TLD-OPS

TECHNICAL

SHUT DOWN THE AUTHORITATIVE NAME SERVERS

CONTACT THE REGISTRY SERVICE OPERATOR AND INFORM THEM ON THE ISSUE

CONTACT THE
ANYCAST
OPERATOR AND
INFORM THEM ON
THE ISSUE

SHUT DOWN THE REGISTRATION PLATFORM

START LOOKING IN AVAILABLE LOG FILES

RESTORE THE CORE DATABASE

REINSTALL THE COMPROMISED SYSTEMS

TECHNICAL ASSESSMENT & COLLECT EVIDENCE OF THE HACKED SYSTEMS

START ANSWERING TICKETS AND OTHER REQUEST RECEIVED OVER THE SUPPORT EMAIL ADDRESS

CREATE A LIST OF MODIFIED DOMAIN NAMES TO IDENTIFY VICTIMS

CREATE A LIST
OF ADDED
DOMAIN NAMES

BLOCK ACCESS TO THE REGISTRATION SYSTEM

CHANGE
ALL PASSWORDS

**DOWNLOAD
THE PASSWORD
LIST FROM THE
PASTEBIN**

INSTALL A SIEM

LEGAL

CALL LAW ENFORCEMENT

ADVISE THE MANAGEMENT ON COMMUNICATION STRATEGY

CONTACT AN EXTERNAL INCIDENT RESPONSE COMPANY TO ASSIST IN DEALING WITH THE ISSUE

**ADVISE TO
MINIMIZE THE
COMMUNICATION**

ADVISE FULL TRANSPARENCY TO MANAGEMENT

REACH OUT TO LOCAL TELECOM PROVIDERS TO RESTART THEIR RESOLVERS

PASS FINDINGS TO LAW ENFORCEMENT

**CONTACT
REGISTRARS
TO CHANGE
PASSWORDS**
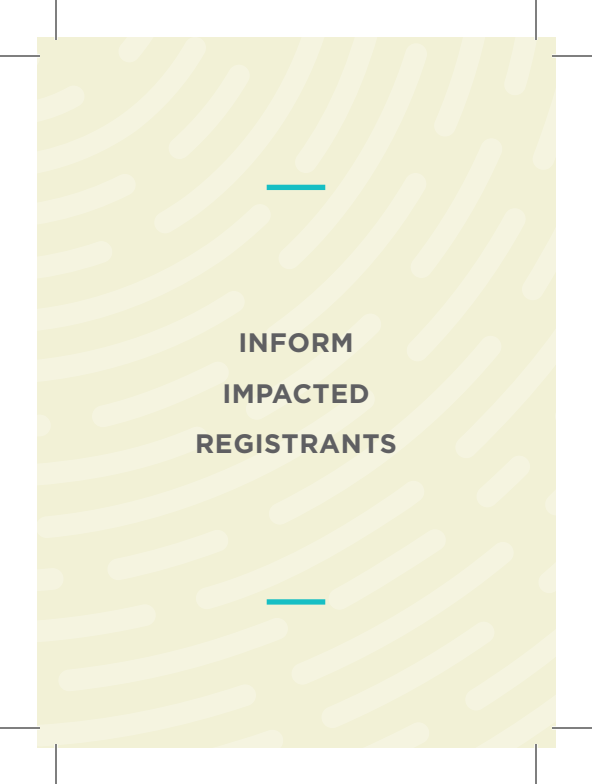
INFORM THE EUROPEAN DATA PROTECTION BOARD ON THE ISSUE
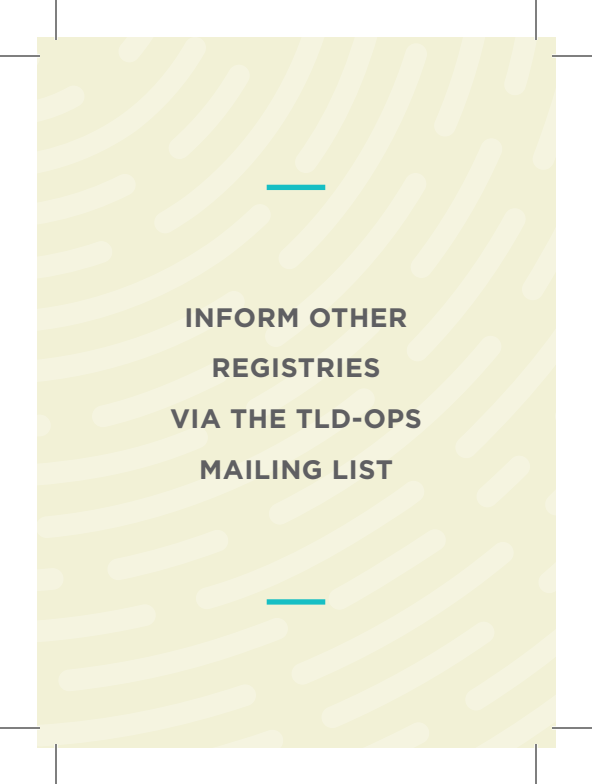
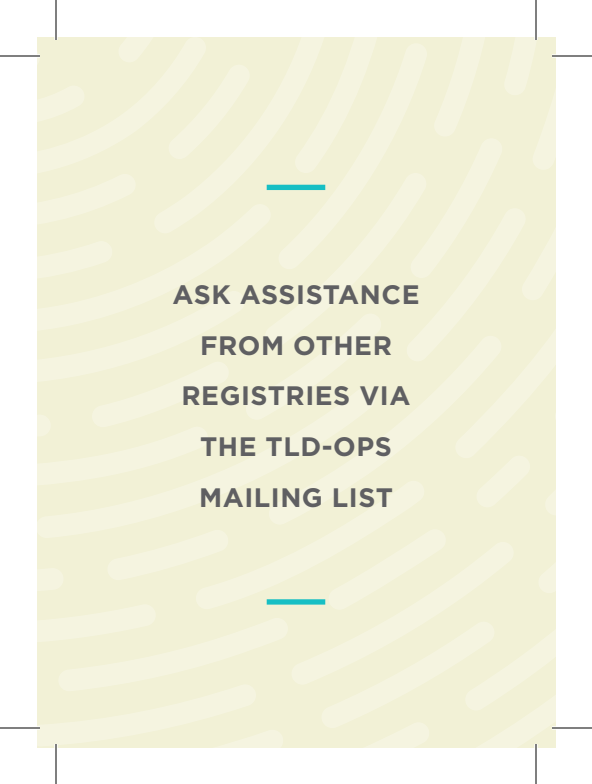# FILE THE INCIDENT WITH LAW ENFORCEMENT

INFORM
INSURANCE
COMPANY

INFORM

IMPACTED

REGISTRANTS

INFORM OTHER REGISTRIES VIA THE TLD-OPS MAILING LIST

ASK ASSISTANCE FROM OTHER REGISTRIES VIA THE TLD-OPS MAILING LIST

TLD-OPS

COMMUNICATION

ICANN|ccNSO

**SEND OUT A
STATUS UPDATE ON
SOCIAL MEDIA**

**SEND OUT
A MESSAGE ON
SOCIAL MEDIA**

ANSWER
THE PRESS

PREPARE

COMMUNICATION

ON ROLL BACK

WRITE PRESS

RELEASE(S)

WRITE TEMPLATES FOR THE CRISIS COMMUNICATION

SEND THE PRESS STATEMENTS ON THE IMPACT

NO COMMUNICATION ON PUBLIC CHANNELS UNTIL CONFIRMED BY LEGAL AND GENERAL MANAGER

**SEND INTERNAL
STATUS UPDATE**

**HIRE CRISIS
COMMUNICATION
SPOKESPERSON**

DENY THE BREACH

**SEND EMAIL TO
TLD-OPS FOR HELP**

TLD-OPS

GOVERNANCE / MANAGEMENT

ICANN | ccNSO
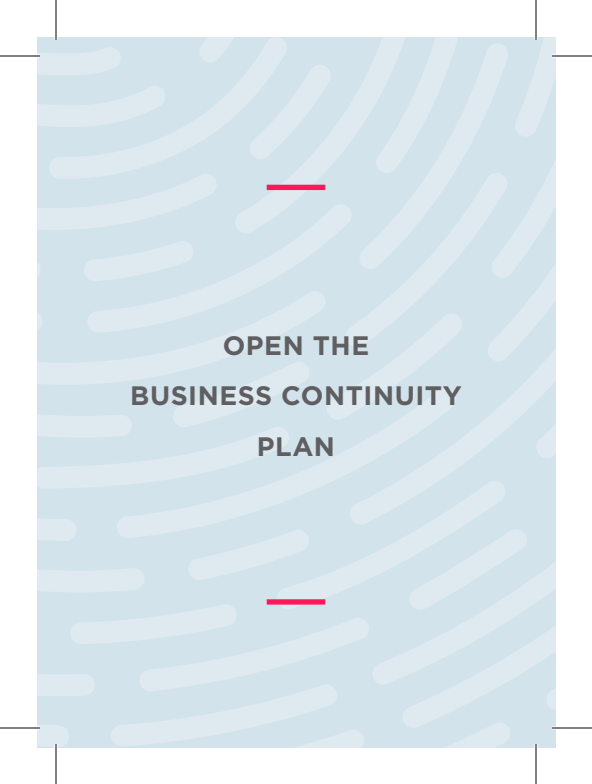
DECLARE A DISASTER SITUATION

SUMMON THE
CRISIS TEAM

**OPEN THE
BUSINESS CONTINUITY
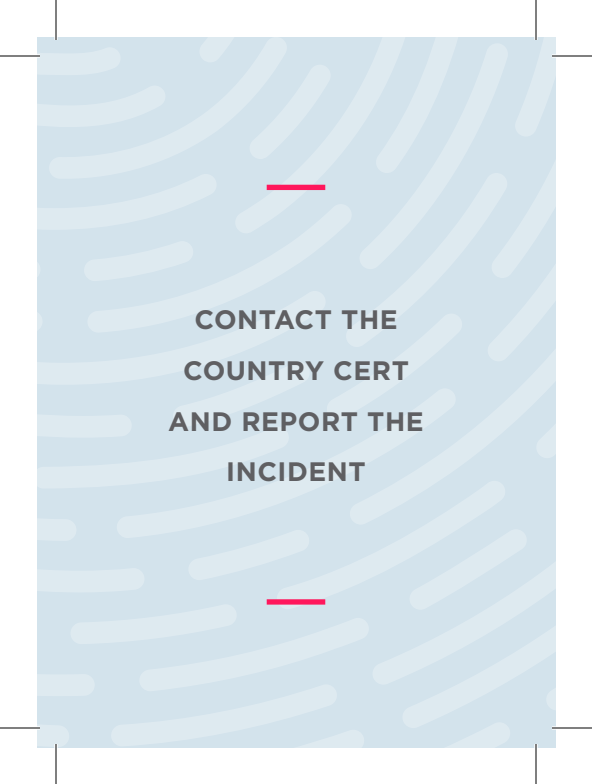PLAN**

CONTACT
THE OVERSEEING
AUTHORITY / BOARD

INFORM
GOVERNMENTAL
OVERSIGHT BODIES

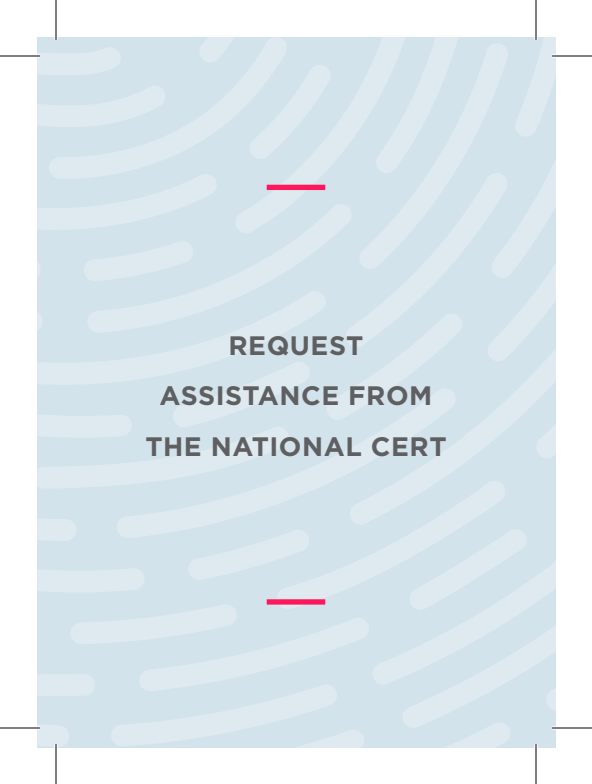# CONTACT THE COUNTRY CERT AND REPORT THE INCIDENT

GIVE A PRESS CONFERENCE

GIVE STATUS UPDATE TO GOVERNMENTAL OVERSIGHT BODIES

DECLARE END OF CRISIS AND STEP DOWN - BACK TO BUSINESS AS USUAL

REQUEST
ASSISTANCE FROM
THE NATIONAL CERT

INFORM ICANN

CONTACT IANA 24/7

EMERGENCY LINE

BLAME TLD-OPS :-)