Risk Assessment

Source: freely inspired from Gemalto Information Security Risk Assessment

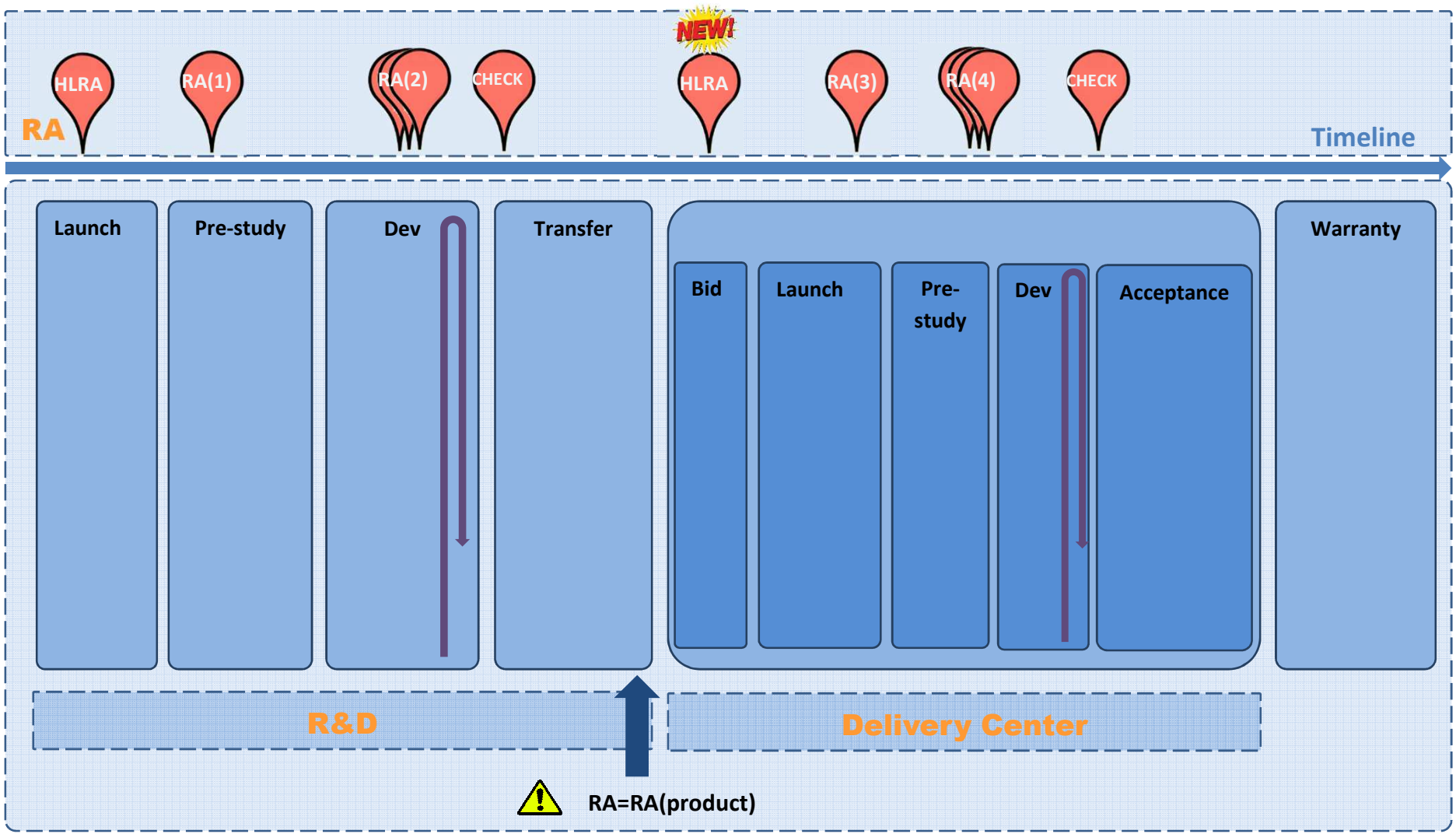
Security Objective

Guarantee the fundamental **security properties** of the **systems** and **services** we deliver to customers and of the **data** they handle

Security Properties

- **Confidentiality**
  - Ensure that an information is protected against unauthorized disclosure
- **Integrity**
  - Ensure that a system, a service or a data is protected against unauthorized or improper modifications
- **Availability**
  - Ensure that a system, a service or a data is accessible and usable by authorized users whenever needed
- Authenticity
  - Ensure that a system, a service or a data is authentic and issued by the genuine entity
- Authorization
  - Ensure that a system, a service or a data can only be accessed by authorized entities
- Non-repudiation
  - Ensure that an authorized entity cannot deny having performed an action on a system

Security Activities



(1): If HLRA highlights a risk. Hypothesis have to be made about the deployment

(2): Iterations are required if we have a new BA (i.e. data or service), SA, vulnerability,

(3): Usually a RA aggregation is required. Need to check the deployment hypothesis made by R&D

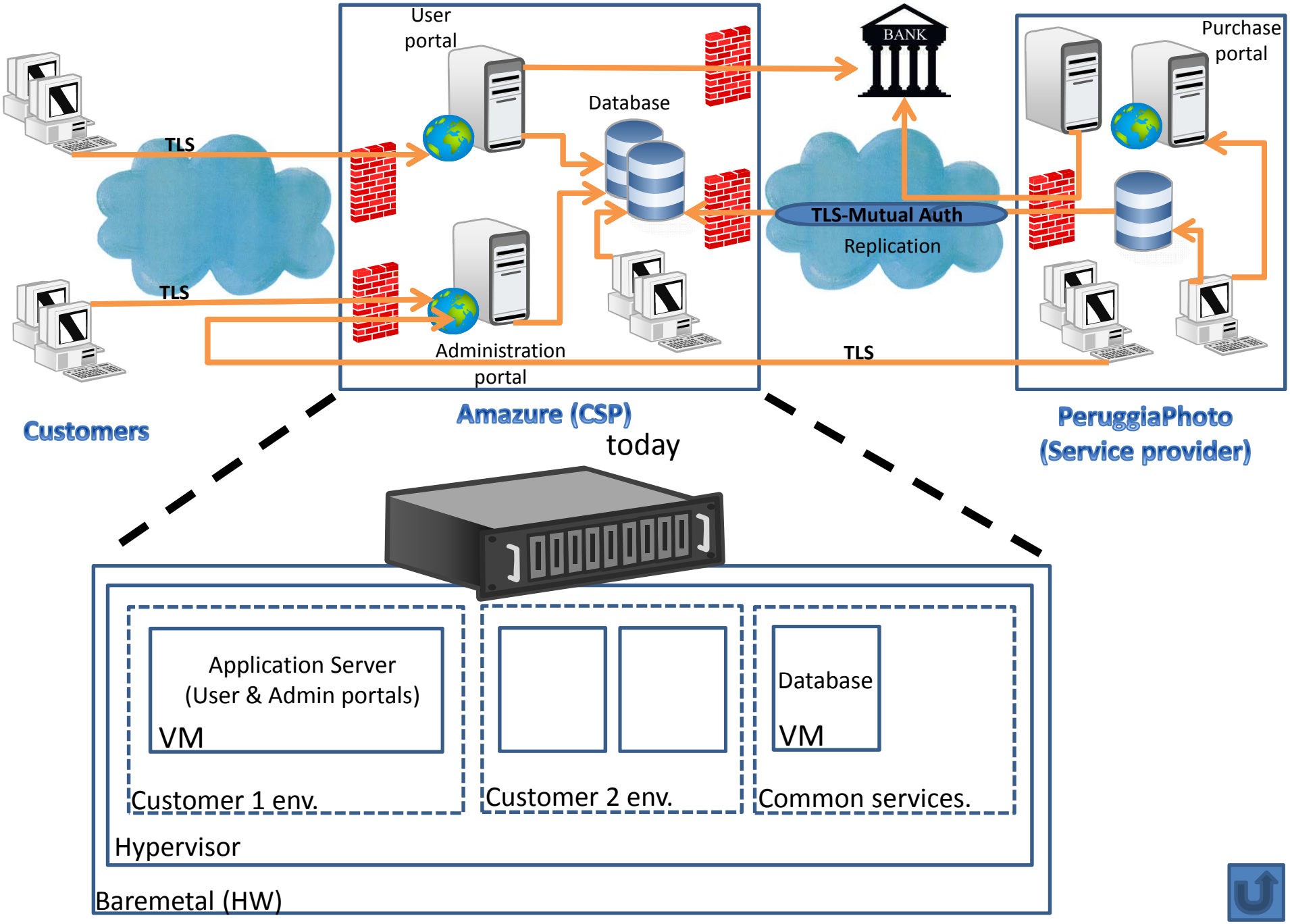
(4): Depends on deployment decisions. Iterations are required if we have a new feature, SA, vulnerability

Let’s do a first RA!

Solution description

- As a solution provider we want to promote a web service in order to:
  - Order digital photo prints online at **PerruggiaPhoto**
  - Upload your photos & order digital prints or other gifts
  - Free online photo storage

- We plan to deploy our service in the « cloud » with **Amazure**


User
portal
Database
BANK
Purchase
portal
TLS
TLS
TLS-Mutual Auth
Replication
Administration
portal
TLS
Customers
Amazure (CSP)
PeruggiaPhoto
(Service provider)
today
Application Server
(User & Admin portals)
VM
Database
VM
Customer 1 env.
Customer 2 env.
Common services.
Hypervisor
Baremetal (HW)

Solution actors

- The Solution **Sponsor**

  The one who pays for the solution, the requester

- Solution **Builders (development team and CSP team)**

  The ones in charge to develop, integrate and host the solution

- Solution **Users (you and me)**

  The ones that use the solution and its services

- **Administrator(s)** and **operator(s)** of the solution

  For example the one in charge to maintain the solution either as a CSP administration team or as a development maintenance team

Question

- **What has value** in the proposed solution?

- What are the **added values** of this solution ?

Could be…

- For the User
  - Photos
  - Account personal data (age, sex, address)
  - Password
  - Preferences on products (behavior, location)
  - Photo **service**
- For the Service provider
  - Product data (list, providers, prices)
  - Administration **service**
  - Transaction list

called **business assets**

- Could have also been:
  - CSP database
  - CSP Firewall
  - User Web Portal
  - Administration Web Portal
  - Hypervisor

called **supporting assets**

Sensitive data?

- Depends on
  - Data Type
  - Data Quantity
  - Data Combination
  - For what need

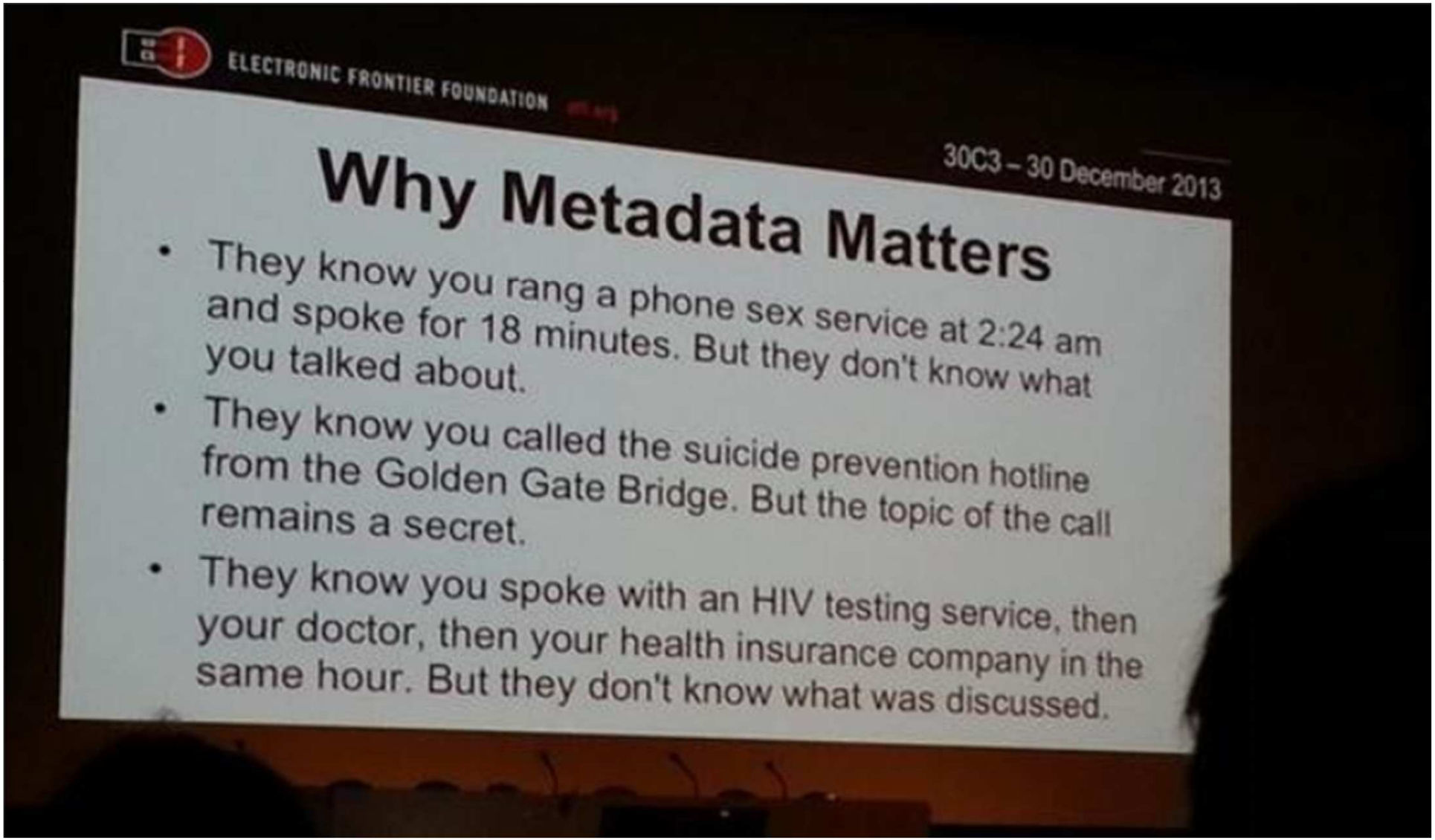
- Localization data alone (or other metadata)=> No
  - But what if we have a huge number of localization data? What's about privacy?

- Email alone => No
  - But what if we have a huge number of emails ? What's about e-reputation?

- Payment transactions list => No
  - But what if i want to buy stocks and I see the number of transactions is slightly increasing

- Your name => No this is public
  - But what if combined with address and social security number?

Metadata


ELECTRONIC FRONTIER FOUNDATION
30C3 – 30 December 2013
Why Metadata Matters
• They know you rang a phone sex service at 2:24 am and spoke for 18 minutes. But they don't know what you talked about.
• They know you called the suicide prevention hotline from the Golden Gate Bridge. But the topic of the call remains a secret.
• They know you spoke with an HIV testing service, then your doctor, then your health insurance company in the same hour. But they don't know what was discussed.

Restricted data

1.	**Authentication Verifier**
	An Authentication Verifier is a piece of information that is held in confidence by an individual and used to prove that the person is who they say they are. In some instances, an Authentication Verifier may be shared amongst a small group of individuals. An Authentication Verifier may also be used to prove the identity of a system or service. Examples include, but are not limited to: •Passwords •Shared secrets •Cryptographic private keys

Restricted data

6.	**Payment Card Information**
	Payment card information is defined as a credit card number (also referred to as a primary account number or PAN) in combination with one or more of the following data elements: •Cardholder name •Service code •Expiration date •CVC2, CVV2 or CID value •PIN or PIN block •Contents of a credit card's magnetic stripe

Restricted data

7.	**Personally Identifiable Education Records**
	Personally Identifiable Education Records are defined as any Education Records that contain one or more of the following personal identifiers: •Name of the student •Name of the student's parent(s) or other family member(s) •Social security number •Student number •A list of personal characteristics that would make the student's identity easily traceable •Any other information or identifier that would make the student's identity easily traceable

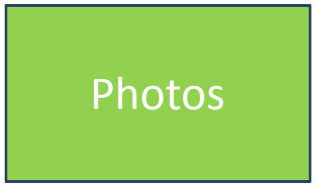
Restricted data

8.	**Personally Identifiable Information ("PII")**
	For the purpose of meeting security breach notification requirements, PII is defined as a person's first name or first initial and last name in combination with one or more of the following data elements: •Social security number •State-issued driver's license number •State-issued identification card number •Financial account number in combination with a security code, access code or password that would permit access to the account •Medical and/or health insurance information

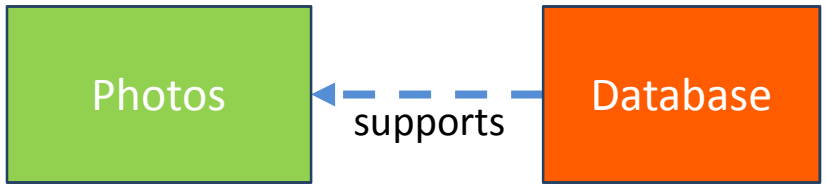
Restricted data

9.	**Protected Health Information ("PHI")**
	PHI is defined as "individually identifiable health information" transmitted by electronic media, maintained in electronic media or transmitted or maintained in any other form or medium by a Covered Component, as defined in Carnegie Mellon's HIPAA Policy. PHI is considered individually identifiable if it contains one or more of the following identifiers: •Name •Address (all geographic subdivisions smaller than state including street address, city, county, precinct or zip code) •All elements of dates (except year) related to an individual including birth date, admissions date, discharge date, date of death and exact age if over 89) •Telephone numbers •Fax numbers •Electronic mail addresses •Social security numbers •Medical record numbers •Health plan beneficiary numbers •Account numbers •Certificate/license numbers •Vehicle identifiers and serial numbers, including license plate number •Device identifiers and serial numbers •Universal Resource Locators (URLs) •Internet protocol (IP) addresses •Biometric identifiers, including finger and voice prints •Full face photographic images and any comparable images •Any other unique identifying number, characteristic or code that could indentify an individual

Data model



Data model



Question

- Let focus on Photos and forget our solution for this question
  - What **security properties** have to **be protected** when dealing with photos?
  - In other words, what could be the **target** of an attack against photos?

Consider the point of view of the service provider and of users

Photos could be…

- Stolen or temporarily not accessible on the web site

⇒ **Availability** property broken

- Tampered and no more usable

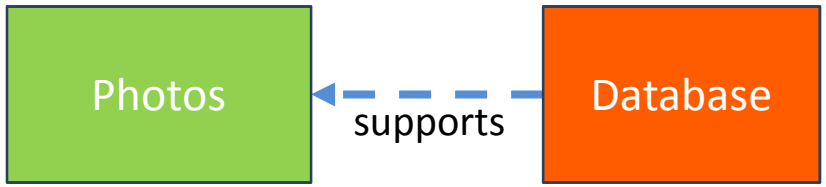
⇒**Integrity** property broken

- More or less attractive according to amounts

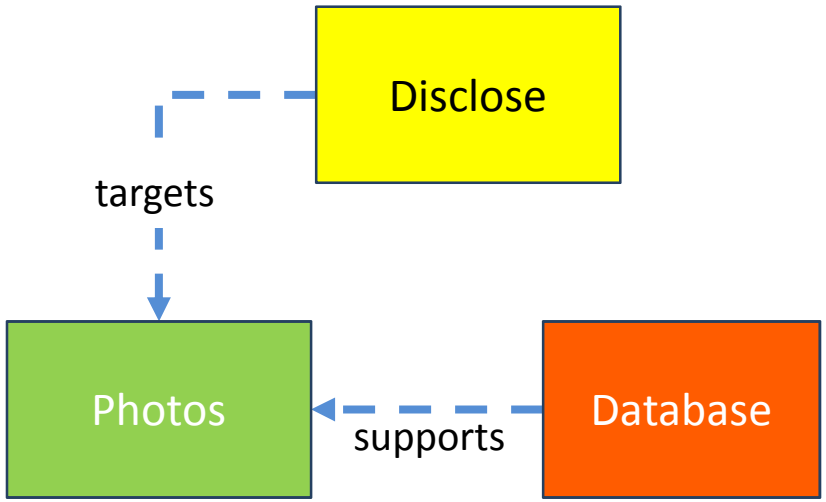
⇒**Confidentiality** / **privacy** of amounts to be considered

- Etc…

Data model



Data model



Question

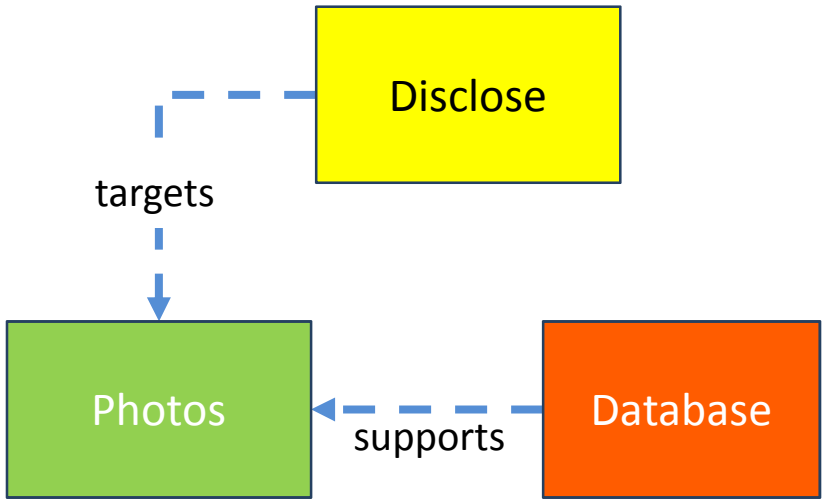
- Back to the solution…
- **Who** can threat or attack someone's photos?

Could be…

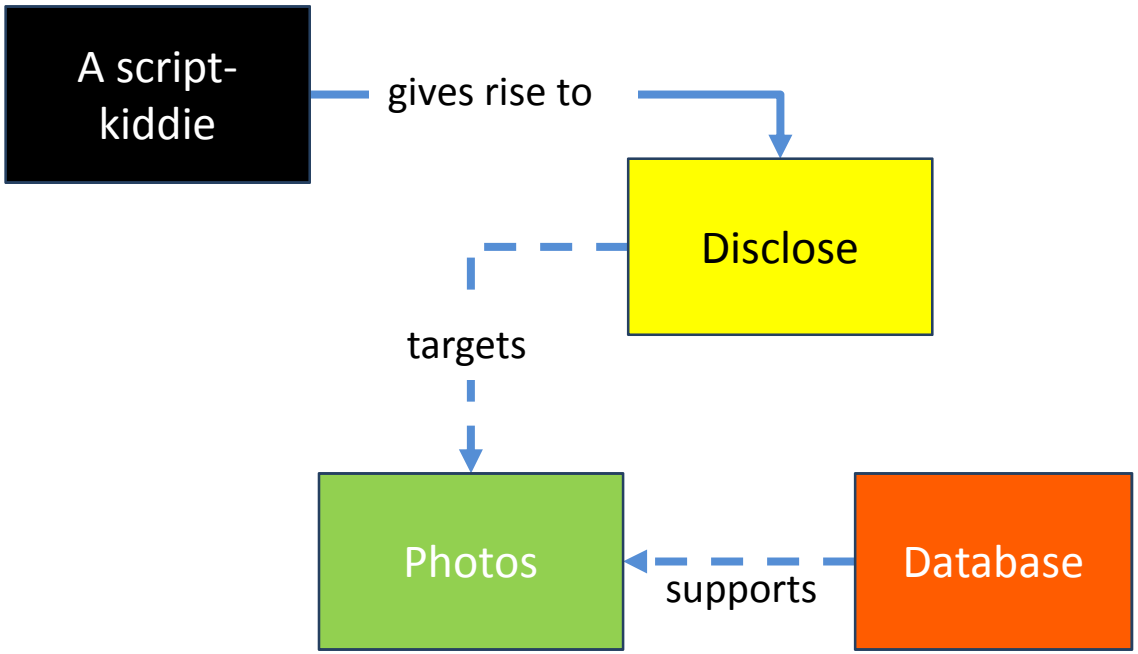
- Someone you know
- Someone on internet
- A Governement agency
- Someone in charge of maintenance or administration

$\Rightarrow$ Being the threaten entities, they are called **threat agents** (or **attacker**)

Data model



Data model


A script-kiddie
gives rise to
Disclose
targets
Photos
supports
Database

Question

- **How** would a threat agent attack ?

Could be by…

1. Exploiting a XXE on the user web portal
2. Then, exploiting a SQLI to access customer data
3. Then, deciphering data offline

$\Rightarrow$ We talk about **attack path** made of multiple **attack steps**

***Note**: several attack paths may exist for a given threat*

Question

- **How** or **why** can a threat agent would attack your asset?

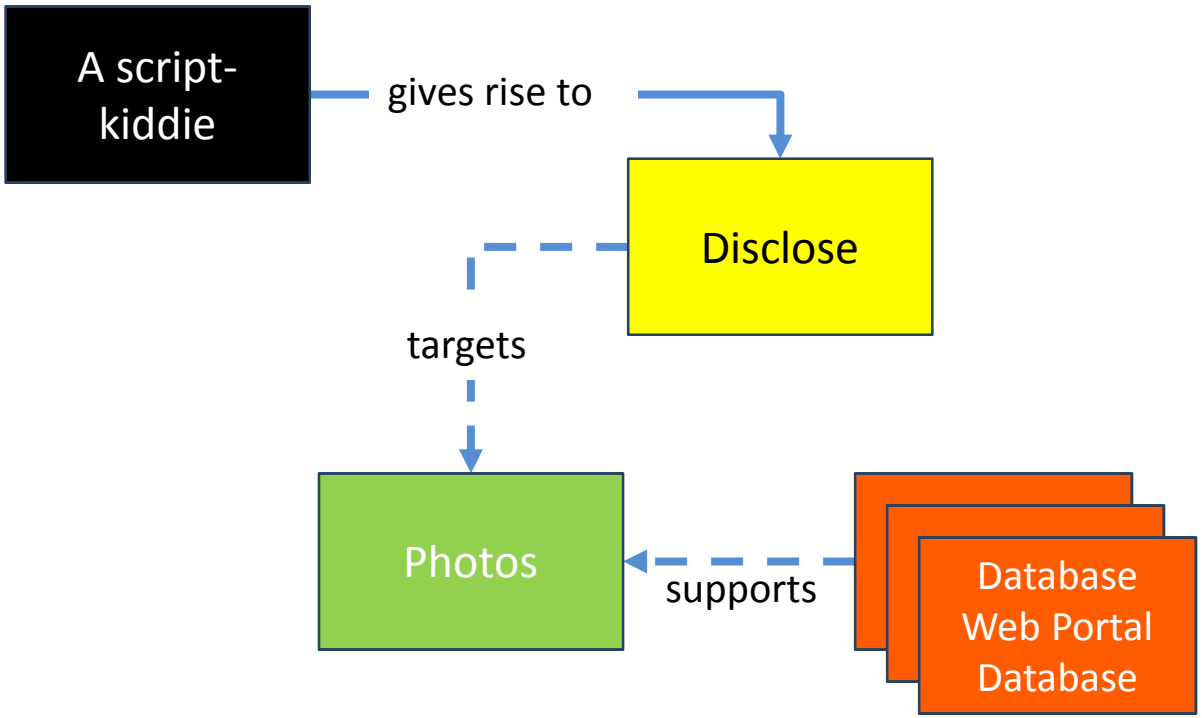
By exploiting vulnerabilities

- Following the considered attack path we do see some potential vulnerabilities :
  - No sensitive data encryption
  - SQL injection allows to access to customer data
  - XXE allows to exfiltrate customer data
  - Etc…

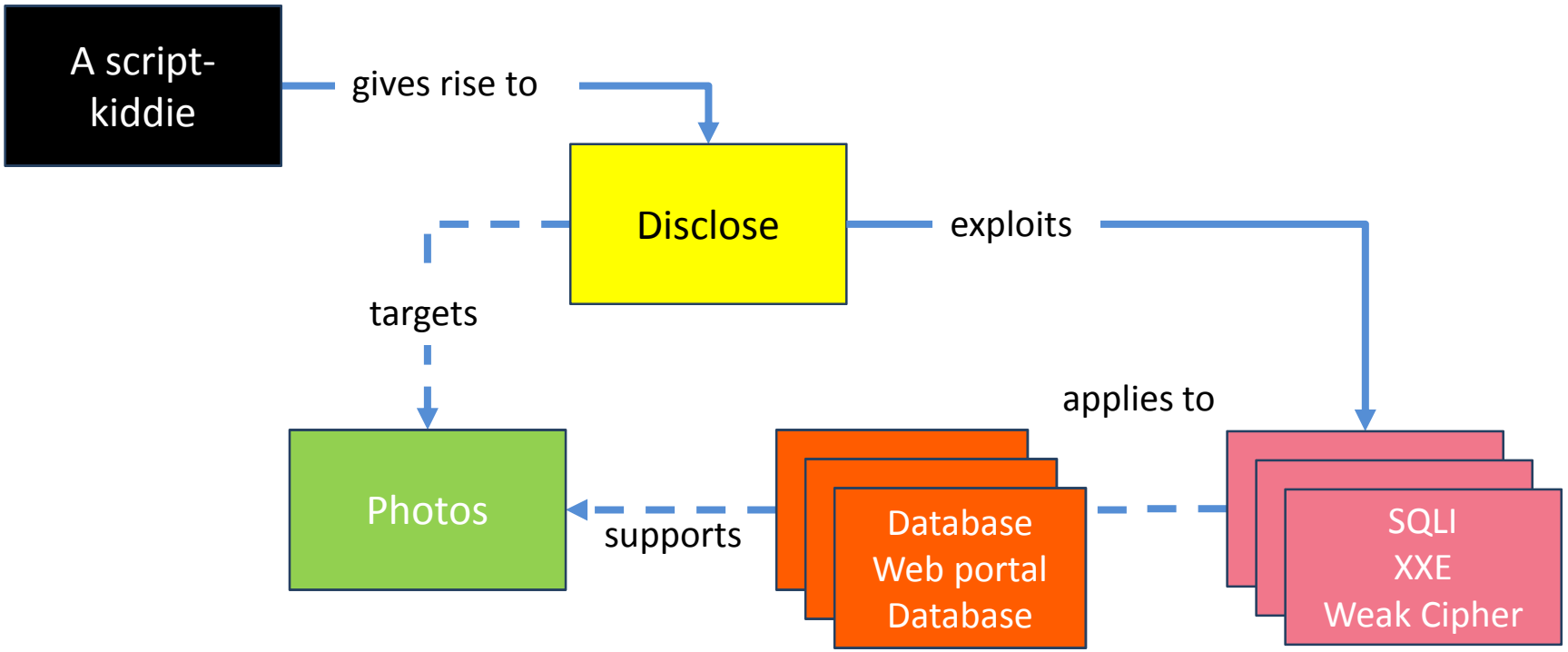
*Note: all those **vulnerabilities** are related to **supporting assets***

- These vulnerabilities can be of different types :
  - Architecture: multi-tenant infrastructure without segregation
  - Design: a logging third-party library known as vulnerable is chosen
  - Implementation: a weak cipher suite is used to encrypt data
  - Deployment: User Web portal is deployed on a non hardened OS
  - Operations: the administrator has access to customer data without control

Data model


A script-kiddie
gives rise to
Disclose
targets
Photos
supports
Database
Web Portal
Database

Data model


A script-kiddie
gives rise to
Disclose
exploits
targets
applies to
Photos
supports
Database
Web portal
Database
SQLI
XXE
Weak Cipher

Question

- **What** does a threat agent **need** to be able to attack successfully?

The threat agent could need…

- To know how to find and exploit an SQLI on the web portal
- To know how to find and exploit an XXE
- To know how to decrypt the data

⇒ The threat agent would need several **skills** and **means**; we talk about threat agent **potential/resources**

***Note**: required skills and means are not restricted to the proposed solution but can refer to any other protections*

- To know that sensitive photos have just been uploaded into the web site storage area

⇒ Such contextual information help to create the **opportunity**

Question

- **What** could **motivate** a threat agent to act ?

***TIPS**: Consider a script-kidded that would want to steal your photos*

Motivation can be…

- To increase the attacker e-reputation

In that case motivation is **ego** boost

- Just to get some money or, to become rich

In both those cases motivation is **greed**

- Impoverishing or mocking the victim

In that case the main motivation can be **revenge**

- Just to get some money to redistribute to poor

Here it is more **ideology** (e.g. Robin Hood ☺)

Question

- At the end **what** will **make** a threat agent **to attack or not** ?

Should be a trade-off

- Between the needed threat agent **ressources** and the **opportunity**
  - Resources / means
  - Skills / knowledge
  - Opportunity / context
- And, the **interest** of the threat agent to act
  - Motivation
  - « ROI »
  - **Value of** the targeted **asset for the threat agent**
- We are talking about **likelihood**

Question

- Still considering a script-kiddie that would want to steal your photos via the user web portal.

- **How** can you **protect** yourself against such threat ?

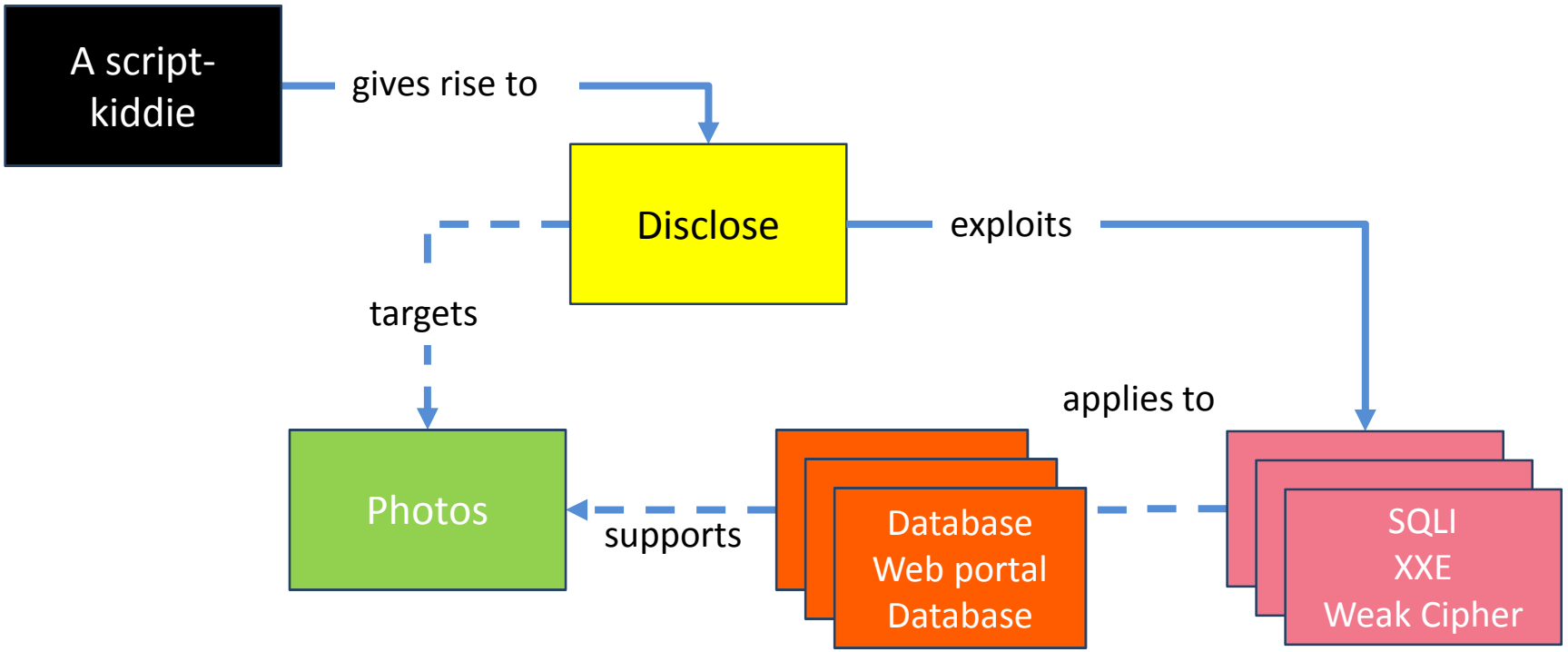
Could be by …

- Using a strong cipher suite
- Integrating a WAF to protect the web portal
- Fixing the vulnerabilities on the user portal
- Configuring the firewall to forbid the access to the outside from the user web portal
- Training the developers on security guidelines
- Planning regular penetration testing

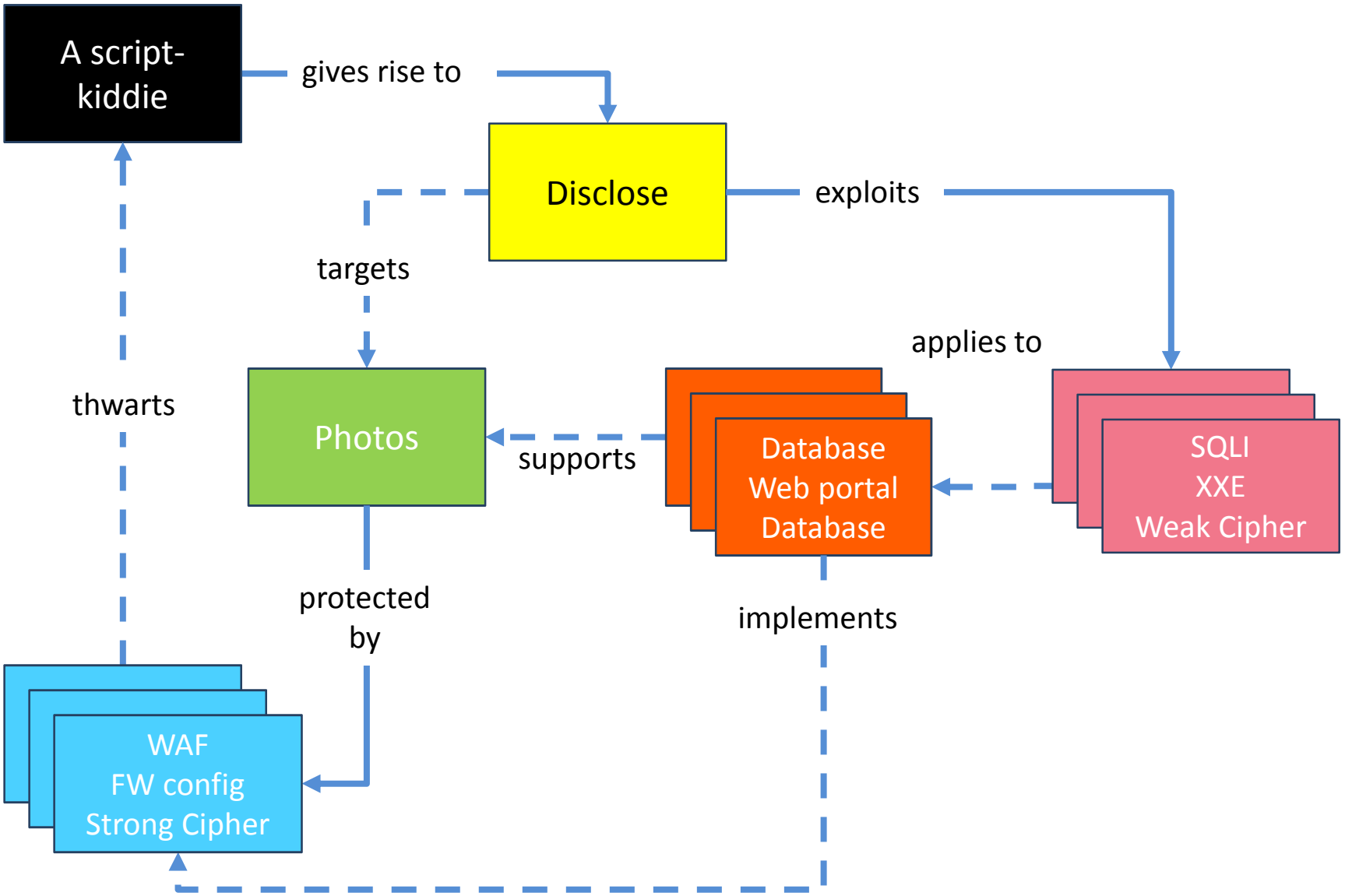
$\Rightarrow$ These protections are called **security functions** or **security controls**

*Note: these security functions or security controls are implemented on **supporting assets***

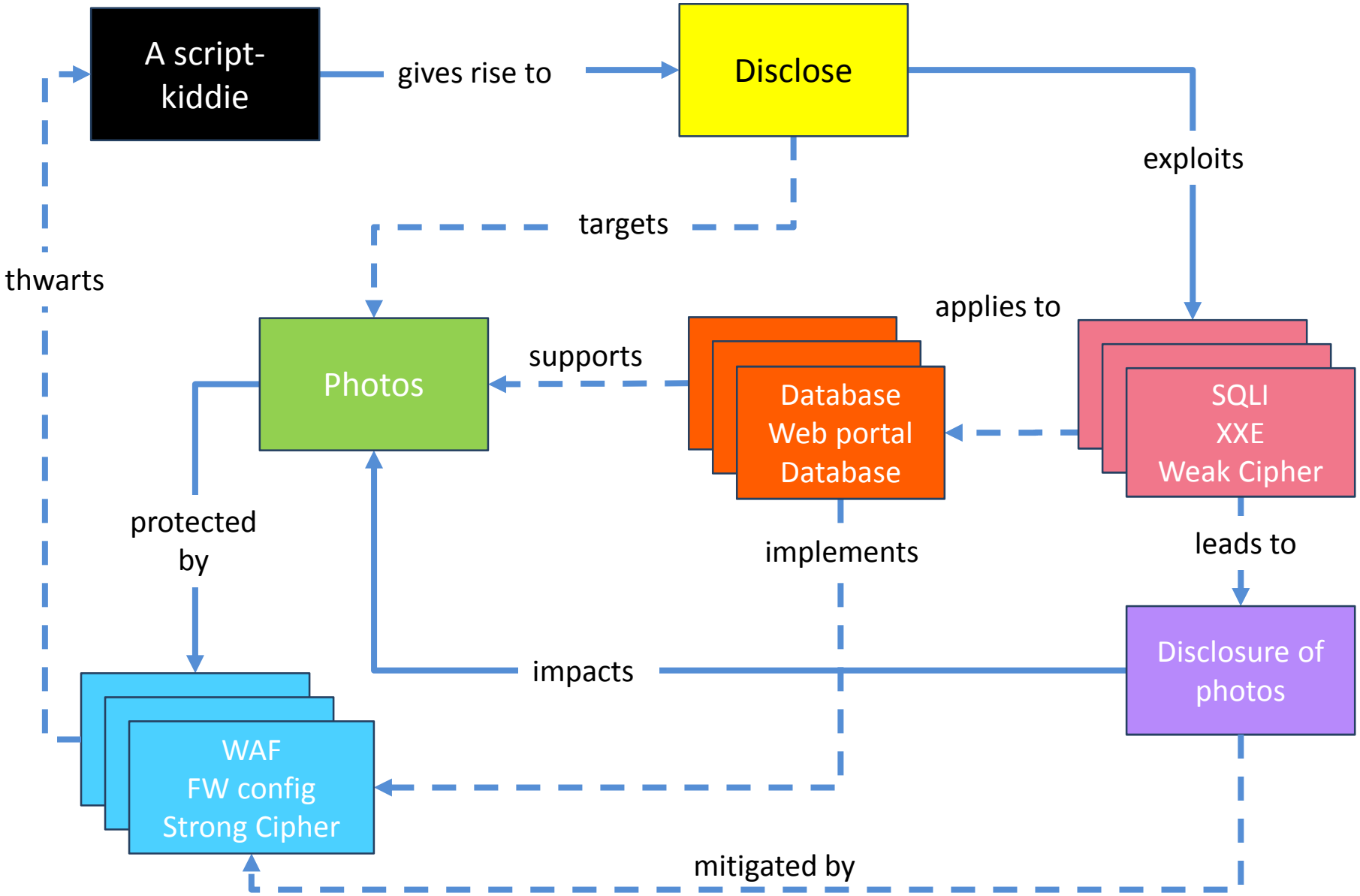
Data model


A script-kiddie
gives rise to
Disclose
exploits
targets
applies to
Photos
supports
Database
Web portal
Database
SQLI
XXE
Weak Cipher

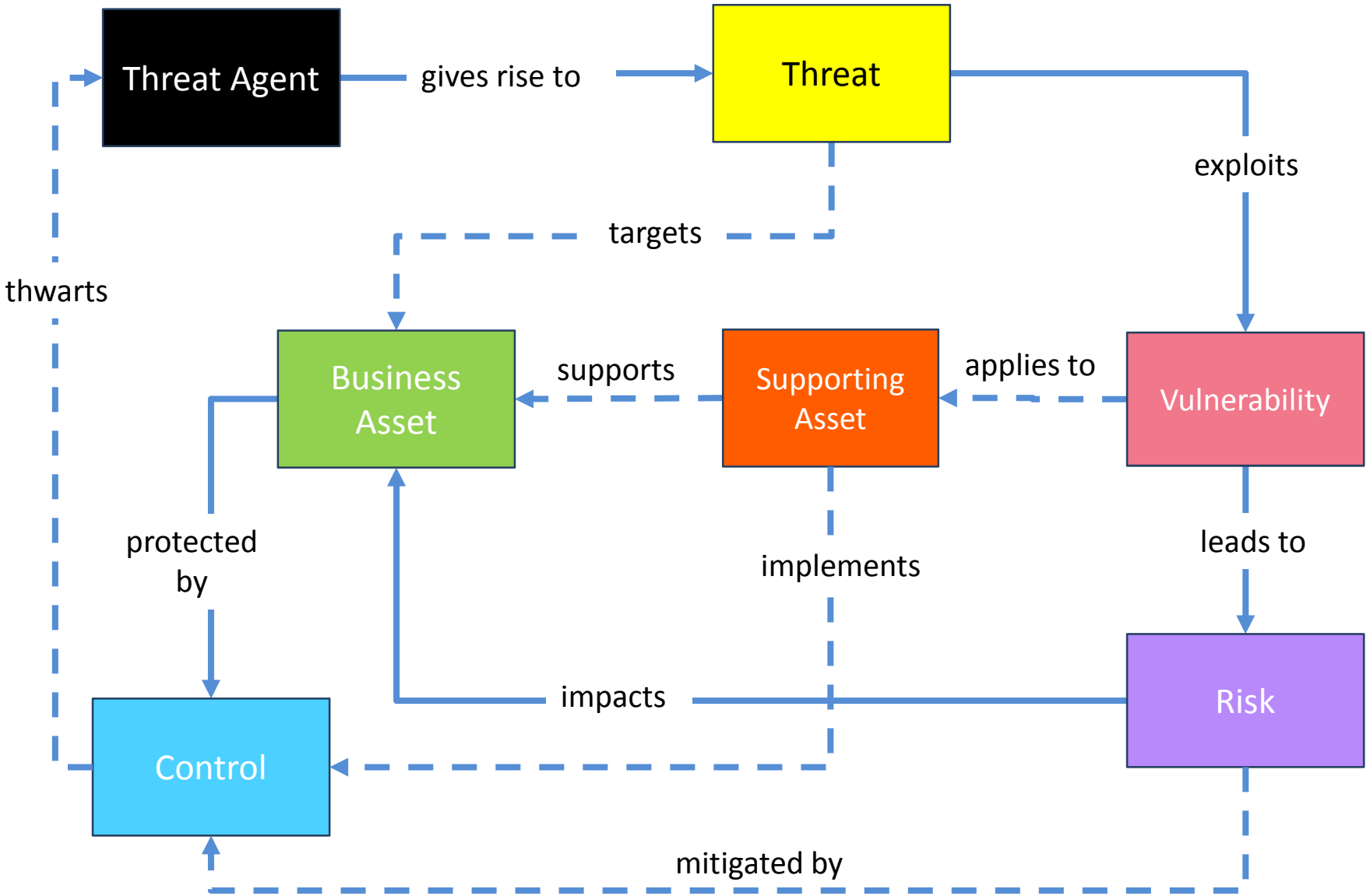
Data model


A script-kiddie
gives rise to
Disclose
exploits
targets
applies to
thwarts
Photos
supports
Database
Web portal
Database
SQLI
XXE
Weak Cipher
protected by
implements
WAF
FW config
Strong Cipher

Data model


A script-kiddie
gives rise to
Disclose
exploits
targets
thwarts
applies to
Photos
supports
Database
Web portal
Database
SQLI
XXE
Weak Cipher
protected by
implements
leads to
impacts
Disclosure of photos
WAF
FW config
Strong Cipher
mitigated by

Data model


Threat Agent
gives rise to
Threat
exploits
targets
thwarts
Business Asset
supports
Supporting Asset
applies to
Vulnerability
protected by
implements
leads to
impacts
Risk
Control
mitigated by

Expressing Risk

- It's possible to express the risk as a feared event, or a use case
  - Misuse case or abuse case

- So user story templates work

  In order to **<Motivation>,** as a **<Threat Agent>**, I can **<Threat class>** this **<Business Asset>**, via **<Attack Path>** [compromising this (these) **<Supporting Asset>** by exploiting this (these) **<Vulnerability>]**

- Example
  - In order to **boost his ego,** as an **script-kiddie**, I can **disclose** these **photos**, via [compromising this **database**, by exploiting this **lack of input/output validation**]

How to evaluate the risk

Question

- What may be the **likelihood** the risk scenario occurred ?

Likelihood (1/3)

Occurrence		Probability	
Q1: Did it happen in my company? (Internal Events)	Q2: Did it happen in another company? (External Events)		
It never happened	It never happened (no similar events seen in media)	Low	1
It happens several times a year	It happens several times a year (can be seen in specialized media)	Medium	2
It happens several times a month	It happens several times a month (can be seen sometimes in major media)	High	3
It happens at least once a week	It happens several times a week (can be seen always in major media)	Very high	4

Probability of occurrence = MAX(Q1,Q2)

Likelihood (2/3)

Complexity			Value	
Q1: What is the company knowledge required?	Q2: What is the technical knowledge required?	Q3: What countermeasures are in place?		
It can be done by an external user without any knowledge	No knowledge is required	No countermeasures are in place	Low	1
It can be done by an external user with some knowledge	Some knowledge or research are required	Some countermeasures are in place	Medium	2
It can be done by an external user with a very good knowledge (e.g. ex-employee)	Some knowledge and research are required	Countermeasures are in place but their efficiency has not been checked	High	3
It can be done by an insider or with the complicity of an insider	Advanced knowledge and research are required	Efficient countermeasures are in place	Very high	4

Complexity = (Q1 +Q2 + Q3) / 3

Likelihood (3/3)

Likelihood		Occurrence			
		1	2	3	4
Complexity	4	1	1	1	3
	3	1	2	2	3
	2	2	3	4	4
	1	2	3	4	4

Question

- What is the **impact** if the risk scenario occurred ?

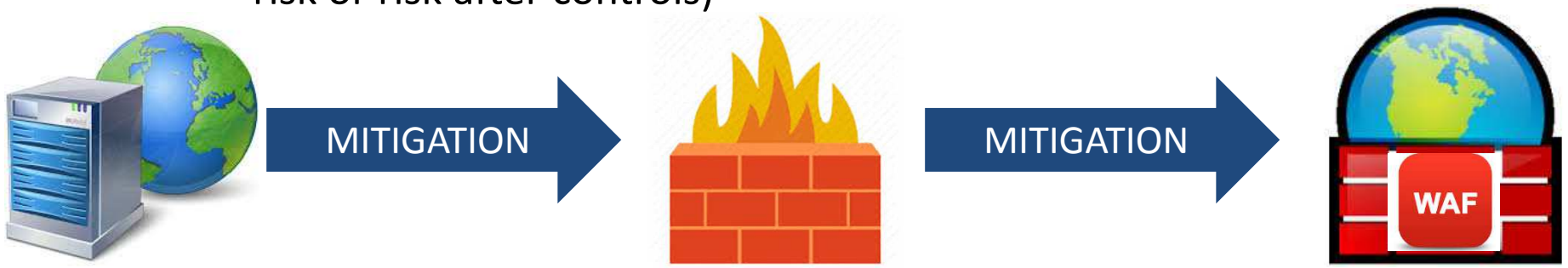
Impact of an attack vs value of an asset

- For the user, the impact is not only the value of the stolen photos, it may also be a loss of reputation
- For the service provider, the impact may be a **loss of reputation** for itself or for its photo service
- In general, the **impact** of an attack can be
  - Financial
  - Legal
  - Against reputation
  - Against activity

Residual Risk

- Risk cannot be eliminated, but it can be **reduced to an acceptable level**

- Inherent risk
  - The risk before any controls, or other mitigating factors, are in place (the gross risk or risk before controls)
- Residual risk
  - The risk that remains after controls are taken into account (the net risk or risk after controls)



Inherent risk: **HIGH**

Residual risk: **MEDIUM**

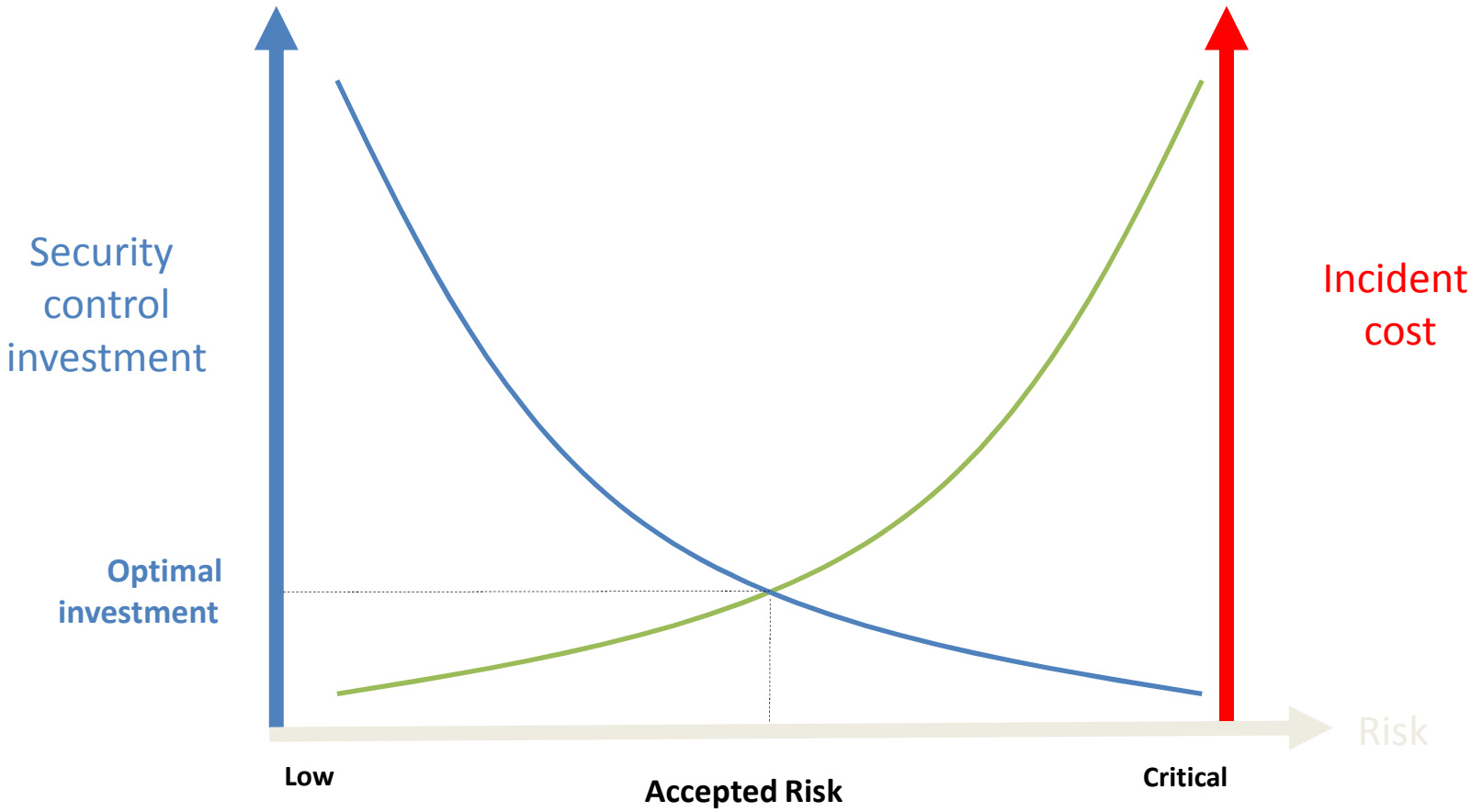
Residual risk: **LOW**

How to manage the risk

Risk Treatment

- Risk can be dealt with in 4 different manners
- **Avoid**
  - Come up with alternatives so that the risk is not realized
- **Transfer** (assignment)
  - Pass on the risk to someone else
- **Mitigate** (reduction)
  - Eliminate (or significantly decrease) the level of risk
- **Accept**
  - Do nothing

Risk And Cost



Control

- Any solution put in place to mitigate the risk level
  - A.k.a. countermeasure
  - On supporting assets
- 3 categories of controls
  - Administrative
    - Laws, regulations, policies, practices and guidelines
  - Logical
    - Application and technical controls (systems and software), such as firewalls
  - Physical
    - Locked rooms, video surveillance systems, gates and barricades or use of guards
- 3 types of effects
  - Preventive
    - Prevent the loss or harm from occurring
  - Detective
    - Monitor activity to identify instances where practices or procedures were not followed
  - Corrective
    - Restore the system or process back to the state prior to a harmful event

Example Of Control

- Server application doesn't perform escaping of untrusted data before building SQL statements
- Therefore there is a risk that "An attacker can disclose user passwords stored in the database by exploiting the lack of output validation"
- The risk can be mitigated by
  - The systematic (and correct) use of prepared statement and/or the escaping of untrusted input
  - The deployment of a Web Application Firewall
- It's a logical and preventive control

Threat modeling strategy

- Asset centric (ISO 27005)
- Feared event (based on a threat agent e.g. NSA, or based on an abuse-case aka misuse-case)
- Architecture centric (Microsoft)
- Attacker centric (e.g. NSA)

- **The strategies can be combined for more efficiency**
  - e.g. if my server is (ab)used for file sharing then it cannot be easily detected by looking at the architecture

Deep dive in RA

Risk generic formula

- The possibility that an attacker will cause harm or loss to an asset
- Risk is expressed on a scale with **LOW** / **MEDIUM** / **HIGH**

Risk = **(Impact** + **(Likelihood** **+** **Vulnerability)/2)/2**

- **Note 1:** Risk = Inherent Risk
- **Note 2:** the inherent risk is the risk that an activity would pose if no controls or other mitigating factors were in place

Formulas & Ranges

- **Impact**: **HIGH** [7-10] / **MEDIUM** [4-6] / **LOW** [0-3]
- **Likelihood**: **HIGH** [7-10] / **MEDIUM** [4-6] / **LOW** [0-3]
- **Risk**: **HIGH** [7-10] / **MEDIUM** [4-6] / **LOW** [0-3]

- **Vulnerability**: **HIGH** [7-10] / **MEDIUM** [4-6.9] / **LOW** [0-3.9] (CVSS)

Risk[0/10] = **(Impact[0/10] +** (**Likelihood[0/10] +** **V[0/10])/2)/ 2**

Common Vulnerability Scoring System v2 (CVSS)

- **Common Vulnerability Scoring System**

- Base Score

- Access Vector (Local / Adjacent / Network)
- Access Complexity (High / Medium / Low)
- Authentication (Multiple / Single / None)

- Impact on CIA (None / Partial / Complete)

- Temporal Score

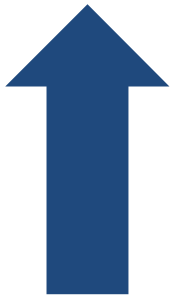
- Exploitability (Not defined / Unproven Exploit / POC / Functional Exploit / High)
- Remediation level (Not defined / Official fix / Temp fix / Workaround / Unavailable)
- Report Confidence (Not defined / Unconfirmed / Uncorroborated / Confirmed)

- Have a look to : https://nvd.nist.gov/CVSS-v2-Calculator

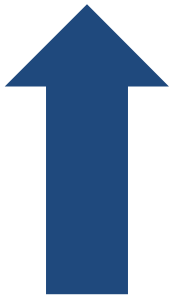
Calculating Risk

Threat
Threat Agent (resources, skills, opportunity,…)
Motivation (asset value for the attacker)

Risk = (Impact + (Likelihood + Vulnerability)/2)/2

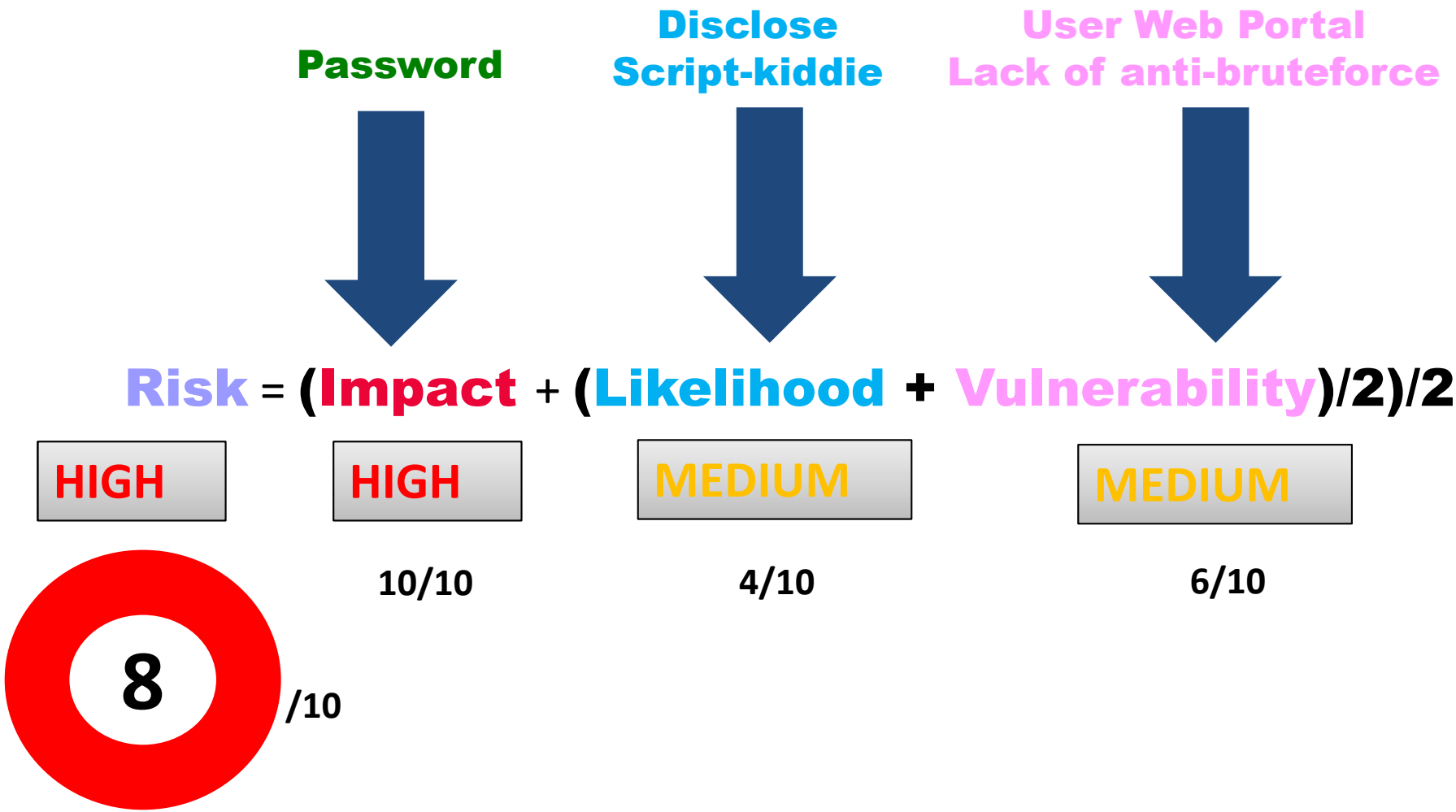


Business Asset value
(for a Security property)



Supporting Asset
CVSS

Calculating Risk



Threat Agent

- Insider
- Criminal
- Competitor
- Criminal Organization
- Government Agency
- Researcher
- Activist
- Script kiddie
- User
- R&D employee
- Operational employee
- Maintenance employee
- IT employee

Threat categorization by Microsoft

Spoofing

Can an attacker gain access using a false identity?

Tampering

Can an attacker modify data as it flows through the application?

Repudiation

If an attacker denies an exploit, can you prove him or her wrong?

Information disclosure

Can an attacker gain access to private or potentially injurious data?

Denial of service

Can an attacker crash or reduce the availability of the system?

Elevation of privilege

Can an attacker assume the identity of a privileged user?

Supporting Asset

- Database
- Operating System
- Application Server
- Application module
- File
- Log
- Web service
- Web User interface
- Remote API
- Local API
- Crypto key
- Software Application
- Service Provider
- Hardware device
- Computer
- Human
- Network
- Server
- Source code
- Organization
- Location
- Processus
- Interface

Granularity matters… (e.g. on Supporting Asset)

- Computer
  - Keyboard
  - Mouse
  - Screen
  - Base unit
    - Motherboard
      - CPU
      - …
    - Memory
    - Hard disk
    - Power Supply
    - Operating System
      - Applications
      - …

Vulnerability

Keylogger (hardware)

Vulnerability

Keylogger (hardware)

Vulnerability

Keylogger (software)

Granularity increases RA workload…!

Vulnerability category (OWASP based)

- API Abuse
- Authentication Vulnerability
- Authorization Vulnerability
- Availability Vulnerability
- Code Permission Vulnerability
- Code Quality Vulnerability
- Configuration Vulnerability
- Cryptographic Vulnerability
- Encoding Vulnerability
- Environmental Vulnerability
- Error Handling Vulnerability
- General Logic Error Vulnerability
- Input Validation Vulnerability
- Logging and Auditing Vulnerability
- Password Management Vulnerability
- Path Vulnerability
- Protocol Errors
- Range and Type Error Vulnerability
- Sensitive Data Protection Vulnerability
- Session Management Vulnerability
- Synchronization and Timing Vulnerability
- Unsafe Mobile Code
- Use of Dangerous API

Note that a vulnerability can be expressed as a “lack of” something (e.g. a lack of control…)

Business Asset

- Service
  - Payment Service
- Data
  - PAN

Depends on your business…

Data Classification

POTENTIAL IMPACT			
Security Objective	**LOW**	**MEDIUM**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Property Definition: Confidentiality

Confidentiality (for data and service) is the property that information is not made available or disclosed to unauthorized individuals, entities or processes

Property Definition: Integrity

Integrity (for data and service) is the property of protecting the accuracy and completeness of assets, in other words the property that ensure that the asset has not been modified by unauthorized entities

For example:

- the integrity for a service can be the way to insure that the process is not subverted (e.g. a web service is defaced is an integrity violation)

Property Definition: Availability

Availability (for data and service) is the property of being accessible and usable upon demand by an authorized entity

Availability (for service) is related to the Service Level Agreement of the service itself agreed with the customer.

Property Definition: Authenticity

Authenticity (for the one who produces the data or the service) is the property that an entity is what it claims to be, or in other words, the property that assure that the asset has been produced by a genuine entity

For example:

- the authenticity for a mail can be provided by its signature
- the authenticity for a web service can be provided by the certificate of this web service

Property Definition : Authorization

Authorization (for data and service) or access control is the property that ensure that access to assets is authorized and restricted based on business and security requirements, or in other words, the property that assure that asset can be accessed only by entities with the right privileges

For example:

- the authorization for a service can be the validation of the access rights of the authenticated user before to proceed

Property Definition : Non-repudiation

Non-repudiation or accountability (for service and data) is the ability to prove the occurrence of a claimed event or action and its originating entities, or in other words, the property that assure that authorized access to the asset cannot be denied (e.g. signature or log files)

For example:

- the non-repudiation for a mail can be provided by its signature
- the non-repudiation for a service can be provided by an audit log