TLD-OPS BCP/DR Playbook

Version 1.0.2

December 3rd, 2019

Table of Content

Contents

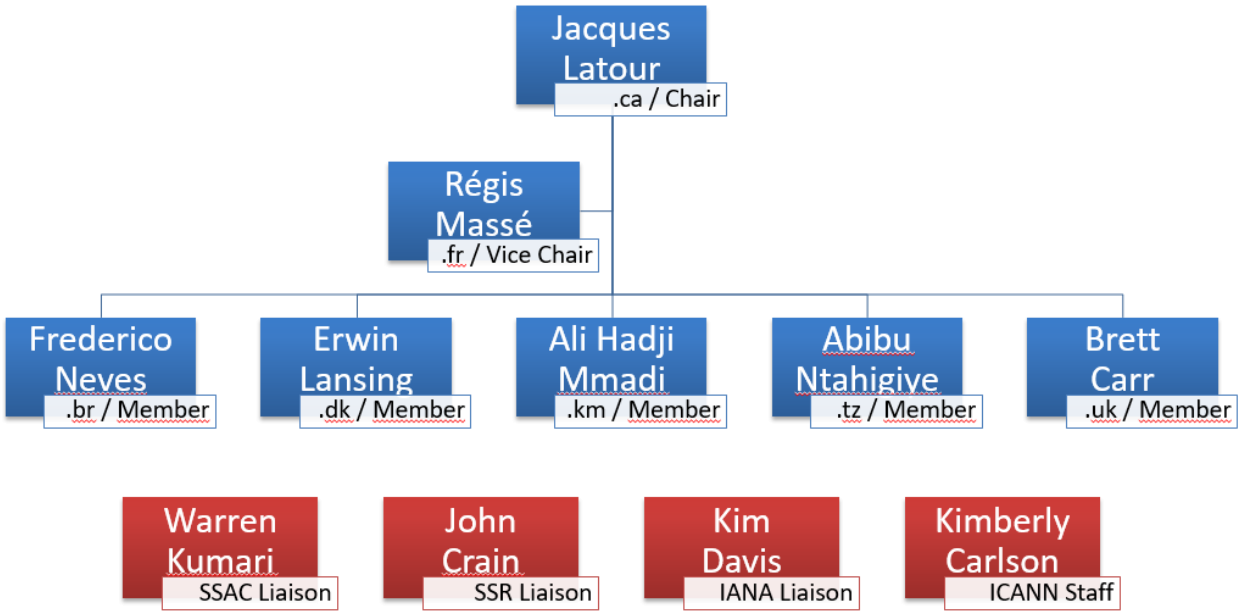
Introduction

About TLD-OPS: ccTLD Security and Stability Together

TLD-OPS is the incident response community for and by ccTLDs and brings together people who are responsible for the operational security and stability of their ccTLD. The goal of the TLD-OPS community is to enable ccTLD operators worldwide to detect and mitigate incidents that may affect the security and stability of ccTLD services, such as DDoS attacks, malware infections, and phishing attacks. The aim of TLD-OPS is to further extend members' existing incident response structures, processes, and tools and not to replace them. TLD-OPS is open to every ccTLD, irrespective of ccNSO membership.

About: https://ccnso.icann.org/en/resources/tld-ops-secure-communication.htm

Special thanks to Dirk Jumpertz, Security Manager from EURid for his outstanding contribution to this document and project.



TLD-OPS Standing Committee

How to use this document

This playbook aims to offer a hands-on guideline to whoever wants to implement a business continuity strategy within a smaller registry operator. Its target audience is oriented towards upper and/or middle management. It assumes that the registry operator has the commitment, sponsorship and mission from its supervising body (be it a Board, governmental representation or any other form) to develop resilience against disruptive events in the form of a business continuity plan.

As this document tries to be as practical as possible, it contains a number of practical example tables that can be copied and used in the different stages of the development and implementation.

It also contains some examples which could be used as templates or as inspiration to develop business continuity/disaster recovery plans.

Finally, the reader will find occasional “Action boxes” in the document which contain actionable suggestions and tips: a small description of an activity and by whom it should be done.

What is Business Continuity?

Business Continuity is the capability of an organization to continue delivery of products or services that are important to the ccTLD registry operator’s business and stakeholders at acceptable, predefined levels following a disruptive incident.

Note that Business Continuity does not necessarily focus on solely technical disruptive incidents. Any disruptive incident that affects the operational readiness of an organization can trigger the Business Continuity Plans. It is therefore important for an organization to understand what can impede the operational readiness.

Business continuity versus disaster recovery

Business continuity plans (BCP) and disaster recovery plans (DRP) are related but not interchangeable even though one will find similarities when looking for templates via Google e.g. The former consists of a plan of action focussing on delivering regular business during a crisis; the latter is a subset and involves procedures to restore vital systems in the shortest time possible that the business requires.

Differently said a Business Continuity Plan will contain references to a number of Disaster Recovery Plans. For the purpose of this document, we will develop Business Continuity Plans that contain a plan of action for a specific scenario.

How to achieve this goal?

By using some guidance of the ISO 22301 standard on Business Continuity, one can create a global framework that helps to create, managing and improving on the Business Continuity Plans.

As the operational mission of domain managers is mostly identical within the world of ccTLDs a common simplified approach can be used that focuses on practicality rather than complex, time-consuming and sometimes abstract techniques to develop the right business continuity plans.

Relation with the ISO/IEC 27001:2013 standard

The ISO 27001 standard focuses on Information Security which boils down to developing, implementing, monitoring and improving controls to maintain levels of Confidentiality, Integrity and Availability - abbreviated as CIA. For an IT service company, this shares quite some overlap with Business Continuity.

There is a difference though: where the ISO/IEC 27001 focuses on achieving the required C, I and A levels during normal operations and foresees necessary mitigation through technology and procedures; the ISO 22301 focuses on disruptive incidents that incapacitate the organization and foresees plans to act on the incidents.

To understand the difference between the ISMS (Information Security Management System) and the BCMS (Business Continuity Management System) some examples to illustrate might be useful:

- *Redundant storage with RAID protection and duplication is typically introduced to increase integrity and availability (ISO/IEC 27001).*
- *Fire drill exercises are organized to make sure casualties are minimal in case a real fire breaks out (ISO 22301).*
- *Antivirus endpoint protection is deployed to protect laptops, desktops and mobile devices from cyber threats (ISO/IEC 27001).*
- *Drilled procedures in case of a successful ransomware attack are part of the Business Continuity Plans on the other hand (ISO 22301).*

Scope (of this document)

This document serves as guidance in implementing the basis of Business Continuity and Disaster Recovery within a small registry operator.

It should help to answer the following questions:

- How to determine the business continuity scope?
- How to determine risks?
- How to embed Business Continuity in the company DNA?
- What is needed for an effective business continuity strategy?
- What are the Vital Materials?
- How to draft a business continuity plan or disaster recovery plan?
- How to do business continuity exercises?
- How to improve?

Normative references

This document is based on:

- ISO 22301:2012 – Societal Security – Business continuity management systems – Requirements.
- ISO 31000:2009 – Risk management – Principles and guidelines.
- ISO/IEC 27001:2013 - Information technology -- Security techniques -- Information security management systems -- Requirements

Terms and definitions

See ISO 22301:2012 for Terms and Definitions used throughout this document.

See RFC2119 to understand requirement levels.

Context of the organization

Even though most ccTLDs have a very similar service portfolio and mission, there is always a substantial difference that will give direction to the Business Continuity Strategy. In general, one could say though that the operational mission of most ccTLDs is to:

- manage the name server infrastructure for its TLD.

- manage the public services, essential to a ccTLD. More specifically, this would be a corporate website and an administrative lookup service like WHOIS or RDAP.
- manage some kind of registration services which allows direct or indirect registration of domain names. This can be a human interface like a website or a dedicated machine-to-machine interface like EPP.
- and last but not least, the registry will manage a number of corporate business support systems that might not have much external visibility, but are essential for the organization to function (e.g. email, intranet, fileserver, etc…)

The purpose of this first step is to understand who relies on the organization and therefore has certain expectations that need to be met during a disruptive incident and who the organization requires to fulfil its mission.

Understanding the organization and its context

A first high-level step to build an effective Business Continuity strategy is to understand thoroughly the business and its stakeholders. Stakeholders will have specific expectations, requirements and formulate obligations that need to be taken into account within the scope. Therefore, it is always a good exercise to list the stakeholders, describe who or what they are and finally review their expectations with regard to operational resilience and business continuity. This activity should preferably be done by management to capture the right input. The column “relevance to BC” captures the relation of the expectation with Business Continuity. Some expectations might not be related; while others might be considered very important. To that extent one can use HIGH, MEDIUM, LOW and N/A to indicate the relevance. Example: if an expectation is considered highly relevant to business continuity, it basically means that the stakeholder has high expectations - practically, a stakeholder might expect that “it ALWAYS works”, meaning the DNS is always up; then the relevance will be HIGH.

The following table is a non-exhaustive list with some **examples** that can be used to help in this exercise. In practice, it is advisable to first review & update the table and identify the stakeholders, name them (for the interviews), think about phrasing the expectations in short sentences and finally assess their relevance to business continuity.

Stakeholder	**Expectations**	**Relevance to BC**
Government	100% DNS availability Registry accuracy integrity Registry system availability Center of expertise in DNS Research and development in DNS Abuse of domain names	HIGH HIGH HIGH n/a n/a n/a

ICANN	IANA ccTLD registration	n/a
Board	100% DNS availability Registry accuracy integrity Corporate system availability	HIGH HIGH MEDIUM
General Public	DNS availability Domain registration availability	HIGH HIGH
c-CERTs	Security information Access to registrant data	LOW n/a
Employees	Corporate system availability	HIGH
Law Enforcement	Domain registration integrity	LOW
Registrars	Domain registration availability	MEDIUM
Registrants	Domain resolution availability Domain registration integrity	LOW LOW
Local ISP	Domain resolution DNSSEC support	HIGH n/a
Resolver Community	Access to the zone file	n/a

Table 1

Such a list will help in defining the high-level priorities on business continuity.

The Supply Chain

In a modern enterprise, organizations rely on a number of partners, suppliers, service providers, etc… these have obviously an important impact on the Business Continuity Strategy and therefore one should understand the organization's dependence on its supply chain. It is a valuable and indispensable exercise to list all suppliers that have an impact on the operational mission of the organization.

A practical way in creating the list is asking the finance department a list of all the suppliers, with a short description of what they actually supply. From that list, one can determine which suppliers have an actual impact on operational resilience. Example: a data centre provider will evidently have a HIGH relevance to the BC; a furniture provider like "Ikea" on the other hand will be less relevant.

Depending on the effect of an incident with the supplier we use a different impact label:

Impact	**Effect**
CRITICAL	Immediate
HIGH IMPACT	Within a week or 7 days
MEDIUM IMPACT	Within a month or 30 days
LOW IMPACT	Longer than a month or 30 days

Table 2

The following table is an **example** to aid in creating this supplier list:

Supplier (name)	**Description**	**Relevance to BC**	**Impact**
ISP	Internet Service Provider	HIGH	CRITICAL
Credit Card Processor	An entity that facilitates communication between the merchant and the cardholder's bank	MEDIUM - HIGH	HIGH IMPACT
Phone Company	Landline provider	MEDIUM	MEDIUM IMPACT
Postal Service	Postal (mail) provider	LOW	LOW
Power Company	Restoral of power		
Payroll Company	Pay employees		
Computer Service Company	Buy desktop for employees, servers for services		
Network/ISP Providers			
Mobile Network Operators			
Insurance company			

Table 3

Determining the scope of business continuity

Operational continuity as the cornerstone of the BC strategy

Operational continuity encompasses all activities that are required to run "business as usual". This implies supporting stakeholders like registrars, registrants and the general public from a technical, commercial and legal point of view. It also implies running all technical services to register and manage domain names, support the business and last but not least make sure the TLD namespace is available to all on the Internet.

A large part of the technological implications should be tackled by standard engineering practices and therefore Business Continuity focuses on assessing an inventory of disruptive incidents and their presumed and estimated outcome on the operational readiness. It defines mitigation through policies, procedures and where needed technology.

The scope of business continuity can, therefore, be summarized as

> The management of **preventive** and **corrective** measures through policies, procedures, tests and technology to guarantee **operational readiness and continuity** in the face of **disruptive** events both of a **technical** and **non-technical** nature.

Leadership

Developing and maintaining an effective and efficient Business Continuity strategy is an ongoing effort that requires support from the highest management. Therefore the best place to harbour and support initiatives related to business continuity is the management team or even the board.

Even though regular reviews are required to keep the plans up to date and relevant, management should also take the initiative to embed Business Continuity into all layers of operations (technology, engineering, purchase, operations, etc…).

ACTION: implement and monitor at least a yearly review cycle by the management team.

Planning

This section answers the question how to develop practical business continuity plans that take into account the threats & vulnerabilities that are relevant for the registry operator as well as the impact on the operational resilience of the organization.

We'll first start with the creation of a threat/hazard register which will help us in defining in which areas we need to address business continuity. Do note that some threats are difficult, if not impossible to mitigate or be prepared against. It is worthwhile to investigate the threat and assess strategic options. These might not translate in a Business Continuity Plan, but in strategic choices[1] in the longer term.

To translate the threats and hazard into actual risks we need to understand the impact on the operational readiness and resilience. A simplified risk assessment methodology can be used to help in determining which scenarios should be tackled. From this assessment, a number of scenarios will translate into tactical Business Continuity Plans while other scenarios will lead to a Business Continuity Strategy which can be used as input for the supervising authority and further strategic decisions.

Once it is clear which threats/hazards require an actual Business Continuity Plan, the plan can be created based on a generic template. This template should then be used as a guideline for all departments to prepare procedures where needed.

Develop a Threat/Hazard Register

The threat/hazard register is a valuable list of sources of disasters that could have a dramatic impact on the operational resilience of the organization. The following list of threats is based on the book Business Continuity Management (4th edition) - ISBN 978-1-931332-35-4 and expanded with recent emerging events.

When assessing these threats, an organization should estimate the likelihood of the event based on available statistical data. The probability of occurrence (likelihood) is scaled as follows:

1. Highly Likely: a yearly or more frequently recurring event
2. Likely: an event happening on average every three years
3. Rare: an event happening every ten years
4. Unlikely: an event happening once every 50 years or more
5. OoS: Out of Scope – these are not taken into account in the Business Continuity

Likelihood is not based on internal statistics but on relevant statistics for the region, country, business and environment[2]. It is important to underline that people have to score the likelihood (table 7 and 8) and impact (table 6) of the risks with the current security controls in place. Threats are based on statistics; without specific controls in place.

[1] A typical example might be Political Instability which can be extremely difficult to mitigate, yet as a ccTLD, it is important that this is taken into account in the overall Business Continuity Strategy.

[2] A typical example of weather related events like tornados might be very relevant to parts of the US, but completely irrelevant to other parts of the US.

Threat category	Threat	Applicable	Likelihood
Natural Disasters	Fire	☐	_____
	Flood	☐	_____
	Hurricane/tornado/typhoon	☐	_____
	Adverse weather	☐	_____
	Earthquake	☐	_____
	Landslide/avalanche	☐	_____
	Volcanic activity	☐	_____
	Tsunami	☐	_____
	Lightning strikes Subsidence	☐	_____
	Contamination	☐	_____
	Insect infestation	☐	_____
	Rodents	☐	_____
	_____	☐	_____
HR & Medical	Loss of key personnel	☐	_____
	Epidemic Illness	☐	_____
	Skills/staff shortage	☐	_____
	Family matters	☐	_____
	Theft	☐	_____
	Malicious damage (sabotage)	☐	_____
	Extortion	☐	_____
	_____	☐	_____
Cyber	DDOS	☐	_____
	Hackers	☐	_____
	Data loss	☐	_____
	Ransomware	☐	_____
	Cyberwar related activities	☐	_____
	_____	☐	_____
External	Recession	☐	_____
	Civil disobedience	☐	_____
	Terrorist activity	☐	_____
	War/invasion	☐	_____
	Political interference/policy changes	☐	_____
	Burglary	☐	_____
	Technology changes / relevance	☐	_____
	_____	☐	_____
Financial	Cash Flow/liquidity problems	☐	_____
	Starvation of capital	☐	_____
	Financial malfeasance	☐	_____
	Bad debt	☐	_____
	Interest risk	☐	_____
	Exchange rate risk	☐	_____
	Treasury exposure	☐	_____
		☐	

	_____		_____
Technology & Infrastructure	Network failure – global	☐	_____
	Electricity – Grid failures	☐	_____
	AC failures	☐	_____
	Data centre failures	☐	_____
	Component failures[3]	☐	_____
	_____	☐	_____
Supply Failure	Service level failure	☐	_____
	Quality defects	☐	_____
	Loss of supplied services	☐	_____
	Failed outsourcing/supply contract	☐	_____
	Out of stock situations	☐	_____
	Loss of other critical assets	☐	_____
	Vendor lock-in	☐	_____
	_____	☐	_____

Table 4

It stands without reason that a registry operator should focus on the threats that are relevant for his/her region and business context; the above non-exhaustive list serves as an example. It's also possible to start with a set of threats/hazards and expand later on.

ACTION: the BC coordinator or manager might want to focus on known threats and/or hazards and expand from there on in the regular review cycle.

Risk Assessment and Management

What is Risk? Risk types.

Risk, as defined in the ISO 31000 standard is: "the effect of uncertainty on objectives" which is a very generic high level and abstract definition. Translated to business continuity and operational resilience and continuity, risk would be "the effect of a disruptive event on the operational mission of a ccTLD registry operator".

If one is inclined into doing a formal yet simple risk assessment the following table can be used:

[3] Component failures is a generic umbrella to refer to malfunctioning computer systems, power supplies, computer memory, disks, etc… one can decide to put this into the scope of Business Continuity or assume this is mitigated in the design and architecture of the infrastructure by default (i.e. redundant power supplies, RAID disk systems, ECC memory in servers, etc…).

Risk	Description
Financial	The event causes direct and indirect costs to the organization. Depending on the financial stability of the organization, certain financial losses are acceptable.
Operational	The event hinders the organization in executing its operational mission (i.e. the Domain Name Services are interrupted).
Reputational	The event might cause reputational damage that has a direct or indirect impact on the operational mission.
Legal	The event causes legal challenges that can lead to penalties or even criminal convictions.
Governance	The event causes political fall-out and non-compliance which can lead to termination of a concession contract or political interference.
Human	The event causes physical harm to employees (or their families).

Table 5

Every risk has evidently different levels and depending on the level one can decide to take it under consideration of the business continuity plans. Some examples:

- a financial loss of 1M€ might lead to the factual bankruptcy of the registry operator.
- an event leading to the criminal conviction of individuals might not be acceptable to the registry operator.
- an event causing bodily harm to employees might not be acceptable.

The table is non-exhaustive and the registry operator can decide what to use at which levels. The following table illustrates five levels of risk per risk type. It is up to the registry operator to decide the applicability of these levels and the actual values.

Type	NULL or n/a	Low	Medium	High	Critical
Financial	the risk doesn't exist or is not applicable	< 1.000 USD	< 10.000 USD	< 100.000 USD	> 100.000 USD
Operational		impacts an individual	impacts a department	impacts the registry	impacts the public
Reputational		internal	user groups (ICANN, CENTR)	public	media / political

Legal		administrative penalty	fine < 10.000 USD	fine < 100.000 USD	fine > 100.000 USD, personal liability or criminal conviction
Governance[4]		board	local government	political scrutiny	termination of registry
Human		level is not used	level is not used	family of co-workers	personal injury

Table 6

It is advisable to color code the different levels as this can be used afterwards to create a visual heatmap of all the applicable risks versus the risks incurred.

Simple Risk Assessment / Business Impact Assessment

Adding the different risks as described above to the threat/hazard matrix gives a simple tool to look Business Impact.

Let's take an example to illustrate this. The scenario is DDOS attacks on the ccTLDs operational infrastructure (including, but not limited to, the domain name server for the .tld as well as the registration services; we assume the registry operator has a small infrastructural footprint where all services are combined and no anycast provider is utilized for the DNS).

Threat category	**Threat**	**Applicable (Y/N)**	**Likelihood**
Cyber	DDOS	YES	Highly Likely
Risks	**Level**		
Financial	MEDIUM	DDOS attack doesn't cause any direct costs as it doesn't cause any physical destruction of property. The biggest cost is people dealing with the incident. There is of course an indirect cost incurred as there are no domain names registered while under attack.	

[4] Governance risks are possibly the most difficult and at the same time the most specific types of risks. For some registries the risk might not even exist. This requires management to clearly define and describe how the registry depends on external influences.

Operational	CRITICAL	The entire .TLD is not available or intermittently available. This has a huge operational impact on the internet. Similarly other services like the corporate website, the public WHOIS and other registration services are impacted.
Reputational	HIGH / CRITICAL	The incident will be noted by anyone on the Internet.
Legal	HIGH	In the aftermath of the incident, registrants and registrars might file complaints on lost revenue. (This depends on the T&C of the registry as well as the jurisdiction of the registry.)
Governance	HIGH	As most ccTLDs can be considered Operators of Essential Services (to quote the EU NIS directive); it is safe to assume there will be quite some inquiries from the government.
Human	NULL	No employees will be directly or indirectly impacted with bodily harm by this event.
RTO	For the DNS is zero; the service should never be down. All other services that are impacted by the DDOS should be available within a business day.	
RPO	For the DNS: degradation of the services to 50% of the name server capacity is acceptable; all other services should be fully accessible, degradation of the capacity is acceptable up to 50%.	

Table 7

The RTO or Recovery Time Objective defines how quickly the service should be restored. This reflects the expectation of the stakeholders and/or legal or contractual obligations. Do note that different RTOs can be defined for one threat or hazard as this depends on the services impacted.

The RPO or Recovery Point Objective describes to what level the services should be restored. This can take many forms like reduced capacity (less nameservers available e.g., reduced capacity of a server e.g., etc…), delayed services, data restore up to a certain point, etc…

RTO and RPO should be purely based on business input and not be reliant on “what is possible” when the incident happens.

This assessment gives a good indication that the threat should be taken into account and the risk treatment is required.

Risk appetite and treatment

There are roughly 5 ways of dealing with risks:

1. Accept the risk (do nothing).
2. Avoid the risk (come up with an alternative plan).
3. Reduce the risk (change the equation).
4. Contain the risk (minimize the impact).
5. Transfer the risk (give it to someone else, insurance).

Business Continuity Plans are all about option 4, where through predefined actions the impact is countered and the operational mission is restored to a predefined level.

The outcome of the Business Impact Assessment on the other hand should also be taken into consideration as it might lead to preliminary steps (Step 3, reduce the risk) and actions to reduce the risk and attain the RTO and RPO.

Let's return to the previous example and investigate what can be done to reduce the risk to an acceptable level.

In this specific case, it's clear that the DNS has absolute priority, public services like the corporate website and the public WHOIS function are on a second place and last but not least are the registration services.

Threat category	**Threat**	**Applicable (Y/N)**	**Likelihood**
Cyber	DDOS	YES	Highly Likely
Risk Mitigation			
Accept the risk	not applicable		
Avoid the risk	impossible, DDOS attacks are initiated by unknown adversaries.		
Reduce the risk	the existing infrastructure will not be able to guarantee the expected RTO/RPO requirements. A possible solution is to utilize an anycasting solution for the DNS and/or scrubbing services for the other services		
Contain the risk	develop a DDOS Business Continuity Plan (using the ccNSO DDOS mitigation handbook as a reference) including additional technical measures (like temporary relocation of some services),		

	communication plan and a support plan
Transfer the risk	not applicable

Table 8

The risk treatment plan will then contain the different actions that are distilled from the above table. Some can be implemented immediately, others might require additional budget and further approval and planning.

Risk Treatment Plan

When doing the initial risk assessment/business impact assessment, a number of scenarios will lead to unacceptable levels of risk or the RTO/RPO expectations and requirements cannot be guaranteed at present.

This gap can be closed by specific actions to reduce the risks. These measures must be recorded and put in a plan, called a risk treatment plan. The risks treatment plan is not part of the business continuity plan, but exists in parallel. It consists of additional investments, re-engineering of existing services and/or infrastructure, outsourcing certain activities, etc...

The Business Continuity Plan

Before we can draft the plan, some terminology might need an explanation. As mentioned before the BCP serves as a guideline and a plan of action to manage a crisis when a specific disruptive event has taken place.

High level, a crisis is almost always handled in the same way:

1. assess the situation
2. contain the event
3. recover to predefined levels within the RTO (Recovery Time Objective) and RPO (Recovery Point Objective)
4. step down

Note that the end of a crisis, marked with the step down, doesn't imply that the organization has returned to the "before incident" situation. "Step down" means that the crisis team considers the crisis under control, the service has been restored, the organization can execute its operational mission. This doesn't imply that all damage has been repaired.

An example might further illustrate and clarify this: *during the weekend, vandals destroyed and pillaged the main registry office. IT equipment was stolen, furniture destroyed, basically the organization cannot work from the office due to damages and investigations going on. The BCP is activated and dictates that when the office is not accessible, telephones are rerouted to*

mobile devices, employees are informed to stay home and work from home until further notice (this implies that teleworking is not an issue). The crisis team handles initial contact with law enforcement, insurance and other parties and makes sure the above BCP is executed. Once this is done the service will be restored to an acceptable level and the organization can continue its operational mission. The crisis team assigns resources to further handle the case and bring the office back to its previous state. At that moment the crisis team steps down and resumes its normal operational role. Evidently in a small organization there will be overlap simply due to the limited resources available.

Vital Materials is a set of information (digital and/or physical) that is absolutely required to manage the incident. These can be contracts, contact information for specific services (e.g. network providers, scrubbing services, the landlord, authorities, etc…), logins and passwords, physical assets like keys, etc… don't forget to adequately protect this sensitive material while at the same time keep it accessible during a crisis.

The Business Continuity Plan: once the scenarios have been identified that have the highest risk, it's time to draft a plan. One could decide to write down a detailed plan with every single step to execute during a disaster. While this is perfectly possible, disasters tend to lead to unexpected side events which make it difficult to write every single step that needs to be done. From experience, an overall guideline reprising the essential steps during crisis handling is more usable. Such a plan can then be used during training, testing and simulation.

One should also look into the effect of the scenario. It makes no sense to write multiple BC plans that in the end might have different scenarios, but lead to the same plan. A typical example is an incident which makes the office unavailable/not accessible. Whatever the reason is (a fire, a strike, electrical outage, a flood, Black Friday), is not really relevant, the result is the same. This can then be translated into one BC plan.

The template below is compact and reprises all the above discussed steps to handle the disaster. It also helps in defining some preparationary tasks. **Do note that improvisation during a crisis is the worst possible outcome.** The template is in the end nothing but a cheat sheet to help the crisis team in dealing with the situation and be prepared.

BUSINESS CONTINUITY PLAN (TEMPLATE)			
Reference:	[REFERENCE]	Threat Type	Assets impacted
Scenario:	*Describes the conditions that triggered the Plan. This can be an event, a time, a specific condition, etc…*		
ACTIVATION:	*When is the plan activated? This can be immediately at detection or a number of hours after the incident took place.*		
RTO:	*Recovery Time Objective*		
RPO:	*Recovery Point Objective*		
Crisis Team:	*Who is the crisis team? Who will actually tackle the incident? Use names of employees, partners, suppliers to prevent ambiguity.*		
Priorities:	*What are the priorities? This should be interpreted as a sequential list.*		
Assessment:	*The initial stage of dealing with a disruptive incident is assessing the extent of the incident. Describe what factors should be taken into account.*		
Containment:	*Describe what the course of action is to prevent further worsening of the situation.*		
Recovery:	*Describe the course of action to restore minimal operational readiness, taking into account the priorities defined above.*		
Step down:	*Once the operations are recovered, the crisis team steps down and leaves instructions for further actions to return to the before the incident stage.*		

Communication:	*Define internal and external communication, including the message as well as the distribution list and including the means. Always start with the internal communication.*
Vital Materials:	*List of resources required to tackle the incident. This is part of the preparation phase. The plan doesn't contain the actual content, but is limited to references (it is the responsibility of the different department leads and/or partners to maintain this content, keep it up to date and accurate and portable where possible)*
Records:	*What records should be produced during and after the crisis. These records are useful for evidence gathering, lessons learned and a trace of the actual incident.*

Table 9

In annex are some examples of BC Plans.

Support

Resources

The initial effort to set up a business continuity (management) system can be quite time consuming, but the above methodology should make this practical and doable for a smaller organization.

Once the inventories and listings have been drafted, the effort becomes more sustainable as only yearly reviews are needed to update the plans taking into account the changing threat and hazard landscape, e.g. cyber attacks were mostly in the realm of science fiction in the early 2000's; today they should be seen as a clear and present danger.

In a small organization the best place to manage and guide the successful development of a business continuity plan is at the management level and the project should be given sufficient support and focus.

There's no real need to appoint a dedicated business continuity manager, in some cases the BC strategy might be even more effective when embedding this into the responsibilities of the entire organization.

Awareness

A successful Business Continuity Strategy requires awareness throughout the entire organization and understanding that it should be on anyone's radar.

Regular awareness sessions are therefore an absolute must.

Communication

As the template and example Business Continuity Plans show, communication (internal and external) plays a very important role in crisis management.

It's therefore quite important to:

1. decide which means of communication will be used. Example: telephone, texting, messaging, Twitter, email, etc…
2. prepare communication templates (improvised communication can really kill the credibility of an organization during a crisis).
3. pre-define and prepare to whom the communication should be sent, e.g. "our registrars" is not an actionable definition. A pointer to a list of email addresses that is kept up to date, is.
4. set-up priorities and schedules for the communication (e.g. Tweet an update every 60 minutes, send an email at the start and end of the incident).
5. evaluate the need for an external crisis communication consultant to help setting up the communication strategy and plans, but also to train people dealing with the press.

Operation

Once the BCP has been drafted; it should be embedded in day to day business and nominal operations. This means that Business Continuity must play a role in all engineering, business processes and workflows.

This implies that business continuity plays a role in different areas such as: procurement, legal, engineering, operations, communications.

Some examples to clarify this:

- some servers and network equipment are purchased. The request for proposal (RFP) that is sent to vendors mentions **redundant power supplies** and dual **network interface cards** for maximal redundancy.
- a service is **outsourced**, the RFP mentions explicitly the expected business continuity measures that are expected from the service provider.

BC exercises

It's fine to develop plans to cope with a specific disaster scenario, but without any test or drill, the plan remains a *paper tiger*.

Testing and drilling the BC plans is therefore a critical component in an effective Business Continuity Strategy. Just like firefighters train firefighting; the crisis team should spend some time in actually testing and drilling the plans.

There are two ways of doing this. There is the so-called Table Top eXercise or TTX and the actual controlled simulation.

Table Top eXercises (TTX)

These "paper" exercises are meant to review procedures and are extremely helpful to drill teams. They require relatively little preparation.

A TTX can be a role playing exercise where all involved parties sit around the table and everyone plays his and her role. **An independent "master of the ceremony"** will guide the team through the different steps of scenario, interspersed with occasional unexpected additional events.

A major disadvantage of the TTX is the difficulty to convey a sense of urgency and reality to the participants.

ACTION: it is essential that the entire organization goes through the BC plans at least once a year with a critical eye on feasibility. BC plans are living documents that will need to be adapted to a changing environment.

Simulations

Ideally Business Continuity Plans are tested against real life simulations. During these simulations, the response of the different teams or partners is checked to validate the effectiveness of the teams as well as the feasibility of the plans.

By drilling the different plans, the teams will be accustomed to what they need to do when the event actually happens.

Evidently it's not always easy to actually simulate the incident (e.g. power loss in the data center); but realistic scenarios can be proposed.

Some examples:

- ransomware outbreak. A user calls the helpdesk to ask what to do as the screen claims the laptop has been seized and some bitcoins are asked in exchange to unlock the computer. The purpose of this exercise is to test the response of the support team.
- office is not accessible due to rat infestation. Evidently there are no rats, but the purpose is to test the communication with employees.

Improvement

Essential to any effective Business Continuity Strategy is to review the plans, risk assessment, list of stakeholders, list of threats and hazards etc… at least once a year or if significant changes have taken place.

These changes are typically initiated by a number of actions:

- emerging legislation
- outsourcing
- mergers and acquisitions
- new services
- change of stakeholders
- emerging technologies
- change of the threat landscape
- an incident
- ...

Annex: Summary of Tasks

This annex services to summarize the different tasks described in the document. This can be used as a checklist to aid in implementation.

1. make an inventory of all **stakeholders** and their expectations, identify which expectations are relevant to business continuity (table 1)
2. make an inventory of all **suppliers**, describe what they supply and identify the relevance to the business continuity and the impact (table 3)
3. use table 4 to create a **threat and hazard register**, mark which are applicable and what the likelihood is
4. use table 5 to identify which **risks** are applicable to the organization; use table 6 to define the different levels per risk
5. take the threat and hazard register (table 4) and copy the applicable threats and hazards in the **business impact assessment** (table 7). One can summarize all these tables in a heatmap where the levels of risk are color coded as shown in the example below:

Threat Category	**Threat**	**Financial**	**Operational**	**Reputational**	**Legal**	**Governance**	**Human**
Cyber	DDOS	Medium	Critical	High/ Critical	High	High	Null

6. expand table 7 that was used for the simple business impact assessment and add **risk treatment** to it (table 8). There will be a number of threats that result in an unacceptable risk if not mitigated; hence from the risk treatment results a risk treatment plan that contains actions to reduce the risk. This doesn't imply that risks are then neutralized, it does imply that the risks are reduced.
7. Create the **Business Continuity Plans** using table 9 as a template for those threats and hazards that are deemed a real threat with a high impact to the organization.

Annex: Example Business Continuity Plan

BUSINESS CONTINUITY PLAN (TEMPLATE)			
Reference:	[REFERENCE]	Threat Type	Assets impacted
Scenario:	*Describes the conditions that triggered the Plan. This can be an event, a time, a specific condition, etc…*		
ACTIVATION:	*When is the plan activated? This can be immediately at detection or a number of hours after the incident took place.*		
RTO:	*Recovery Time Objective*		
RPO:	*Recovery Point Objective*		
Crisis Team:	*Who is the crisis team? Who will actually tackle the incident? Use names of employees, partners, suppliers to prevent ambiguity.*		
Priorities:	*What are the priorities? This should be interpreted as a sequential list.*		
Assessment:	*The initial stage of dealing with an disruptive incident is assessing the extent of the incident. Describe what factors should be taken into account.*		
Containment:	*Describe what the course of action is to prevent further worsening of the situation.*		
Recovery:	*Describe the course of action to restore minimal operational readiness, taking into account the priorities defined above.*		

Step down:	*Once the operations are recovered, the crisis team steps down and leaves instructions for further actions to return to the before the incident stage.*
Communication:	*Define internal and external communication, including the message as well as the distribution list and including the means. Always start with the internal communication.*
Vital Materials:	*List of resources required to tackle the incident. This is part of the preparation phase. The plan doesn't contain the actual content, but is limited to references (it is the responsibility of the different department leads and/or partners to maintain this content, keep it up to date and accurate and portable where possible)*
Records:	*What records should be produced during and after the crisis. These records are useful for evidence gathering, lessons learned and a trace of the actual incident.*

CYBER: HACK

BUSINESS CONTINUITY PLAN			
Reference:	BCP-xxx.yy	CYBER: HACK	Global
Scenario:	Evidence shows that the registry's infrastructure was hacked and compromised. An alien actor has installed software, created accounts, remote access tools, etc… to infiltrate the registry. Potentially (sensitive) data was exfiltrated. .		
ACTIVATION:	IMMEDIATELY AT THE DETECTION		
RTO:	24 hrs		
RPO:	Data Loss of 24 hrs.		
Crisis Team:	Legal Mgr. - +CC 123 55 88 - ivan.horvat@registry.tld Tech. Mgr – +CC 123 44 55 – juan.perez@registry.tld BC Mgr – +CC 123 33 66 – jane.doe@registry.tld Gen. Mgr - +CC 123 56 44 - yamado.toro@registry.tld		
Priorities:	Protect availability and integrity of the name servers and the .tld zone. If needed isolate the name server infrastructure. Isolate the hacked systems. Collect evidence.		
Assessment:	If proof is found that data was leaked, activate also the BCP for data breach. Assess and make an inventory what systems are compromised. Which services are impacted? Is the DNS impacted, the registration platform, internal systems, the website? Double check the name server infrastructure. Does the hacker have a permanent foothold? Is the hacker present at the moment of detection?		

	Is external help needed from a companies specialized in cyber incidents (is there evidence of state actors)?
Containment:	Make sure the name server infrastructure is protected and isolate the name servers from the impacted area. Disable or shut down impacted systems. Do not try to repair or fix compromised systems or fight the intruder. Concentrate on isolating the compromised systems. Try to collect evidence; do not tamper with evidence
Recovery:	Systems impacted should be rebuilt and redeployed. If end user equipment is compromised, new systems are deployed.
Step down:	Once the compromised systems have been isolated and shut down and services are restored using rebuild and redeployed systems; the crisis team assigns a team to handle the following activities: 1. Contacting law enforcement and file a complaint. 2. Make sure compromised systems are stored securely and log files are set aside as evidence. Analyze the integrity of the core database (are there traces of changes?).
Communication:	Internal communication only Initial communication to all that our systems have been compromised and that we are isolating the compromised systems. Stress that further communication to the outside world will be handled by Comm Mgr, Legal Mgr directly. External communication: Inform stakeholders (board, authorities) Inform registrars if systems are being taken down (i.e. website, whois, EPP) and inform them of the further steps being taken. Inform law enforcement.
Vital Materials:	Documentation of the infrastructure and set-up. Password vaults to access different systems. Deployment and staging infrastructure to deploy new infrastructure.

	Distribution lists for communication (registrars, employees)
Records:	Create a record of the incident, what was discovered, what actions have been done, what evidence was collected. Do this during the crisis handling and not posteriori.

EXTERNAL: TERRORIST ATTACK

BUSINESS CONTINUITY PLAN			
Reference:	BCP-xxx.yy	EXTERNAL: TERRORIST ATTACK	Office
Scenario:	A terrorist attack occurred close to the corporate office(s) of the registry. Close means either the same city or within a radius of 25 km. This plan is applicable 24/7.		
ACTIVATION:	IMMEDIATELY		
RTO:	Undefined		
RPO:	Undefined		
Crisis Team:	Office responsible - +CC 123 44 55 - jan.modaal@registry.tld HR Mgr - +CC 123 66 23 - maija.meikalainen@registry.tld BC Mgr – +CC 123 33 66 – jane.doe@registry.tld Gen. Mgr - +CC 123 56 44 - yamado.toro@registry.tld		
Priorities:	Safety of the employees.		
Assessment:	Depending on the gravity of the attack, the consequences can be problematic (lock-down public transport, SWAT teams deployed, etc…). First and foremost, employees and their families must be safe. As the registry supports working from home, co-workers should not stay in, nor come to the office.		
Containment:	If the situation permits, the office will be closed immediately and employees are sent home. If the attack is too close to the office, employees are advised to stay put and follow the instructions of law enforcement and governmental sources.		

Recovery:	The Office Responsible will check that all employees are informed and accounted for. He/she will inform all employees that the office is closed and off limits until further notice. The Office Responsible will report the situation to the HR Manager or the BC Manager. The HR Manager or BC Manager will inform the appropriate departments and managers to take over activities where applicable
Step down:	The Office Responsible will follow instructions from law enforcement and official sources and inform employees when the office is re-opened.
Communication:	Internal communication only Initial communication verbally or via texting (SMS) by the Office Responsible to employees affected. Follow-up communication via email by Office Responsible, HR or BC Manager.
Vital Materials:	Employee list with phone numbers and email addresses.
Records:	Employee record that all co-workers have been informed and are accounted for.

CYBER: RANSOMWARE

BUSINESS CONTINUITY PLAN			
Reference:	BCP-xxx.yy	CYBER: RANSOMWARE	Office & End user equipment
Scenario:	A ransomware infection made a limited number of MS Windows laptops unusable and locked down. The infection can be localized in one office or is spreading through the organization.		
ACTIVATION:	IMMEDIATELY AT THE DETECTION		
RTO:	Within a working day.		
RPO:	Data loss of one working day.		
Crisis Team:	Tech. Mgr – +CC 123 44 55 – juan.perez@registry.tld BC Mgr – +CC 123 33 66 – jane.doe@registry.tld Gen. Mgr - +CC 123 56 44 - yamado.toro@registry.tld		
Priorities:	Protect availability and integrity of the Windows Server infrastructure. Isolate the infected systems. Re-stage the infected systems.		
Assessment:	Is the infection spreading? Who was/is patient zero? Can we isolate the infection?		
Containment:	Isolate the infected machines (i.e. shutting down network links to the data center); Shutdown non-infected systems either remote or, if this seems impossible, have users shut down their systems.		
Recovery:	Infected systems must be considered as lost and will have to be reinstalled. Potentially some employees might be offline for a few days.		

Step down:	The crisis team assigns a team to: 1. Identify the ransomware and check for signatures or other methods of detection; 2. Identify the initial strain… how was patient zero infected? 3. Create isolated network environments (wired and wireless) where the infection took place; non-infected systems should be started up and double checked if indeed they were not infected by the malware; 4. Create a plan to reinstall laptops that were infected. For remote offices this can be a problem and might need sending an onsite engineer. 5. File a formal complaint with law enforcement and/or other authorities depending on legal obligations / recommendations.
Communication:	<u>Internal communication only</u> Inform all employees of the outbreak of the ransomware and instruct them to immediately shut down their (Windows) laptops (use email, phone and messaging).
Vital Materials:	Documentation of the infrastructure and set-up. Password vaults to access different systems. Distribution lists for communication (employees).
Records:	Create a record of the incident, what was discovered, what actions have been done, what evidence was collected. Do this during the crisis handling and **not** posteriori.

Annex: The Workshop

Timeline of the workshop

	Description	Timing in min	Who
1	Presentation of the handbook - Distribute the DR/BCP Plan document	45	
2	Q&A on the handbook	15	
3	Fill in the forms - BIA - BCP - based on your own ccTLD - Distribute the DR/BCP template	45	
4	Discuss the result of the form	30	
5	Set up the teams (max of 5 teams) - Distribute cards, OK Registry and Cyber Hack BCP Plan	5	
6	Get familiar with the cards	10	
7	5 rounds of actual simulation exercise (TTX)	60	
8	Debrief of the exercise	30	

(240 minutes)

Presentation & fill in the forms exercise

Do a 45 min presentation + 15 min Q&A about the document to highlight the main topics.

During 45 minutes we let the participants

1. Make a list of stakeholders and write down their expectations
2. Review the threat register - which are applicable?
3. What risks are important to the organization and identify the levels.
4. Select a threat and do a Business Impact Assessment (BIA) on it
5. Based on that threat, define a Business Continuity Plan (BCP) ; list the elements of the Vital Materials

Stakeholder list

The stakeholders in this list are just examples. Feel free to add stakeholders that have not been mentioned and you believe are relevant. Relevance to BC: HIGH, MEDIUM, LOW, n/a

Stakeholder	Expectations	Relevance to BC
Government	_____ _____ _____	_____ _____ _____
ICANN	_____ _____ _____	_____ _____ _____
Board	_____ _____ _____	_____ _____ _____
General Public	_____ _____ _____	_____ _____ _____
Law Enforcement	_____ _____ _____	_____ _____ _____
Registrars	_____ _____ _____	_____ _____ _____
Registrants	_____ _____ _____	_____ _____ _____
	_____ _____ _____	_____ _____ _____
	_____ _____ _____	_____ _____ _____

Threat register

Check which threats are applicable and what the likelihood is based on statistical information.

Threat category	Threat	Applicable (Y/N)	Likelihood
Natural Disasters	Fire Flood Hurricane/tornado/typhoon Adverse weather Earthquake Landslide/avalanche Volcanic activity Tsunami Lightning strikes Subsidence Contamination Insect infestation Rodents _____	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐	_____ _____ _____ _____ _____ _____ _____ _____ _____ _____ _____ _____ _____
HR & Medical	Loss of key personnel Epidemic Illness Skills/staff shortage Family matters Theft Malicious damage (sabotage) Extortion _____	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐	_____ _____ _____ _____ _____ _____ _____ _____
Cyber	DDOS Hackers Data loss Ransomware Cyberwar related activities _____	☐ ☐ ☐ ☐ ☐ ☐	_____ _____ _____ _____ _____ _____
External	Recession Civil disobedience Terrorist activity War/invasion Political interference/policy changes Burglary Technology changes / relevance _____	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐	_____ _____ _____ _____ _____ _____ _____ _____
Financial	Cash Flow/liquidity problems Starvation of capital Financial malfeasance	☐ ☐ ☐ ☐	_____ _____ _____

	Bad debt Interest risk Exchange rate risk Treasury exposure _____	☐ ☐ ☐ ☐	_____ _____ _____ _____ _____
Technology & Infrastructure	Network failure – global Electricity – Grid failures AC failures Data centre failures Component failures[5] _____	☐ ☐ ☐ ☐ ☐ ☐	_____ _____ _____ _____ _____ _____
Supply Failure	Service level failure Quality defects Loss of supplied services Failed outsourcing/supply contract Out of stock situations Loss of other critical assets Vendor lock-in _____	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐	_____ _____ _____ _____ _____ _____ _____ _____

Likelihood:

1. Highly Likely: a yearly or more frequently recurring event
2. Likely: an event happening on average every three years
3. Rare: an event happening every ten years
4. Unlikely: an event happening once every 50 years or more
5. OoS: Out of Scope – these are not taken into account in the Business Continuity

[5] Component failures is a generic umbrella to refer to malfunctioning computer systems, power supplies, computer memory, disks, etc… one can decide to put this into the scope of Business Continuity or assume this is mitigated in the design and architecture of the infrastructure by default (i.e. redundant power supplies, RAID disk systems, ECC memory in servers, etc…).

Risk matrix

Type	NULL or n/a	Low	Medium	High	Critical
Financial	the risk doesn't exist or is not applicable				
Operational					
Reputational					
Legal					
Governance[6]					
Human					

[6] Governance risks are possibly the most difficult and at the same time the most specific types of risks. For some registries the risk might not even exist. This requires management to clearly define and describe how the registry depends on external influences.

Business impact assessment

Take one of the threats defined in the threat register that has a clear impact on business continuity and assess the impact on the different risks based on the risk matrix. The likelihood is reprised from the threat register.

Likelihood:

1. Highly Likely: a yearly or more frequently recurring event
2. Likely: an event happening on average every three years
3. Rare: an event happening every ten years
4. Unlikely: an event happening once every 50 years or more
5. OoS: Out of Scope – these are not taken into account in the Business Continuity

The RTO (Recovery Time Objective or how fast must the business be back after interruption) and RPO (what amount of data loss can we accept) are defined by the business (this might be a contractual, legal, governance requirement), it should not take into account what is technical possible or not possible.

Threat category	**Threat**	**Applicable (Y/N)**	**Likelihood**
		Y	
Risks	**Level**	**Motivation / description / explanation**	
Financial			
Operational			
Reputational			
Legal			

Governance		
Human		
RTO		
RPO		
Risk Mitigation	“n/a” or describe plans to mitigate the risk	
Accept the risk		
Avoid the risk		
Reduce the risk		
Contain the risk		
Transfer the risk		

Business continuity plan

BUSINESS CONTINUITY PLAN (TEMPLATE)			
Reference:	[REFERENCE]	Threat Type	Assets impacted
Scenario:	*Describes the conditions that triggered the Plan. This can be an event, a time, a specific condition, etc…*		
ACTIVATION:	*When is the plan activated? This can be immediately at detection or a number of hours after the incident took place.*		
RTO:	*Recovery Time Objective*		
RPO:	*Recovery Point Objective*		
Crisis Team:	*Who is the crisis team? Who will actually tackle the incident? Use names of employees, partners, suppliers to prevent ambiguity.*		
Priorities:	*What are the priorities? This should be interpreted as a sequential list.*		
Assessment:	*The initial stage of dealing with a disruptive incident is assessing the extent of the incident. Describe what factors should be taken into account.*		
Containment:	*Describe what the course of action is to prevent further worsening of the situation.*		
Recovery:	*Describe the course of action to restore minimal operational readiness, taking into account the priorities defined above.*		
Step down:	*Once the operations are recovered, the crisis team steps down and leaves instructions for further actions to return to the before the incident stage.*		

Communication:	*Define internal and external communication, including the message as well as the distribution list and including the means. Always start with the internal communication.*
Vital Materials:	*List of resources required to tackle the incident. This is part of the preparation phase. The plan doesn't contain the actual content, but is limited to references (it is the responsibility of the different department leads and/or partners to maintain this content, keep it up to date and accurate and portable where possible)*
Records:	*What records should be produced during and after the crisis. These records are useful for evidence gathering, lessons learned and a trace of the actual incident.*

Business continuity plan

BUSINESS CONTINUITY PLAN (TEMPLATE)			
Reference:	[REFERENCE]	Threat Type	Assets impacted
Scenario:			
ACTIVATION:			
RTO:			
RPO:			
Crisis Team:			
Priorities:			
Assessment:			
Containment:			
Recovery:			
Step down:			

Communication:	
Vital Materials:	
Records:	

Description of the simulation exercise (TTX)

The exercise is completely scripted and consists of 5 rounds of 10 minutes each. At the start of every round, the team is given input and must react on the input given using the appropriate Business Continuity Plan.

To facilitate this, a set of cards is distributed among each team. These cards contain practical actions that are executed as reaction on the input received at the start of the round.

Participant can select up to 3 actions (cards) per round which are set aside for later discussion. Cards are grouped in 4 categories: TECHNICAL; LEGAL; GOVERNANCE; COMMUNICATION, which basically represent the technical department, the legal department, the general management, the communication department.

During a round additional information can be injected in the exercise; this additional information should be processed by the team and can lead to a change of action.

After 5 rounds the cards are collected and discussed on a number of topics to collect feedback of the participant.

Description of the Registry

You are employed at "**OK registry**", the registry operator for the .ok ccTLD. OK, also known as Old Kontry, is a small European country with approximately 50k inhabitants. Because of its liberal policies, the .ok top level domain is quite popular and has 372.304 domain names registered as of November 1st 2019. .ok domain names are sold through a worldwide network of approximately 250 registrars.

Old Kontry is a unitary parliamentary constitutional monarchy.

Old Kontry is not part of the EU.

The registry is located in the capital and is part of the "**University of OK**", but operated independent (management, financial and technical); the university is the overseeing authority though.

For its backend services, it utilizes the MegaRyCorp. Inc., a DE registry service provider specialized in backend services for registries. 1 US anycast provider is responsible for the DNS services, but the registry has 3 older unicast name servers running from the university network.

For its web presence (corporate website, social media, etc…) the registry relies heavily on a local creative, data and technology agency, part of an international group.

Besides the hidden master name server and the authoritative name servers, the registry runs an EPP server, a WHOIS server and a registrar extranet which has the same features as the EPP and some more.

Because of its popularity and importance to the local economy the **OK government** has adopted legislation over the last few years that are in line with the European GDPR on personal data protection and the NIS directive on the protection of critical infrastructure and operators of essential services. It also assigned the Ministry of Telecommunications as the overseeing compliance and policy authority.

"**OK registry**" is a small organization with 7 people working directly for the registry. It can rely for IT support for laptops/desktops/email/etc… on the university.

It employs 3 engineers (1 developer, 1 sysadmin, 1 network engineer) who take care of the registrar webportal, monitoring, legacy name servers, firewalls, (W)LAN, registrar support and technical reporting.

There's a General Manager, Sales & Marketing Manager, Finance Manager and a Legal Manager; the technical team reports directly to the general manager. Business continuity management falls under the responsibility of the legal manager.

BCP plan for CYBER: HACK

BUSINESS CONTINUITY PLAN			
Reference:	BCP-101.01	CYBER: HACK	Global
Scenario:	Evidence shows that the registry's infrastructure was hacked and compromised. An alien actor has installed software, created accounts, remote access tools, etc… to infiltrate the registry. Potentially (sensitive) data was exfiltrated.		
ACTIVATION:	IMMEDIATELY AT THE DETECTION		
RTO:	24 hrs		
RPO:	Data Loss of 24 hrs.		
Crisis Team:	Legal Mgr. - +CC 123 55 88 - ivan.horvat@registry.tld Tech. Mgr – +CC 123 44 55 – juan.perez@registry.tld BC Mgr – +CC 123 33 66 – jane.doe@registry.tld Gen. Mgr - +CC 123 56 44 - yamado.toro@registry.tld		
Priorities:	Protect availability and integrity of the name servers and the .ok zone. If needed isolate the name server infrastructure. Isolate the hacked systems. Collect evidence.		
Assessment:	Assess and make an inventory what systems are compromised. Which services are impacted? Is the DNS impacted, the registration platform, internal systems, the website? Double check the name server infrastructure & service. Does the hacker have a permanent foothold? Is the hacker present at the moment of detection? Is external help needed from a companies specialized in cyber incidents (is there evidence of state actors)? Has data leaked and if so what type of data has leaked? What is the impact of the leaked data?		

Containment:	Make sure the name server infrastructure is protected and isolate the name servers from the impacted area. Disable or shut down impacted systems. Do not try to repair or fix compromised systems or fight the intruder. Concentrate on isolating the compromised systems. Try to collect evidence; do not tamper with evidence
Recovery:	Systems impacted should be rebuilt and redeployed. If end user equipment is compromised, new systems are deployed.
Step down:	Once the compromised systems have been isolated and shut down and services are restored using rebuild and redeployed systems; the crisis team assigns a team to handle the following activities: 1. Contacting law enforcement and file a complaint. 2. Make sure compromised systems are stored securely and log files are set aside as evidence. Analyze the integrity of the core database (are there traces of changes?).
Communication:	**Internal communication:** Initial communication to all that our systems have been compromised and that we are isolating the compromised systems. Stress that further communication to the outside world will be handled by Sales & Marketing Mgr. or the Legal Mgr. directly. **External communication:** Inform stakeholders (university board, authorities) Inform registrars if systems are being taken down (i.e. website, whois, EPP) and inform them of the further steps being taken. Inform law enforcement. Publish on regular basis progress on Social Media accounts and the public website.
Vital Materials:	Documentation of the infrastructure and set-up. Password vaults to access different systems. Deployment and staging infrastructure to deploy new infrastructure. Distribution lists for communication (registrars, employees, stakeholders)
Records:	Create a record of the incident, what was discovered, what actions have been done, what evidence was collected. Do this during the crisis handling and not posteriori.

Scenario of the exercise

ROUND 1: input FRI, 05:00 PM

- a security researcher contacts the general manager of the registry operator that he found evidence on pastebin of an excerpt of a database that seems to point to the registry's extranet used by their registrars.
- the researcher checked the hashed passwords on pastebin and managed to quite easily "crack" some of the passwords. As expected "password123" is quite common. He confirms that he logged on to the registrar extranet at some specific times (he gives those times to the manager).
- the pastebin is still online and the researcher also found some evidence that someone is selling the credentials on the dark web.
- he believes there is sufficient evidence to assume someone hacked the registry and that the malicious actor has started to cash in on his handiwork.

This is the initial information received by the registry. How will the manager react, what will he/she do? From here the manager must be fed with some additional information depending on his course of action. Remember to keep an eye on the clock. The participants have only 15 minutes per round.

PICK 3 CARDS

ROUND 2: input FRI, 08:00 PM

- 3 hours have passed since the initial discovery
- someone tweets the link to another pastebin with the hashtag #freeDomains4All #longLive.OK; it's a copy of the original pastebin.
- the tweet gets picked up and retweeted; the hashtag is amended with #itWorks.

PICK 3 CARDS

ROUND 3: input FRI, 10:00 PM

- 2 hours have passed
- the registry operator is contacted by the press, they want to know what's going on and ask for a formal statement.
- the registry operator's manager gets a phone call from the national television.
- the engineers are still looking into the matter, but haven't found yet where the leak came from.

PICK 3 CARDS

BONUS ROUND: input (3 minutes before the end of the round)

To make the exercise extra interesting, additional information can be injected. In real life, events do not follow a predictable pattern, certainly not during a crisis. Bonus rounds only deliver additional information that needs to be parsed and acted upon before the end of the round.

- the engineers have some good and some really bad news.

- they have found were the hackers had entered the system and traced what has changed.
- they also noticed that more than 50k additional domain names had been registered and an undefined number of existing domain names had been altered; some of them are high profile domain names.
- they suggest to roll back the DNS and reach out to the major Internet Service Providers to reload their resolvers

UPDATE 3 CARDS

ROUND 4: input SAT: 06:00 AM

- 8 hours have passed
- the national CERT contacts the registry operator; they have received some intelligence about the origin of the attack
- the social media of the registry operator are bombarded with questions by concerned domain name holders and registrars
- the generic mailboxes have exploded with more than 5.000 email received
- the media contacts the registry operator again for updates and are asking why it is taking so long to fix the issue
- the relevant supervising ministry (e.g. telecommunications) is contacting the registry operator's general manager, they want status updates and a debriefing of the impact of the incident

PICK 3 CARDS

ROUND 5: closure SUN: 09:00 AM

- 21 hours have passed
- engineering has rolled back the database to Thursday 11:47 PM, which was the most recent backup without evidence of the modified domain names
- name servers have been reloaded
- the vulnerability, exploited by the hackers, was fixed
- all registrar credentials have been reset
- support received a list of domain names, registrars and registrants which were impacted
- there's a major backlog in support with more than 10.000 emails in the support tickets and countless angry tweets
- several bloggers & vloggers have picked up on the issue and posted their opinions

PICK 3 CARDS

END OF EXERCISE - PAUSE

The participant will need a break ☺

DEBRIEF

Each team presents their cards.

For an effective and efficient exercise, it is important to correctly debrief and discuss the actions of the team. Therefore the output of the crisis team must be captured either in writing or by recording. The debrief should focus on a number of topics:

1. what is the general reaction on the exercise?
2. how well was the business continuity plan followed?
3. where did the team start to improvise?
4. did they feel adequate and up to the task?
5. what did they learn?
6. what improvement is needed?

Cards

Have these cards printed on business cards sized format, eventually use different colors per category.

	TECHNICAL	LEGAL / BC MANAGEMENT	COMMUNICATIONS	GOVERNANCE / MANAGEMENT
1	Shut down the authoritative name servers	Call Law Enforcement	Send out a status update on Social Media	Declare a disaster situation
2	Contact the registry service operator and inform them on the issue	Advise the management on communication strategy	Send out a message on Social Media	Summon the crisis team
3	Contact the anycast operator and inform them on the issue	Contact an external incident response company to assist in dealing with the issue	Answer the press	Open the Business Continuity Plan
4	Shut down the registration platform	Advise to minimize the communication	Prepare communication on roll back	Contact the overseeing authority / board
5	Start looking in available log files	Advise full transparency to management	Write press release(s)	Inform governmental oversight bodies
6	Restore the core database	Reach out to local telecom providers to restart their resolvers	Write templates for the crisis communication	Contact the country CERT and report the incident
7	Reinstall the compromised systems	Pass findings to Law Enforcement	Send the press statements on the impact	Give a press conference
8	Technical assessment & collect evidence of the hacked systems	Contact registrars to change passwords	No communication on public channels until confirmed by legal and general manager	Give status update to governmental oversight bodies
9	Start answering tickets and other request received over the support email address	Inform the European Data Protection Board on the issue	Send internal status update	Declare end of crisis and step down - back to business as usual
10	Create a list of	File the incident with	Hire crisis	Request assistance

	modified domain names to identify victims	law enforcement	communication spokesperson	from the national CERT
11	Create a list of added domain names	Inform insurance company	Deny the breach	Inform ICANN
12	Block access to the registration system	Inform impacted registrants	Send email to TLD-OPS for help	Contact IANA 24/7 Emergency line
13	Change all passwords	Inform other registries via the TLD-OPS mailing list		Blame TLD-OPS :-)
14	Download the password list from the pastebin	Ask assistance from other registries via the TLD-OPS mailing list		
15	Install a SIEM			

The deck of card is available for download on the TLD-OPS web site in the Adobe indesign format, ready to be send to the print shop.

WORKSHOP TIPS & TRICKS:

This section contains tips and tricks for the DR/BCP exercise, please email TLD-OPS if you have any new insight on how to make the TTX better.

- Identifying Stakeholders, Threats and Risks, is not a one person job. Continue to express this.
- Some threats are “scary”, that it is all the more reason to document it and have a plan for it.
- Have the individual exercise also identify which functions/groups/individuals within each TLD actually acts as BCP Manager; identify their actual Stakeholders
- Some may struggle with Financial impacts – having business people helps with this; business continuity is a collective exercise
- Clarify within your organization who fulfil the role of BCP Manager, is it legal, PMO, Finance, CIO, CSO, CEO, COO?
- Perhaps start the game by handing out the following 3 card to each team