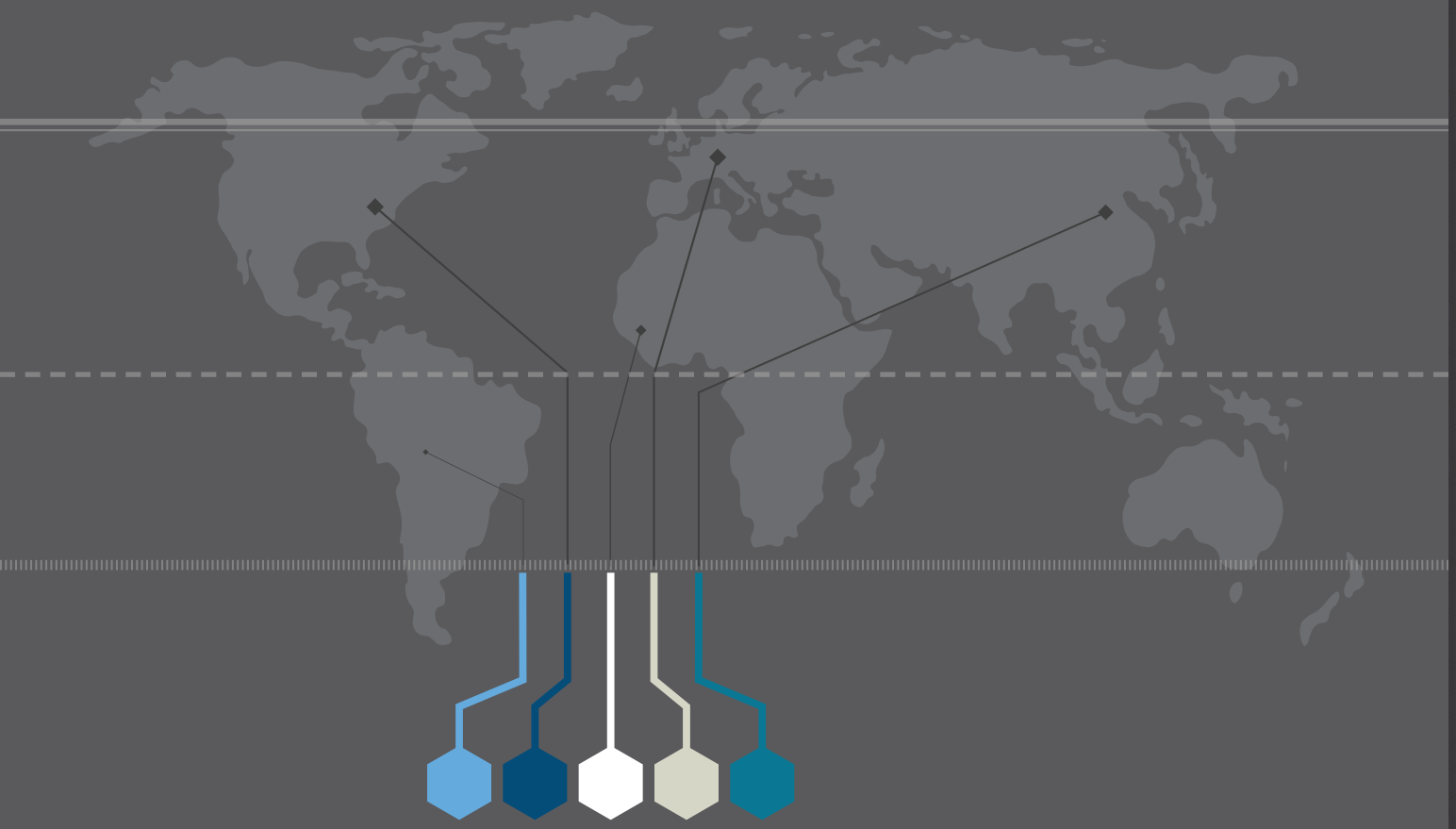
THE COST OF DOING NOTHING:
THE BUSINESS CASE FOR PROACTIVE ANTI-ABUSE



SECUREDOMAIN FOUNDATION

JUNE 2015

INTRODUCTION | WHAT'S IN A DOMAIN NAME?

The Domain Name System (DNS) is one of the most revolutionary innovations in human history, spurring unparalleled global interconnectivity, freedom of communication, and entirely new industries. Yet, the overwhelming success of DNS puts it at the epicenter of criminal activity too. Domain name abuse plays a significant role in the perpetration of cybercrime, providing infrastructure for phishing, spam, and the command and control of botnets. In the second half of 2014 alone, there were 95,321 distinct domain names used for phishing according to the Anti Phishing Working Group, 27,253 of which were registered by phishers specifically for malicious purposes.[1] This cybercrime phenomenon has a significant financial impact on the entire Internet ecosystem,[2] with one study putting the price tag at a staggering $400 billion (USD) annually for consumers and businesses.[3]

Despite the significant consequences of domain name abuse, stopping cybercriminals from abusing the DNS is no easy task. Even if a domain name is taken down, the malicious site behind it can still remain on hosting servers, accessible via IP addresses, and, rather quickly, return to the DNS with a newly registered domain name assigned to it.[4] This well-known cat and mouse game means that all types of Internet infrastructure providers have a role to play in thwarting cybercrime. To address this, legal requirements have evolved over the past decade in the form of contracts and policies to create an impetus for registrars, registries, and hosting companies to act on abuse complaints. This has effectively enshrined anti-abuse into the normal course of business for many Internet infrastructure providers, especially registrars.

the cost of cybercrime is $400 billion per year

In order to better understand the business costs domain name abuse imposes on Internet infrastructure providers, the Secure Domain Foundation (SDF) surveyed registries, registrars, and hosting providers. Although the survey was open to all three groups, this first report focuses on registrars and the issues unique to them.

[1] APWG, Global Phishing Survey: Trends and Domain Name Use in 2H2014, May 27, 2015, http://docs.apwg.org/reports/APWG_Global_Phishing_Report_2H_2014.pdf

[2] German ISPs spent 2 million Euro to establish a botnet call center in an effort to mitigate infections on their customers' computers. See generally Ross Anderson, et. al., Measuring the Cost of Cybercrime, WEIS 2012, http://wiki.adaptive.cs.unm.edu/readings/2012%2005%20Anderson_WEIS2012%20measuring%20cost%20of%20cybercrime.pdf;

[3] McAfee, Net Losses: Estimating the Global Cost of Cybercrime, *Center for Strategic and International Studies*, June 2014, http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf

[4] CENTR, Analysis of Blocking and Redirection of Domain Names as Tools to Restrict Access to Content, p. 3 (2012), https://centr.org/CENTR-Paper-Domain_blocking

SECURE DOMAIN FOUNDATION | KEY FINDINGS

- Bad customers are bad for business
- Reactive anti-abuse does not appear to offer any economic advantages for registrars and can actually cost more money in terms of human resources spent addressing abuse complaints
- Registrars could likely save money if complainants provided thorough, accurate, and relevant information in their initial complaint. A standardized complaint form could help address this issue.
- The time and money expended reviewing abuse complaints does not scale but instead equates to a relatively fixed minimum cost per abuse complaint
- Domain name abuse stemming from domain names sold by resellers can create additional labor costs because of the added back-and-forth communication between a registrar and their reseller to resolve an abuse complaint
- Proactive anti-abuse that prevents would-be bad customers from becoming customers or weeds them out once they are registrants can lower the number of abuse complaints and therefore save money
- Registrars fall into three anti-abuse profiles: proactive, passive, and reactive

SDF surveyed registrars, registries, and hosting companies. Each was asked to provide basic profile information about the size and type of their business. Respondents also were asked to describe their anti-abuse practices from the time of sale through the point at which a complaint was filed, investigated, and closed. Additionally, respondents were queried about the cost at each point in their anti-abuse process and variables that might affect such costs. Lastly, those surveyed were asked for suggestions on how to improve anti-abuse efforts. All of the questions solicited open-ended, free response answers to get a better sense of the wide range of issues affecting respondents' involvement in anti-abuse activities.

This inaugural SDF research effort did not achieve a high survey response rate. Some companies expressed concern about divulging information related to their domain name abuse encounters while others simply did not respond to requests for participation. Nonetheless, the analysis in this report is drawn from the responses of registrars managing a combined total of more than 35 million registered domain names, roughly 12 percent of the market share.[5] Accordingly, the survey results provide meaningful conclusions and showcase useful anecdotes for understanding the costs of domain name abuse.

For context, this report highlights relevant legal, reputation, and financial factors likely to influence the business climate in which Internet infrastructure providers operate.

[5] Based on Verisign's estimated total of 284 million registered domain names. See Verisign, The Domain Name Industry Brief, Vol. 11, Issue 4, Jan. 2015, https://www.verisigninc.com/assets/domain-name-report-january2015.pdf

LEGAL

There are many legal requirements imposed upon Internet infrastructure providers to reactively or proactively take action against domain name abuse or respond appropriately to domestic legal processes such as court orders. Cumulatively, terms of service agreements, domestic laws, ccTLD registry contracts, and ICANN contracts prohibiting abusive behavior create incentives for Internet infrastructure providers to act against domain name abuse, which can translate directly into business costs. Specific to registrars, legal dynamics are shaped, in part, on whether the registrar is an ICANN-accredited gTLD provider or an independent ccTLD.

To maintain ICANN accreditation, new and recently accredited gTLD registrars must comply with enforcement obligations under section 3.18 of the 2013 RAA. Among other responsibilities, this provision requires that registrars undertake reasonable investigations into abuse complaints and not merely wait until the receipt of a court order to commence the investigative process.[6] Instead, section 3.18.2 requires registrars to review well-founded reports of illegal activity from "law enforcement, consumer protection, quasi-governmental or other similar authorities" within 24 hours.[7] Even if a registrar is subject to a local law requiring a court order then it still must notify ICANN of the relevant law and the reason for its failure to investigate such reports. These obligations effectively mean that abuse reports cannot simply be ignored because the consequence of inaction could be the loss of accreditation.

- Legal requirements to respond to abuse complaints create compliance costs for ccTLD and gTLD registrars
- ccTLD and gTLD registrars face legal pressures to act because of internal policies, terms of service agreements, local laws, and contracts
- The 2013 RAA requires gTLD registrars to investigate and not ignore abuse and WHOIS inaccuracy complaints
- Lawsuits and court orders can increase business costs

[6] John Horton, Section 3.18 of the 2013 RAA: Reasonable Investigations, Appropriate Responses, CircleID, Dec. 8, 2014, www.circleid.com/posts/20141208_section_318_raa_reasonable_investigations_appropriate_responses/

[7] ICANN, 2013 Registrar Accreditation Agreement, https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en

LEGAL *cont.*

Like many anti-abuse frameworks, Section 3.18 is not without controversy. For example, the extent to which Section 3.18 compels action in certain circumstances, such as when there are duplicate complaints, may be interpreted differently by various parties.[8] Nonetheless, even if somewhat ambiguous, it is clear that Section 3.18 creates compliance obligations for gTLD registrars that can translate into resource costs. Likewise, another compliance obligation stems from Section 3.7.8 of the 2013 RAA and the WHOIS Accuracy Specification.[9] This requires a registrar to investigate WHOIS inaccuracy complaints and ultimately suspend domain names that fail to comply with such requirements, creating another impetus for registrar involvement.

Beyond ICANN contracting parties, there are 256 ccTLDs,[10] none of whose registrars may be bound by the 2013 RAA. Nonetheless, most ccTLDs are subject to the national laws of their respective countries and define their anti-abuse policies through terms of service agreements.[11] Consequently, the degree to which a ccTLD faces legal and contractual pressure to combat abuse varies.[12] However, like their gTLD counterparts, ccTLDs generally prohibit domain name abuse in their user agreements and employ anti-abuse desks to handle complaints. In many cases, ccTLDs are more diligent in combating abuse; and in some cases, not.

[8] Joseph Wright, ICANN Compliance, Domain Registrars Clash on New Whois, Abuse Report Language, Bloomberg BNA, April 23, 2015, www.bna.com/icann-compliance-domain-n17179925626/

[9] Supra note 7

[10] Markus Jakobsson, 4.4.7 CCTLDs: The Sovereign Domain Extensions, The Death of the Internet (July 2012)

[11] A comprehensive list of ccTLD terms of service policies can be found at Hexonet, ccTLD Domain Name Policies, May 13, 2014, https://www.hexonet.net/legal/ccTLD_domainname_policies_na

[12] Thibault Verbiest, et. al., Study on the Liability of Internet Intermediaries, Markt/2006/09/E Service Service Contract ETD/2006/IM/E2/69, Nov. 12, 2007, 104-5, http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf

REPUTATION

In an era of widespread malware, botnet, phishing, and spam websites inundating email inboxes and private networks, many cybersecurity solutions utilize blocklists and whitelists to regulate traffic.[13] This creates the risk that a TLD with a bad reputation might be completely blocked. Similarly, traffic from specific IP addresses, email addresses, and other attributes can end up blocked. Ultimately, a registrar deriving significant portions of their income from the registration of malicious domain names may become the target of law enforcement. This reality, coupled with increased inventory from new TLDs,[14] makes reputation an important factor in attracting clients to sustain and increase domain name registrations and revenue.

There are business incentives for maintaining a good reputation instead of spending time, money, and resources to repair a reputation down the road. Consequently, some registrars devote resources to responding to complaints in media coverage, on social media, and through Better Business Bureau (BBB) offices (North America).

[13] He Liu, et. al., On the Effects of Registrar-level Intervention, LEET 2011, https://cseweb.ucsd.edu/~klevchen/llfkmvs-leet11.pdf

[14] Michael Berkens, New gTLD's Registrations Top 5 Million; .Science & .Link Break 100K: We Break Down the Numbers, The Domains, April 10, 2015, www.thedomains.com/2015/04/10/new-gtlds-registrations-top-5-million-science-link-break-100k-we-break-down-the-numbers/

FINANCIAL BURDENS

Internet infrastructure providers pay the salaries of employees that handle abuse complaints or contract with outside entities to do so. Many of these in-house employees fulfill multiple roles within the company, often serving as attorneys. This means that the time spent investigating and responding to an abuse complaint could decrease productivity in another area for a company. Adding to this conundrum, registrars fielding a high level of complaints might need to increase the size of their abuse teams as a result.

Beyond labor costs, there are more discrete financial risks. Registrars may be subject to credit card charge backs, comprised of refunds and penalties, when it is later determined that a domain name was purchased through fraudulent means. Over time, repeated credit card charge backs can increase the transaction rate charged by registrars' payment processors. Legal costs, from defending lawsuits or complying with court orders, also can impose significant financial burdens on registrars dealing with domain name abuse. Taken together, increased financial costs for the registrar may be passed on to consumers through the form of increased registration fees, which might make a registrar less competitive than a competitor with lower domain name abuse overhead costs.

- **labor costs**
- **charge backs**
- **penalties**
- **increased fees**
- **legal costs**

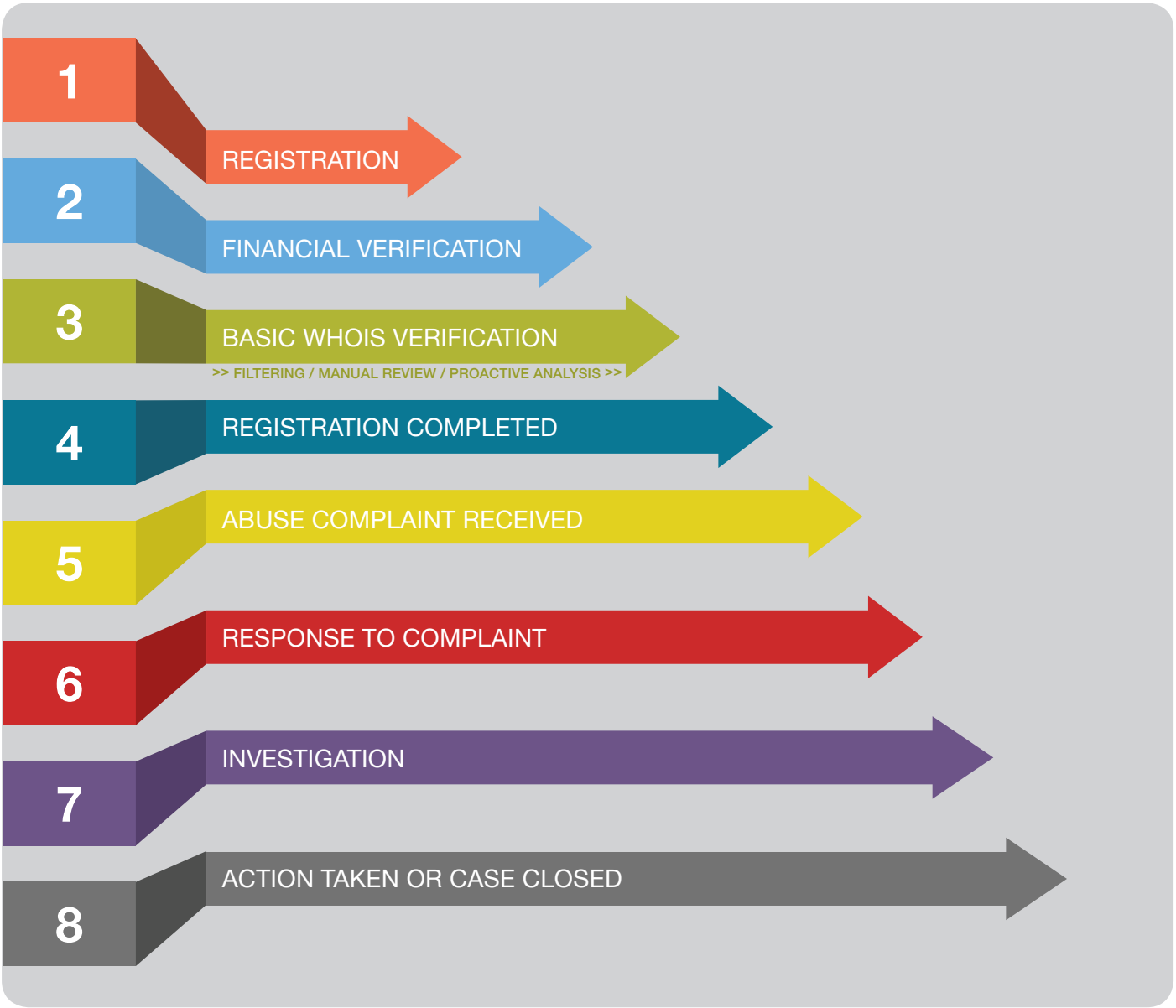
Within the aforementioned legal, reputation, and financial framework, survey respondents were asked to describe their anti-abuse practices, costs, and ideas for improvement. Responses indicated that there are many common elements in each registrar's domain name abuse complaint response process.

POINT OF SALE

Respondents' specific approaches to domain name abuse ranged from purely reactive to highly proactive, and everything in between. One respondent simply verifies the validity of would-be customers' payment methods. Doing a bit more, one large registrar undertakes a manual review of both reseller accounts as well as potential-registrants flagged for suspicious credit card information. Whereas another registrar blocklists certain words, such as "paypal," to prevent new spoofed registrations. Going further, some of the registrars proactively assess whether or not the customers' credentials match those used in known malicious activity. This includes correlating IP addresses to determine whether they have been associated with domain names registered purely for phishing, botnets, or spamming.

Each of the respondents requires that their customers consent to terms of service that prohibit the use of registered domain names for malicious purposes.

DOMAIN NAME REGISTRATION SCREENING & COMPLAINT PROCESS



Upon receipt of an abuse complaint, all of the respondents described a similar process that involved a manual review to assess the validity of the accusations and determine the appropriate course of action. This commonality is likely influenced by the requirements of RAA 3.18, terms of service agreements, and best practices.

COMPLAINT PROCESS *cont.*

The complexity of the circumstances, including the potential privacy or business interests of a customer, and the overall legitimacy of allegations affect how much time a registrar spends to resolve a complaint. The standard process begins with the receipt of a complaint into a (automated) queue system, followed by a manual review of the complaint to determine the next course of action, and corresponding with the complainant to gather information if necessary. Next, domain name accounts with blatant, obvious violations are suspended, and the customer is notified. One large registrar indicated that they offer an offending customer seven days to correct a problem and provide identification before automatically suspending their account. Notably, content-based complaints[15] or complaints involving the potential hacking of a legitimate business' domain name involve greater back and forth communication with the complainant and registrant.

Other variables can affect the beginning of the abuse complaint process. For example, ICANN accredited registrars might receive complaints forwarded by ICANN, triggering further back-and-forth communication. Similarly, when relevant, a registrar will notify the appropriate reseller that an abuse complaint has been filed related to a domain name that they sold. These factors can increase the staff hours spent conducting the investigation process.

After an initial investigation, baseless complaints are dismissed with no further action taken. For the rest, resulting actions include responding to the complainant with the registrar's findings, educating a complainant, taking down the relevant domain name,[16] and, for cases involving credit card fraud, refunding money and paying a credit card chargeback. Other potential actions not mentioned by the respondents include transferring control over an abusive domain name for DNS sinkholing, unmasking the privacy of the offending registrant's WHOIS information, and exposing other domain names held by an account tied to blatant malicious activity. These options become possible for many registrars once a registrant has breached the terms of service.

All of the respondents agreed that the most expensive part of the abuse complaint process involved the labor costs of conducting the aforementioned review and correspondence steps. From the responses, the amount of time spent manually reviewing a single complaint ranged from an average of 15 minutes for one registrar to 10 hours for another. This amount

[15] This can be due to the fact that sometimes a Web hosting provider or Email service provider would be the more appropriate party to handle a complaint.

[16] Takedowns can be performed using a variety of methods. See ICANN SSAC, SSAC Advisory on Impacts of Content Blocking via the Domain Name System, SAC056, Oct. 9, 2012, https://www.icann.org/en/system/files/files/sac-056-en.pdf

COMPLAINT PROCESS *cont.*

of time translated into registrars spending anywhere from 80 cents (USD)[17] to roughly $65,[18] with one registrar estimating that it spends $30,000 annually to address complaints for its 850,000+ domain name business.

Credit card chargebacks seemed to be a minor issue for respondents. When faced with such fees, a registrar must refund the purchase price of the domain name and pay a fee to the credit card processor. Such fees vary. However, one indicated that it pays 14 Euros per credit card chargeback. If this happens often, then the afflicted registrar risks facing higher credit card processing fees, which can significantly affect a registrars' bottom line.

Most respondents indicated that court orders could increase the costs of addressing an abuse issue because of the time spent complying and the potential financial costs associated with hiring outside counsel. However, one respondent indicated that court orders sometimes reduce the costs associated with abuse complaints by saving the registrar time that would otherwise be spent investigating the validity of a complaint. Nonetheless, the same respondent indicated that lawsuits drastically increased the overall costs of abuse complaints.

[17] This seemingly trivial amount translates to costs of at least $100,000 per year for this particular registrar. Their costs range from $0.80 to $2.40 per complaint, putting their annual abuse costs in the $100,000 to $280,000 range.

[18] Based on a response indicating costs of 60 Euros per complaint.

PROACTIVE ANTI-ABUSE EFFORTS

In the absence of an abuse complaint, the results varied as to what degree registrars did anything to identify and mitigate domain name abuse. Three registrars indicated that they do not take any anti-abuse efforts unless they receive an abuse complaint or notification from a CERT. Others take proactive steps by employing ongoing screening for malware and phishing as well as working with cybercrime fighting NGOs. One registrar indicated that it scrutinizes its resellers to ensure that they will not pose a threat to its business by selling domain names that will be used for malicious purposes.

From the survey data, it is clear that registrars also vary with the degree to which they take proactive steps to ensure WHOIS accuracy. Some registrars merely contact a customer to correct a WHOIS record upon notification of an inaccuracy. Others proactively try to determine the veracity of their customers' WHOIS records.

There was a stark contrast in the number of abuse complaints received by registrars employing anti-abuse measures to screen out would-be registrants versus those that only respond to complaints. Notably, one purely complaint-driven registrar received nearly half as many complaints as a much larger proactive registrar despite managing only 20 percent as many domain names. The survey data demonstrated a strong correlation between being wholly reactive and the number of abuse complaints received, suggesting that proactive measures can drastically reduce the number of abuse complaints. Reducing the number of abuse complaints received is a significant factor in reducing the costs spent on domain name abuse efforts.

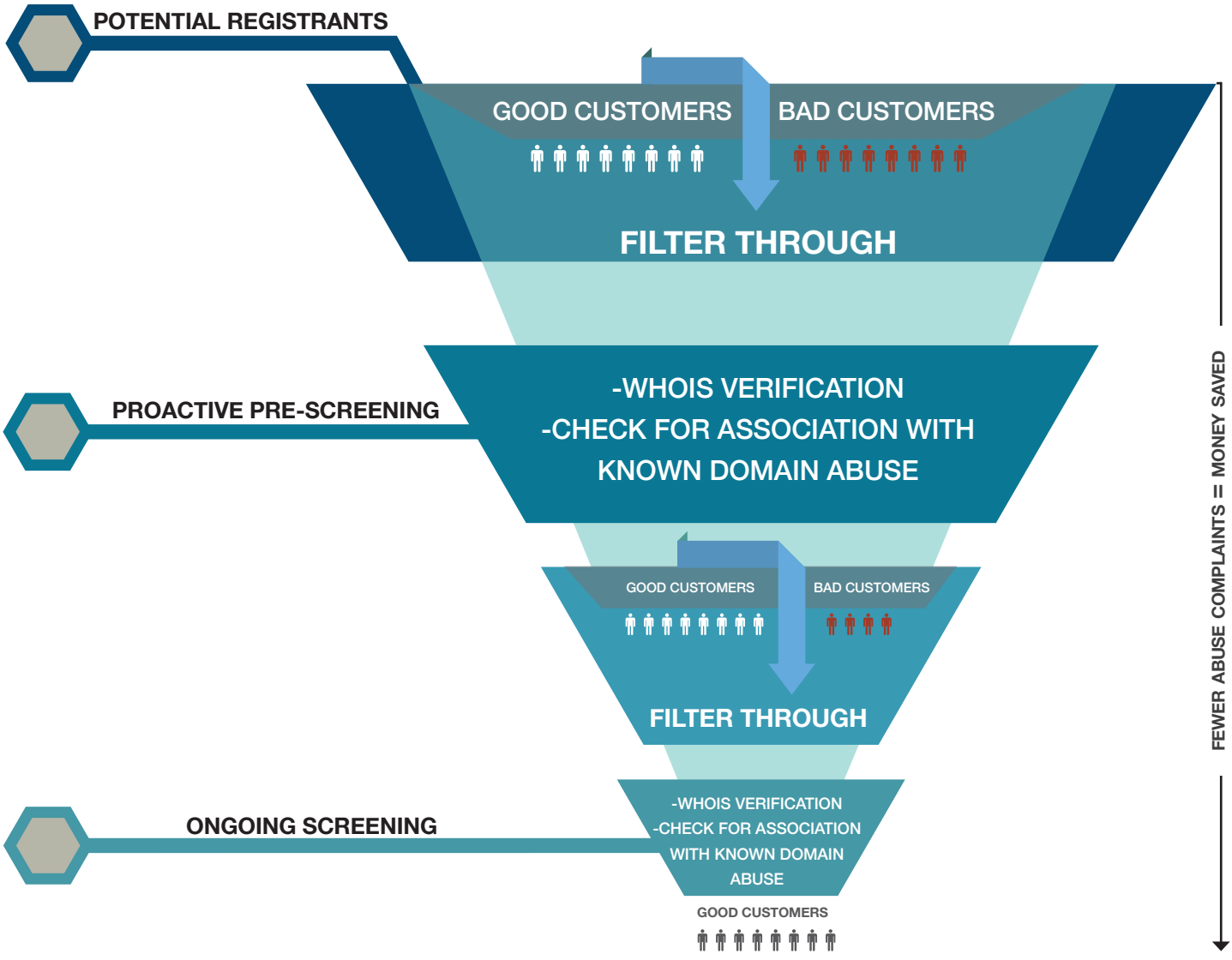
SUGGESTIONS FROM RESPONDENTS

Respondents were asked for suggestions on how to improve anti-abuse efforts, save costs, and prevent cybercrime. There was consensus on the need for the appropriate parties to receive relevant information to respond to abuse. For some, this means that content-related, intellectual property issues should be addressed with the website owner before involving a registrar and, in the context of domain name abuse, that hosting companies should work in tandem to stop malicious activities on their servers. To better accomplish this, one respondent suggested the creation of a universal domain name abuse complaint form to ensure that the complainant enters enough relevant information for an abuse allegation to be appropriately routed, investigated, and resolved with minimal back-and-forth communication.[19]

The survey data indicates that registrars perceive that there is a DNS literacy gap on the part of complainants. This means that there is an opportunity to improve the degree to which victims, attorneys, and law enforcement understand the domain name abuse process and how to find the parties best equipped to act on complaints. Notably, one respondent indicated that the time spent chasing down hosting companies that provide server space for malicious sites could be reduced if there was an automated system to extract name server information and automatically forward complaints to hosting companies. Taken together, the results highlight the potential business efficiencies that could be gained from proactive technical and interpersonal collaboration amongst Internet infrastructure providers.

[19] This concept can be found in other areas such as the insurance industry, in which a complainant uses a standard form to file a complaint.

CONCLUSIONS AND OPPORTUNITIES



Bad customers are bad for business. Proactive anti-abuse measures, such as screening potential customers' association with domain names, email, IP and physical addresses, as well as WHOIS data associated with maliciousness can prevent abuse complaints down the road. Once a potential-customer becomes a registrant then the contractual relationship defined by terms of use make many registrars wary of taking

swift and decisive action to shut down a domain name until after they have invested time to gather overwhelming evidence of domain name abuse. Nonetheless, proactive screening of customers' domain names for association with maliciousness can flag problems before they take the form of potentially time-consuming abuse complaints.[20]

This report indicates that many of the costs associated with domain name abuse are not fixed but instead variable costs, dependent upon the frequency of abuse complaints, time spent investigating them, and the degree to which fraud leads to financial penalties such as credit card chargebacks. Consequently, reactive anti-abuse measures, which have a strong correlation to abuse desk labor costs, do not scale well. However, there are opportunities to save money throughout the domain name registration process. A collaborative, community-based approach can help to better scale anti-abuse efforts to prevent one registrar's former bad customer from becoming another registrar's current problem. Ultimately, if a registrar is known as one that takes proactive steps against domain name abuse then that makes them less attractive for would-be domain name abusers and less likely to be inundated with abuse complaints.

Looking ahead, ICANN has increased its compliance budget.[21] For gTLD registrars, this might translate to increased scrutiny of WHOIS accuracy and Section 3.18 investigation practices, perhaps leading to more onsite audits. Regardless, proactive anti-abuse measures appear to be good for business and for promoting principles of industry self-regulation in a potentially transformative era in Internet governance. Doing nothing about domain name abuse except reacting to complaints can cost a registrar a lot more money in resources, time, and reputation.

[20] This method is touted as a best practice by the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG) and the London Action Plan (LAP). See M3AAWG & LAP, Domain Names and IP Addresses, Best Practices to Address Online, Mobile, and Telephony Threats, June 1, 2015, p. 33, https://www.m3aawg.org/sites/default/files/M3AAWG_LAP-79652_IC_Operation-Safety-Net_BPs2015-06.pdf

[21] ICANN, Contractual Compliance 2014 Annual Report, Feb. 13, 2015, https://www.icann.org/en/system/files/files/annual-2014-13feb15-en.pdf

SDF plans to contribute solutions to the domain name abuse reporting process to ensure that complainants provide necessary information to the appropriate party. Specifically, SDF members, in tandem with the broader DNS infrastructure community, can develop model domain name abuse complaint forms and, more importantly, model anti-abuse processes.

SDF hopes that more Internet infrastructure providers will participate in future research to support this important dialogue. Furthermore, SDF plans to conduct quantitative analyses on technical data about domain names associated with malicious activities. By assessing a greater pool of data, future research can extrapolate a more nuanced understanding of the ways in which different variables, such as business models, affect anti-abuse costs.