Involucrando al sector privado, la sociedad civil y la comunidad técnica para responder a las amenazas cibernéticas

Peter Cassidy

Secretary General, Co-founder

Founding Director, Principle Architect
## Getting It Done

- Involving the private sector, civil society and technical community to respond to cyberthreats?
- Building crowds requires defining a common, deeply characterized problem
- Definition of parts of the solution that can be cooperatively established and maintained
- Crowd assembles itself over time
Objective: Unified Responses to Cyberthreats Become Routine

- We win by defining what part of a predictable threat belongs to everyone and should be managed by all stakeholders in cooperative schemes.
- Once there, developing and maintaining resources becomes a matter of working toward operational consensus.
- Requires a lot of listening across borders, industry verticals and cultures.
Two Opportunities for Unified Engagement of Cyberthreats

- **Data Exchange**
  - (APWG FTP-based URL Block List established 2004)

- **Cybersecurity Awareness Messaging**
  - (STOP. THINK. CONNECT. launched October 2010)
Unified Cybercrime Event Data Exchange
Cybercrime Event Data Clearinghouse

APWG maintains eCX as a member-operated, nonprofit data switch to route cybercrime event data between stakeholders, today delivering nearly 200 million cybercrime event records per month.

APWG members specified an anyone-to-anyone distribution model in 2003 that has held its relevance to this day.

Data resources available to any industry, government or academic enterprise that needs consistently categorized and classified cybercrime event data.
Event Data Simplest & Most Used in Security and Forensic Applications

THE UBL feeds web addresses of phishing websites to APWG members on a near realtime basis, a data module useful for many security routines and forensic applications related to financial cybercrimes.

MAL IP feeds IP addresses to APWG members that are reported to be associated with activity often associated with financial crimes or the activities typically prefatory to cybercrimes.

APWG
Unifying the Global Response to Cybercrime
Data Flows I/O in August 2016

- 12,355 authenticated user POSTs instantiated 12,355 new report records
- 1,395,230 requests for data from eCX users during the month
- 179,638,196 Records returned for all data requests
- All exchange managed through API
- User relationships managed through one user agreement
Unified Cybersecurity Awareness Messaging
STOP. THINK. CONNECT. Campaign

- The global STOP. THINK. CONNECT.™ public-awareness campaign is the first-ever and only globally coordinated cybersecurity messaging suite to help all digital citizens stay more secure online.
- The campaign maintains a service-mark slogan, logo and brief advisory suite.
- The assets are managed by the non-profit STOP. THINK. CONNECT. Messaging Convention, Inc. a Georgia corporation co-managed by two non-profits, APWG and NCSA.
The Opportunity for Globally Unified Cybersecurity Awareness Messaging

- Online safety messaging: discordant, fragmented
  - Too many uncoordinated campaigns creating apparent discord
- APWG proposes a ‘Messing Convention’ to its members in early Spring, 2009
  - Unified messaging scheme would provide slogan, logo and advisory suite to be used in common by all sectors
- White House in May 2009 calling for a cybersecurity campaign focused attention
- Initial muster at Fox Interactive in June 2009 assembled 20+ companies, think tanks and federal government agencies
Campaign Asset Development Based on Extensive Research

- APWG and NCSA directed development in **two phases** over 14 months:
  - Interrogation of security experts to determine exposures to be covered
  - Development of language and symbols to transmit essential safety principles to engage those exposures

- Messaging Convention managed development under **two directives**:
  - Messaging should be positive and actionable
  - Fear-based messaging will not be considered
Campaign Essential Kit

- **Slogan and logo**
  - Can provides mnemonic for all cyber education/awareness assets

- **Advisory suites**
  - One basic advisory suite covers the essentials
  - Additional sets cover key aspects of mobile tech, social networking, gaming, etc.

- **Videos, radio ads, PSAs on the way**

- **New content from curators**
State of the Campaign Today

- Completed campaign assets already deployed for nearly 6 years
  - 13-nation global deployment footprint expanding apace
  - 24 national curators under memorandums of cooperation
  - 500+ (commercial, gov’t & NGO) licensees worldwide

- APWG working with multilateral treaty organizations such as the Commonwealth of Nations, Organization of American States, Europol EC3 and the IGF to propagate and maintain the campaign

- Still, today, some 29 national curators are in due diligence mode preparing for accession
Thirteen Nations Deployed and Growing

- France
- Japan
- Antigua and Barbuda
- Tonga
- Nigeria
- Mongolia
- USA
- Bangladesh
- Armenia
- Belize
- Switzerland
- Jamaica
- Spain

Latest campaign deployments:
- Antigua and Barbuda
- Tonga

In fast-track deployment mode this week:
- Latvia
- Czech Republic
- Sudan
Memorandums of Cooperation With National Ministries, CERTs and NGOs

- Armenia – Armenia Education Center and Internet Society of Armenia
- Antigua and Barbuda – Ministry of Information, Broadcasting, Telecommunications & Information Technology
- Bangladesh – Bangladesh Computer Council
- Belize – Ministry of National Defense (* in last approval phase)
- Canada – Public Safety Canada (2012/Harper Administration)
- Czech Republic – NCBI / Safertnernet.cz
- Dominica – Ministry of Information Science Telecommunications and Technology
- Ecuador – Centro de respuesta a incidentes informáticas del Ecuador
- France – CECyF (Ministère de l’intérieur / Ministère des finances)
- Italy – Poste Italiene
- Japan – Council of Anti-Phishing Japan (JP CERT)
- Jamaica – Ministry of Science, Technology, Energy and Mining
- Latvia – IMCS UL / CERT.LV
- Spain – Instituto Nacional de Ciberseguridad de España, S.A.
- Mongolia – Mongolia CERT
- Nigeria – CSEAN
- Panama – Autoridad Nacional para la Innovación Gubernamental
- Paraguay – Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICS)
- Poland – NASK
- Slovakia – Preventista.sk
- Slovenia – Slovenian Computer Emergency Response Team (SI-CERT)
- Switzerland – Swiss Internet Security Alliance (SWITCH/SwissPost)
- Kingdom of Tonga – Ministry of Information & Communications
- USA – NCSA (Department of Homeland Security)
- Uruguay – Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC)

Latest agreements signed:

- Slovenia
- Czech Republic
- Latvia
- Tonga
Hybrid Vigor: Campaign Invites Flexibility in Deployment Scenarios

- The Messaging Convention has entered into cooperative memorandums with a number of different kinds of curating enterprises
  - Government ministries
  - Government agencies
  - National CERTs
  - Trade associations (like APWG)
  - Hybrid special purpose NGO
  - National postal service
STOP. THINK. CONNECT.
Meet the National Curators
First national STOP. THINK. CONNECT. campaign in East Asia

The STOP. THINK. CONNECT.™ campaign in Japan is curated by the Council of Anti-Phishing Japan which recruited a group of some 20 technology companies, e-merchants and business infrastructure firms to manage its deployment

Operational as of December 2014

February 2016 deployed original STC posters at all 160 subway stations of the massive Tokyo Metro

Leadership is shared by JP CERT, Trend Micro and Hitachi Data Systems.

See: stopthinkconnect.jp
Campaign Architecture - Japan

- STC is evolved into a keystone for cybersecurity awareness outreach instrument for stakeholders addressing the general public and for industry actors.
- Can play to a crowd and, through industry, talk ‘inside baseball’
France

- Memorandum of Cooperation completed for the Republic of France in December 2015 by the French Center of Excellence Against Cybercrime, signed by IG of **Gendarmerie Nationale**
- CECyF is a public private partnership with management provided by French Interior
- Website launched in February 2016
- SEE: cyberprevention.fr
Campaign Architecture - France

CECyF employs the campaign to create a virtual omnibus channel for a number of cyber-security programs France manages.
Jamaica

- Jamaica organized its STOP. THINK. CONNECT.™ campaign through a coalition of the Ministry of Science, Technology Energy and Mining with the collaboration of the Jamaica Bankers Association.

- Its launch in January of 2016 garnered national media attention from the first day of the campaign.

- See: stopthinkconnect.org.jm
Campaign Architecture - Jamaica

- Under the leadership of Jamaica CIRT and MSTEM ministry, the campaign is an outreach and advisory scheme that brands and extends all general-public awareness programs in Jamaica.

- The one-stop shop provides STC-themed presentations to Boards, civil society groups and:
  - Posters in schools, churches and civic organizations;
  - This year, distributing a student cybersecurity handbook.

- Leveraging STC, the MSTEM ministry is developing plans for a full scale observance of Cybersecurity awareness month for this October.
**Switzerland**

- **SWITCH**, the national CERT and ccTLD manager, arranged for the MoC through Swiss Internet Security Alliance (SISA), an NGO largely managed by SWITCH and PostBank Switzerland.

- Campaign launched in late 2015. First in Europe to prepare and present materials for local languages. So far, German and French.

- See: stopthinkconnect.ch
Campaign Architecture - Switzerland

- STOPTHINKCONNECT.CH is employed for both broad cybersecurity awareness programming and for deep discussion of contemporary threats like ransomware.
- Links on the Ransomware campaign page point to anti-malware resources, educational materials and to police agencies for reporting cybercrimes related to ransomware.
Spain

• **Cibervolunterios**, a national-scope NGO dedicated to young people’s online safety, entered into licensing agreement with the Messaging Convention in 2013 and launched their own national STC campaign website.

• **INCIBE** (national CERT of Spain) signed the MoC in late 2015 and will be coordinating with Cibervolunteros and other organizations going forward.

• See: parapiensaconectate.es
Bangladesh

- First STOP. THINK. CONNECT. campaign launched in South Asia
- First STOP. THINK. CONNECT. campaign website launched under a .gov ministerial domain name: stopthinkconnect.gov.bd
- **National Data Center**, under the Bangladesh Computer Center/ICT Division completed the MoC on December 12, 2015
- Campaign website launched in early 2016 in English.
- National CERT working to develop an instantiation of the campaign website in Bengali
- APWG correspondence working to develop campaign beach head in the region, into a more coordinated deployment footprint
Armenia

- Joint memorandum of cooperation completed for Armenia in May 2016 by the Armenia Education Center and the Internet Society of Armenia
- Website launched in April of 2016
- Worked up translations of the advisories, posters and technical advisories packaged in the campaign
- See: safe.am/stopthinkconnect/stc.html
Unifying the Global Response to Cybercrime

The USA campaign was launched in 2010 by the Department of Homeland Security with DHS contractor National Cyber Security Alliance. Campaign adopted since then by hundreds of IT, security, financial services, retail and services companies, government agencies and NGOs.

See: stopthinkconnect.org
Nigeria

- **Cyber Security Experts Association** of Nigeria joined the Messaging Convention as a licensing partner of the campaign assets in 2015.

- CSEAN and DigitalSENSE Africa unveil the Nigerian national STOP. THINK. CONNECT.™ on June 11, 2016 at the annual DigitalSENSE forum conference.

- Messaging Convention working to help partnership cultivate its footprint in Nigeria and the West African region, coordinating with national campaigns in due diligence phase.

- See: stopthinkconnect.ng
Mongolia

- Established February 2016
- Curator: Mongolian Cyber Security Response Team
- Status: Live in English, working on translation into standard Mongolian
- See: http://apwg.alert.mn
Growing Community of Curators Assures Campaign’s Future

First conference for global stakeholders working to upgrade users **at scale** with a people-as-infrastructure perspective.

Curators presenting: Armenia, Latvia, Nigeria, USA, France, Spain, Switzerland, Slovenia

Program Partners: OAS, Commonwealth Secretariat, Europol & IGF
Concluding Discussion

- Involving the private sector, civil society and technical community to respond to cyberthreats? It’s all about:
  - Expressing the definitive problem statement
    - Identifying the part of the problem that belongs to everyone
  - Establishing and maintaining the assets over time to cultivate the crowd’s interests
  - Cultivate the stakeholder community that supports the common solution space enterprise
Thank you

- Peter Cassidy
- pcassidy@stopthinkconnect.org
- +1 617 669 1123