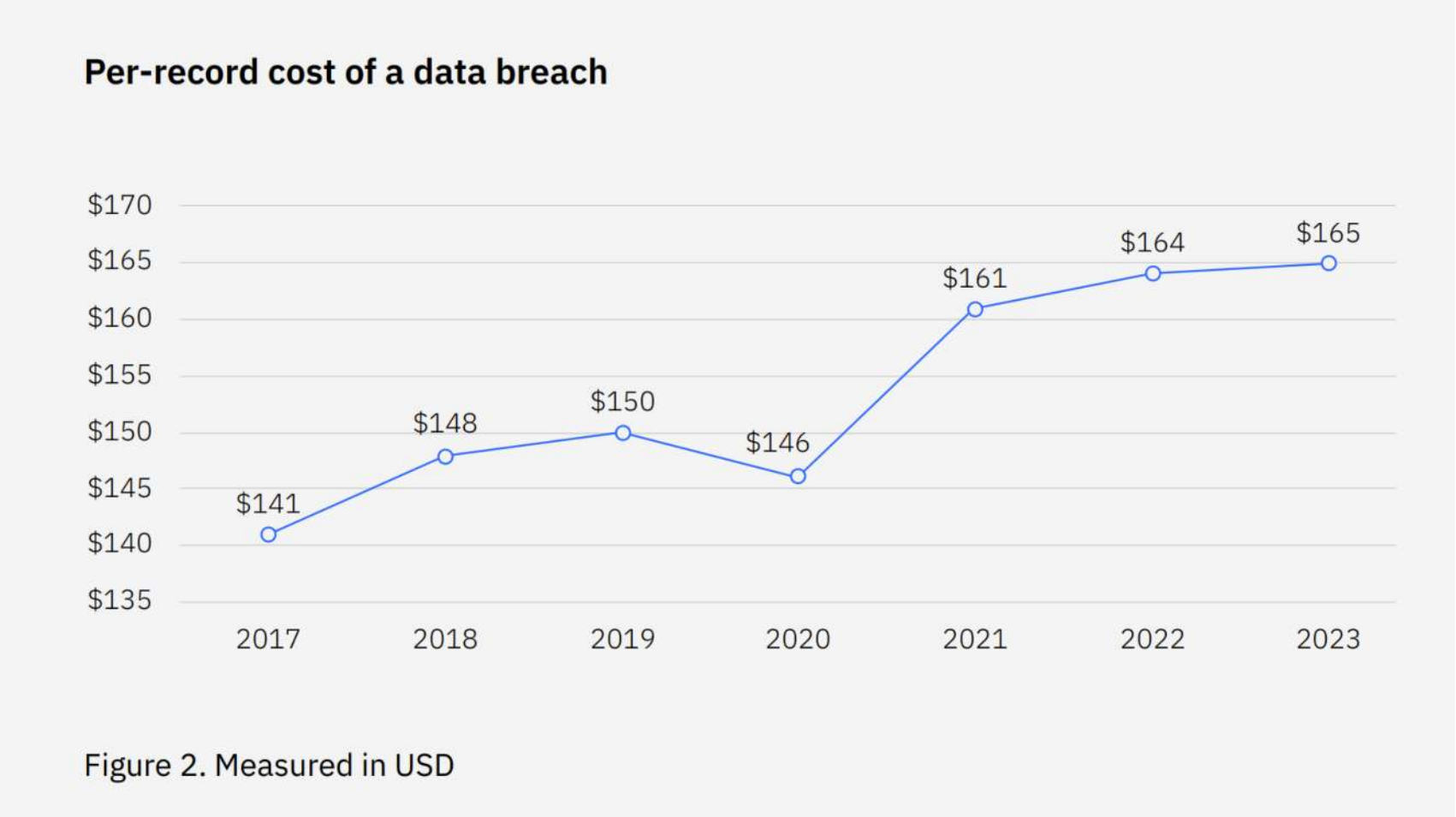
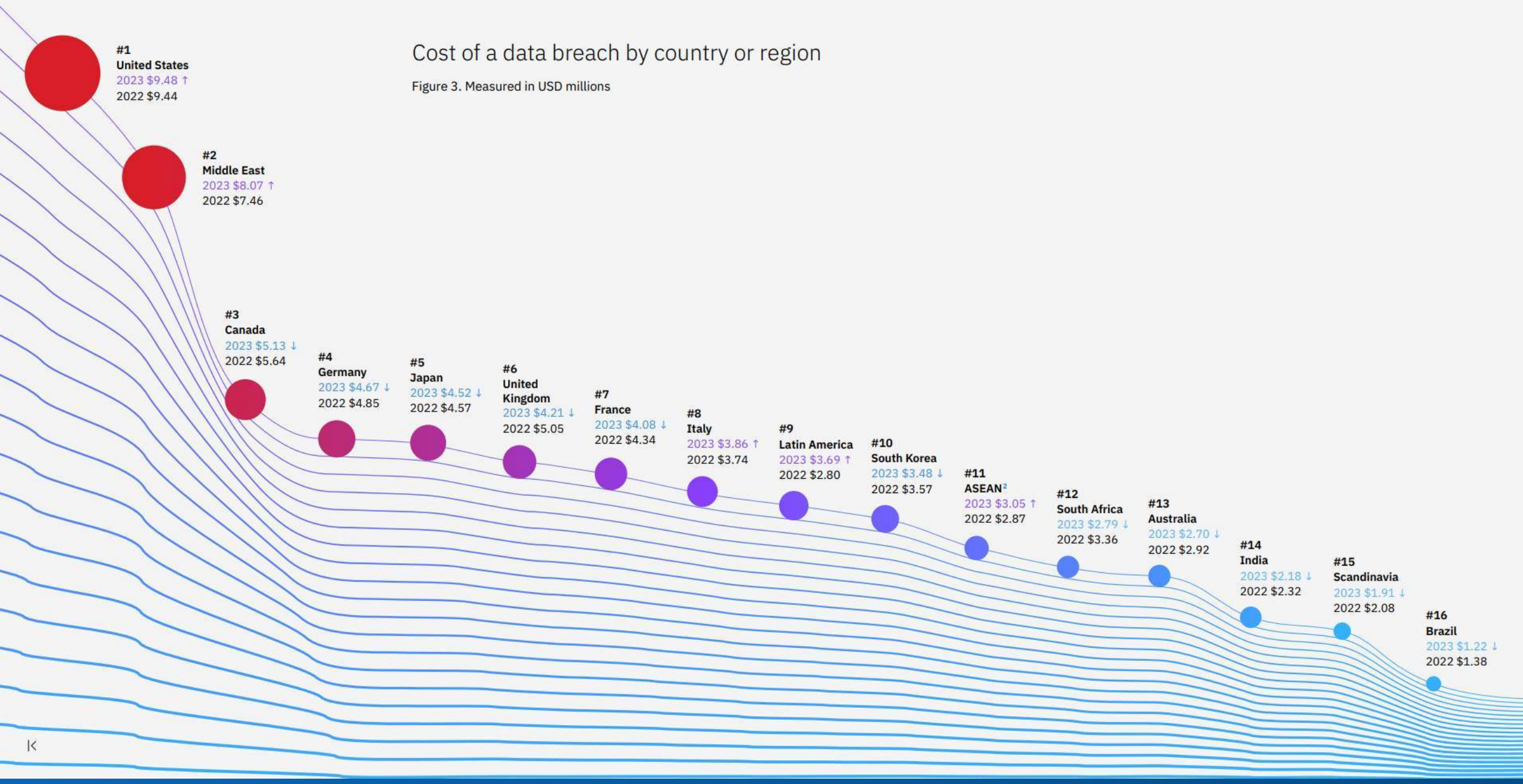


Figure 2. Measured in USD

Cost of a data breach by country or region

Figure 3. Measured in USD millions



Costo promedio de data breach por industria

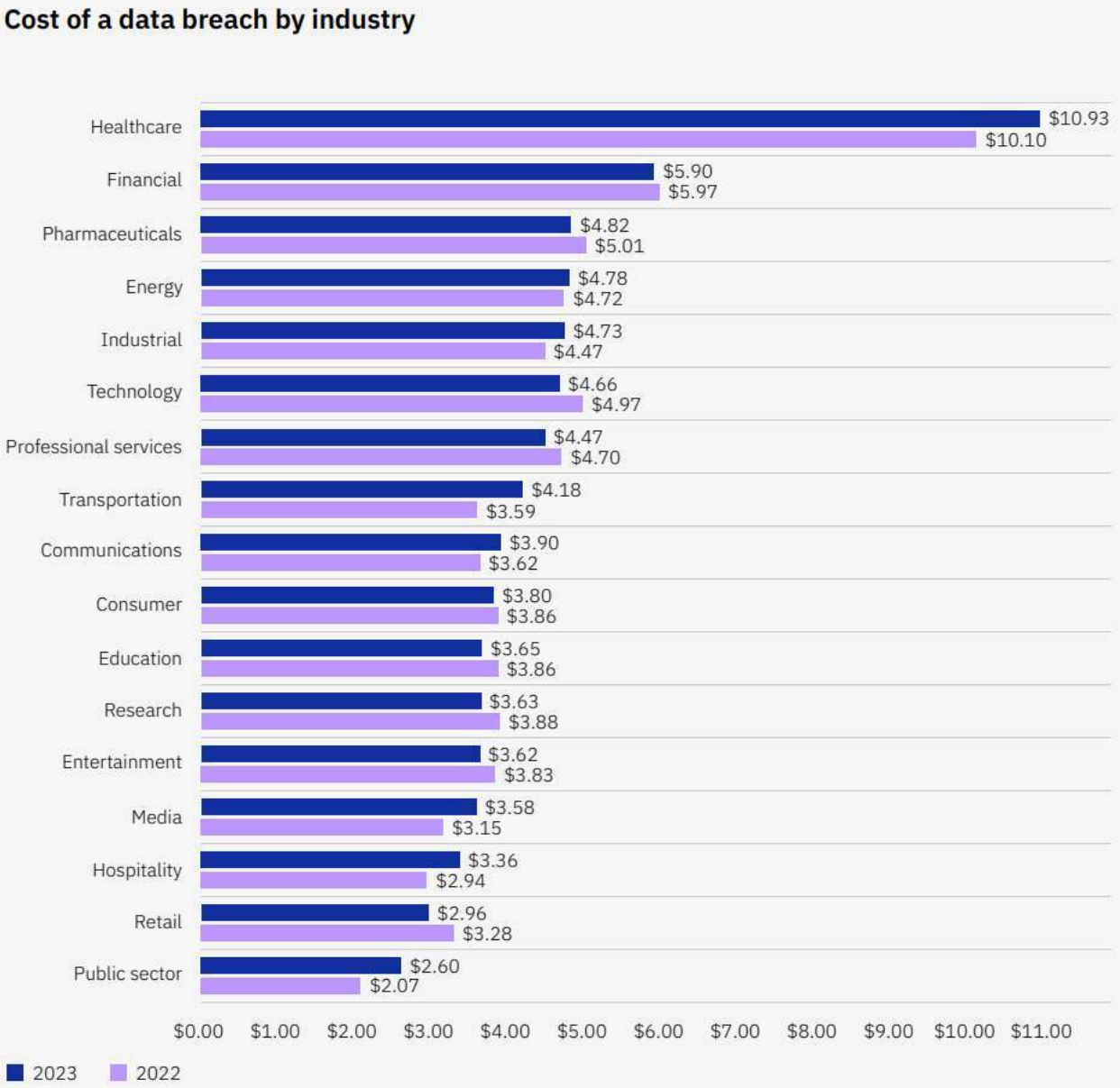
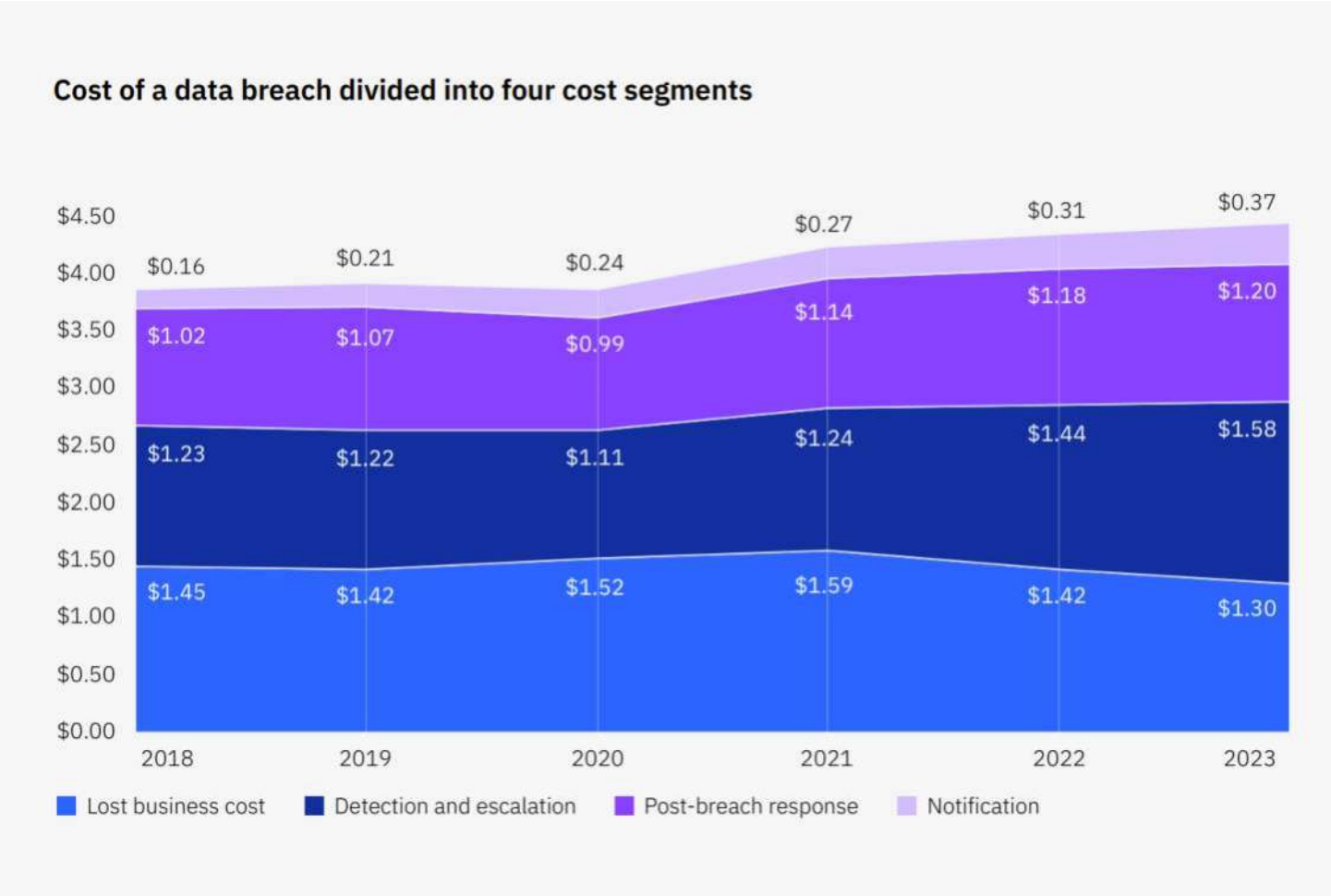
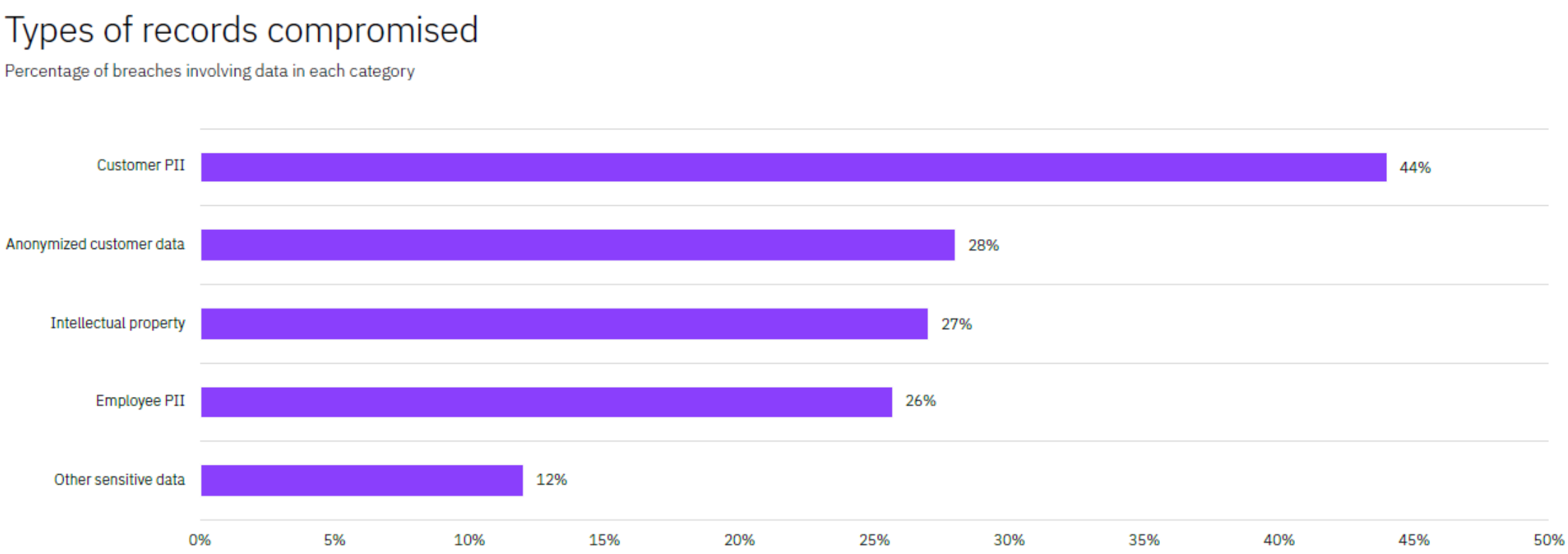


Figure 4. Measured in USD millions

Costo total de data breach dividido en cuatro categorías



Tipos de registros comprometidos



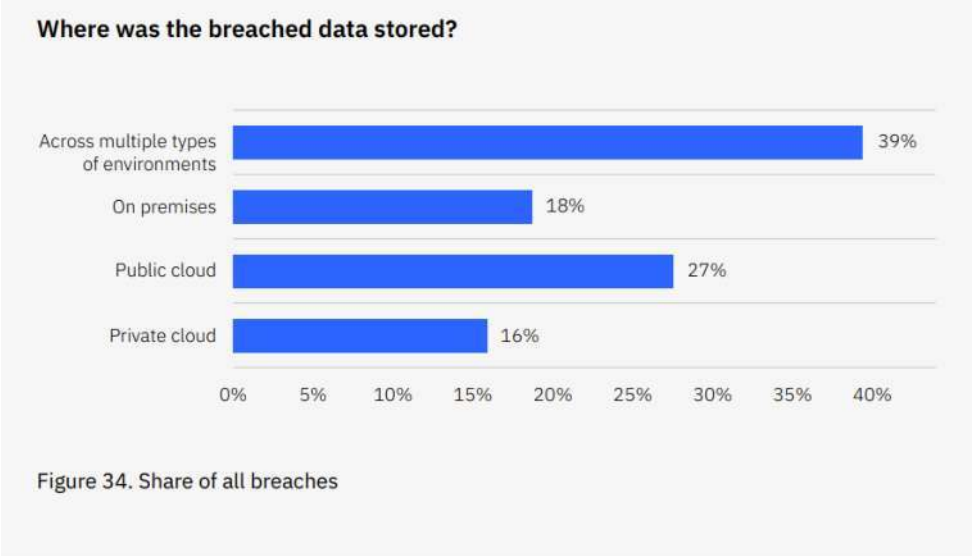


Figure 34. Share of all breaches

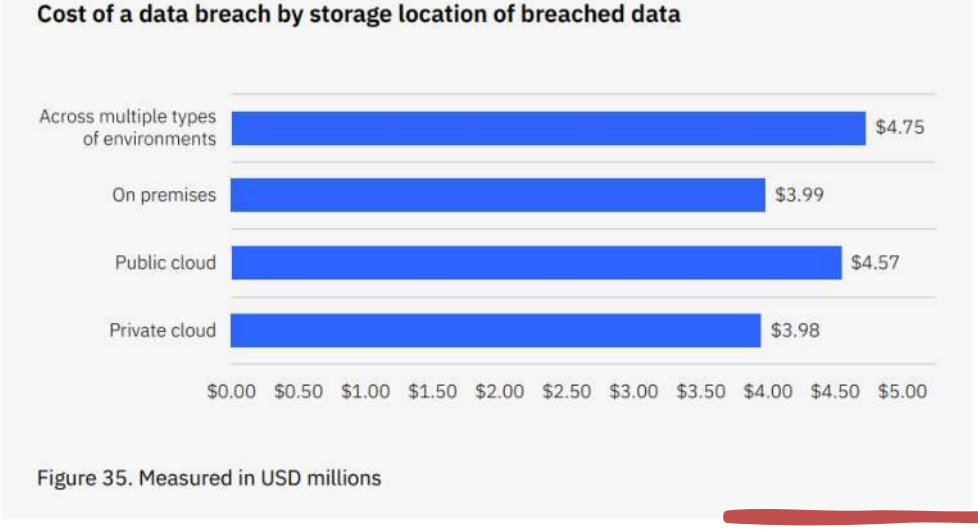


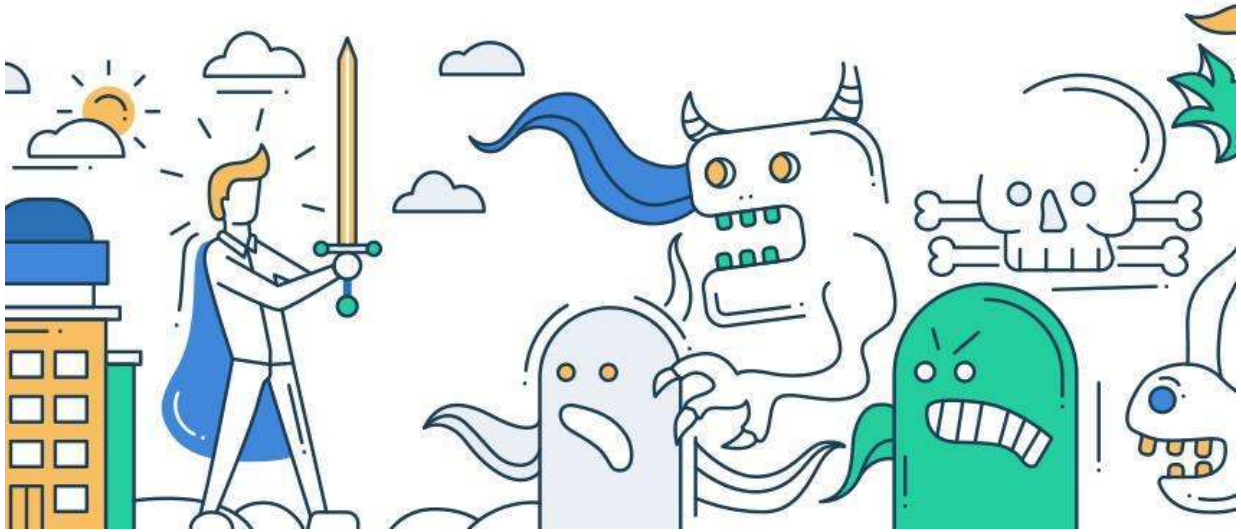
Figure 35. Measured in USD millions

[Adiós a la nube: por qué las empresas están volviendo a ser dueñas de su infraestructura (xataka.com)]

Cloud no e garantía de seguridad

Definición de Vector de Ataque

Ruta o camino que utiliza un atacante para tener acceso a su objetivo



Key finding

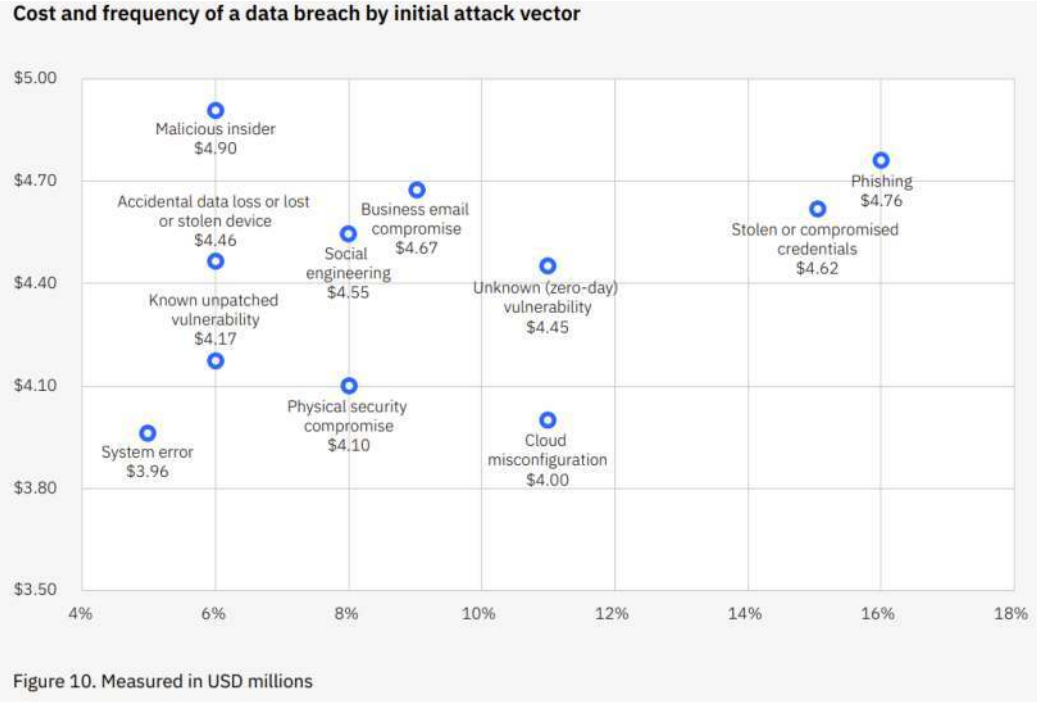
$5.01m

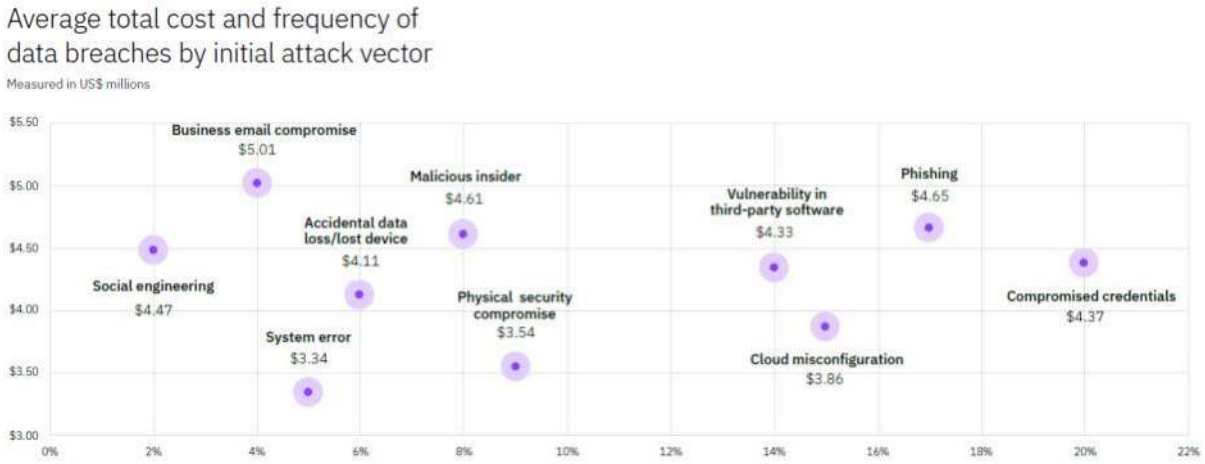
Average total cost of a breach caused by business email compromise

Vectores de Ataque comunes

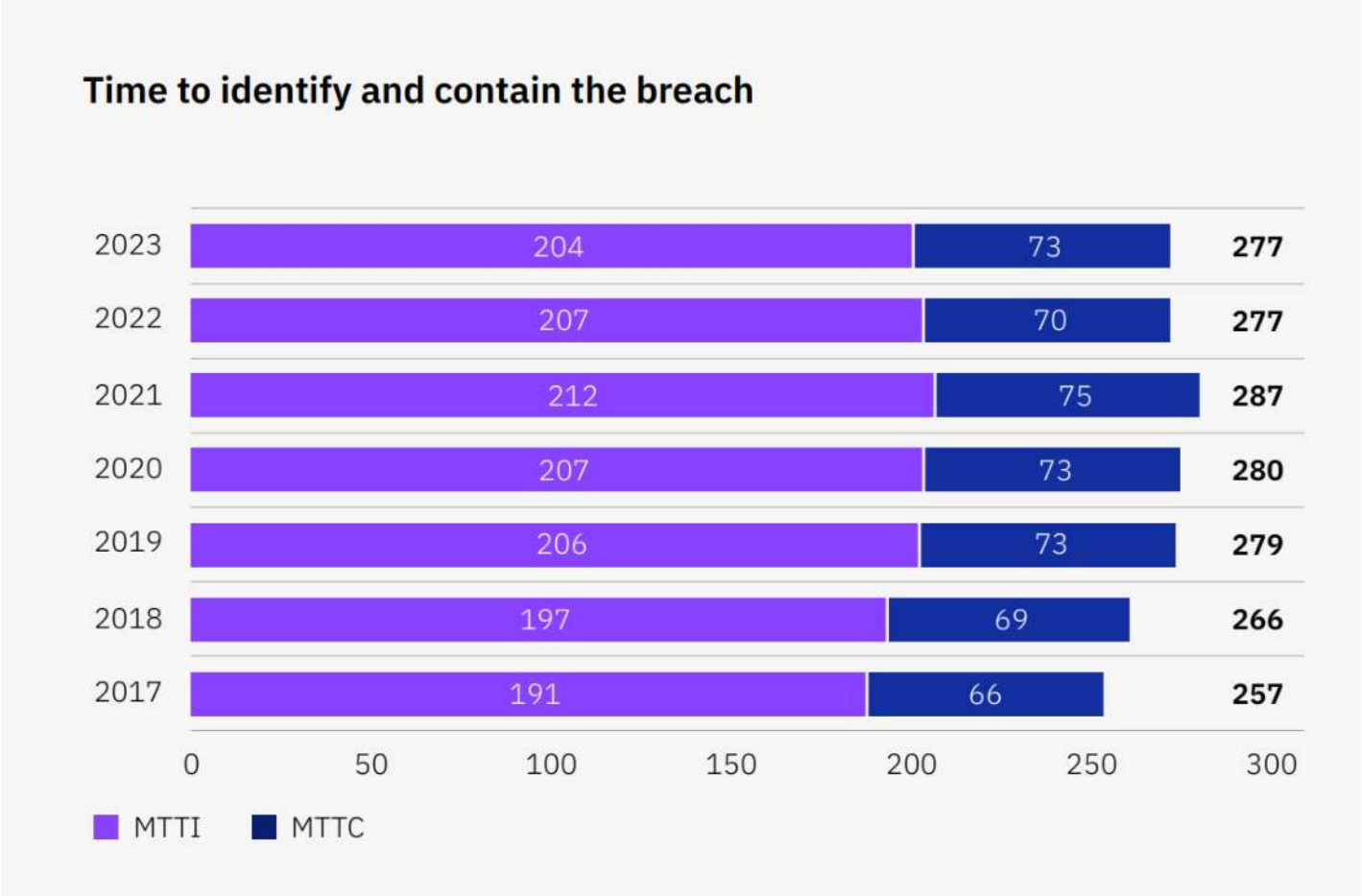
- Credenciales comprometidas
- Compromiso de correos corporativos
- Insiders
- Phishing
- Compromiso de Seguridad Física
- Ingeniería Social
- Vulnerabilidad de software de terceros
- Pérdida accidental de datos o dispositivos
- Configuración deficiente de Cloud
- Otras configuraciones deficientes

Costo promedio y frecuencia de data breach por vector de ataque inicial

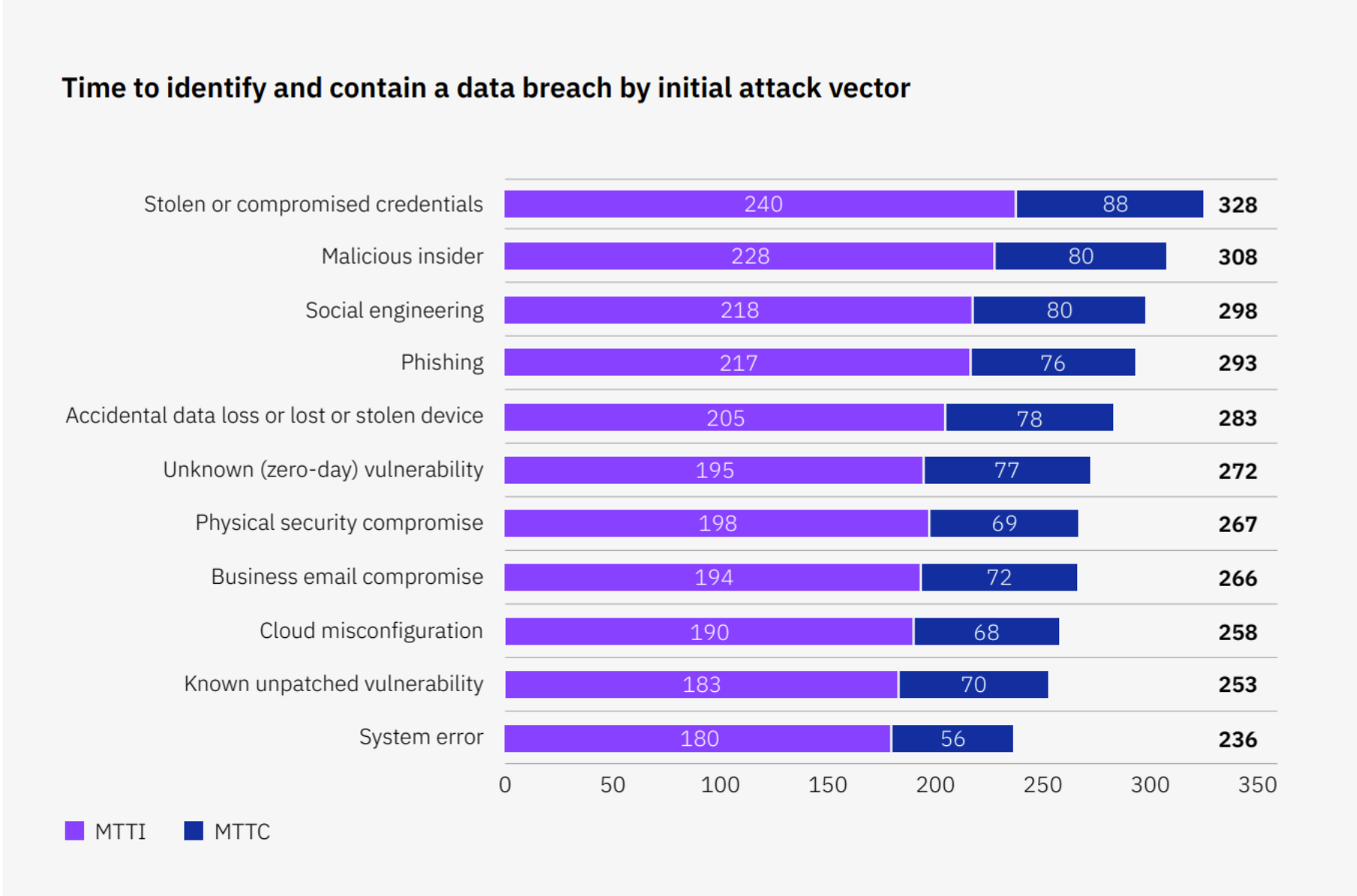




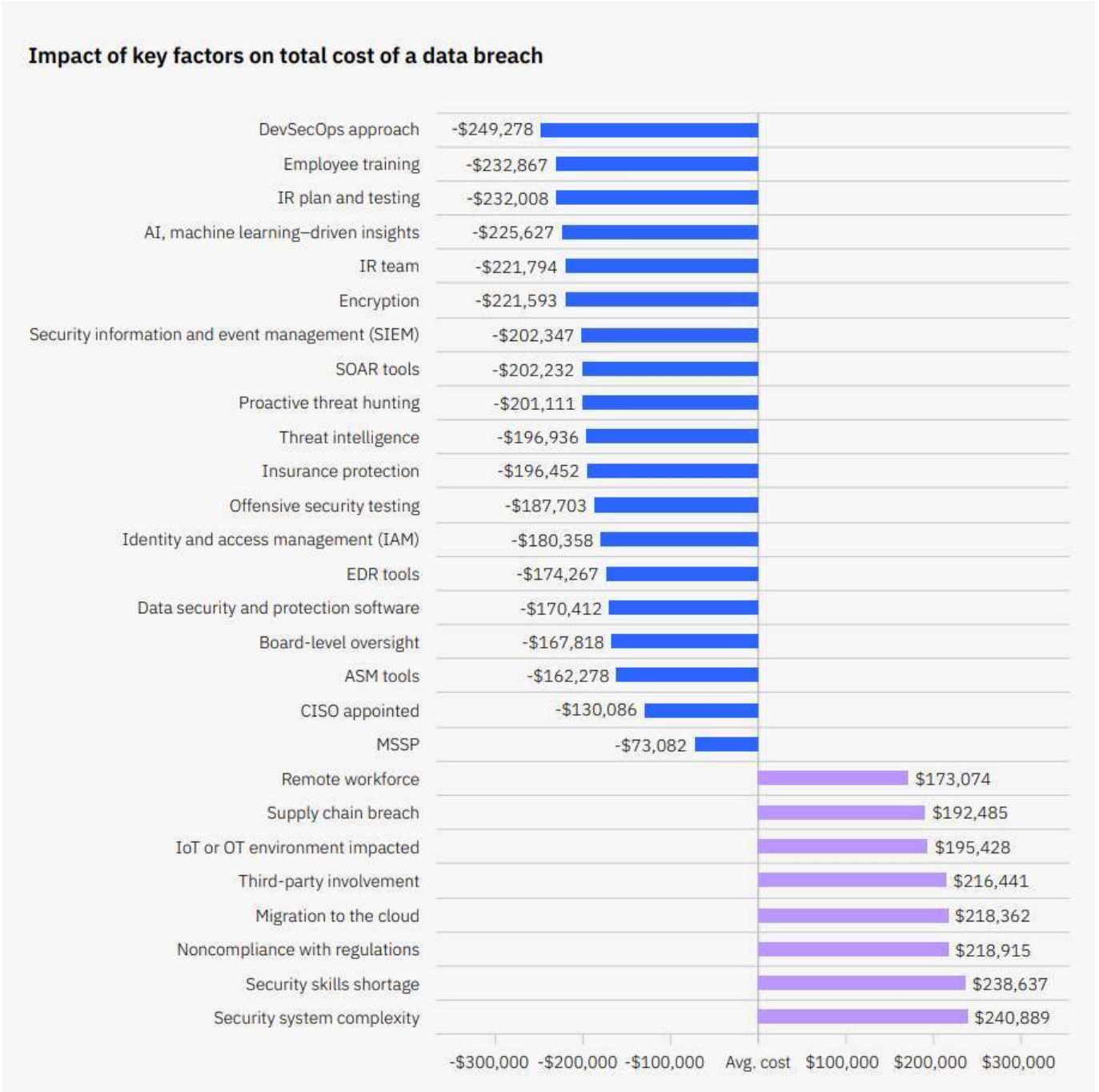
Tiempo promedio para identificar y contener un data breach



Tiempo promedio para identificar y contener un data breach por vector de ataque inicial



- Impacto de fatores claves en costo total de un brecha de datos



COVID-19 consideraciones

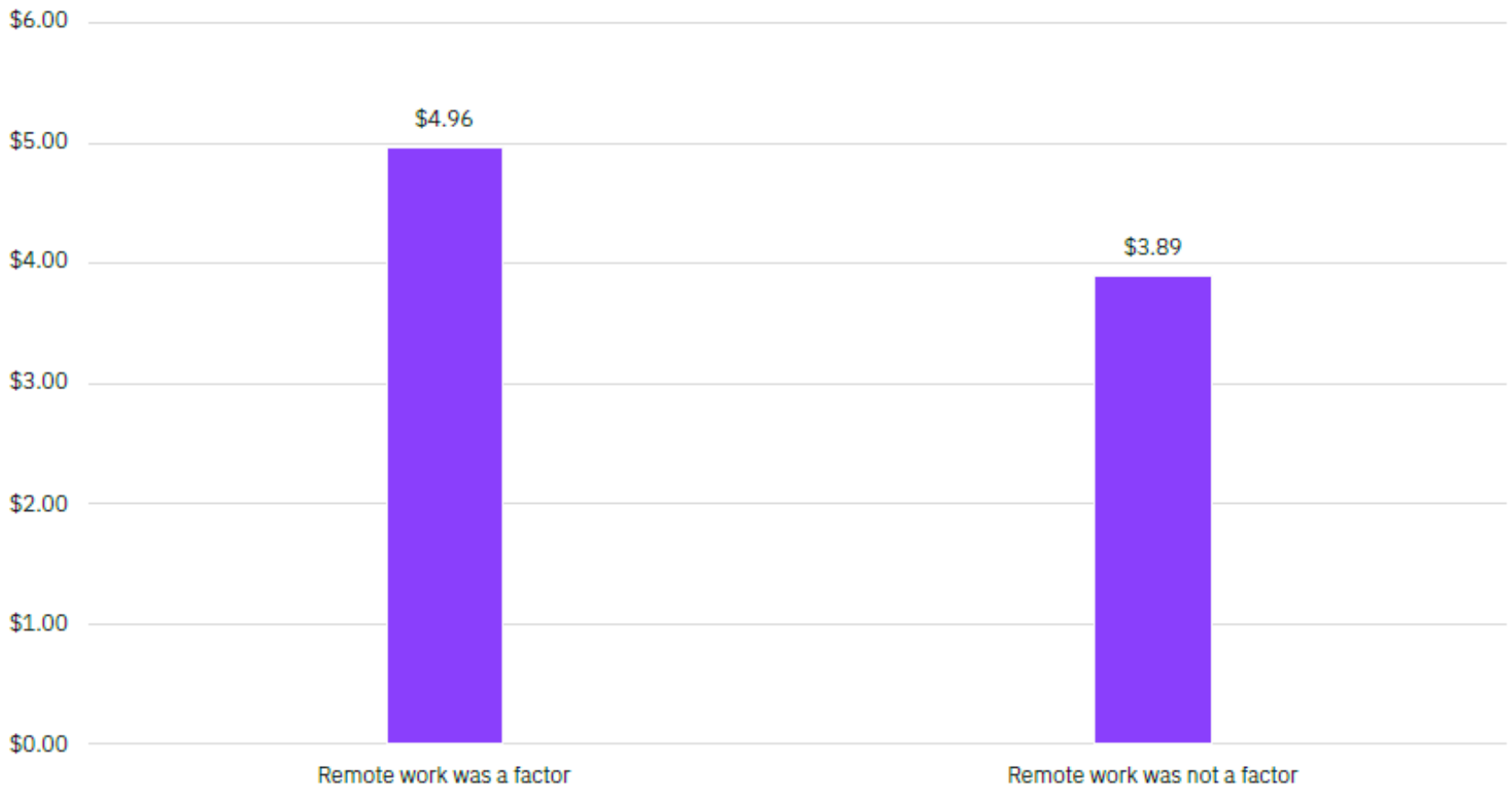
Empresas forzadas a operar remotamente

Inexperiencia en Teletrabajo seguro

Especialización de delincuencia en vulnerabilidades asociadas

Average cost of a data breach where remote work was a factor

Measured in US$ millions



NATURALEZA DE LAS AMENAZAS

Figure 2. Who are the victims?

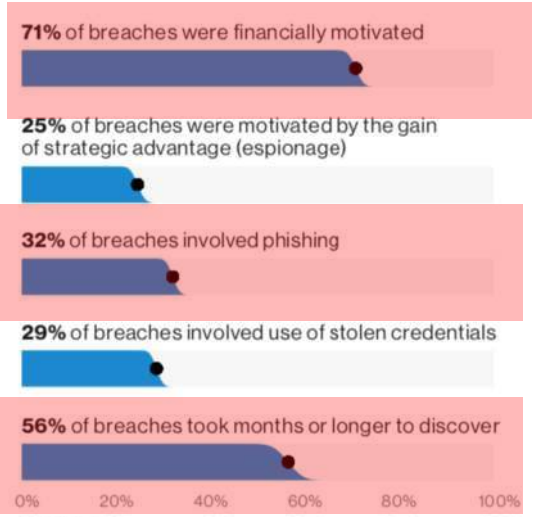


Figure 5. What are other commonalities?

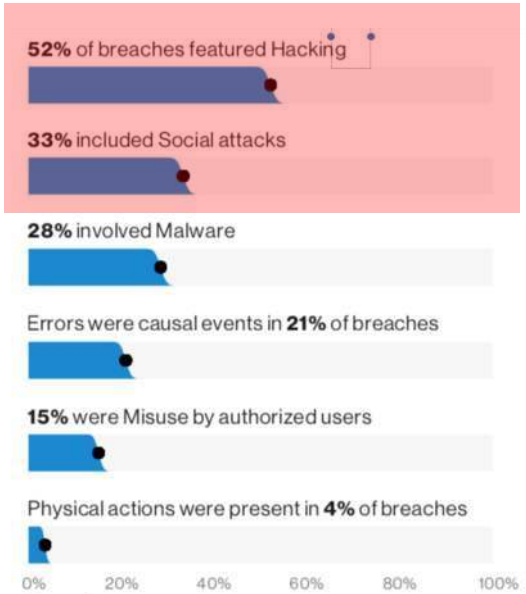


Figure 3. What tactics are utilized?

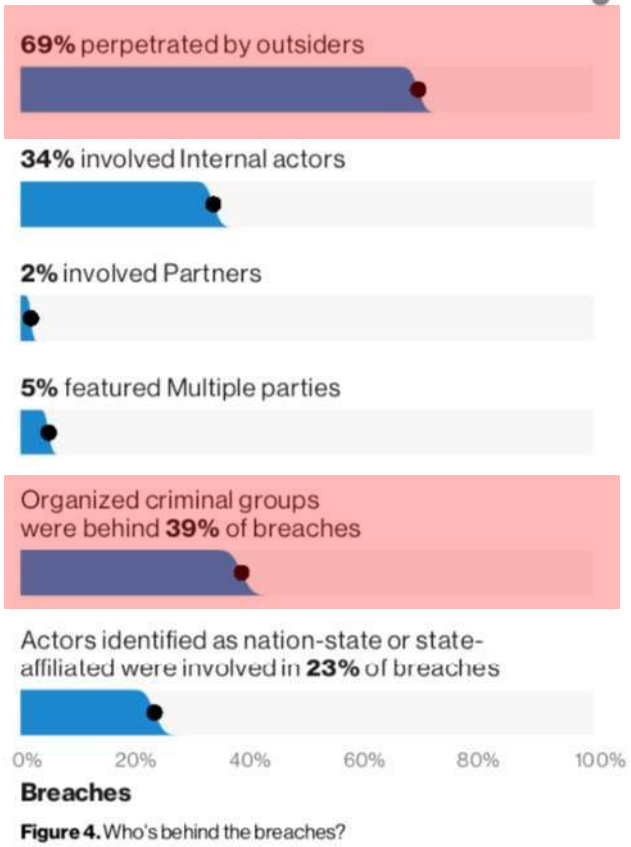


Figure 4. Who's behind the breaches?

NATURALEZA DE LAS AMENAZAS

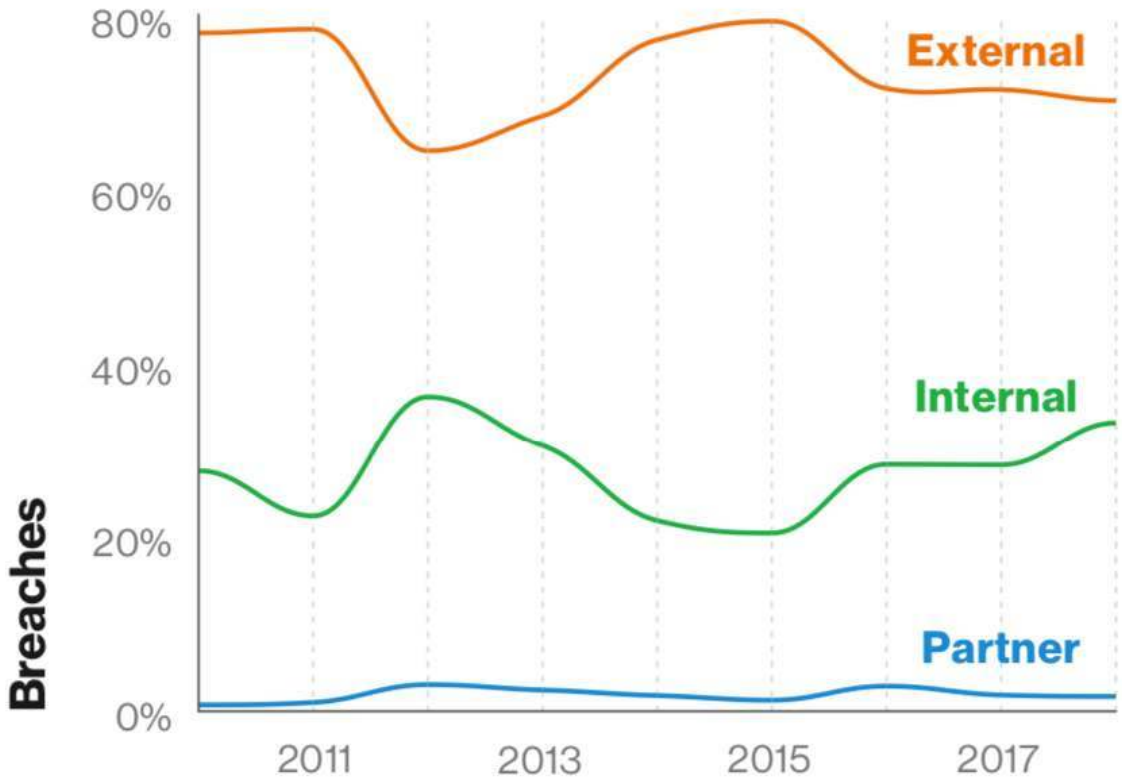


Figure 6. Threat actors in breaches over time

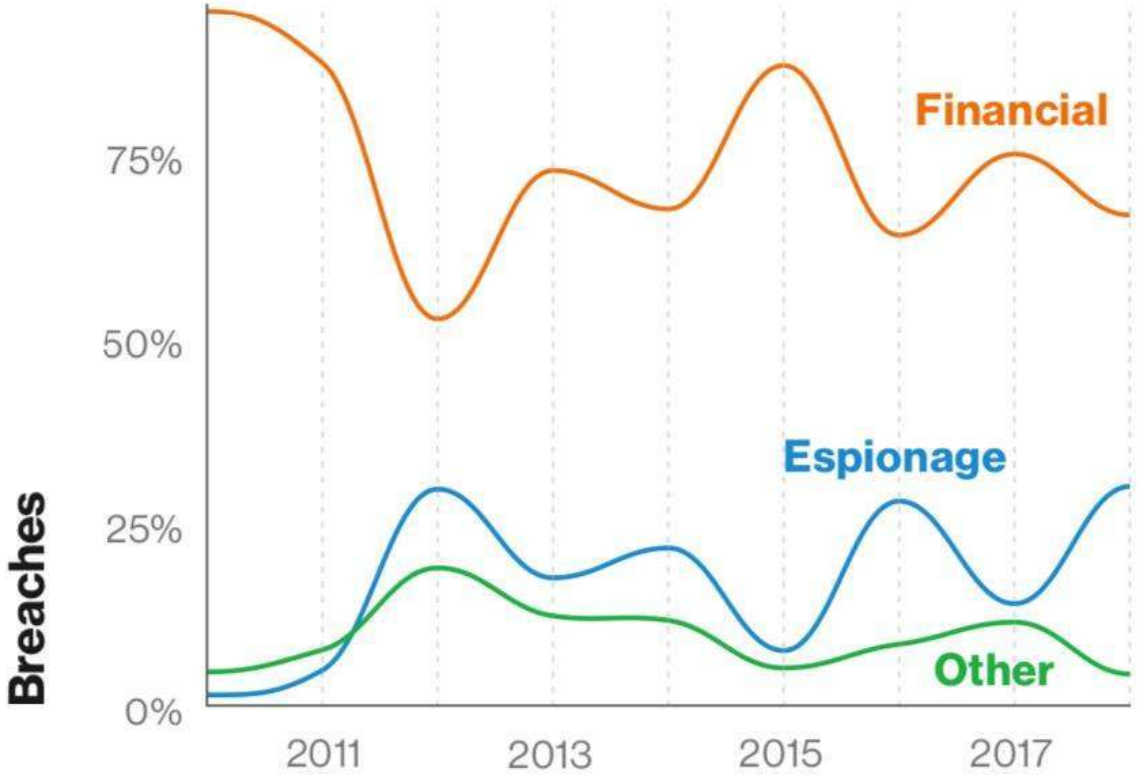


Figure 7. Threat actor motives in breaches over time

NATURALEZA DE LAS AMENAZAS

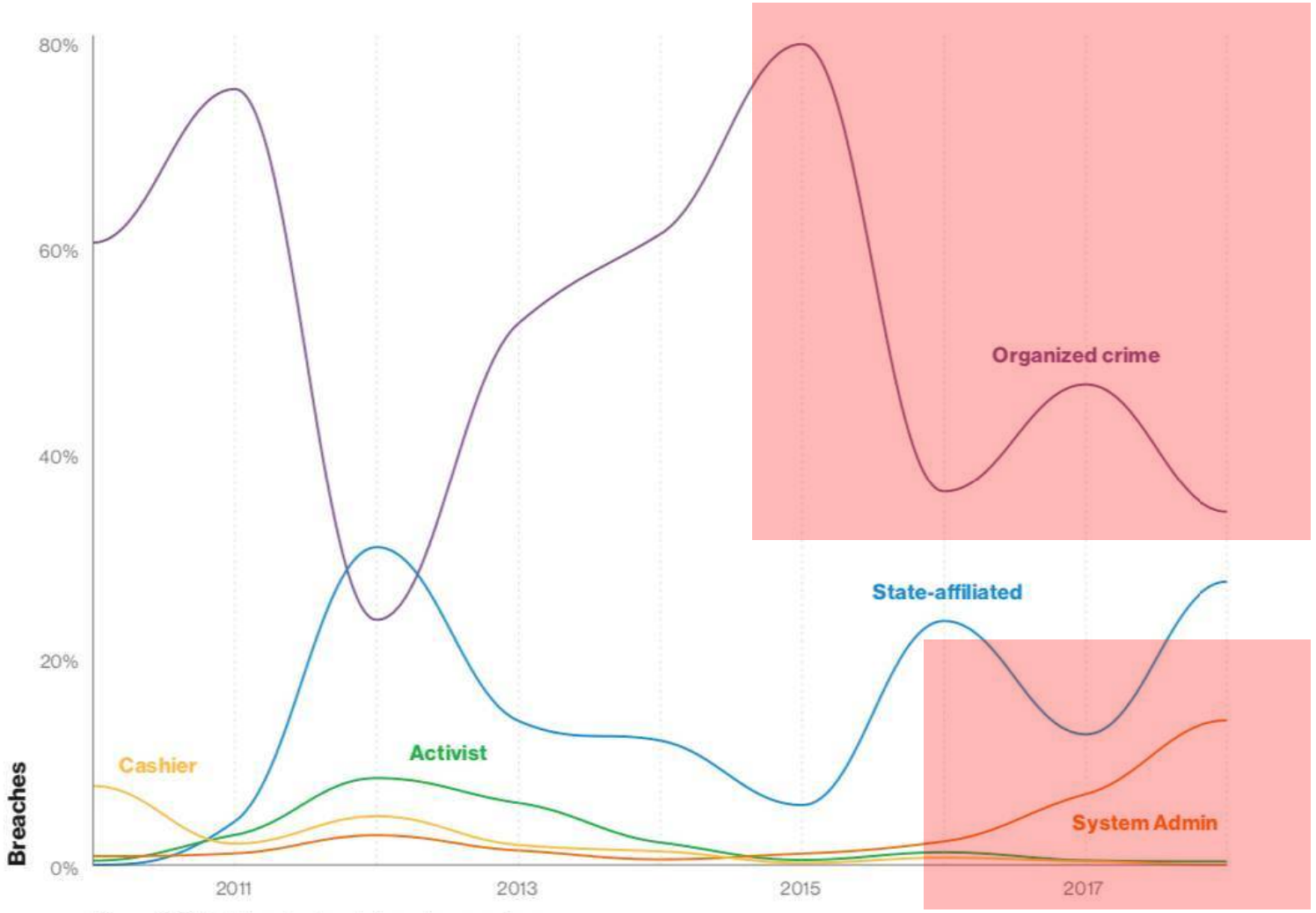


Figure 8. Select threat actors in breaches over time

¿Cómo han sido los últimos años?

1. Los mayores costos se asociaron a **pérdidas de negocios**.
2. Las brechas de datos causarán **daños por años** en los afectados.
3. **Ciclos de vida** de robos de datos y contención **más largos**.
4. **Ataques maliciosos**, principal causa de pérdida/robo de datos.
5. Pérdidas por fallas de sistemas y errores humanos siguen costando millones.
6. Medidas tecnológicas **mitigan los costos**.
7. Tener **personal especializado** de respuesta reduce los costos.
8. Medidas de **seguridad automáticas** reducen costos.
9. Los **Servicios Cloud no son garantía de seguridad**