From: Rod Rasmussen
Date: Wednesday, July 25, 2018 at 12:11
To: Jonathan Matkowsky
Cc: "accred-model@icann.org" "gdpr@icann.org"
Subject: [Ext] Re: [Accred-Model] Codes of conduct

Jonathan,

Thank you very much for your thoughts here! To me, this analysis of yours screams for standards so that this can scale, otherwise we will end up with a system that is far too much dependent upon manual determination of issues by all parties to be useful in the real world of abuse that moves at automated speeds (i.e. the bad guys registering or compromising domains at scale (each using thousand of domains per day via automation). My thesis is that you need a well-defined taxonomy of abuse types, domain abuse scenarios (e.g. abusively registered, compromised in-part, compromised in-full), and threat level (e.g. ongoing mass attack, ongoing targeted attack, potential attack). From that you can build a matrix of what information is required, what information about requestors can be readily revealed, and who is requested to make what kind of actions and in what timeframe. For example, for a wide-scale, current phishing attack using a compromised website, a very timely response (within minutes or hours) of a technical contact and registrant contact e-mail and phone number would facilitate solving both the phishing attack and the potential for the registrant to be exposing PII of its own users given that their website tied to a domain is compromised. The identity of the requestor would not need to be confidential in such a scenario since they *want* the registrant to know that the registrant has a serious problem to solve that could put the registrant in dire straits vis-a-vis GDPR. Separately, a detection of potentially malicious set of domain registrations that have a high probability that they will be used to launch various fraudulent and illegal scams based on prior observed behavior could result in a longer-term response (day/days) with full information about the registrant of the domain(s) and even other domains registered at near the same time, being provided with the

requestor's information not being revealed to the registrant without them going through process themselves. The main thing is to agree on what information is appropriate to reveal and how long the responses should take. From there, all parties can build automated systems to create and accept responses for contact information requests, with attestation of the harms driving the actual process that ensues.

It's all about proportionality and the ability for various harms to be balanced in a non-biased fashion. I think that if we can approach the various scenarios dispassionately and scientifically, we could provide solid guidance on how any request for registration contact information is dealt with across all registrar/registry players *and* requestors. The key is putting together a good matrix that all stakeholders can live with, and then making sure people involved in this in all roles understand how to work within the system properly and *do*so.

The current ad-hoc situation on both the requestor and provider sides is untenable and is already on the path to major negative consequences for all. Beyond the waste of manpower and unintentional abetting of crime that we're already seeing, my major fear is that these negative consequences eventually draw the attention of various national governments whose citizens are being abused, who then decide how things should work instead of the parties actually involved. That scenario historically doesn't work out well for the affected parties.

My 2 cents.

Cheers,

Rod Rasmussen
Speaking personally and not on behalf of any organization I am part of.