JOINT REGIONAL ccTLD ORGANISATION SURVEY REPORT

ccTLD Disaster Preparedness

Joint Regional survey between AFTLD, APTLD, CENTR and LACTLD

PUBLIC VERSION - THIS REPORT HAS BEEN ANONYMISED.

References made to individual ccTLDs have mostly been removed from this report. Members of AFTLD, APTLD, CENTR and LACTLD have access to the full version.

Survey period: Jan-Feb 2018

Responses (55): .ae, .au, .be, .bi, .br, .ca (2), .ch(2), .ci, .cl, .cr, .cz, .de, .dk, .ee, .es, .fi(2), .id, .il, .is, .it, .jp, .ke, .la(2), .lk, .ls, .lt, .lv, .mg, .mn, .my, .nl, .no, .nu, .nz, .om, .pa, .pl, .pr, .py, .qa, .rs, .ru, .rw, .sa, .se, .si, .sn, .tn, .uk, .vu, .مصر (xn--wgbh1c).

Background: Puerto Rico was recently hit by one of the strongest hurricanes in recent history, resulting in significant problems for the .PR registry. In light of these developments, AFTLD, APTLD, CENTR and LACTLD ran a joint survey on the topic of disaster preparedness - something that concerns many of our members. The aim of the survey was to collect information on the types of disasters and emergencies ccTLDs around the world have faced and different approaches to how they deal with the challenges.

Highlights

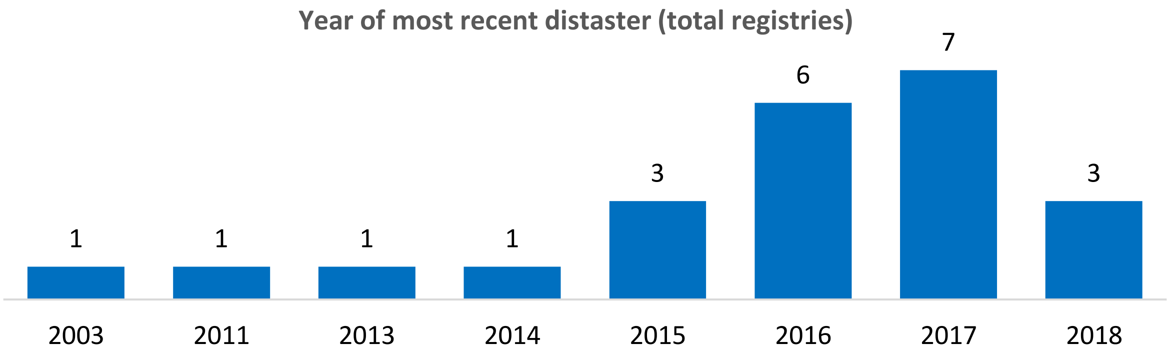
- 46% of TLDs reported a recent disaster
- The leading majority (25% of respondents whose TLD reported a recent disaster) were attributed to **cyber-attacks or security** compromise.
- 50% of respondents who experienced disaster in their organisation estimated that the time taken to recover operations was **under 6 hours**.
- **Lost customer confidence** was rated as the most impacted aspect of a disaster experience.
- 43% of respondents felt that staff in their organisations are only **partially set up** to perform remote recovery of operations. Organisations with large domain counts (> 50 000) are generally set-up to perform remote disaster recovery if needed.
- The majority of organisations (86%) use either **instant text (SMS) messaging** or email services to communicate with relevant personnel during disaster events.
- 78% of ccTLDs (globally) consider their organisation either **prepared or very prepared** for a disaster/emergency.

Introduction

Defining a 'disaster/emergency': For the purposes of the survey, an emergency or disaster has been defined as any event that causes business or operations to cease (for example, public facing website IT system go down, registry website goes down, etc.)

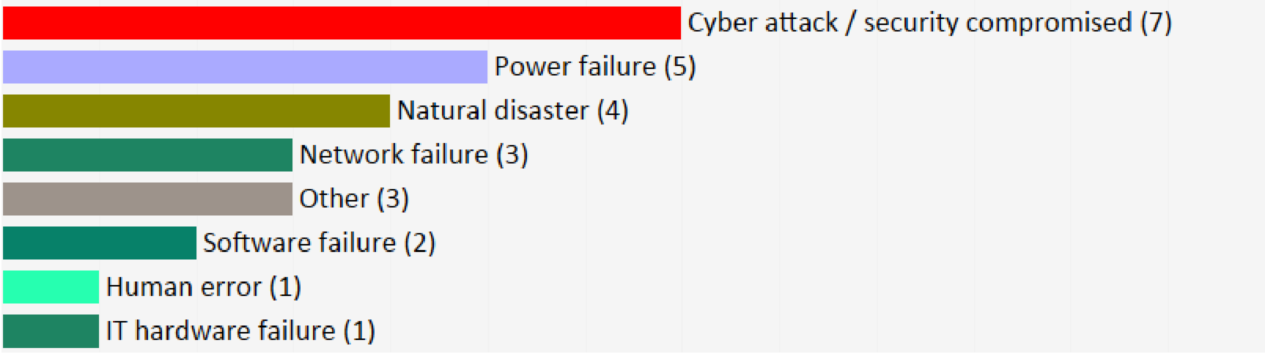
56% of organisations represented in the survey have not had a disaster/emergency, whilst 44% (25 registries) reported that they have experienced one. See Annexe 1.1 for data.

Respondents were asked to state the date of their last disaster/emergency. The following chart shows the number of organisation affected in the years that disasters were noted. 7 disasters or emergencies occurred in 2017, and 3 have already occurred in organisations this year (2018). See Annexe 1.2 for detailed month/date data.

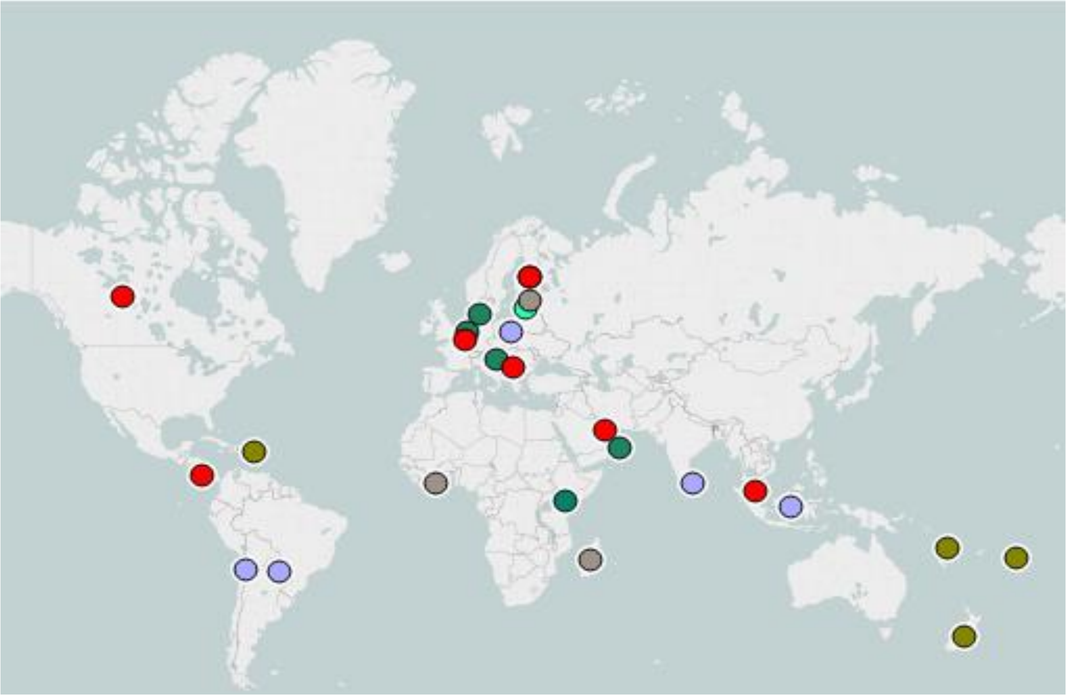


Causes of disaster/emergency

The majority of disaster/emergency causes were attributed to cyber-attacks/ security compromise (25% of organisations) followed by power failure (18%). Information entered as 'other' that matched any of the defined categories was included in the following chart. See Annexe 1.3 for data.



The map below shows locations of disasters by their type (colour coded according to above)



Details of disaster/emergency

	Political inspired DDOS attack.
	Apache Struts 0-day vulnerability - CVE-2017-5638.
	In an accident one truck impacted a power line tower. We had a blackout in our main office for 4 hours.
	A combination of minor circumstances, caused the network equipment to shut down at both sites, to prevent a split-brain situation.
	Cooling system failure on our primary server housing location.
	DDOS attack. It was due to implementing a new registry system.
	UPS in data centre on fire.
	A bug in the registry software erroneously triggered delete of 1120 name servers. Bulk delete of non-authorized sunrise applications triggered this bug which resided in the sunrise module of the registry software. This affected 9900 domains that were being served by the 1120 name servers.
	Power failure due to bad weather conditions.
	incorrectly interpreted command on networking device resulted into blocking of selective outgoing traffic.
	Website and mail server failed.
	Failing core switches which were both in a Master situation instead of Master-Slave situation.
	Hurricane Heta destroyed most infrastructure.
	6.3 magnitude earthquake in Christchurch.
	It happened during system refresh.
	Hurricane Maria.
	Main distribution of power down for 4 days. Fire in the substation. Another time a strike kept the personnel out of the office for 3 weeks.
	Registry web site was down for 1/2h due to DDoS attack.
	Loss of data on primary location.

Key challenges

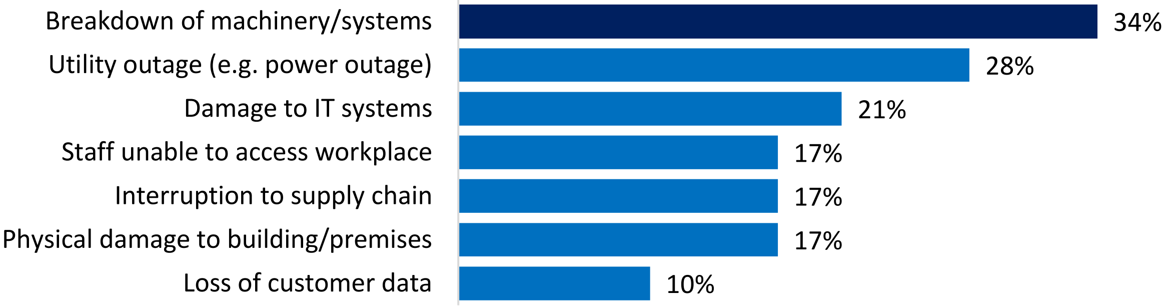
Respondents reported a wide variety of major challenges including:

- directly dealing with immediate safety or infrastructure damage threats (3)
- difficulty identifying the source of the disaster (3)
- recovering or restoring services (5)
- communications difficulties (4)

	Communication track with relevant peers (network admins and internet exchanges).
	Relatively few challenges in the process of dealing with the issue; we could have improved our internal and external communications.
	Transfer resources to a safe environment. Granting High Availability in event of disaster
	Normalise telephony systems and service for customer assistance.
	Had to change to a new website (one and only way to buy our domains) in less than a week.
	Time to identify the root cause.
	To make sure heat hadn't damaged systems, after working order was restored.
	Communication (what, when, how, to whom).
	Have no control on 3rd party data centre.
	The challenge was affected client/public control that hampered concentration on problem solving i.e. clients kept inquiries ongoing even after a public notification was shared and this affected technical teams focus on sorting out the issue.
	Restoring services with new hardware.
	Spent too much time (about an hour) to diagnose and understand cause of the problem.
	Impact in social reputation.
	Trying to discover what the issue was, since all networking was down.
	To get Internet working.
	No impact to our company.
	Our team is small that why it takes time for us to shift from one site to another to solve the problem and bring services up at short time.
	Finding a place with electrical power and Internet services from where our staff could work safely.
	Keep supplying enough fuel for the power generator.
	Recover the reputation impact.
	DDoS attack on registry IT infrastructure in 2013.
	Recovery of services.
	Getting the telecommunication network up and running again.

Key Impacts

Respondents were asked to tick areas that were most impacted by the disaster. The most cited impact was Breakdown of machinery or systems, with the least reported area impact being reported as loss of customer data. See Annexe 1.4 for data.

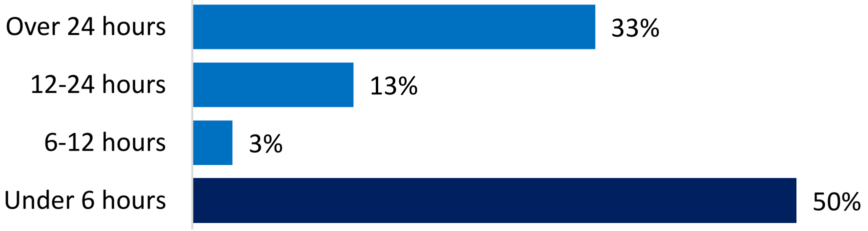


Other impacts of the disaster:

	service interruption for non-critical services
	We needed stop telephonic client attention and the staff left the office, after two hours of the begin the emergency. We apply the protocol of outage energy in the main office according to our plans.
	Changes to the code of our website
	Registrars' access to registry was down and zone file wasn't updated
	Services unavailable
	Outage of 9900 domains i.e. 9900 domains went offline due to lack of delegation info (name servers) until the records were reinstated
	Availability of some services running on secondary interfaces
	Unavailable website and mail server
	Interruption on daily operation
	Cannot Access some service
	Public web was inaccessible.

Recover of essential services

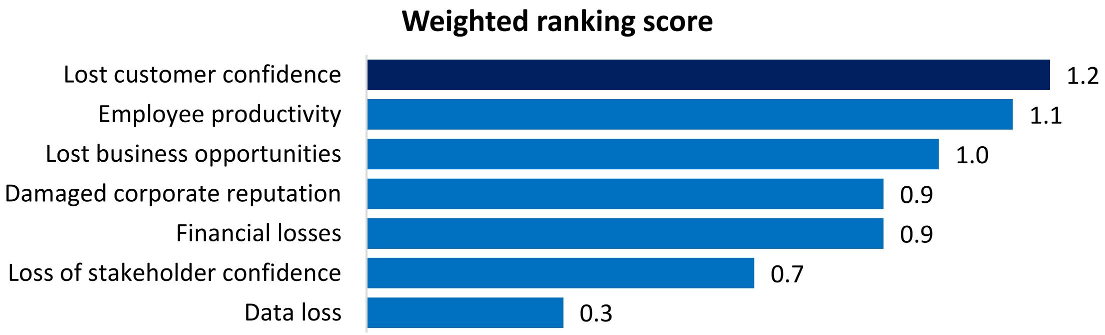
Respondents were asked to estimate the time taken to recover essential services in the event of the previous disaster. The majority (50 %) estimate that this took less than 6 hrs. The second most cited estimate was longer than 24 hours (33%). See Annexe 1.5 for data.



Organisational impacts

Respondents were asked to rate the aspects of impact on their organisation from none, low, medium and high. A weighted average score was applied to produce the chart below. Lost customer confidence was rated as the most impacted aspect, whilst employee productivity rated as the second most impacted area of organisations. Data loss was rated as the lowest impact aspect on their organisation *. See Annexe 1.6 for data.

*For registries where two responses were received, both responses were included in the calculation.



Lessons learnt

Respondents were asked to list or describe important lessons learnt from their most recent disaster experiences. One of the most common themes centred around preparation, planning and documentation for disasters and creating a recovery procedure or plan that is reviewed and tested regularly (cited by 36% respondents who answered this question). Communication was also frequently listed – both internal communication (staff knowing their roles in disaster recovery) and external communication (informing registrars about disaster) were cited as well as a focus on backup policies and protocols.

One notable response was the recommendation of a requirement to have a manual key to open doors with locks that are electronically operated – which in the case of power failure would not unlock (.nl). This comment serves as a good prompt to review basic physical security and locking systems throughout your organisation premises which could be similarly affected during the event of power failure.

	Decide (and communicate) upfront how much you want to invest in DDOS protection. If that turns out to be insufficient, sit out the attack and invest in cloud solutions for all internet facing services (cost efficiency).
	Review disaster recovery plan periodically.
	Work your plan. Communication is a discipline; do it in a disciplined way. Ensure everyone knows their role.

	White-list all registry services to registrars.
	Have a good backup policy. Have a highly redundant environment have a good policy of resumption of service. Have a safe environment.
	The importance of appropriate documentation and protocols for continuity of operations.
	Higher security standards in our website and better emergency protocol.
	consider turning off the split-brain prevention feature.
	It is important to have detailed contracts. Documentation must be up-to-date. Have a hot-copy of database in other location.
	That we need DDoS protection agreement(s) with your ISP(s) Or for example F5 Silverline service.
	More communication to registrars is needed.
	Having Disaster Recovery Centre is best way to faster recovery.
	Thorough tests need to be done to software/systems especially after an upgrade is done by developer.
	Deal with the problem.
	Keep backup hardware to a ratio with the total number of running hardware
	we need more reliable external monitoring.
	We have to prepare some emergency plan in order to avoid the possible impacts of a big disaster.
	Well tested and updated disaster recovery plan is important
	A normal key for access to server room (instead of electronic key, which did not work). All further procedures were in place.
	We were well prepared and had good resources.
	Need to have a BCP and alternate premises plan in place
	Need to have disaster plan for emergency cases
	The importance of developing a risk management and disaster recovery plan.
	Have a plan. Have the people to know their role. Be prepared.
	Always follow processes identified.
	Keep good relations with upstream providers.
	Plan for the worst and hope for the best :).
	Safe and secured premises of data storage and power supply.

Instant messaging for disaster communications

The majority of organisations (86%) use either instant text (SMS) messaging or email services to communicate with relevant personnel during disaster events.

Has instant text (SMS) or email message service	44
Does not have instant messaging service	6

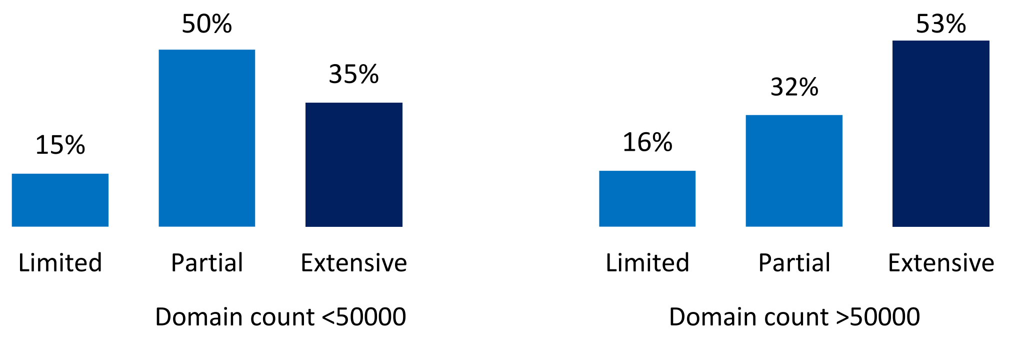
Incident response team

76 % of organisations reported that they do have an incident response team.

Has a dedicated incident response team	38
Planning to develop an incident response team	9
Does not have incident response team	3

Remote recovery

43% of respondents felt that staff in their organisations are **partially** set up to perform remote recovery of operations. Organisations with large domain counts (> 50 000) are better prepared in general recover operations remotely, shown in the chart below*. See Annexe 1.7 for data.



*.ci and .cl domain count data not available.

Additional comments on remote recovery

	Our DR plan is built around the expectation of remote work.
	VPN access to both primary and backup sites.
	Access via VPN.
	Depends on disaster/emergency type. Some activities must be done in site.
	We have been working on a strategy for more than a year and this year we plan to have an improved version by the end of the year.

	Our disaster recovery strategy is based on a fully remote-controlled IT system environment. Relevant (IT) employees are equipped with mobile devices and our IT systems are located in redundant data centres operated by professional data centre providers.
	Management segment of our network is covering all our service locations and vital infrastructure is remotely manageable.
	IT managers have 24/7 standby for disaster.
	It mainly depends on the type of disaster!
	We have an office in the city separate to headquarters location to keep on providing minimum service in case we face disaster.
	Our servers are hosted in a data centre and therefore most technical operations are conducted remotely unless there is a physical damage/interruption.
	A lot of systems are not accessible outside the company LAN, so for them to be recovered one will have to be on site.
	Some legacy systems limit that ability.
	We strongly support on remote recovery.
	It was limited during the first two hours of the incident, since networking was down.
	You have to physically restore antennas etc.
	Geographic diversity of servers and datacentres, replication of core data and services across sites, backup operation support contracts, alternative offsite office space in multiple parts of the country, satellite phones
	The registry was housed in an AT&T bunker; consequently, we were able to access it remotely.
	It depends on the type of incident. In case of hardware failure, a little bit can be done remotely.
	Key response person has remote access to infrastructure of registry
	.rw registry technical staffs have modems to enable them to work remotely at any time of the day.
	Vanuatu is made up of Islands with ocean separating the islands. When the backbone infrastructure is destroyed, it affects the whole country.

Disaster Recovery Plans (DRP)

71% of 54 respondents have a disaster recovery or contingency plan. Basic details from respondents are provided in the table below.

	We have a comprehensive framework to manage such an eventuality.
	Plans have been developed in accordance with Business continuity - ISO 22301. They are operational, and review and testing is done at regular intervals.

	It's a business continuity plan that address risk evaluation for important processes. The result is a guide that provides instructions to keep the risks under control and a basic how-to document to start the recovery plan if needed.
	We have an extensive and practiced DR/BCP process with requisite documentation. It is a challenge keeping it current
	Depends of kind of disaster/emergency. For example, in the case of a big earthquake, after verifying all personnel and family are safe and sound, people able must go to headquarters to execute the recovery plans
	We have a disaster recovery plan we have been working on for more than a year which we plan to have completed by the end of 2018. We focus on having all our servers and website up and running in the less amount of time possible. We already have several anycast services, so we are currently focusing on having absolutely every one of our services and servers up and running in the least amount of time. We also have an emergency plan for dealing with the media and social networks.
	Germany's ccTLD Registry Operator, DENIC (.de), has taken another logical step towards sustainable societal security and reliability: On 28 November 2016, the German certification body TÜV Nord confirmed DENIC's successful Business Continuity Management (BCM) certification in accordance with ISO 22301. Published in 2012, the international ISO 22301 standard specifies the requirements for planning, establishing and implementing such measures in the framework of corporate planning that are to ensure continued operation of a business in case of disruptive incidents when they arise. This approach shall reduce the downtimes resulting from major disturbances of information systems or disasters to a minimum or even prevent or entirely exclude such incidents, in line with the requirements imposed by risk management and information security.
	We have a recovery plan in case our primary datacentre is unavailable and can switch to our dark centre in about 12 hours with less than 1 hour of data loss.
	1. Evacuation plans for rooms and buildings. 2. Communication instructions. 3. Behavioural guidelines for various emergencies 4. communication channels for different IT disaster situations 5. information on first aid measures. 6. Training.
	The contingency plan is part of our implemented BIA.
	We have very comprehensive plan which has considered probable but also very unlikely risks.
	It's based on several realistic scenarios.
	We use ISO 27001 and ISO 22301 as implementing business continuity plan for office and data centre.
	Main .it services are replicated in Milano at the Milan Internet eXchange point (MIX) and the data are synchronised in real time.

	We have an office in city other than the headquarters location to keep on providing minimum service in case we face disaster.
	We have a Business Continuity Plan (BCP) and technical Disaster Recovery Plan (DRP) that are updated and tested annually or whenever there is personnel change(s). We also have a hot site with full replica of all the registry systems.
	Backup site to record the data twice a week.
	According to the DR plan we maintain proper backups and alternate systems at DR site to provide the minimal service level to the customers.
	There is server/service recovery plan but not data centre recovery plan. 1. all the servers are backed up on two places, one on site, different data centre, the other one on a remote site. if the server fails, a system image backup is available, and the backup is done every midnight. There are many applications running on virtual environment, that is also backed up, a whole virtual environment, and per host within the environment. Backups take about 2 hours to be loaded. The distance between the DR site and the main site is 9 km, and the technical officers stays 8 km away from the office.
	DRP is reviewed annually, it provides information and describes processes in case of major infrastructure and business failures.
	MYNIC is ISO 22301:2013 certified, related documents are, - Business Recovery Plan Procedure - Incident Response Plan Procedure.
	We have a twin data centre principle, both running production services. Several guide books are in place for different types of outages (IT technical, business continuity and DDoS).
	Failover to standby site.
	Most focus on planning ahead. All staff has separate responsibilities. Extra material in stock at all time.
	It is an extensive plan that is reviewed and updated every 12 months.
	We had a disaster recovery plan and tested.
	Basically, we have two-tiered locations that work in an active-active mode. The third location is used for remote backups and, if necessary, can serve as a recovery site.
	- Employee training - monitoring - notification - gathering of experts - case study - the adoption of the plan or situation, measures.
	We do have a disaster recovery plan which includes a step-by-step on how to switch to our remote site (registry backup) located at 10 km from the main registry site in case of any disaster.
	In <four hours Go-live with our back-up (mirror) site.
	Work in progress.
	We are processing since we will be iso27001 certified.
	We have a Business Continuity Plan, Recovery Plans and a Crisis Management Plan.

	Offshore back up and offshore secondary DNS servers

Good-will measures

57 % of respondents reported that their disaster recovery plan does not provide good-will measures (e.g. registration/deregistration extension periods or other measures) to safeguard their customers’ interests in their disaster recovery plans.

Provides good-will measures	16
Does not provide good-will measures	21

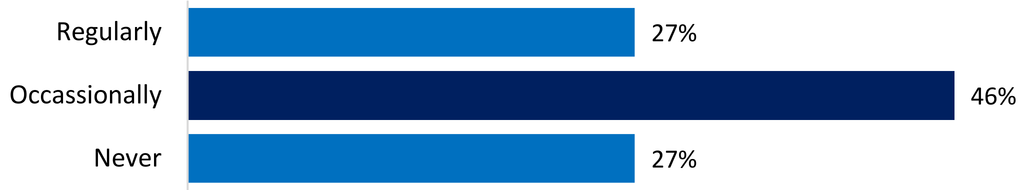
Detailed comments on good-will measures

	Emergency registration/deregistration is not in scope. BCM is focused on an always 'up' scenario by deploying maximum redundancy.
	At the time of a large-scale disaster such as the earthquake in Kumamoto (in 2016) and Tohoku (in 2011), we exempted registration fee from registrants in the disaster area.
	yes, we do for government sectors
	We can provide limited service as far as the main DNS infrastructure in available during the disaster period.
	No, but the plan is to have the registry software hosted on another provider as a contingency plan.
	We think of it not for a long time.
	Not applicable with .nl.
	Yes, but that is the responsibility of our sub-contractor. .SE.
	Not necessary as it is not anticipated that our systems would go down due to multiple sites and geographic diversity.
	Before we do any maintenance or any big change on the system we inform all our customer and we give them period time when we finish it and all our change happen after working hour so that will not interrupt our customer work.
	Not for now, but we are working on it with registrars.
	No in general, but by the case.
	Our disaster recovery plan is very technical, but we are still working on it in order to build a DR plan in the context of the entire organisation
	Processing as mentioned in previous question on developing a disaster recovery plan.

Frequency of disaster testing

14 respondents (27%) of respondents reported that their organisations never perform disaster testing.

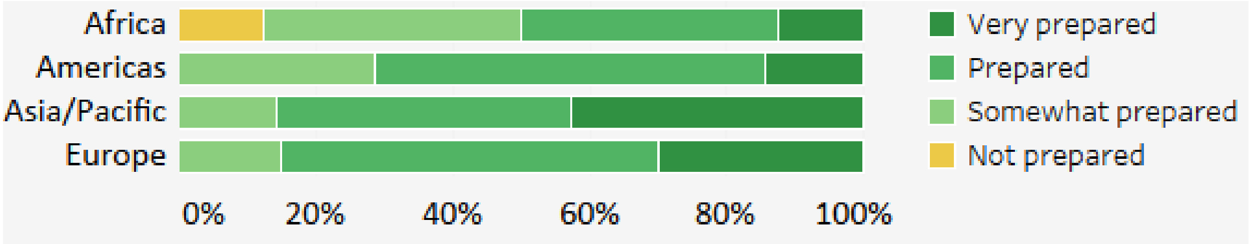
See Annexe 1.8 for data.*



*4 respondents each had two respondents providing different responses to the above question. Both responses were counted in the above chart.

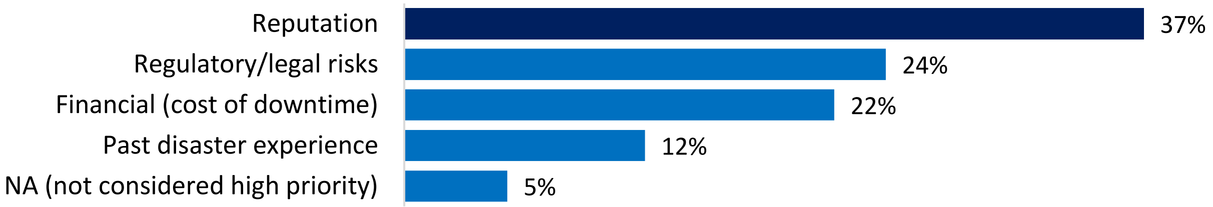
Self-assessed preparedness to disasters

78% of ccTLDs (globally) consider their organisation either *prepared* or *very prepared* for a disaster/emergency. The following chart shows the breakdown of these preparedness ratings by region of the TLDs whose representatives responded to this question. See Annexe 1.9 for data.



Reasons for improving DRP

Reputation was cited as the most common reason (37% of respondents) for improving disaster recovery plan and processes. 71% of respondents who cited 'Past disaster experience' as a motivator for improving their DRP suffered from a disaster experience as listed in the second question in this survey. See data in Annexe 1.10.

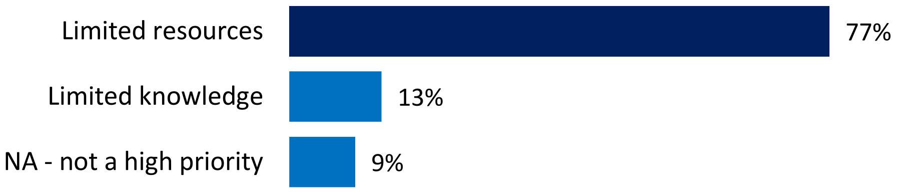


Additional comments

	Critical infrastructure.
	Imperative DNS Service Continuity.
	A domain name Registry can be considered a critical infrastructure and it is very important to assure that everything works properly.
	Continuous improvement of our capabilities (ISO27001).
	We see it as our duty to provide a robust and resilient service.

Barriers to regular disaster testing and planning

‘Limited resource’ was the most common barrier to regular disaster testing and planning (77 % of respondents). See Annexe 1.11 for data.



Additional comments

Our readiness to disaster/emergency is reasonable
No barriers
Lack of people

Disaster plan procedures

References that some of the TLDs have suggested include:

- “disaster recovery and business continuity, The Art of Service.” (book suggested by .br)
- http://www.bcmpedia.org/wiki/Main
- ISO 27001 standard
- The ISO22301 standard and its associated supporting materials are very useful.

Annexe 1.1 Organisation impacted by disaster or emergency

Yes	23
No	28

Annexe 1.2 Date of last disaster or emergency

NA	03/2016	NA	08/2016
NA	03/2017	NA	04/ 2015
NA	09/2016	NA	02/2018
NA	01/2018	NA	12/2003
NA	2014	NA	02/2011
NA	01/2013	NA	02/2017

NA	09/2016	NA	10/ 2017
NA	10/2017	NA	02/2015
NA	01/2018	NA	10/2017
NA	12/2017	NA	Q1 2016
NA	12/2017	NA	03/2015

Annexe 1.3 Type of disaster

Disaster type	**TLDs**
Cyber attack / security compromised	7
Power failure	5
Network failure	3
Natural disaster	4
Software failure	2
IT hardware failure	1
Human error	1
Other	5

Annexe 1.4 Impacts of the disaster

NA

Annexe 1.5 Incident response recovery time

*TLDs with two respondents having different responses are ***bold*** in the table below. All responses were counted for the bar chart.

Under 6 hours	14
6-12 hours	1
12-24 hours	4
Over 24 hours	10
No response	23

Annexe 1.6 Impact on organisation ratings

NA

Annexe 1.7 Remote recovery capability

Remote recovery ability	**TLDs**
Limited	8
Partial	23
Extensive	20

Annexe 1.8 Frequency of disaster testing

*TLDs with two respondents having different responses are ***bold*** in the table below. All responses were counted for the bar chart.

Frequency of disaster testing	**TLD**
Never	14
Occasionally	24
Regularly	14

Annexe 1.9 Ability to recover rating

*TLDs with two respondents having different responses are ***bold*** in the table below. All responses were counted for the bar chart.

Level of preparedness	**TLDs**
Not prepared	1
Somewhat prepared	12
Prepared	20
Very prepared	15

Annexe 1.10 Reasons for improving disaster recovery capability

Reason	**TLD**
Regulatory/legal risks	28
Financial (cost of downtime)	24
Reputation	39
Past disaster experience	13
NA (not considered high priority)	6

Annexe 1.11 Barriers to disaster/emergency planning

Reason	TLD
Limited resources	39
Limited knowledge	7
NA – not a high priority	5