Building a PSIRT for a Standards Organization

Jim Duncan

2025-04-10

TLP:CLEAR

Intro - What, Who, How

- This talk is about the Trusted Computing Group's circumstance
  - But intended as a guide for any standards group to stand up a PSIRT
- Your presenter is a CSIRT/PSIRT pioneer
  - Worked on the response to the Morris Worm
  - Developed and delivered the first CSIRT classes for USENIX
  - First full-time PSIRT member at Cisco Systems
  - Involved with FIRST since 1990
- At Juniper Networks, served as TCG alternate board member

Standards Organizations

- The Trusted Computing Group (TCG)
  - Develops and champions a range of secure designs and protocols
  - Perhaps most known for the Trusted Platform Module (TPM)
  - But also Trusted Network Connect and secure storage solutions, and more
  - Highly likely that every phone and laptop in this room as a TCG TPM in it!
- However, what matters here is about TCG as a standards group
  - Modern, productive standards organization with worldwide membership, dozens of active working groups with industry-wide participation and impact
  - Face-to-face members' meetings, globally, at least three times per year
  - *Note well: These are competitors working together on a common goal.*

The Problem

- Everybody has vulnerabilities. No surprise, right?
  - Surpassed by the number of people talking about others' vulnerabilities!
  - I personally witnessed "hallway conversations" about alleged flaws
    - These were not managed uniform disclosures to all affected parties
    - I also realized that any major issue would be wrangled by the member companies independently, with lopsided outcomes
- With support from my employer and like-minded board members, we sought a solution.
  - (Thank you, Seth Ross at Juniper Networks!)

The Proposed Solution

- TCG Board created Vulnerability Response Subcommittee (VRS)
  - Studied the issue for 10 months, and received and resolved 150+ comments
  - Produced a Vulnerability Response Framework (VRF) as guidance
- VRF recommended a Vulnerability Response Team (VRT)
  - Reports to the VRS; provides a buffer between VRT and larger organization
  - VRT members are nominated by TCG Board (or "Contributor" members) and vetted by VRS until optimum staffing is achieved
  - Thereafter, VRT service outlasts any change in Board membership
    - But does end if TCG membership ends

Major Topics

- "Resolving a report" v. "resolving a vulnerability"
  - Major focus is ensuring that reports of alleged flaws are relayed to the affected parties for final resolution
- Oversight committee v. response team
  - The VRS is managerial, not hands-on; the VRT does the heavy lifting.
- Misalignment of confidentiality expectations
  - Standards group members tend to handle secrecy different than do PSIRTs.
    - For example, "Need-to-Know" is rarely invoked, if ever.
- Intellectual Property (IP) handling and legal consultation
  - IP is existential for a standards group!

Major Unforeseen Obstacle

- Small number of members (including board) were alarmed
  - PSIRT activities still a new concept
  - Concerns were expressed about losing control of IP during an incident
- Objection was not unexpected but we were surprised at seriousness
- Standards org PSIRTs mimic typical standards group activities
  - And in some other ways, PSIRT activities inside a standards org are a microcosm of a Multi-Party Coordinated Disclosure event.
  - Major difference is the shortened publication timeline, but otherwise the same
- We successfully allayed the members' concerns.

Roles and Responsibilities

- Team members are incident managers (IMs) primarily
  - Not subject-matter experts (SMEs)
  - Not developers/standards authors/working group members
  - IMs are assigned to new reports round-robin
- SMEs are essential but may not know how flaws are handled
  - When needed, an SME is nominated by the affected workgroup chair
  - IM reaches out to the candidate SME to explain operating constraints
  - If it doesn't work out, outreach is ended; a different SME is nominated
  - IM reaches out to the new candidate, and so on, until agreement is reached

Team Staffing and Oversight

- Ideal number of VRT members is 4 to 6 (currently 5)
  - Nominated by board member (or "Contributor Advisor"); approved by VRS
  - As noted earlier, appointment to the VRT outlasts board membership
    - One of many measures to insulate VRT members from outside influence
  - Also recall VRT members are expected primarily to be incident responders
    - To date, all have been PSIRT members for their individual employers
- VRT members elect co-chairs from amongst themselves
  - Co-chairs manage the VRT itself; VRT members manage specific incidents
  - VRT member names are drawn round-robin as each new report is received

Issue Types

- Vendor product flaw (i.e., a TCG member's flaw)
  - Notify the affected member
  - Determine if other members may be affected and communicate as needed
- Specification or Reference Document
  - Notify the affected working group(s)
  - Proceed as though a typical PSIRT case
- TCG Reference Code
  - Nobody is supposed to run reference code, but it happens!
  - Proceed as if a typical PSIRT case

Non-TCG Issues

- Specification or Implementation questions
  - Not a VRT issue; decline or hand off to the appropriate working group chair
- Non-TCG vulnerability
  - Not a VRT issue; decline; if possible forward to the proper team for resolution

Multi-Party Coordination

- A reported issue may actually be larger than TCG
  - Identify a national CSIRT to coordinate; notify and collaborate
  - Most likely this will be VINCE but the policy allows for others if needed
- Conversely, the TCG VRT may be contacted by a coordinator
  - Handled as described earlier; IM is selected round-robin, VRT is engaged
- Be aware that a really big incident may become confusing if a coordinator is working with the TCG VRT while also working directly with one or more TCG members
  - Flexibility, grace and common sense will be invaluable.

Administrative Support

- Like any workgroup/committee, VRT gets support from the TCG administrative support team, "TCG-Admin"
- One member of TCG-Admin is *ex officio* a member of the VRT
  - Monitors notification channels and activates the team as needed
  - Organizes and attends VRT meetings
  - Uses tooling (PGP/GPG, Signal, etc) as appropriate
  - All this in addition to the usual workgroup responsibilities

Tooling

- TCG VRT has a "/security" page detailing how to engage
  - Multiple methods are supported for reporting issues
  - TCG-Admin monitors all such channels and activates VRT when needed
- Team members are proficient with PGP/GPG
- Issues are scored with CVSS
- Info-sharing and sensitivity are managed with TLP labels
- Alternative communications channel is provided via Signal
- And there's no need to become a CNA
  - Multiple VRT members work for existing CNAs; just ask one if a CVE is needed

Communications Approvals and Legal Consultation

- Normally, all external communications and published statements must be approved by the full board of directors
  - Typical for a standards organization; IP protection is critically important
- TCG may need to publish in hours, perhaps minutes
  - For VRT requests, approval can be granted by board officers, not full board
- VRT may need to consult with TCG Legal on short notice
  - Normally, any interaction with legal counsel must be approved and funds allocated by the board of directors with a "not-to-exceed" expense cap.
  - VRT has a standing pre-approved allocation of a few hours of Legal's time

What Did We Miss?

- Review the existing Crisis Management Plan for alignment.
  - Technically, this is still an open task.
- Review membership requirements for possible problems
  - Organizations may have different classes of membership
  - Obligations between members and the larger org may contain surprises
  - I haven't uncovered any concerning issues
  - But I believe it's a valid area for investigation across standards orgs generally
  - Technically, this too is still an open task(!)
- Research the history of the organization for earlier flaws
  - You may uncover an issue that's still open and that needs to be resolved.
  - Pre-VRT incidents may provide valuable insight for future incidents.

Results

- TCG VRT officially stood up in 2019Q3
  - Initially expected 2-3 incidents per year
  - And the resulting average (as of 2025) is about 1-3 issues annually
- Every comment has been complimentary
  - I have not heard any negative comments, just praise for the team.

Key Takeaways (in no particular order)

- Standards groups need a vulnerability process and policy.
- This is about resolving a report versus resolving a vulnerability.
- Engage with SMEs one-on-one, with great constraint.
- Internal multi-party coordination will be needed.
- Intellectual Property is existential.
- Negotiate express processes for publishing and decision-making.
- Review membership requirements for possible problems.
- Separate oversight (VRS) from operations (VRT).
- Protect the membership of the response team.

Comments?
Questions?