Centre for Internet and Society
G-15 (top floor), Hauz Khas,
New Delhi - 110016
India
W: http://cis-india.org

24 December 2014

To:
Mr. Steve Crocker, Chairman of the Board
Mr. Fadi Chehade, CEO and President
Mr. Geoff Bickers, Team Lead, ICANN Computer Incident Response Team (CIRT) & Director of Security Operations
Mr. John Crain, Chief Security, Stability and Resiliency Officer
Members of the ICANN-CIRT & ICANN Security Team

Sub: Details of cyber-attacks on ICANN

We understand that ICANN recently suffered a spear-phishing attack that compromised contact details of several ICANN staff, including their email addresses; these credentials were used to gain access to ICANN's Centralized Zone Data System (CZDS).[1] We are glad to note that ICANN's critical functions and IANA-related systems were not affected.[2]

The incident has, however, raised concerns of the security of ICANN's systems. In order to understand when, in the past, ICANN has suffered similar security breaches, we request details of all cyber-attacks suffered or thought/suspected to have been suffered by ICANN (and for which, therefore, investigation was carried out within and outside ICANN), from 1999 till date. This includes, naturally, the recent spear-phishing attack.

We request information regarding, *inter alia*,

(1) the date and nature of all attacks, as well as which ICANN systems were compromised,
(2) actions taken internally by ICANN upon being notified of the attacks,

[1] See *ICANN targeted in spear-phishing attack*, https://www.icann.org/news/announcement-2-2014-12-16-en.
[2] See *IANA Systems not compromised*, https://www.icann.org/news/announcement-2014-12-19-en.

(3) what departments or members of staff are responsible for security and their role in the event of cyber-attacks,
(4) the role and responsibility of the ICANN-CIRT in responding to cyber-attacks (and when policies or manuals exist for the same; if so, please share them),
(5) what entities external to ICANN are involved in the identification and investigation of cyber-attacks on ICANN (for instance, are the police in the jurisdiction notified and do they investigate? If so, we request copies of complaints or information reports),
(6) whether and when culprits behind the ICANN cyber-attacks were identified, and
(7) what actions were subsequently taken by ICANN (ex: liability of ICANN staff for security breaches should such a finding be made, lawsuits or complaints against perpetrators of attacks, etc.).

Finally, we also request information on the role of the ICANN Board and/or community in the event of such cyber-attacks on ICANN. Also, when was the ICANN-CIRT set up and how many incidents has it handled since its existence? Do there exist contingency procedures in the event of compromise of IANA systems (and if so, what)?

We hope that our request will be processed within the stipulated time period of 30 days. Do let us know if you require any clarifications on our queries.

Thank you very much.

Warm regards,
Geetha Hariharan
Centre for Internet & Society
W: http://cis-india.org
T: Contact Information Redacted
E: