Bloomberg BNA

Electronic Commerce & Law Report™



COOPERATION FOR CYBERSECURITY

Cyberspace threats have become a paramount concern and are presently destabilizing the global order. Government alone cannot solve this threat. The authors propose a public-private partnership model that strikes a balance between the competing interests of government and private industry to ensure a successful partnership with effective results.

# Public-Private Partnerships for Cybersecurity

By Adam Palmer, Rich LaMagna, and Doug DePeppe

## Introduction

It is unlikely that federal agent Eliot Ness considered partnership with the private sector as a key strategy when he attempted to catch the notorious gangster Al Capone in the 1920s. However, public-private partnership is now necessary in confronting cybercrime and other cybersecurity threats. Prior to the creation of the internet, a successful law enforcement strategy was relatively straightforward: a structured government entity—a law enforcement agency—tasked with addressing a known kind of criminal threat, normally limited to national borders. Criminal activity might have varied in complexity and sometimes required forensic analysis of evidence, but it generally did not require investigators to possess advanced computer skills. Moreover, crime prevention, investigation, and prosecution were viewed as dimensions of an inherently governmental function. Today on the internet, a far different strategy is needed.

*Adam Palmer (JD, MBA, CISSP) is a globally recognized cybersecurity law and policy expert living in Europe. Doug DePeppe (LLM, JD) participated in two White House-directed initiatives on cybersecurity and is a recognized cybersecurity thought leader and international consultant living in Colorado. Rich LaMagna (MALS, CPP) is a former U.S. federal law enforcement and technology industry senior executive and recognized IP and cybersecurity expert living in the D.C. area.*

The internet has turned law enforcement strategy ''upside down.'' Cybercrime presents an asymmetric threat involving criminal schemes that cross international borders, utilize private global communications networks, require highly technical investigative skills, and necessitate cooperation among many internet security stakeholders. The model of a small police task force of ''Untouchables'' chasing Al Capone has been replaced by the need for an integrated global effort.

## The Case for Partnering

Private sector corporations that build and control the backbone networks of the internet provide critical support to identify and trace cybercrime activity. These private sector partners provide not only critical access to networks on which evidence is distributed, but also necessary technical expertise. However, like choosing a close friend in life, selecting the right trusted security partner is both important and often difficult. The rewards of finding and building a partnership are many, but the mere creation of a partnership presents new and unique challenges to traditional models of law enforcement.

Global cybercrime is estimated to cost approximately $388 billion annually with a substantial growing risk of identity theft.[1] Creating a scalable, cost-efficient response to this threat requires law enforcement to leverage private sector partnerships. The private sector can respond more quickly than government. Private companies also provide technical expertise that investigators may not possess. In turn, private sector entities benefit

[1] Norton by Symantec, *Norton Cybercrime Report 2011.*

 ISSN 1098-5190

from a law enforcement partnership by expanding their toolkit of solutions to include actual arrests of suspects, asset seizure, and other sanctions that can provide long-term deterrence.

Given the variety and complexity of information-sharing needs, it is impossible to identify a single best partnership model that will be successful. Rather than attempt to propose a single model that can succeed in all situations, the purpose of this paper is to analyze existing partnership models, address challenges to partnership, and identify common attributes that exist across successful public-private partnership models.

## Defining Roles: Understanding the Gap Between Public and Private Sector

In its 2008 ''Guidelines for Cooperation between Law Enforcement and Internet Service Providers against Cybercrime,''[2] the Council of Europe (''COE'') outlines broad strategic goals and benefits to a public-private partnership fighting cybercrime. While beneficial in providing broad strategic guidance, these guidelines do not address two critical elements of public-private partnerships:

1. Membership: The term ''Internet Service Provider'' in the COE guidelines is limited and does not address the broader group of critical ''electronic services provider'' partners, including security vendors, internet infrastructure providers, cloud technology providers, and device manufacturers. These private sector groups form critical components of the cyber landscape and should be considered for inclusion in any successful partner program.

2. Strategic Focus: The COE guidelines focus on ''encouraging'' behavior, but fail to substantively address the specific strategic challenges that cause many partnership efforts to be unsuccessful. Despite the obvious benefits of a public-private partnership, significant obstacles to a successful partnership must be directly addressed and resolved.

## Fundamentally Different Viewpoints

Public and private entities have fundamentally different viewpoints related to intelligence sharing, goals, approach structure, and the regulatory environment, as described below.

### Intelligence Sharing.

Private sector entities, particularly financial companies, may fear harm to their brand's trusted reputation or possible regulatory scrutiny following disclosure of data security issues. These entities are inclined to conceal data breaches and intelligence threats so as to minimize harm to their brand reputation.

This view of cybersecurity intelligence—as a competitive advantage that should be safeguarded rather than shared—produces a challenging environment for partnership to succeed. Moreover, government entities are inclined to view all information as classified. While receptive to receiving information, government may not reciprocate by sharing intelligence. Such a dynamic quickly discourages private sector participation when there is a perceived lack of two-way data sharing.

### Goals.

When responsive action is required against cyber attacks, private entities are strongly inclined to adopt short-term, stop-gap measures in order to mitigate risk. In contrast, government entities typically adopt a long-term, all-encompassing, arrest-focused view. These views inevitably conflict when a private entity attempts to halt a cyberattack with haste, while law enforcement officials spend months (or years) building a successful case for prosecution.

Such divergent views have led to ''competitive'' strategic approaches for combating cybercrime. The private sector may exclude law enforcement in favor of a ''disruption strategy'' that attempts to pressure cybercriminals by blocking access to technology networks. By intending to make cybercrime operations difficult and unprofitable, this approach also places secondary focus on arrest of the actual criminal.

### Regulatory Environment.

Both U.S. and European industries operate within complex privacy regulatory schemes. For global entities to effectively cooperate, it is generally necessary for shared information to be non-personally identifiable and non-classified. Further concerns arise when threat data is shared with governments considered untrustworthy.

While it is possible to overcome these obstacles through appropriate data-sharing guidelines and restricted member access, these concerns are frequently cited for non-participation in partnership programs. This issue, however, may be more a result of legal staff lacking experience in these areas of policy, rather than an actual legitimate barrier to partnership.

### Structure.

The standard government strategy model involves centralized control and administration of programs that implement proposed solutions. When private sector support is needed, it is contracted, and complex regulatory processes govern the relationship between government and industry.

A public-private partnership offering a non-contract, decentralized execution model represents a new strategy that empowers industry to operate in an integrated fashion with government. Legal frameworks, trust, incentives, and other factors must develop as enablers for a robust public-private partnership model to flourish.

## Goals of Partnership: A Shared Responsibility

Both industry and government have a mutual benefit in developing and maintaining effective partnerships on various levels. In order for these partnerships to function properly and effectively, there must be agreement as to the goals of the partnership.

### Improved Cybersecurity.

The ultimate goal of cooperation between government agencies and the private sector is to stop the malicious activities in cyberspace, thereby reducing the amount of cybercrime on the internet and improving cybersecurity.

[2] http://www.coe.int/t/informationsociety/documents/Guidelines_cooplaw_ISP_en.pdf.

   ISSN 1098-5190

The achievement of this goal is only possible through two-party cooperation since neither side possesses all of the information or capability to stop cybercriminals.

### Deterrence.

Another goal of public-private partnerships is to deter cybercrime by presenting a united front between government and the private sector. This demonstrates strategic resolve in combating cybercrime, thereby creating a deterrence to criminals.

If criminals are aware of these efforts and sense true economic and legal pressures, they will be discouraged from committing further crimes.

### Intelligence Sharing.

For government and industry to be effective in combating cybercrime, information sharing is essential. This information must be actionable intelligence rather than voluminous amounts of data. Through intelligence collection, analysis, and data sharing, preventive measures—even new technologies—can then be adopted that improve defenses against cybercrime.

### Preparedness.

Situational awareness enabled through a public-private partnership also raises the readiness level of all participants. With greater preparedness, members can more readily respond to incidents—and prevent attacks before they happen.

## Overview of Industry and Government View

In the post-9/11 era, public-private partnership has emerged as a mechanism of choice to position society in a mutual protection strategy against an ''inside-out'' threat. This ''inside-out'' threat, often referred to as an ''asymmetric'' threat, forces changes in security approaches because it presents unforeseen attack vectors which may cause significant damage to both public and private infrastructure.

The public-private partnership enables the government to use resources near this infrastructure to counter cyber attacks. This model moves toward a counter-asymmetric strategy that is better able to address threats to critical infrastructure. The essence of this model, therefore, is to leverage private resources with governmental power in order to counter attacks that threaten critical infrastructure.

### Private Sector Cyber Readiness.

Notwithstanding the Report of the U.S. 9/11 Commission[3], which was insightful in its description of the ''way forward'' in a new era of asymmetric threats, most governments have not adequately educated society about the challenges of modern asymmetric threats—especially in the context of cyberspace. To most private citizens and corporations, protection from catastrophic threats remains an inherently governmental function.

### Information Sharing Barriers.

The private sector is constrained by compliance, competition, trust, and legal concerns. These concerns cause uncertainty and hesitancy. Risk-averse enterprises, however, may fail to recognize the business case for instituting a pro-government cooperation model. Although the maturity of the public-private partnership model may need to strengthen before industry fully embraces it, the risk of survival to the enterprise is far greater by attempting a ''stand-alone'' independent protection model.

### Government Leadership.

Government must recognize the structural, cultural, and legal impediments to realizing a fully empowered and mature public-private partnership model. Government has repeatedly claimed that the cyber threat represents one of the most grave threats to national security and international stability. The public-private partnership model has been advanced as the mechanism to involve all of society in a mutual protection pact. As such, government bears a substantial burden for transitioning society into a new framework of cybersecurity in which the fundamental feature is an integration of the public and private sectors.

## Comparison of Partnership Models

The contrasting strategic viewpoints of government and the private sector create challenges to a successful partnership. However, despite these obstacles, there is little debate regarding the obvious potential benefits of a public-private partnership. Therefore, the appropriate focus is to analyze the best model for a successful partnership that can minimize difficulty and provide the greatest benefit.

A successful partnership must be founded upon reciprocal information sharing, trust, and shared benefit. In the last decade, five primary models have emerged for a cybersecurity public-private partnership. These models may be classified as:

- Non-profit information sharing at global level;
- Distributed information sharing at community level;
- Centralized information sharing at community level;
- Closed government; and
- Industry informal collaboration

### Non-profit Information Sharing at Global Level.

This model creates a non-profit corporation that serves as a neutral intelligence-sharing entity. The non-profit secures the privacy of information, provides analysis of raw data, and converts data into intelligence that is shared with both public and private entity members who have been vetted. The principal advantage of this model is the opportunity for actionable intelligence to be created and shared among trusted partners at minimal cost. This model also provides a centralized global point of intelligence gathering.

However, this model's principal fault is that it lacks an incentive for mutual participation. Information sharing in this model must be encouraged by mandating that ''only those who give will receive.'' In actual practice, however, this is rarely enforced. Competitive concerns in the private sector and government fears of releasing confidential information frequently drive lack of cooperation.

[3] http://www.9-11commission.gov/report/911Report.pdf.

This model also raises questions about the value of a centralized resource. Co-location of assets at a central location encourages shared participation, but it is not a total solution. If law enforcement agents assigned to this central group are not the ''best'' case agents, there may be little value in their centralized co-location.

Additionally, the centralized collection of data may actually be a negative by failing to provide actionable localized intelligence. While a global view is helpful, participants may be frustrated by the lack of data that impacts their specific industry or local community. If the information is perceived as weak, law enforcement and private enterprise may lack incentive to take action based on the information.

### Distributed Information sharing at Community Level.

Effective security is expensive, yet an asymmetric threat—especially the advanced persistent threat—necessitates competent capability centers that can scale to respond to regional incidents. Under this model, distributed capability may be linked virtually on a shared basis so that no single location bears the brunt of the expense.

Certain cybersecurity functions require on-site support; however, analysis, malware repositories, coordination, administration, planning, and other functions may be distributed. A secured portal, database, and other operations support technologies could be hosted in a cloud platform for distant locations to access and utilize.

This model would allow for initial development and scaling of cybersecurity capability centers without having to incur the expense of a capability center in every community.

### Centralized Information Sharing at Community Level.

Some communities require a comprehensive cybersecurity capability center. This determination is based on community size, resources, critical infrastructure, and other needs. Community participants, both industry and government, function as both data providers and data users.

The capability center functions as a malware repository, analysis and reporting center, incident responder, and interagency facilitator, as well as other functions determined by the community's needs.

Trust among the members is pivotal to the success of such an enterprise; accordingly, confidentiality and information-sharing mechanisms that protect data providers from attribution, embarrassment, and harm from disclosure are important components of the center's operations.

### Closed Government.

This model is focused primarily on developing a core police operations center with external outreach minimized to support only government threats. This model requires high government spending since the core of the model is built on expanded police outreach.

The value in this model is primarily derived from arrests and international police cooperation. The benefits of this model are that information can be tightly controlled among government entities. This model, however, requires high costs to develop and maintain, with minimal involvement of the private sector beyond a supporting capacity.

### Industry Informal Collaboration.

This is the reverse of the closed-government model. In this model, an industry member company (or companies) creates a private sector group that may include limited involvement from government. Police partnership in this model may vary from highly involved to very limited. In the highly-involved model, the private sector group may focus efforts on training and supporting police. However, in a more closed form, this model may exclude police in favor of a ''disruption'' strategy that attempts to pressure cybercriminals through civil legal actions. This closed model may still provide support to police, but the emphasis will be on private sector action and not arrests.

## P.A.R.T.N.E.R.—A Road Map for Success

Considering the guidelines outlined below, a partnership program will create a solid foundation for success by addressing the most significant challenges. Ultimately, success depends not only on the willingness of partners to participate actively, but also on their agreement to essential guidelines. Trust is the key ingredient in forming a successful partnership—this can't be emphasized enough.

Encouraging enterprises and government to share information is very difficult, but if data-sharing agreements are very specific and carefully drafted, actionable intelligence can be shared. Mutual recognition of their shared roles is also key to a successful cybersecurity partnership. Government investment in developing partnership models, promoting community capacity building, and supporting education and awareness initiatives is critical. Similarly, industry must stop viewing cybersecurity as a competitive issue, but rather as a shared ecosystem-protection concern.

While no single partnership model may be a total solution in every instance, certain characteristics should be included in every partnership effort to increase the likelihood of success. Below is an outline of these elements in a strategic guideline termed ''P.A.R.T.N.E.R.'' We believe that the P.A.R.T.N.E.R. strategy provides a ''road map'' to the development of a successful public-private partnership.

### Platform Neutrality.

A neutral non-profit entity serves as the best platform for supporting a successful partnership. Both government and the private sector must be comfortable in an environment that is trusted and neutral. Effective partnership should be built on a foundation that is not subject to pressures of government intrusion or revenue generation beyond operational costs. This model also provides the best framework within which to develop shared-intelligence frameworks that do not violate national privacy laws or raise concerns regarding inappropriate business relationships between government and industry.

### Authority.

A successful partnership must include government entities and industry groups across international borders. Members must possess executive authority over critical internet assets and a willingness to take action

  ECLR ISSN 1098-5190

on case intelligence. Partner members must commit resources to fund the project adequately and provide the technical expertise necessary for success.

### Rules for Data Sharing (Enforced).

The desire to involve law enforcement or large network providers may result in relaxed demands on participation in data sharing. Any member that does not share data should be subject to the strict exclusionary rules of the partnership, regardless of the entity's importance. A non-participating partner serves no purpose. As long as the correct framework for sharing non-personal and non-classified information is in place, there should be no grounds for refusing to share data. Failure to reciprocate in data sharing will doom any partnership effort.

### Trust.

Confidentiality must be strictly enforced through legal agreements and technical privacy controls. No data will be shared in an environment in which trust is not reasonably guaranteed.

### No Open Membership.

If everyone is a member, then no one benefits. Too many groups measure success by the number of members. The actual measure of success should be based on assuring substantive participation from a small number of trusted members. Every effort should be made not to create regional or segmented groups, as this directly hinders the borderless investigation of cybercrime. However, the goal should be cooperation among participants rather than simply a large number of members.

### Encourage Benefits.

Public relations, network security, and arrests are all appropriate value propositions for a partnership program. Each member must respect the different goals of partners and encourage appropriate value return. Reasonable confidentiality for case work can be maintained while still supporting members who desire to acknowledge their participation in success publicly. Supporting value benefits from member participation will encourage long-term success.

### Responsive.

A cyber attack on one partner will affect another partner later. Each member of the partnership must exercise care and concern for all attacks, not just those affecting the specific member. Both government and private sector members must receive and share valuable intelligence and consider an attack on one member as an attack on all members.

## Conclusion

The internet age is presenting new challenges upon society. Cyberspace threats have become a paramount concern and are presently destabilizing the global order. Government alone cannot solve this threat. Similarly, the risk to industry is too great to defer to the inherently governmental-function model of the Capone era.

Today on the internet, security and preparedness are a collective responsibility. The public-private partnership model is the preferred method for addressing modern risks from cybercriminals. Several versions of this model have been advanced, but a model incorporating the P.A.R.T.N.E.R. guidelines attempts to strike a balance between the competing interests of government and private industry to ensure a successful partnership with effective results.