


UNIVERSITY  
OF TRENTO - Italy




**Cyber Security Risk Assessment**  
**Fall 2016**

*Lecture 06 – Asset Identification*  
*Fabio Massacci*

Fall 2015 Fabio Massacci - EIT Security Engineering



UNIVERSITY  
OF TRENTO - Italy



**Identify Assets**

- ***First step in risk management***
  - You can't plan the protection of something if you don't know what you're protecting
- ***Intangible, mission critical, activities are what you want to protect***
  - Protection of privacy in burglary case
  - Separation between aircrafts in Air Control Tower
- ***Tangible supporting assets are what you can protect***

UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL

## Identify Assets...

- **Goal: 99.999 percent up time**
- **Failover cluster**
- **RAID**

UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL

## What are we protecting?

- **Tangible Assets from picture**
  - Three servers
  - Four connection links
  - A raid driver
  - A load balancer
  - Two DBMS Software
- **What for?**
  - Never discussed beforehand
- **Key (Intangible) activities:**
  - Potential students check out degrees offer when university rankings get out
  - University provides key data in case of adverse meteo events
- **Are tangibles correct?**

Fall 2015 Fabio Massacci - EIT Security Engineering

UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL

## Business Impact Analysis

- **How do we get to supporting assets?**
  - Start with what matters in a sudden loss

```


graph TD
    A[Define the scope] --> B[Identify objectives of activities]
    B --> C[Identify critical functions & processes (intangibles)]
    C --> D[Map functions & processes to IT systems (supporting assets)]
  
```

UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL


## Identify Activities

- **Rough Classification**
  - System functions or services
  - Data or information
- **Other activities can often be re-mapped**
  - E.g. Reputation → lost because you have not delivered a service or you have disclosed some data
- **Identify critical functions/ information for the business**
  - If you don't deliver that there is pretty much no point in delivering the rest
    - If you can't graduate students because you don't know their grades → organizing a spotless ceremony is pretty much useless
- **Priority → Eliminate single points of failure (SPOF)**
  - Part of a system that can cause entire system to fail
  - If SPOF fails, entire system fails
- **Failure of**
  - Confidentiality
  - Integrity
  - Availability
- **When do you want to identify a single point of failure?**
  - Before it fails?
  - Or after if fails?
  - But in some cases you don't know they exists...

Fall 2015 Fabio Massacci - EIT Security Engineering




UNIVERSITY OF TRENTO




## System Functions: Manual and Automated

- **Manual**
  - Written (paper) records
  - Manuals of procedures
- **Automated**
  - Hardware
  - Software
- **People operating the above**
  - Knowledge of process




UNIVERSITY OF TRENTO - Italy




## System functions - all or nothing?

- **When analyzing system functions do not think they are monolithic**
  - It might be possible to protect one part and not the other
  - Or provide a “degraded” mode (eg confidentiality is lost but integrity is preserved)
- **Example - Adrian Cockcroft et al. from Netflix on design principles**
  - Fail Fast: Set aggressive timeouts such that failing components don’t make the entire system crawl to a halt.
  - Fallbacks: Each feature is designed to degrade or fall back to a lower quality representation. For example if we cannot generate personalized rows of movies for a user we will fall back to cached (stale) or un-personalized results.
  - Feature Removal: If a feature is non-critical then if it’s slow we may remove the feature from any given page to prevent it from impacting the member experience.
- **Design only possible if you break the super-high level function into “smaller” functions**
  - streaming selected videos in the database VS
  - show database, search and select, stream selected

Fall 2015 Fabio Massacci - EIT Security Engineering



UNIVERSITY OF TRENTO - Italy



## Data and Information Assets

- **Data protected by:**
  - Access controls
  - Backups


Organization

Customer


Intellectual property

Data warehousing

Data mining

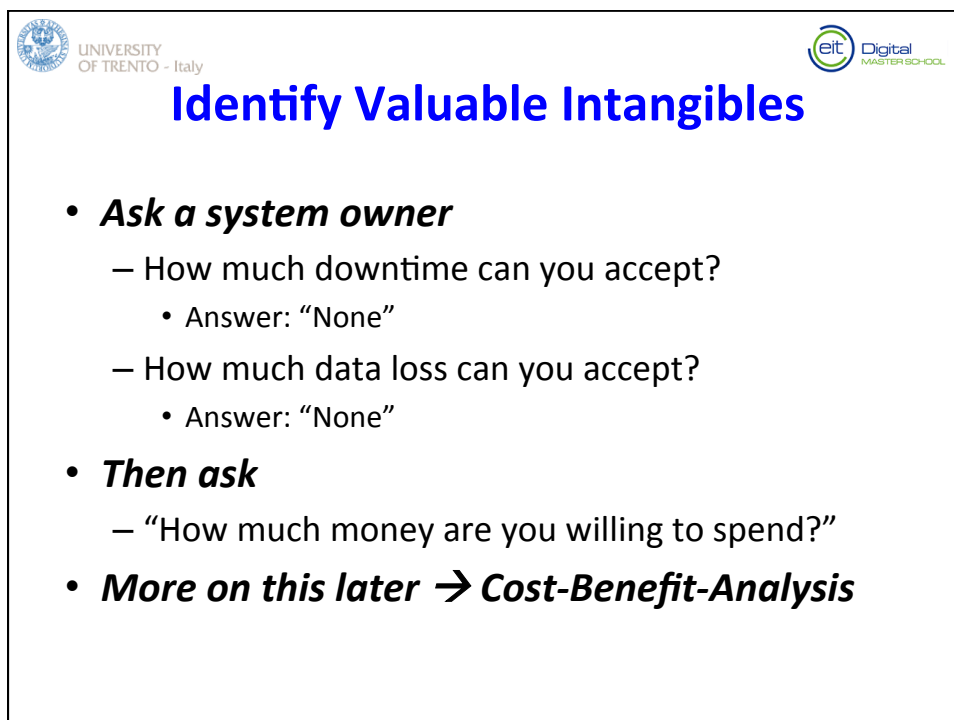
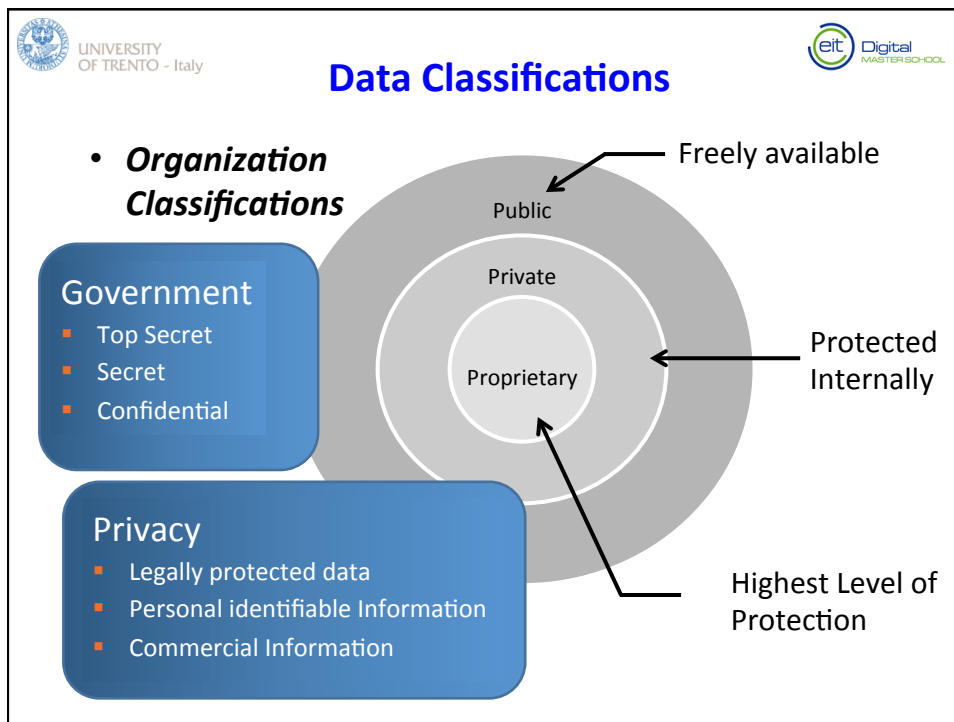


UNIVERSITY OF TRENTO - Italy



## Role of Data in Organization

- ***Value of data often overlooked***
- ***Classifying important step***
- ***Without classifications***
  - Users may not recognize the value
  - Users may not protect
  - IT may not backup as often as needed
- ***Some data is warranted protection by law***
  - Legal liabilities might follow



UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL

## Business Impact Analysis

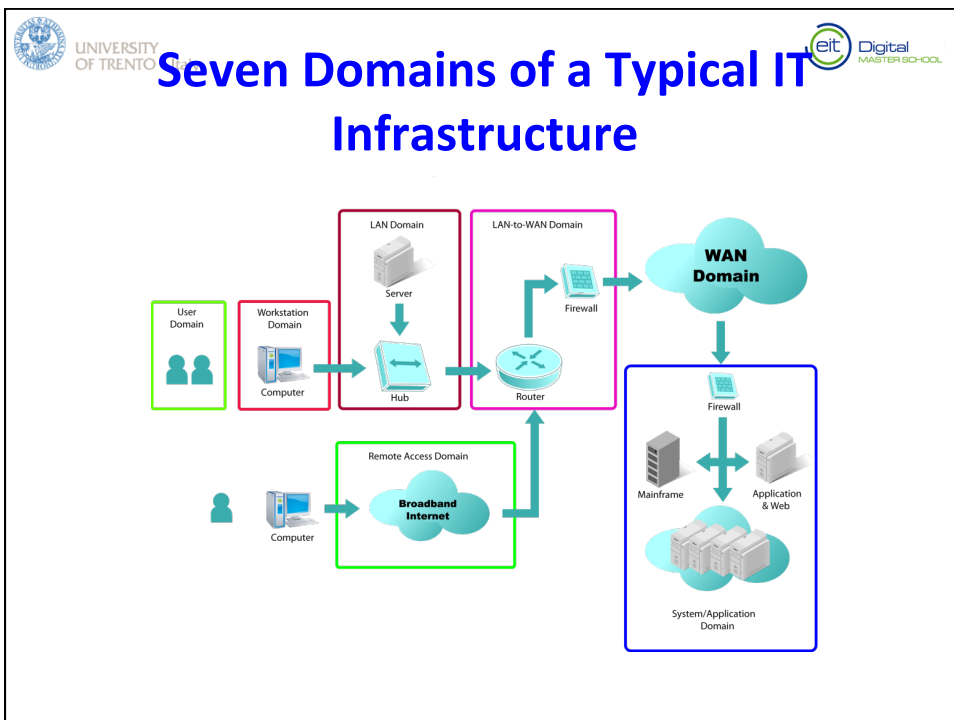
- **How do we get to supporting assets?**
  - Start with what matters in a sudden loss


Define the scope

Identify objectives of activities


Identify critical functions & processes (intangibles)

**Map functions & processes to IT systems (supporting assets)**





UNIVERSITY  
OF TRENTO - Italy




## Asset and Inventory Management

### Inventory management


- Used to manage hardware inventories

### Asset management

- Used to manage all types of assets; much more detailed data than an inventory management system




UNIVERSITY  
OF TRENTO - Italy




## Software Assets

- ***Operating system and applications***
- ***OS specifics should include:***
  - Hardware system where it's installed
  - Name of the operating system
  - Latest service pack installed
- ***Application specifics should include:***
  - Name of the application
  - Version number
  - Service pack or update information if available






UNIVERSITY  
OF TRENTO - Italy




## Hardware Assets

- **Computers:**
  - Servers, desktop PCs
- **Networking devices:**
  - Routers, switches
- **Network appliances:**
  - Firewalls, spam appliances
- **Information you need to know:**
  - Location
  - Manufacturer
  - Model number
  - Hardware components, such as processor and random access memory (RAM)
  - Hardware peripherals, such as add-on network interface cards (NICs)
  - Basic Input/Output System (BIOS) version




UNIVERSITY  
OF TRENTO - Italy




## Personnel Assets

- ***The people working for you***
- ***When any function or process depends on a single person, he/she becomes a single point of failure***
- **Reduce risk by:**
  - Hiring additional personnel
  - Cross-training
  - Rotating jobs




UNIVERSITY OF TRENTO - Italy




## People is most frequent SPOF

- **Email dated: October 1st, 2016**
  - Initially I started using this MSL (Master Schooll segment, but after a while it appeared that this plaza segment has more than 2200 members.
  - Almost **all contact persons** automatically become member of this plaza.
  - Also the person that had administrator rights (<A>) is already gone for several years and nobody knows how to access this plaza
  - and **EIT Digital Office** does not want to give **me** or <B> the administrator rights.
  - Instead they suggested to open a new plaza MSL 2016. It is the proposal to use this plaza for our <stuff>.
  - I have checked and you both are member so you should see the MSL 2016 segment in your list.
  - Please use this plaza.
- **Several things gone wrong here but in particular**

Fall 2015 Fabio Massacci - EIT Security Engineering




UNIVERSITY OF TRENTO - Italy




## People is most frequent SPOF

- **Email dated: October 1st, 2016**
  - Initially I started using this MSL (Master Schooll segment, but after a while it appeared that this plaza segment has more than 2200 members.
  - Almost **all contact persons** automatically become member of this plaza.
  - Also the person that had administrator rights (<A>) is already gone for several years and nobody knows how to access this plaza and **EIT Digital Office** does not want to give **me** or <B> the administrator rights.
  - Instead they suggested to open a new plaza MSL 2016. It is the proposal to use this plaza for our <stuff>.
  - I have checked and you both are member so you should see the MSL 2016 segment in your list. Please use this plaza.
- **Several things gone wrong here but in particular**
  - **EIT Digital Office** has likely a badly designed system in which everybody with admin access can do whatever → immortality assumption when <A> worked there (they won't change, they can't make mistakes)
  - <A> set-up a bad access policy
  - <A> is gone...

Fall 2015 Fabio Massacci - EIT Security Engineering




UNIVERSITY  
OF TRENTO - Italy




## Facilities and Supplies

- **Assets consume other assets**
  - Software, Hardware & Wetware (aka people) are always somewhere
  - ... and they can break and also consume resources possibly from other organizations
- **Inputs**
  - Energy, raw materials is you are producing stuff
  - Maintenance
  - Other services (e.g. in the cloud)
- **Location**
  - If there is a flood...



UNIVERSITY  
OF TRENTO - Italy



## Cascading Failures from Suppliers

- **April 21, 2011**
  - Amazon Web Service Elastic Block Storage goes down in one region
    - Amazon operates multiple regions, allowing users to add redundancy to their applications by hosting them in several regions. When one region experiences performance problems, customers can shift workloads to an unaffected region.
  - Reddit, HootSuite link-sharing tool, Quora (question-and-answer service), Facebook app for Microsoft go down
  - Netflix slow down but not much
    - “Our architecture avoids using EBS as our main data storage service, and the SimpleDB, S3 and Cassandra services that we do depend upon were not affected by the outage.”
    - “Netflix uses Amazons Elastic Load Balance (ELB) service to route traffic to our front end services. We utilize ELB for almost all our web services.”
    - This meant that when the outage happened last week we had to manually update all of our ELB endpoints to completely avoid the failed zone,
- **December 2012**
  - Amazon Elastic Load Balancers goes down
  - Netflix takes a bad hit as well

Fall 2015 Fabio Massacci - EIT Security Engineering



## Suggested Readings

- ***Textbook (Managing Risk in Information Systems, 2nd ed)***
  - Chapter 6.
- ***Netflix Lessons Learned From Outage***
  - <http://techblog.netflix.com/2011/04/lessons-netflix-learned-from-aws-outage.html>
  - <http://techblog.netflix.com/2012/12/a-closer-look-at-christmas-eve-outage.html>
- ***The San Francisco SysAdmin***