Guidance on Public-Private Information Sharing against Cybercrime

Based on the Recommendations for Public-Private Partnership against Cybercrime of January 2016
This document does not aim to address complex questions related to the implementation of penal codes or mutual legal assistance treaties since the sharing of information related to personal data, for example, is often difficult to achieve. Instead, the document seeks to address the space that exists prior to recourse to legal instruments. It addresses the voluntary sharing of information between parties based on trust and a desire to stop cybercriminals in their tracks prior to execution of further crime. Therefore, according to this document, “information” should not be interpreted as evidence or a type of intelligence usually shared by intelligence services.
Foreword

Jean-Luc Vez
Managing Director, Head of Public Security Policy and Security Affairs Member of the Executive Committee World Economic Forum

There were multiple developments in cyberspace in 2016, and while cyberattacks show no signs of abating, there have been continued efforts to address this global phenomenon.

With the Recommendations for Public-Private Partnership against Cybercrime report launched in January 2016, the World Economic Forum managed to create consensus and support among its Partners on what needs to be done jointly to better tackle cybercrime and its consequences. By continuing to catalyse dialogue and cooperation between government and private industry, it is our conviction that cybercrime and its negative consequences can be reduced.

The principles outlined in the Recommendations 2016 must be put into action to stop cybercriminals. The first element that was explored in 2016 was information sharing. If the challenges posed by cybercrime are to be surmounted, the sharing of information is vital. Technology is continuously evolving, causing new threats and vulnerabilities. The exchange of knowledge and ideas across sectors and industries is now recognized as a key factor in reducing the risks and consequences of cyberattacks. It allows businesses to better protect themselves, whether before or after an attack, and assists law enforcement agencies and the judiciary in investigating, apprehending and prosecuting cybercriminals. In short, information sharing allows for a more efficient fight against cybercrime.

Since embarking on the Cybercrime Project in 2015 (a pillar of the Forum System Initiative on Shaping the Future of Digital Economy and Society), what has struck us most is that while both the public and private sectors acknowledge the need and importance of cooperation, they often fall short when it comes to determining what exactly information sharing means. Therefore, the first step in implementing the Recommendations is to ask, what information should be shared and how should it be shared? This Guidance report aims to answer these questions so they can be used as a basis for public and private actors to develop and take further action.

Our deepest thanks are extended to the project members and participating constituents who through their dedication and knowledge sharing have made this work possible. It is our goal in 2017 to continue the implementation of the Recommendations 2016 and make progress in this important field which impacts us all.
Acknowledgements

This publication was prepared by Jean-Luc Vez, Managing Director, Head of Public Security Policy and Security Affairs, Member of the Executive Committee, World Economic Forum, and Ushang Damachi, Project Lead, Global Crime and Public Security, World Economic Forum

This publication was created with the input and contributions of the following individuals and companies/organizations to which sincere thanks and gratitude are extended:

Zainab Ahmad, Counsellor for Transnational Organized Crime and International Affairs, Department of Justice, USA
Peter Beshar, Executive Vice-President and General Counsel, Marsh & McLennan US Companies (MMC)
Adam Blackwell, Ambassador in Residence, William J. Perry Center for Hemispheric Defense and Security Studies (NDU), National Defense University, USA
Jamie Brown, Director, Global Government Relations, CA Technologies
Kevin Brown, Vice-President, BT Security, BT Group Plc
Marcelo Camara, Security Innovation Manager, Banco Bradesco
Alan D. Cohn, Adjunct Professor, Georgetown University Law Center, USA
Juan Colombas, Chief Risk Officer and Member of the Executive Committee, Lloyds Banking Group Plc
Michèle Coninsx, President, Eurojust
Debra Farber, Senior Director, Privacy, Security & Risk, Global Public Policy Department, Visa Inc.
Rich Fennessy, Chief Executive Officer, Kudelski Security Inc.
Andrew Gould, Detective Chief Inspector, Serious & Organized Crime Command, Fraud & Linked Crime Online, Metropolitan Police, United Kingdom
Pär Gunnarsson, Vice-President and Chief Security Officer, Group Security, Ericsson
Andrzej Kawalec, Chief Technology Officer, Enterprise Security Services, Hewlett Packard Enterprise
Jean-Paul Laborde, Assistant Secretary-General, Counter-Terrorism Committee Executive Directorate, United Nations
Rob Leslie, Founder and CEO, Sedici
Marco Mille, Head of Security, Siemens AG
Noboru Nakatani, Executive Director, Global Complex for Innovation, INTERPOL
Sundeep Oberoi, Global Head Delivery – ESRM, Tata Consultancy Services Ltd
Brent Phillips, Chief Information Security Officer, Zurich Insurance Group
Marc Porret, Legal Officer, Counter-Terrorism Committee Executive Directorate, United Nations
Ellen Richey, Vice Chairman, Risk and Public Policy, Visa Inc.
Jon Rigby, Director Cyber, AlixPartners
Dmitry Samartsev, CEO, BI.ZONE, Sberbank
Anton Shingarev, Vice-President, Public Affairs, Kaspersky Lab
Andrew Stanley, Chief Information Security Officer, Royal Philips
Jürgen Stock, Secretary-General, INTERPOL
Bruce Swartz, Deputy Assistant Attorney-General, US Department of Justice
Anne-Lise Thieblemont, Director of Global Technology Policy and Industry Relations, Qualcomm Incorporated
Lodewijk Van Zwieten, Senior Prosecutor, Eurojust
Stefan K. Vogt, Chief Information Security Officer, Credit Suisse Group
Rob Wainwright, Director, Europol
Steven Wilson, Head of Business, European Cyber Crime Centre, Europol

Geneva, Switzerland, January 2017
**Introduction**

When speaking of businesses and cybercrime, it is no longer a matter of whether a company will suffer a cyberattack but when that attack will occur and where in the attack lifecycle it is detected and contained. Unlike other types of crime, cybercrime is borderless, making it all the more harmful. Current legal systems are not advanced enough yet in this domain to fully protect industries from perpetrators. As such, it is generally recognized globally that to better deal with the negative aspects of the digital world, international cooperation between actors is required especially when it comes to sharing information. Hence, both public and private sectors understand that cybercrime can only be defeated by building trusted relationships across the world, voluntarily joining forces to fight this global threat.

Tackling cybercrime cannot be resolved unilaterally. Cybercriminals innovate, they do so with speed and by communicating and sharing information with each other. Public and private sectors must mirror these actions and find effective ways of sharing information to mount a more effective campaign against cybercriminals.

Information-sharing communities and platforms already exist around the world, such as the Cyber-security Information Sharing Partnership (CiSP) in the United Kingdom, and the National Cybersecurity and Communications Integration Center (NCCIC) and National Cyber-Forensics & Training Alliance in the United States. In addition, there are many multiple Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs) aligned by organizational industry. Despite this, clear processes and agreed standards on the type of information to be shared and the methods for doing so are lacking.

When consulting the public and private sectors, it became clear that the sharing of information raises two key questions: What type of information should be shared? How should it be shared? This report aims to provide insight on these two key questions by addressing the “what” and the “how” of public-private information exchange related to cybercrime. It seeks to build on the *Recommendations for Public-Private Partnership against Cybercrime*, published in January 2016, that call for increased cooperation between business and law enforcement at national and international levels. Recommendations 1 and 2 address the topic of information sharing:

1. Public and private sectors should share more information related to cyber threats, vulnerability and consequences
2. Public and private sectors should work to strengthen existing platforms, create new platforms and coordinate these platforms to increase information-sharing and improve investigations and prosecutions

In general, there are two main motives for sharing information. The first is a victim’s wish to limit the damage and consequences of a cyberattack and to help the investigations. The second relates to preventing an attack, when certain information has been detected, so the wish is to help others. In the former, the information will be more detailed, and will usually be shared with investigative and prosecutorial entities. With the latter, the breadth of information shared might be smaller but will reach a wider audience and enable entities to prioritize cyber defences to either prevent or mitigate against attacks.

This report is intended as a tool to help implement the Recommendations and enable efficient and beneficial information sharing. The goals are better detection, prevention and response to cybercrime, in a way that protects the customer as well as citizens’ privacy. A centralized exchange of data practices and experiences is vital if cybercrime is to be curbed.
What Type of Information Should Be Shared?

Key considerations
- Share all information not limited by legal constraints
- Information sharing should be a two-way street
- No sharing personal information without checking applicable legal framework
- Better to share processed data than raw data

How Should Information Be Shared?

Key considerations
- Real-time and 24/7 sharing
- Secure channels
- Know your counterpart
- Share processed data
What Information Should Be Shared?

Cyberspace is a vast domain. It contains an infinite amount of information with endless possibilities on what knowledge can be shared between actors on national and international levels. Consequently, instead of listing numerous types of digital information, we have broken it down into five categories: (a) indicators of compromise; (b) modus operandi; (c) attributing factors; (d) best practices and lessons learned; and (e) prevention, detection and protection measures. These categories represent the items we consider to be pivotal in thwarting cybercrime. They are “quick wins” in information sharing as they are mainly free of legal and regulatory constraints and can be shared without legal consequences and significant obstacles. They also respect customer- and citizen-privacy.

Context is as important as content in information sharing. The circumstances and basis upon which the information is being shared play a vital role. Understanding why information is being shared will:

- Impact the willingness to engage in data exchange
- Increase the frequency with which it occurs
- Help the sharing party to determine exactly what to share so the data provided is useful and protects privacy
- Provide a clearer picture of what the receiving party will do with the information

A decision to share information should be made only when the criteria stipulated in the considerations listed below have been met.

Key considerations

Prior to sharing information, the following considerations should be made to enhance the effectiveness of data exchange.

1. Presumption of sharing: Share information not limited by legal constraints

For knowledge-sharing to be effective, the parties involved should not only share the information they are legally compelled to share but also they should share the information they are not legally prohibited from sharing. This can help law enforcement and does not impinge on privacy rights of customers and citizens. For reasons ranging from lack of trust to competition and work prioritization, actors often have valuable information they are not legally prohibited from sharing but choose not to do so. By overcoming these reservations, the knowledge shared can help to reduce the risk of cybercrime – after all, there is common acknowledgement by public and private sectors that there is a joint interest in communicating and exchanging data. The more varied the type of information shared, the greater the chances of curbing an attack since it enables actors to learn from each other.
2. No sharing of personal information without checking the applicable legal framework

The focus of this guidance is intended to be on non-personal information. When personal data is part of the information shared, the party providing the information should check the applicable legal framework to ensure there are no restrictions in sharing the data. However, sharing information with law enforcement agencies and with private entities may be subject to different legal regimes. Personal information that is not relevant to mitigating a cyber-threat or breach should also not be shared. For example, a person’s education or medical condition typically does not play a material role in detecting, preventing and tackling a cyber-threat and, consequently, should not be shared.

3. Information sharing should be a “two-way street”

Reciprocal information sharing is a big incentive. Both public and private sectors must share information with each other: i.e. company to company; law enforcement agency to law enforcement agency; company to law enforcement agency; and the reverse. What better way to encourage future sharing than the knowledge that the information provided is relevant and has been put to good use. Both parties may possess valuable information, but often there is the perception that one of them seldom gets much in return. However, it must not be forgotten that the private sector has limitations due to high competition, and law enforcement agencies are subject to strong constraints on providing information. Therefore, attempts should be made to understand these limitations and manage expectations in this regard.

Law enforcement agencies, in particular, should continue to recognize the benefits of sharing with the private sector the successes and outcomes of tackling cybercrime. If the private sector or other sharing party is made aware of the outcomes of cases and of how the information provided led to a successful conviction, this will serve as motivation to continue to do so. Even if prosecutions do not take place, law enforcement agencies should share experiences on how information has strengthened their ability to deal with cybercrime.

4. Better to share processed data than raw data

Consideration must also be given to the quality of the data shared and ensure that it is clear and precise. The recipient must be able to determine rapidly what is at stake, what has to be done, and what is expected. For this reason, care should be taken to analyse and filter information from its raw format. The processing of data also provides a mechanism for ensuring that personal information is not included in the exchange.
Types of Information to Be Shared

a. Indicators of Compromise (IOCs)
No single organization has all the data and insights needed to prevent a cyberattack. Cybercrime cannot be fought alone. Cybercriminals use different methods of attack and transform rapidly. IOCs provide stark warnings that a network has been compromised enabling the parties concerned to anticipate cyber breaches and take the necessary steps. Accordingly, any type of identified malware would help third parties protect themselves and be alert to incoming attacks. The tracking and reporting of IOCs facilitate detection and response to cybercrime and allow for the development of more efficient defence mechanisms.

Examples of IOCs to be shared:
- Unusual network activity
- Login failures
- Unusual privileged account user activity
- Change of systems configuration
- Logins from non-business locations facilitate detection and response of cybercrime
- IP addresses;
- Counterfeited device identifiers: techniques exist to detect connected counterfeited devices on cellular networks
- Technical aspects of attacks: tools exist which facilitate the systematic discovery of new technical aspects of attack; e.g., the YARA tool allows for the identification and classification of malware (while it does not provide the answer to identification of all malicious items, it has proved to be popular)

Government and private industry tend to have extensive monitoring operations that give them exposure to an array of IOCs as well as indicators of attack, which, when combined, can be a more powerful force against criminal cyber activity.

b. Modus operandi: Tools, techniques and procedures (TTP)
What better way to defeat your adversaries than by knowing their methodology? Awareness of cybercriminal behaviour and modus operandi is imperative to the prevention and detection of cybercrime. Knowing what cybercriminals do and how they do it – their tools, techniques and procedures (TTP) – allows for deeper understanding and recognition of the source of a threat, suspicious patterns and malware, which in turn leads to a stronger defence against cybercrime. Cybercriminals are constantly innovating and communicating, which gives them the ability to use the same methods of attack on multiple victims. Circulating identified TTP among non-criminal actors will help to slow the rate at which criminals operate since they will have to develop new techniques for new attacks.

c. Attributing factors
This refers to what is also known as subscriber data. This type of data is regularly requested as part of criminal investigations, and has the most impact on electronic communication companies.

Generally, data is categorized as follows:
Traffic data. This data comprises information on the routing, timing and duration of calls, emails and text messages. It excludes the content. More specifically, as per article 1(d) of the Council of Europe’s Convention on Cybercrime (2001), “traffic data means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration, or type of underlying service.”
This information is typically used for billing and payment and to meet regulatory obligations such as data-retention requirements. A subscriber must usually be informed prior to the use of its traffic data for marketing or value-added services.

**Content data.** As the name implies, this data refers to what is contained in the telecommunication.

**Subscriber data.** As per the Council of Europe’s Cybercrime Convention Committee (T-CY), subscriber information refers to:
- The identification of the customer who has used a known IP address at a specific time; or
- The identification of the IP address used by a customer of an internet service provider whose identity is already known.

This definition is based on the previously referred to Convention on Cybercrime (2001) which specifies in article 18(3)(b) that subscriber information includes “the subscriber’s identity, postal or geographic address, telephone and other access number”.

Unlike traffic and content data (which provide in-depth information about subscribers’ activities and communication), subscriber data presents the least contention and the least infringement on the personal rights of individuals. Therefore, for the purposes of this document, the term “attributing factors” refers to only the IP address and name associated with it. It does not include anything that has to do with traffic and content data as described above which present more contentious issues.

Given these aspects, and considering that this data plays a pivotal role in criminal investigations by helping to identify the source of threats and crimes, it should constitute part of the information that is readily shared between parties seeking to resist cybercrime. Having said this, the sharing of subscriber information should be limited to malicious IP addresses (those reasonably believed to be related to threats or attacks). To preserve the privacy of customers and citizens, the sharing party should not be inclined to provide any type of information deemed personal unless it is specifically tied to a cybercrime.

**Example of successful international information sharing**

- In cybercrime, victims are often reluctant to report an attack and engage in the wider sharing of information for fear of reputational loss, material loss and litigation. The aviation industry, however, has proved the opposite. After an incident, companies often release highly detailed reports, including elements of what went wrong. These reports are vital, as not only airline companies but also aircraft manufacturers and everyone else in the aviation industry use these to improve their methods and procedures, improving security and avoiding future incidents. An example of such a report is the one published after the 1998 Swissair Flight 111 disaster.
- The Swiss Transportation Safety Investigation Board publishes reports on accidents and incidents within the transport industry with the same goals – prevention and security.
- Outside the aviation industry, the detailed technical report issued after the recent cyberattack on the Swiss technology company RUAG is another example of how widespread sharing can be put to good use.

Thus, where there is no contradiction to laws and regulations, every effort should be made to share subscriber data. This data is a core element of what would render data exchange particularly beneficial and has the potential to be rapidly implemented. It is recognized that in certain jurisdictions an IP address can be considered personal information. As outlined at the beginning of this document, no sharing of personal information should take place without checking the legal framework, and only information that is reasonably believed to be tied to a cyber threat or attack should be shared.

**It must be noted that in certain instances, and in certain regions, this information is readily shared. However, it is not the case globally as the sharing of this type of data is often subject to national laws.** This seriously hampers investigations and apprehending criminals. Variations in laws cause a reliance on mutual legal assistance (MLA), which can be time-consuming and burdensome. Criminals, however, act with speed and agility so by the time MLA comes into effect they will have moved on to other victims and developed new ways of executing cybercrime. In many ways, they can be said to have the advantage and the only way to circumvent this is for non-criminal actors to combine forces and exchange these attributing factors.
d. Best practices and lessons learned

The sharing of best practices and lessons learned is one of the easiest ways of enhancing security against cybercriminals. Not only does it avoid duplication of efforts but also it allows organizations to engage in a multifaceted and subsequently a more productive approach to combating cybercrime. It is by learning from each other that gaps can be identified and stronger defences put in place. Disseminating lessons learned from dealing with cybercrime can help others in establishing the correct defensive mechanisms to prevent a reoccurrence. These include matters such as how to improve incident-response plans so that once an attack occurs disruption can be minimized and business continuity ensured. This throws the burden back on the attackers and slows their actions as they can no longer rely on similar methods to attack multiple victims. Collaborative work is a necessity and, more importantly, the sharing of best practices, experiences and lessons learned helps actors from around the world realize that they share similar challenges – common ground on which greater communication and trust can be built.

e. Prevention, detection and protection measures

Cybercrime cuts across sectors and industries. While the concerns and impacts may be different, the negative consequences criminal cyber activity has on an organization are the same, irrespective of the sector and industry. Some industries will mainly be concerned with client data; for others, it might be intellectual property. This means each industry will focus on developing measures that protect their activities and permit easier prevention and detection within their scope of activity.

These measures are what the US Cybersecurity Information Sharing Act of 2015 fittingly refers to as “defensive measures”. They can be summarized as actions applied to an information system or the content therein to “detect, prevent, or mitigate a known or suspected cybersecurity threat or security vulnerability”. While the focus tends often to be on information posing a direct threat or vulnerability, the actions taken to protect a system should not be neglected. Protective measures can prevent a cyber-breach.

Although defensive measures are necessary, they should not be the only actions. Participating in forums where methods of prevention, detection and protection are shared alerts actors to items they might not have previously considered and provides alternative approaches to dealing with cybercrime. Indeed, certain mechanisms and intrusion-detection systems used in one industry could be adapted to other industries.
For a long time, there has been no formal framework for how information is to be shared, which impedes the process. However, governments are realizing that for information sharing to be used to the fullest extent, the private sector and other parties must have ways of communicating the often vast wealth of data they are privy to. A recent example of this is the guidance issued in June 2016 by the US government on the sharing of cyber-threat indicators and defensive measures, while protecting privacy, as a result of the Cybersecurity Information Sharing Act 2015.

Key considerations
When determining how to share information, the following items should be considered:

1. Know your counterpart

   Prior to sharing information, a key consideration is to know your counterpart. This concept is twofold and involves:
   - Ensuring that good relations are maintained between both public and private sectors. This is pertinent for private industry which is encouraged to actively engage with local/regional authorities as well as other opportunities for information sharing in the jurisdictions in which they operate. Frequent interaction with authorities allows for easier determination of which governmental institutions and/or person is responsible for cyber breaches before the actual breach occurs. Waiting for an attack to happen is counter-productive; knowing your partner in advance facilitates reporting and other processes that need to be fulfilled when an attack happens. This can be achieved, for example, by: (i) knowing your national/regional law enforcement agency; (ii) joining a local Community Emergency Response Team (CERT) programme; and (iii) contacting INTERPOL’s Cyber Fusion Centre (see p.13).
   - Ensuring that the party with which data is being shared is legitimate, will put the data to good use and will not use it for purposes other than to further the fight against cybercrime.

2. Real-time and 24/7 sharing

   Though not always possible, actors should endeavour to share information in real-time as it enables prompt corrective actions to be taken, thereby limiting the impact of criminal cyber activity. The type of information being shared will frequently determine how quickly and how often the information is shared. For example, best practices do not necessarily need to fall within the real-time and 24/7 category; they can be exchanged later.

   As mentioned, real-time and 24/7 sharing is not always achievable. For instance, investigations and prosecutions span lengthy periods and it can be some time before law enforcement agencies and the judiciary can share back information with industry informing them that the provided information has led to an arrest and subsequent conviction. Hence, while the importance of real-time information sharing cannot be emphasized enough, expectations on this happening consistently cannot be too high, though parties should nonetheless try to achieve it. Whatever the means chosen to share information, parties should strive to do so as quickly as possible so the necessary preventative or remedial actions can be taken.

3. Secure channels

   Knowledge exchange habitually involves sensitive information and having secure information-sharing channels is essential. Encryption can play an essential role to safeguard the data. Encoding the information being exchanged means that only the intended recipient can access it thereby assuring the integrity and authenticity of the data.
Methods of Sharing Information

The following outlines the various ways in which actors can partake in information sharing:

a. Information Sharing and Analysis Centers (ISACs)

ISACs play a pivotal role in the information-sharing process; they can be said to act as mediator between the party sharing the information and the receiving party(ies) of this information. The ISAC acts as a centre-point of information-sharing activity. It will filter, analyse and organize the information received before sharing it more widely with other members, other ISACs and with law enforcement agencies. There are many ISACs worldwide and many exist according to industry; e.g., the Retail Cyber Intelligence Sharing Center (http://www.r-cisc.org/). Joining an ISAC and using it as a mechanism for information sharing is an effective method for dealing with how to share the information. ISACs are based on voluntary membership and tend to have pre-established relationships with government authorities and, as such, have the public-private representation necessary to enrich the information-sharing process. ISACs prevent individual organizations having to figure out who should be contacted to relay information and how to contact them. It enables information to be distributed to a wide net of actors across the globe at once.

b. Cyber centres and cooperation frameworks

Participation in cyber centres of cooperation presents an effective method of accessing pertinent cyber information and being able to share information with other participating members. These centres (which tend to be regional or national) are hubs of knowledge, support and information on cybercrime. Such centres and frameworks provide multistakeholder solutions to information gathering and investigation into criminal cyber activity. They are based on the notion that cybercrime is a shared responsibility with several components required: (i) assessing the cyber environment; (ii) information sharing; (iii) operational cooperation; and (iv) training and capacity building. INTERPOL’s Cyber Fusion Centre within its Global Complex for Innovation in Singapore (https://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation), Europol’s Joint Cybercrime Action Taskforce (J-CAT) (https://www.europol.europa.eu/ec3/joint-cybercrime-action-taskforce-j-cat), and Japan’s Cybercrime Control Center (JC3) (https://www.jc3.or.jp/index.html), for example, are all frameworks on this basis. They convene government and private industry to collect and analyse digital information.

Being public-private operations means these centres are well-placed not only to obtain information but also to receive information and distribute it further, both nationally and internationally.

Examples of processes used to facilitate cooperation

– The sharing of information via cooperation centres and cooperation frameworks can be further facilitated by STIX (Structured Threat Information Exchange) and TAXII (Trusted Automated eXchange of Indicator Information) standards, which have been spearheaded by the US Department of Homeland Security (DHS). They provide an automated way of sharing information, relieving some of the burdens related to the manual work and filtering of information prior to sharing. STIX assists in systematizing the language of the information, and TAXII provides for the automated exchange of the information.

– This is achieved through the DHS Automated Indicator Sharing (AIS) initiative (https://www.dhs.gov/ais); a prime example of a cooperation framework utilizing STIX and TAXII. The AIS programme operates on a voluntary basis and enables automated sharing of information between public and privately owned entities under the framework of CISA 2015.

– An additional cooperation framework is the previously mentioned Joint Cybercrime Action Taskforce initiated by Europol. It provides a platform for exchange, data gathering and investigation into criminal cyber activity. It embraces the fact that fighting cybercrime is a shared responsibility and as such requires the engagement of multiple stakeholders.

c. Working groups/networks

A lot of information sharing that occurs is by informal mechanisms. Even in cases where an informal network has been established it is often the case that these are simply groups of actors from various sectors that come together and undertake to learn from each other to enhance their cybersecurity and threat-awareness. Communication tends to be mostly by email or by posting information on a shared system. As long as the groups consist of diverse participants, these groups and networks represent a positive step in partaking in knowledge exchange.
Conclusion

While there have been positive developments in efforts to tackle cybercrime, more progress can be made. Cyberspace still has many gaps, notably the discrepancies in regulation and legislation across jurisdictions. These disparities mean that pinpointing an exact process on information sharing is not easy. We hope this document not only enhances information sharing but also creates new processes on both national and international levels and streamlines existing information sharing so it becomes second nature.

Knowledge is a powerful tool – it is instrumental in ensuring strong defences against cybercrime. Threats differ according to sector and industry, and the participation of a range of actors in information sharing enhances awareness and increases protection for all. Knowledge exchange yields greater efficiency, innovation and resourcefulness. By encouraging actors to be innovative and understand the importance of sharing information with their counterparts, including those around the world, they will be more creative and inventive in crafting protective, detective and defensive mechanisms to counter criminal cyber activity.

What remains at the heart of the fight against cybercrime is that public and private sectors are committed to the same goals because they share the same interests. Information sharing intensifies the efforts to engage in mutual activity that will identify strengths and weaknesses of this fight and subsequently allow for better investment and allocation of resources to achieve successful outcomes.
Information sharing should be a “two-way street”, p8
Council of Europe (2013), T-CY Guidance Note #8


Better to share processed data than raw data, p8

Indicators of Compromise, p9


Modus operandi: Tools, techniques and procedures (TTP), p9


Attributing factors, p9
Council of Europe (2013), T-CY Guidance Note #8


Best practices and lessons learned, p11


Prevention, detection and protection measures, p11


Know your counterpart, p12


Information Sharing and Analysis Centers (ISACs), p13


Cyber centres and cooperation frameworks, p13


Mitre, Structured Threat Information eXpression — STIX. Available at https://makingsecuritymeasurable.mitre.org/docs/stix-intro-handout.pdf


Conclusion, p14

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.