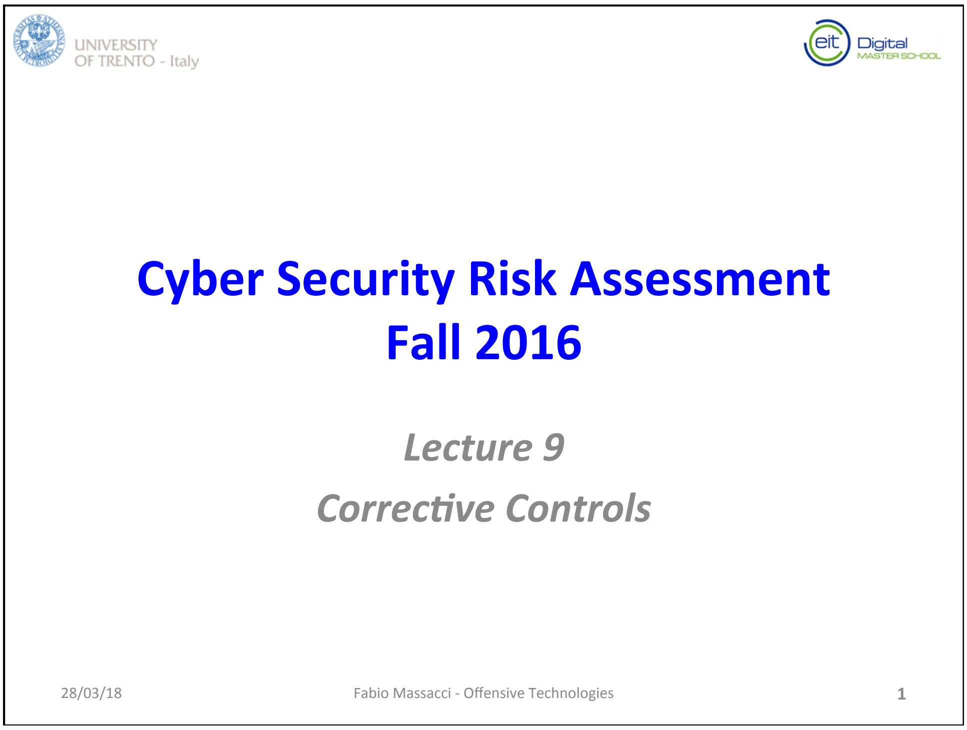


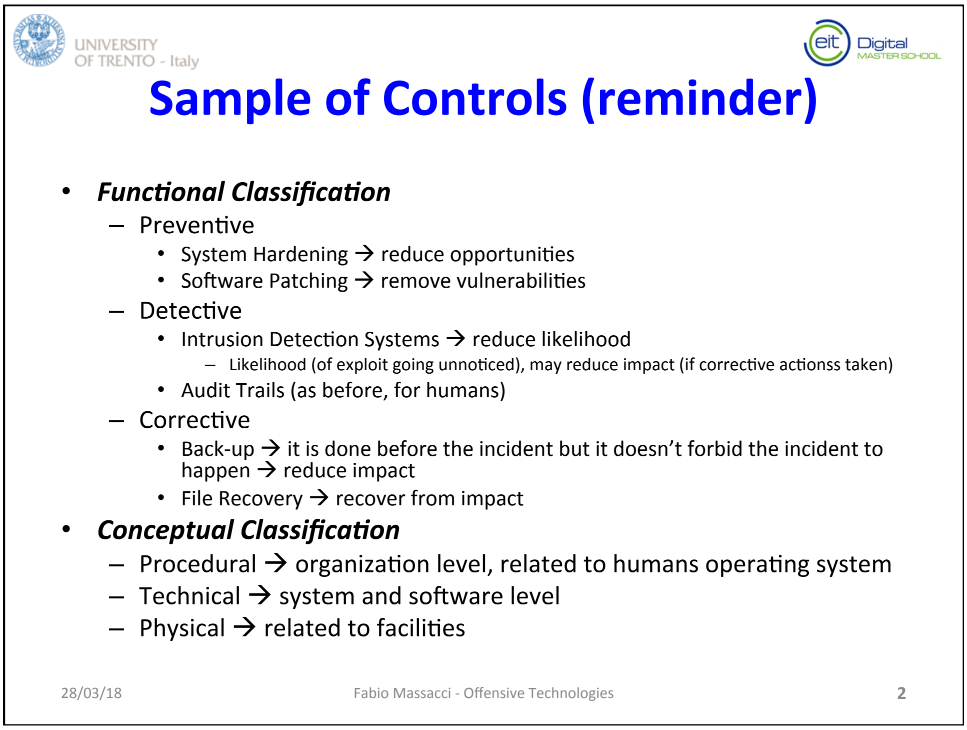
UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Cyber Security Risk Assessment
Fall 2016

Lecture 9

Corrective Controls

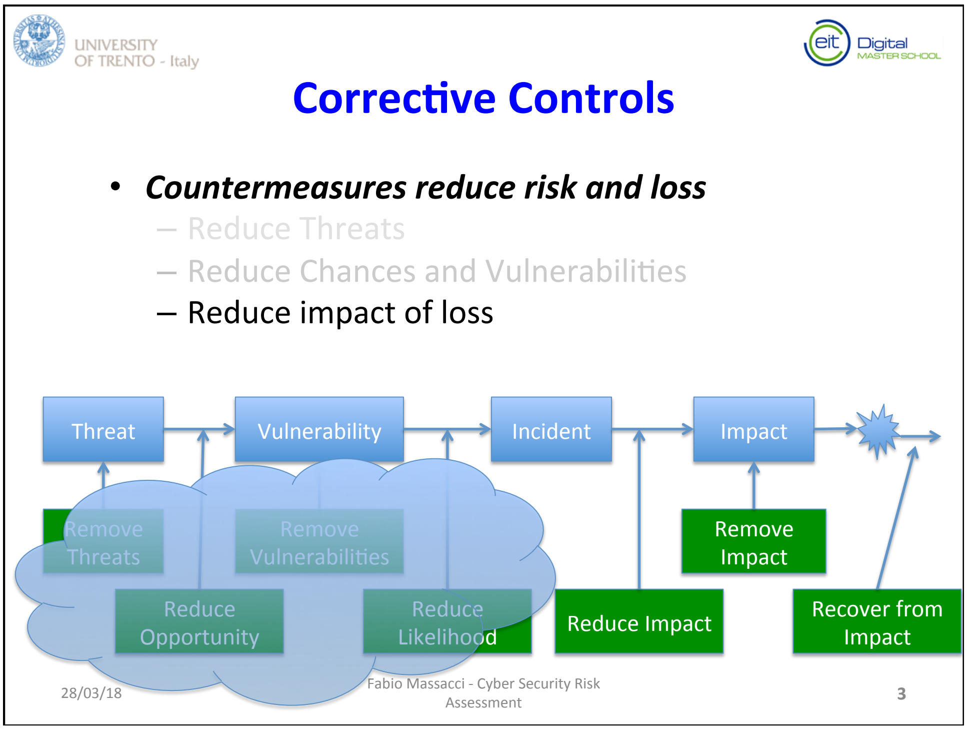


UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Sample of Controls (reminder)

- ***Functional Classification***
  - Preventive
    - System Hardening → reduce opportunities
    - Software Patching → remove vulnerabilities
  - Detective
    - Intrusion Detection Systems → reduce likelihood
      - Likelihood (of exploit going unnoticed), may reduce impact (if corrective actionss taken)
    - Audit Trails (as before, for humans)
  - Corrective
    - Back-up → it is done before the incident but it doesn't forbid the incident to happen → reduce impact
    - File Recovery → recover from impact
- ***Conceptual Classification***
  - Procedural → organization level, related to humans operating system
  - Technical → system and software level
  - Physical → related to facilities



UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Corrective Controls

- ***Countermeasures reduce risk and loss***
  - Reduce Threats
  - Reduce Chances and Vulnerabilities
  - Reduce impact of loss

Threat

Vulnerability

Incident

Impact

Remove Threats

Remove Vulnerabilities

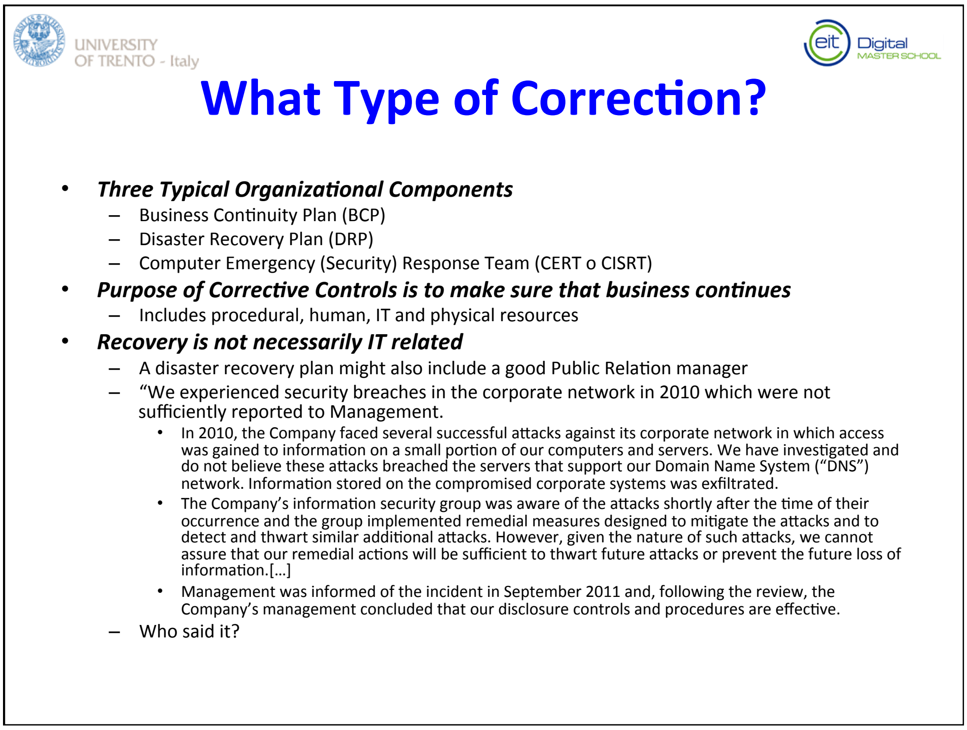
Reduce Opportunity

Reduce Likelihood

Reduce Impact

Remove Impact

Recover from Impact



UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

What Type of Correction?

- ***Three Typical Organizational Components***
  - Business Continuity Plan (BCP)
  - Disaster Recovery Plan (DRP)
  - Computer Emergency (Security) Response Team (CERT o CISRT)
- ***Purpose of Corrective Controls is to make sure that business continues***
  - Includes procedural, human, IT and physical resources
- ***Recovery is not necessarily IT related***
  - A disaster recovery plan might also include a good Public Relation manager
  - "We experienced security breaches in the corporate network in 2010 which were not sufficiently reported to Management.
    - In 2010, the Company faced several successful attacks against its corporate network in which access was gained to information on a small portion of our computers and servers. We have investigated and do not believe these attacks breached the servers that support our Domain Name System ("DNS") network. Information stored on the compromised corporate systems was exfiltrated.
    - The Company's information security group was aware of the attacks shortly after the time of their occurrence and the group implemented remedial measures designed to mitigate the attacks and to detect and thwart similar additional attacks. However, given the nature of such attacks, we cannot assure that our remedial actions will be sufficient to thwart future attacks or prevent the future loss of information.[...]
    - Management was informed of the incident in September 2011 and, following the review, the Company's management concluded that our disclosure controls and procedures are effective.
  - Who said it?

Elements of a BCP

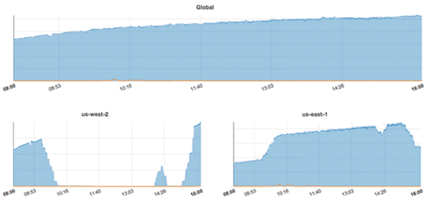
- ***Purpose, scope, assumptions***
- ***System description and architecture of impacted tangible assets***
- ***Responsibilities***
- ***Implementation***
  - Phases
  - Technical Instruments
  - Typically through individual DRPs
- ***Plan training, testing, and exercises***
- ***Plan maintenance***

Purpose and Scope

- ***Not everything is essential for the operation to keep going***
  - No Landing at airport might be acceptable if planes can be re-routed to a nearby one
  - If laser guided landing not possible, visibility landing might be neeeded
- ***BCP scope identifies what is essential (and how much does it cost to keep it running)***
- ***Typically achieved through a Business Impact Analysis***
  - Identify critical business functions (CBFs)
  - Identify critical processes supporting the CBFs
  - Identify critical IT services supporting the CBFs, including any dependencies
  - Determine acceptable downtimes for CBFs, processes, and IT service
- ***BIA qualitative so far, it can be also quantitative → forthcoming lectures***

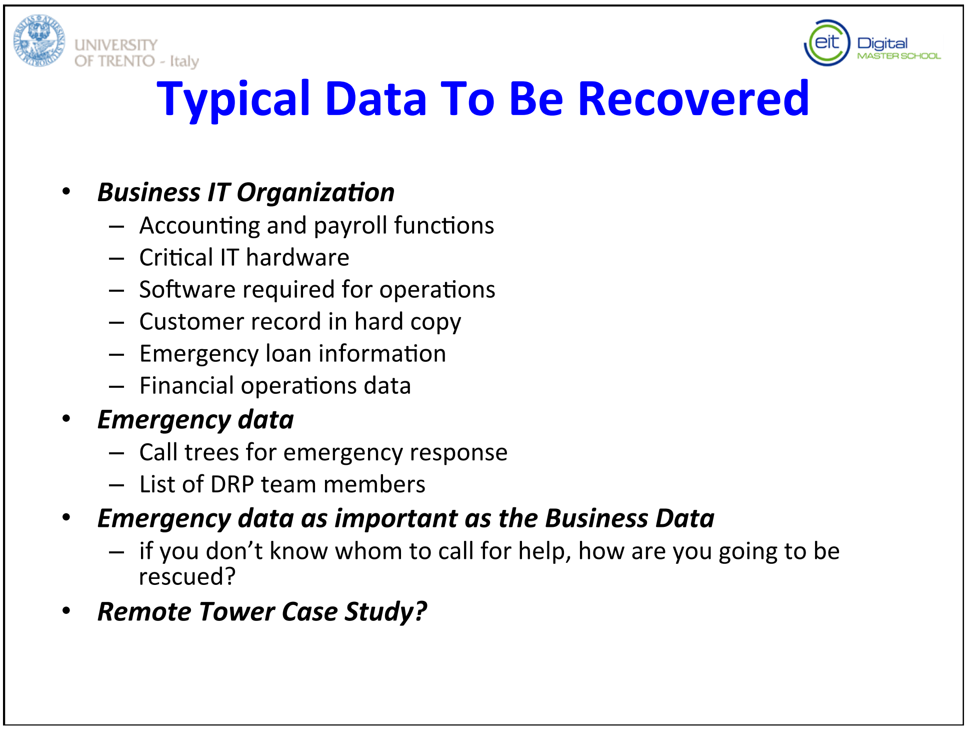
Netflix example

- ***"Our metric of interest is customer engagement, which we measure as the number of video plays that start each second."***
- ***Exercise of disruption***
  - "most of our attention stays focused on the top row."
  - In the bottom row, you can clearly see traffic evacuate from the west region.
  - The east region gets a corresponding bump in traffic as it steps up to play the role of savior.
  - As long as the aggregate metric follows that relatively smooth trend, we know that our system is resilient to the failover."
  - http://techblog.netflix.com/2015/09/chaos-engineering-upgraded.html
- ***Then this needs to be passed over to the technical infrastructure***



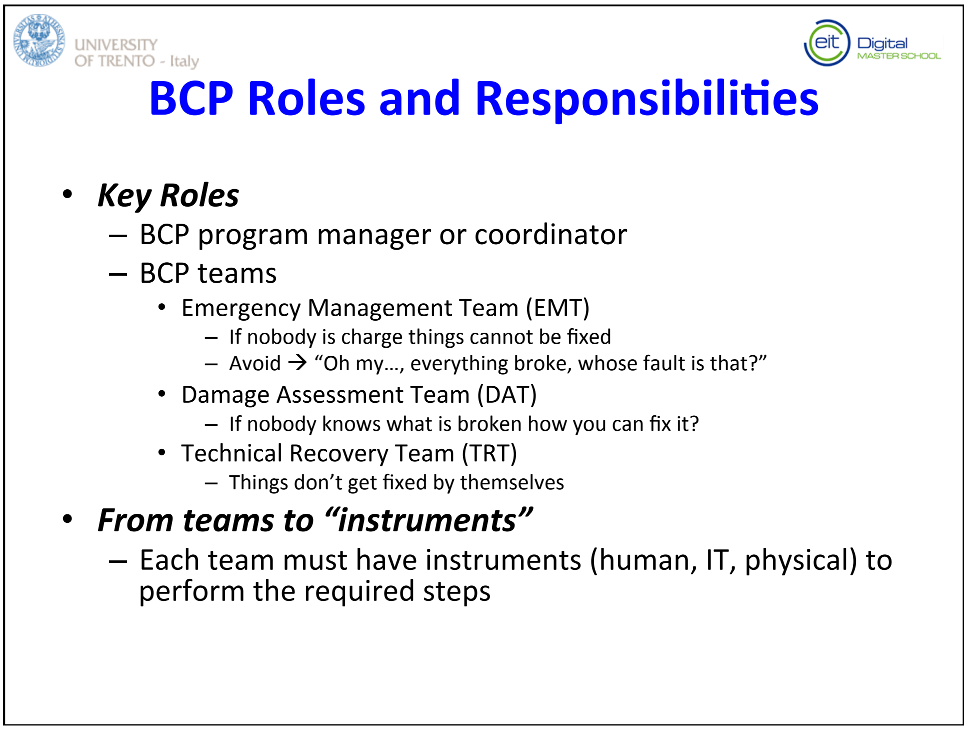
Identification of Tangible Assets

- Identify all critical components for the system
- Identify all equipment ~ servers, switches, routers
- Include databases hosted on the system
- Include files ~ documents or spreadsheets
- Include necessary supplies



Typical Data To Be Recovered

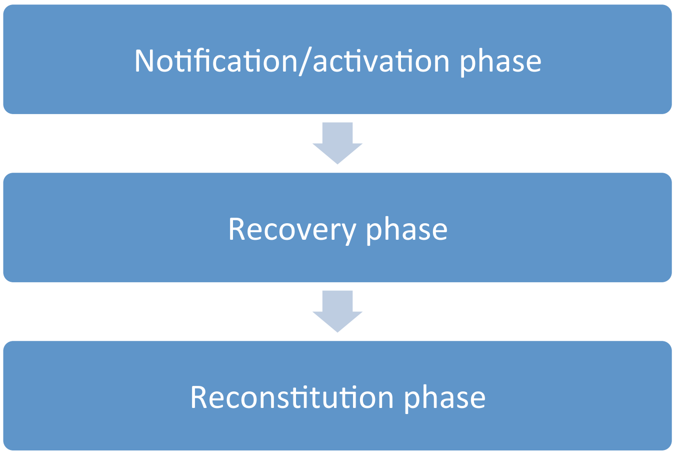
- ***Business IT Organization***
  - Accounting and payroll functions
  - Critical IT hardware
  - Software required for operations
  - Customer record in hard copy
  - Emergency loan information
  - Financial operations data
- ***Emergency data***
  - Call trees for emergency response
  - List of DRP team members
- ***Emergency data as important as the Business Data***
  - if you don't know whom to call for help, how are you going to be rescued?
- ***Remote Tower Case Study?***



BCP Roles and Responsibilities

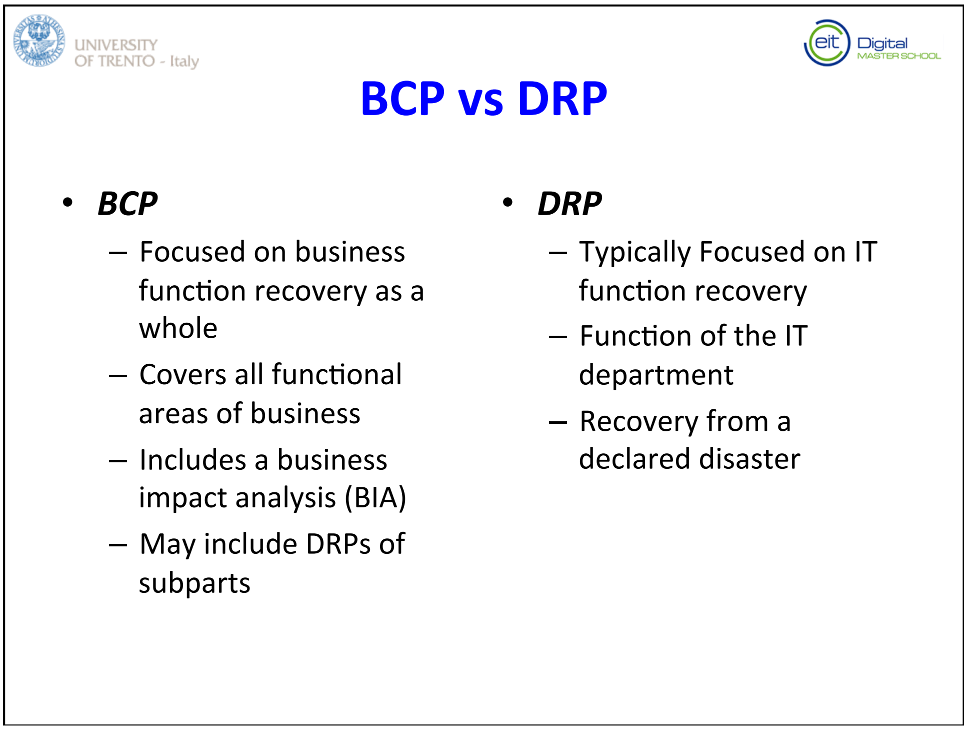
- ***Key Roles***
  - BCP program manager or coordinator
  - BCP teams
    - Emergency Management Team (EMT)
      - If nobody is charge things cannot be fixed
      - Avoid → "Oh my..., everything broke, whose fault is that?"
    - Damage Assessment Team (DAT)
      - If nobody knows what is broken how you can fix it?
    - Technical Recovery Team (TRT)
      - Things don't get fixed by themselves
- ***From teams to "instruments"***
  - Each team must have instruments (human, IT, physical) to perform the required steps

Phases within a BCP Plan



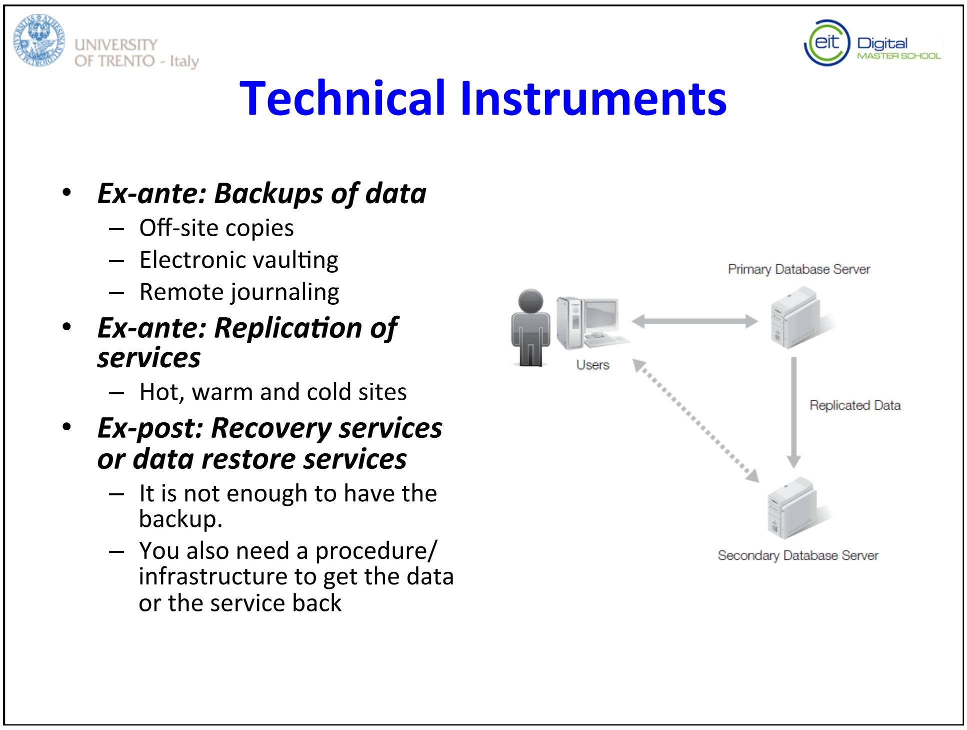
Implementation through DRPs

- ***What is a Disaster Recovery Plan?***
  - A plan to restore a critical business process or system to operation after a disaster
  - A component of the overall BCP
  - Other names:
    - Contingency planning, Business resumption planning, Corporate contingency planning, Business interruption planning, Disaster preparedness
- ***DRP key terms:***
  - Critical business function (CBF)
  - Maximum acceptable outage (MAO)
  - Recovery time objectives (RTO)



BCP vs DRP

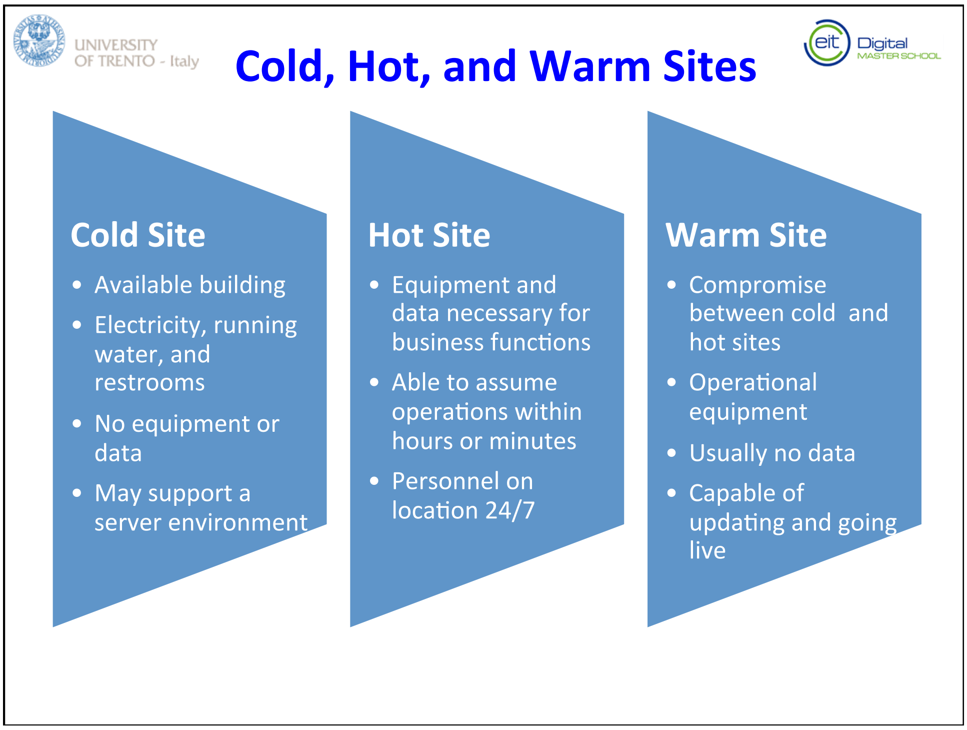
- ***BCP***
  - Focused on business function recovery as a whole
  - Covers all functional areas of business
  - Includes a business impact analysis (BIA)
  - May include DRPs of subparts
- ***DRP***
  - Typically Focused on IT function recovery
  - Function of the IT department
  - Recovery from a declared disaster



Technical Instruments

- ***Ex-ante: Backups of data***
  - Off-site copies
  - Electronic vaulting
  - Remote journaling
- ***Ex-ante: Replication of services***
  - Hot, warm and cold sites
- ***Ex-post: Recovery services or data restore services***
  - It is not enough to have the backup.
  - You also need a procedure/ infrastructure to get the data or the service back

Primary Database Server
Users
Replicated Data
Secondary Database Server



UNIVERSITY OF TRENTO - Italy

Cold, Hot, and Warm Sites

Cold Site

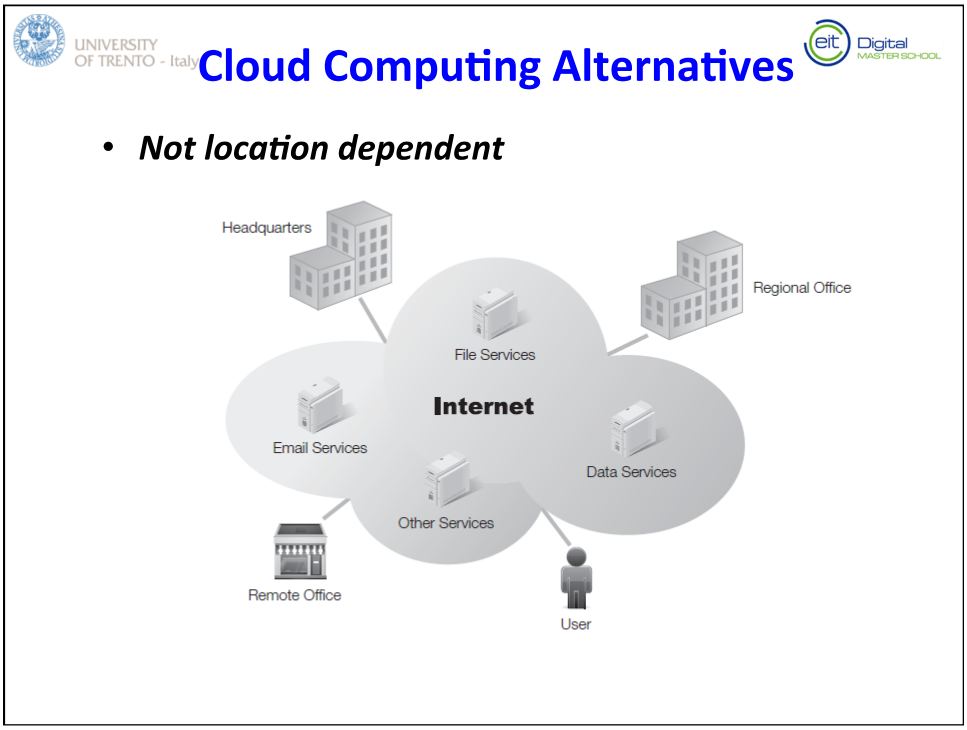
- Available building
- Electricity, running water, and restrooms
- No equipment or data
- May support a server environment

Hot Site

- Equipment and data necessary for business functions
- Able to assume operations within hours or minutes
- Personnel on location 24/7

Warm Site

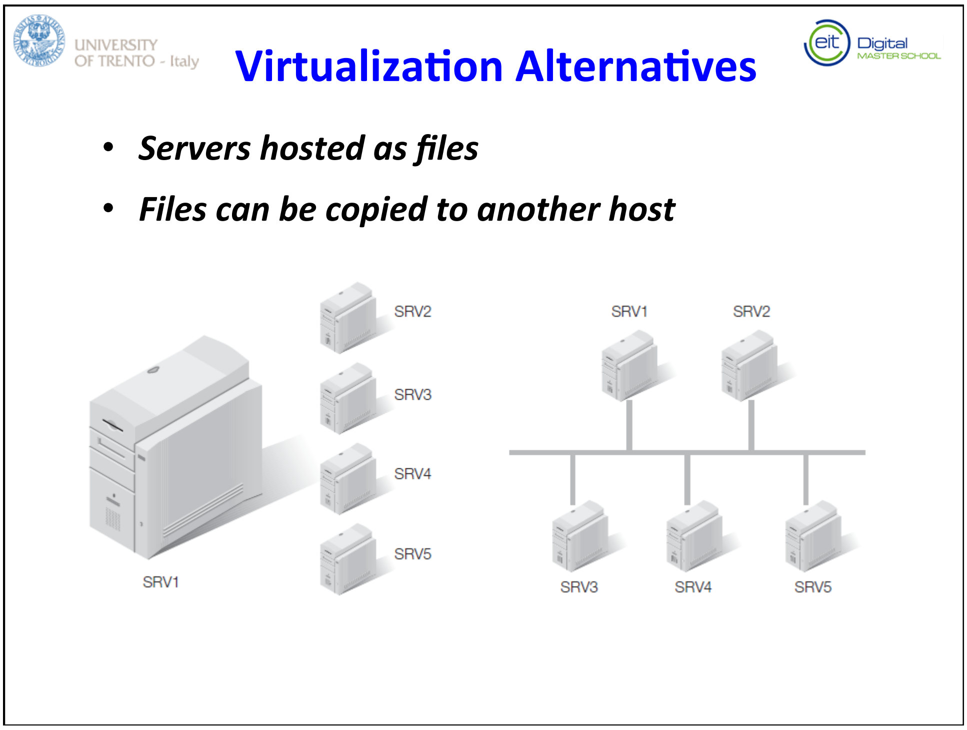
- Compromise between cold and hot sites
- Operational equipment
- Usually no data
- Capable of updating and going live



UNIVERSITY OF TRENTO - Italy

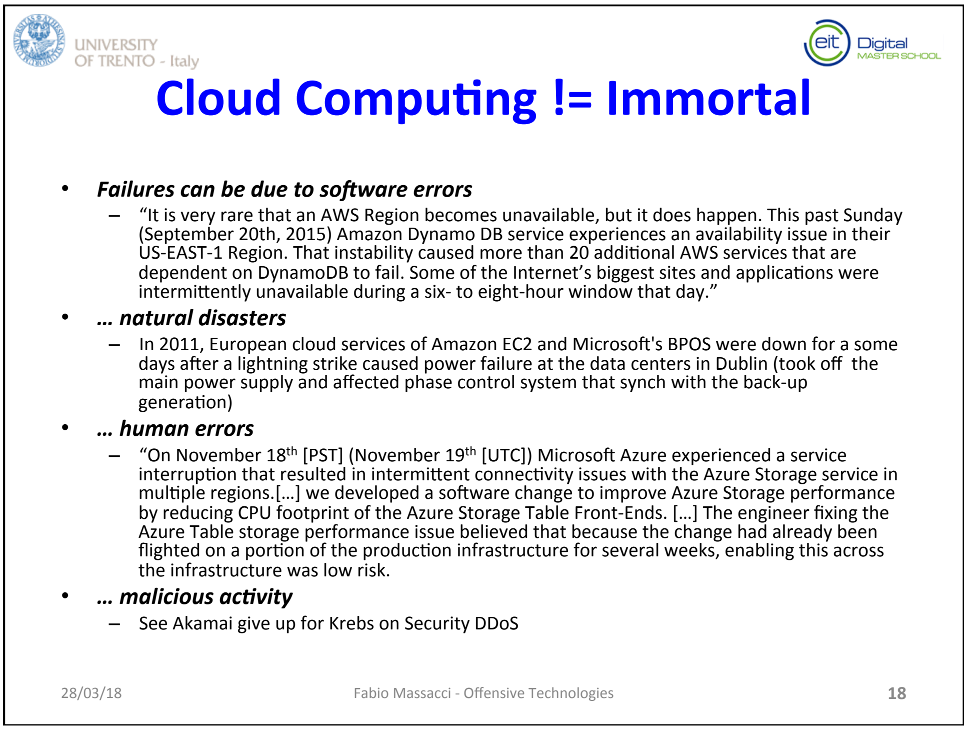
Cloud Computing Alternatives

- ***Not location dependent***



Virtualization Alternatives

- *Servers hosted as files*
- *Files can be copied to another host*



Cloud Computing != Immortal

- ***Failures can be due to software errors***
  - "It is very rare that an AWS Region becomes unavailable, but it does happen. This past Sunday (September 20th, 2015) Amazon Dynamo DB service experiences an availability issue in their US-EAST-1 Region. That instability caused more than 20 additional AWS services that are dependent on DynamoDB to fail. Some of the Internet's biggest sites and applications were intermittently unavailable during a six- to eight-hour window that day."
- ***… natural disasters***
  - In 2011, European cloud services of Amazon EC2 and Microsoft's BPOS were down for a some days after a lightning strike caused power failure at the data centers in Dublin (took off the main power supply and affected phase control system that synch with the back-up generation)
- ***… human errors***
  - "On November 18th [PST] (November 19th [UTC]) Microsoft Azure experienced a service interruption that resulted in intermittent connectivity issues with the Azure Storage service in multiple regions.[…] we developed a software change to improve Azure Storage performance by reducing CPU footprint of the Azure Storage Table Front-Ends. […] The engineer fixing the Azure Table storage performance issue believed that because the change had already been flighted on a portion of the production infrastructure for several weeks, enabling this across the infrastructure was low risk.
- ***… malicious activity***
  - See Akamai give up for Krebs on Security DDoS

BCP Best Practices

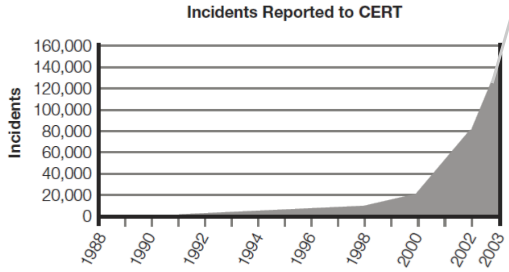
- ***Complete the BIA early***
- ***Exercise caution when returning functionality from alternate locations***
  - Restore least critical functions first
  - Review and update the BCP
- ***Test all individual pieces of the plan***
- ***Conduct test exercises of the plan***
  - Conduct live test of the plan

Conduct Live Test of Plan

- ***Doable for Cloud IT systems → Netflix Chaos Monkey***
  - "We have found that the best defense against major unexpected failures is to fail often. By frequently causing failures, we force our services to be built in a way that is more resilient. […]
  - Chaos Monkey is a service which runs in the Amazon Web Services (AWS) that seeks out Auto Scaling Groups (ASGs) and terminates instances (virtual machines) per group. […]
  - Within an ASG, Chaos Monkey will select an instance at random and terminate it.
  - The ASG should detect the instance termination and automatically bring up a new, identically configured, instance."
- ***Acceptable for Netflix, Gmail, Microsoft, etc.***
  - Consequence for Netflix if live tests actually fail?
    - People won't see "House of cards" tonight.
  - For Microsoft failure's
    - "We reverted the change globally within 30 minutes of the start of the issue […] a subset of Virtual Machines that required manual recovery"
- ***Close to impossible to do life test on a physical production systems***
  - Can't "revert", nor "manually restart" a crashed aircraft
  - Chernobyl Nuclear Disaster was an example of a test on a production system
  - Uberlingen Air disaster

Growth of (Malicious) Incidents

- ***Computer Incidents***
  - 1988 – one incident was news
  - 2003 – 137,529 incidents
  - 2013 – Off the chart



Growth of Incidents in Perspective

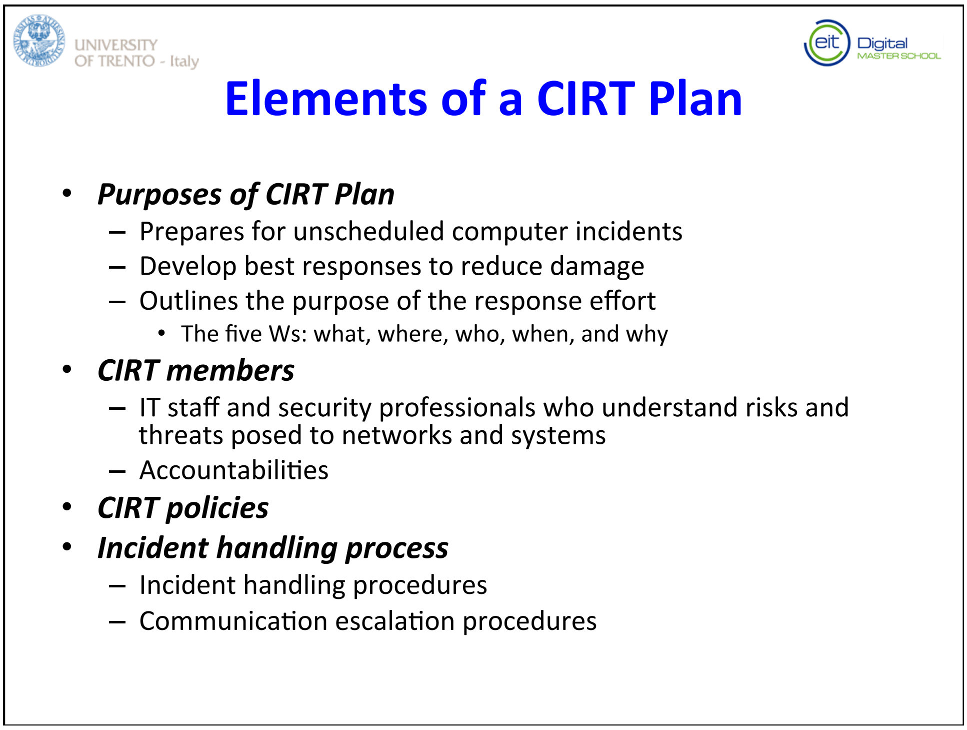
- ***Computer Incidents***
  - 1988 – one incident was news
  - 2003 – 137,529 incidents
  - 2013 – Off the chart
- ***BUT***
- ***Deaths in car accidents***
  - 1990 – 1.1 million
  - 2013 – 1.4 million

Computer Security Incident

- ***Violation, or imminent threat of a violation of a security policy or security practice***
- ***Examples***
  - Denial of service (DoS) attack
  - Malware code
  - Unauthorized access
  - Inappropriate usage
  - Multiple component

What Is a Computer Incident Response Team Plan?

- ***Computer incident response team (CIRT)***
  - A group of people that will respond to incidents
  - AND a technical infrastructure to support them (SOC = Security Operation Center)
- ***A CIRT plan:***
  - Is a formal document that outlines an organization's response to computer incidents
  - Formally defines a security incident
  - May designate the CIRT team

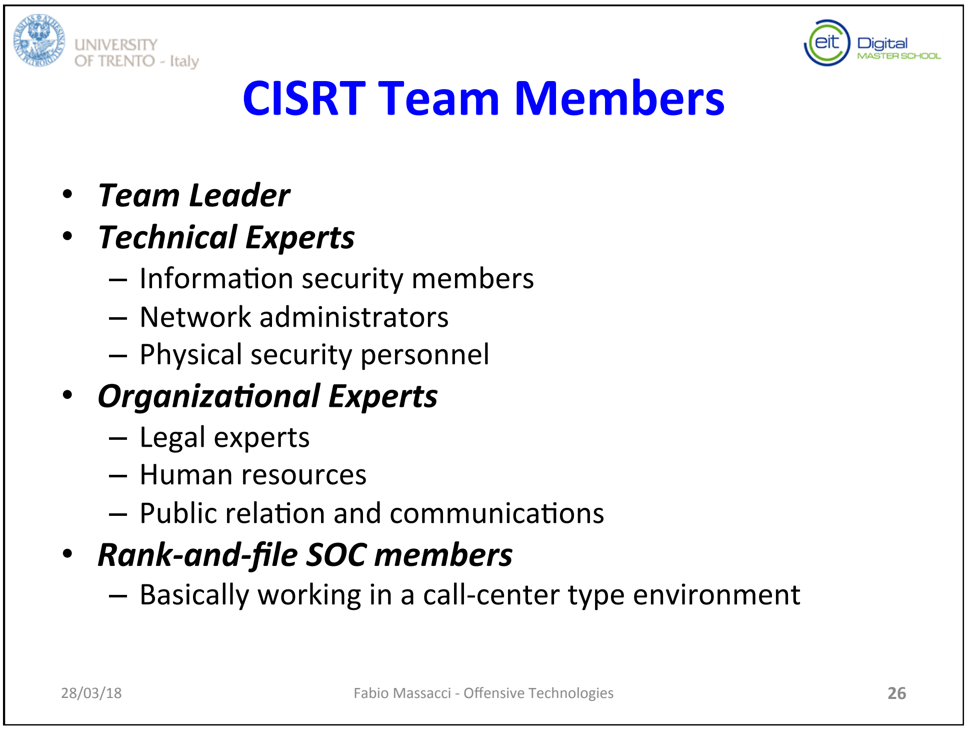


UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Elements of a CIRT Plan

- ***Purposes of CIRT Plan***
  - Prepares for unscheduled computer incidents
  - Develop best responses to reduce damage
  - Outlines the purpose of the response effort
    - The five Ws: what, where, who, when, and why
- ***CIRT members***
  - IT staff and security professionals who understand risks and threats posed to networks and systems
  - Accountabilities
- ***CIRT policies***
- ***Incident handling process***
  - Incident handling procedures
  - Communication escalation procedures

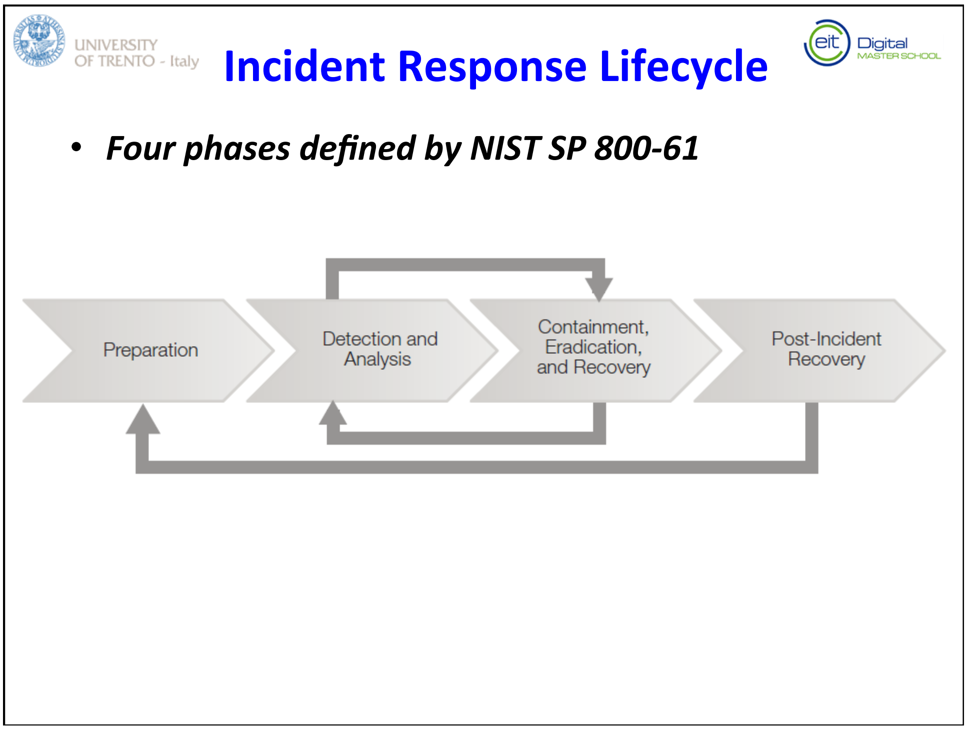


UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

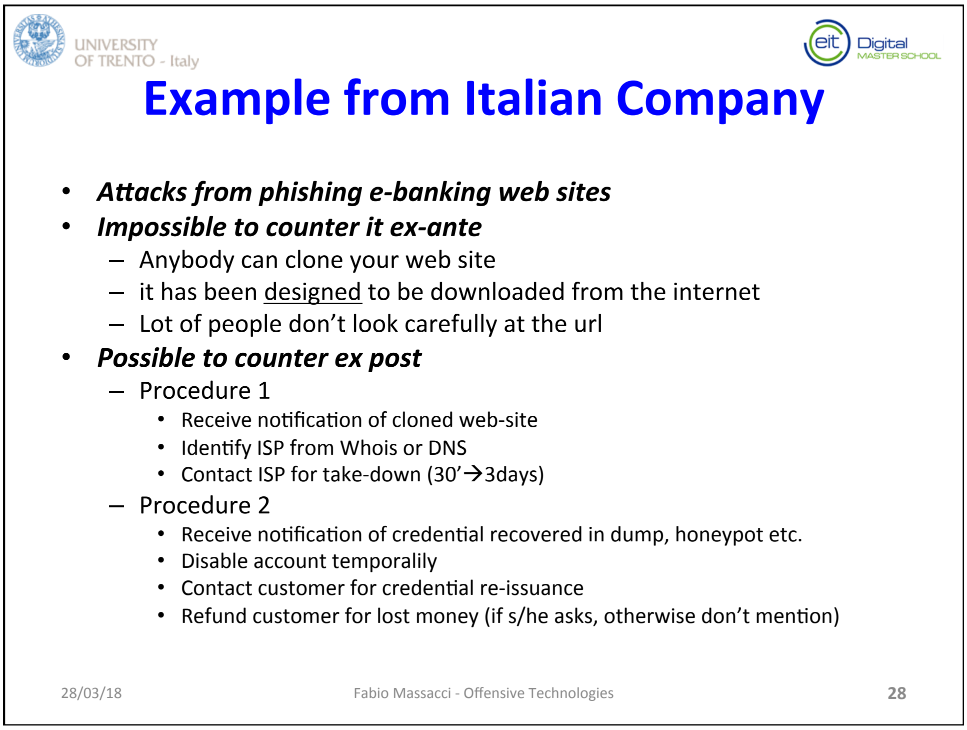
CISRT Team Members

- ***Team Leader***
- ***Technical Experts***
  - Information security members
  - Network administrators
  - Physical security personnel
- ***Organizational Experts***
  - Legal experts
  - Human resources
  - Public relation and communications
- ***Rank-and-file SOC members***
  - Basically working in a call-center type environment



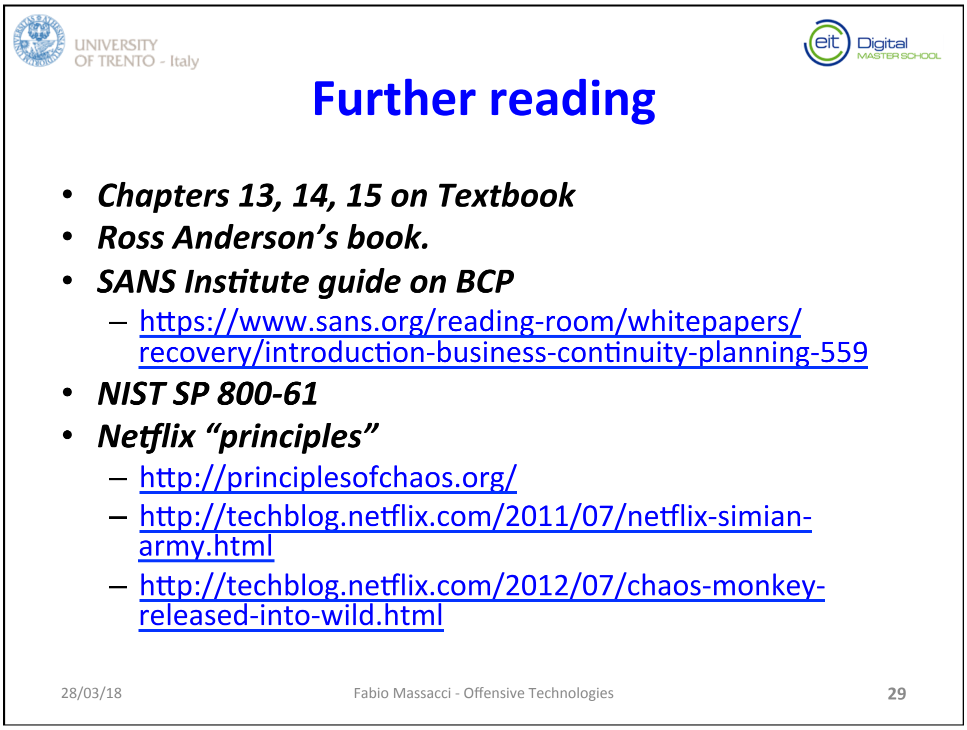
Incident Response Lifecycle

- ***Four phases defined by NIST SP 800-61***



Example from Italian Company

- ***Attacks from phishing e-banking web sites***
- ***Impossible to counter it ex-ante***
  - Anybody can clone your web site
  - it has been designed to be downloaded from the internet
  - Lot of people don’t look carefully at the url
- ***Possible to counter ex post***
  - Procedure 1
    - Receive notification of cloned web-site
    - Identify ISP from Whois or DNS
    - Contact ISP for take-down (30’→3days)
  - Procedure 2
    - Receive notification of credential recovered in dump, honeypot etc.
    - Disable account temporalily
    - Contact customer for credential re-issuance
    - Refund customer for lost money (if s/he asks, otherwise don’t mention)



Further reading

- *Chapters 13, 14, 15 on Textbook*
- *Ross Anderson's book.*
- *SANS Institute guide on BCP*
  - https://www.sans.org/reading-room/whitepapers/recovery/introduction-business-continuity-planning-559
- *NIST SP 800-61*
- *Netflix "principles"*
  - http://principlesofchaos.org/
  - http://techblog.netflix.com/2011/07/netflix-simian-army.html
  - http://techblog.netflix.com/2012/07/chaos-monkey-released-into-wild.html