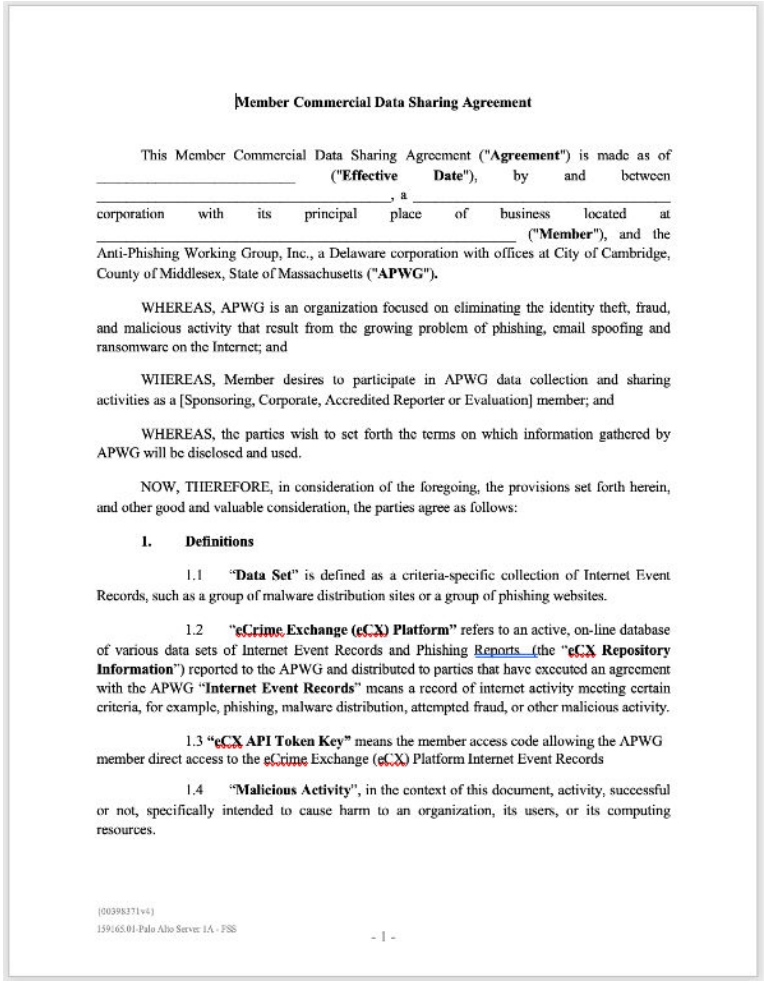
Establishment and Maintenance of Data Exchange Trust Infrastructure:

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

APWG Data Mobilization Strategy: Cultivate Data Sharer Trust

- Data sharing – particularly impeding 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 _____ corporation with its principal place of business located at _____ ("**Member**"), and the Anti-Phishing Working Group, Inc., a Delaware corporation 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 ransomware 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 active, on-line 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 meeting 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.

{00398371v4}
159165.01-Palo Alto Server 1A - FSS

- 1 -

- APWG treats member / data-sharers operating under our DSA like equals in a mutualist enterprise
- APWG members under DSA have full read/write access to the the eCX's API endpoints and eCX Work Groups
  - New reports and corrections to existing reports
- DSA spells out explicitly: data usage and license terms; submission rules; and liability/ indemnification schemes
- Corporate counsel has what he or she needs to determine if risk attendant data exchange has been reasonably addressed on behalf of their enterprises
  - Without that, for incorporated entities of any size, programmatic data exchange cannot be programmatically animated

Auditability Key to Trust – Like Any Business Process

- APWG eCX does not release the identity of the data submitter but data submission is NOT anonymous
- By design, submitters can be are routinely traced to submitted data, if and when the APWG's authorized personnel need to resolve data fidelity issues or other operational exigencies

Terms of Usage Bounds Trust Domain and Enables Accountability

- Data submitters need assurance clearinghouse 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 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 decides affirmatively

Data Sharing Agreement + Auditability Balances 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 management 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, and 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
- An old story, one of timeless utility in risk management

Why an NGO-Managed Clearinghouse?

- For equitable balance of 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 (LEAs, businesses, churches and taverns) is fighting the same threats – fires; pirates; and measles – civilizations (ones that endure;)) organize non-profit clearinghouses to inform common defense infrastructure
- For the above, zip-code specific fire histories (insurance trade groups); piracy maps (insurance/maritime trade organizations); case data (public health/inoculation management) have been established for decades and, in some cases, for centuries to manage predictable risks
- In today's global confrontation against cybercrime: APWG eCrime eXchange (eCX) – since 2004

Contact: APWG

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