CWE/CAPEC Board Meeting #1

Tuesday August 4, 2020 @ 1200-1400 EDT
Thursday August 6, 2020 @ 1000-1200 EDT

(two meetings were held to maximize attendance; minutes reflect a combination of meetings)

Members in Attendance

Paul Anderson -- GrammaTech
Drew Buttner -- MITRE (CWE/CAPEC, Board Moderator)
Bill Curtis -- CISQ
Chris Eng -- Veracode
Jason Fung -- Intel
Jay Gazlay -- DHS CISA
Alex Hoole -- Micro Focus
Joe Jarzombek -- Synopsys
Jason Lam -- SANS
Chris Levendis -- MITRE (CVE)
Jason Oberg -- Tortuga Logic
Kurt Seifried -- Cloud Security Alliance
Chris Turner -- NIST (NVD)
Andrew van der Stock -- OWASP

Review of Previous Action Items

Item Number	Action Item	Responsible Party	Status	Comments

Agenda with Discussion Summary

A) CWE/CAPEC Board Mission and Objectives

- MISSION : The mission of the CWE/CAPEC Board is to set and promote the goals and objectives of the CWE/CAPEC Program to ensure the ongoing adoption, coverage, and quality of CWE/CAPEC.
- VALUE : Members of the CWE/CAPEC Board work with each other and the community to advise and advocate for the CWE/CAPEC Program. Through open and collaborative discussions, board members provide critical input regarding domain coverage, coverage goals, operating structure, and strategic direction.
- OPERATION : The CWE/CAPEC Board operates in a manner that enables it to best deliver on its mission. A specific manner of operation is intentionally absent to enable the board to shape itself in the most efficient and effective way.

A member asked if the CWE/CAPEC Board has, or should work to create, bylaws. Currently there are no formal bylaws. Board members were in agreement that bylaws are something that could be put together, and if done should be put together by the board itself. It was agreed that this should be an agenda topic for the next board meeting.

ACTION : Chris Levendis will circulate the CVE Board Charter. (once current is approved)

FUTURE AGENDA : Discuss the need for bylaws.

Discussion was had about how CWE/CAPEC can help the community by creating a precise standard/understanding of what is a weakness, what is a vuln, and what is an attack. A member also mentioned that if you don't have the right metadata recorded you can't do much with things like machine learning. It was suggested to add a field for their strength of belief in their mapping, also add a box for if a CWE exists. It was agreed that discussion around both of these topics should continue on the mailing list.

ACTION : Further discussion around the definition of terms, and on potential information fields to collect/maintain should be had via the board mailing list.

B) Member Introductions

First Meeting:

Drew Buttner
Bill Curtis
Joe Jarzombek
Chris Levendis
Jason Fung
Paul Anderson
Kurt Seifried
Andrew van der Stock
Jason Oberg
Jason Lam
Jay Gazlay

Second Meeting:

Drew Buttner
Alex Hoole
Chris Turner
Chris Eng
Joe Jarzombek
Chris Levendis

C) Communications

- Currently Established
    i. communications through email list, members only
    ii. public archive through Nabble
- Questions
    i. Should a non-publicly archived list be established?
    ii. How frequently should online/phone board meetings be held?
    iii. How far in advance should the board meetings be scheduled?
    iv. Should the board meetings be recorded?
    v. Where should board-related artifacts (e.g., meeting minutes) be stored?

A member asked if the CVE Board has a need for a non-public list. (answer – CVE does) It was mentioned that certain discussions are in fact appropriate for a private list, an example of discussions around the removal of a board member was brought forward. Another example presented was around voting on contentious issues. It was stated that CVE uses its private list very sparingly but that it is important to have.

ACTION : The moderator will set up a private, non-publicly archived email list.

A member asked that since CWE/CAPEC is funded by the US Government, can someone request the contents of a private list. It was mentioned that the list is run by MITRE, and since MITRE is not part of the Government, they are not bound by the Freedom of Information Act.

ACTION : The moderator will discuss with MITRE's general counsel and get an official answer.

A member mentioned that the board meetings should be event driven, maybe meeting before a new version, or when a key decision/direction is needed. Beyond that, quarterly meetings seem appropriate. A different board member suggested monthly, or even every other month, meetings. However, the monthly idea was met with some push back and considered too much. The members agreed to hold the next board meeting a few weeks out, and then revisit the frequency discussion as part of the agenda.

FUTURE AGENDA : Discuss the frequency of future board meetings.

The members were in full agreement that any set meetings like quarterly meetings should be put on the calendar well in advance, and that an online poll (e.g., Doodle) should be leveraged for event driven meetings.

The members were in full agreement that future board meetings should be recorded, but that the recording should be kept private to the board. It was noted that there is very little that can be done to enforce individual board members from sharing. Need to rely on policy and charter. Members agreed that a sharing private conversations, recordings, or documents should be grounds for removal from the board.

ACTION : The moderator will setup recordings for future meetings.

The members were in full agreement about the need for a member-only document repository. (e.g., GitHub) A member stated the desire to avoid having multiple places to look for things.

ACTION : The moderator will research and make a proposal back to the board regarding both a private and a public document repository.

D) Participation

- Questions
    i. What participation expectations / requirements should be in place?

ii. Should there be a rule about inactivity?

Members agreed that there should be some expected level of participation. However, it was also mentioned that participation via email could offset a lack of participation in meetings. The board needs to be flexible in its expectations. It was noted that CVE is also actively debating this question. Potential language was presented … "a reasonable expectation that board members participate, lack of participation is handled on a case by case basis". It was mentioned that a set of bylaws would be helpful in this case.

It was mentioned that watching the recording should be considered as participation.

Discussion was also had around the use of chat technology (e.g., Slack) One challenge that was mentioned with such technology was maintaining public archiving for transparency.

FUTURE AGENDA : Discuss participation expectations.

E) Topic Introduction

- Questions
  - i. discussion about a formal board agenda process
  - ii. how does the board bring topics to the table?
  - iii. how should actions be tracked?

The members were in full support of an online collaboration tool (e.g., Trello) to help gain consent around agenda topics. It was mentioned that topics not accepted should be listed as such so that they are recorded.

It was mentioned that if a member proposes an agenda item, then they should also provide a description.

Discussion was also had about the board using the agenda to set a longer-term roadmap for CWE/CAPEC, and enabling planning around the topics.

ACTION : The moderator will research options and establish an online collaboration capability.

F) Board Membership

- Current Situation
  - i. 15 members (14 + moderator)
  - ii. only one per organization
- Questions
  - i. discussion around size, addition of new members, process
  - ii. backups / stand-ins

Discussion started around the size becoming too big and making the board unwieldy and ineffective. The members agreed that growth would need to be carefully monitored. Focus on new members should be about what they bring to the board that isn't already represented.

The discussion switched to the notion of backups / alternates. In other words, if a board member is unable to attend a call, can they name an alternate at their organization to attend in their place. Alternates would also be helpful if certain topics were on the agenda. Should be some limit to the number of alternates, and only one vote if voting. There was full agreement around the notion of alternates as framed by this discussion.

It was agreed that this is an area that bylaws would be very helpful with.

FUTURE AGENDA : Further discussion on this topic should be continued in future meetings.

G) Press

- Questions
    i. How should the board handle press requests?
    ii. How should the board handle press releases?

It was mentioned that the CVE board gets frequent media inquiries, and the desire is for a program response instead of a MITRE response. The members agreed that there should be a shared response to inquiries. Members agreed that any inquiry should be passed around to board members along with a timeframe, and those that can and want to respond should be allowed.

The members agreed that any press release from the board should be more coordinated. An example was presented where the board has a chair that handles and coordinates the release.

Members also discussed the notion that not all board members will agree on every point, but that board members should support the decisions of the board.

ACTION : Further discussion on the topics of press inquiries and press releases should be had via the board mailing list.

H) Update on 2020 CWE Top 25

- Update
    i. To be released on Thursday August 20
- Questions
    i. What potential press opportunities for the release might exist?
    ii. How can board members help promote the release?

It was stated that the board should focus on helping the community understand the difference between vulnerabilities and weaknesses

Discussion was also had regarding the board being a source of guidance. Using the Top 25 as an example, the board should consider establishing guidance around the following:

- *What is the Top 25, and about what are the right ways to leverage it?*
- *Opportunity to educate the public about the deficiencies of the process, and the risks that will never part of the top25.*
- *Request continuous feedback for how to make the Top 25 better.*

It was mentioned that the CWE Top 25 is technology agnostic. This makes it hard to determine what is really the most important for a user.

It was also mentioned that the board should help the community understand how CWE/CAPEC aligns to external standards.

I) New Business

- Open floor for discussion.

Members brought up the ideas of a hardware-related Top 25, a data-protection view, and working with NIST to tag CVEs with software vs hardware. It was agreed that in the interest of time that all of these ideas should be discussed via the board mailing list.

ACTION : Further discussion on the topics of a hardware-related Top 25, a data-protection view, and tagging CVEs with software vs hardware should be had via the board mailing list.

J) Next Meeting

- When should next meeting be scheduled?
- What topics should be on the agenda?

Next meeting to be scheduled in the late August / early September timeframe.

Action Items Going Forward

Item Number	Action Item	Responsible Party	Status	Comments
2020.08.06.01	Circulate the CVE Board Charter to the CWE/CAPEC board members.	Chris Levendis	Not Started	Assigned on 2020/08/06.
2020.08.06.02	Further discussion around the definition of terms, and on potential information fields to collect/maintain should be had via the board mailing list.	ALL	Not Started	Assigned on 2020/08/06.
2020.08.06.03	Establish a private, non-publicly archived email list for CWE/CAPEC board members.	Drew Buttner	Not Started	Assigned on 2020/08/06.
2020.08.06.04	Request clarification from MITRE’s general counsel regarding the ability for a non-board member to request the contents of a private list through the Freedom of Information Act or the Patriot Act.	Drew Buttner	Not Started	Assigned on 2020/08/06.
2020.08.06.05	Establish a capability to record the board meetings.	Drew Buttner	Not Started	Assigned on 2020/08/06.
2020.08.06.06	Research and make a proposal for both a private and a public document repository.	Drew Buttner	Not Started	Assigned on 2020/08/06.
2020.08.06.07	Research options and establish an online meeting agenda collaboration capability.	Drew Buttner	Not Started	Assigned on 2020/08/06.

2020.08.06.08	Further discussion on the topics of press inquiries and press releases should be had via the board mailing list.	ALL	Not Started	Assigned on 2020/08/06.
2020.08.06.09	Further discussion on the topics of a hardware-related Top 25, a data-protection view, and tagging CVEs with software vs hardware should be had via the board mailing list.	ALL	Not Started	Assigned on 2020/08/06.