Disaster and emergency preparedness in ccTLD Registries

Joint Survey Results

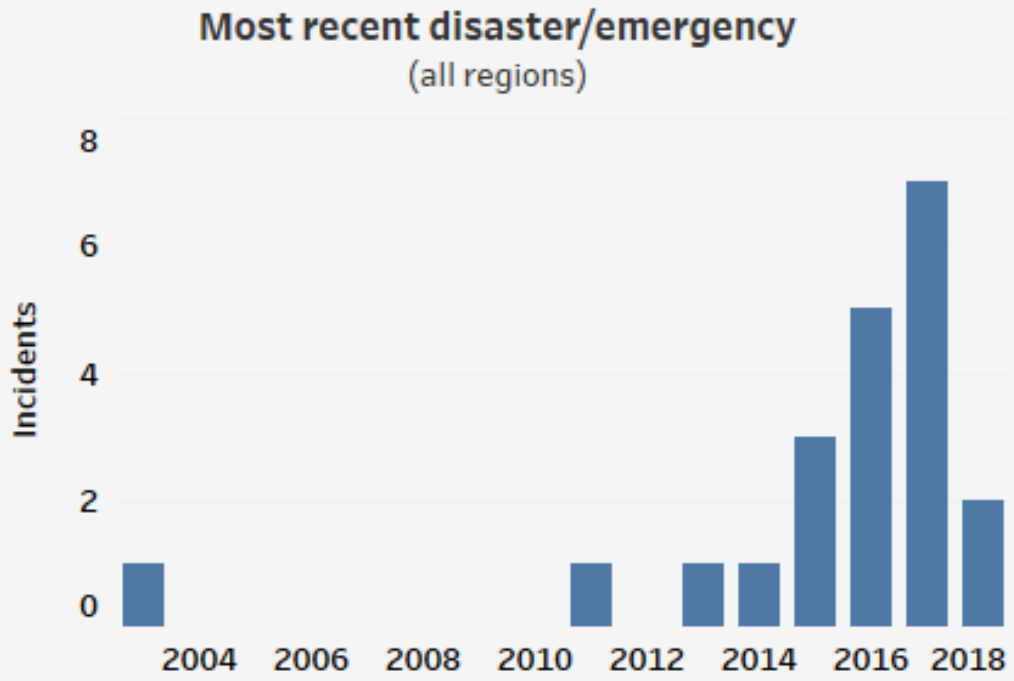
Survey period: Jan-Feb 2018
Unique Responses: 50 ccTLDs

.ae, .au, .be, .bi, .br, .ca, .ch, .ci, .cr, .cz, .de, .dk, .ee, .es, .fi, .id, .il, .is, .it, .jp, .ke, .la, .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, .) مصرxn--wgbh1c)

"Disaster": *defined in survey as any event that causes business or operations to cease.*

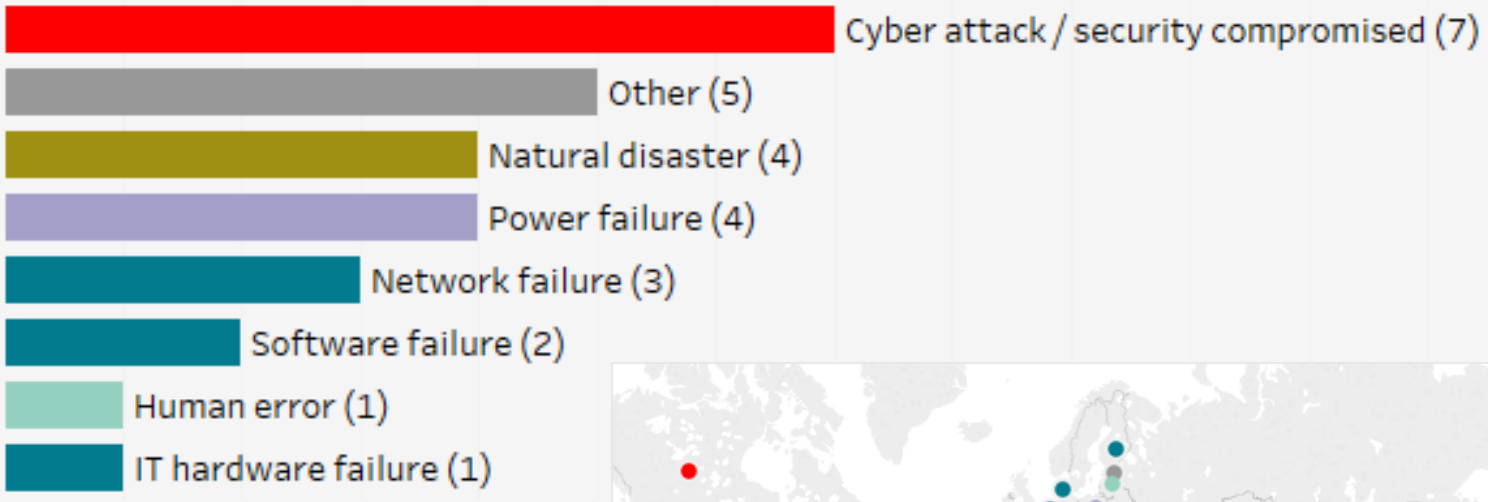
Incidents on the rise?

- **44%** of ccTLDs have been impacted by some sort of disaster/emergency over the past 15 years
- Of the most recent incidents, most were in 2017



Report available to survey respondents in coming weeks

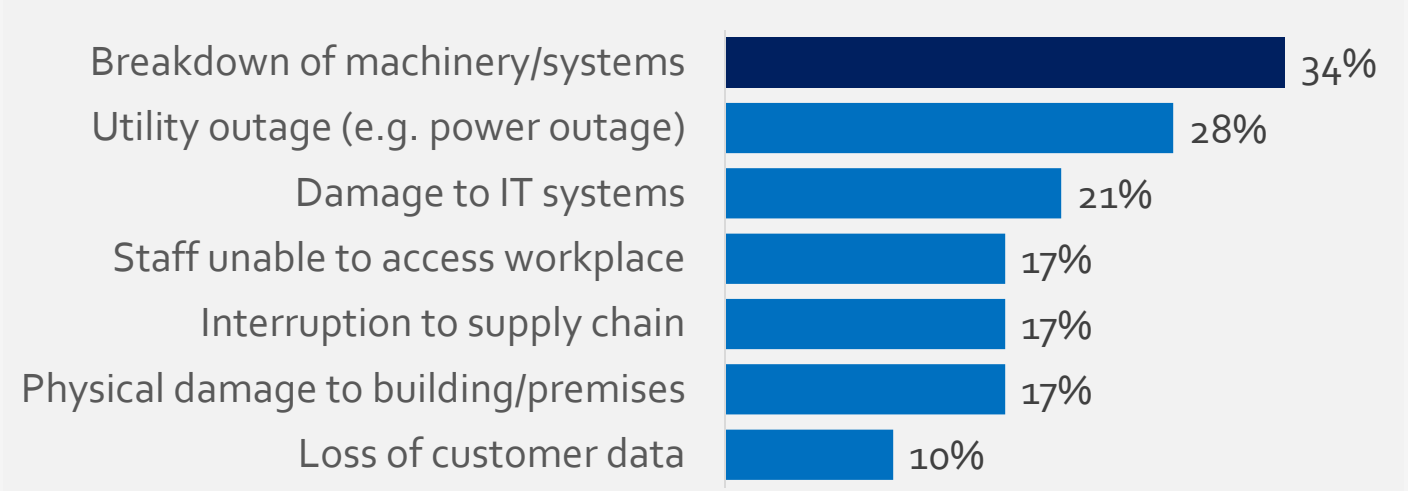
Cyber attack/security compromise are most common cause of incidents (25%)



Report available to survey respondents in coming weeks

Impacts from incidents

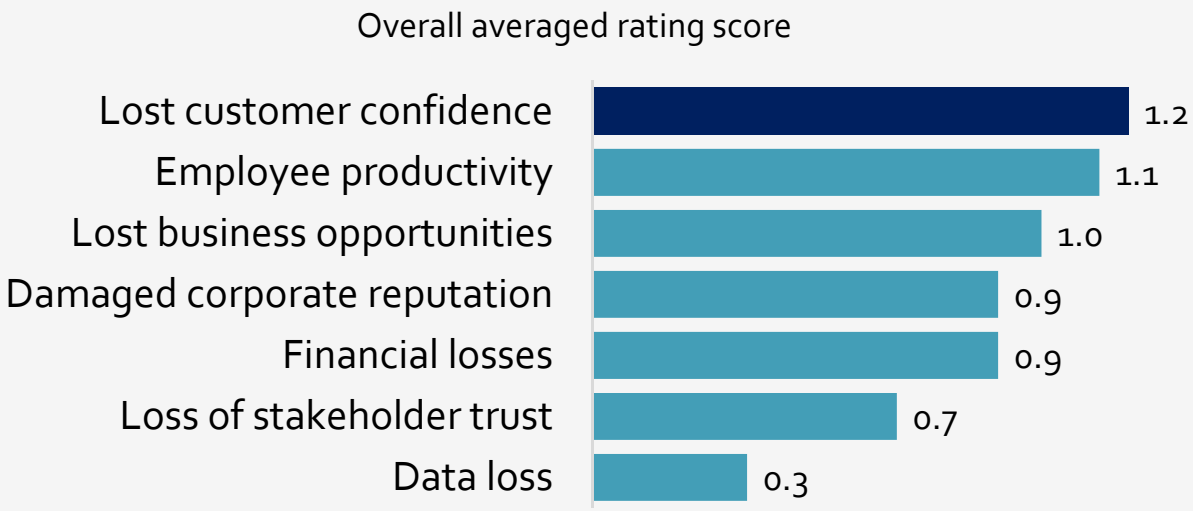
Breakdowns of machinery/systems reported as biggest impact from disasters/emergencies



Report available to survey respondents in coming weeks

Other impacts to the organisation

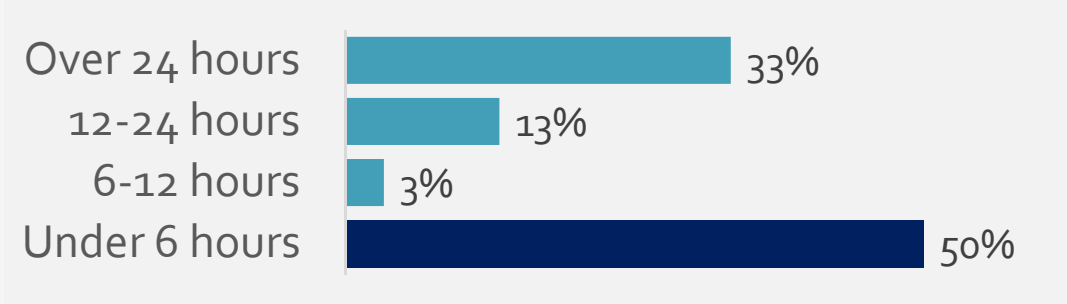
Loss in customer confidence was rated the most impacted area as a result of disasters/emergencies. Data loss was rated as the least impacted aspect.



Report available to survey respondents in coming weeks

Response time

50% of respondents were able to recover essential operations/services in **under 6 hours**



Report available to survey respondents in coming weeks

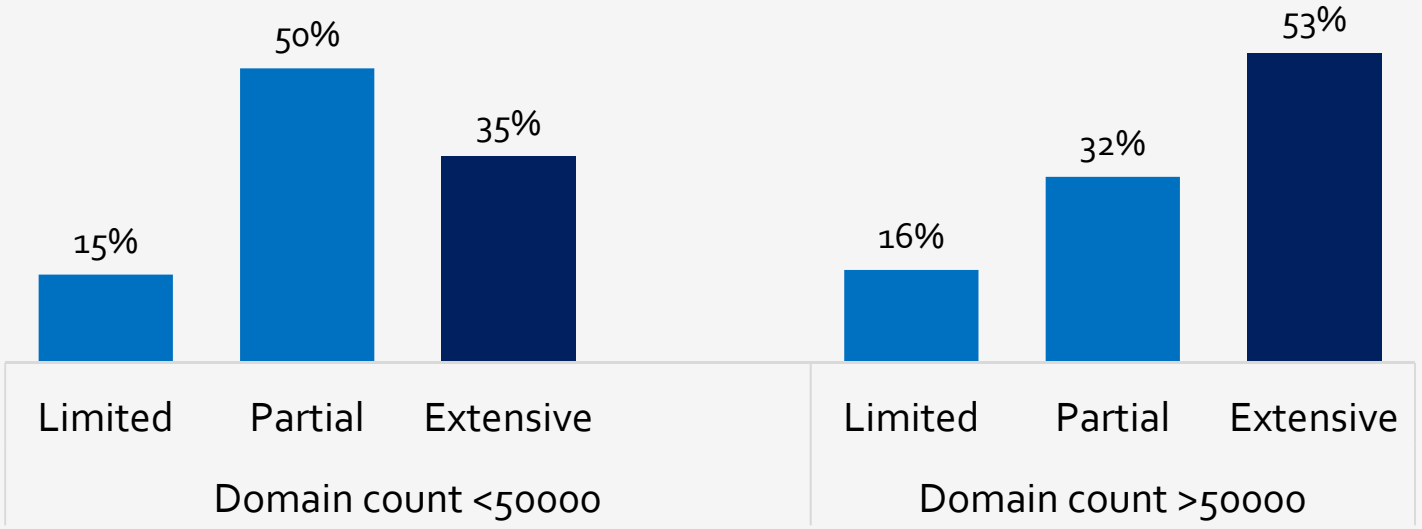
Incident response

- **86%** of organisations have instant text (SMS) or email messaging services for communication during disaster/emergency events
- **75%** of organisations have a dedicated incident response team

Report available to survey respondents in coming weeks

Remote Recovery

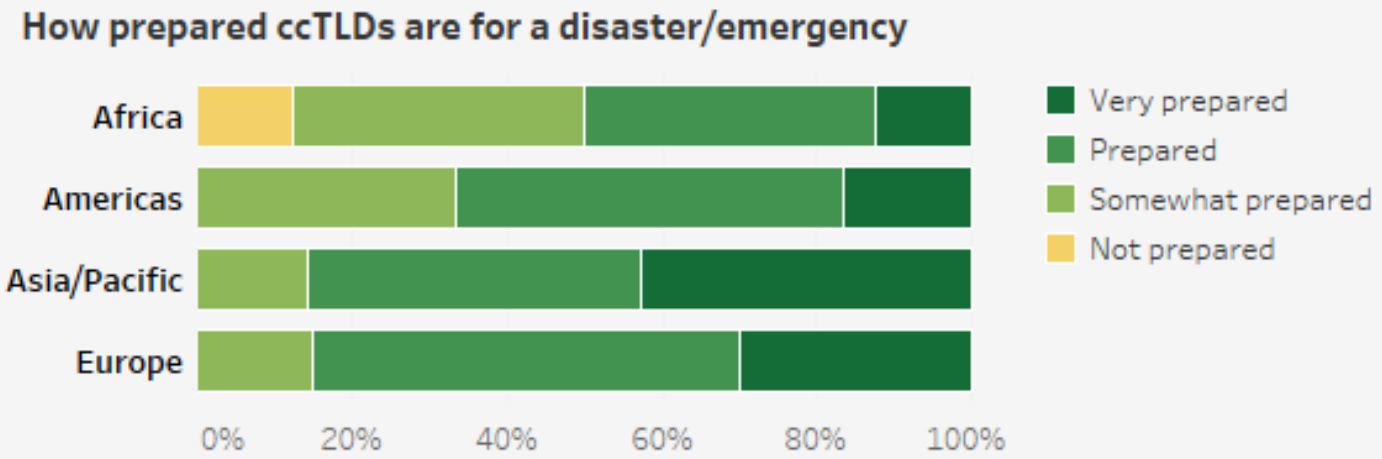
- **43% of respondents** estimate their staff are **partially** set up to perform remote recovery.
- Organisations with large domain counts (>50000) are better prepared to recover operations remotely.



Report available to survey respondents in coming weeks

Overall preparedness for a disaster/emergency

78% of ccTLDs (globally) consider their organisation either *prepared* or *very prepared* for a disaster/emergency



Want advice?
Considering talking to 'very prepared' registries in your region:
.au, .be, .ca, .de, .dk, .no, .nu, .nz, .om, .qa, .ru, .tn, .uk, .vu

Report available to survey respondents in coming weeks

Lessons learnt

- Prepare (recovery plan) and document
- Regular testing (recover plan)
- Communication
- Data backup

Report available to survey respondents in coming weeks

Key points

- Half of ccTLDs globally have faced some sort of disaster/emergency
- Most incidents relate to cyber security
- Breakdown of machinery is most common immediate impact. Loss of customer confidence rated a high impact to the organisation.
- Incidence response times are mostly under 6 hours. Most have response teams and instant message communication in place. Larger registries are better prepared.
- 78% of ccTLDs (globally) consider their organisation either prepared or very prepared for a disaster/emergency

Report available to survey respondents in coming weeks

Resources

- Most organisations provided some details on their current disaster recovery plans in the survey (see report for details).
- The following TLDs are able to share their current plans if you wish to contact them: .au, .ca, .ch, .ci, .cr, .id, .ke, .la, .ls, .nl, .pr, .tn, .uk, .vu
- **“Disaster recovery and business continuity, The Art of Service.”** (book suggested by .br)
- .ci – directly contact ciso@nic.cl
- http://www.bcmpedia.org/wiki/Main_Page (.de suggestion)
- ISO27001 standard (.la suggestion)
- ISO22301 standard (.uk suggestion)

Thanks for your attention

A survey report will be made available to survey respondents in the coming weeks

Any questions on data: patrick@centr.org