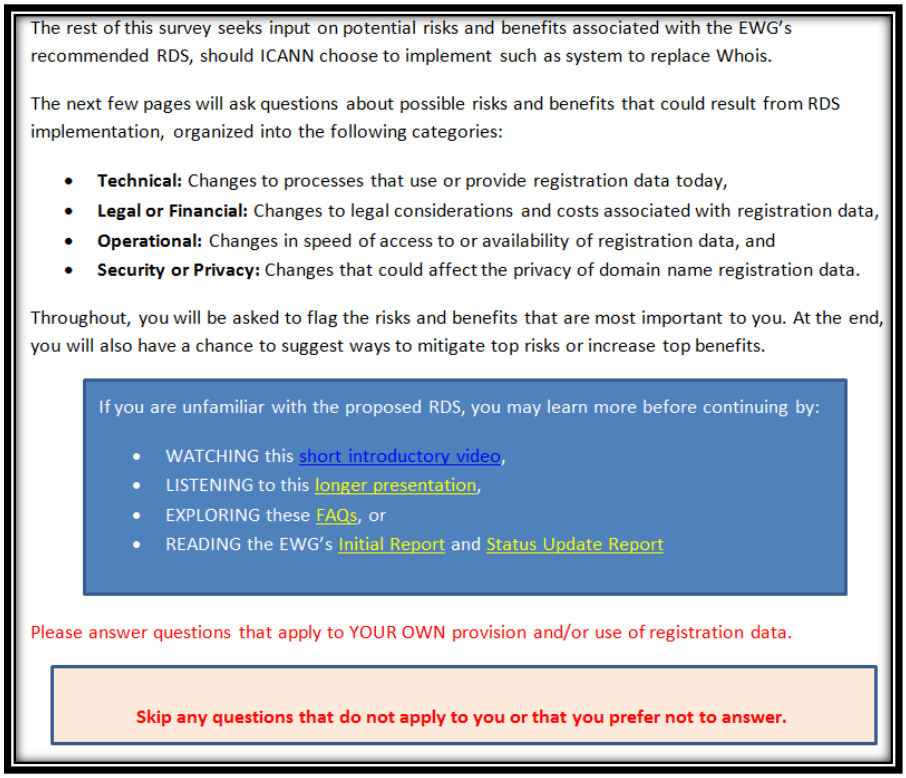
Pesquisa de riscos do RDS – Resumo dos resultados

Em março de 2014, o grupo de trabalho de especialistas sobre serviços de diretório de gTLDs (EWG) convidou todas as partes que fornecem ou usam dados de registro de nomes de domínio de gTLD a participar de uma pesquisa de riscos do RDS, incluindo registrantes, registradores, registros e a ampla variedade de pessoas, empresas e outras organizações que atualmente usam os dados do WHOIS. Essa pesquisa ofereceu aos participantes uma oportunidade de contar ao EWG os riscos e vantagens que o serviço de diretório de registro (RDS) de última geração poderia proporcionar-lhes.

Este documento resume os riscos e vantagens do RDS identificados por meio dessa pesquisa. O EWG utilizou as respostas a essa pesquisa para identificar e reduzir riscos imprevistos e desnecessários durante a preparação de seu relatório final (publicado em 6 de junho de 2014). O EWG também recomendou que essas respostas fossem utilizadas como contribuição ao realizar uma futura avaliação de riscos completa no RDS proposto.

Desenho da pesquisa

A introdução mostrada abaixo define a etapa fornecendo o histórico para quem não está familiarizado com o RDS e agrupando os riscos e vantagens em 4 categorias:



The rest of this survey seeks input on potential risks and benefits associated with the EWG's recommended RDS, should ICANN choose to implement such as system to replace Whois.

The next few pages will ask questions about possible risks and benefits that could result from RDS implementation, organized into the following categories:

- **Technical:** Changes to processes that use or provide registration data today,
- **Legal or Financial:** Changes to legal considerations and costs associated with registration data,
- **Operational:** Changes in speed of access to or availability of registration data, and
- **Security or Privacy:** Changes that could affect the privacy of domain name registration data.

Throughout, you will be asked to flag the risks and benefits that are most important to you. At the end, you will also have a chance to suggest ways to mitigate top risks or increase top benefits.

If you are unfamiliar with the proposed RDS, you may learn more before continuing by:

- WATCHING this short introductory video,
- LISTENING to this longer presentation,
- EXPLORING these FAQs, or
- READING the EWG's Initial Report and Status Update Report

Please answer questions that apply to YOUR OWN provision and/or use of registration data.

Skip any questions that do not apply to you or that you prefer not to answer.

Para cada categoria, foram mostrados aos entrevistados exemplos de possíveis riscos e vantagens, e foi-lhes solicitado o seguinte:

- *Selecione TODOS os riscos técnicos que podem afetar VOCÊ.*
- *Selecione DOIS (2) riscos que mais poderiam afetar você.*
- *Selecione DOIS (2) riscos com a maior probabilidade de ocorrência.*
- *Selecione QUALQUER risco do RDS recentemente apresentado que não seja um risco já conhecido do Whois.*

-- Publicado em 28 de julho de 2014 --

Pesquisa de riscos do RDS – Resumo dos resultados

Os entrevistados também foram incentivados a adicionar outros riscos e vantagens possíveis. Este resumo das respostas da pesquisa identifica os riscos e vantagens citados com maior frequência, juntamente com as adições indicadas por escrito.

Visão geral das respostas

Esta pesquisa inicial de riscos do RDS foi realizada em inglês, coletando 182 respostas parciais até 12 de junho de 2014. Mais de 100 entrevistados concluíram a pesquisa toda.

Todas as respostas, exceto uma, foram enviadas antes da publicação do relatório final do EWG. Como tal, esses resultados oferecem feedback sobre o RDS conforme foi proposto no relatório de atualização do EWG (11 de novembro de 2013) e apresentado na ICANN48 em Buenos Aires. Esses resultados não devem ser exibidos como feedback sobre as propostas finais do RDS detalhadas no relatório do EWG de junho de 2014. Não obstante, essas respostas ajudaram o EWG a entender o que os usuários e provedores de dados do Whois consideram potencialmente significativo e impactante, além dos possíveis riscos e vantagens associados a *qualquer* RDS de última geração.

Dados demográficos dos entrevistados

- Representação global, incluindo América do Norte (68%), Europa (35%), Ásia (20%), América Latina (14%), África (12%) e Oceania (10%)[1]
- Divididos igualmente entre aqueles que USAM e FORNECEM dados de registro:
    - 84% usam dados de registro solicitados do Whois
    - 63% contribuem com dados e 24% coletam, armazenam ou transmitem dados do Whois
    - Entre aqueles que USAM os dados, há registrantes (45-57%), usuários individuais da Internet (50%), usuários comerciais da Internet (50%), equipe técnica da Internet (40%), pesquisadores da Internet (41%), investigadores da OpSec (36%), detentores de propriedade intelectual (27%), outros investigadores (14%), órgãos responsáveis pela aplicação da lei (5%) e aproximadamente 20 outros.
    - Entre aqueles que FORNECEM dados, há pessoas físicas (65%), pessoas jurídicas (59%), registradores (14%), registros (9%), provedores de serviços de procuração (5%) e terceiros (5%).

Riscos técnicos do RDS

- Possíveis impactos técnicos negativos citados com maior frequência (104 respostas):
    1. Eu poderia não ter mais acesso público anônimo a todos os dados de registro (69).
    2. O credenciamento para acesso a dados bloqueados poderia ser trabalhoso (65).
    3. Minhas práticas de acesso a dados de registro poderiam precisar de mudanças (62).
- Riscos identificados como os mais impactantes/mais prováveis: 1 e 2 acima.
- Além dos riscos listados explicitamente, mais riscos técnicos identificados:
    - O novo RDS poderia afetar as partes que fornecem Whois (8) histórico e inverso
    - O acesso automático poderia não estar mais disponível (6)

[1] Observação: várias respostas são permitidas; o total é superior a 100%

- Não seria possível obter informações sobre criminosos, parceiros comerciais ou solicitantes (3)
- O tempo de resposta para obter dados ou para o registro poderia aumentar (2)
- Os direitos de privacidade poderiam ser violados (2)
- Fonte única de falha/riscos técnicos SAC061 (2)
- Informações em lote para organismos encarregados do cumprimento da lei e spammers – dois grupos com maior incidência de abuso
- Os dados pesquisáveis publicamente desaparecerão
- Os [logins] que posso usar poderiam precisar ser alterados inicialmente e durante o processo, devido à rotação de pessoal
- Transferência/migração
- Questão interjurisdicional apresentada
- Não há um exame público detalhado dos dados de registro nos registradores que tolere dados falsos
- As alterações dos dados de registro podem exigir certificados SSL
- Quebra o modelo de DNS autorizado
- Eu perco a visibilidade de registro de quem está acessando meus dados pessoais em algumas circunstâncias
- Perco a possibilidade de controlar ou limitar o acesso a minhas informações diretamente
- Custos de desenvolvimento, garantia de qualidade (QA), revisão e atualização, sem receita para compensá-los

Observação geral: os entrevistados identificaram todos esses riscos como técnicos, mas muitos estão realmente englobados como outros tipos de riscos, computados em outras partes desta pesquisa.

Vantagens técnicas do RDS

- Possíveis impactos técnicos positivos citados com maior frequência (89 respostas):
  1. Os dados de registro que acesso poderiam ser mais precisos (58).
  2. O acesso aos dados de registro poderia ser mais uniforme e consistente (56).
  3. Eu poderia ter um melhor acesso aos dados bloqueados de que realmente preciso (41).
- Vantagens identificadas como as mais impactantes/mais prováveis: 1 e 2 acima
- Além das vantagens listadas explicitamente, foram identificadas outras vantagens técnicas:
  - Aumento na precisão dos dados (por meio do gerenciamento e validação dos contatos)(8)
  - Meus dados poderiam ser acessados por quem tiver direito legal para isso, em lugar de serem publicados para que todo mundo os veja
  - Eu poderia identificar mais facilmente os invasores cibernéticos reincidentes e em série antes de iniciar um processo judicial ou uma denúncia à UDRP e, com isso, economizar fundos e recursos de meus clientes
  - Sempre deverei fornecer a porta 43 de Whois, mas isso não é um problema

- Os dados de registro acessados provavelmente serão mais aplicáveis, úteis e significativos
- A transferência de domínio entre os registrantes será mais fácil (os dados do WHOIS permanecerão os mesmos e não será mais necessário dividir o resultado do Whois)
- Redução do impacto negativo devido à exploração de dados em grande escala - por exemplo, menos spam

Riscos jurídicos e financeiros do RDS

- Possíveis **impactos jurídicos e financeiros negativos** citados com maior frequência (102 respostas):
  1. A quantidade de dados de registro disponíveis gratuitamente a todos poderia diminuir (68).
  2. Meu custo total por obter dados de registro poderia aumentar (66).
  3. A notificação ou o registro de acessos do RDS poderia comprometer as investigações ativas (51).
- Risco identificado como o mais impactante/mais provável: 1 acima
- Além dos riscos listados explicitamente, foram identificados outros riscos jurídicos e financeiros:
  - Poderia dificultar o rastreamento de infratores de marcas comerciais ou spammers. (3)
  - O tempo utilizado para o acesso aos dados poderia ser maior (3)
  - Sem o acesso público a todos os dados, eu poderia fazer menos inovações de valor agregado.
  - Excessivos TLDs novos provocam o aumento dos custos e muitos registros de má fé.
  - A falta de transparência dos proprietários do site (especialmente os sites comerciais com transações monetárias ou contribuições de dados pessoais) pode ser um risco para os consumidores.
  - Pode ser difícil confirmar as informações sobre outros domínios que o registrante tiver ao confirmar a qualificação no domínio restrito.
  - A falha não seria localizada. Um alvo para 'ataques' jurídicos, DOS, de controle e outros
  - Poderia ser solicitado que eu fornecesse informações não existentes (por exemplo, endereço físico para correspondência, pois existem pessoas sem residência fixa que têm nomes de domínio registrados)
  - A criação de um monopólio dos dados do Whois reprimirá a inovação e centralizará demais o poder sobre a "lista telefônica" da Internet em um local.
  - Em algumas situações, o fato de eu estar bisbilhotando não é um dado que eu gostaria de compartilhar, nem mesmo com pessoas que poderiam ser confiáveis em outras circunstâncias.
  - Quero que meus dados do Whois estejam disponíveis a todas as partes interessadas como estão agora
  - Os registros da UE e de outros lugares com leis de proteção de dados não poderão exportar dados ao RDS, diminuindo consideravelmente sua utilidade.

- A carga dos custos e uma possível desvantagem jurídica são colocadas sobre os registrantes, registradores e registros com uma vantagem mínima para as partes afetadas e máxima para outros.

Vantagens jurídicas e financeiras do RDS

- Possíveis **impactos jurídicos e financeiros positivos** citados com maior frequência (68 respostas):
  1. O aumento na qualidade dos dados de registro poderia reduzir as custosas ineficiências (42).
  2. O cumprimento contratual das obrigações relacionadas aos dados poderia ser mais forte (35).
  3. Poderia ser mais fácil obter acesso legal aos dados de registro bloqueados (35).
- Vantagens identificadas como as mais impactantes/mais prováveis: 1 e 2 acima
- Além das vantagens listadas explicitamente, foram identificadas outras vantagens jurídicas e financeiras:
  - O meu risco de ter grandes quantidades de dados pessoais (inclusive dados comerciais que envolvem pessoas) diminuirá dramaticamente.
  - Fazer conexões facilmente entre os proprietários de domínios e as redes de detecção
  - Eu poderia transferir a culpa à ICANN ou ao provedor do RDS pela falta de transparência e ficar menos responsável.

Riscos operacionais do RDS

- Possíveis **impactos operacionais negativos** citados com maior frequência (87 respostas):
  1. Meu acesso aos dados de registro poderia ser impedido por falha do RDS (68).
  2. Meu acesso aos dados bloqueados poderia ser demorado pelo credenciamento lento (66).
  3. Meu acesso aos dados de registro poderia ser mais lento pelos gargalos do RDS (65).
  4. Os dados de registro retornados pelo RDS poderiam não estar sincronizados com as atualizações recentes (56).
- Riscos identificados como os mais impactantes/mais prováveis: 2 e 3 acima
- Além dos riscos listados explicitamente, foram identificados outros riscos operacionais:
  - A transmissão e revelação de respostas dos serviços de procuração e privacidade credenciados poderiam ser mais longas (7)
  - Nossa empresa estaria em perigo de acordo com as decisões de políticas do RDS.
  - O acesso bloqueado ao público não permite a transparência dos consumidores para quem eles estão pagando por serviços ou ao inserir informações pessoais
  - Violação de dados
  - Pode haver aumento da dificuldade/demora ao lidar com spam/ataques/problemas da rede vindos de fontes externas.
  - Os dados bloqueados para o nível de credenciamento podem não cumprir os requisitos reais.
  - Regras arbitrárias evitarão necessidades de acesso válido.

-- Publicado em 28 de julho de 2014 --

- Desejo que TODAS as partes tenham acesso a MEUS dados usando a tecnologia estabelecida atualmente.
- Sites desonestos que operam por meio de programas de afiliados da rede serão mais facilmente protegidos contra os organismos encarregados do cumprimento da lei, provedores de serviços e os consumidores que foram enganados.
- Deve-se implementar e manter o novo processo e sistema quando o status quo não for quebrado.
- Mais tempo, receitas e oportunidades perdidos pelo aumento do contato inicial por parte de consultores de IP sem experiência que utilizarão de forma errada ou não aproveitarão adequadamente o novo sistema.

Vantagens operacionais do RDS

- Possíveis **impactos operacionais positivos** citados com maior frequência (61 respostas):
  1. A transferência e a revelação das respostas das procurações credenciadas poderiam ser mais curtas (40).
  2. Eu poderia ter acesso a dados de registro de alta velocidade e mais confiável (40).
  3. O acesso autenticado em tempo real aos dados bloqueados poderia ser mais rápido do que atualmente (39).
  4. O tempo de resposta do RDS poderia ser mais uniforme e previsível do que no Whois (35).
- Vantagens identificadas como as mais impactantes/mais prováveis: 2 e 4 acima.
- Além das vantagens listadas explicitamente, foram identificadas outras vantagens operacionais:
  - O RDS agregado pode ser mais compatível com recursos como WhoWas e Whois inverso (7)

Riscos de segurança e privacidade do RDS

- Possíveis **impactos de segurança e privacidade negativos** citados com maior frequência (70 respostas):
  1. Meus dados de registro poderiam ser mais vulneráveis a ataques externos (40).
  2. Meus dados de registro poderiam ser mal utilizados pelo operador do RDS (40).
  3. Eu poderia ter que fornecer uma identidade verificável para registrar um domínio de gTLD (24).
- Riscos identificados como os mais impactantes/mais prováveis: 1 e 2 acima
- Além dos riscos listados explicitamente, foram identificados outros riscos de segurança e privacidade:
  - Os "usuários individuais da Internet" geralmente são proprietários de direitos e devem ter a possibilidade de acessar o registro relevante para investigar a violação on-line (5)
  - Preocupação de que os usuários individuais que necessitam ter acesso poderiam ser excluídos
  - O fornecimento de um e-mail ou número de telefone válido é essencial para que os proprietários de direitos investiguem a violação

- Minhas consultas de dados de registro poderiam ser mal utilizadas pelo operador do RDS.
- Eu poderia ter de comprometer direitos que tenho como pessoa jurídica ou física tendo que escolher entre uma ou outra -- quando o registro e uso do meu nome de domínio são claramente compatíveis com ambos. Portanto, seria solicitado que eu renunciasse aos direitos de uma categoria de direitos, embora eu tenha legalmente direito aos benefícios de ambas.
- Risco da privacidade pessoal de que meus dados se tornem mais disponíveis como administrador do nome de domínio
- Perda de registros devido aos requisitos adicionais; as empresas em formação podem não ter identificadores comerciais etc., mas ainda necessitam de um domínio.
- Os agressores externos agora terão um grande alvo piscando em vermelho.
- Minha identidade pessoal pode ser forçadamente associada a um domínio pertencente a e controlado pela entidade corporativa, e não por mim pessoalmente
- Organizações e indivíduos maliciosos aproveitarão a possibilidade de ocultar suas informações nos dados bloqueados, tornando mais difícil que os funcionários de segurança e conformidade os investiguem com sucesso.
- Não posso registrar um domínio anonimamente
- Ter de revelar meus motivos para acessar dados. Eles são legítimos, mas são assunto meu, e não da ICANN.
- Os dados de registro poderiam estar menos acessíveis aos atores de segurança, marca e outros organismos encarregados pelo cumprimento da lei do setor privado.
- Meus dados de registro estarão mais vulneráveis a terceiros, incluindo aqueles que lidam com funções de segurança privada para empresas privadas e que querem mais acesso às informações pessoais e confidenciais em vários gTLDs.
- Possibilidade de ser citado em um processo judicial como resultado da disponibilidade de meu nome com a empresa
- A oferta de acesso em camadas ao organismo encarregado do cumprimento da lei é uma forma de oferecer acesso extra, e é uma via para ordens judiciais e intimações. Não é o tipo de oportunidade ou processo com o qual a ICANN deva envolver-se.
- Futuras decisões da política de dados de registro poderiam ser tomadas por uma única entidade.
- O acesso de terceiros poderia infringir as leis locais, a retenção de dados ou a privacidade e apresentar exposição jurídica ao cliente sem meu conhecimento.
- O acesso de terceiros ou a concessão de dados armazenados poderia criar uma ferramenta poderosa para uso abusivo de meus dados ou os dados do meu cliente.
- O novo sistema pode ser um novo vetor de ataque.

Vantagens de segurança e privacidade do RDS

- Possíveis **impactos de segurança e privacidade positivos** citados com maior frequência (55 respostas):
    1. Meus dados de registro poderiam ser melhor protegidos contra o mau uso (37).

2. Meus dados de registro poderiam estar seguros de maneira mais uniforme (31).
3. Eu poderia publicar um ID de contato reutilizável em lugar do meu nome (29).
4. Uma parte menor de meus dados de registro poderia estar disponível de forma pública e anônima (27).

- Vantagens identificadas como as mais impactantes/mais prováveis: 2 e 3 acima.
- Além das vantagens listadas explicitamente, foram identificadas outras vantagens de segurança e privacidade:
  - As regras de validação, autenticação e autorização serão aplicadas de forma consistente e podem ser facilmente auditadas (7)
  - Eu faria a atualização de minhas informações de contato para que fossem mais precisas, já que meus assediadores não teriam acesso a elas
  - Necessário para oferecer certificação jurídica ou física
  - Melhor acesso aberto à entidade jurídica

Mais percepções

Os entrevistados ofereceram 30 comentários sobre **riscos inevitáveis**, elaborando os riscos identificados anteriormente:

1. O acesso aos dados de registro atualmente disponíveis gratuitamente diminuirá.
2. Os riscos 5a, 5b, 9b (alteração nas práticas, redução no acesso público disponível gratuitamente) são inerentes ao RDS.
3. Qualquer entidade que controle um ponto de acesso central singular para recuperar dados de registro sempre terá um poder excessivo sobre um bem público.
4. A questão do acesso ilimitado aos dados, até mesmo por quem tem credenciais, é um assunto que a comunidade precisa entender melhor. Um grande risco é que o RDS provavelmente não verificará pesquisas de grande amplitude por parte de atores do estado e terceiros.
5. Se a arquitetura falhar, nós não teremos acesso disponível às informações. Ou o acesso de credenciamento leva muito tempo.
6. Possibilidade de obter informações de maneira eficiente e oportuna (para apoiar os clientes que realizam investigações de sites desonestos)
7. Possibilidade de proteger os consumidores de compras e/ou a inserção de dados pessoais em sites desonestos (devido à falta de transparência do proprietário do site)
8. O armazenamento e fornecimento centralizado do Whois para todos os registros em qualquer tipo de banco de dados (em lugar dos registradores e registros) aumenta a exposição às violações de dados.
9. Um sistema como este será um ímã para aqueles que desejem hackear bancos de dados, o que pode resultar na repetição de serviços lentos e interrupções.
10. Acredito que é possível que alguém forneça algumas informações corretas na hora do registro, mas como isto será mantido?
11. A conformidade com as regulamentações da ICANN não é o único motivo para oferecer acesso ao WHOIS. Na prática, o registro sempre deverá fornecer acesso ao WHOIS na porta 43 e na porta 80, aumentando o custo e o risco.
12. O RDS quebra um princípio fundamental da Internet - devolução do poder e controle. Ele faz isso apresentando numerosas questões interjurisdicionais novas de maneira tecnicamente deficiente.
13. Ignora os seguintes problemas: 1) como encontro um servidor de Whois para uma área; 2) domínios "privados" abertos para registro "público"; 3) a base instalada, práticas e ferramentas existentes.
14. O novo mecanismo determina que muitos dados sejam ocultos. Isso levará a um aumento do risco para o público, já que os domínios [problema] não serão acionados e encaminhados. A evidência também seria perdida para os organismos encarregados do cumprimento da lei.

15. O sistema atual exige que seja fornecida uma grande quantidade de dados. Esses dados são vulneráveis à captura no envio ou no armazenamento por parte quem tem uma posição ética ambígua, bem como de quem tem objetivos ilegais.
16. Quando os seres humanos estão envolvidos, as falhas são inerentes ao sistema.
17. A centralização do controle sobre quem pode acessar os dados de registro do nome de domínio e o requisito de algum tipo de validação da pessoa ou entidade que acessa os dados de registro do nome de domínio geram um risco inevitável de monopólio e redução da possibilidade de que os organismos encarregados do cumprimento da lei e os investigadores de segurança identifiquem efetivamente comportamentos abusivos na Internet. Esses riscos parecem inevitáveis [em qualquer modelo].
18. Um processo de registro de domínio mais lento em geral será inevitável se os dados de registro agora precisarem ser validados.
19. O RDS propõe estender o acesso bloqueado aos organismos encarregados do cumprimento da lei de todos ou da maioria dos países. Portanto, seu verdadeiro objetivo é expor os registrantes individuais à investigação por parte de organismos externos, a quem eles não têm nenhuma obrigação de obedecer nem motivos legítimos para submeter-se. Portanto, o RDS inerentemente contém falhas.
20. Qualquer mecanismo para registros anônimos sofrerá abuso. Forçar os transgressores a registrar-se com um DBA e uma caixa postal pelo menos oferecerá uma pequena barreira à entrada ao registro de domínio com fins criminais.
21. O acesso aberto e o impedimento da replicação em lotes dos dados de registro são práticas opostas aos interesses da exploração do registro de domínio; portanto, é inevitável que qualquer novo RDS estabelecido pela ICANN "corrija" esses "problemas" com o Whois atual.
22. Fica claro que os autores do relatório estão altamente focados na proteção da privacidade de um número relativamente pequeno de registrantes de domínio com necessidades especiais de privacidade. No entanto, os casos legítimos desse tipo são muito poucos… As alterações propostas obstruirão enormemente o trabalho dos "idealistas" e resultarão em um ecossistema de domínio mais propenso ao abuso e com maior probabilidade de ser preenchido com dados imprecisos e sem utilidade.
23. Ter Big Data é obviamente um risco maior que não pode ser completamente evitado.
24. Qualquer centralização de dados apresenta o risco inevitável de um ponto único de falha: hackers, criminosos cibernéticos e entidades mal intencionadas, como governos rebeldes ou governos que desrespeitam os direitos humanos e civis, só precisam procurar as informações privadas em um único lugar.
25. Qualquer restrição do acesso público às informações sobre a identidade de um proprietário de domínio dificulta mais a pesquisa contra malware e spam.
26. Pelo espantoso histórico da ICANN em operações e conformidade, é completamente improvável que isso funcione.
27. Meus dados de registro serão localizados em outro país, em cuja jurisdição eu não confio.
28. Parece que o novo sistema do RDS melhorará consideravelmente a privacidade do registro de dados, promovendo, assim, o discurso livre, que, em minha opinião, constitui o fundamento e a beleza da Internet. Minha única preocupação em termos de riscos inevitáveis é em relação aos operadores e funcionários, bem como às pessoas e organizações que terão ou poderiam ter acesso ilimitado e/ou sem controle a todos os dados de registro.
29. O serviço centralizado é arriscado e desnecessário, além de colocar a ICANN em complicados problemas jurídicos que podem ser evitados. Vejamos algumas outras soluções possíveis.
30. Independentemente do tipo ou estrutura de teatro kabuki que possa acompanhar onde o RDS foi originado ou o que ele possa minimamente oferecer como vantagem a qualquer um, além dos interesses dos organismos encarregados do cumprimento da lei ou TM, este RDS será visto como uma fonte de dados da qual os governos abusarão.

13 entrevistados forneceram respostas detalhadas e justificadas sobre os **riscos aceitáveis**:

Pesquisa de riscos do RDS – Resumo dos resultados

1. O risco é aceitável dependendo dos recursos técnicos que existem atualmente (computação de alto desempenho, distribuição baseada em nuvem e tecnologia de failover para aumentar a disponibilidade etc. (5)
2. Desde que seja desenvolvido com técnicas geralmente aceitas projetadas para garantir a disponibilidade e segurança, as preocupações serão atenuadas.
3. Os sites não comerciais (que não têm função de e-commerce ou requisitos de entrada de dados) apresentam menos risco aos consumidores e a quem se esforça por protegê-los (empresas, organismos encarregados do cumprimento da lei etc.). Menos transparência nesses sites seria aceitável.
4. A possibilidade de abordar diferentes leis de privacidade é um risco aceitável que pode afetar os negócios.
5. O risco de violação da segurança dos dados de acesso bloqueado é aceitável, já que o risco ainda é menor do que no atual banco de dados do WHOIS público.
6. O risco de Big Data pode ser aceitável com um desenho cuidadoso e supervisão operacional. A falta de acesso às informações necessárias por nível de acesso bloqueado pode ser melhorada por uma cuidadosa análise dos requisitos das partes interessadas.
7. A ICANN receberia menos 'taxas' como resultado da implementação do RDS. O RDS proposto reduzirá o volume de registro atual do mercado devido à forma prejudicial na qual um consumidor deve fornecer grandes quantidades de dados para poder realizar uma compra inicial.

24 formas de **reduzir ou mudar os riscos** foram sugeridas pelos entrevistados:

1. Medidas tomadas para melhorar a precisão
2. Os riscos de falha/gargalos do RDS devem ser gerenciáveis por meio de uma forte supervisão do operador do RDS.
3. Recursos de Whois/WhoWas inversos poderiam ser criados no RDS
4. A redução dos dados disponíveis gratuitamente poderia ser melhorada por meio de uma rigorosa análise dos elementos de dados atualmente públicos e somente eliminando o acesso público àqueles para os quais a necessidade dessa eliminação possa ser estabelecida objetivamente.
5. Elaboração de um processo leve de credenciamento que gere uma credencial persistente.
6. A identificação do uso de um nome deve ser justificada. A resposta deve ser baseada apenas na denúncia. Se a solicitação for válida, então poderá ser dada uma resposta.
7. O registrante receberá um aviso de que as informações foram solicitadas? E, nesse caso, identificará a parte solicitante?
8. Os principais riscos do RDS podem ser evitados apenas implementando os aspectos validadores no atual paradigma. Se for necessário que todos os dados de registro correspondam a um formato específico, isto pode ser realizado por uma política da ICANN, em vez de um novo RDS.
9. Talvez uma forma de diferenciar sites comerciais de sites não comerciais para oferecer mais transparência nos primeiros pudesse reduzir os riscos.
10. Pelo menos alguns dos riscos podem ser reduzidos utilizando uma abordagem agrupada onde cada registro armazene suas próprias informações.
11. Repensar todo o esquema e coletar dados de contato mínimos. Aplicar os princípios padrão de proporcionalidade, privacidade por desenho e privacidade por padrão.
12. Exigir limites de tempo razoáveis para as respostas aos contatos após os quais os domínios podem ser suspendidos pendentes de resposta.
13. Armazenar menos dados.
14. O acesso ao Whois pode e deve permanecer anônimo e aberto para todos os usuários da Internet.
15. Os tempos de processamento para validação dos dados de registro devem ser reduzidos o máximo possível, de modo que os administradores de domínios possam executar seus domínios de maneira eficiente e efetiva com mínimo tempo de espera devido aos procedimentos de validação.
16. Permitir a escolha dos consumidores na seleção de um provedor de validação seria sensato, para que os provedores fossem incentivados a manter baixos os custos e os tempos de processamento para serem competitivos.

-- Publicado em 28 de julho de 2014 --

17. Centralizar a validação com um pequeno grupo ou forçar a validação por meio de um provedor específico diminuirá o incentivo para manter o processo rápido e econômico.
18. Permitir o registro de domínio por qualquer um (não apenas por pessoas consideradas com necessidade de proteção por alguma organização) de forma completamente anônima, sem fornecer nenhum dado de registro. Se quase não houver dados de registro, não haverá problema com o acesso público a todos eles.
19. Eliminar o anonimato no registro.
20. Alguns riscos podem ser facilmente diminuídos por uma abordagem em fases para a implementação do RDS, por exemplo, tornando opcionais quaisquer requisitos de informações adicionais por um período e, ao mesmo tempo, disponibilizando dados na infraestrutura existente do WHOIS. Isso significará que o sistema de RDS pode desenvolver-se e qualquer bug/problema pode ser facilmente resolvido sem afetar o sistema existente. Portanto, uma vez que esteja estabelecido e que os problemas de integração tenham tido tempo suficiente para serem resolvidos, os registradores/registros podem realizar a mudança. Eu sugeriria que um período adequado para que os dados adicionais fossem opcionais e para a sobreposição dos serviços seria de aproximadamente 3 anos; isto proporcionaria tempo suficiente para alterar os sistemas e oferecer o treinamento adequado aos clientes.
21. Eliminar todos os registros de "procuração", exigir a precisão dos dados de registro, exigir que os registros restrinjam o acesso em lotes, exigir acesso aberto, mas limitado por taxas, ao Whois a todos os dados de registro e proibir a venda de dados de registro em lotes por parte dos registros e registradores.
22. Eliminar o incentivo financeiro para que os registradores ou outros vendam serviços de registro de privacidade. Atualmente é uma fonte de dinheiro, como foram os números de telefone não listados para as empresas de telefonia. Garantir que os registradores não ganhem *nada* ao oferecer serviços de registro do tipo de procuração ou privacidade. Garantir que os registrantes que tenham uma necessidade legítima de registro do tipo de privacidade ou procuração paguem uma taxa suficiente para demonstrar que realmente precisam desse serviço, com toda a arrecadação dessas taxas destinada a uma instituição pública de caridade (garantindo, assim, que a ICANN também não tenha nenhum incentivo para estimular os registros de procuração ou privacidade)
23. Uma melhor consulta sobre os dados solicitados em vez do nível de acesso bloqueado.
24. Para reduzir o risco de abuso de acesso aos dados de registro privados, esse acesso deve ser aprovado por documentos legais assinados por um juiz ou outra autoridade judicial.
25. Superar as percepções de Snowden/Kafka/Orwell do abuso geral por interesses fanáticos, tornando todos os acessos e solicitações ao sistema 100% transparentes para a visualização do público.
26. Superar a resistência a mudanças gerais, criar um método para aumentar as vantagens e reduzir as desvantagens para os registrantes, registradores e registros, como o uso de um sistema de validação centralizado para os registros.

13 entrevistados sugeriram formas nas quais os **riscos seriam bem compensados com vantagens**:

1. As possíveis vantagens dependem de como for implementado (2)
2. Qualquer risco associado à diminuição do acesso (atualmente gratuito e público) aos dados poderia ser reduzido se a comunidade garantisse uma maior precisão dos dados que requerem acesso bloqueado. A redução do acesso sem o aumento da precisão seria uma falha enorme em qualquer novo sistema proposto (2).
3. Embora um banco de dados agregado possa aumentar os riscos de segurança, estes podem ser melhorados por meio de um desenho e supervisão adequados, e um serviço ubiquitariamente disponível que exiba os resultados em um formato consistente poderia justificar esses riscos.
4. Um acesso diferenciado por camadas em troca de dados melhores (ou seja, mais completos e mais precisos) seria uma compensação possível.
5. O RDS proposto apresenta várias vantagens que compensam os riscos. O fácil acesso aos dados precisos do registrante é crítico para a aplicação dos direitos da propriedade intelectual on-line. Um sistema de RDS que melhore o acesso e a precisão desses dados seria extremamente vantajoso para os detentores de propriedade intelectual e seus consultores ao abordar a violação de IP e outros abusos relacionados por parte de registrantes de nomes de domínio e outros usuários da Internet.

-- Publicado em 28 de julho de 2014 --

6. Se os custos de validação e os prazos puderem ser controlados e mantidos ao mínimo, as vantagens do sistema proposto poderiam ser um intercâmbio justo pelas vantagens propostas do sistema. Se os custos não forem controlados, eles superarão gravemente as vantagens.
7. O aprimoramento da qualidade dos dados no banco de dados do Whois é muito importante e compensador. A vinculação dos registrantes de maneira consistente com seu portfólio completo de domínios também é muito importante e compensadora. Com isso, garante-se que, quando uma imprecisão nos dados do ponto de contato para um domínio for identificada e corrigida, ela será corrigida em todos os pontos em que existir.
8. O aprimoramento do acesso programático (sem limites de taxa arbitrários ou mal concebidos etc.) também seria tremendamente útil.
9. O acesso uniforme/confiável/utilizável dos dados corretos é uma clara vantagem, já que os riscos podem ser minimizados por um desenho e consulta cuidadosos.

25 entrevistados ofereceram **outros comentários** ao final da pesquisa, como segue.

1. A proposta carece de recursos concretos para elevar a precisão prática dos dados (a possibilidade de contato dos registrantes) significativamente acima do nível dos dados de referência do RAA de 2013 e PICs (para novos gTLDs). Eles devem ser definidos. De forma semelhante, um banco de dados mais rico que fornecesse serviços aprimorados como dados históricos poderia ajudar a justificar a redução do acesso público a esse recurso.
2. Uma vantagem é permitir que identifiquemos os registrantes que tentem ocultar sua identidade para poder continuar com as atividades maliciosas e distribuir malware.
3. A possibilidade dos usuários e ferramentas de terceiros usarem o sistema Whois atual para acessar e salvar as informações do WHOIS para fins de histórico é crítica. Qualquer sistema de RDS proposto deve garantir essa possibilidade. Isto pode ser feito diretamente, através do próprio RDS, ou indiretamente, continuando a permitir que as ferramentas de terceiros/clientes o façam.
4. Conceder um controle monopolista desse bem público a uma única entidade consiste em uma perda para o mundo com poucas vantagens, o que não ocorreria com outros meios menos centralizados.
5. Por que há tantos novos gTLDs? Esta decisão é desastrosa para os proprietários de marcas, porque leva ao aumento dos custos de proteção de IP. Neste momento, estamos enfrentando muitos registros de má fé, embora os períodos experimentais para muitos gTLDs novos ainda não tenha começado. Como pequena empresa, talvez você não tenha dinheiro suficiente para registrar-se em tudo para evitar registros de má fé. Por outro lado, os custos de recursos jurídicos são altos.
6. O fato de ter um Whois verificado é da maior importância, devido ao anonimato da Internet. Nós procuramos os infratores e os dados imprecisos não são mais aceitáveis.
7. Eu apoio totalmente o esforço para tornar os dados do WHOIS mais precisos. Seria uma mudança positiva SE um banco de dados centralizado e fechado não dificultasse a obtenção das informações, demorasse o processo de obtenção das informações, tivesse um teto na quantidade de informações que podem ser obtidas, criasse longos processos para que as empresas obtivessem credenciamento para acessar as informações ou criasse problemas de transparência para os usuários da Web. Grande parte da minha preocupação reside em que a comunidade de segurança cibernética possa proteger efetivamente os consumidores contra sites desonestos que possam tirar vantagem de um banco de dados fechado.
8. O acesso público/bloqueado para certos elementos de dados é uma boa proposta. Seria útil consultar mais detalhes em torno aos objetivos de revelação aceitáveis, avaliação desses solicitantes e como os usuários do acesso bloqueado são considerados responsáveis etc., para comentar sobre isso.
9. Em geral, qualquer movimento para centralizar os dados aumenta muito os riscos de hackers explícitos e ocultos, espionagem invisível e isenta de responsabilidade do governo, modos de falha em larga escala e interferência política. Embora alguns dos objetivos do RDS sejam valiosos, eles não superam os riscos totalmente previsíveis. Os maiores riscos do RDS são a perspectiva de ter que pagar pelo acesso às informações públicas do WHOIS e/ou a perda do acesso público às informações básicas de gerenciamento da rede, incluindo a atribuição de blocos de endereços IP, localização física e caixas de correio de abuso.

Qualquer proposta que não proteja o acesso público e gratuito e a disponibilidade continuada desses itens de informações deve ser retirada da mesa tão rápida e definitivamente quanto possível.

10. Ainda não tenho certeza de como podemos garantir a "precisão" dos dados de registro; os dados do primeiro dia (no registro) são uma coisa, e outra é a "verificação periódica", que acredito que é a mais importante. Na minha opinião, podemos ter de terceirizar isto a uma "agência" em cada localidade (país ou talvez cidade) para fazer a verificação, mas isso pode levar novamente a questões sobre a precisão e o padrão.
11. Os dois grupos de indivíduos que o registro médio gostaria de evitar que tenham acesso em lotes aos dados do Whois são spammers e organismos encarregados do cumprimento da lei. Fornecer informações em lotes a um desses grupos prejudicaria irreparavelmente a reputação do registro. Um sistema de RDS centralizado exige que o registro coloque sua reputação nas mãos de um terceiro.
12. Deve haver aceitação de que nem todas as partes têm o mesmo protecionismo pelas leis locais, que as solicitações de dados transnacionais podem não prosseguir devido a problemas políticos externos. Um recurso vital na luta contra o crime cibernético organizado será perdido com o RDS.
13. Como registrante individual, atualmente uso uma função de privacidade/procuração disponibilizada pelo meu registrador para proteger minha identidade individual do acesso casual e desnecessário do público geral, o que eu acho útil como precaução contra o assédio pessoal anônimo. Eu gostaria de ver essas funções de privacidade compulsórias regularmente disponíveis sempre que usar qualquer registrador, para garantir um mercado de registro completamente competitivo em todos os registradores, e não apenas um subconjunto voluntário de registradores.
14. O risco que mais me preocupa é o custo pela validação de meus dados de registro e a autenticação para que eu acesse os dados bloqueados. Também me preocupam os tempos de processamento e o atraso geral que esses procedimentos causarão.
15. O RDS é uma ótima ideia. Ele ajudaria a resolver muitos problemas se fosse implementado corretamente. Espero poder ter alguma contribuição. No entanto, esta pesquisa específica não foi bem feita.
16. Francamente, este sistema parece ser tão mal planejado como os serviços de "privacidade do WHOIS" atualmente disponíveis. O uso deles simplesmente fere a transparência de uma organização e, portanto, sua reputação on-line. Obrigado por ouvir minha opinião.
17. Não vejo vantagens, mas sim muitos riscos pelo uso indevido ou roubo de dados. Idealmente, a necessidade de fornecer dados de registro para o registrador seria eliminada - se não houver dados de registro, não haverá risco de abuso ou roubo.
18. Minha preocupação é poder lidar com vários tipos de ataques da rede/spam/intrusões/inundação de dados etc. É ABSOLUTAMENTE essencial que exista um contato válido e que esse contato lide efetivamente com os problemas da rede relatados a ele. Isso significa que o contato deve ter a autoridade e possibilidade técnica de assegurar que seu domínio não é a fonte do abuso. O sistema atual, especialmente aqueles domínios ocultos atrás de procurações, NÃO fornece a segurança de que o registrador/procuração tratará (ou possa tratar) de determinadas questões de maneira oportuna. Se as procurações devem ser permitidas, deve ficar ABSOLUTAMENTE claro que qualquer um que estiver listado em pesquisas/consultas publicamente acessíveis é responsável pelo comportamento do domínio que estiver protegendo, incluindo a total possibilidade de fechar o domínio em caso de abuso significativo na rede.
19. O maior risco reside em como será gerenciado o acesso às informações "bloqueadas", se serão cobradas taxas e qual será o peso do processo de credenciamento para obter o acesso. Se esse processo for caro ou pesado, isso afetará seriamente as operações comerciais básicas, o contato com os proprietários de domínios, a pesquisa e várias outras áreas de gerenciamento e pesquisa de domínios.
20. Eu penso que este processo proposto é uma solução em busca de um problema, alimentada por argumentos enganosos a modo de camuflagem por parte de pessoas impulsionadas por visões políticas dogmáticas.
21. Eu acho que não houve uma análise cuidadosa dos requisitos de privacidade de entidades comerciais/corporativas, físicas ou jurídicas. Os registrantes individuais/físicos devem oferecer a possibilidade de ser contatados de alguma maneira para permitir a solução dos problemas que afetam os outros e ainda devem ter sempre o direito ao anonimato, exceto no caso de uma petição judicial adequada. Por outro lado, entidades jurídicas com restrições limitadas (como abrigos para mulheres,

algumas organizações políticas em perigo), NÃO DEVEM ter anonimato. É absolutamente inadequado para elas, especialmente as empresas comerciais, operar anonimamente e os dados DEVEM ter acesso público/anônimo. Em segundo lugar, deve haver um processo pelo qual o anonimato possa ser tirado das entidades que comprovadamente não cumpram os requisitos para o anonimato.

22. Nós sofremos muito com os spammers e botnets que usam dados falsos para ocultar a propriedade dos domínios. As informações do Whois podem e devem ser claras e bem definidas. Não é uma dificuldade exagerada obter serviços de hospedagem de outras entidades, mas é operacionalmente útil ser claro sobre quem está no comando dos servidores de DNS para um domínio específico.
23. Em minha opinião, a privacidade é muito mais importante do que o acesso público aos dados de registro.
24. Como não há vantagens, parem de fazer o que estão fazendo. Se o sistema funciona, não o modifiquem. Não esqueçam que muitos dos registrantes DESEJAM que seus dados de Whois estejam acessíveis da mesma forma que estão agora, e aqueles que não o desejam podem utilizar a POB ou a proteção de privacidade oferecida pelo registrador.
25. O RDS é muita coisa de uma só vez e uma má ideia. Ele cria encargos para aqueles que menos se beneficiam, sem custos reais para aqueles que mais se beneficiam.

Finalmente, aproximadamente 5 dos 182 entrevistados apimentaram a maioria ou todos os campos de texto de formato livre com respostas que não abordaram diretamente as perguntas, mas, em vez disso, declararam que o RDS é uma má ideia ou não oferece vantagens.

-- Publicado em 28 de julho de 2014 --