This document was compiled in real time from the stakeholder discussion on working group presentations at the December 2 multistakeholder meeting on Collaboration on Vulnerability Research Disclosure. No attempts to edit or organize the raw notes have been made.
http://www.ntia.doc.gov/other-publication/2015/multistakeholder-processcybersecurity-vulnerabilities

---

Adoption and Awareness Working Group Notes

Wanted outcomes

Inclusion of vuln disclosure process/program as a requirement for cyber insurance

DOC/NTIA + other parts of government to use its credibility to spread awareness/adoption, especially to increase consumer awareness, driving vendor awareness

Bridge with Economic Incentives WG to deal with challenge of breaking down adoption barriers

Raise the cost of compromise – via media; need different coverage

Identify current and optimal communication channels for awareness programs – which existing channels are good, which new channels are needed

FAQ/position paper on eternally returning questions

Multi-party can be basic topic, especially for those grabbing open source code (i.e. tiny orgs) – they'll need to deal with multi-party disclosure right away, so they'll need a plan for it immediately

Draft procurement requirements – having a common set of language built into future supply chain ecosystems as well as renewals

Market stimuli is important – need some way to inform consumers, encourage them to ask questions

Need to differentiate between mass and enterprise consumers; make procurement decisions very differently; there's limited hope in mass (i.e. home) consumers driving this

"Campaign" on education has to be multi-prong; consumers are a piece, but their role is limited; consumers can have an impact, but there need to be developers that can fix the issues first → that's how Economics feeds into Awareness

More information always good, but markets vary; markets in which there are no alternatives don't work as well via consumer pressure

FDA sees valuable role of regulatory incentives; FDA convening a public workshop in January on medical device and health care security; calling out plenary/breakout sessions dedicated to vulnerability disclosure; that will be a way to raise awareness and adoption and to add regulatory incentives

Target audiences? Mass consumers – won't have a big effect, but we can have a bigger effect on enterprise consumers. We should go after larger groups, researchers, and new vendors.

Value of FBI adoption

Merging working group efforts?

Safety –

Multi-party – narrow scope; adoption is disclosure broadly; multi-party is a subset of that – so it should remain separate but feed up into Awareness and Adoption WG

We don't need to dump everything at once; we need a campaign – media coverage, etc to create new norms (that results in raised adoption) → so as Multi-party is better developed, merge with Awareness and Adoption

Safety Working Group Notes

# Things we can deliver quickly (small wins)

- One pagers – material that can fit on a single page that is highly accessible/digestible
    - How is the "safety industry" different? (dynamics, time horizons, etc.)
    - We need a welcome wagon! (one-pager: this is the value of having coordinated disclosure! Very short and sweet.)
    - Glossary is key so that we have a common understanding across stakeholders
        - E.g., medical device industry uses words we use in very different ways.
    - Boilerplate … the minimal "welcome mat" case for bringing an initial disclosure policy and process to a safety organization.
- Comments
    - Is safety different?
        - The risks are certainly different, and parts played by people involved to manage that risk can be different.
        - We consider safety and security differently… (e.g., a scalpel is safe in the Medical industry if it can be used by a physician in the way intended by design, but not unsafe because it can be used to stab people.)
        - Josh thinks that many of the issues are similar but than in some cases very different.

- Safety case may be a superset of the vanilla disclosure case (e.g., many terms in the “equation” for the more complicated case are zero so it looks simple in the vanilla case).
- Different in multiple aspects, e.g., if a researcher discloses a vuln in a vanilla case the worst case is they get sued for non-criminal stuff; in the safety case someone could be charged for murder.
- Safety may just be a case of special circumstances… e.g., you need to do some more crazy stuff in safety. (Josh points out that this basically reduces to the superset).
- Nuclear plants are very very special. E.g., not disclosure to the public, potentially for a very long time. It also means you might want to treat the content of a disclosure differently (e.g., no proofs of concept for vulns delivered in safety?). Researchers in the field also seem to treat it differently (e.g., more patience waiting for a fix or disclose).
- Not clear to some why you’d want to treat safety industry differently…

Multi-vendor Working Group Notes

# going forward

- Need to illustrate the simple case first
-
- Will need to get to more complicated cases subsequently
- Question: how many people feel like we could fold this in under other efforts? E.g., through FIRST or through Adoption and Awareness?
    - Yes, for FIRST and yes for A&A
    - Both groups are struggling for engagement so it’s not necessarily a good idea to dilute further
- Question: did the problem statement make sense?
    - Counter-q: would you be doing use cases that are multi-vendor?
        - A: it can be very hard to encompass the variety of the ecosystem in use cases.
        - A: would like to not have to repeat things or waste time working on things others are doing.
        - Need to map out how people participate in FIRST’s vuln coord SIG, everyone is welcome!
            - Don’t have to be a member of FIRST to participate.
- Document challenges that multi-party adds to vanilla vuln disc.
    - Even just explaining that is doable and valuable.
- Having a set of documented cases is very valuable for understand how we can learn from past MP disc cases
    - When embargo failed, secrecy relationships, etc.

- Miscellaneous:
  - Software industry could learn a lot from auto industry non-software multi-vendor coordination.
    - But they're not so good at software cyber supply chain (Katie said it!)
  - May want to think of ad hoc/improvisational guidelines that could be useful outside of documented cases

Econ Incentives Working Group Notes

Problem Statement evolution:

* There are perverse incentives to various parties involved in Vulnerability Disclosure

*Parties: Vendor, Researcher, Consumer, Enterprise

*Look for opportunities to partner between researchers and vendors

Economics of dealing with security vulnerabilities – reasons for secure coding, when/how/why to fix, Why not to sue

Open markets don't incentivize everyone equally, works for the researcher, not necessarily for the vendor or enterprise

Awareness to take on the awareness campaign for how vulnerability management is handled presently

The software/service owner should be involved in the disclosure

Publish data from mature organizations on the value of incorporating what they've learned from writing secure code and following best practices

Quality cycles and creating predictability in patches creates delays that are not advantageous to researchers

Liability comes with breaches and data exfiltration, from regulators (FTC) and Tort suits/actions