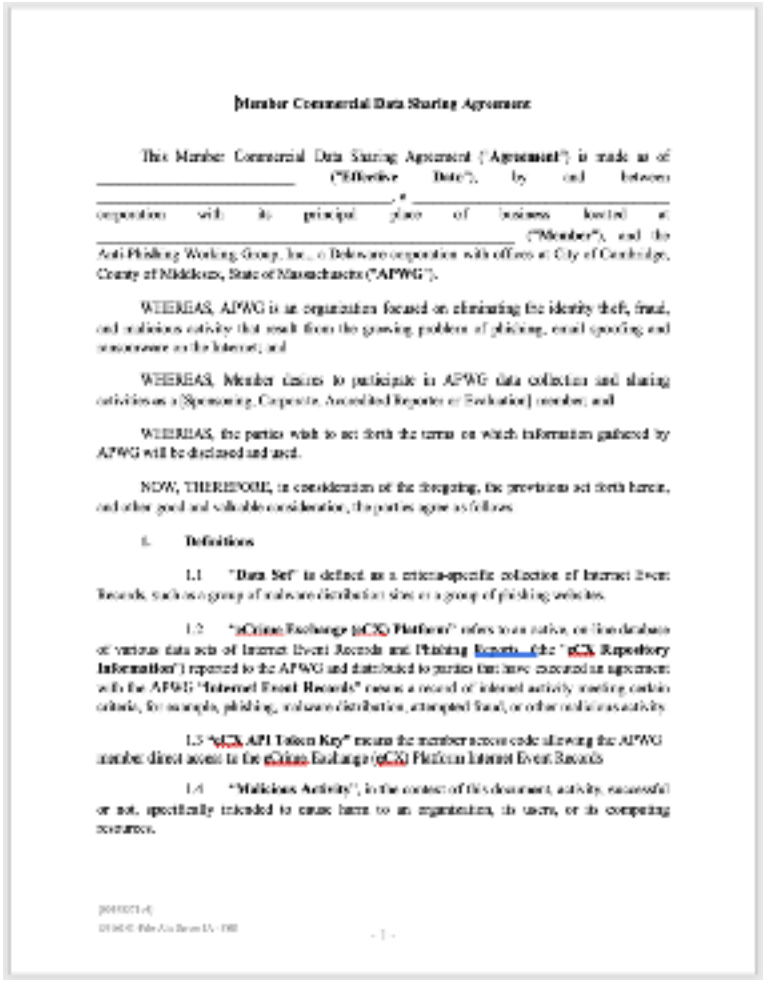
Establishment and Maintenance of the APWG eCrime eXchange Trust Architecture:

As Essential As Operational Infrastructure Curation for the Programmatic Exchange of Cybercrime Event Data

APWG Data Mobilization Strategy: Cultivate Data Sharer Trust

- Data sharing – part-icularly to inform systems to impede events – is all about trust
- Everybody following explicit and precise usage rules builds trust
- Articulation of common expectations and action executing them in deed builds trust
- Empowerment as a data contributor — as well as consumer — builds trust

APWG Data Sharing Agreement: Key to Cultivation of Data Sharer Trust



Member Commercial Data Sharing Agreement

This Member Commercial Data Sharing Agreement ("Agreement") is made as of _____ ("Effective Date"), by and between _____, a _____ organization with its principal place of business located at _____ ("Member"), and the Anti-Phishing Working Group, Inc., a Delaware organization with offices at City of Cambridge, County of Middlesex, State of Massachusetts ("APWG").

WHEREAS, APWG is an organization focused on eliminating the identity theft, fraud, and malicious activity that result from the growing problem of phishing, email spoofing and crimeware on the Internet; and

WHEREAS, Member desires to participate in APWG data collection and sharing activities as a [Sponsoring, Corporate, Accredited Reporter or Evaluation] member; and

WHEREAS, the parties wish to set forth the terms on which information gathered by APWG will be disclosed and used.

NOW, THEREFORE, in consideration of the foregoing, the provisions set forth herein, and other good and valuable consideration, the parties agree as follows:

1. **Definitions**

1.1 "**Data Set**" is defined as a criteria-specific collection of Internet Event Records, such as a group of malware distribution sites or a group of phishing websites.

1.2 "**eCrime Exchange (eCX) Platform**" refers to an online database of various data sets of Internet Event Records and Phishing Reports (the "**eCX Repository Information**") reported to the APWG and distributed to parties that have executed an agreement with the APWG. "**Internet Event Records**" means a record of internet activity involving certain criteria, for example, phishing, malware distribution, attempted fraud, or other malicious activity.

1.3 "**eCX API Token Key**" means the member access code allowing the APWG member direct access to the eCrime Exchange (eCX) Platform Internet Event Records.

1.4 "**Malicious Activity**", in the context of this document, activity, successful or not, specifically intended to cause harm to an organization, its users, or its computing resources.

- APWG treats members operating under our Data Sharing Agreement (DSA) like equals in a mutualistic enterprise
- Members under DSA have full read/write access to the the eCX's API endpoints
  - New reports/corrections to existing reports
- DSA spells out explicitly: a) data usage and license terms; b) submission rules; and c) liability / indemnification scheme
- Corporate counsel has all the essentials to determine if risks attendant data exchange have been addressed on behalf of their enterprises — and meet their respective risk management requirements

Auditability Key to Trust – Like Any Business Process

- APWG eCX does not release the identity of the data submitter but data submissions to eCX are NOT lodged anonymously
- By eCX design, submitters can be associated with submitted data, if and when the APWG's authorized personnel need to resolve data fidelity issues or address other operational exigencies

DSA Terms of Usage Bounds Trust Domain and Enables Accountability

- Data submitters need assurance that clearing-house members can't do silly things with their data
  - Data may be kind-of sensitive (i.e. "we found it before other people did") and I may not want my sensitive data going public / rogue
- When a member institution submits data, its personnel want to know what other members can do with it
- The DSA frames and answers those questions so corporate counsel can make a rational decision on participation
- Data flows only after counsel authorizes initiation of correspondence

Data Sharing Agreement + Auditability Balances Data Sharers' Interests

- APWG works with operations personnel most often – but our DSA recognizes that counsel directs and bounds participation
- Operations gets data – but corporate counsel also must have the instrumentation that they require to manage risks
- APWG retains curatorial authority to act on behalf of users in maintaining data fidelity and timeliness
- With the DSA and a neutral curator, data sharers are assured:
  - A) You know the rules,
  - B) the other data sharers know the rules, too; and
  - C) the curator can see if you follow them or not and act on behalf of the community of data sharers to discipline data correspondents participating in the clearinghouse

Why an NGO-Managed Clearinghouse?

- To balance risk management, access to data, and relevance of data corpora, an independent, user-supported NGO model just works – as it always has for as long as humanity has been managing predictable risks
- Ancient truth: When everyone (LEOs, businesses, churches and taverns) is fighting the same threats – fires; pirates; and measles – civilizations (i.e. ones that endure) organize non-profit clearinghouses to inform a common-defense infrastructure
- Among the most familiar threats, zip-code specific fire histories (insurance reporting bureaux); piracy maps (insurance/maritime trade organizations); case data (public health management) have been established for decades and, in some cases, for centuries to manage predictable risks and common menace
- In the global confrontation against cybercrime, the clearance house for our cybercrime epoch is: the APWG eCrime eXchange (eCX) – since 2004

Contact: APWG

- The Directors
- info@apwg.org
- +1 617 669 1123