New gTLD Applicant and GDD Portal Issue: Questions & Answers / Information for RySG

INFORMATION REQUESTED BY THE REGISTRY STAKEHOLDER GROUP

(Discussed on 10 June 2015 at 20:00 UTC Registry Stakeholder Call)

Reporting and Communications

Q1: When did ICANN become aware of the incidents?
A1: As previously reported, a user notified us on 27 February.

Q2: How did ICANN become aware of the incidents?
A2: As previously reported, a user notified us on 27 February.

Q3: Did ICANN report the incidents to any government or law enforcement agency? If so, when and to whom?
A3: Not at this time. However, ICANN reserves all of its rights with respect to the portal issue. By reserving its rights, ICANN is leaving the door open to various actions that may be taken with respect to any unauthorized access.

Q4: Why did ICANN take so long to inform the affected Applicants and Registry Operators?
A4: ICANN used the time period between 30 April 2015 and 27 May 2015 to afford users whose login credentials were used to view data belonging to other portal users ample time to provide a fulsome account of their activities and to provide certifications. We also used this time to verify that access was authorized in certain instances.

Q5: ICANN correspondence to Applicants and Registry Operators was marked "CONFIDENTIAL". Yet, in some cases, letters were sent to outdated contact person or entity. Why? What was ICANN's intent?
A5: The letters were marked "confidential" as they were communications from ICANN to the primary contact for the applicant or registry operator. Primary contact information is maintained by the applicants and contracted parties. This is the information we used to identify the primary contact.

Q6: Would ICANN provide a detailed chronology (including (a),(b),(c), (d) above) for all major security incidents or technical glitches that have affected TAS, CZDS, RADAR and any other ICANN core systems and "lessons learned" from those incidents?
A6: Please refer to the following links for information on the chronology of recent events:

- TAS, April 2012:
  - https://www.icann.org/news/announcement-2012-04-12-en.
  - http://newgtlds.icann.org/en/applicants/tas/interruption-faqs.

- CZDS, April 2014:
  - https://www.icann.org/resources/pages/czds-2014-03-03-en (See "CZDS News.")
- RADAR, May 2014:
  - https://www.icann.org/news/announcement-2-2014-05-28-en.
- Spearphishing attack, November 2014:
  - https://www.icann.org/news/announcement-2-2014-12-16-en.

Read more information on current and planned IT activities at https://www.icann.org/news/blog/hardening-icann-s-it-and-digital-services.

Product Testing and Launch and Management Oversight

Q7: What were the acceptance testing procedures for the two portals (the New gTLD Applicant and the GDD Portal customized from Salesforce software) before they were rolled out?

A7: *Applicant Portal*: This was developed by a third-party. At that time ICANN did not have a QA team, so all unit, functional and integration testing was conducted by the contractor. The users conducted functional user-acceptance tests in conjunction with the partner prior to rollout. ICANN IT was not directly involved in any development or testing; it supported data migration only. Data validity was confirmed by ICANN IT.

GDD Portal: This was developed by a third-party leveraging the existing framework from the Applicant Portal. At that stage, ICANN did have a QA team that was transitioning from the third-party to ICANN staff. Testing at that time was focused on functionality and data-integrity only. Full user-acceptance testing was performed by ICANN users prior to roll-out.

Q8: Who (ICANN staff/executive) signed off before they went live?

A8: ICANN staff, including members of the Global Domains Division executive team, approved the launch of the portals.

Q9: How does ICANN Management ensure proper oversight over its systems and data security obligations?

A9: ICANN has procedures in place and is accelerating its efforts to harden its systems. For more specific information, please refer to the blog published at https://www.icann.org/news/blog/hardening-icann-s-it-and-digital-services.

Q10: For future IT related RFPs, would ICANN consider a public comment period or other mechanisms to give the community an opportunity to provide comment or input to ensure their design and functionality are cost-effective and meet the need of users.

A10: ICANN follows its published Procurement Guidelines, which are intended to ensure that products and services are purchased with the correct specifications, at the appropriate level of quality and for the appropriate value. For more information on the methodology and related information including Request for Proposals, please refer to ICANN's procurement guidelines published at https://www.icann.org/en/system/files/files/procurement-guidelines-21feb10-en.pdf.

ICANN Investigation and Findings

Q11: How can ICANN be sure that other systems were unaffected, and that only specific data records were accessed? Are findings to date based upon audit logs or other WORM data recording mechanisms?

A11: The systems that house this application are isolated physically and logically from other systems. There is no shared network, data or authentication with any other system. For additional information, please refer to the 27 May 2015 announcement published at https://www.icann.org/news/announcement-2015-05-27-en.

Q12: Would ICANN provide a more detailed description of the methodology used by those who analyzed the data?

A12: At this point we are not providing this level of detail.

ICANN Enterprise Risk Management and Data/ Systems Security

Q13: When was the last enterprise risk audit carried out on ICANN' IT systems before the incident?

A13: An audit was conducted in June-July 2014 by a third-party. This resulted in a 16-project roadmap for FY15 and part of FY16. Our most recent annual audit was conducted by a third-party this in May-June 2015. For more information, please visit:

- RFP, 23 April 2014 "Information Security Assessment": https://www.icann.org/resources/pages/governance/rfps-en.
- Blog post, 1 July 2015: https://www.icann.org/news/blog/ciio-perspectives-volume-3.
- Blog post, 9 June 2015: https://www.icann.org/news/blog/hardening-icann-s-it-and-digital-services.

Q14: Did any audits prior or after the incident identify security vulnerability of these two portals? If so, what has been done to mitigate? When was the last enterprise risk audit carried out on ICANN' IT systems before the incident?

A14: As noted above, ICANN engaged a third-party to assess its systems in June-July 2014. We took the individual recommendations and sorted them in many ways. This resulted in a 16-project roadmap for FY15 and part of FY16. Our most recent audit by a third-party was conducted in May-June 2015.

On a concurrent but separate track, ICANN recently engaged the services of an expert-knowledge firm to review our Salesforce.com implementation. The review highlighted several areas where we could harden our platform. We have since released multiple software patches to address these issues. We expect to complete all work no later than the end of calendar year 2015. For more information, please visit:

- Blog post, 1 July 2015: https://www.icann.org/news/blog/ciio-perspectives-volume-3.
- Blog post, 9 June 2015: https://www.icann.org/news/blog/hardening-icann-s-it-and-digital-services.

Q15: Was the decision to outsource IT services to one vendor (https://www.icann.org/resources/board-material/resolutions-2015-04-26-en#2.h) resulted from a recommendation by an enterprise risk audit?

A15: No. It was a business decision to reduce complexity and enhance management control. We consolidated services from eleven different vendors into a single vendor.

- "IT Services Outsourcing RFP" issued on 11 August 2014: https://www.icann.org/resources/pages/governance/rfps-en.

Q16: What measures and processes have been put in place as safeguards against unauthorized access to or use of personal data or sensitive business information and to ensure coordination between internal staff/functions and outsourced IT service providers with clear roles and responsibilities? How will they be reviewed and updated to stay "ahead of the game"?

A16: ICANN sincerely regrets this incident. We continue to deploy security-based updates on a regular basis. Enhancing the security controls and privacy of the ICANN portals is part of a broader, multi-year effort to harden all of ICANN's digital services. For additional information, read the blog post published at https://www.icann.org/news/blog/hardening-icann-s-it-and-digital-services.

Q17: How does ICANN plan to continually monitor the integrity of its systems going forward?

A17: As indicated above, we continue to deploy security-based updates on a regular basis. Enhancing the security controls and privacy of the ICANN portals is part of a broader, multi-year effort to harden all of ICANN's digital services. For additional information, read the blog post published at https://www.icann.org/news/blog/hardening-icann-s-it-and-digital-services.

Q18: What remedies might be available to affected Applicants or Registry Operators?

A18: Our ultimate goal is to provide the ICANN community with flawless services. We have started work to achieve this goal by baselining everything we have – services, platforms, security, people, processes etc. ICANN is committed to improving our performance continually, and to reporting on our progress periodically. An example of this is the blog post published at https://www.icann.org/news/blog/hardening-icann-s-it-and-digital-services.

NEW GTLD APPLICANT AND GDD PORTAL ISSUE QUESTIONS & ANSWERS (*Published 2 March 2015*)

Q1: What is the nature of this issue?

A1: An issue was reported that could potentially affect users of the New gTLD Applicant and GDD (Global Domains Division) portals. Under certain circumstances, an authenticated portal user could potentially view data of, or related to, other users. Access to, and data in, these portals is limited to New gTLD Program applicants and New gTLD registry operators.

Q2: How was the issue addressed?

A2: The configuration was updated to address the reported issue.

Q3: Was any data exposed to an unauthorized party?
A3: There is currently no indication that this issue resulted in any actual exposure of data to an unauthorized party. We are continuing to investigate.

Q4: Did an unauthorized party access the portals?
A4: There is no indication, at this time, that anyone other than those authorized to access the portals did so.

Q5: What type of information is in these portals?
A5: These portals contain information from applicants to ICANN's New gTLD Program and New gTLD registry operators such as attachments to new gTLD applications or other forms submitted by applicants and/or registry operators.

Q6: What are the New gTLD Applicant and GDD portals?
A6: They make up a system that can be accessed only by New gTLD Program applicants and ICANN's New gTLD registry operators. It is not a system that is open and available to the general public. Authenticated applicants use the portals to carry out evaluation and contracting processes.

Q7. Why did you take the portals offline?
A7: An authorized user notified us about the issue on 27 February 2015. Upon notification, the team confirmed the reported issue and took the portals offline to address the issue.

Q8: What is the current status of the system?
A8: Access to the New gTLD Applicant and GDD portals was restored on 2 March 2015.

Q9: When will you give us additional information?
A9: We will provide updates as the investigation continues.

Q10: What if I have further questions?
A10: If you have further questions, please send an email to customerservice@icann.org. Updates will be published at https://www.icann.org/news and http://newgtlds.icann.org/en/announcements-and-media/latest.