SECURENINJA

Shakeel

SecureNinja

The CyberSecurity Experts

Chief Ninja (CEO)

Washington DC

SecureNinja

The CyberSecurity Experts

Pentagon Force Protection Agency

US Air Force

SecureNinja

America Online

Cigital

JP Morgan

General Dynamics

CompUSA

Fortify

Hewlett Packard

What Are We Trying To Protect?

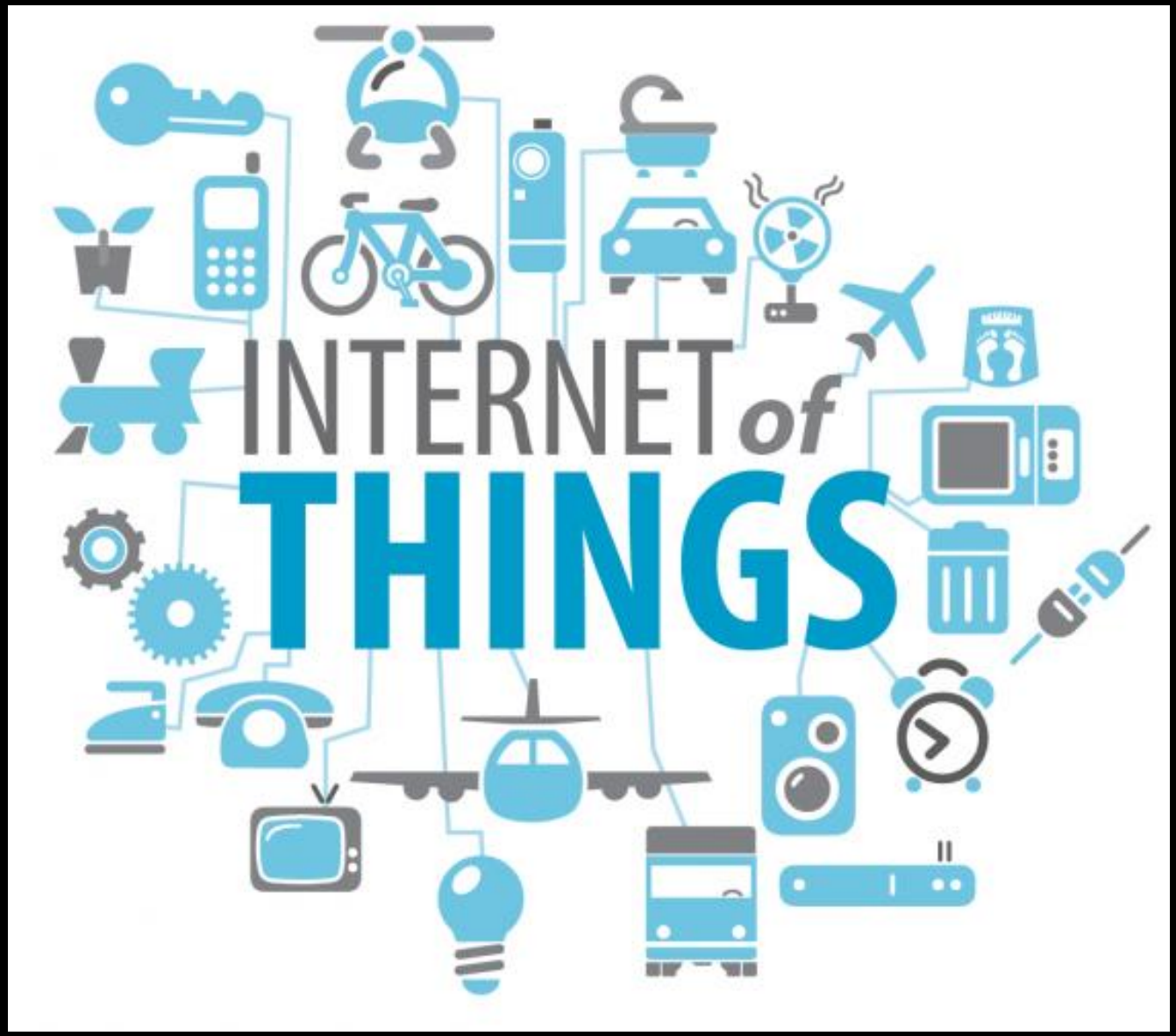
- The valuable properties of anything is considered an asset
  - Data – CIA, privacy, accountability
  - Time – Launch delay, processing delay, etc.
  - Money – can't make sales, can't process transactions
  - Reputation and Brand – loss of trust
  - Legal – compliance, contractual regulation
  - Government -Military, Intel; Mission Critical Systems

The “Human” Weakness

Humans are consistently the weakest link for security issues in any organization

The “Enterprise” Weakness

Organizations cannot rapidly improve their security posture as fast as technology changes.



SecureNinja

The CyberSecurity Experts

CyberSecurity Challenges

- Connectivity & Internet of Things
  - More users are connecting, not less!
  - Think mobile, web, internet, intranet, even Classified
- Increasing Complexity
  - Systems are getting bigger & distributed faster than ever!
  - More technologies, software components, interfaces!
- Extensibility / 3rd Party / Partners
  - Systems are constantly evolving and changing on the fly!
  - More frameworks, plugins, open source software, API's
- Compliance, Regulations, & Standards
  - Security regulations, rules, audits, etc. are confusing

The (In)Security Problem - Verizon Report 2013

- 18 Organizations, 27 countries, 621 Breaches, 47K Incidents
- 78% of intrusions took little or no specialist skills
- 75% of attacks were opportunistic, companies weren't targeted
- 62% of breach detection takes months or years
- 70% of breaches discovered by 3rd party
- Top motivations for security breach - Financial and Espionage

The (In)Security Problem - Verizon Report 2013

Who are the victims?

37% of breaches affected financial organizations (+)

24% of breaches occurred in retail environments and restaurants (-)

20% of network intrusions involved manufacturing, transportation, and utilities (+)

20% of network intrusions hit information and professional services firms (+)

38% of breaches impacted larger organizations (+)

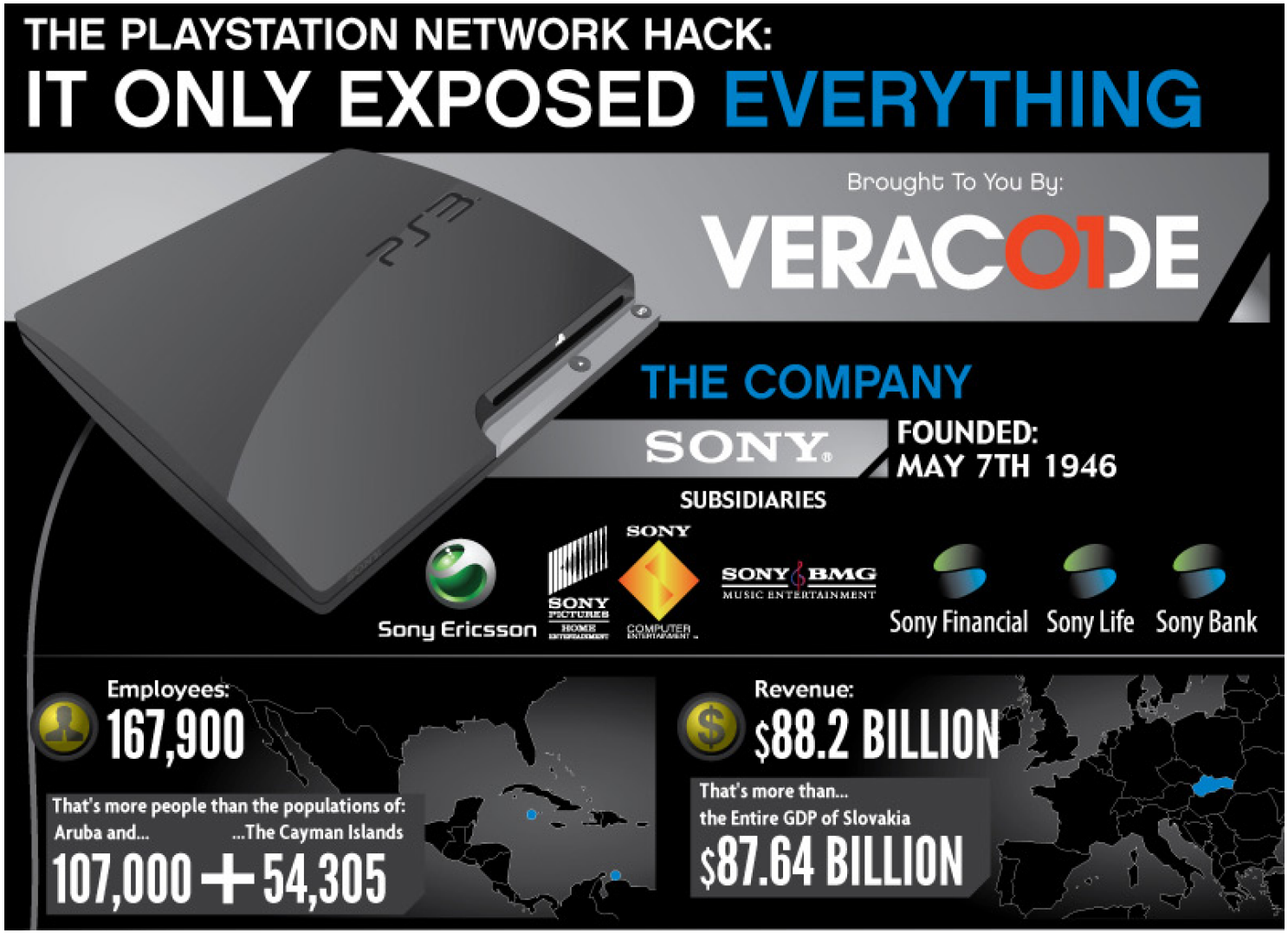
different countries are represented

Victims in this report span restaurants, retailers, media companies, banks, utilities, engineering firms, multi-national corporations, security providers, defense contractors, government agencies, and more across the globe. A definite relationship exists between industry and attack motive, which is most likely a byproduct of the data targeted (e.g., stealing payment cards from retailers and intellectual property [IP] from manufacturers).

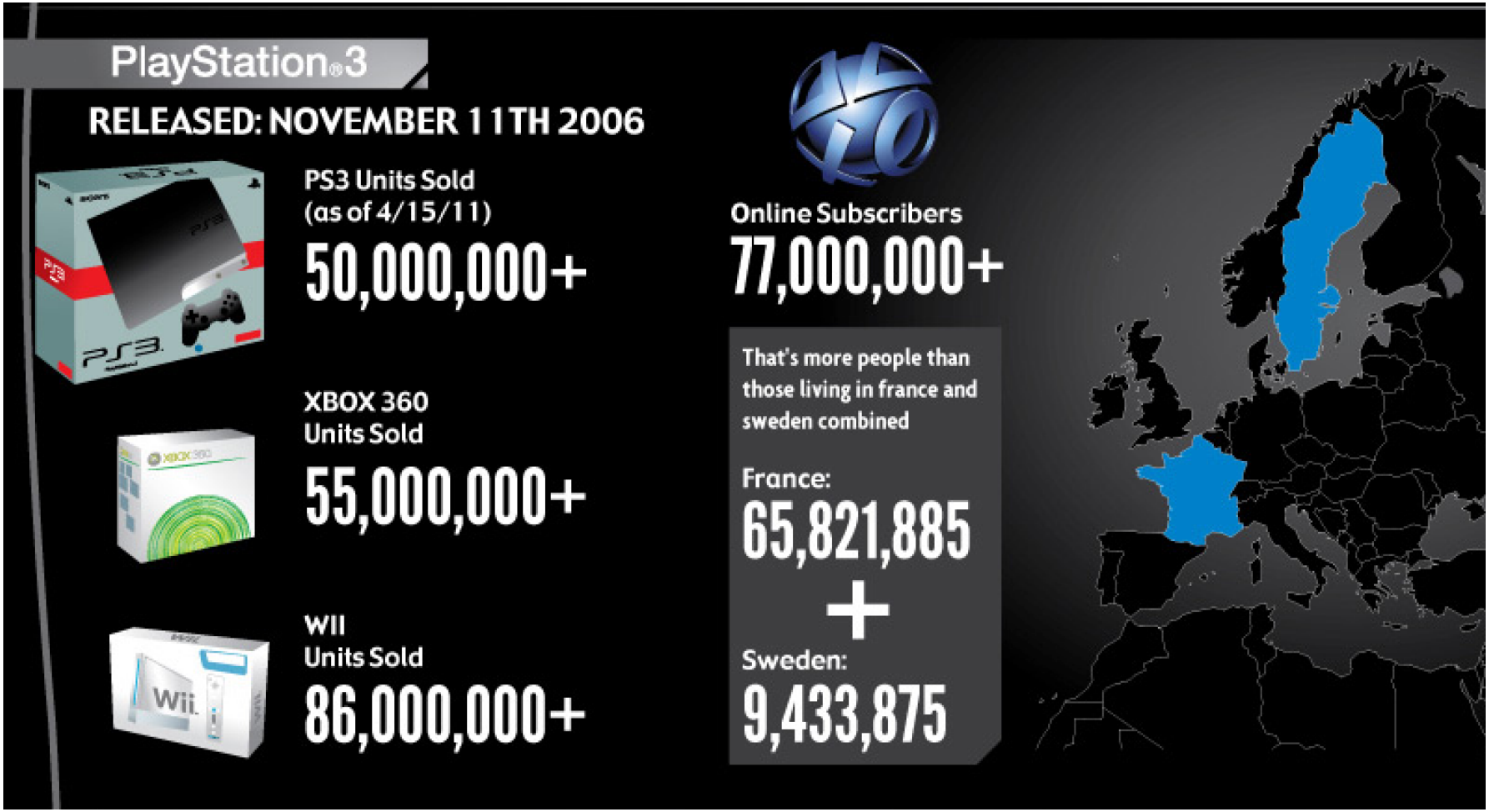
The ratio among organizational sizes is fairly even this time around, rather than tipping toward the small end of the scale as it did in our last report.

Case Study

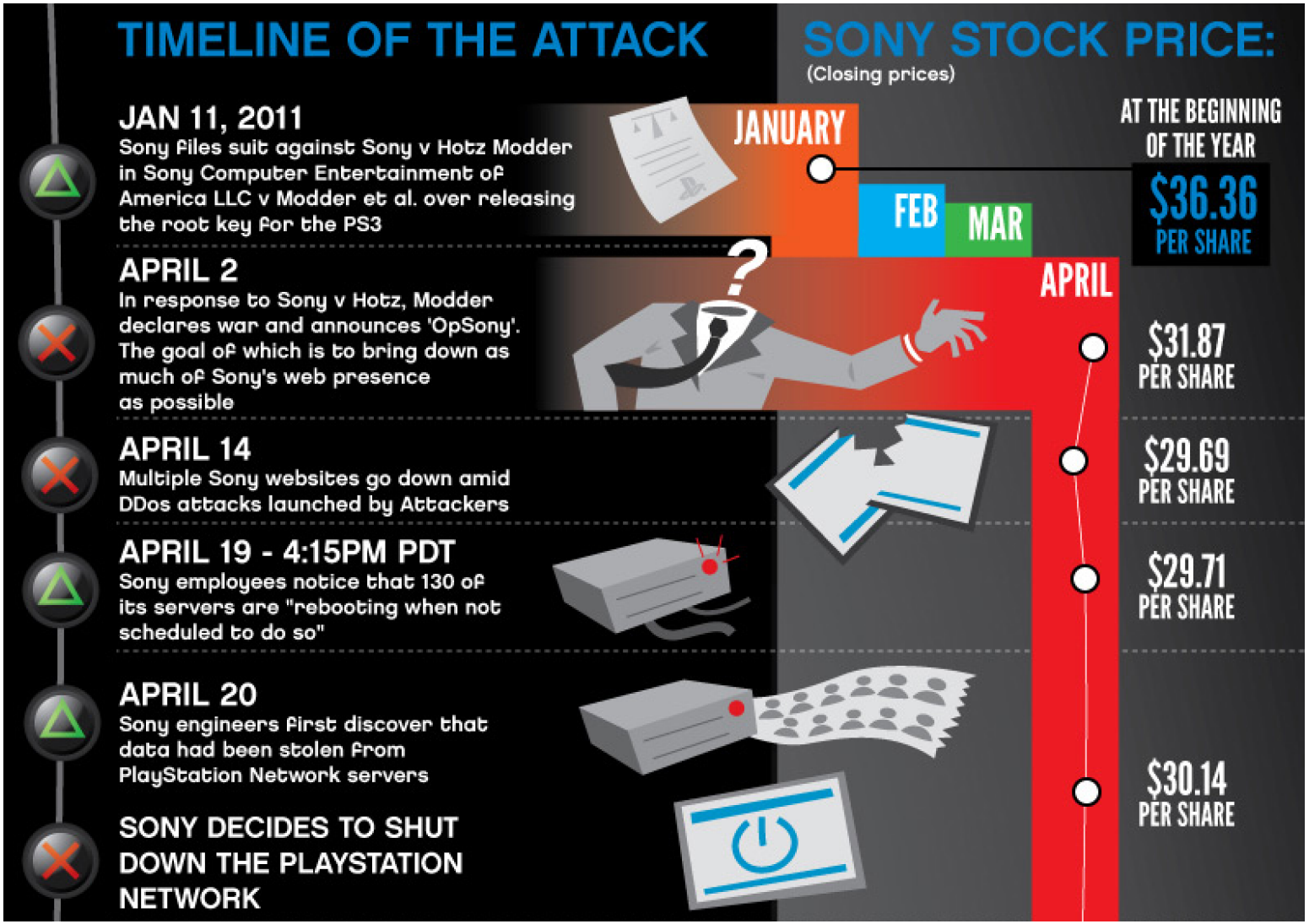
The (In)Security Problem - SONY HACK



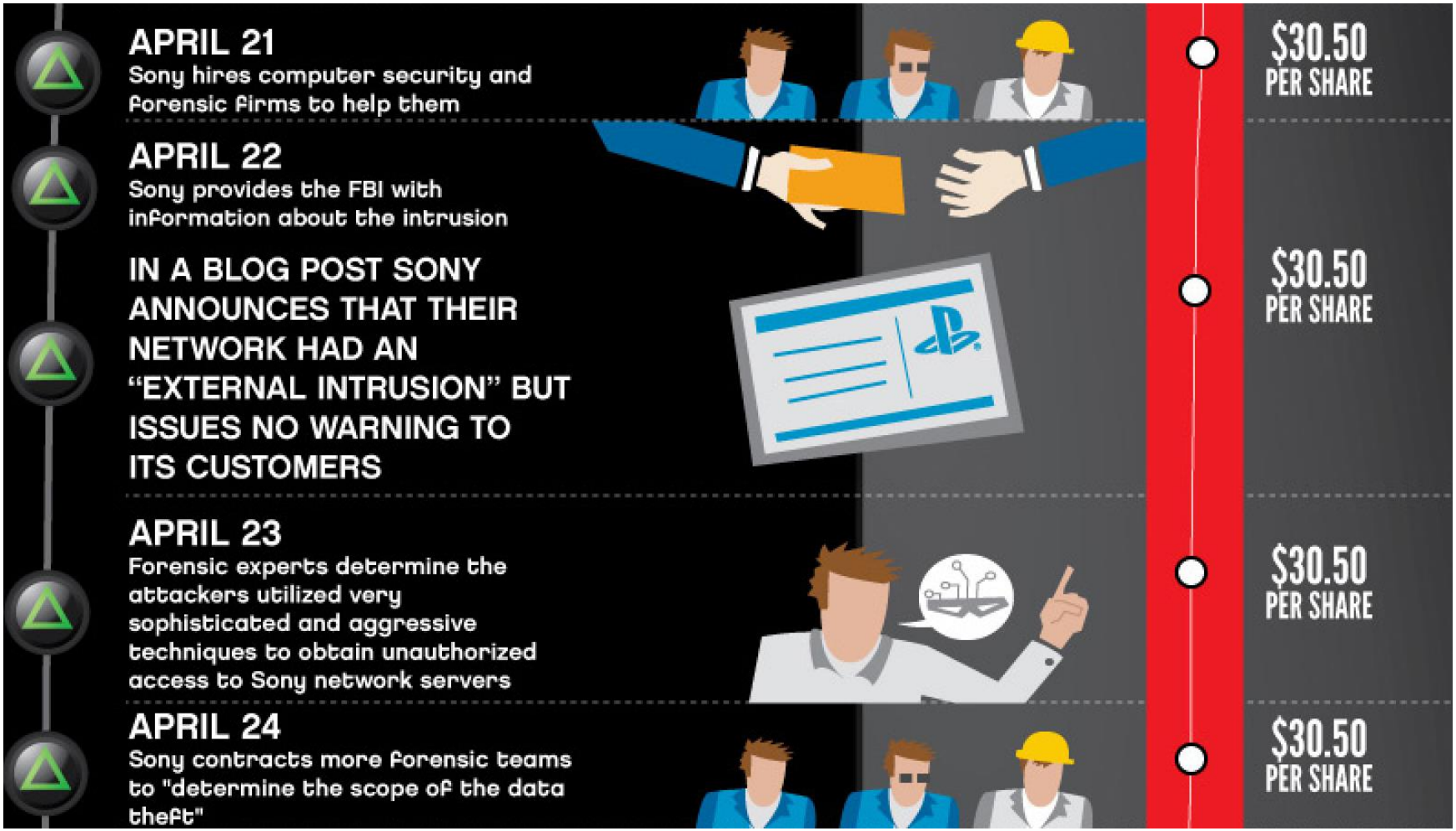
The (In)Security Problem - SONY HACK



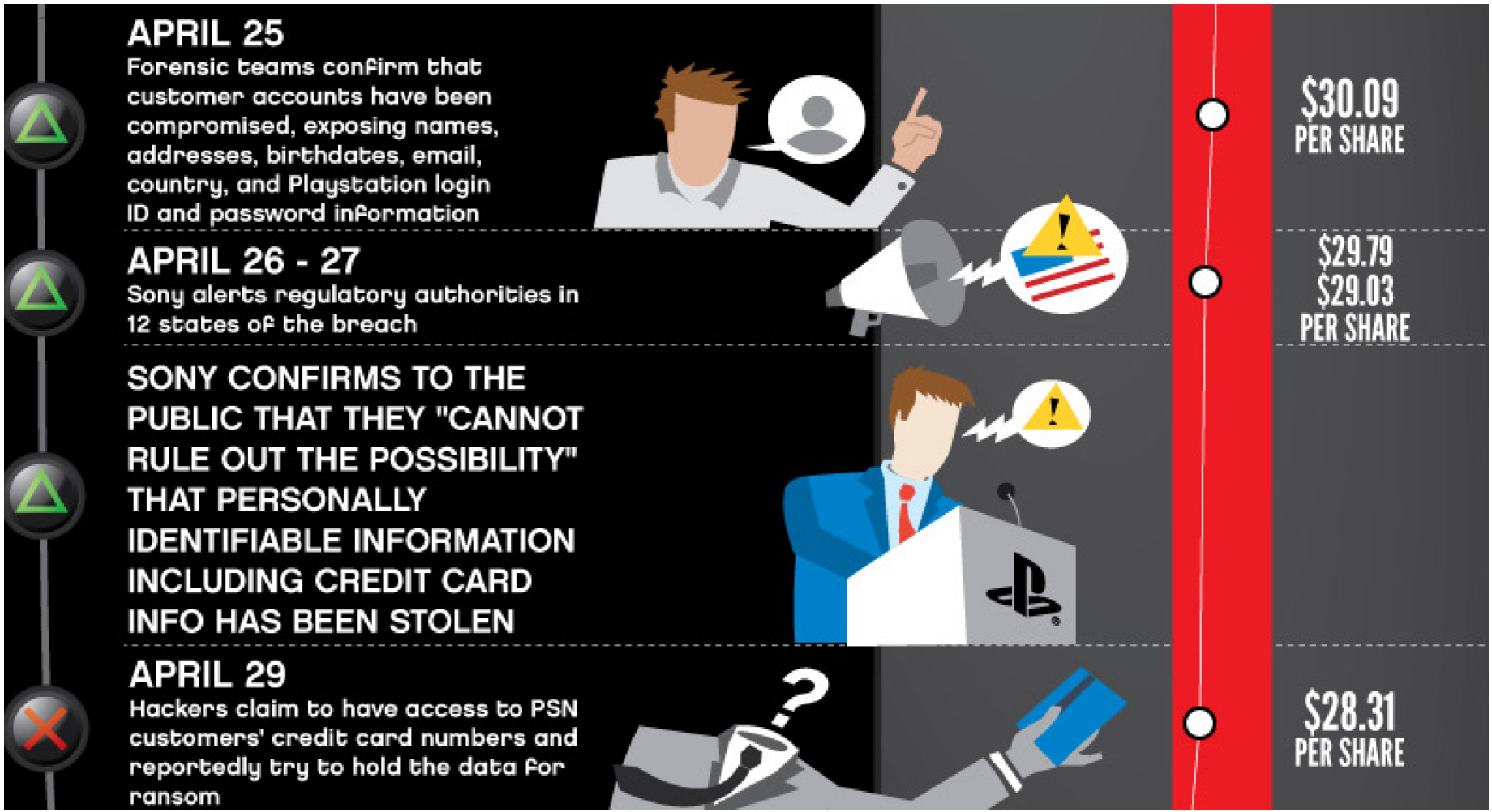
The (In)Security Problem - SONY HACK



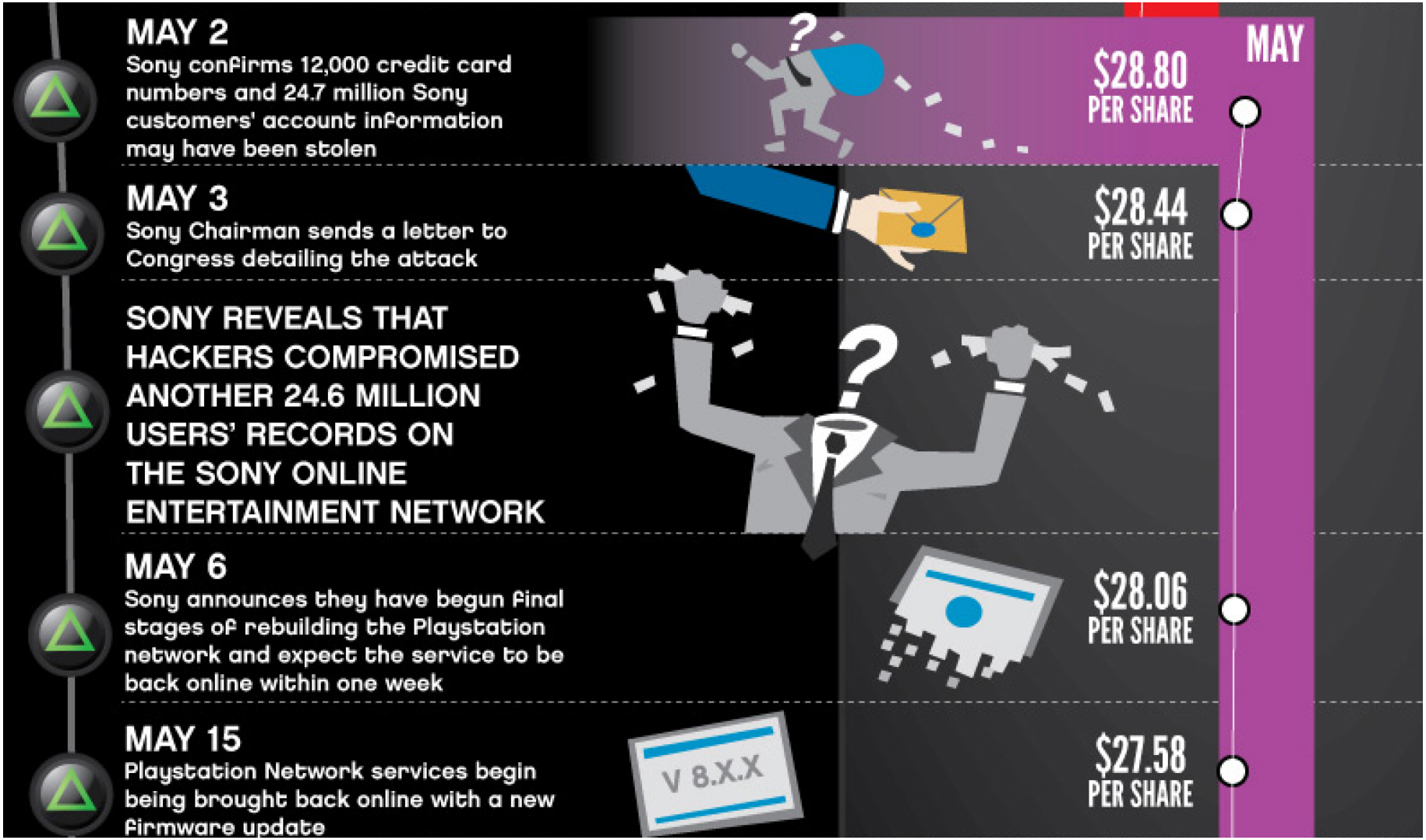
The (In)Security Problem - SONY HACK



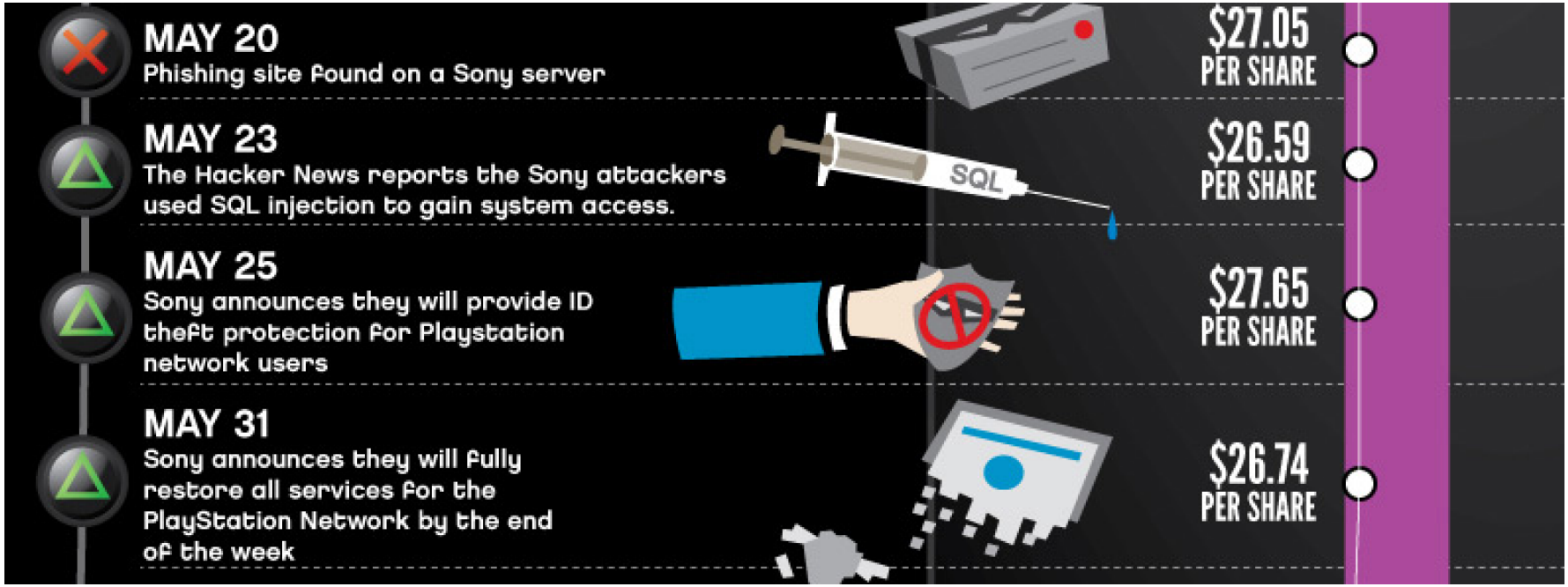
The (In)Security Problem - SONY HACK



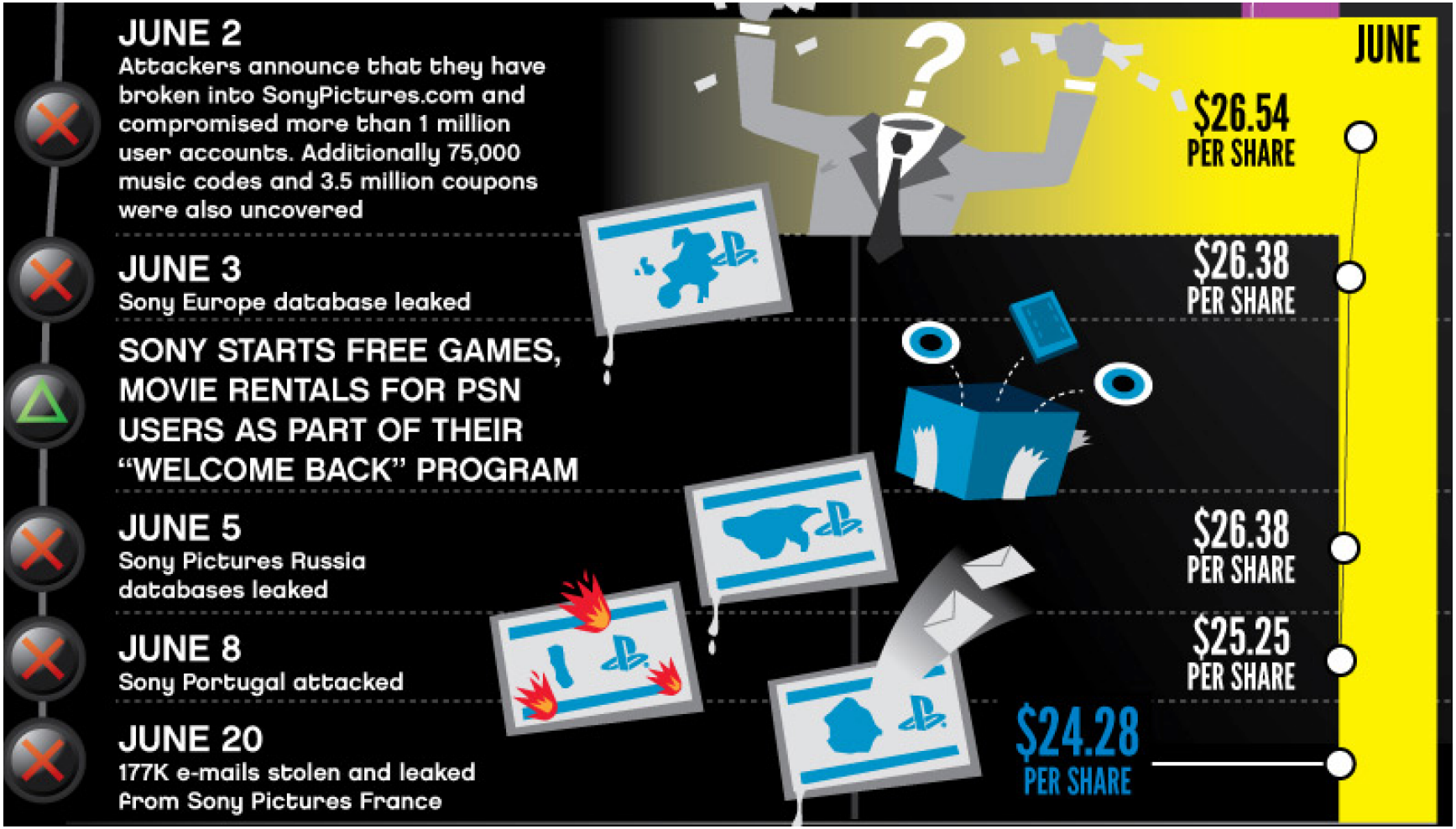
The (In)Security Problem - SONY HACK



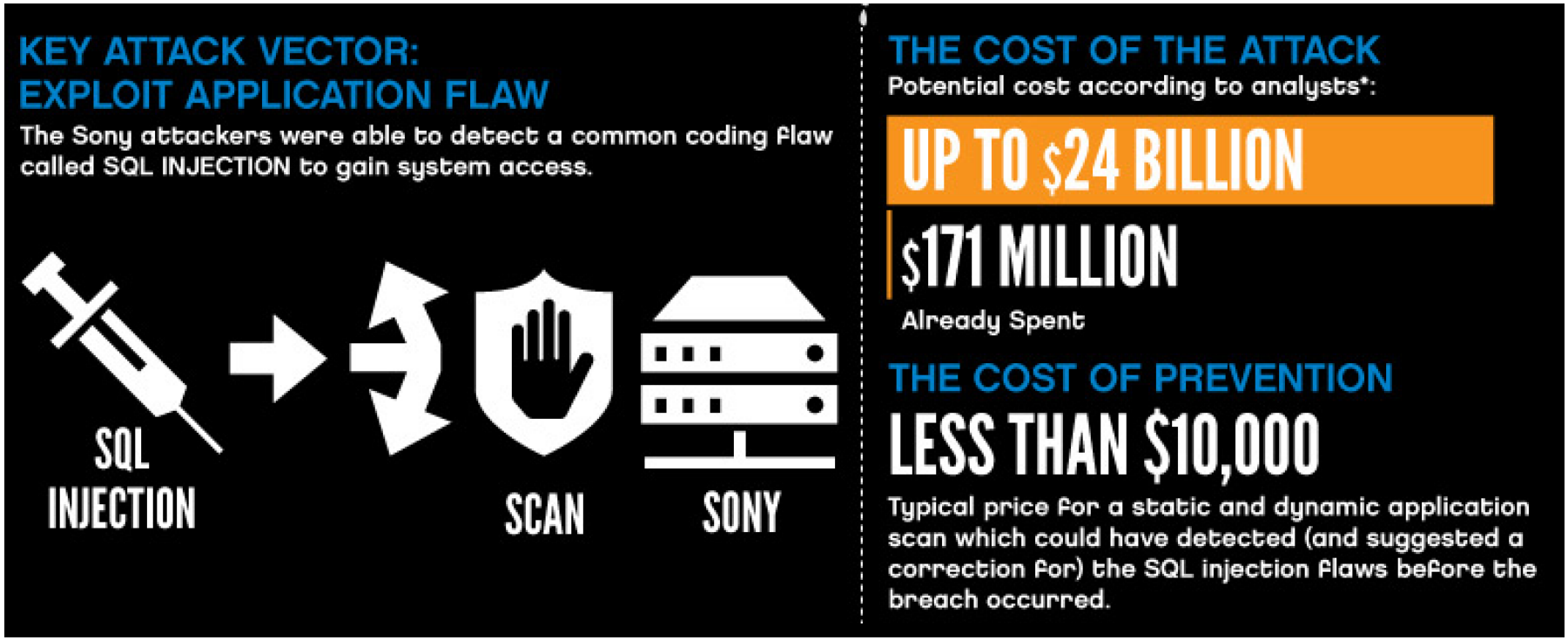
The (In)Security Problem - SONY HACK



The (In)Security Problem - SONY HACK



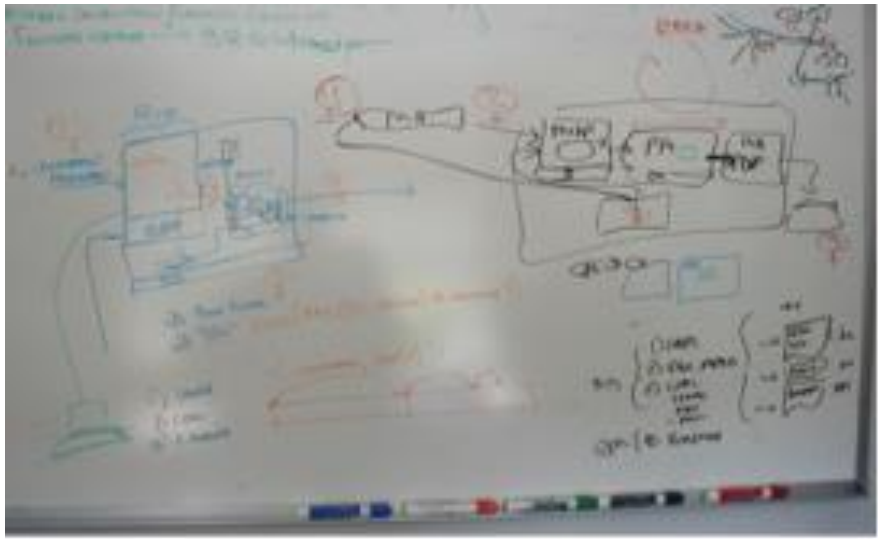
The (In)Security Problem - SONY HACK

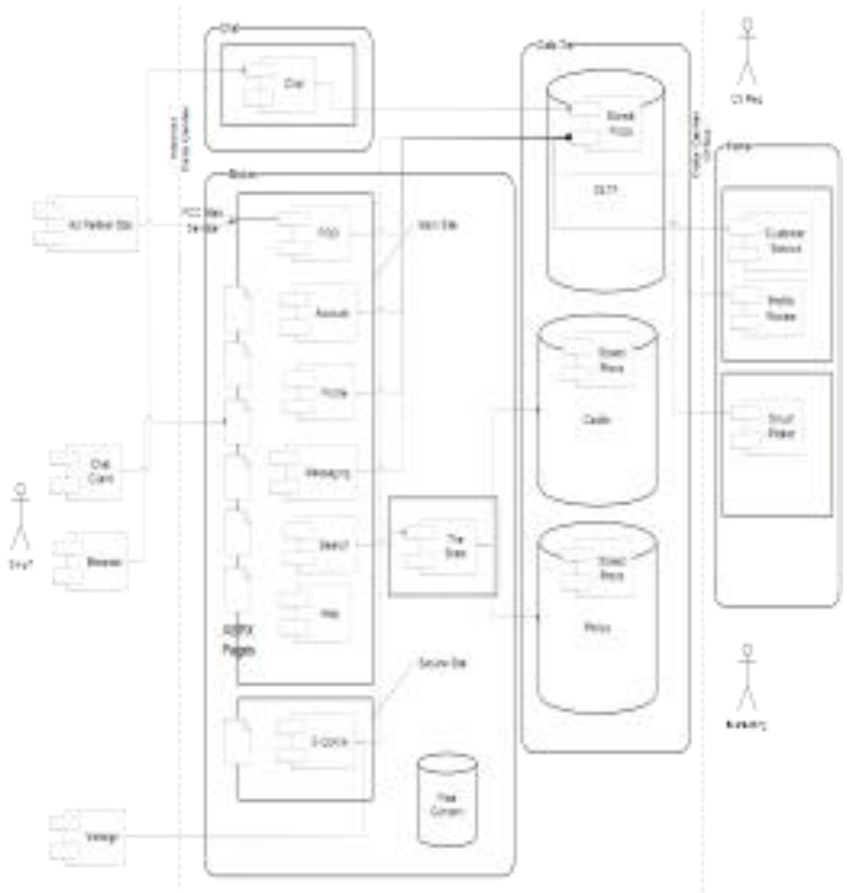


The (In)Security Problem - SONY HACK

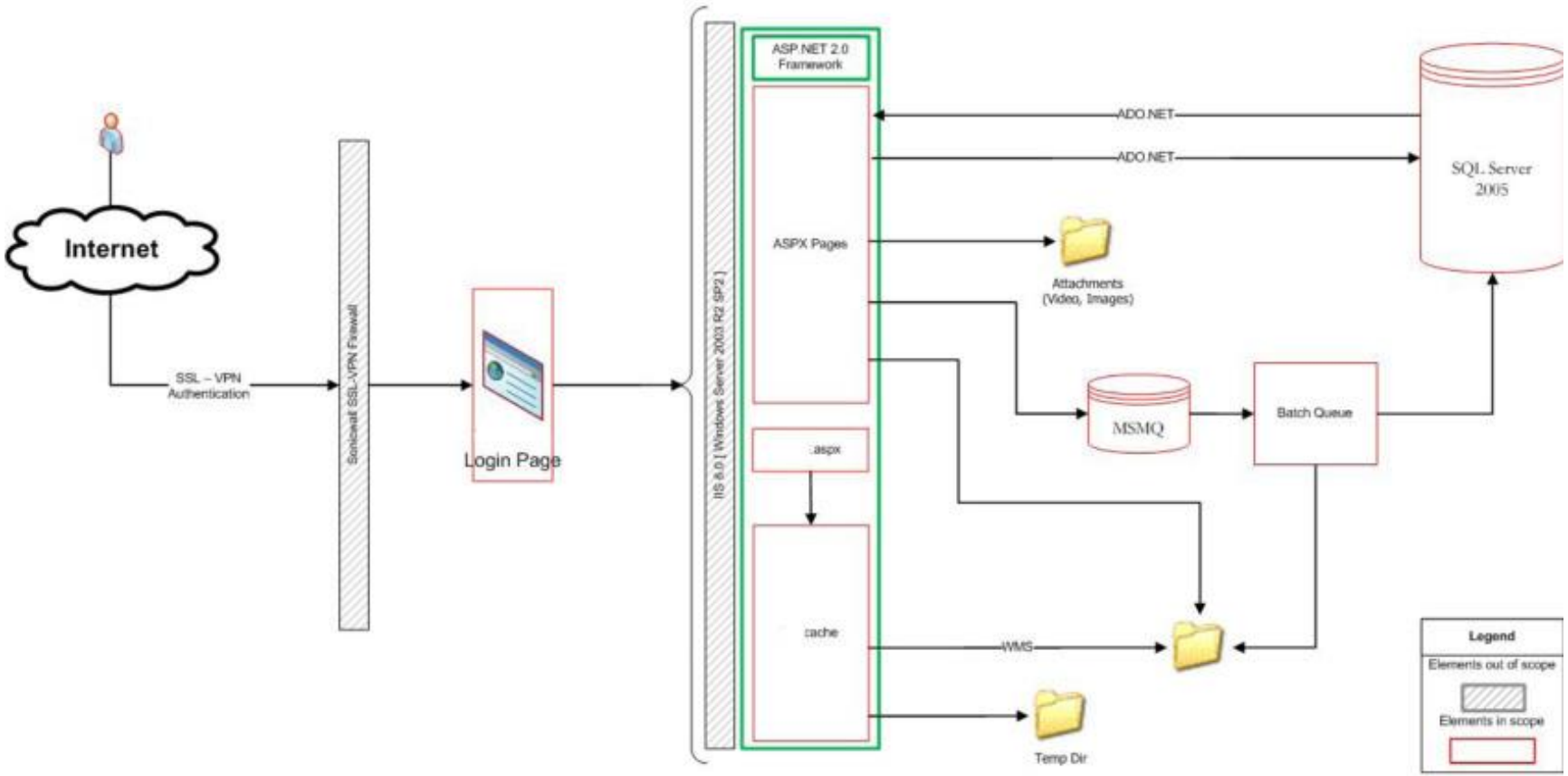
http://www.youtube.com/watch?v=_SDCV00ErEs#t=37

Architecture Diagram - 1st Draft

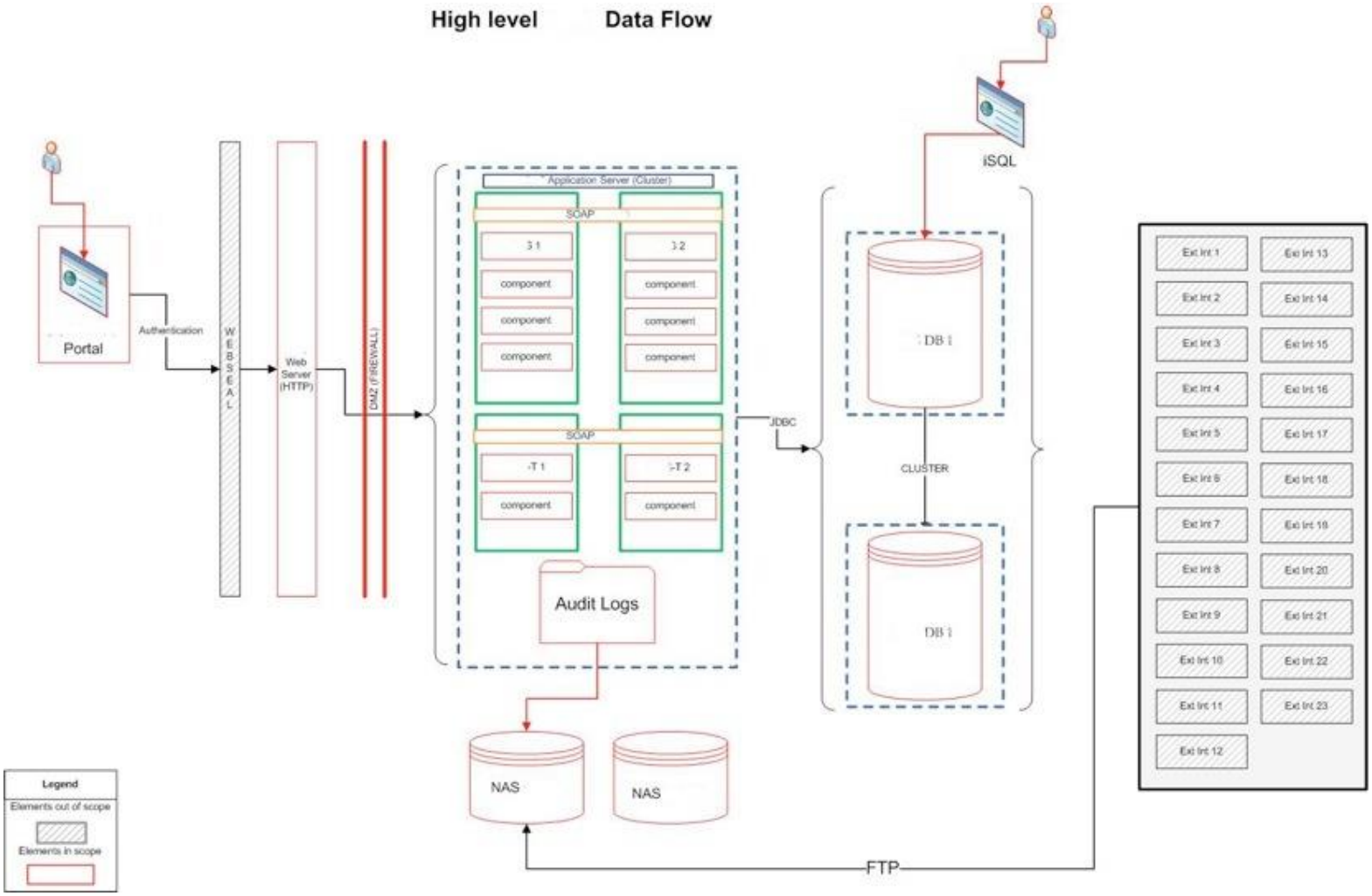




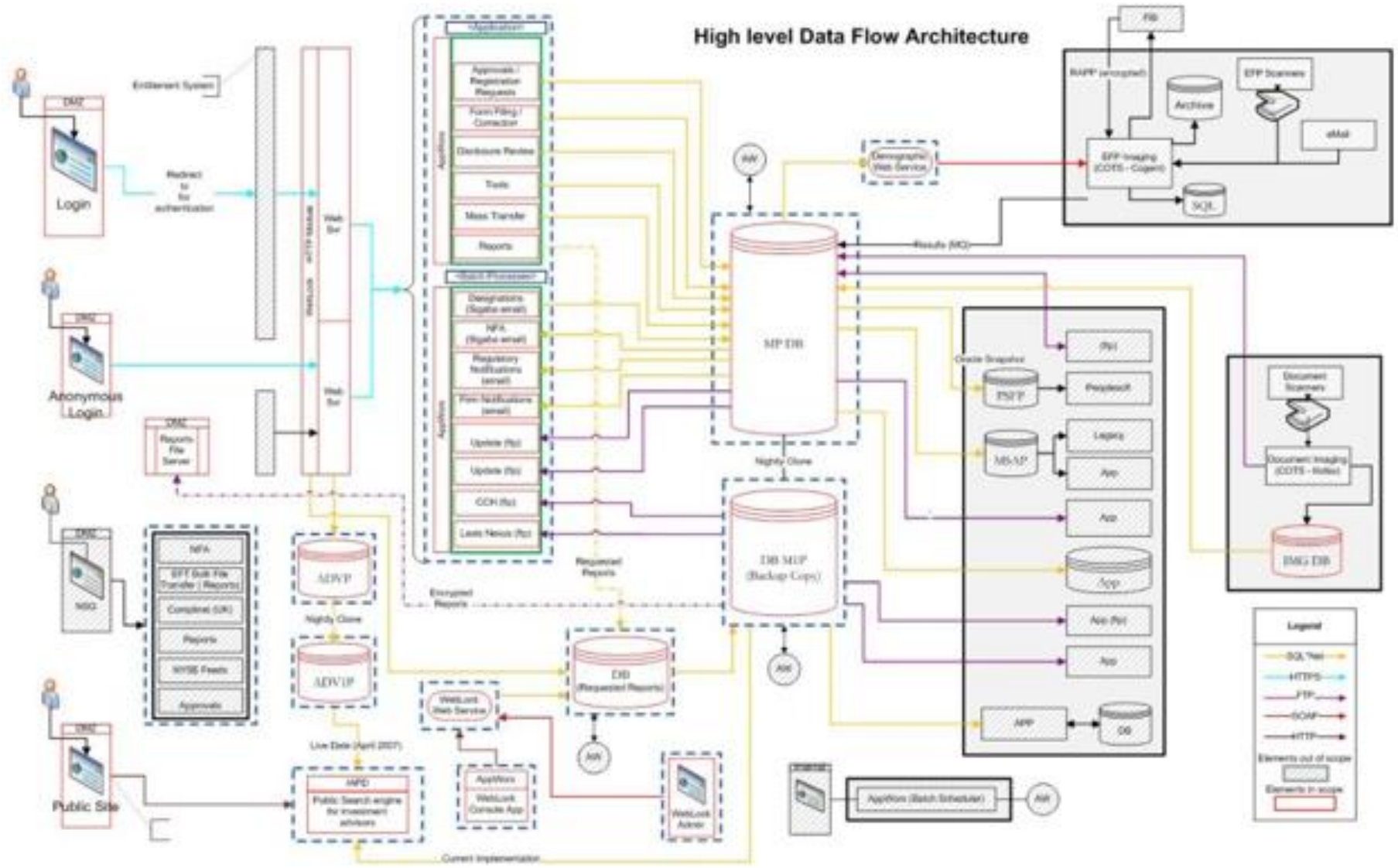
Architecture Diagram - 2nd Draft



Architecture Diagram - 3rd Draft



Architecture Diagram - Final Draft



SecureNinjaTV

SecureNinja

The CyberSecurity Experts

SecureNinja

The CyberSecurity Experts

Check us out at

SecureNinja.com

Watch SecureNinjaTV on

www.youtube.com/Secureninja