SAC 044
A Registrant's Guide to Protecting Domain Name Registration Accounts

A Report from the ICANN
Security and Stability
Advisory Committee
(SSAC)
05 November 2010

Preface

This is a report by the Security and Stability Advisory Committee (SSAC) describing measures a domain name registrant should consider to protect domain name registration accounts against misuse. In the report, SSAC recommends measures that organizations or individuals should consider to protect their domain name registration accounts and domain names against a range of threats that may result in temporary or permanent loss of domain name registrations and the possible, consequent loss or disruption of Internet presence.

The SSAC advises the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocation systems. This includes operational matters (e.g., matters pertaining to the correct and reliable operation of the root name system), administrative matters (e.g., matters pertaining to address allocation and Internet number assignment), and registration matters (e.g., matters pertaining to registry and registrar services such as WHOIS). SSAC engages in ongoing threat assessment and risk analysis of the Internet naming and address allocation services to assess where the principal threats to stability and security lie, and advises the ICANN community accordingly. The SSAC has no official authority to regulate, enforce or adjudicate. Those functions belong to others, and the advice offered here should be evaluated on its merits.

The contributors to this report, reference to the committee members' biographies and statements of interest, and committee members' objections to the findings or recommendations in this report, are at end of this report.

Table of Contents

1. Executive Summary

Domain name registrations in domain name registration accounts are as important in the virtual world as their brick-and-mortar assets are in the physical world. Individuals and organizations should thus consider measures to protect virtual assets against a range of threats or circumstances in the virtual world that may result in temporary or permanent loss of domain names.

This report attempts to catalog measures that registrants should consider to protect their domain name registration accounts and the domain names managed through these accounts. The report describes the threat landscape for domain names, and identifies a set of measures for organizations to consider. The report also considers risk management in the context of domain names so that an organization can assess its own risk and choose appropriate measures. The report explains that an organization can implement these measures using its own staff ("in house"), contracted third parties, or a registrar or registry. It discusses the merits of implementing certain measures versus outsourcing these to contracted third parties or registrars and identifies circumstances where redundant measures are worth consideration. Lastly, the report provides lists of questions organizations should ask registrars and registries concerning their registration processes and protection mechanisms. The list can be used to obtain valuable and important information about registrar processes so that organizations can make informed decisions when choosing a registrar(s).

This report specifically targets individuals or organizations that recognize that the operational value of a domain name in use is extremely or critically important. These parties are keenly aware of the need for assurances that domain name resolution is highly available and that names in a domain consistently resolve as intended. The report assumes that the reader has some familiarity with domain name registration processes, the domain name system, and other technical and operational aspects of providing Internet presence. The report is likely to be of greatest value to individuals who perform administrative or technical staff activities; however, other parties (legal counsel, management) may benefit by gaining insight into the security threats and mitigation measures recommended in the report as well.

Readers familiar with SAC040, *Measures to Protect Domain Registration Services Against Exploitation or Misuse*[1] will note certain similarities and overlap among the topics covered here. SAC040 identifies practices registrars can share with customers (registrants) so that registrar and registrant can jointly protect registered domains against exploitation or misuse, and discusses methods of raising awareness among registrants of the risks relating to even a temporary loss of control over domain names and associated DNS configurations. As such, SAC040 is registrar-focused. This report focuses on registrants to help them recognize the critical importance of domains they have registered

[1] Security and Stability Advisory Committee, *Measures to Protect Domain Registration Services Against Exploitation or Misuse* (19 August 2009) <http://www.icann.org/en/committees/security/sac040.pdf>.

and seek information that will help them implement measures of their own as well as seek out measures from registrars to protect their domain names against loss or misuse. The reports are thus intended to be complementary.

2. Introduction

Domain names represent the online identification or personification of individuals, businesses, and other organizations. Domain names often include names of products and services, including trademarks or service marks ("brands"). Individuals and organizations often protect their celebrity (personal or stage name), trademarks, brands, and intellectual properties against theft, misuse, and reputational harm in the physical world. The domain name registrations in domain name registration accounts are as important in the virtual world as their brick-and-mortar assets are in the physical world. Individuals and organizations should thus consider measures to protect virtual assets against a range of threats or circumstances in the virtual world that may result in temporary or permanent loss of domain names and the possible, consequent loss or disruption of Internet presence (web).

Certain threats to domain names are external and malicious. Consider an attacker who actively seeks to gain unauthorized access to a domain name registration account in order to control ("hijack"[2]) a domain name or to alter Domain Name System (DNS) information associated with that domain name. These acts are often related. Altering DNS information is a common objective of a registration account compromise. Specifically, the attacker seeks to alter DNS configuration information associated with a domain name(s) in the account so that domain name resolution directs web visitors to an impersonation site, phishing site, a web defacement site, or to a web site that is used to host malicious code (malware) or other illicit content.[3] An attacker may also alter the DNS configuration in order to route the organization's mail or web traffic though monitoring hosts so that he can monitor or capture sensitive information such as user credentials that the attacker could then use to perpetrate fraud or theft. Such unauthorized modifications of DNS configuration information can result in the loss or disruption of Internet presence, loss of communications (email, Internet voice, streaming media or collaboration applications), reputational or even direct financial harm.

Loss or disruption of Internet presence can also occur when registrants do not take adequate internal measures to protect domain names they register. For example, a party other than the current registrant may be interested in a particular domain name. This interested party may closely monitor that name as its registration nears its expiration so that he may register the domain should the current registrant fail to do so. Loss of the domain name in such circumstances is the result of the registrant's failure to take adequate *internal* measures to ensure that domain names are renewed promptly. If the lapse in renewal was an oversight or error, the organization might lose the registration and be forced to pursue a potentially expensive and time-consuming dispute resolution process to regain the use of the domain name.

[2] Wikipedia, "Domain Name Hijacking," <http://en.wikipedia.org/wiki/Domain_hijacking>.
[3] Wikipedia, "DNS Hijacking," <http://en.wikipedia.org/wiki/DNS_hijacking>.

Various measures are available to domain name registrants to protect their domain names. Prior incidents involving domain names indicate that registrants may be unfamiliar with such measures, that they do not avail themselves of the measures sufficiently to mitigate threats to domain names, or that they do not take measures to protect the asset or operational value of domain name registrations until they fall victim to an attack or poor domain name management. [4]

This report attempts to catalog measures that registrants should consider to protect their domain name registration accounts and the domain names managed through these accounts. The report assumes that the reader has some familiarity with domain name registration processes, the domain name system, and other technical and operational aspects of providing Internet presence. As such, it is likely to be of greatest value to individuals who perform administrative or technical staff activities; however, other parties (legal counsel, management) may benefit by gaining insight into the security threats and mitigation measures recommended in the report as well.

Readers familiar with SAC040, *Measures to Protect Domain Registration Services Against Exploitation or Misuse* will note certain similarities and overlap among the topics covered here and in SAC040. [5] SAC040 is registrar-focused. This report focuses on registrants to help them recognize the critical importance of domains they have registered and seek information that will help them implement measures of their own as well as seek out measures from registrars to protect their domain names against loss or misuse. The reports are thus intended to be complementary.

3. Threat Landscape

Prior SSAC reports and advisories describe threats to domain name registrations and registration accounts. These include:

Unauthorized access to domain registration account. Similar to other online accounts, domain registration accounts provided by registrars are vulnerable to many forms of attack that result in the compromise of account identities and authentication credentials (e.g., a user name and password). An attacker may obtain identities and credentials in several ways. He may guess them, capture them from a host containing credentials, or capture them as they are entered (i.e., as they are key-stroked or transmitted from a client application/host to a server). He may acquire them using social engineering techniques or by conducting a phishing attack against a registrant or a registrar, or by attacking the

[4] High profile incidents involving domain names are described in SAC007, *Domain Name Hijacking Report*, <http://www.icann.org/announcements/hijacking-report-12jul05.pdf> and SAC040, *Measures to Protect Domain Registration Services Against Exploitation or Misuse*, <http://www.icann.org/en/committees/security/sac040.pdf>.

[5] Security and Stability Advisory Committee, *Measures to Protect Domain Registration Services Against Exploitation or Misuse* (19 August 2009) <http://www.icann.org/en/committees/security/sac040.pdf>.

registrar or registry directly.[6] Domain name registration account compromises of this kind are often precursors to additional attacks. These include:

1. *Malicious or unintentional (erroneous) alteration of DNS configuration information*. Maliciously introduced changes to the DNS name server configuration information associated with a domain name may result in the resolution of the domain name to an IP address(es) other than the address(es) the domain registrant intended. Such changes can result in the loss or disruption of the registrant's Internet services (e.g., web or email) or the intentional and malicious redirection of visitors away from the registrant's intended servers to an attacker's servers, which may host defacement, phishing or other malicious or criminal activities.[7] Lack of coordination or administrative error can introduce changes to DNS name server configuration information with the similar consequences as malicious alteration. Such changes can result in the loss or disruption of the registrant's Internet applications or services, or could expose the registrant's organization to attack.[8]

2. *Malicious or unintentional (erroneous) alteration of contact information*. Whether by error or as a result of an attack, changes to the contact configuration information associated with a domain name may result in:

    a. The unauthorized transfer or wrongful taking of control of a domain name from the rightful name holder (domain name hijacking);[9]
    b. Disruption of delivery of registrar correspondence to the domain name registrant or authorized administrators (e.g., non-delivery of email correspondence because the email address points to a non-deliverable recipient or an invalid domain);
    c. The filing of a report of WHOIS inaccuracy against the registrant which could lead to an suspension or deletion of the domain name, or a report that falsely or incorrectly associates a domain with an abuse and causes a suspension of the domain; and
    d. The deletion of a domain name registration by the unauthorized party (or in general, the unauthorized alteration of any domain setting accessible via a registrar's domain account management tools, including renewal

[6] Security and Stability Advisory Committee, *Advisory on Registrar Impersonation Phishing Attacks* (26 May 2008), <http://www.icann.org/en/committees/security/sac028.pdf>.
[7] Op. cit.
[8] Consider a circumstance where a typographical error by an authorized party sets the IP address of one several DNS name servers for a domain name to an IP address that is not from the IP numbering space allocated to the organization. All but the incorrectly configured name servers will resolve domain names as expected. If the organization is high profile and constantly targeted, an attacker could note the addressing anomaly and attempt to gain control of the host at the exploitable address. If successful in gaining control of this address, the attacker could operate a name server for the domain name and populate the zone data for that domain with malicious DNS records.
[9] Security and Stability Advisory Committee, *Domain Name Hijacking Report* (SAC007) (12 July 2005) <http://www.icann.org/announcements/hijacking-report-12jul05.pdf>.

options, domain locks, etc.). Such malice or error can cause a disruption of name service, malicious name resolution, or loss of the registration of the domain name itself.

Failure to renew a domain name registration. A renewal lapse occurs when, by choice or oversight, a registrant allows a domain name registration to expire. A different party may register the domain name after the expiration of relevant grace periods. In some cases, the activities of the new registrant may prove harmful to the interests of the registrant who permitted the registration to expire.[10] In other cases, the registrant may lose the domain name and be forced to find another domain name (thereby absorbing the costs of switching to a new domain name) or to pursue a potentially costly and time-consuming dispute resolution process to regain control of the domain name.

Non-renewal of a domain name associated with a DNS Name Server. Problems may arise when the registrant of a domain name *A* uses a DNS name server in domain *B* for domain name resolution, and the registrant of domain name *B* accidentally or intentionally allows its domain name registration to expire. In circumstances where coordination across well-intentioned parties is lost, the expected resolution of domain *A* may be interrupted or may become unpredictable due to *A's* dependence on the name server in domain B; in other circumstances, a new registrant of domain *B* may configure domain *A*'s DNS information for malicious purposes, including phishing attacks, email interception, and redirection of Internet users to different websites with different and possibly harmful content.[11] While domain *A* can be restored to proper function by updating the registry with a new name server (perhaps on domain *A* or *C*), this can present operational challenges to accomplish in the extreme short term.

Certain organizations may also need to consider additional forms of registration abuse, including cybersquatting or front running.[12] These malicious uses and other abuses are out of scope for this report, which is focused on existing registrations in control of a registrant, but may be mitigated using measures and considerations described elsewhere.[13]

4. Risk Management and Domain Names

Operationally, domain names are user-friendly identifiers that can be resolved using the DNS to determine the Internet (IP) addresses of hosts that provide services for that domain (e.g., web, mail, social networks, voice, etc.). The operational value of a domain

[10] Security and Stability Advisory Committee, *Renewal Considerations for Domain Name Registrants* (29 June 2006) <http://www.icann.org/en/committees/security/renewal-advisory-29jun06.pdf>
[11] Security and Stability Advisory Committee, *Problems caused by the non-renewal of a domain name associated with a DNS Name Server* (7 July 2006) <http://www.icann.org/en/committees/security/renewal-nameserver-07jul06.pdf>
[12] Security and Stability Advisory Committee, *Advisory on Domain Name Front Running* <http://www.icann.org/en/committees/security/sac022.pdf>.
[13] Registration Abuse Policies Working Group, *Initial Report* (12 February 2010) <http://gnso.icann.org/issues/rap-wg-initial-report-12feb10-en.pdf>.

name in use – specifically, the assurance that name resolution is highly available and that names in a domain consistently resolve as intended – is of extreme importance to most registrants. Consequently, domain name registrations should be considered as an asset and therefore included in business processes such as asset management, provisioning and risk management programs.

Models for asset management, provisioning and risk management typically include the following considerations:

- Identify the value of an asset (tangible or intangible);
- List the ways in which that value is threatened (loss, theft, misuse);
- Determine how the threat can be realized, i.e., what makes the domain name vulnerable to attack or exploitation;
- Determine the probability or risk that each threat poses;
- Determine how the risk can be mitigated or reduced;
- Determine the cost of mitigating or reducing the risk to an acceptable level of risk and cost; and
- Determine the appropriate budget/priority and implement risk mitigation or reduction.

A domain name registration deserves the same rigor as other inventoried, valued, or sensitive digital or physical assets. Domain name registration management shares many characteristics of provisioning management in large-scale networks. For example, the primary operations in provisioning and in domain name registration are {add, delete, change}. Best practices applied in provisioning management seek to assure that only authorized parties perform these operations in proper sequence, in a timely and auditable manner, with low probability of omission, intrusion or error. Such best practices can be extended to include domain name registration management and registration services.

It is ultimately the responsibility of the registrant to assess the risk of attack against domain names and DNS configuration and to implement protective measures that reduce the registrant's exposure to attack to an acceptable degree. Registrants can implement certain of these measures directly. Registrars or other third parties may also offer services that obviate the need for the registrant to implement certain measures directly, or that complement measures the registrant implements, i.e., to provide redundant or multiple defenses against certain threats.

Domain names and DNS configuration are information assets. They have an inherent underlying value in enabling business to occur and communication to flow and without which individual, business or societal aims and objectives would be impacted to varying degrees. The specific value of domain name registrations and DNS configurations vary greatly across domain name registrants, within their portfolios, and over time.

To fully assess the risks against a domain name, registrants must consider the business impact of a *realized* risk (e.g., a successful attack resulting in the loss of operation or

ecommerce presence), both in terms of quantitative and qualitative costs against their day-to-day business operations and ultimately their business objectives.

Business impact is not measured solely in terms of the replacement value of a domain name, but also the short, medium and long-term effect if a domain name or DNS configuration were to result in degraded or lost operation, for whatever reason, over any period of time. This impact may be in terms of lost revenue, increased expenses, loss of productivity, damaged reputation, or loss of goodwill.

SSAC strongly encourages registrants to conduct a business impact assessment in order to understand how much of an interruption can be tolerated before the impact is material. Include a review of domain name assets a part of a predictable annual business process – a budgeting process, business planning, or performance review cycle – to encourage at least once-yearly attention to the assets. This business impact assessment approach is useful in that it focuses on the impact of a security related event, rather than the multitude of threats or vulnerabilities present in the environment.

5. Measures to Protect Domain Registrar Account Compromise

This section describes protective measures that registrants should consider implementing to protect against domain registration account compromise. Several measures in this section are mentioned in SAC40 as measures that registrars could offer. Here, we describe how these measures could be implemented directly by a registrant.

5.1 Protection Against Unauthorized Account Access

The SSAC encourages registrants to consider the following measures to protect against unauthorized account access.

Protect account credentials. Registrants are encouraged to manage access account credentials for registrar accounts according to a policy based on these common practices:

1. Maintain a list of authorized contacts for each domain registration account;
2. Advise authorized contacts that they are responsible for keeping secret the account credentials for domain registration accounts, and that they must not disclose or share passwords;
3. Identify measures authorized contacts must take should they discover that credentials have been disclosed;
4. Authorized contacts must compose passwords used to access a registration account using applicable organizational policies and commonly recognized best practices for composition (e.g., length and complexity), re-use, and longevity;[14]

[14] For example, http://technet.microsoft.com/en-us/library/cc784090%28WS.10%29.aspx or http://www.linuxsecurity.com/content/view/117700/171/

5. Alternatively, if the registrar supports a form of multi-factor authentication (e.g., a hardware or software token), authorized contacts must keep the token safe from loss, damage, or unauthorized use;
6. Use different credentials for each account;
7. Partition particularly sensitive or important domain registrations into an account whose credentials are held by more senior personnel;
8. Securely escrow all registration account credentials;
9. Define and implement a recovery process with detailed auditing;
10. Define the circumstances where recovery is permitted, who has authority to recover credentials from escrow, and who is to be notified when escrowed credentials are accessed;
11. Changes in personnel authorized as contacts for a registrar account should cause new credentials to be created and old credentials to be revoked. (This may require coordination with a registrar, i.e., in cases where the registrant intends to change the user account identifier.); and
12. Employee resource management processes such as employee termination and employee transfer should be modified to check if the employee has domain registration account access. The processes could be modeled after similar checks for employee access to other assets, such as financial accounts.

These policies can be implemented as part of a large organization's workflow. They can be implemented by an individual or smaller organization using methods as simple as a checklist, ledger or desktop password security application.

Take advantage of routine correspondence from registrar(s). Registrars use electronic mail as a way to convey notices and obligations to registrants.[15] Consider using each such correspondence as an event triggering a workflow or registration related action. For example:

1. Use domain name renewal notifications to trigger a review or renewal action by staff responsible for Intellectual Property and Trademark matters, marketing, or generally any group that should decide whether to renew or allow a registration to expire.
2. Use WHOIS accuracy reporting obligation notifications to trigger action by staff to review and then confirm or update the registration information that must be publicly accessible via WHOIS services.
3. Use configuration change notifications to trigger checks by technical staff to verify that the changes are authorized and correct. Registrars may issue change notifications for any of the following events:

[15] Correspondence varies across registrars. Certain registrars may issue notifications that are not mentioned here.

a. *Domain name servers*. Unauthorized or erroneous additions, deletions or changes to the list of domain name servers (or the IP addresses registered for those servers) that resolve the subdomains (labels) of a domain can result in disruption of service and should be confirmed by staff responsible for managing the organization's DNS.

b. *Contact information*. Changes to registrant, administrative, or technical contact information should be confirmed to prevent attempts to divert ownership or correspondence away from authorized representatives of the organization.

c. *Changes to domain status at registry*. Registrars and registries coordinate the state (status) of a domain name in a registry using provisioning protocols.[16] Registrars publish the status of a domain via WHOIS. Changes to domain status should be confirmed to assure that the domain is in the organization's desired operational state.

d. *Changes to domain status at registrar*. Certain registrars allow domain-specific settings (e.g. private registration, domain forwarding, autorenew) that are held at the registrar. Changes to these services can have both long-term and short-term impact and therefore changes should be confirmed.

4. Use notifications regarding changes to or pending expiration of credit card or other payment methods and associated billing information to trigger checks by accounting personnel to ensure that changes are authorized and correct, needed payments are scheduled, and scheduled payments are not declined.

5. Designate a responsible party for each notification or have the notification trigger the creation of a ticket in a ticketing system. Such measures ensure that no notifications are ignored or are not responded to in the necessary or appropriate timeframe.

6. Define required responses and establish a clear SLA for each response to each type of event.

7. In order to protect email delivery against disruption attacks, contact email addresses for a domain should be assigned to mail servers named outside that domain and registration account. For example, if the domain example.net is managed through an account *A* at registrar *X*, use email addresses assigned from a different domain (example.biz) managed through an account *B* (and possibly at registrar *Y*). This measure prevents an attacker who succeeds in compromising a domain account from preventing delivery of notification emails by altering DNS configuration for a domain.

SSAC encourages registrants to consider authenticated correspondence for their workflows, such as secure email. In the absence of authenticated email, email-based workflows should be spoofing-resilient. Measures to mitigate spoofing include avoiding

[16] Guide to Domain Name Status Codes, <http://www.wdbc.com/domain/status-codes.cfm>.

the use of hyperlinks in email, and verifying the accuracy of the email notification that triggers the workflow by some means your organization accepts as trusted.

Maintain documentation to "prove registration".[17] Registrants are encouraged to maintain documentation in case disputes or other situations arise where there is a need to "prove registration."[18] Suggested documentation includes:

- Copies of registration records;
- Billing records, especially ones that show payments have been made;
- Logs, archives, or financial transactions that associate a domain name with content that you, the rightful registrant, published.
- Telephone directories (Yellow Pages), marketing material, etc. that contain advertising that associates you, the registrant, with the domain name;
- Correspondence to you from registrars and ICANN that mentions the domain name; and
- Legal documents, tax filings, government-issued IDs, business tax notices, etc. that associate you, the registrant, with the domain name.

5.2 Domain Name Points of Contact Considerations

In all generic Top Level Domains (gTLDs) and most country code TLDs (ccTLDs), registrants are required to provide three points of contact when registering a domain name.[19] The registrant is the individual or entity on record as having registered the domain. The other contacts are role contacts:

- A technical contact is responsible for technical matters related to a domain, such as DNS operation;
- An administrative contact has authority to represent the registrant to the registrar in administrative matters; and
- A billing contact is responsible for payment and financial matters.

These points of contact are critically important. At most registrars, these points of contact have authority to make certain changes to registration information, including name server information for DNS operations. The SSAC encourages registrants to consider the following when identifying domain registration points of contact.

Use separate identities for registrant, technical, administrative, and billing contacts. Consider creating unique points of contact for registrant, technical, administrative, and

---

[17] Evacuation Kit for Domain Name Holders, <http://securityskeptic.typepad.com/the-security-skeptic/2009/10/evacuation-kit-for-domain-name-holders.html>.

[18] Uniform Domain Name Dispute Resolution Policy (26 August 1999), <http://www.icann.org/en/dndr/udrp/policy.htm>.

[19] Registrar Accreditation Agreement (17 May 2001), <http://www.icann.org/en/registrars/ra-agreement-17may01.htm>.

billing contacts. Identifying multiple points of contact offers an organization some protection in situations where a single contact is provided for all roles and that contact ceases to be employed by an organization, or in a circumstance where the only identified contact is not available to resolve a problem or respond to a reported abuse of the domain name. Distinct points of contact also offer some diversity in managing domain names. Each of these contacts can represent departments or divisions in an organization that are responsible for some aspect of domain name management. For example, while legal staff or an IP&T department may be best suited to manage the registrant role, IT may be best suited to manage the technical role, corporate communications may be best suited to manage the administrative role, and finance best suited to manage the billing role.

Small businesses can seek assistance from web hosting companies, ISPs, resellers, or registrars to apply this kind of diversity.[20] Provide your business entity contact as the registrant contact information to retain your association with the domain. Use your business entity contact as the billing contact as well to ensure you receive payment requests. Identify a web hosting company, ISP, reseller, or registrar as the technical or administrative contact. A small business may want to consider identifying its hosting company, ISP, reseller, or registrar as the technical or administrative contact. Such external parties often have stronger internal controls and may be better able to track changes or resolve technical problems than the small business would implement.

Incorporate registrar email correspondence into domain management. Ask your registrar for a list of correspondence routinely issued by email, and consult with your registrar to determine which of your email contacts is used for routine correspondence. Use your email system to route correspondence to the organization's point of contact that is responsible for responding to or taking action. For example, consider whether you can route registrar email correspondence so that your technical contact receives DNS configuration change notices, your legal department receives renewal and WHOIS accuracy notices, etc.[21]

Identify domain name registration points of contact by role. In cases where a domain name is registered to an organization (business entity), consider creating points of contact that do not create a relationship between any natural person or employee. This action may help an organization avoid disputes over ownership of a domain. An example of the elements of a domain registration where "role" identities could be employed for the domain example.net appears below:

```
Domain Name: EXAMPLE.NET
Domain Registration Date: 09-MAR-1994
```

[20] A sole proprietor (individual) may find it convenient to outsource one or more of these roles to an external service, but in terms of security exposure, centralizing all the roles in the sole proprietor may be appropriate and sufficient.

[21] Consider similar routing strategies if your business relationship with a registrar includes fax or phone correspondence. While these are not as frequently used, it may be useful for your organization to consider how you might be able to integrate fax, voice, and email so that appropriate points of contact receive notifications irrespective of the communications medium the registrar uses.

```
Domain Expiration Date: 09-MAR-2012
Domain Last Updated Date: 01-APR-2010
.
.
.
Registrant Name: EXAMPLE NETWORKS, INC.
Registrant Organization: EXAMPLE.NET
.
.
.
Registrant Email: EXAMPLENETWORKSINC@EXAMPLE.NET
.
.
.
Administrative Contact Name: DOMAIN ADMINISTRATOR
Administrative Contact Email: DOMAINADMINISTRATOR@EXAMPLE.NET
Technical Contact Name: DOMAIN TECHNICAL OFFICER
Technical Contact Email: DOMAINTECHNICALOFFICER@EXAMPLE.NET
```

In this hypothetical registration, the domain name is registered under the name of the incorporated business. Unique contact names and email addresses are created for the technical and administrative points of contact. Responsibility for such accounts can be passed to replacements as the role changes hands from one employee to a successor without the threat of an employee claiming ownership of the domain registration. (Note that change controls described in the section, *Protecting account credentials,* are particularly important when role accounts are employed.)

Add diversity to email contacts to reduce single points of failure or attack. SAC040 explains how email is an important form of contact for registrars for routine correspondence and notifications, and that attackers attempt to defeat this popular form of automated notification when they compromise a domain name registration account. Specifically, when an attacker succeeds in compromising a domain registration account, he will attempt to block delivery of email notifications to targeted registrants by altering DNS configuration information so that email notifications will not be delivered to any recipient in the domains the attacker controls through a compromised account (e.g., registrant's identified administrative or technical contact email addresses hosted in the domain).

Access to *all* the domains in a domain name registration account is commonly granted through a single user account. This access also allows an attacker to modify contact and DNS configuration information for all domains managed through the user account. Thus, if Example Networks, Inc. manages the domains example.net, example.com, and example.biz from the same domain name registration account and that account is compromised, the attacker can alter DNS and block delivery of mail to *all* of these domains.

Registrants should consider the benefits of using mail domains for contact emails that are managed separately from the domains that can be accessed from an individual domain registration account so that an attacker cannot interfere with a registrar's ability to contact the registrant. Registrants should also consider other measures to mitigate this threat. For example, a registrant could distribute its domain name registrations across multiple domain name registration accounts (and possibly across different registrars). Example

Networks, Inc. could manage example.com using account "examplenetworks1" and example.net using account "examplenetworks2". Email addresses for points of contact for example.com could then be assigned from a mail domain operated under example.net. Similarly, email addresses for points of contact for example.net could be assigned from a mail domain operated under example.com. Registrants who do not want to rely on email notifications are encouraged to consult with registrars to determine whether they can receive change notifications through alternative communications methods (telephone, fax, SMS).

Individuals or small businesses can implement a similar defensive measure. Create email accounts for points of contact through an email service provider that has earned a positive reputation for managing its mail service.

Keep key email accounts secure. Email is an important component of registrant-registrar communication. Key email accounts receive registrar notifications and registration account password reset/recovery messages and thus should only be accessed by authorized parties. Maintain the security of key email accounts by strengthening client authentication. Use encryption (TLS extensions for SMTP) to protect mail client-server communications from eavesdropping. Maintain secure operations at the mail server that hosts key email accounts as well. For example, mail servers that host key email accounts should be Internet standards compliant. Consider adopting some form of email reputation, data integrity or authentication system and follow best sender, forwarding, and antispam practices published by such organizations as the Messaging Anti-Abuse Working Group (MAAWG)[22] and the Anti-Phishing Working Group (APWG)[23] so that your mail servers will not be reported to spam blacklists.

Improve change control and coordination. Large organizations often implement resource management to deal with changes in personnel or equipment to domain registrations that must be coordinated across departments or business units. These are characterized as "add, drop, change" processes. Domain name management shares characteristics with such resource management structures. Organizations should consider the value of using registrar correspondence to trigger intra-organizational activity. For example, an organization may want to have the technical contact for a domain name notify all departments whose system configurations include name servers upon receipt of a confirmation email from a registrar when a change to DNS name servers for the domain is made. Organizations should consider the value of implementing measures to notify registrant, technical, or administrative contacts when changes are made to any contact or configuration information for any domain name registered by the organization.

Maintain accurate external contacts. The SSAC encourages registrants to catalog points of contact information for registrars where they have domain registration accounts and make these available to all internal and contracted parties who are involved in domain name management. Registrar points of contact of particular interest for registrants include any contact that may assist the registrant in a business, operational or

[22] MAAWG Publications <http://www.maawg.org/published-documents>.
[23] Anti-Phishing Working Group <http://www.antiphishing.org>.

security matter. The list may include general information contacts, false WHOIS and abuse contacts, and (where applicable) internal contacts responsible for your account portfolio, abuse, spam, etc.

6. DNS Hosting Considerations

Domain name registration services and hosting of authoritative name service ("hosting DNS") for a domain name are distinct operations. Certain organizations host authoritative name service internally. Others rely on their registrar(s) to host DNS. Still others choose an external provider other than a registrar to host DNS such as Internet service providers or managed services providers. Depending on the extent to which an organization relies on high availability of its DNS, multiple DNS hosting agents may be utilized to provide resiliency or diversity.

Certain measures already recommended to protect domain registration services against misuse or abuse also should be considered for DNS hosting. For example, many of the practices registrants should consider to protect domain name registration account access (Section 5.1 above) and maintaining points of contact information can be applied to parties that host DNS, irrespective of whether that party is a registrar or other external agent. In particular, organizations or individuals that engage external parties to manage DNS and provide authoritative name service must be able to contact that service provider for business, technical and security related matters. They should also maintain accurate registrant, technical, and administrative contact information for registrants of any external domain names (such as "glue" records) that the organization relies upon for any internally managed DNS operations.

Two other areas of DNS operations merit consideration: zone data management and DNSSEC support.

6.1 Zone Data Management Considerations

A zone file contains all the DNS configuration information for a given domain name.[24] (This information is separate and distinct from the domain name registration information maintained for the domain name.) Each element of a zone file is called a resource record. Resource records can define (among other things) delegations within a domain (i.e., sub-domains), name and email servers for the domain, and hosts named within the domain. Via resource records, the zone contains associations between IP addresses and host names, and may identify host name aliases that are used to distinguish among multiple Internet services hosted at a common IP address (canonical names or CNAMEs).

Organizations or individuals submit zone data to a DNS provider (whether a registrar or managed service provider) in several forms. Certain registrars or managed DNS providers provide web, email, or other submission forms to simplify DNS configuration. Such forms reduce the customer's involvement in composing a zone file to the minimum input

[24] See, for example, Zone file, <http://en.wikipedia.org/wiki/Zone_file>.

necessary. For example, the web form may ask the customer to identify the host name and IP address information for his web and email services. Once input, the web application generates and publishes a complete zone file on the customer's behalf. In other arrangements, the customer may compose a zone file in its entirety. The managed DNS provider will typically validate the configuration and then publish it.

Given the variety of resource records one can configure into a zone file, organizations or individuals who employ an external agent to manage DNS should understand what is included when the agent configures the zone file. In particular, it is important to understand what resource records the external agent includes when composing a default zone file configuration so that you fully understand what Internet services the DNS will indicate you provide, and the IP addresses at which these services will be reached. By obtaining a complete list of default settings from your provider, you will be aware of all the services the DNS advertises as reachable within your domain.

Organizations should ask managed DNS providers to disclose their redirection and non-existent domain handling policies. Certain providers may by default redirect names that do not resolve (e.g., typographical errors such as ww.example.com when www.example.com was intended) to pay per click or other advertising (landing) or promotional pages.[25] Inquire whether you are able to opt-out of such handing or whether you have any influence over the advertising that will appear on such pages.

As mentioned above, zone files and zone data are distinct from domain name registration records. Ask your managed DNS provider how you can obtain a copy of your zone files for archival or restoration purposes. Maintain archives of the zone file you believe is accurate and complete for each domain name you have registered so that you can assist in the restoration of DNS in the event your managed DNS provider experiences a temporary, sustained, or permanent disruption of service. As discussed for domain name registrations, consider using change notifications you may receive from your manage DNS provider as triggers to obtain a (new) copy of your zone from the external agent who manages your zone.

6.2 DNSSEC Support Considerations

DNS Security Extensions (DNSSEC) uses encryption methods to provide operational-level protection against the unauthorized alteration of DNS information.[26] DNSSEC provides origin authentication of DNS information and thus provides protection against impersonation attacks: a recipient of a DNSSEC-signed response to a query on your domain name is assured that the resource record came from you, the authoritative provider of DNS information for this domain.

---

[25] Security and Stability Advisory Committee), *Preliminary Report on DNS Response Modification*, (SAC025) <http://www.icann.org/en/committees/security/sac032.pdf>.

[26] See DNSSEC Protocol RFCs at <http://www.dnssec.net/rfc>.

DNSSEC also provides data integrity and thus provides protection against cache-poisoning and related (e.g., Kaminsky[27]) attacks: a recipient of a DNSSEC-enabled response to a query on your domain name is assured that the DNS data in the response has not been altered. Lastly, DNSSEC provides *authenticated denial of existence* for a particular name (an assurance that the domain does not exist in the zone file). This feature assures a recipient of a DNSSEC-enabled response containing a non-existent domain (NXDOMAIN) that the domain is truly not in your zone file and thus prevents certain denial of service attacks.

DNSSEC support is a new service offering from registries, registrars, and managed DNS providers. We encourage you to consider implementing DNSSEC, either directly, or through your chosen registrar or a managed DNS provider. DNSSEC makes use of public key cryptography, which introduces a number of additional key management activities and requires that certain DNSSEC-specific resource records must be included in your zone file. You must coordinate these activities with your registrar, managed DNS provider (if other than your registrar) and the TLD in which your domain is registered.

Whether you choose to generate keys and undertake the responsibility to manage and protect them or whether you outsource these operations is an important decision. For maximum flexibility, ask candidate DNSSEC providers to explain their key generation and signing procedures, measures for key protection, and key revocation and change management procedures. Compare these to measures you may implement for other cryptographic keys in your organization, or compare them against available guidelines.[28] DNSSEC support is relatively new among registries, registrars and managed DNS providers, so consider how important it will be for you to outsource the entirety of the process or to have the flexibility to manage DNS and DNSSEC across multiple parties, thus affording you the ability to run DNS internally, through your registrar or have an agent other than your registrar manage DNS, with all the necessary support functions.

Be prepared to discuss and work with external parties to coordinate support, including:

- ❏ The ability to import and export your keys;
- ❏ The ability to import and export your zone file;
- ❏ Mechanisms and methods to un-sign a signed domain;
- ❏ The ability to import new NS RR set without DNS service disruption;
- ❏ The ability to sustain DNS services until you explicitly instruct a managed DNS provider to conclude operations; and
- ❏ The ability to set up DNS services in advance of an (incoming) transfer.

[27] See <http://www.networkworld.com/news/2008/080608-kaminsky-many-ways-to-attack.html>.
[28] For example see *The Secure Domain System (DNS) Implementation Guide*, National Institute of Standards and Technology, <http://csrc.nist.gov/publications/nistpubs/800-81r1/sp-800-81r1.pdf>.

7. Measures to Detect or Prevent Unauthorized Change Activity

Routine monitoring to detect, isolate, and identify suspicious or anomalous behavior is a common, proactive best practice across networking and security disciplines. For example, network administrators routinely query or "ping" hosts to determine if they are operational or offline. Application (e.g., web) administrators routinely query applications hosted on operational systems to determine whether they are responding to queries as the intended configuration would dictate. And security administrators query or scan security systems such as firewalls to determine if the system is enforcing the intended security policy (e.g., by allowing approved connections and blocking connections that are not approved).

Database operators make similar efforts to verify that the database is available and that the data returned in response to a query are accurate. The WHOIS service and the DNS are essentially distributed databases that are updated, maintained and operated by registrars and registries. Registrants have a stake in assuring that data associated with domain names they have registered in both of these databases are accurate and available. This section discusses the utility of monitoring the WHOIS service and the DNS to verify that your domain name registrations have not been altered without authorization and that the DNS is resolving your domain names as you intended.

7.1 Monitoring for WHOIS Change Activity

Organizations and individuals should consider measures to routinely monitor registration information for all registered domains. Proactively monitor domain name registrations using the WHOIS service of your registrars, registries, or third party operators. A representative response to a WHOIS query appears below:

```
Domain Name:ICANN.ORG
Created On:14-Sep-1998 04:00:00 UTC
Last Updated On:26-Mar-2010 15:12:28 UTC
Expiration Date:07-Dec-2012 17:04:26 UTC
Sponsoring Registrar:GoDaddy.com, Inc. (R91-LROR)
Status:CLIENT DELETE PROHIBITED
Status:CLIENT RENEW PROHIBITED
Status:CLIENT TRANSFER PROHIBITED
Status:CLIENT UPDATE PROHIBITED
Status:DELETE PROHIBITED
Status:RENEW PROHIBITED
Status:TRANSFER PROHIBITED
Status:UPDATE PROHIBITED
Registrant ID:CR12376439
Registrant Name:Domain Administrator
Registrant Organization:ICANN
Registrant Street1:4676 Admiralty Way
Registrant Street2:Suite #330
Registrant City:Marina del Rey
Registrant State/Province:California
Registrant Postal Code:90292
Registrant Country:US
Registrant Phone:+1.3103015817
Registrant FAX:+1.3108238649
Registrant Email:domain-admin@icann.org
```

```
Admin ID:CR12376441
Admin Name:Domain Administrator
Admin Organization:ICANN
Admin Street1:4676 Admiralty Way
Admin Street2:Suite #330
Admin City:Marina del Rey
Admin State/Province:California
Admin Postal Code:90292
Admin Country:US
Admin Phone:+1.3103015817
Admin FAX:+1.3108238649
Admin Email:domain-admin@icann.org
Tech ID:CR12376440
Tech Name:Domain Administrator
Tech Organization:ICANN
Tech Street1:4676 Admiralty Way
Tech Street2:Suite #330
Tech City:Marina del Rey
Tech State/Province:California
Tech Postal Code:90292
Tech Country:US
Tech Phone:+1.3103015817
Tech FAX:+1.3108238649
Tech Email:domain-admin@icann.org
Name Server:NS.ICANN.ORG
Name Server:A.IANA-SERVERS.NET
Name Server:C.IANA-SERVERS.NET
Name Server:B.IANA-SERVERS.ORG
Name Server:D.IANA-SERVERS.NET
DNSSEC:Signed
DS Created:26-Mar-2010 15:12:06 UTC
DS Maximum Signature Life 1:3456000 seconds
DS Created:26-Mar-2010 15:12:28 UTC
DS Maximum Signature Life 2:3456000 seconds
```

Compare the results against the registration data you expect to find. In particular, and for each domain name you have registered, ask the following questions:

- Does the date indicated as the last date on which the registration was modified match the date you most recently made an authorized change to your registration?
- Are the data returned in WHOIS responses for registrant, technical, and administrative contacts for this domain name complete and accurate (i.e., the data are exactly what you intended to be published)?
- Are the names servers listed in the registration record the exact list of name servers that provide authoritative name service for your organization?
- Is the sponsoring registrar the registrar with whom you do business for this domain name?
- Is the status of the domain what you expect it to be? (Refer to section 7.3 Setting and Monitoring Domain Status.)
- Do the creation and expiration dates for the domain registration match the dates you registered the domain and the date on which your current registration expires?
- Is the DNSSEC signing information correct? (Refer to section 6.2 DNSSEC Support Considerations.)

Inaccuracies or omissions in the data returned from one or more WHOIS services merit immediate action. Organizations can model this action after other problem resolution or incident responses your organization uses and should take into consideration factors that justify escalating the event from a trouble report to an incident. For example, organizations should distinguish a change that was necessary and non-threatening but did not receive all internal authorizations – for example, the technical contact modified DNS but did not notify the registrant or administrative contact – from a change that is strongly indicative of an attack – for example, the sponsoring registrar and registrant contact information have changed without authorization from any responsible party within the organization.

As the responses from WHOIS servers are generally stable and consistent over time, it is possible to automate WHOIS monitoring using scripting languages available from common operating systems. Execution of scripts that query WHOIS service(s) at regular intervals, compare the registration data in the response against expected data, and generate an alarm(s) if the comparison fails can provide a detection system to protect against erroneous or malicious alteration of domain name registrations.

Commercial client applications and interactive web applications are also available to perform these and similar automated tasks. Some of these applications are straightforward and can be used routinely by individuals, small businesses, or any organization that has a small enough number of domains that manual monitoring is worth the effort. Certain registrars and third party domain name protection services will monitor and safeguard domain name registrations for their customers. Given their relative technical simplicity, these services are frequently free or incorporated into of a larger brand-protection package.

7.2 Monitoring DNS Change Activity

Organizations and individuals should consider measures to routinely monitor the operational status and zone data published by authoritative name servers for all registered domains. The objectives of this monitoring activity are to assure that name service for each domain name registered by your organization remains configured as you intended it to be and returns complete and accurate data in accordance with DNS standards and best practices.[29] Prior to monitoring DNS change activity, test your name server configurations carefully, and archive copies of what your tests confirm as the baseline correct configuration. Next, implement or contract a third party to monitor for change activity at all of your name servers. Conceptually, this monitoring involves the following confirmation activities:

1. Are the name servers identified in the WHOIS response for the domain name the complete and accurate set of name servers that your organization has identified as providing authoritative name service for the domain?

[29] RFCs 1034, 1035 (tbd)

2. Are the name servers published in the TLD zone file for the domain name the complete and accurate set of name servers that your organization has identified as providing authoritative name service for the domain?
3. Are the name servers operational (e.g., do the hosts respond to a ping or simple DNS query)? Are they performing as expected?
4. Are all the name servers secured (hardened against known attacks)? Are all software (OS, name server) packages current with respect to approved versions (e.g., tested and approved by your technical staff), released hot fixes and patches?
5. Are the name servers responding in manners consistent with your baseline correct configuration?
6. Do all the name servers that provide authoritative name service for the domain return complete and correct zone data for all formulations of DNS queries against the zone?

It is possible to automate DNS monitoring using scripting languages available from common operating systems. Execution of scripts that query name servers at regular intervals, compare the zone data in the response against expected data, and generate an alarm(s) if the comparison fails can provide a detection system to protect against erroneous or malicious alteration of zone data.

Commercial client applications and interactive web applications are also available to perform zone data checks and name server configuration checks. Some of these applications are straightforward and can be used routinely by individuals, small businesses, or any organization that has a small enough number of domains that manual monitoring is worth the effort. Certain registrars and third party domain name protection services will monitor and safeguard zone data for their customers. Given their relative technical simplicity, these services are frequently free or incorporated into of a larger package, perhaps as part of an outsourced DNS service or web monitoring service.

For registrants that use domain names as part of their operational environment, such DNS consistency checking services are also useful as troubleshooting tools when diagnosing operations issues. Underlying DNS issues can lead to surprising results that are difficult to diagnose simply because DNS is generally so reliable.

7.3 Setting and Monitoring Domain Status (Domain Locks)

As described above, a registrant typically registers a domain name through an agent for a registry, called a registrar. A registry maintains a database of delegations (labels) and details of domain names registered in a TLD. For ICANN gTLDs and many ccTLDs, the registrar typically communicates with a TLD registry to add the label to the registry database using the Extensible Provisioning Protocol (EPP, RFC 5730). This provisioning protocol structures the communication over a client-server relationship between the registrar (client) and registry (server). The protocol allows both the registrar and the registry to set certain statuses on domain names. Several of these status codes, also known as *domain locks*, are important for registrants, as they control what actions may be

performed on a registered domain name; in particular, certain of these status codes are intended to help prevent registry changes that the registrant either did not intend or authorize.

7.3.1 Registrar (Client) Status Codes

Certain registrars permit registrants to control one or more registrar (client) status codes. The following status codes, also known as *registrar locks*, are of particular importance to registrants:

clientTransferProhibited. When set, the registry will not allow a registrar to accept a transfer of the domain name away from the sponsoring registrar. Certain registrars automatically keep the clientTransferProhibited status set on domain names and registrants use a third party authorization process between the "transfer-from" registrar, the "transfer-to" registrars and the registry to protect against unauthorized transfers.

clientUpdateProhibited. When set, the registry will not make changes to the registration details of the domain name. Certain registrars automatically unlock and re-lock this status when a registrant has successfully logged into a domain account. Other registrars allow registrants to unlock and re-lock this status through a domain management interface.

clientDeleteProhibited. When set, the registry will reject requests to delete a domain name from the registry.

The SSAC encourages registrants to make certain that clientTransferProhibited is set to prevent unauthorized or unintended transfer of a domain away from the rightful registrant to a different party (e.g., a hijacker). SSAC also encourages registrants to make certain that clientUpdateProhibited is set to prevent changes to registration contact or DNS configuration information without first unlocking this status.

Many registrars issue notifications when certain client status codes are modified. These notifications are extremely important because they may forewarn registrants of unauthorized registration account access.

Client status information is typically returned in responses to WHOIS queries, as illustrated in the following partial WHOIS response:

```
Domain Name: WESTBANKIOWA.COM
Registrar: DIRECTNIC, LTD
Whois Server: whois.directnic.com
Referral URL: http://www.directnic.com
Name Server: NS1.LH.NET
Name Server: NS2.LH.NET
Status: clientDeleteProhibited
Status: clientTransferProhibited
Status: clientUpdateProhibited
Updated Date: 08-jul-2009
Creation Date: 03-jun-1998
Expiration Date: 02-jun-2013
```

We encourage registrants to incorporate routine checks of registrar locks in WHOIS monitoring activities.

7.3.2 Registry (Server) Status Codes

Certain registrars and registries work cooperatively to offer registrants the ability to add server status codes (*registry locks*) as an additional layer of protection beyond client status codes. Registars submit requests for registry locks (serverDeleteProhibited, serverUpdateProhibited, serverTransferProhibited) for domain name(s) at the request of a registrant. The registry verifies that the registrar submitting the request is the registrar-on-record for the domain names prior to setting the lock. Once the locks are enabled, the registry uses a highly secure verification and authentication process to assure that changes requests have been authorized by the registrant, through the registrant's (chosen) registrar-on-record).

Registry lock information is returned in WHOIS queries, as illustrated below:

```
Domain Name: example.com
Registrar: MarkMonitor.com
Whois Server: whois.markmonitor.com
Referral URL: http://www.markmonitor.com
Name Server: NSF.WELLSFARGO.COM
Name Server: NSG.WELLSFARGO.COM
Name Server: NSH.WELLSFARGO.COM
Status: clientDeleteProhibited
Status: clientTransferProhibited
Status: clientUpdateProhibited
Status: serverDeleteProhibited
Status: serverTransferProhibited
Status: serverUpdateProhibited
Updated Date: 18-nov-2008
Creation Date: 28-apr-1993
Expiration Date: 29-apr-2013
```

We encourage you to consider setting registry locks as a complement to registrar locks for a second level of security against unauthorized transfer, deletion or change of registration information associated with your domain names.

We also encourage registrants to incorporate routine checks of registry locks in WHOIS monitoring activities.

DNSSEC information is returned in WHOIS responses, as illustrated in the abbreviated WHOIS response for ICANN.ORG, below:

```
Domain Name:ICANN.ORG
Created On:14-Sep-1998 04:00:00 UTC
Last Updated On:26-Mar-2010 15:12:28 UTC
Expiration Date:07-Dec-2012 17:04:26 UTC
Sponsoring Registrar:GoDaddy.com, Inc. (R91-LROR)
Status:CLIENT DELETE PROHIBITED
Status:CLIENT RENEW PROHIBITED
Status:CLIENT TRANSFER PROHIBITED
Status:CLIENT UPDATE PROHIBITED
Status:DELETE PROHIBITED
```

```
Status:RENEW PROHIBITED
Status:TRANSFER PROHIBITED
Status:UPDATE PROHIBITED
Registrant ID:CR12376439
Registrant Name:Domain Administrator
Registrant Organization:ICANN
.
.
.
Name Server:NS.ICANN.ORG
Name Server:A.IANA-SERVERS.NET
Name Server:C.IANA-SERVERS.NET
Name Server:B.IANA-SERVERS.ORG
Name Server:D.IANA-SERVERS.NET
DNSSEC:Signed
DS Created:26-Mar-2010 15:12:06 UTC
DS Maximum Signature Life 1:3456000 seconds
DS Created:26-Mar-2010 15:12:28 UTC
DS Maximum Signature Life 2:3456000 seconds
```

We encourage registrants to incorporate routine checks of DNSSEC "signed" status and signature information in WHOIS monitoring activities and that you factor DNSSEC into your DNS change activity monitoring.

8. Considerations When Choosing a Domain Registration Service Provider

Prior sections of this report describe measures organizations can implement to protect domain name registration accounts from misuse and to protect against error or unauthorized alteration of domain name registration data. Certain organizations may want to provide some or all of these measures using internal staff and resources. Other organizations may want to outsource; i.e., they will look for a domain registrar or another trusted party to protect domain names and registration accounts, or they will look for a registrar or another trusted party to complement in-house protective measures with further measures as an additional line of defense.

Domain registration service providers (registrars) have different target markets and service delivery models. SAC040 identifies two discernable models to illustrate that there is variation in the marketplace, but the registration service market is very competitive and registrars have implemented new service offerings since the publication of SAC040 and SSAC anticipates further market evolution.[30] In addition to domain name registration services, a growing number of (registrar) businesses now operate on behalf of

[30] From SAC 040, pages 9-1: "One popular service model offers domain name registration services at modest to low prices. Service delivery is highly automated and designed with an emphasis on processing transactions quickly, in high volume, in a consistent and repeatable manner that often minimizes opportunities for human error", *and* "A second registration service model offers protective measures to meet the needs of customers who place a high value on their domain names, consider their domain names and online presence to be business-critical, or recognize that their business or brands may be highly-targeted for abuse or criminal activities… The business model for these registrars is focused on handling individual transactions with a very low probability of error. The registrar caters to customers who place a premium on domain portfolio protection and are willing to pay a premium for human assistance (in particular, assistance by an account specialist assigned to the customer)."

organizations to provide as well as trusted parties outsourced domain management, online fraud protection, or online brand protection services.

Not only must organizations take these variations into consideration when choosing among ICANN-accredited registrars or third parties, organizations that register domains in ccTLDs also must consider the registration services that are idiosyncratic to the operators of those ccTLDs. While certain ccTLDs make arrangements with ICANN-accredited registrars to provide registration services, some ccTLDs perform registrations as part of their registry operation, and others make arrangements with business partners of their choice (who are not ICANN-accredited registrars). Even when using ICANN-accredited registrars to register domains in a ccTLD, the registrars abide by the ccTLD-specific rules, not standard ICANN rules.

Thus, in outsourcing scenarios, organizations will want to identify registrars and trusted parties that offer commensurate or complementary protective measures to those measures they have implemented internally and choose the best suited among these candidates to support them. This section discusses the information an organization should gather and the questions it should ask so that it can make an informed choice.

Organizations should select from and ask registrars and third party services about the availability of services such as those listed below in order to make an informed decision when choosing among candidates for managing domain registration services.[31] Most questions on the list are intended to help an organization build a picture of the set of services it would obtain by choosing a candidate registrar or third party service. Other questions are intended to help an organization determine whether it will have access to the same information they may currently rely upon to evaluate the integrity and effectiveness of in-house operations. Certain questions are the kind an organization might ask of any potential business partner and are intended to assist organizations in identifying registrars and third parties based on business practices and past performance (history).

Registrars or trust parties may publish some of this information on their web sites or in marketing collateral. Organizations can also obtain certain information through sales or service agents, or as a response to a request for product (RFP). Services in the list may result in additional cost beyond registration fees.

Many of the questions in this section address technical security issues. Readers should note that registrars have different policies with respect to disclosing answers to questions. In particular, certain registrars prefer to keep certain aspects of their security policies guarded, even from their customers, to prevent disclosure to the broader market or malicious actors. Readers should also note that certain security or protective measures may be available at additional cost over the basic registration fee.

---

[31] Individuals and businesses with one or few domains whose service needs may be satisfied by registrars that target consumer markets may wish to consider the article, *Top Ten Things to Consider When Registering a Domain Name*, available from Consumer Reports WebWatch <http://www.consumerwebwatch.org/pdfs/domainname.pdf>.

Question	Reason to Ask
What forms of documentation do you recognize as proof that a customer is the rightful registrant of a domain?	See the section entitled *Maintain documentation to "prove registration"*. Having the documentation your registrar needs to pursue a dispute request on hand can expedite resolution of your claim as rightful registrant of a deleted or wrongly transferred domain. Registrars that insist on legal documents, government IDs, etc. make registrant impersonation and hijacking more difficult.
Do you provide domain management services through a web interface? Can a customer request that the web-based registration interface be disabled for his account? Can a customer request that web-based access be restricted to a specific client system or application?	Web access to a registration account is convenient, but registration account portals, like all web applications, are vulnerable to attacks. Ask this question if you believe reducing exposure to web based attacks is necessary to minimize risk to your domain name assets. Certain registrars may implement some form of machine identification, system registration, client digital certificates, or secure cookie. Inquire about these.
What form of authentication do you use for customer login?	Passwords are the predominant method of authentication among registrars. You may conclude from your risk assessment that multi-factor authentication or verification by a designated registrar account representative is appropriate.
Do you provide a designated account representative?	Certain registrars assign a designated representative to an account. This representative verifies the authenticity of customers prior to processing change requests. Your risk assessment may lead you to conclude that you require exceptional measures for all domain name related administrative matters.
What forms of customer verification do designated account representatives use to verify the authenticity of a customer?	Government-issued form of identification such as passport, license, military ID, security questions are typical identification instruments.
What mechanisms do you employ to secure account login and domain management transactions? What mechanisms do you employ to detect attempts at unauthorized access?	Registration account transactions are typically authenticated and encrypted. Look for additional protective measures; for example, registrars may impose password complexity criteria; take additional measures to protect against password guessing attacks by limiting failed login attempts, etc.
What type of digital certificates do you use for server authentication in SSL transactions (Standard, Extended Validation)?	Certificate issuing authorities perform more thorough investigations of applicants for extended validation certificates than standard certificates. EV certificates add a measure of trust and confidence: the registrar has proven it is legally established business with a verifiable identity.
What form of account password recovery or reset do you support?	You should know whether the registrar provides automated password/recovery or requires human interaction/verification so that your internal processes and workflows are properly coordinated.

Question	Reason to Ask
Do you maintain domain registration account access or activity reports or logs? Do you provide domain registration account access activity reports or logs to registrants?	Understanding who is accessing registration accounts, how frequently, and for what purposes is as valuable a tool for domain name security as any other asset security (database, network, intranet). Your risk assessment may lead you to conclude that you need to incorporate this visibility into existing logging and reporting practices.
Do you offer per-domain access controls (or are all operations available to a user for all domains once the registration account user is authenticated)?	SAC040 notes that "Access to a domain registration account affords unrestricted access to all domains registered under that account, to users and attackers alike" and encourages registrars to offer customers "the ability to control which points of contact are able to make changes to contact and DNS confirmation information, initiate or authorize a domain transfer…"
Do you provide customers with the ability to set client status locks at a registry to block unauthorized transfer, delete, or update? Do you provide customers with the ability to set server status to block unauthorized transfer, delete, update (for registries that offer this service)?	See the section entitled Setting and Monitoring Domain Status (Domain Locks)
What is your preferred method of communication to notify customers of changes to registration accounts and domain registration data?	Registrars typically prefer to use email for correspondence with registrants.
What additional methods of communication do you use, and under what circumstances do you use these?	You should know what additional methods of communication registrars use, and when, so that your internal processes and workflows are properly coordinated.
Can you provide a list of change notifications or confirmations you send via email? Can you provide sample electronic copies of email correspondence?	See Incorporate registrar email correspondence into domain management in the section entitled Protection against unauthorized account access
Do you use any form of secure email or email authentication (DKIM, sender IP verification, PGP)?	Secure email increases the level of confidence that notifications from registrars are legitimate.
What measures do you take to protect customers against registrar impersonation (phishing) attacks?	Look for registrars that aggressively monitor and quickly respond to registrar impersonation attacks and that use community sites/blogs or other non-email methods to notify registrants of such attacks.
Do you host authoritative name service for customers?	Certain organizations may benefit from outsourcing name service for their domains to a registrar who has more capacity, diversity and DNS competency than the organization can afford.
Do you perform redirection or wildcarding of non-existent subdomains in a customer's domain by default? Can my organization opt-out of this practice?	SAC032[32] explains the risks associated with redirection and recommends that customers opt-out of this practice.

[32] Security and Stability Advisory Committee, P*reliminary Report on DNS Modification*, SAC032, <http://www.icann.org/en/committees/security/sac032.pdf>.

Question	Reason to Ask
What forms of DNS monitoring do you provide for customers? What types of DNS configuration and zone checking procedures do you implement? Do you provide name server or zone data activity reports or logs to customers?	See the section entitled Monitoring DNS change activity
Do you provide WHOIS monitoring services? How frequently does the WHOIS service update?	See the section entitled Monitoring WHOIS change activity Delays in WHOIS updates can thwart monitoring scripts
Do you provide privacy protection services? Directly or through a business partner?	Ask registrars to explain the disclosure practice, whether and how you are notified when law enforcement or another party is provided access to the privacy protected registration information, and whether you are provided with the identity of the inquiring party
Do you support DNSSEC? If yes, describe DS processing, measures for key protection, and key revocation and change management procedures.	See the section entitled DNSSEC Support Considerations
Do you provide customers with descriptions of incident and abuse response practices? What assistance do you provide customers in cases involving a domain hijacking or dispute over rightful registration?	This information is useful to you if you must pursue a domain related incident such as a phishing attack against one of your domain names, so that your internal processes and workflows are properly coordinated.
Do you provide customers with abuse or incident points of contact information?	SAC038 recommends that registrars provide an abuse point of contact and make contact information publicly available. [33] Ask what hours of operation these points of contact are available, and what authority do these points of contact have when dealing with abuse or circumstances requiring urgent attention.
What certifications or regulations has your organization satisfied (demonstrated compliance, e.g., PCI, ISO 27000…)? What external audit services, if any, do you employ?	Knowing that the registrar has satisfied such certifications will increase your level of confidence that the registrar is a business entity you can trust.
Have you ever been issued a notice of breach of agreement from ICANN for failure to comply with the terms of the registrar accreditation agreement?	Knowing that the registrar has satisfied its contractual obligations with ICANN will increase your level of confidence that the registrar is a business entity you can trust.
Do you participate in the ICANN Data Escrow program?	If your registrar participates in the ICANN Data Escrow program and the registrar ceases its operations, information associating your organization with the domains you have registered has been securely archived and your registration (and DNS services) can be restored through an interim registrar or registrar of your choosing.

[33] Security and Stability Advisory Committee, *Registrar Abuse Contacts*, SAC038, <http://www.icann.org/en/committees/security/sac038.pdf>.

Question	Reason to Ask
Do you offer any services or features that distinguish your registrar from other registrars?	This is an intentionally open-ended question that provides registrar operators to describe services or features that may be unique or that may be useful to certain registrants.

9. Registry Considerations

Generally, registrants do not do business directly with gTLD and certain ccTLD registries. What registries an organization determines are appropriate TLDs for domains they register is a topic that is out of scope for this report. However, there are certain service and operational aspects of registries that we believe merit registrant consideration. In particular, several of the considerations mentioned in this section relate to service offerings that can be facilitated through a registrar.

Question	Reason to ask
Do you support a registry side lock?	See the section entitled Setting and Monitoring Domain Status (Domain Locks)
Describe your DNS infrastructure (diversity, etc.)	Certain organizations may want to consider capacity, diversity and DNS competency of a registry operator when choosing a TLD in which to register domains.
Do you support multifactor authentication of registrars?	Multifactor authentication of enhances security registrar-registry transactions. Ask the registry to identify the factors in authentication system (software or hardware tokens, passwords, certificates) and how they are managed.
What is your zone file access policy	Many organizations make use of TLD zone files to monitor domain name registrations for phishing attacks, infringements against trademarks and intellectual property.
Do you accept registrations from registrars other than ICANN accredited registrars?	The business and operational criteria ICANN accredited registrars must satisfy is well documented at ICANN.ORG. Ask what criteria the registry sets for registrars who are not ICANN accredited.
Do you provide an interface to enable registrars to submit DNSSEC records?	See the section entitled Making Use of and Monitoring DNSSEC.
What is your policy regarding abuse and malicious domains?	This information is useful to you if you must pursue a domain related incident such as a phishing attack against one of your domain names, so that your internal processes and workflows are properly coordinated.
Do you publish an abuse hotline/POC? Do you support 24x7 abuse support to registrars?	While registrants normally deal with domain name related incidents through registrars, it is important ton know what options the registry may offer under exceptional circumstances.

Question	Reason to ask
How frequently does the WHOIS service update?	Delays in WHOIS updates can thwart monitoring scripts
What certifications or regulations has your organization satisfied (demonstrated compliance, e.g., PCI, ISO 27000, SysTrust…)? What external audit services, if any, do you employ?	Knowing that the registry has satisfied such certifications will increase your level of confidence that the registry is a business entity you can trust.
Do you offer any services or features that distinguish your registry from other registries?	This is an intentionally open-ended question that provides registry operators to describe services or features that may be unique or that may be useful to certain registrants.

10. Summary and Conclusions

In this report, we have attempted to raise appreciation and awareness of the growing importance of domain name registrations. We have explained that domain names are personal or corporate assets and encouraged you to protect them accordingly. We have explained how you or your organization can manage domain name registrations and mitigate risk by either implementing protective measures directly or by choosing a domain name registrar who can mitigate risks effectively on your behalf. We have provided a list of questions to ask both registrars and registries that will help you make informed choices when selecting a registrar.

11. Acknowledgments, Statements of Interests, and Objections and Withdrawals

In the interest of greater transparency, we have added these sections to our documents to provide the reader information on three aspects of our process. The Acknowledgments section lists the members who contributed to this particular document. The Biographies and Statements of Interest section points to the biographies of the Committee members and any conflicts of interest, real, apparent or potential, that may bear on the material in this document. The Objections and Withdrawals section provides a place for individual members to disagree with the content of this document or the process for preparing it.

11.1 Acknowledgments

The committee wishes to thank the following SSAC members and invited guests for their time, contributions, and review in producing this Report.

David Conrad
Jim Galvin
Duncan Hart
Jeremy Hitchcock
Warren Kumari
Xiaodong Lee
Dan Simon

Bruce Tonkin
Rick Wilhelm

11.2 Statements of Interest

SSAC member biographical information and Statements of Interest are available at: http://www.icann.org/en/committees/security/biographies-07jul10-en.htm.

11.3 Objections and Withdrawals

There are no objections or withdrawals.