Abuse Desk Common Practices

Messaging Anti-Abuse Working Group (MAAWG)
Collaboration Committee
October 10, 2007

Introduction and Methodology

This document was assembled with the feedback received in the Abuse Desk Best Practices sessions in three MAAWG members' meetings beginning in October, 2006.

The intent of this document is to present options for abuse desk administrators for addressing common problems faced by abuse desks. This is **not** intended to represent an absolute set of best practices. It is our belief that what is "best" is frequently determined by the particular circumstances of the network/mailboxes served by the abuse desk.

Annalivia Ford from AOL and Laurie Jill Wood from Charter Communications served as editors of this document.

Table of Contents

I. Abuse Desk Operations

A. Prioritizing Abuse Complaints

Abuse desks rarely have enough staff to work the thousands of complaints and escalations received on a daily basis. Abuse administrators must set priorities and then create systems to access tickets on a priority basis. The major request categories are listed below in the order in which most MAAWG Collaboration Committee members prioritize them:

Life Threatening-Emergencies

- Most MAAWG members prioritize life-threatening emergencies as their highest priority. This can include threats against customers, made by customers or against employees. It may include bomb threats against call centers, emails from runaways or Internet activity preceeding child abduction.

- Often the abuse desk serves as the contact point for security issues. It is important to have a life-threatening incident response plan in place to anticipate emergencies. This should include cell phone numbers for in-house counsel and their alternates, particularly for guidance on release of confidential information. It should also include 24X7 contact points for call centers and NOCs.

- While most life-threatening emergencies will come in via phone, ticketing systems should provide a way of flagging tickets containing key words that would indicate an emergency notification by individuals who do not know the appropriate escalation path.

Law Enforcement Requests

- Law enforcement requests can include reports of child pornography or solicitation of minors as well as crimes involving adults. It can include preservation requests, litigation customer ID requests, or law enforcement intercept requests.

- Law enforcement requests are sometimes submitted directly to an abuse desk or escalated through the legal department for investigation. Many ISPs designate a special phone number with 24X7 coverage for the exclusive use of law enforcement. In larger ISPs this is staffed 24X7. In smaller ISPs it may route to an on-call cell phone.

- The law enforcement phone number can be advertised to law enforcement as part of a law enforcement Web page including educational information such as instructions for reading a source IP from an email header and information on doing RIR (ARIN, AfriNIC, APNIC, LACNIC, RIPE) lookups. Some ISPs may also communicate this number to law enforcement through community education. Additionally, U.S. ISPs who provide phone service may communicate the escalation point to law enforcement as part of their PSAP (911) filings.

- For law enforcement requests via email, many MAAWG members find that it is helpful to create a unique mailbox such as lawenforcement@domain.com.

Legal Department Requests

- Many abuse desks receive identification requests from their legal departments. Most MAAWG members prioritize these just after law enforcement requests. Legal department requests can include customer records to fulfill a civil litigation court order or copyright infringement notices.

Malicious Activity

- Malicious activity can include phishing sites, phishing email solicitations, DDOS attacks, malware distribution, and malware hosting. Conceivably it would include virus infection also, although that was not specifically mentioned in the most popular responses. Any activity that would endanger the safety of the network or customers is the next priority for almost all MAAWG members.

Spam

- Although all the responsibilities listed above are high priority, they are also typically a relatively low volume. After they are taken care of, ISPs devote most of their time to dealing with spam.

- For this project, the MAAWG Collaboration Committee did not set a priority between inbound and outbound spam. Within a given abuse organization, either inbound or outbound mail may be regarded as more important.

Port Scans

- Port scanning is the last priority for most abuse desks. Although it may be the precursor of abusive activity, most MAAWG members feel that pursuing the activities listed above are a better use of their time.

Note on Blocking and Unblocking: If the abuse desk and postmaster are in a combined group, the abuse desk will also have to prioritize blocking issues. Most members felt that these issues were important, but would still be a lower priority than legal and law enforcement issues. The scope of the event (the number of customers impacted) would play a role in determining its priority.

B. Auto-Acknowledgement of Abuse Complaints

The MAAWG Collaboration Committee members were evenly split on whether it is worthwhile to provide auto-acknowledgements (auto-acks) to Internet users filing complaints against the member or its customers. However, even those who were against auto-acknowledgements were often in favor of some form of communication with the submitter.

In Favor:

- At least half of the members who were in favor of providing auto-acks felt it was helpful for educational purposes. They include explanations of specific return codes, give the URL to a Web site with FAQ and instructions, or clarify what kind of forensic evidence will be required in order to process the complaint.

- Other members thought auto-acks were helpful for providing a tracking number that can facilitate follow-up.

- Members also felt that it was useful to provide an auto-acknowledgement so that the sender knows the complaint was received, thereby reducing phone calls and repeat submissions.

Against:

- Approximately half of the members who voted against auto-acknowledgements still felt that it might be acceptable to send one per submitter per day. However they were against any more than that.

- Half of the members voting against also reported that instead of sending an auto-acknowledgement they will follow-up directly with their business customers.

- Some members felt that it was not desirable and/or necessary to have back and forth interactions with submitters.

- Other members were concerned about deliverability of messages.

C. How to Get Spam Complaint Submitters to Send in the Right Information?

Most ISPs need a full Internet header in order to investigate a spam complaint. However, relatively few Internet users know this and/or know how to provide it. [A standard accepted format for abuse complaints called ARF (Abuse Reporting Format) has been defined as common industry practice. See www.shaftek.org/publications/drafts/abuse-report.]

- The majority of the MAAWG Collaboration Committee members felt that trying to educate customers was not nearly as effective as providing an easier solution. They recommend integrating a "Report as Spam" button into the Web mail application.

- Members were also in favor of "pressuring" email vendors to incorporate an easy way to handle full headers into the email client.

- A small number of members were still hopeful that providing instructions and a link to a Web site with the formatting examples would be successful in enabling customers to send the correct information with their complaint.

- Several MAAWG members would be interested in an Outlook plug-in to enable a "Report as Spam" button to be incorporated into the desktop application, as long as the support burden is minimal.

- Another member felt the solution was to encourage all customers to use the same POP/email client.

- Another member felt that it was no longer necessary to try to persuade Internet users to send in headers since customers are now using their ISP's own feedback loop. However, the member would still recommend sending a bounce back to submitters who are filing abuse complaints with instructions on resubmitting the complaint with full header.

- One member suggested asking the user to forward the email.

D. How to Deal with Blocked Senders Requesting Unblocking?

This can be a time consuming matter for understaffed abuse desks, and can require judgment calls that cannot easily be made by an inexperienced staffer.

- The simplest option would be to grant unblocking when it is requested. This alleviates the necessity of judgment calls, arguments with senders or time-consuming research. The overwhelming majority of the vote was for this approach because if the sender had not fixed the issue that caused the block it would be reinstated quickly, so damage would be theoretically minimal.

- An option that would address the difficulty of making judgment calls is to keep a history of a sender's behavior, including blocks and unblocking requests. This would enable less-experienced staffers to have the security of a written record to refer to and evidence to present to the sender if a conversation is needed. There was some support for keeping a history, and only allowing a finite number of block/unblock repetitions. A variation on that idea is to keep the history and allow infinite repetitions but with increasingly slower response times. The end result being that the more often a sender is blocked, the longer it takes him to get unblocked and the more difficult the unblock process becomes.

- Another proposed solution was to use the NDRs (Non-Delivery Reports) to resolve a block in various ways. One was to include a FAQ for an automated removal process in the NDR or a link to it. The second was to allow non-customers a limited number of daily removals, with the instructions enclosed in the NDR. The third was to include the reason for the block in the NDR with a phone number for eventual resolution, AOL-style.

E. Political Email

MAAWG members considered how best to handle email from politicians for jurisdictions in which there is a distinction between political bulk mailing and spam. This mail is often sent to large mailing lists and can be trapped in spam filters.

- Over half of the Collaboration Committee members felt that the best way to handle this was to put the decision in the hands of users. They recommended that email filters offer a "no political email" option that is configurable by the end user. Then the filter would need to establish criteria for identifying political email.

- In the absence of a user-configurable option, the next most popular solution was to give the benefit of the doubt to political organizations, including elected officials, political activists and other non-profit organizations. However, if the sender establishes a practice of using spamware or sends mail to traps, then the sender should lose its whitelist status.

- One quarter of the members felt the best solution was to recommend that political campaigns use unique "from" email addresses per mailing so that if one mailing is blocked as spam, the next mailing may still get through.

- Another technique for politicians recommended by members was to send a preview email to a small subsection of the target market to determine whether it is accepted.

F. Self-Help Tools

ISPs and email providers often provide self-help tools for their customers but historically have had low adoption rates. The MAAWG Collaboration Committee members were almost evenly split between two solutions:

- The most strongly recommended solution was to provide customers with a security portal that would contain free tools such as remote virus scans and spyware detection. One member suggested that it also include an escalation path to making contact via chat and email to reduce the likelihood of customers calling in. Most members felt that a security portal was more effective than burying the tools among other customer service information.

- The next most desirable solution was to provide the customer with tools integrated into their use of the system. Including a self-help URL inside a bounce-back message would be helpful so that the user can click through to get help on this topic. A "Report as Spam" button was mentioned again in this category as one of the easiest, most effective customer tools.

G. Backscatter

A large percentage of spam is sent from a spoofed email address – the Return Address is not the true sender. When the mail is delivered to a system with an auto-responder message, the bounce-back is delivered to an innocent third-party whose email address was forged. Since many spam messages are sent to invalid email addresses, a large number of bounce-backs can be generated. At best, this is an annoyance for the bounce-back recipient and a burden for their ISP. At worst, the volume of bounce-backs being sent to the recipient can be so large that it is classified as spam and puts the recipient and bounce-back ISP at risk for blacklisting. These misdirected bounce-backs are referred to as "backscatter."

- The most popular solution for dealing with backscatter was to develop a monitoring tool that will track backscatter and remove mail from the queue that can be classified as backscatter.

- Some committee members suggested that it should not return bounces mail if SPF authentication result was "fail" or "soft fail." These members reported good results with this technique.

- The next most popular solution to backscatter is BATV (Bounce Address Tag Validation). This is a system that verifies the "from" address on email by the receiving ISP.

- A third solution was to offer end-users the option to refuse all bounce-backs. This would need to be a user-configurable option.

- Another solution recommended by members was to check a message for deliverability on the way into the email system. If it cannot be delivered, the ISP would not send a bounce-back message. However, an inline SMTP response indicating the message is not deliverable might still be useful.

H. Building Priorities in an Abuse Desk

The earlier survey question asked what the abuse desk priorities should be. This question addresses how to manage the data to address these priorities.

- Approximately two-thirds of the MAAWG Collaboration Committee members thought the best solution was to reach out to trusted reporters, such as other ISPs and law enforcement agencies, and provide them with escalation points for issues that have a large impact or need escalation for other reasons. The MAAWG Contact Database is an example of such a system. It may be more effective than maintaining one's own contact list because, on a personal list, contacts become out-of-date as employees move on to new responsibilities and companies. An online, shielded contact database allows the opportunity to send a message to the most recent "contact-of-record" as well as offering the escalation point some anonymity and protection from misuse.

- Two members recommended providing a private list, as above, but also recommend setting up mail filters to identify tickets that may need immediate attention, such as those coming from .gov domains (U.S.) or containing the words "police" or "litigation."

- The remaining third of the collaboration committee members favored setting up uniquely named mailboxes which would be available only to law enforcement.

II. Abuse Desk Management

A. How Do You Help an Abuse Tech Develop a Career Path?

This particular topic had overwhelming support for two approaches:

- Helping the employee determine what they want to do, identifying the skills needed, then providing formal training to gain them. Cross-training in related fields can also assist in an eventual career-path decision.

- Rotating employees through various abuse desk responsibilities, thus enabling them to learn different aspects of the job and avoid stagnation. This approach allows employees to discover what their strengths and weaknesses are, as well as opening their minds to new possibilities. A happy side effect of this approach is that people get to look at things from several angles and often have ideas on how to improve processes to the benefit of all.

- Members also noted that, with the knowledge that not everyone is ideally suited for abuse work, the abuse desk can be used as a starting point and encourage the development of skills and systems knowledge than can be used elsewhere in the company.

B. How Does One Motivate an Abuse Tech to Stay Positive?

The most important factors in this appear to be "communication" and "validation."

- Keeping abuse employees up to date with information and pending changes, maintaining clear honest communication, giving importance to their ideas and opinions, as well providing them honest feedback and generous praise seem to have the most support. Abuse work is generally a thankless task, and feeling as though upper management is being supportive and recognizes the importance of their contribution is a great boost.

- Involving employees in abuse-related decision-making, asking them for their ideas, opinions and possible solutions, then making it clear that those thoughts were taken into serious consideration; empowering technicians to make decisions regarding the work they are doing, and having management back them up when those decisions are assailed by irate customers received an equal share of votes.

C. How Do You Show the Consequences of Not Having a Fully Staffed Abuse Desk to Management?

There were a variety of techniques suggested to convey the importance of fully staffing the abuse desk:

- Gathering metrics and linking them directly to lost revenue was the majority winner. Showing the material consequences of not controlling a spam problem is often extremely compelling. Some example metrics: storage costs, transport costs, maintenance and man hours from dealing with the extra mail load, cost of lost customers resulting from blocked mail, unresolved calls to support with resulting loss of customer satisfaction.

- Requesting cycles from interns or under-utilized employees on other teams to help deal with the load can often gain the desired attention from management, as well as allowing for some optimization of workload.

- Showing the correlation between spam complaints and blacklists can also be helpful.

- One option that was presented semi-seriously was suggesting that the CEO and his peers work the abuse queue for a week. While such a proposal is unlikely to actually come to fruition, the idea is sound. Depending on company size and structure, having someone from management who is involved with abuse staffing decisions shadow the abuse desk for awhile could be illuminating.

- It may also be useful to remind management that the abuse desk is often the first time a non-customer will experience the company since it is one of the few areas of the company to interact with non-customers. Poor service can reflect badly on the company.

- If management suggests outsourcing the abuse desk overseas to save money, one member suggested reminding management of national security concerns resulting from sharing abuse/vulnerability information. If outsourcing is necessary, it is important for the corporate team to maintain close coordination with the outsource team.

- An alternative to maintaining or increasing the number of abuse desk staff is to implement technical solutions. If salary budgets are tight, alternatives might include blocking traffic on port 25, using DPI (deep packet inspection) or other technical solution.

D. Should the Abuse Team Be Responsible for Inbound Spam? Should the Team Be Focused Only on Abuse Coming from the Network?

Most ISPs voted in favor of separating these functions. However, they also felt it was important to keep communication flowing between the groups since inbound and outbound abuse management share a lot of the same aspects and knowledge.

E. What Is Considered to Be the Biggest Stumbling Block for an Abuse Worker?

- Indiscretion regarding customer privacy issues was the landslide winner: disclosing personally identifiable information to an individual or company that has no right to it. This opens the employee and his employer to legal and liability issues and is to be avoided at all costs.

- Failing to enforce policies due to pressure from sales people seems to be an issue.

- Overstepping the boundaries of the job by troubleshooting a customer's technical problems, caring too much or not enough about the work, caving in to customer demands just to get them off the phone, not being forthright with customers, giving information to the wrong customers, and being unwilling to say "I do not know" all got votes.

- The only option that failed to get any votes at all was "inappropriate language."

F. How Does One Manage Abuse Desk Employees that Are Technically Proficient But Lack People Skills?

- Realigning the team to take advantage of diverse skill sets. Putting the soft skills people in front and having them talk to the customers. Channeling the technical communications through those people.

- Allowing technically-oriented people to utilize technical communication tools versus personal communication: Web forms, templates, or having them check with another person who does have the social skills before sending potentially incendiary emails.

- Avoiding this issue by hiring the right people and training them extensively got the next largest vote, but this is an approach that many abuse desks do not have the luxury of using. The flip side of this idea is "do not hire them," but again that is not always an option.

- Allowing techs to sit in on calls and escalations handled by people with good soft skills helps them learn how to approach an angry customer or a politically sensitive situation with confidence. Sending such people to mandatory soft-skills training, having managers follow up with them, and rewarding improvement also got a vote.

- If all else fails and the employee is worth retaining, finding a slot for them that is not customer facing is a last resort.

III. Definitions

The authors realize that the audience for this document may include attorneys, engineers and others not directly involved in abuse desk management. It may also include readers from many different countries. Therefore, to improve communication, the definitions below explain how these terms are used in this document. This may or may not be consistent with how these terms are used in other documents, including other MAAWG publications.

ARF – Abuse Reporting Format. A commonly agreed upon format among ISPs for submitting abuse complaints to each other. This allows a technical tool to parse and aggregate the complaints. Complaints that do not conform to ARF must be reviewed by humans and take much longer to process.

ARIN – American Registry for Internet Numbers, ARIN.net. Organization responsible for assigning IP addresses within North America.

Auto-Ack – Auto-Acknowledgements. An electronically generated email to advise the sender that an email has been received and provide further instruction regarding follow-up.

CALEA – Communications Assistance for Law Enforcement Act. A law passed in the United States to facilitate wiretaps of telephone and Internet communications.

DDOS – Distributed Denial of Service Attacks. Internet attacks across multiple pathways to one target.

DMCA – Digital Millennium Copyright Act. A U.S. law that protects copyright holders from unauthorized electronic transmission. Under this act, U.S. ISPs receive notices from copyright holders who believe that the ISP's customers are infringing copyrights.

NDR – Non-Delivery Reports. This refers to an email that is generated automatically to advise the sender that their email was not accepted by the recipient's email server.

NOC – Network Operations Center, usually operated 24/7 by an Internet Service Provider.

PSAP – Public Safety Answering Point. An agency that is responsible for handling emergency safety (911) calls within the United States. U.S. telephone providers are responsible for providing PSAPs with emergency escalation paths within their organization.

RIR – Regional Internet Registry. The organizations responsible for assigning IP addresses. These include ARIN (North America), AfriNIC (Africa), APNIC (Asia Pacific), LACNIC (Latin America), and RIPE (Europe). All of these sites provide lookup tables to determine the source of an email address based on the sender's IP address, if the IP address has been assigned within their geographic service area.