



# MEASURING THE CYBERSECURITY PROBLEM



Copyright © 2013 EastWest Institute  
ISBN: 978-0-9856824-3-9  
Cover illustration by Dragan Stojanovski

The views expressed in this publication do not necessarily reflect the position of the EastWest Institute, its Board of Directors or staff.

The EastWest Institute is an international, non-partisan, not-for-profit policy organization focused on confronting critical challenges that endanger peace. EWI was established in 1980 as a catalyst to build trust, develop leadership, and promote collaboration for positive change. The institute has offices in New York, Brussels, Moscow and Washington. For more information about the EastWest Institute or this paper, please contact:

The EastWest Institute  
11 East 26th Street, 20th Floor  
New York, NY 10010 U.S.A.  
1-212-824-4100  
communications@ewi.info

[www.ewi.info](http://www.ewi.info)

# MEASURING THE CYBERSECURITY PROBLEM

By **Karl Frederick Rauscher** and **Erin Nealy Cox**



**EASTWEST INSTITUTE**

*Forging Collective Action for a Safer and Better World*

## About the Authors

### **Karl Frederick Rauscher**

Karl Rauscher is a Distinguished Fellow and the Chief Technology Officer of the EastWest Institute, serving its mission to convene strategic dialogue, reframe intractable problems, and mobilize resources for a safer, more stable and more secure cyberspace. In leading the institute's Worldwide Cybersecurity Initiative (WCI), he oversees strategic Track 2 bilaterals among the world's cyber super powers (China, India, EU, Russia and the U.S.), pioneers policy for norms of behavior for cyber conflict, advances emergency preparedness for crises in cyberspace and unleashes private sector leadership with innovative problem solving.

He recently led and authored reports for three major bilaterals: China-U.S. Fighting Spam to Build Trust, and Russia-U.S. Working Towards Rules of Cyber Conflict - Rendering the Geneva and Hague Conventions in Cyberspace, and Russia-U.S. Critical Terminology Foundations. He also led the IEEE Reliability of Global Undersea Communications Cable Infrastructure (ROGUCCI) Study, which provides guidance for improving the resilience of the critical international infrastructure that underpins the Internet. Consistent with the "think and do" character of the Institute, Karl works with stakeholders to champion the implementation of the recommendations associated with these reports.

### **Erin Nealy Cox**

As Executive Managing Director at Stroz Friedberg, Erin Nealy Cox contributes to the management and day to day operations of Stroz Friedberg, in addition to having overall responsibility for the Dallas, Minneapolis and Chicago offices. As such, she supervises cybersecurity, digital forensic, Internet investigations and electronic discovery assignments for major law firms, government agencies and corporate information technology departments involved in criminal, civil, regulatory and internal investigations. She also serves as the firm wide practice lead for the cyber security practice. As a result, she specializes in the supervision of data breach cases involving outsider and insider threats, as well as, economic espionage cases facilitated by the Internet.

Her experience extends to leaks of confidential information, wiping, mass deletion and other forms of spoliation, and computer-enabled theft of trade secrets and insider information. She regularly consults on the technical and strategic aspects of initiatives to protect computer networks from malware and malicious code, online fraud, and other forms of illicit Internet activity. As a result, she is a trusted advisor to top executives, in-house lawyers, and outside counsel.

# CONTENTS

<b>Foreword</b>	7
<b>Preface</b>	9
<b>1. Executive Summary</b>	10
<b>2. Introduction</b>	12
2.1 Brief History of the Initiative	12
2.2 Objectives	13
2.3 Value Proposition for Participants	14
2.4 Scope	15
2.5 Gap Analysis	16
2.6 Proposed Process	20
2.7 Frequently Asked Questions	22
<b>3. Key Observations</b>	28
<b>4. Recommendations</b>	32
4.1 Trusted Entity for Cybersecurity Statistics	34
4.2 Voluntary Data Contributions	36
4.3 Bona Fide Benchmarks	38
<b>5. Conclusions</b>	40
Appendix A: Cyber40	41
References	42

The following individuals served as subject matter experts during the development of this report. Their contributions from their respective fields of experience as a stakeholder, a corporate manager or technical expert were essential to the analysis, conclusions and guidance presented herein.

**Greg Alexander**, Priceline  
**Burke Autrey**, Ristken Software Services  
**Kamlesh Bajaj**, Data Security Council of India  
**Michael Barrett**, FIDO Alliance  
**Joe Barton-Holme**, RBS Group  
**Frank Biller**, Hitachi Consulting Corporation  
**Raymond Bonelli**, IEEE CQR  
**John Carlson**, BITS  
**Maria Livanos Cattai**, ICC (fmr Chair)  
**Eric Cole**, McAfee  
**Art Dahnert**, Overwatch System Ltd  
**Liu Deliang**, Asia-Pacific Institute for Cyberlaw Studies  
**Daniel Kriz**, ITIC  
**Richard E. Krock**, IEEE CQR; ATIS NRSC  
**Francisco Ginel**, Telefonica  
**John Harrison**, Landitd Ltd.  
**Stacey Hartman**, CenturyLink, ATIS NRSC  
**William A. Heinrich**, BNSF  
**Selahaddin Karatas**, Solidpass  
**Li Yongkui**, Huawei  
**Daniel Nowak**, VSS Monitoring  
**Michael O'Reirdan**, Comcast  
**Audrey Plonk**, Intel  
**Ramses Martinez**, Yahoo  
**Earl Rasmussen**, Net'Q  
**Andrea Rigoni**, Global Cyber Security Center  
**Neil Rondorf**, ICPC Chairman, LEIDOS  
**Vartan Sarkissian**, Knightsbridge Cybersystems  
**Bill Smith**, PayPal  
**Andrew Steingruebl**, PayPal  
**Mike St John-Green**, Independent Consultant  
**Shane Tews**, 463 Communications  
**Karim Toubba**, Juniper Networks  
**Jerry Upton**, Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG)  
**Scott Vowels**, Comerica Bank  
**Brett Wahlin**, McAfee  
**David Weisman**, PayPal  
**Eric Werner** (deceased)  
**Zhou Yonglin**, Internet Society of China

Special appreciation is also here expressed to the following EWI staff for their project management of the breakthrough group activities: **Franz-Stefan Gady, Alison Kung, Anneleen Roggeman** and **Nathan Wendt**.

Everyone knows that we have a cybersecurity problem on our hands.

But just how bad is it? Is it getting better or worse, and by how much? Governments and corporations are spending tens of billions annually to address the known and perceived cybersecurity concerns. What is the return on these massive expenditures? There is insufficient data to make such a determination. It is unclear how we would know if we were making progress.

Everyday tens of trillions of dollars flow across a cyberspace that we know is riddled with cybersecurity problems. However, our measurements of the problem to date are insufficient to answer many important questions. We have gone too far down this path without making important observations about these problems, such as their relative frequency and evolution over time.

Furthermore, a significant disconnect exists within many corporations, where the leadership is unable to justify increased security methods or spending due to a lack of measurement information. Having trusted metrics and performance benchmarks will significantly reduce this information asymmetry between security and executive leadership in numerous organizations.

This report presents a bold solution to this problem that involves private sector leadership aimed at promoting trust and cooperation. That is what is needed to make use of existing information that is separately held by individual companies.

We applaud this private sector initiative to tackle this predicament in a straightforward way. Governments, businesses and the public all stand to gain when the course outlined in this report is completed.

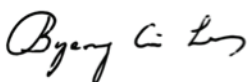
Please join us in lending support to the implementation of these recommendations.



**Kamlesh Bajaj**  
CEO, Data Security Council of India  
Founder Director of Computer Emergency  
Response Team (Cert-In)



**Maria Livanos Cattai**  
Fmr. Secretary-General, International  
Chamber of Commerce



**Byeong Gi Lee**  
Member, National Academy of Engineering  
of Korea (NAEK)  
Fmr. President, IEEE Communications Society  
Fmr. Commissioner, Korean Communications  
Commission, Ministry of Communications and IT



**Vartan Sarkissian**  
CEO, Knightsbridge Cybersystems  
Fmr. CEO, Rawrip






# PREFACE

**T**his paper presents three actionable recommendations for the private sector. If implemented, they will be decisive in realizing a breakthrough for much-needed measurement of the cybersecurity problem.

The simple truth is that no one knows how bad the cybersecurity problem really is. Yet, as our mutual friend Phil Reitinger has observed, the trends—increased complexity, increased connectivity and increased criticality—are all forces that will make the problem worse. Without measurements, most classical quality control principles cannot be applied. And that is the situation we are now in. We do not have even an order-of-magnitude estimate of some of the most basic aspects of the cybersecurity problem that can be validated. While there are many surveys conducted around the world that provide some insights, there is nothing that brings the available information together so that we can see the whole picture. Quality management principles and approaches of problem-solving have been essential throughout the world in raising the standard of living in countless ways. We need measurements so that we can understand our current situation, prioritize and calibrate investments and evaluate improvement performance. We are flying without instruments.

Our deep appreciation is expressed here for the subject matter experts who contributed to this work. Their maturity, expertise and “can do” attitude were essential to the formulation of this paper.

The next steps will require vision, initiative and leadership. The first steps may appear to be bold, but they need to be taken. We welcome volunteers from all sectors—ICT, energy, financial services, transportation, retail, medical and others. Anywhere computers are used, transactions made and records kept there are businesses that can contribute data and make our goal of measuring cybersecurity a reality.



**Karl Frederick Rauscher**  
Chief Technology Officer & Distinguished  
Fellow, EastWest Institute

Bell Labs Fellow

Chair Emeritus, IEEE Technical Committee on  
Communications Quality & Reliability (CQR)



**Erin Nealy Cox**  
Executive Managing Director, Stroz Friedberg

Former Assistant United States Attorney  
(Northern District of Texas)

Former Chief of Staff and Sr Counsel (Office of  
Legal Policy), U.S. Department of Justice

# 1. Executive Summary

“To measure is to know.”

- Lord Kelvin

Cybersecurity has fast risen to the top of priorities for governments and businesses around the world. Governments are spending billions of dollars, and the annual aggregate worldwide cost has been conjectured to reach the order of one trillion U.S. dollars.<sup>1</sup> Both the spending and overall costs are anticipated to rise annually, the former predicted on the order of 10 percent annually for the foreseeable future.

The breadth of concern spans the globe, confirmed by the interest of each of the Cyber40 countries that have joined the EastWest Institute’s Worldwide Cybersecurity Initiative.<sup>2</sup> However, despite all of this attention, energy and investment, the size of the cybersecurity problem is still a matter of speculation and debate. The main reason for this state of affairs: there are no widely accepted statistics at a global level on even the order of magnitude of the most basic dimensions of the problem such as the frequency and ex-

tent of cybersecurity compromise incidents.<sup>3</sup>

Other problems that receive as much attention are better understood in quantitative terms: the number of casualties from a war, the amount of national debt or the volume of oil spilled from an accident. But the number of cybersecurity compromises has remained elusive. Insufficient aggregation of available data translates into a lack of capability to access the magnitude and impact of cybersecurity breaches and compromises on the public and private sectors.

There are good reasons for this lack of available data. Individually, companies usually have this information. However, a compromised company has a fiduciary responsibility to protect its reputation.<sup>4</sup> The information can result in a competitive disadvantage. Typical media coverage of existing cybersecurity compromises often includes alarming headlines. This plays into the ongoing narrative that we may be “walking on thin ice” and suggests that the company’s clients may suffer the negative consequences. Such reporting is seldom able to offer much context such as relative benchmarks for similar corporations to the one in question.<sup>5</sup> A key challenge for this endeavor is to be straightforward and effective in educating the public on the numbers when presented. Just as the single numbers of the Richter Magnitude Scale and Saffir-Simpson Hurri-

1 Gopal Ratnam & Tony Capaccio, “Cyber Security May Gain in Pentagon’s Budget Review, Lynn Says,” Bloomberg, 12 May 2011. <http://www.bloomberg.com/news/2011-05-12/cyber-security-may-gain-in-pentagon-s-budget-review-lynn-says.html>; “Official Reveals \$650M Cyber Security Spending Plans,” Government Computing, 26 April 2011. <http://central-government.governmentcomputing.com/news/2011/apr/26/650m-cyber-security-spending-plans-ian-mcghie>; The 2009 World Economic Forum was the platform for this statement by McAfee CEO Dave DeWalt; see “Unsecured Economies Report: Protecting Vital Information,” 2009.

[http://www.cerias.purdue.edu/assets/pdf/mfe\\_unsec\\_econ\\_pr\\_rpt\\_fnl\\_online\\_012109.pdf](http://www.cerias.purdue.edu/assets/pdf/mfe_unsec_econ_pr_rpt_fnl_online_012109.pdf). This number is disputed for its potential conflict of interest from its source since a shocking figure may promote desirable marketplace perception, but this is further to the points underpinning the motivation for this study and report.

2 See Table 2, Section 2.

3 An example measure of limited scope is the Information Security Breaches Survey, [http://www.pwc.co.uk/eng/publications/isbs\\_survey\\_2010.html](http://www.pwc.co.uk/eng/publications/isbs_survey_2010.html).

4 Key Observation No. 7, “Brand Protection Is a Responsibility,” Section 3, p.39.

5 Key Observation No. 9, “Media Expectations Are ‘Perfection’ by Default,” Section 3, p.38.

cane Wind Scale gauge the magnitude of the energy release in an earthquake, cybersecurity compromise measurements should be similarly meaningful and usable.

This paper presents three recommendations that, if implemented, can solve the current problem by breaking through the logjam of issues that prevent effective data collection, analysis and reporting. While these recommendations are primarily for the private sector, governments can benefit significantly from their implementation. The first recommendation provides guidance to establish a safe means for sensitive data to be collected, analyzed and used to provide meaningful statistics:

#### **RECOMMENDATION 1. Trusted Entity for Cybersecurity Statistics**

The private sector should establish a trusted environment for the aggregation of statistical data that can be used to support measurements of the cybersecurity problem on a worldwide basis.

The second recommendation seeks to obtain the representative sample data to be used by the established trusted entity. There is a call to private sector companies to voluntarily provide minimal statistical data about their performance.

#### **RECOMMENDATION 2. Voluntary Data Contributions**

Private sector companies should voluntarily provide statistical data to an established trusted entity that will use the

data to support the measurement of the cybersecurity problem.

The third recommendation fosters the development of a quantitative framework that will produce meaningful and reliable benchmarks for the broad range of stakeholders. There is a call to subject matter expert volunteers to develop a consensus approach to data analysis, representation and reporting.

#### **RECOMMENDATION 3. Bona Fide Benchmarks**

Qualified subject matter experts should collaborate to develop statistical methods for analyzing the voluntarily submitted data and for reporting benchmarks.

The remainder of this document is organized and prepared to help the reader understand the problem and the reasoning for the proposed approach. There is a keen awareness throughout of the need to demonstrate a compelling value proposition to potential participants, particularly those that would submit data voluntarily. The following sections highlight an analysis of the problem and discussion of the major issues related to it, including frequently asked questions (Introduction, Section 2); key observations from the analysis conducted (Key Observations, Section 3); the complete presentation of the three recommendations (Recommendations, Section 4); and a summary (Conclusion, Section 5).

Despite all of this attention, energy and investment, the size of the cybersecurity problem is still a matter of speculation and debate.

# 2. Introduction

“Whenever I run into a problem I can’t solve, I always make it bigger.”

- Dwight D. Eisenhower,  
34th President of the United States

Cybersecurity is a big problem for many companies—and an even bigger problem for global society as a whole since the already substantial costs for securing operations and assets in cyberspace are only expected to grow in both the short and long term. Among the core difficulties for individual companies that handle the cybersecurity problem on their own: how to figure out the degree to which the problem is growing from year to year and how to gauge whether their efforts are effective enough to protect themselves. Alone, individual companies can’t see the “big picture” to understand how they are doing relative to others. This is one of those problems that can be dealt with more effectively with cooperation among peer companies.

This section briefly reviews the history of EWI’s Cybersecurity Initiative; the objectives of the initiative and the report; the value proposition for participants; example output; the report’s scope; a gap analysis that considers existing initiatives; and frequently asked questions.

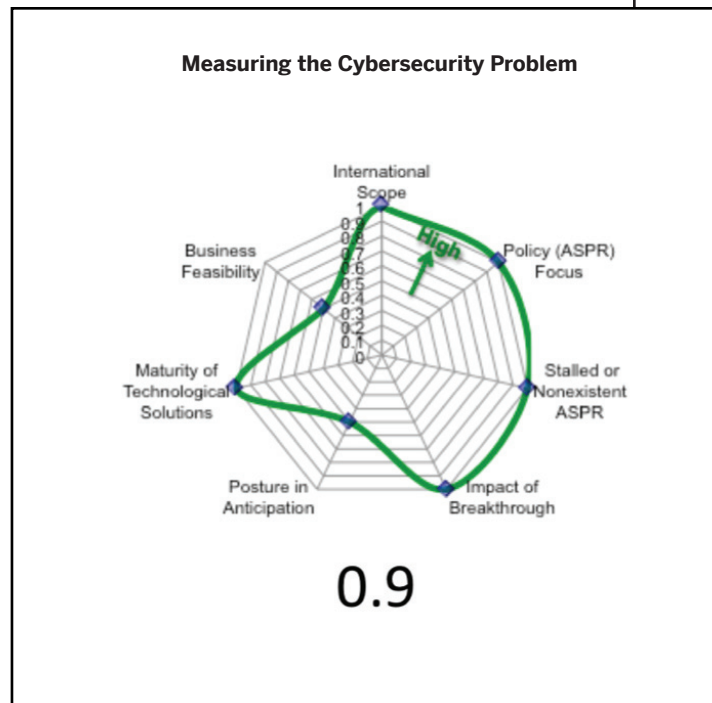
## 2.1 Brief History of the Initiative

In May 2010, the EastWest Institute, with the technical co-sponsorship of the IEEE, convened about 400 stakeholders and subject matter experts from more than 40 countries for the first Worldwide Cybersecurity Summit in Dallas.<sup>6</sup> Their focus was on solving critical international policy roadblocks that are major impediments to cyberspace safety, stability and security. Measuring the Cybersecurity Problem (MCP) was determined to be one of the top five areas from more than 25 priorities that were discussed in the summit’s working program.<sup>7</sup>

The MCP priority was based on a systematic evaluation of seven criteria that define the EastWest Institute’s distinct mission in cyberspace. Specifically, the area was evaluated based on the degrees to which: the matter is **international**; the problem is **policy-related**; progress is **stalled** or non-existent; a solution would bring **significant benefit**; the subject is being **neglected**; the needed **technologies are mature**; and **business**

<sup>6</sup> The First Worldwide Cybersecurity Summit – Protecting the Digital Economy,” Dallas, May 2010. <http://www.ewi.info/dallas>.

<sup>7</sup> Distinct from the more general discussion of ‘information sharing,’ the focus from the beginning that captured the high ranking was on the aspects of quantifiable information and the goal of measurement.



**Figure 1.**  
**Ranking Across EWI Criteria**

**support** is feasible. As seen in Figure 1, the MCP subject was rated as follows:

- High - for being international in scope<sup>8</sup>
- High - for being focused on Agreements, Standards, Policies and Regulations (ASPR)<sup>9</sup>
- High - for the ASPR being stalled or nonexistent<sup>10</sup>
- High - for the impact of a breakthrough<sup>11</sup>
- Medium - for posture in anticipation, i.e. the relative proactive to reactive mode
- High - for the maturity of technological solutions<sup>12</sup>

- Medium - for business feasibility

In determining the viability of a policy breakthrough for this issue, the authors initially focused on the two weaker scores (i.e. “medium”) for the “posture in anticipation” and “business feasibility.” The former refers to the fact that, on a spectrum that ranges from being reactive to being proactive, this subject is at the midpoint; and the latter, “business feasibility,” means that a sustainable business model is not straightforward but is feasible under the right conditions. Details on how the obstacles will be navigated are provided throughout this report, but are found most notably in the value proposition of Section 2.3 and the gap analysis of Section 2.5.

<sup>8</sup> In short, cybersecurity is a worldwide issue due to intense connectivity through transactions and ICT supply chain interdependencies. Additional elaboration is provided in Section 4, Question 6.

<sup>9</sup> The proposed solutions as outlined in this report are oriented around (a) voluntary agreements for the protection, aggregation and reporting of sensitive data, and (b) corporate policies whose deployment would precipitate the voluntary submission of minimal, scrubbed statistical data.

<sup>10</sup> Agreements and policies are described in the above note are insufficient at a global level.

<sup>11</sup> The better understanding achieved with measurements would be expected to directly impact the level and direction of spending, provide a grip for conducting improvement performance evaluations and otherwise serve as objective reference criteria for a wide range of decision making.

<sup>12</sup> There exist highly trusted information sharing environments, technologies and procedures.

The MCP subject was taken up in private consultations with stakeholders, worked on by an international team of subject matter experts and featured in rigorous working sessions in subsequent Worldwide Cybersecurity Summits (London in 2011 and New Delhi in 2012). The near complete draft of this report was supported at the New Delhi event.

## 2.2 Objectives

As with other parts of EWI’s Worldwide Cybersecurity Initiative, the goal for the MCP activities is to make the world a safer and better place. The specific objectives of this MCP

To date, there has not been a mechanism to trigger, or any vehicle to facilitate and sustain, the organization of willing parties to produce measurements of the cybersecurity problem. This report is intended to serve as that trigger.

activity are to provide two figures that do not presently exist: i) an order of magnitude measurement of the cybersecurity problem and ii) the rate of change of (i) over time.

To support this objective, this report presents three immediately actionable recommendations, which, if implemented, would break through the current situation where the cybersecurity problem is inadequately measured. The report seeks to compel the primary actors to create the essential initial momentum and to guide these actors through the necessary steps to establish a sustainable measurement capability.

## 2.3 Value Proposition for Participants

To date, there has not been a mechanism to trigger, or any vehicle to facilitate and sustain, the organization of willing parties to produce measurements of the cybersecurity problem. This report is intended to serve as that trigger. If successful, the resulting output will be a sustainable capability to measure the problem.

But who are the primary actors and how will they be motivated?

Given the expertise and ownership of the private sector, its leadership will be essential. A key part of this initiative is encouraging bold private sector leadership, or private-sector-led Private-Public Partnership (PPP).

The most difficult challenge will be motivating companies to participate. Thus, the value proposition for candidate participants must be strong.

There are substantial benefits to be realized when the cybersecurity problem can be measured on a global basis. The landscape of interests can be summarized as follows:

- **Government:** would benefit from **increased competence to assess the current situation**, see trends, and prioritize resources and fine-tune policy measures.
- **Industry Infrastructures** (ICT, energy, financial services, transportation, medical, retail, etc.): in addition to benefitting in the same ways as governments, would also be able to

understand how they **compare to the best performers and gain early insights into trends**.

- **Individual Companies:** in addition to benefitting from what is described above, would see value from:
  - » Having **benchmarks for average performance (all companies)**.
  - » Having **benchmarks for best-in-class performance (as a participant)**.
  - » Enhancing **due diligence** in the management of the cybersecurity problem so that board of directors and senior management can ascertain the problem (more information as a participant).
  - » Understanding the **return on investment** for expenditures made on cybersecurity<sup>13</sup> (more information as a participant).
  - » **Protecting brands** when a cybersecurity compromise does happen because of the media's general familiarity with performance norms for corporations<sup>14</sup> (all companies).
  - » Avoiding **costly and otherwise burdensome government regulations (all companies)**.
- **Individuals:** would also benefit from knowing reasonable benchmarks for the retailers, banks and others that they entrust with their personal information.

Our examination of the "business feasibility" criterion indicates that there are existing models of voluntary data collection, analysis and reporting.<sup>15</sup> Subsequent analysis suggests that the conditions could be created that would make it acceptable for companies to voluntarily contribute limited quantifiable-type data on cybersecurity compromises to a trusted entity.

<sup>13</sup> Key Observation No. 4, "Countermeasure Evaluations Lack Rigor," Section 3, p.38.

<sup>14</sup> "Brand Protection Is a Responsibility," *supra* n 4; Media Expectations Are 'Perfection' by Default," *supra* n 5.

<sup>15</sup> Key Observation No. 10, "Trusted Information Sharing Precedents Have Been Set," Section 3, p.40.



## 2.4 Scope

In considering a solution to measuring the cybersecurity problem, there are seven major dimensions that need to be examined. These dimensions are in the general categories of governance, breadth and information:

- Governance-related
  - » Leading sector (private or public)
  - » Posture in supporting (voluntary or mandated)
- Breadth-related
  - » Geographic (international, regional, national or local)
  - » Infrastructures (all, multiple or single)
- Information-related
  - » Focus (incidents, threats, knowledge, advice, policy, outages or other specific concerns)
  - » Type (quantitative or qualitative)
  - » Objectives (measurement, notification, collaboration, protect infrastructure, response, prevent problems, promote business or other specific concerns)

The remaining discussion on scope briefly describes the options within these parameters. This discussion lends insights into the forging of the proposed solution in Section 4, Recommendations.

### 2.4.1 Leading Sector

The public or private sector can lead an initiative to measure the cybersecurity problem. There are numerous forums representing these two options, and some even attempt to combine them by sharing leadership between these two sectors.

The advantages of government-led forums are that (i) they can have authority to force behaviors (e.g., in the form of regulations or other mandates) and (ii) they have a natural funding stream in the form of taxes. A disadvantage of government-led forums is that they tend to be slower relative to private sector initiatives. The advantages of private sector-led forums are that (i) they can be faster and (ii) they do not force behaviors and thus require more rigorous development of compelling value propositions for participants. A

disadvantage is that creating the initial required momentum is often much more difficult. In the final analysis of advantages and disadvantages, private sector-led initiatives are preferred.

The solution proposed in this report calls for private sector leadership to create a trusted environment for both collecting statistics and generating reports to the public.<sup>16</sup>

### 2.4.2 Motivation of Participants

The motivation for key actors to participate in this initiative can be either internal or external. Internal motivation is that which produces voluntary action and is typically based on a value proposition that appeals to a core interest. Means of external motivation include government regulations or other mandates. As indicated immediately above in Section 2.4.1, the advantages of private sector, voluntary participation outweigh forced behaviors. The key is to provide the right motivation to participate.

### 2.4.3 Geographic

Initiatives to measure the cybersecurity problem can focus on small areas (localities, provinces, nations or regions), target larger regions or span the globe.<sup>17</sup>

Any measurement is more valuable than none. However, cyberspace is global, and therefore the dimension of this space suggests that the appropriate measure must include its real contour. The complexity, pervasiveness and size of cyberspace is readily apparent in the crisscrossing architecture of international locations utilized in a typical corporate cloud deployment, the number of countries a network operator may connect (198 for Vodafone), or the number of world-

<sup>16</sup> Recommendation No. 1, "Trusted Entity for Cybersecurity Statistics," Section 4.1, p.45; Recommendation No. 2, "Voluntary Data Contributions," Section 4.2, p.48; Recommendation No. 3, "Bona Fide Benchmarks," Section 4.3, p.51.

<sup>17</sup> It is noted here that some cybersecurity companies have measurements that cover their customer base, which could have considerable international reach; however, in the end such measurements are limited by their market share footprint and technology. Key Observation No. 2, "The Cybersecurity Problem Is Waiting to Be Reckoned," Section 3, p.36.

The solution proposed in this report calls for private sector leadership to create a trusted environment for both collecting statistics and generating reports to the public.

wide Facebook users (>1.1 billion).<sup>18</sup> Measurement attempts that lower their aim to a span that is less than the global contour are immediately handicapping their potential.<sup>19</sup> For these reasons the proposal submitted in this report is for a global contour.

#### 2.4.4 Infrastructures

There are a number of infrastructures that support societies around the world, such as communications, energy, transportation, government services, health care, food and water. The spectrum of infrastructures included in a measurement can be a single infrastructure, a subset that includes multiple infrastructures, or the entirety of the components.

The scope of this initiative is to be inclusive of all infrastructures. In doing so, it is understood that it may be necessary to maintain distinctions between the statistics of distinct sectors.

#### 2.4.5 Focus of Information

The information collected should be limited to that which directly supports the goal of measuring the cybersecurity problem. The primary ways to measure negative experiences are frequency and magnitude. Thus, the number of incidents and their magnitude seem to be the starting point for the information to be collected. Other forums that are gathered for purposes related to cybersecurity do include different types of information, such as perceived threats or other knowledge about malicious actors and advice on defending against these challenges.

#### 2.4.6 Type of Information

The basic types of collectable information are qualitative or quantitative. As noted immediately above in Section 2.4.5, the two primary measures are frequency of incidents and the magnitude of these incidents, both of which

<sup>18</sup> Vodafone advertisement on London's Heathrow Express trains. "'Union Jack' livery for Heathrow Express fleet," Rail Express, 9 May 2011. <http://www.railexpress.co.uk/news/union-jack-livery-for-heathrow-express-fleet>.

<sup>19</sup> For example, if a national measurement initiative for County A does not account for cybersecurity compromises happening outside of its jurisdiction in County B, where some its companies conduct data processing and storage, its measurement scope is misaligned from the start with the architecture of the domain it is seeking to measuring.

are quantities. Thus the proposal presented in this report is one that seeks quantifiable information.

Most existing forums that collaborate on cybersecurity issues deal in primarily qualitative information.

#### 2.4.7 Objectives of the Information

In this report, the purpose for collecting, aggregating and analyzing cybersecurity compromise incident and magnitude information is to measure. Other objectives of other forums include notification, such as for viruses; collaboration, for problem solving; infrastructure protection, for best practice development and sharing; emergency response, for crisis management (e.g., a distributed denial of service attack); problem prevention, for recommendation implementation or for promoting business or other specific interests.

Again, as discussed in Section 2.4.6, the distinction of the objective of this information gathering for measurement purposes distinguishes this initiative from others.

### 2.5 Gap Analysis

It follows from the scope, analysis and determinations presented in Sections 2.2 through 2.4, that the solution for measuring the cybersecurity problem is defined by specific criteria. The value proposition must be clear and compelling for key participants, and include the following criteria: (a) the private sector leads, (b) the motivation for submitting statistical information is voluntary, (c) the span is worldwide, (d) the breadth is inclusive of all key infrastructures, (e) the focus is on incident frequency and impact, (f) the type of information collected is quantitative and (g) the objectives for the collected information is measurement. These target criteria are presented in Table 1.

Throughout this study, others forums were reviewed to determine if an existing entity was poised (i.e. chartered and operating) to serve as a model for this kind of global measurement. Obviously, if one could be found, it would increase the speed for an implementable solution and could also reduce unnecessary redundancies. Unfortunately, no such entity could be found. A representative subset of the types of organizations considered in the gap analysis is provided in Table

The information collected should be limited to that which directly supports the goal of measuring the cybersecurity problem.



**Table 1. Target Criteria Defining the Solution Space**

	Governance-Related		Breadth-Related		Information-Related		
	Sector Leading	Motivation of Participants	Geographic	Infrastructures	Focus	Type	Objectives
Solution Space	private	voluntary	worldwide	full spectrum	incidents	quantitative	measurement

2.<sup>20</sup> As seen here, the typical focus areas are

information regarding threats, incidents and advice.<sup>21</sup>

20  
 BITS: The Technology Policy Division of the Financial Services Roundtable. <http://www.bitsinfo.org>.  
 CERTs: Computer Emergency Readiness (or Response) Teams, including both public and private sector managed entities.  
 CPNI: Centre for the Protection of National Infrastructure. <http://www.cpni.gov.uk>.  
 FCC CSRIC: Federal Communications Commission, the Communications Security, Reliability and Interoperability Council. Formerly NRIC, a federal advisory committee act (FACA) body chartered by the U.S. congress. <http://www.csric.org>.  
 DSC: Data Security Council of India NASSCOM. <http://www.dsci.in>.  
 EBITT: E-Business, IT and Telecoms Commission, of the International Chamber of Commerce (ICC). <http://www.iccwbo.org/policy/ebitt>.  
 ENISA: European Network and Information Security Agency. <http://www.enisa.europa.eu>.  
 FIRST: Forum of Incident Response and Security Teams. <http://www.first.org>.  
 FS-ISAC: Financial Services Information Sharing and Analysis Center. <http://www.fsisac.com>.  
 ICPC: International Cable Protection Committee. <http://www.iscpc.org>.  
 ISACs: Information Sharing and Analysis Centers. <http://www.isaccouncil.org>.  
 ISC: Internet Systems Consortium. <http://www.isc.org>.  
 MAAWG: Message Anti-Abuse Working Group. <http://www.maawg.org>.  
 NIAC: National Infrastructure Advisory Council. <http://www.dhs.gov/national-infrastructure-advisory-council>.  
 NRSC: Network Reliability Steering Committee of the Alliance for Telecommunications Industry Solutions (ATIS). <http://www.atis.org/nrsc>.  
 NSIE: Network Security Information Exchange of the U.S. President's National Security Telecommunications Advisory Committee (NSTAC). [http://www.ncs.gov/nstac/reports/fact\\_sheet/NSTAC\\_08.pdf](http://www.ncs.gov/nstac/reports/fact_sheet/NSTAC_08.pdf).  
 WARPs: Warning, Advice, and Reporting Points. <http://www.warp.gov.uk>.

### 2.5.1 Nonprofit and Government Organizations

A most basic observation of the subset of evaluated organizations included in Table 2 acknowledges that there are already considerable activities in the broad space of information sharing. In fact, over 100 active information-sharing bodies were considered.<sup>22</sup> These forums are valuable to their constituents as is evidenced by the thousands of participants involved in these proceedings. The value propositions for these forums relate to information exchange: those participating bring value by sharing insights not generally available in the public domain or in their individual companies and receive value as they are recipients of the same kinds of insights. Throughout this analysis, careful consideration is given to the charters and activities of existing organizations and initiatives.

21 Commercial entities are excluded from this table; however, their consideration is included in quantitative analysis later in this section.

22 For example, there are well over 100 CERTS and CSIRTs around the world, but only one entry here. For more information, see <http://www.cert.org/csirts/national/contact.html>; [www.first.org](http://www.first.org).

**Table 2. Gap Analysis of Existing Information Sharing Fora<sup>23</sup>**

	Governance-Related		Breadth-Related		Information-Related		
	Sector Leading	Motivation of Participants	Geographic	Infrastructures	Focus	Type	Objectives
Solution Space	private	voluntary	worldwide	full spectrum	incidents	quantitative	measurement
BITS	private	voluntary	U.S.	financial services	knowledge	qualitative	collaboration
Breach Notification	public	mandated	various governments	varies <sup>24</sup>	incidents	quantitative & qualitative	notification
CERTs	private or public	voluntary	national	full spectrum	threats	qualitative	alerts
CPNI	public	voluntary	U.K.	essential services	advice	qualitative	reduce vulnerability
FCC CSRIC	public	voluntary	U.S.	communications	threats, knowledge	qualitative	advice
DSCI	private	voluntary	India	began with IT, now expanding	surveys	qualitative	awareness
EBITT	private	voluntary	worldwide	full spectrum	policy	qualitative	promote business
ENISA	public	voluntary	EU	full spectrum	knowledge	qualitative	prevent problems
FIRST	private	voluntary	worldwide	ICT	incidents	qualitative	response coordination
FS-ISAC	private	voluntary	U.S.	financial services	threats	qualitative	prepare and respond
ICPC	private	voluntary	worldwide	GUCCI <sup>25</sup>	knowledge	quantitative & qualitative	protection, measurement
ISACs	private	voluntary	U.S.	multi-infrastructure	knowledge, threats	qualitative	awareness
ISC	industry <sup>26</sup>	voluntary	China	information and communications	knowledge & advice	quantitative & qualitative	policy
M3AAWG	private	voluntary	worldwide	information and communications	knowledge	qualitative	collaboration, improvement
NRSC	private	voluntary <sup>27</sup>	U.S.	communications	network outages	quantitative & qualitative	measurement, improvement
NSIE	public	voluntary	U.S.	communications	national security threats	qualitative	protection
Quest Forum	private	voluntary	worldwide	communications	quality	quantitative & qualitative	improvement
Spamhouse	private	voluntary	worldwide	unrestricted	spam messages	quantitative	track & fight spam
WARPS	private or public	voluntary	Europe	unrestricted	threats, incidents and solutions	qualitative	warn, advice and reporting

Attribute Relative to Solutions Space    Target    Outside

23 These assessments were made by the authors based on publicly available information in the organization charters and published reports, and in most cases, from direct consultations with their representatives.  
 24 E.g., health record banks in Arizona (S.B. 1596), any business in Hawaii (H.B. 678), government systems in Nevada (S.B. 82), telecommunications services in Vermont (H.B. 254). The first laws were enacted in 2002 by the state of California (becoming effective in 2003).  
 25 Global Undersea Communications Cable Infrastructure.  
 26 "Industry" is a more accurate term for Chinese companies than "private."  
 27 The NRSC analyzes both data that is mandated to be reported by the U.S. Federal Communications Commission (FCC) as well as data that it receives from voluntarily submissions of its members. The former is not accomplished by the NRSC, but the latter is. Thus the table indicates "voluntary."

## 2.5.2 Commercial Organizations

Continuing with the gap analysis, having reviewed noncommercial forums, we now shift to commercial entities engaged in quantifiable analyses that produce statistical output. For firms that provide security products and services, there is potential access to a very large pool of data for companies with significant market share.<sup>28</sup> These firms have strong core competencies in the subject matter and access to very early data that would be useful in early trend detection. Nevertheless, there are natural limits that present themselves regarding inherent biases in such information, usually related to the reason the organization has access to the information. For example, in order to make extrapolations beyond their customer base, companies must make assumptions about the performance of their competitors or companies that do not have any similar products or services.<sup>29</sup> In addition, as scholarly and objective as they could be, it is problematic for a commercial firm to serve as a neutral trusted hub for sensitive data collection, analysis and reporting. Because of their commercial status, they are seen as likely to try to influence market conditions, whether or not this perception is justified.

### 2.5.3 The Reality of the Gap Disposition

As seen from the representative examples presented in Table 2, there are a wide range of organizations with a diversity of purposes and characteristics. Yet none of these representative entities, or any of the other entities studied, was aligned with the complete set of target criteria for the solution space (i.e. Table 1). Therefore, the conclusion of the gap analysis is that no existing entity operates in the required solution space. The approach is unique in that it provides a complete set of parameters that define the solution space.

<sup>28</sup> The initiatives of commercial organizations such as software security and security services firms were studied. Report from the initiatives are readily accessible in the public domain, but are not named here to avoid criticism of specific initiatives that are most likely fulfilling their original intent, which is distinct from that of this report.

<sup>29</sup> "The Cybersecurity Problem Is Waiting to Be Reckoned," *supra* n 17.

## 2.5.4 Considerations for Going Forward with Measurement

The best assessments of the frequency and extent of cybersecurity compromises are incomplete. The basis for this conclusion consists of limitations in information access and information quality. First, there is obviously no single entity that has access to all of the data to make an accurate measurement. This would require knowledge of every cybersecurity compromise, or at least those above a certain threshold (e.g., more than 1,000 records affected). That leads us to organizations that have a subset of information and use it to extrapolate figures for the larger set. Section 2.5.2 summarizes the limited utility of such initiatives.

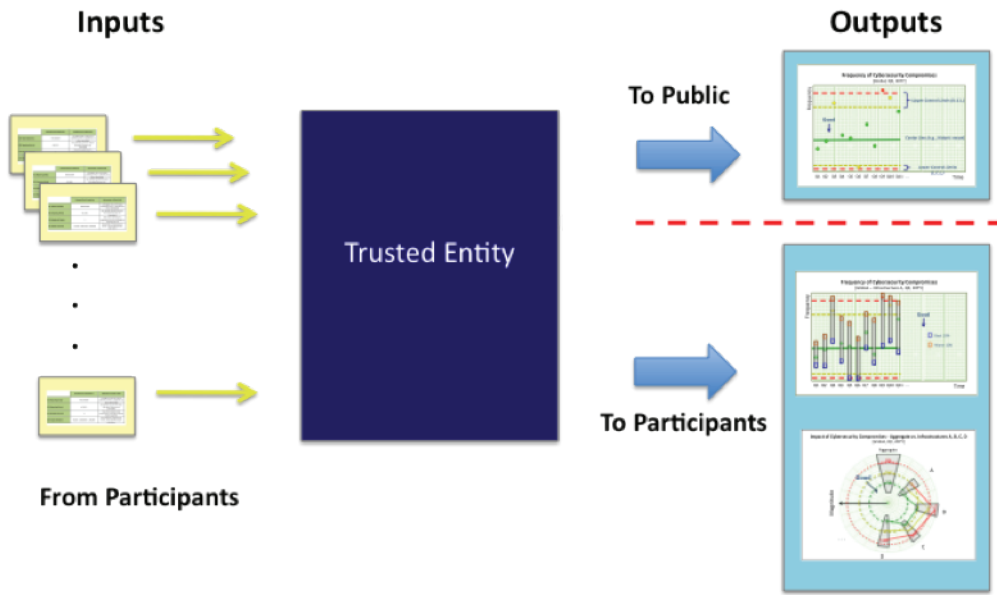
The nature of cybersecurity compromises is such that it is not always possible to detect every incident. But individual companies do have data on those detected compromises. This data is rarely disclosed because of legitimate commercial concerns. Companies such as financial institutions and retail stores have reputations and customers' interests to protect. In addition, they have a fiduciary responsibility to protect their brand. Competitive markets could make such information a marketplace weapon.

Information sharing communities have proven to be highly beneficial, when effectively implemented and nurtured.<sup>30</sup> However, existing communities are fragmented and vary widely in the level of robust exchange. More importantly, there are no worldwide initiatives that focus on collecting quantifiable data from participants for this purpose.

Companies are concerned about unfunded mandates that they may need to comply with. Forty-seven U.S. states and the European Community have moved forward with widely varying requirements for the reporting of data breaches. Some laws require an entity that owns or licenses personal data to report any breaches in the security of that data.

<sup>30</sup> Warning, Advice, and Reporting Points (WARPS), <http://www.warp.gov.uk>; Karl F. Rauscher, "Availability and Robustness of Electronic Communications Infrastructures (ARECI) Final Report," European Commission, March 2007, 102-105. <http://www.anacom.pt/render.jsp?contentId=483155>.

The nature of cybersecurity compromises is such that it is not always possible to detect every incident. But individual companies do have data on those detected compromises. This data is rarely disclosed because of legitimate commercial concerns.



**Figure 2.**  
**High Level**  
**Outline of**  
**Process**

## 2.6 Proposed Process

This report proposes a suite of recommendations that if implemented, could break through the existing obstacles to reaching the goal of an effective measurement. Once operational, the process begins with inputs from volunteering organizations and produces from these inputs two forms of outputs (Figure 2). The inputs and outputs would be agreed upon by the founding participating companies, and are discussed as envisioned in the following subsections.

### 2.6.1 Inputs

The input is simple quantitative statistics on the number of cybersecurity incidents and their magnitude. It is most likely that not all incidents would be reported, but only those that meet a minimum threshold (Table 3). This is to avoid very low impact events from being included, which may skew the more significant, broader statistics. Additional discussion will be needed on this issue among the founding members.

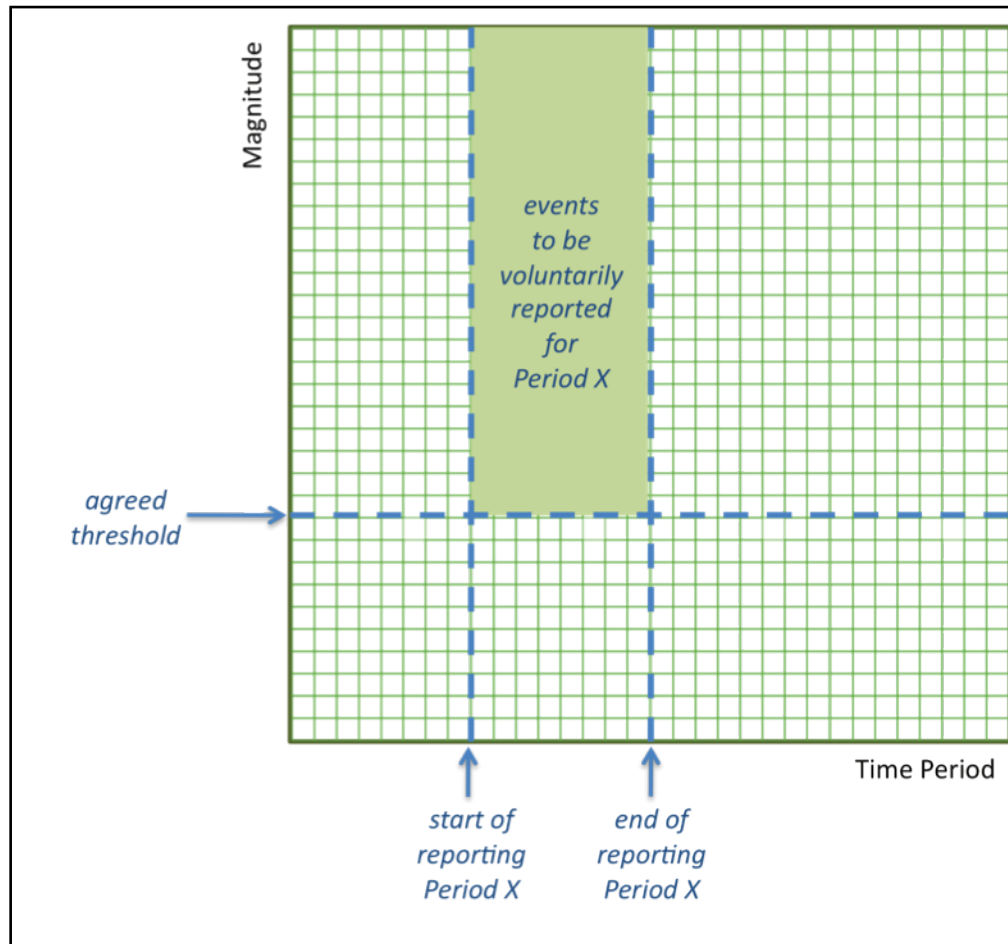
The incidents to be reported would also be associated with a specific time window, such as annual quarters (Figure 3).

Table 4 presents an example of what the input may include: namely, a method of validating a reporting entity, reporting period, number of cybersecurity compromise events and the magnitude of the cybersecurity compromise events. Optionally, the inputs may include indications of which infrastructure the data is associated with and what the cause type may be for each incident; both are included for statistical analysis and presentation only.

As this initiative is led by a volunteer private sector effort, the participating companies are expected to determine the operating practices and procedures. Table 4 represents the suggested minimal statistical and other essential information for the initial discussion by the founding member companies. The first two fields (A and B) are organizational, i.e. they enable the data to be validated and then aggregated. The middle two fields (C and D)

**Table 3. Example Criteria for Event Inclusion in Voluntary Reporting**

Criterion: An event is included if it:	... affects a minimal number of customers	... occurs during a specific window of time
Example	> 1,000	4Q 2013



**Figure 3. Diagram of Qualified Events for Voluntary Reporting**

are the core quantitative inputs and are where the real value lies. There are two major dimensions to measurement: frequency and magnitude of events. The final two fields (E and F) are optional but considered highly beneficial for getting the most value and insight. Founding members may also consider collecting other data—for instance, geographical location and company or market size. However, these could be included during a company's initial registration. Some of these inputs can be useful for normalization calculations. The policy and practice decisions related to the collection of any optional data will be made by the founding members and will add significant value that does not compromise the protection of those participating companies.

### 2.6.2 Outputs

There are two categories of outputs envisioned for this process. The first is a service to the public, as a community of stakeholders for the stability of cyberspace and will be provided in the form of a periodically (e.g., quarterly) published report with statistical averages over time. One possible methodological

framework for presenting the aggregate statistics is Statistical Process Control (SPC). Since its development by Bell Labs in the 1920s, SPC has had a dramatic, transformational role in improving the quality of countless products and services across many sectors around the world. The statistics of this periodic report may be for the aggregate of all sources or may be presented additionally on an infrastructure-level basis. Figure 4 provides an example of how this data may be presented. Decisions regarding optional infrastructure-level statistics will be made by the founding and participating companies and will consider such factors as the number of data points for a given category. In this example chart, the upper and lower control limits provide thresholds that indicate statistical significance, i.e. more significant variation when the thresholds are crossed and therefore a possible statistical trend.

The second output is part of the value proposition for participating companies in the form of additional insights on the statistical distribution of the data that provide benchmarks such as best-in-class performance levels for

**Table 4. Example of Voluntarily Reported Statistical Data**

	Example Data Population	Explanation of Data Field
<b>(A) Reporting Entity</b>	7,001,003,009	a changing code confirming a submitting entity is validated, but never identifiable
<b>(B) Reporting Period</b>	4Q 2013	the calendar quarter for which the report statistics are associated
<b>(C) Number of Events</b>	3	how many cybersecurity compromises occurred during the reporting period
<b>(D) Impact of Events</b>	55,000; 6,000,000; 1,000,000	the number of customers (or clients, records) affected per each event
<b>Optional fields</b>		
<b>(E) Industry Sector</b>	transportation	used to categorize data inputs, enabling sector-specific benchmarks
<b>(F) Compromise Type (frequency)</b>	X (1), Y (2)	used to categorize event types as determined by the submitting source

a given industry. The vehicle for distributing this information will account for the need to protect this confidential information. Figures 4 and 5 depict examples of how a statistical distribution for a given infrastructure and statistical distributions for infrastructure comparisons may be provided to participating companies. It is envisioned that the former would be made public, while the latter would be made available to the participating companies as part of the value proposition motivating their participation. Such a chart would enable a company to gain insights as to how it is performing relative to peers.

Another example of data that would be provided exclusively to participating companies is shown in Figure 6. While Figure 5 is a frequency distribution, Figure 6 is a magnitude distribution.

## 2.7 Frequently Asked Questions

The following questions have come up often during the discussions on measuring the cybersecurity problem and in developing the guidance presented in this report.

### 1. Q: What is the purpose of your work?

A: To provide a reasonably accurate method to measure the worldwide cybersecurity problem.

### 2. Q: If you are successful, who will benefit?

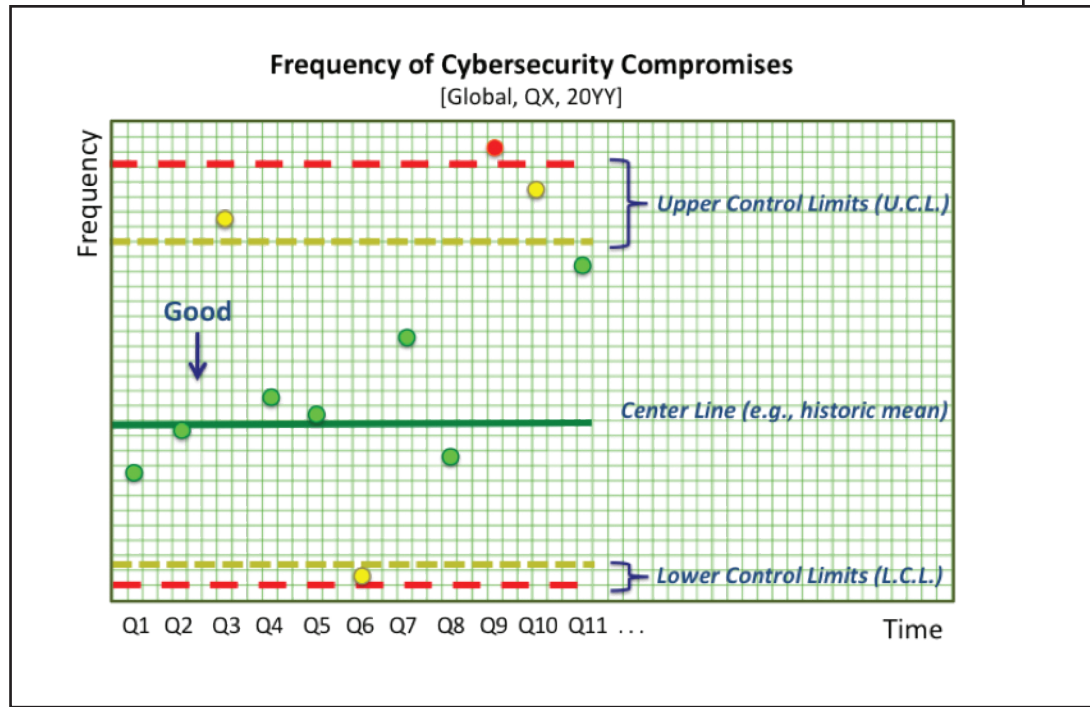
A: Governments, businesses, academia and private individuals stand to benefit significantly from the effective implementation of these recommendations.

Governments would better understand the extremely serious nature of today's cybersecurity risks. As statistics are collected, greater insights will be available. This information could enable the objective evaluation of the needs of future funding and priorities for available strategies for continued improvements.

Businesses could glean similar insights, including benchmarks for performance. Researchers would be better able to apply their resources to solving the most important problems.

Private citizens could gain a better understanding of the seriousness of the problem.





**Figure 4. Example SPC Frequency Chart for Public Reporting**

They could also begin to have an appreciation for what is a reasonable, or best-in-class, expectation for the companies they do business with.

**3. Q: Isn't this already being done?**

A: No.<sup>31</sup> There are a growing number of information sharing groups and professional networks that deal with cybersecurity issues. However, none of them as currently structured and operated provides a measurement of the worldwide cybersecurity problem. The distinction of this breakthrough approach from existing forums is that it is (a) worldwide, (b) voluntary, (c) private sector-led and (d) focuses solely on quantifiable data.

A gap analysis is provided in Table 2 of Section 2.5.

**4. Q: What are the currently best available measurements of the cybersecurity problem?**

A: Available quantitative insights fall into three categories—cost, loss and perspective. The first category is preventative in intent.<sup>32</sup> Known quantities include expenditures for

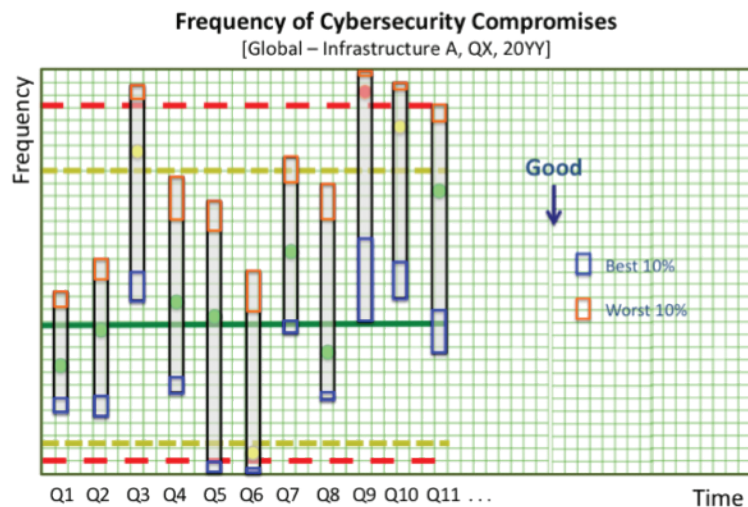
cybersecurity hardware, software, services and research. Many businesses and governments have some level of detail for their budgets for cybersecurity programs. However, there is also a huge hidden cost that is difficult to capture.

A second category is loss, which is also a cost but as opposed to being preventative, it is categorized as absorbed damages. Components for the “cost of poor security” may include lost business and market share, legal suits, brand dilution, augmented need for customer service, stolen intellectual property and opportunity costs.

A third category is measurement associated with a particular company’s perspective or footprint. Cybersecurity and other firms that have a considerable footprint have offered insights. However, this data is limited by their market share, the effectiveness of their products and services in detecting cybersecurity compromises and their ability to use particular data sets.

What is missing is basic performance type measurement, i.e. incident frequency counts and some sense of the magnitude of the impact. At their individual levels, companies see the number of incidents but they are not aggregated for understandable reasons, up to now.

<sup>31</sup> See Appendix A, Gap Analysis.  
<sup>32</sup> One example is a report by the Center for Strategic International Studies (CSIS) entitled: *The Economic Impact of Cybercrime and Cyber Espionage* (2013), <http://csis.org/publication/economic-impact-cybercrime-and-cyber-espionage>.



**Figure 5. Example of Statistical Distribution of Frequency for a Specific Infrastructure**

**5. Q: Why are you doing this at a global level?**

A: Cyberspace is global. Worldwide statistics are needed to measure the space. Cyberspace has no defined borders. Today, multinational companies are inseparable parts of business and society. Their transactions and critical supply chains routinely crisscross the globe.

**6. Q: Will companies ever share this sensitive information?**

A: It is important to keep in mind that with the proposed approach a company's statistical information is not shared with competitors or any other company or government or media outlet. It is only provided to the trusted entity. There are precedents for companies contributing very sensitive operational information for the purpose of supporting industry-level statistical measurements.<sup>33</sup>

Companies are also motivated to avoid regulations in this area. If a voluntary means were in place to accomplish a similar objective,

<sup>33</sup> The ATIS Network Reliability Steering Committee (NRSC) has facilitated the sharing of network outage data among wireline and wireless network operators and service providers for nearly 20 years. Such reliability data is very sensitive given the very competitive nature of this industry in the U.S. The collected data is protected throughout the processes and aggregate statistics calculated that then allow for the industry's identification of trends and benchmarks. Network Reliability Steering Committee, <http://www.atis.org/nrsc>.

then mandated behaviors are far less likely because much of the argument for regulation would be removed as the data would be there already.

**7. Q: Have any companies offered to contribute their cybersecurity compromise data?**

A: Yes. The conditions were most frequently expressed this way: (a) that the trusted environment and procedures can protect their reputations, and (b) that the time and resources associated with supporting the process is minimal.

Companies look at this proposal in a very straightforward manner where the value of participation must exceed the cost of participation. A number of companies are attracted to the idea of becoming a leader that helps found and shape such a trusted entity.

**8. Q: How will having a benchmark be helpful?**

A: Benchmarks establish existing levels of performance, as well as best-in-class performance. Such measurement references will enable companies and consumers to understand what is typical and, more importantly, what is possible. The current expectation held by the media for security performance for many companies is perfection, but this is



not realistic.<sup>34</sup> On the other hand, for some companies performance expectations are very vague and relatively low.

**9. Q: What are the required commitments to implement the recommendations?**

A: The required commitments for effectively implementing the guidance of this report are included in the presentation of each of the three recommendations (Section 4).

**10. Q: How much will it cost?<sup>35</sup>**

A: There are three components to the cost of operating this capability.

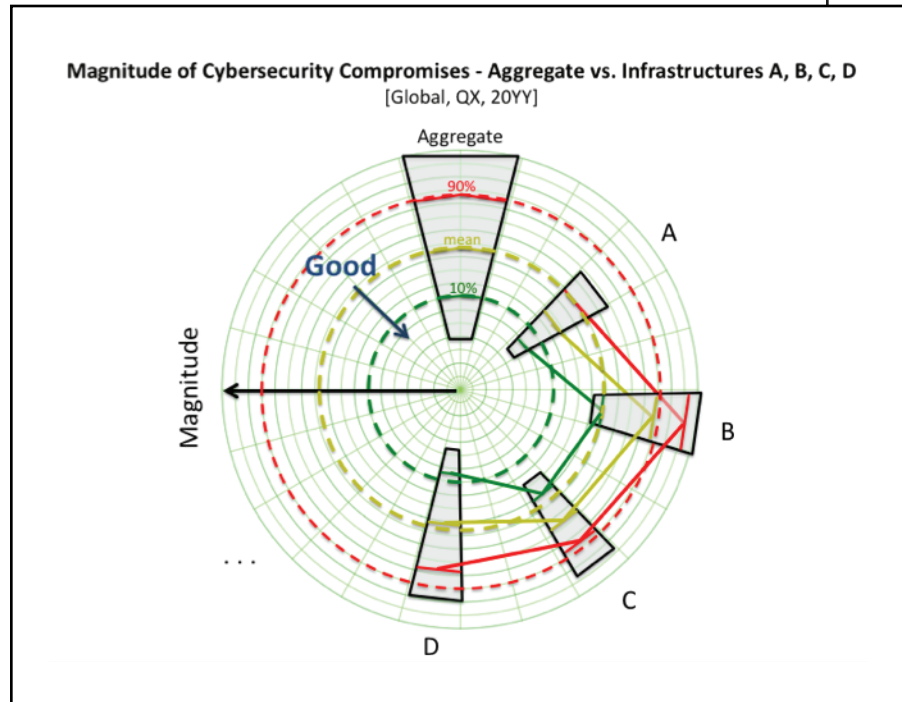
The best estimates depend on assumptions about several factors such as the frequency of reporting intervals and frequency and location of meetings of the participants. Based on existing models and the assumptions about the statistical nature of the data, the initial structure of the trusted entity would be smaller than the typical non-government organizations that most companies have affiliations with and for which they pay membership dues.<sup>36</sup>

First, there is the cost of information collection by participating companies. Since they are most likely already tracking cybersecurity compromises, the actual capture and analysis of the data is already taking place. Depending on the implementation, the anticipated ongoing effort would range from 10 to 100 hours per year for most companies for a quarterly reporting interval along with quarterly virtual meetings.

<sup>34</sup> Even ultra-high reliable systems cannot be said to be always on. The most reliable systems in the ICT industry have uptimes at best of 99.9999% (less than 30 seconds of downtime per system per year) or rarely, 99.99999% (3 seconds). More typical systems like common computers or handheld devices often have downtimes on the order of hours or more (~99.9%).

<sup>35</sup> Given the advantages outlined throughout, a reasonable question to consider is *“How much will it cost to not do this?”*

<sup>36</sup> E.g., Poisson distribution: Relatively infrequent incidents, suggesting that longer reporting intervals are appropriate. Thus the envisioned monthly reporting intervals provide some definition of the amount of times that data must be processed, i.e. not daily.



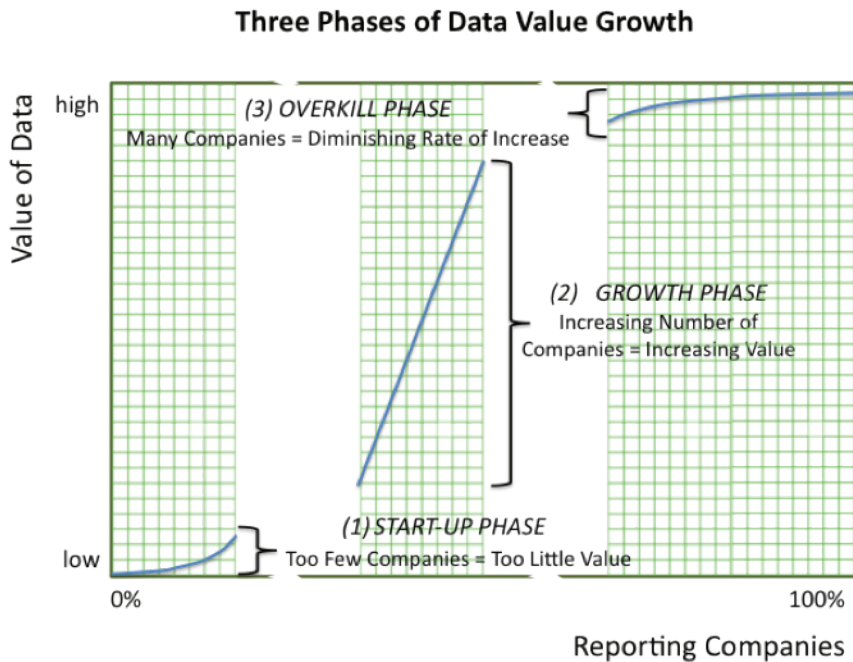
**Figure 6. Example of Statistical Distribution Comparisons of Magnitude across Infrastructures**

This excludes initial training and orientation.<sup>37</sup> It does not include initial internal discussions as to whether to participate or discussions about how to benefit from the insights gleaned from comparing benchmarks, such as average and best-in-class performance. Participating companies would absorb this cost.

Second, there are the actual facilities of the trusted entity. These costs include databases, computers, secure physical facility, possible back-up location and other related expenditures. It is projected that this cost initially would be in the order of magnitude range of \$1 million to 10 million annually. This projection represents an early stage implementation; the expected increase in the number of participating companies would require more customized build out.

Third, there are ongoing operational costs. The core competencies needed to support this will include statistical analysis, technical writing and program management. It is anticipated that neither of these functions would require an initial full-time staff. However, this demand would grow as participation and

<sup>37</sup> For those companies that further volunteer to be involved in the oversight of the trusted entity, additional costs would be incurred. These would be similar to the activities of other industry for the companies are most likely currently engaged in. Expectations for this cost at the upper levels of involvement (i.e. leadership) are anticipated to be on the order of a tenth of a senior management level per year.



**Figure 7. Three Phases of Data Value Growth**

thus the volume of statistics and the number of interfaces increases. It is projected that this cost initially would be in the range of \$1 to 10 million annually.

Participant-elected members would provide internationally representative governance oversight of the trusted entity operation. Participating companies would share the cost.

**11. Q: What specific metrics are being proposed?**

A: There are a considerable number of possibilities. This report deliberately avoids specifying what metrics should be used, though examples are presented in Section 2.6.

During the working meetings, the following points resonated among the participants:

- (a) A frequency and a magnitude measure should be considered;
- (b) A threshold (i.e., compromises affecting more than 1,000 records or 10 percent of customer base) may be needed to make the data collection more manageable;
- (c) Consideration should be given to dividing the data into categories based on industry (i.e., retail stores, transaction services, transportation).

**12. Q: How many contributing companies would be needed to make this successful?**

A: There are two constraints for this answer.

On the lower end, the number of participating companies must be large enough to prevent the identification of a particular company and to reflect the statistical variation within the industry. In the present situation, a relatively low number of participating companies could provide a breakthrough in value with their aggregate statistics, given the existing relative benchmarks. Thus, it is submitted here that the number of companies be on the order of 10 to 100 for the initial phase of implementation. Once the data of 10 companies, and then 100 companies, is aggregated together, the statistical significance of the combined data begins to have a weight not found elsewhere. Consideration must also be given to the size of the companies and their global representation.

On the upper end, the number of participating companies has limited additional return in value once it transitions from an estimate to a more precise measurement. This is quite acceptable as the objective here is to provide a high confidence order of magnitude estimate of the problem. As shown in Figure 7, the increasing value for a growing number of participants reflects a typical "S-Curve" relationship, where the initial value is low, followed by a sharp increase in returned value, which is concluded with a limited return. The order

of magnitude where this final phase begins is more difficult to suggest with the analysis so far.

**13. Q: Is there a preference for the creation of a new organization to serve as the trusted entity, or is it acceptable for an existing organization to adjust its charter to support this need?**

A: There is no preference between these two paths. What is important is that the trusted entity be able to gain the confidence of the candidate companies that would volunteer to provide the needed statistical information.

**14. Q: What are the next steps to make this happen?**

A: Suggested next steps are provided in the presentation of each of the three recommendations (Section 4).

**15. Q: How will the voluntarily submitted data be protected?**

A: The protection of the submitted data is at the very core of the success of this initiative. Since the founding participants will agree to the exact procedures and practices to be implemented, it is inappropriate to detail them here. It is worth noting that there are at least three key aspects of the discussion of protecting the voluntarily submitted data:

**A. Voluntarily Participating Company Protection**

The overarching concern focuses on ensuring that no embarrassment can come to an organization voluntarily submitting data to the trusted entity.

**B. Stand Alone Data Records**

Processes and procedures need to be designed to prevent any individual data record from being associated with a particular company. There are several ways in which this can be accomplished.

**C. Data in the Aggregate**

The envisioned aggregated data presentation will ensure enough contributing entities so that no individual company can be singled out. (See Figure 4).

**16. Q: Are there any precedents for this proposed model?**

A: Yes. Two examples are sufficient to document a critical precedent: the sharing of meaningful, sensitive data on an international scale.

The first example is the Network Reliability Steering Committee (NRSC). The NRSC is a communications industry-led initiative that has, for over 20 years, facilitated the aggregation of sensitive quantitative statistical data on the health of the U.S. networks.<sup>38</sup> The shared meaningful, sensitive quantitative data is on communications network service outage events. The data is shared voluntarily for special studies that identify statistically significant trends.<sup>39</sup> It is interesting to note that, based on the total advertising spent on the U.S. wireless industry, the NRSC model has achieved cooperation within one of the most fiercely competitive industries in the world. Moreover, the reliability dimension of service is precisely one of the most competitive aspects for wireless service. Thus a precedent has been set for collecting the kind of information that is proposed in this report on a cooperative basis.

The second example serves as a precedent for the international scale and is more recent in development. The International Cable Protection Committee (ICPC) is a UK-based nonprofit.<sup>40</sup> The ICPC set a precedent for international data aggregation in 2012 when it implemented a recommendation from from the IEEE-EWI *Reliability of Global Undersea Communications Cable Infrastructure* (ROGUCCI) Report. This report called for the undersea cable industry to accelerate new collaboration among competing companies in order to collect data in a trusted environment and then provide performance statistics to stakeholders who must manage their operational risk with reliance on international connectivity.<sup>41</sup>

<sup>38</sup> The NRSC operates under the auspices of the Alliance for Industry Solutions (ATIS) based in Washington, D.C. <http://www.atis.org>.

<sup>39</sup> While some of the NRSC's data analyses are associated with the U.S. Federal Communications Commission (FCC) mandatory outage reporting requirements, its most insightful and useful studies are consistently based on its special studies undertaken and led by participating companies from industry and supported by voluntarily submitted outage data that is protected by ATIS and its designated contractors.

<sup>40</sup> International Cable Protection Committee. <http://www.iscpc.org>.

<sup>41</sup> Karl F. Rauscher, "Reliability of Global Undersea Communications Cable Infrastructure," ROGUCCI, IEEE, 2010. [http://www.ieee-rogucci.org/files/The ROGUCCI Report.pdf](http://www.ieee-rogucci.org/files/The%20ROGUCCI%20Report.pdf).

The protection of the submitted data is at the very core of the success of this initiative.

# 3. Key Observations

“People’s minds are changed through observation and not through argument.”

- Will Rogers

The following 12 key observations are central reference points for appreciating the need for measuring the cybersecurity problem and for understanding how best to break through the present impasse. These key observations are factors that shaped each of the three recommendations presented in Section 4.

## 1. The Cybersecurity Problem Is Ill-Managed

Despite massive public and private sector expenditures to date, the cybersecurity problem is not well understood from a management perspective, either by governments or industries. Effective management is prevented because necessary quantification of the cybersecurity problem has been elusive until now. Without such basic measurements as benchmarks and other comparison points, quality improvement efforts are problematic at a fundamental level. As one chief risk officer from a top global financial services firm summed it up: “My board has no way of knowing what we should be spending on cybersecurity. I could ask for 10 times as much or half of my budget. They give me what I ask for.”

## 2. The Cybersecurity Problem Is Waiting to Be Reckoned

The problem of cybersecurity has not yet been calculated or counted with confidence. Indeed, independent estimates of the cybersecurity problem do not agree on even the order of magnitude (i.e., 10<sup>2</sup>, 10<sup>3</sup> or 10<sup>6</sup> events/year).<sup>42</sup> Figure 8 depicts this first missing

<sup>42</sup> Magnitude: i.e. the frequency of events or number of records affected.

measurement as Quantity 1 (Q1).

Those measurements that have been published are admittedly for an unrepresentative portion of the problem. That is, corporations providing numbers are limited by both the “footprint” of their customer base and also biased by the detection capabilities of the specific technology they deploy.<sup>43</sup>

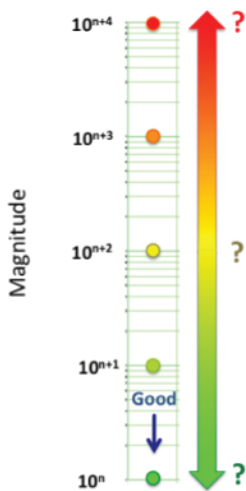
## 3. The Cybersecurity Problem’s Dynamics Are Unmeasured

Without measurements, the changing nature of the problem’s magnitude is unknown. These insights are critical for knowing if the current conditions represent a positive, negative or neutral trend and thus whether the present set of countermeasures are effective or whether a course-correction is needed. Figure 9 depicts this second missing measurement as Quantity 2 (Q2). Once Q1 is established, the dynamics are the next critical concern, i.e. the Q2 positive (a trend indicating the situation is getting worse), negative (a trend indicating the situation is getting better), or zero (neither an improvement nor decline).

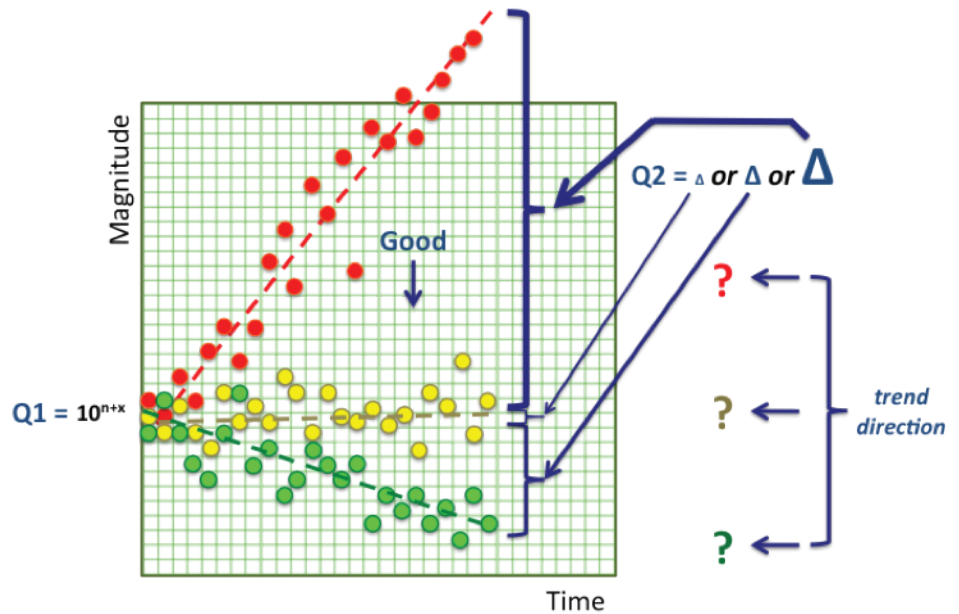
## 4. Countermeasure Evaluations Lack Rigor

Governments, critical infrastructures and enterprises throughout the world are “flying without instruments.” Without effective measurements of the problem over time, there is insufficient feedback to understand the ef-

<sup>43</sup> Section 2.5.2, “Commercial Entities,” p.22.



**Figure 8. Quantity 1 (Q1):  
The Problem's Order of  
Magnitude Is Unknown.**



**Figure 9. Quantity 2 (Q2):  
The Rate of Change Is Unknown.**

fectiveness, or lack of effectiveness, of the resources and methodologies being applied to solve the problem. This uncertainty about the present state simultaneously produces an uncertainty about the future, fueling the growing concern about the use of ICT itself.

## 5. The Cybersecurity Market Thrives Despite the Lack of Effective Measurements

Neither the lack of effective measurement nor the lack of effective management of the cybersecurity problem has prevented governments and enterprises from providing a continuing, and even growing, stream of funding for current approaches to cybersecurity. For well over a decade, the number of firms selling hardware, software and services to address the cybersecurity concerns has been growing, without clear accountability for effectiveness.

At first glance, these jobs may seem good for the economy, as they are high-tech and in an area of growth. However, it does not take long to realize that these expenditure compete with the efficiencies provided by new technologies. It is essential to get the cost

of cybersecurity under control by improving management of this issue.

## 6. Services and Applications Continue to Advance and Be Adopted

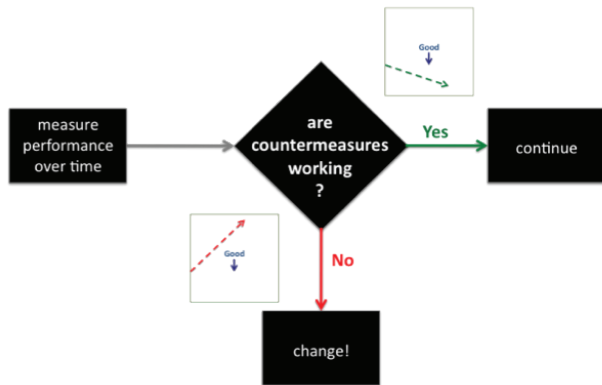
Despite the fact that the cybersecurity problem is unresolved and growing in disruptive potential, individuals, businesses and governments continue to move forward with the adoption of new services and applications, many of which further extend the degree to which they are reliant upon the security of cyberspace.<sup>44</sup>

## 7. Brand Protection Is a Responsibility

The management teams of corporations have a legitimate fiduciary responsibility to their owners and stakeholders to protect

<sup>44</sup> Cloud First was an policy instituted by the U.S. Federal Government's Office of Management and Budget that required agencies to identify 3 cloud initiatives. [http://www.gsa.gov/portal/content/190333?utm\\_source=FAS&utm\\_medium=print-radio&utm\\_term=cloud&utm\\_campaign=shortcuts](http://www.gsa.gov/portal/content/190333?utm_source=FAS&utm_medium=print-radio&utm_term=cloud&utm_campaign=shortcuts).





**Figure 10. Essential Role of Countermeasure Evaluation.**

their organizations' reputation and brand. For this reason, companies are vigilant when it comes to protecting information about compromises to the security of their ICT assets.

Other reasons for non-disclosure include protecting the reputation and brands of their customers in turn, not tipping off the malicious parties that they are aware of their activities and not rewarding those who may be doing so for notoriety.

## 8. Information Sharing Forums Have Come Short of Quantification

Meetings and platforms for sharing information have provided many benefits for those working in the field.<sup>45</sup> Such forums provide a trusted venue where sensitive issues can be discussed, new trends observed and best practices for addressing known problems shared.

There are distinctions between information sharing to support cause analysis and develop countermeasures and purely quantitative analyses. Also, the participants in these groups tend to be problem solvers at the tactical level, whereas managing the cybersecurity problem at an industry or global level is beyond one individual's responsibilities. Such extensions in scope toward quantification could also be viewed as decreasing the immediate and familiar value from the particular forum's established agenda.

## 9. Media Coverage Lacks Accurate Data

Currently, media reports of cybersecurity breaches are presented without the help of an accurate mathematical context to illustrate the frequency of the type of event being reported. Trustworthy benchmarks would be highly valuable both for those doing the reporting and the audience trying to understand the significance of the breach and the relative competence and diligence of the company affected. Benchmarks would serve a key role in setting expectations for reasonable performance with regard to security compromise frequency.

The frequency of most security compromises could be ameliorated with additional investment in the product or service development lifecycle. In many situations, security enthusiasts are capable of providing higher levels of security, but at a development and maintenance cost that would either make products and services less desirable for the current customer base, or require customers to take on the burden of performing additional procedures, or both. A part of the story, too often untold in media reports, is that the level of security is arrived at in part by competitive market pressures that reflect perceived market interests in security. Measurements can bring much needed clarity for the media, the public and the companies involved.

<sup>45</sup> Section 2.5, Gap Analysis, p.19-26.

## 10. Trusted Information Sharing Precedents Have Been Set

There are precedents for the establishment and ongoing operation of successful trusted information sharing environments that serve in providing quantitative industry performance statistics. This is significant and encouraging, as the creation of such an entity is essential to the core concept proposed in this report.<sup>46</sup>

The first example demonstrates how this can be done among fierce competitors. Based on advertising dollars spent over the past decade, it has been argued that the wireless service providers in the United States are one of the most competitive industries in the world. Thus the first example of the 20 year-old Network Reliability Steering Committee (NRSC), is significant in that it has served as a trusted entity for the collection of voluntary submitted, sensitive network outage data.<sup>47</sup>

The second example complements the first in that it is international and more recently established. The International Cable Protection Committee (ICPC), with its constituents, has facilitated the collection of sensitive cable-fault data by a trusted entity with the goal of producing statistics that can be useful to stakeholders of international connectivity, such as financial services firms and many others. While progress has been made with most of the world's regional maintenance agreements who have participated, there are still gaps [in Asia] and with some private agreements that will require confidence-building measures to allow the data to be released in a transparent and useful manner for governments and stakeholders.<sup>48</sup>

<sup>46</sup> Frequently Asked Question 17, Section 2.7, p.33.

<sup>47</sup> The NRSC is operated under the auspices of the Alliance for Telecommunications Industry Solutions (ATIS). <http://www.atis.org>.

<sup>48</sup> The ICPC accomplished this breakthrough to meet the needs of its stakeholders and was following the guidance of Recommendation No. 7, *Measurement for Stakeholder Due Diligence*, of the 2010 Reliability of Global Undersea Communications Cable Infrastructure (ROGUCCI) Report. The ICPC's initial aggregation of industry cable faults was managed on a per ocean level.

## 11. Educated Boards and Senior Management Are Indispensable for Quality Improvement

Quality improvement legend Joseph Juran has observed that "...every successful quality revolution has included the participation of upper management. We know of no exceptions." Effectively engaging the senior leadership of governments and companies is essential. When new objective data is available, they will be equipped with new insights into trends regarding the cybersecurity problem, which in turn will trigger further insights into the effectiveness of existing approaches to solving the problem. They will be called on to make decisions.

The combined parameters of measuring cybersecurity compromises fall into a category of statistics that deals with rare events occurring among a large number of possible opportunities. These sorts of statistics can be easily misunderstood because variations that are normal over time could be misinterpreted as a trend.<sup>49</sup> Therefore, these variations over time require some education in order to understand their significance, to avoid unnecessary actions when no trend is confirmed and to motivate action when a trend is confirmed.<sup>50</sup> Without a proper appreciation for the normal variation, misperceptions will multiply, unhelpful conclusions will be reached and resources squandered.

## 12. Measurement of the Cybersecurity Problem Is a Game Changer

The tangible benefits of understanding the cybersecurity problem in quantifiable dimensions can produce a watershed moment in cyber history. Measuring is an essential element of classical quality control principles that have transformed many other industries. But measuring is one area that has escaped the grasp of cyber industry stakeholders until now.

<sup>49</sup> For example, one event last year and four this year may, or may not, be a normal variation and thus may, or may not, be an indication of a trend.

<sup>50</sup> Figure 3, "Example SPC Frequency Chart for Public Reporting," p.24.

The tangible benefits of understanding the cybersecurity problem in quantifiable dimensions can produce a watershed moment in cyber history.

# 4. Recommendations

“It isn’t so much how busy you are but why you are busy. The bee is praised. The mosquito is swatted.”

- Roger Devlin

This report presents three recommendations that, if implemented, can provide much needed measurement for the order of magnitude of the cybersecurity problem. Such measurement is needed to make our shared cyberspace safer, more stable and more secure.<sup>51</sup>

These recommendations are for the private sector to voluntarily implement. No one is requiring any company to take action on these recommendations. This means that the momentum for this has to be generated organically from within the private sector. This will require vision, initiative and leadership.<sup>52</sup>

In developing and articulating these recommendations, a number of factors were considered:

- The business interests of the companies asked to contribute data.
- The competitive advantages and disadvantages that can be leveraged from cybersecurity compromise data.
- The availability of cybersecurity compromise data.

- The need to provide a strong value proposition to those companies that are candidates for contributing data.
- The essential attributes of existing, successful, trusted information sharing models.
- The certainty that the data being stored is beyond the reach of a government regulator.
- The charters of existing forums that may be possible hosts for this new function.
- The cost to establish a new trusted entity.
- The ongoing operational considerations for the trusted entity.
- The parameters that could change should the recommendations be implemented successfully and the number of participating companies grows (e.g., scalability).

Each recommendation is presented with essential decision-support information to foster its implementation. This information includes important background information, the required commitments, the benefits of implementation, the alternatives and their consequences, next steps and measures of success. For additional discussion of the recommendations, frequently asked questions are included in Section 2.

<sup>51</sup> Key Observation No. 12, “Measurement of the Cybersecurity Problem Is a Game Changer,” Section 3, p.40.

<sup>52</sup> Key Observation No. 11, “Educated Boards and Senior Management are Indispensable for Quality Improvement,” Section 3, p.39.



Table 5. Summary of Recommendations

Recommendation	Title	Primary Actor
1	<b>Trusted Entity for Cybersecurity Statistics</b>	<b>Private Sector<sup>53</sup></b>
2	<b>Voluntary Data Contributions</b>	<b>Private Sector Companies</b>
3	<b>Bona Fide Benchmarks</b>	<b>Individual Subject Matter Experts</b>

<sup>53</sup> This entity should have international status. Ideally, the entity will be a non-profit in order to maximize trust.

## 4.1 Trusted Entity for Cybersecurity Statistics

### Objective

The first recommendation provides guidance for the establishment of a safe means for sensitive data to be collected, analyzed and used to provide meaningful statistics.

### Background

Organizations are increasingly aware of cybersecurity compromises that affect them. However, this information is typically protected from public view for several reasons. For commercial enterprises, these reasons include protecting their organization's reputation and brand and also that of their customers, not tipping off the malicious parties that they are aware of their activities and not rewarding those who may be doing such for fame.<sup>54</sup>

Numerous existing industry forums serve a wide range of useful functions with regard to addressing the cybersecurity problem.<sup>55</sup> However no existing forum has all of the attributes essential to meet the current need for measurement of the problem. Specifically, an entity is needed with leadership that represents multiple sectors and where participation is volunteered pro-actively; where the scope is cross-sector and international; and where the information is quantitative and collected for the singular purpose of aggregate measurement.<sup>56</sup> Furthermore, the nature of information sharing to support cause-analysis toward the development of countermeasures and information aggregation for purely quantitative analyses and measurement is a quintessential difference between existing forums, and

<sup>54</sup> "Brand Protection Is a Responsibility" *supra* n 4.

<sup>55</sup> Appendix A, "Gap Analysis of Existing Fora."

<sup>56</sup> Key Observation No. 8, "Information Sharing Fora Have Come Short of Quantification," Section 3, p.38.

what is yet needed. For the former, partial, subjective and irregularly contributed information is quite useful and acceptable for the forum to be healthy and to create value; however, for the latter, while substantially less information is contributed, this information requires discipline, objectivity and consistency to produce trustworthy and reliable output statistics.

A trusted entity qualified to serve in the collection of sensitive cybersecurity compromises must, first of all, provide the necessary assurances that the interests of the entities voluntarily providing the information will be protected. When participating in this process, companies need confidence that their identity will not be linked with the quantifiable statistics they provide. Fortunately, there are precedents for this type of trusted environment that demonstrate the viability of collecting statistical data on cybersecurity compromises.<sup>57</sup>

### RECOMMENDATION 1.

**The private sector should establish a trusted environment for the aggregation of statistical data that can be used to support measurements of the cybersecurity problem on a worldwide basis.**

### Required Commitments

The effective implementation of this recommendation requires the following commitments from the private sector:

- The private sector must identify a suitable existing trusted entity or create a new one.

<sup>57</sup> "Trusted Information Sharing Precedents Have Been Set," *supra* n 15.

The private sector should establish a trusted environment for the aggregation of statistical data that can be used to support measurements of the cybersecurity problem on a worldwide basis.

- The private sector must develop and implement an appropriate governance structure for the trusted entity.
- The private sector must develop and implement a sustainable funding structure for the trusted entity.
- The trusted entity must protect the data that is entrusted to it.
- The trusted entity must protect the reputations of the companies providing data to it in strict confidence.

### Benefits

The principal value in implementing this recommendation is creating the opportunity for the safe collection of sensitive information by one entity. This aggregation in turn enables quantifiable measures of the cybersecurity problem, enhancing the ability to more accurately inform businesses, policy makers and the public of the present conditions and trends underway.

### Alternatives and Consequences

Alternatives to this approach include the following:

- Continue on the current path where the dimensions of the cybersecurity problem are unknown, with an increasing likelihood that there will be forced compliance with government mandates seeking to solve this problem.
- Defer to government to measure the problem and accept the need to comply with government mandated reporting requirements.

### Next Steps

Suggested next steps for implementing this recommendation include:

- 1-1.** Private sector companies volunteer to be leaders in forming a consortium of founders that will create the trusted entity.
- 1-2.** Founding members create the trusted entity, or adjust the charter of an existing suitable organization and develop the initial procedures for its operation.<sup>58 59</sup>
- 1-3.** The trusted entity, stakeholders and private sectors companies recruit additional companies to join the initiative.

### Measures of Success

The effective implementation of this recommendation can be confirmed with the following measures of success:

- A.** A trusted environment and entity is established.
- B.** Representative stakeholders are instrumental in the development of the environment, ensuring its attractiveness and acceptability for other stakeholders.

<sup>58</sup> Important issues to be worked out include: How will companies be protected? How is the information going to be managed from beginning to end? What kind of technology will be used? How is the process of supporting this affecting a company's business operations? How are you categorizing the data?

<sup>59</sup> This could take the form of validated anonymization.

## 4.2 Voluntary Data Contributions

### Objective

The second recommendation seeks to obtain the representative sample data to be used by the established trusted entity. Here there is a call to private sector companies to voluntarily provide minimal statistical data about the cybersecurity compromises they have experienced. A compelling value proposition is offered for candidate companies.

### Background

As the operations of private enterprises around the world are increasingly reliant upon ICT, these same companies are also increasingly aware of their profound exposure to cybersecurity threats, such as attempts to access sensitive client records.<sup>60</sup> In managing this predicament, companies can typically employ a range of protective measures, including those that employ special technologies and special services.<sup>61</sup> Companies can also track their own organization's experience with cybersecurity compromises over time. However these two elements, i.e. protection and internal measurements, form an incomplete approach and fall short of due diligence in managing the cybersecurity problem.<sup>62</sup>

In addition to protection and internal measurements, the management of this problem requires benchmarks in order to understand achievable and otherwise reasonable performance levels.<sup>63</sup> Companies should know how well their or-

ganization is performing relative to industry benchmarks. Moreover companies need insights into the dynamics of managing the problem on a wider scale in order to understand the trends for this critical area.<sup>64</sup> How does my organization's performance compare to trends on a larger scale? Is the trend of how the problem is being managed getting better or worse and at what rate?<sup>65</sup> Thus benchmarks and insights into the dynamics of the problem on a larger scale are basic and necessary elements of quality management programs that have been glaringly missing for far too long.<sup>66</sup> This recommendation seeks to correct this absence for companies, but requires the voluntary participation of a representative sample of them.

Companies are asked to voluntarily submit a small amount of specific statistical information at regular intervals (e.g., quarterly). The value proposition for these companies is (a) that they will be helping to solve a major global problem with escalating consequences for them, their customers and the world, (b) that, through the publication of statistical averages, they will help to bring much needed clarity in media conversations regarding reasonable expectations for companies (i.e. non-zero compromise performance is unrealistic) and (c) that they will get privileged access to nonpublic aspects of the analyzed data such as statistical distributions that will give them insights into trends and best-in-class performance levels for their industry segment.<sup>67 68</sup> An additional benefit offered to the early

<sup>60</sup> Key Observation No. 6, "Services and Applications Continue to Advance and Be Adopted," Section 3, p.38.

<sup>61</sup> Key Observation No. 5, "Cybersecurity Entering Thrives Despite the Missing Measurements," Section 3, p.37.

<sup>62</sup> Key Observation No. 1, "The Cybersecurity Problem is Ill-Managed," Section 3, p.35.

<sup>63</sup> "The Cybersecurity Problem Is Waiting to Be Reckoned," *supra* n 17.

<sup>64</sup> Key Observation No. 3, "The Cybersecurity Problem's Dynamics Are Unmeasured," Section 3, p.36.

<sup>65</sup> "Countermeasure Evaluations Lack Rigor," *supra* n 13.

<sup>66</sup> "Educated Boards and Senior Management Are Indispensable for Quality Improvement," *supra* n 52.

<sup>67</sup> "Measurement of the Cybersecurity Problem is a Game Changer," *supra* n 51.

<sup>68</sup> Media Expectations Are 'Perfection' by Default," *supra* n 5.

founders of the process is that they will have the opportunity to influence the shaping of this new cooperative framework.

**RECOMMENDATION 2.**

**Private-sector companies should voluntarily provide statistical data to an established trusted entity that will use the data to support the measurement of the cybersecurity problem.**

**Required Commitments**

The effective implementation of this recommendation requires the following commitments from the private sector:

- Private sector companies must cooperate with peers in order to establish protocols and formats for providing limited statistical information to the established trusted entity.
- Private sector companies must be willing to share minimal statistical data on cybersecurity compromises that they experience.
- Private sector companies must provide data within the agreed periodic intervals.

**Benefits**

The value of implementing this recommendation is that it begins the process of collecting critical data that can be used to provide quantifiable measures for cybersecurity. The value of cybersecurity compromise data can be greater when aggregated together and used to generate meaningful statistics.

**Alternatives and Consequences**

Alternatives to this approach include the following:

- An insufficient number of companies contribute data, reducing the statistical value of the data as it is not representative.
- Companies continue to not contribute data resulting in the likelihood of governments requiring companies to provide data within a mandated regime.

**Next Steps**

Suggested next steps for implementing this recommendation include:

- 2-1.** Private sector companies work together to create formats and protocols for providing information.
- 2-2.** Private sector companies volunteer to provide data to the trusted entity.
- 2-3.** Private sectors companies recruit additional companies to join the effort.

**Measures of Success**

The effective implementation of this recommendation can be confirmed with the following measures of success:

- A.** A statically representative number of companies contribute data on an agreed-upon, regular basis.
- B.** There is sufficient participation to be able to divide the aggregated data into more meaningful categories, such as transportation, retail and financial services.

Private-sector companies should voluntarily provide statistical data to an established trusted entity that will use the data to support the measurement of the cybersecurity problem.

## 4.3 Bona Fide Benchmarks

### Objective

This third recommendation ensures the development of a quantitative framework that will produce meaningful and reliable benchmarks for the broad range of stakeholders. Here there is a call for subject matter experts to develop a consensus approach to data analysis, representation and reporting.

### Background

Cybersecurity compromises, though a truly growing concern of high consequence for companies and governments, are still relatively rare events in the context of massively deployed applications of ICT. The significance of this observation is that it regards the type of statistical analysis needed to capture the insights offered from such data and context. One specific key point is that the interpretation of variations of the event frequency over time is not as straightforward as for more frequent events.<sup>69</sup> For example, an observed increase or decrease in the number of events from one year to the next can simply be variation within a “normal” expected range of behavior for the data. An actual deviation from normal (i.e. a trend) will have certain statistical significant indicators.<sup>70</sup> Thus appropriate care must be given to the analysis, presentation and interpretation of the data associated with the measurement of cybersecurity compromises.

The reports from the collected data will be useful to the extent that it can provide a clearer and more accurate picture of the reality of the cybersecurity problem.<sup>71</sup> Thus it is important that the statistics not

only be the most accurate reflection of reality, but also be easy to understand, especially when it comes to confirming an actual statistically significant trend. A key challenge for this endeavor is for these reports to be straightforward and effective in educating the public on the numbers when presented. Thus, as the single numbers of the Richter Magnitude Scale and Saffir-Simpson Hurricane Wind Scale gauge the magnitude of the energy release in an earthquake and the sustained wind of a hurricane (e.g., ‘Category 3’), respectively, so the magnitude of cybersecurity compromise measurements should be meaningful and usable quantity in the public domain. Furthermore, as the normal variations of temperature in a day or week or season are appreciated as just that—“normal variations,” so, too, the reporting should lend itself to effectively distinguishing between significant dynamics in the measurements from those otherwise insignificant.

This recommendation can take a very complex and confusing issue and translate it into its most basis aspects—magnitude and change over time—into quantities that are both understandable and meaningful.<sup>72 73</sup>

### RECOMMENDATION 3.

**Qualified subject matter experts should collaborate to develop statistical methods for analyzing the voluntarily-submitted data and for reporting benchmarks.**

<sup>69</sup> “Educated Boards and Senior Management Are Indispensable for Quality Improvement,” supra n 52.

<sup>70</sup> For example, as determined from Statistical Process Control (SPC).

<sup>71</sup> “Measurement of the Cybersecurity Problem Is a Game Changer,” supra n 51.

<sup>72</sup> Figure 4, “Quantity 1 (Q1): The Problem’s Order of Magnitude Is Unknown,” p.26.

<sup>73</sup> Figure 5, “Quantity 2 (Q2): The Rate of Change Is Unknown,” p.27.



Qualified subject matter experts should collaborate to develop statistical methods for analyzing the voluntarily-submitted data and for reporting benchmarks.

### Required Commitments

The effective implementation of this recommendation requires the following commitments from the private sector:

- Subject matter experts in the fields of statistics, cybersecurity and quality control collaborate to establish procedures for analyzing and representing the aggregated data.
- Stakeholders must participate in the development of the data analysis and representation to ensure that it will be agreeable.

### Benefits

The value of implementing this recommendation is that it ensures that the voluntarily-submitted data is treated with the correct mathematical and statistical methods, that the data is presented in a way that minimizes misinterpretation and can be maximally useful to stakeholders. Given the statistical qualities of cybersecurity compromise data, it is essential that the proper statistical methods be used so that benchmarks are accurately established and appropriately used. Although perfection is not achievable, benchmarks will enable companies and individuals involved to understand what is reasonable and achievable.

### Alternatives and Consequences

Alternatives to this approach include the following:

- The data is analyzed with overly simple statistical methods resulting in increased likelihood of false trends.
- No agreement is reached on the statistical methods to be used resulting in inconsistent representations of the aggregated data.

### Next Steps

Suggested next steps for implementing this recommendation include:

- 3-1.** Subject matter experts in statistical analysis, quality control and cybersecurity work together to develop consensus methodologies for analyzing global cybersecurity compromise data.
- 3-2.** Subject matter experts in statistical analysis, quality control, cybersecurity and the media work together to develop formats for presenting statistics on the aggregated global cybersecurity compromise data.
- 3-3.** Subject matter experts in statistical analysis, quality control, cybersecurity and the media work together to interpret feedback from stakeholders on the usefulness of the provided reports and make adjustments as appropriate.

### Measures of Success

The effective implementation of this recommendation can be confirmed with the following measures of success:

- A.** Consensus procedures and structure are established for handling the data and generating meaningful statistics.
- B.** Order of magnitude statistics are provided on a regular basis for the worldwide cybersecurity problem.
- C.** The generated statistics are used to inform policy makers, businesses and the public.

# 5. Conclusion

“Innovation is a gamble, but so is standing pat.”

- Arthur B. Dougall

**M** *Measuring the Cybersecurity Problem* reports on the analysis, conclusions and guidance of an international group of subject matter experts and stakeholders. Its focus is on driving the implementation of three recommendations for the private sector. These recommendations are actionable and, if implemented, can provide a much needed measurement for the order of magnitude of this problem.

The three critical steps that lie ahead are creating a trusted environment, voluntarily submitting data and developing the appropriate statistical analysis and presentation practices.

The alternatives to taking this approach will have undesirable consequences, such as continuing on a path characterized by “flying without instruments” or unduly burdensome government oversight of private sector operations.

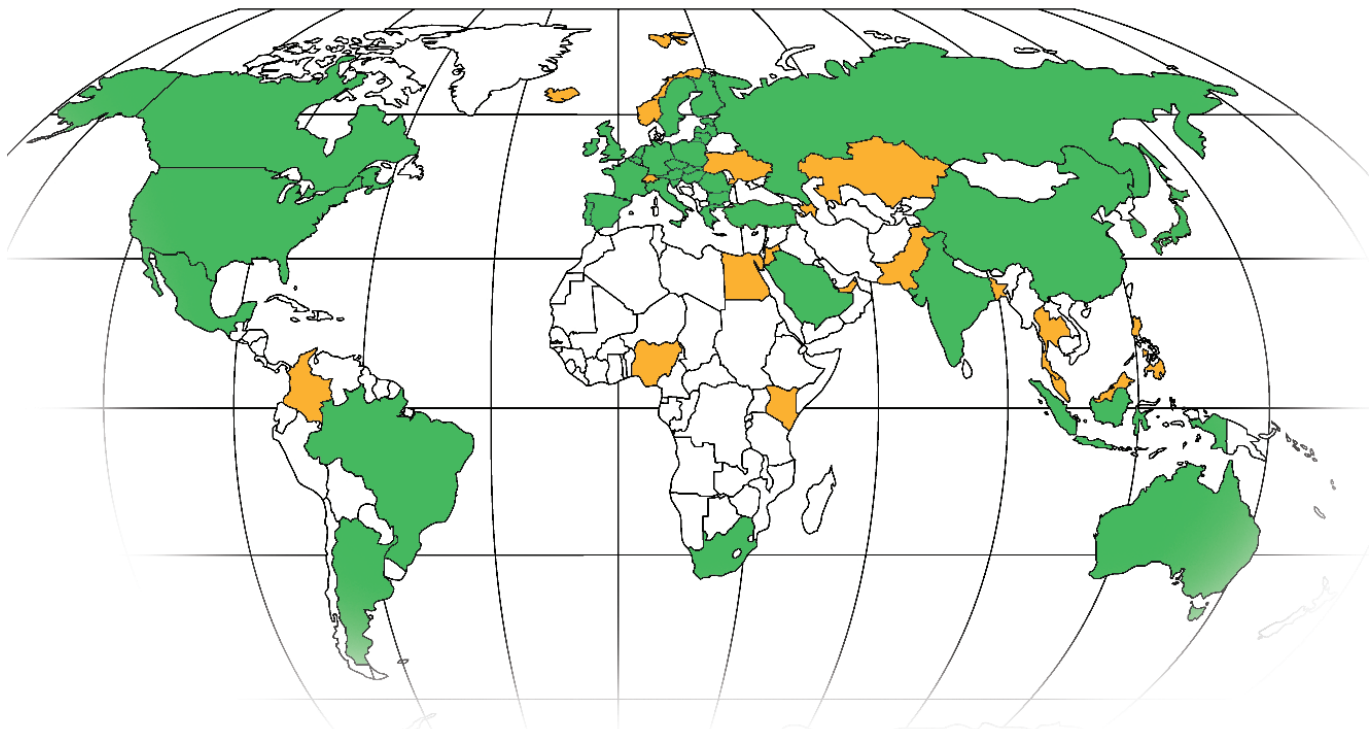
The authors are encouraged that throughout the writing of this report, companies have indicated an eagerness to support such a process if a trusted entity can be formed.

# CYBER40

The G20 + the next most important nations in cyberspace



**EASTWEST INSTITUTE**  
*Forging Collective Action for a Safer and Better World*



## G20 +

- |           |                   |            |                      |
|-----------|-------------------|------------|----------------------|
| Argentina | Japan             | Azerbaijan | Nigeria              |
| Australia | Mexico            | Bangladesh | Norway               |
| Brazil    | Republic of Korea | Cameroon   | Pakistan             |
| Canada    | Russia            | Colombia   | Philippines          |
| China     | Saudi Arabia      | Egypt      | Qatar                |
| France    | South Africa      | Iceland    | Singapore            |
| Germany   | Turkey            | Israel     | Switzerland          |
| India     | United Kingdom    | Jordan     | Thailand             |
| Indonesia | United States     | Kazakhstan | Ukraine              |
| Italy     | European Union    | Kenya      | United Arab Emirates |
|           |                   | Malaysia   |                      |

For more information about the Cyber40 and EWI cybersecurity work, please contact Anneleen Roggeman at [aroggeman@ewi.info](mailto:aroggeman@ewi.info).

## REFERENCES

- ATIS: Network Reliability Steering Committee (NRSC), <http://www.atis.org/nrsc>.
- BITS: The Technology Policy Division of the Financial Services Roundtable, <http://www.bitsinfo.org>.
- Center for Strategic International Studies (CSIS), The Economic Impact of Cybercrime and Cyber Espionage Report, July 2013.
- CERTs: Computer Emergency Readiness (or Response) Teams, including both public and private sector managed entities.
- CPNI: Centre for the Protection of National Infrastructure, <http://www.cpni.gov.uk>.
- Dresner, Stewart and Norcup, Amy, Data Breach Notification Laws in Europe, Privacy Laws & Business, 2009.
- DSCI: Data Security Council of India, <http://www.dsci.in>.
- EBITT: E-Business, IT and Telecoms Commission, of the International Chamber of Commerce (ICC). <http://www.iccwbo.org/policy/ebitt>.
- ENISA: European Network and Information Security Agency, <http://www.enisa.europa.eu>.
- FCC CSRIC: Federal Communications Commission, the Communications Security, Reliability and Interoperability Council. Formerly NRIC, a federal advisory committee act (FACA) body chartered by the U.S. congress, <http://www.csrlic.org>.
- FIRST: Forum of Incident Response and Security Teams. <http://www.first.org>.
- First Worldwide Cybersecurity Summit – Protecting the Digital Economy,” Dallas, May 2010, <http://www.ewi.info/dallas>.
- FS-ISAC: Financial Services Information Sharing and Analysis Center, <http://www.fsisac.com>.
- Gopal Ratnam & Tony Capaccio, “Cyber Security May Gain in Pentagon’s Budget Review, Lynn Says,” Bloomberg, 12 May 2011, <http://www.bloomberg.com/news/2011-05-12/cyber-security-may-gain-in-pentagon-s-budget-review-lynn-says.html>.
- Information Security Breaches Survey, [http://www.pwc.co.uk/eng/publications/isbs\\_survey\\_2010.html](http://www.pwc.co.uk/eng/publications/isbs_survey_2010.html).
- International Cable Protection Committee (ICPC), [www.iscpc.org](http://www.iscpc.org).
- ISACs: Information Sharing and Analysis Centers, <http://www.isaccouncil.org>.

ISC: Internet Systems Consortium, <http://www.isc.org>.

Karl F. Rauscher, "Availability and Robustness of Electronic Communications Infrastructures (ARECI) Final Report," European Commission, March 2007, <http://www.anacom.pt/render.jsp?contentId=483155>.

Karl F. Rauscher, "Reliability of Global Undersea Communications Cable Infrastructure," ROGUCCI, IEEE, 2010, [http://www.ieee-rogucci.org/files/The ROGUCCI Report.pdf](http://www.ieee-rogucci.org/files/The%20ROGUCCI%20Report.pdf).

Maass, Peter and Rajagopalan, Megha, Does Cybercrime Really Cost \$1 Trillion? ProPublica, August 2012.

M3AAWG: Messaging, Malware and Mobile Anti-Abuse Working Group, <http://www.maawg.org>.

NASSCOM: National Association of Software and Services Companies, <http://www.nasscom.in>.

NIAC: National Infrastructure Advisory Council, <http://www.dhs.gov/national-infrastructure-advisory-council>.

NRSC: Network Reliability Steering Committee of the Alliance for Telecommunications Industry Solutions (ATIS), <http://www.atis.org/nrsc>.

NSIE: Network Security Information Exchange of the U.S. President's National Security Telecommunications Advisory Committee (NSTAC), [http://www.ncs.gov/nstac/reports/fact\\_sheet/NSTAC\\_08.pdf](http://www.ncs.gov/nstac/reports/fact_sheet/NSTAC_08.pdf).

"Official Reveals \$650M Cyber Security Spending Plans," Government Computing, 26 April 2011, <http://central-government.governmentcomputing.com/news/2011/apr/26/650m-cyber-security-spending-plans-ian-mcghie>.

Protecting the Digital Economy, Proceedings of the First Worldwide Cybersecurity Summit, Dallas, EastWest Institute, May 2011.

Warning, Advise, Reporting Points (WARPS), <http://www.warp.gov.uk/>.

Worldwide Cybersecurity Initiative Top 5 Breakthrough Areas – Executive Summary, Proceedings of the First Worldwide Cybersecurity Summit, Dallas, EastWest Institute, May 2011.

"Unsecured Economies: Protecting Vital Information," report by McAfee, 2009, [http://www.cerias.purdue.edu/assets/pdf/mfe\\_unsec\\_econ\\_pr\\_rpt\\_fnl\\_online\\_012109.pdf](http://www.cerias.purdue.edu/assets/pdf/mfe_unsec_econ_pr_rpt_fnl_online_012109.pdf).

# EWI Board of Directors

## OFFICE OF THE CHAIRMEN

**Ross Perot, Jr. (U.S.)**

*Chairman*  
EastWest Institute  
*Chairman*  
Hillwood Development Co. LLC  
*Board of Directors*  
Dell Inc.

**Armen Sarkissian (Armenia)**

*Vice Chairman*  
EastWest Institute  
*President*  
Eurasia House International  
*Former Prime Minister of*  
*Armenia*

## OFFICERS

**John Edwin Mroz (U.S.)**

*President, Co-Founder and CEO*  
EastWest Institute

**R. William Ide III (U.S.)**

*Council and Secretary*  
*Chair of the Executive Committee*  
EastWest Institute  
*Partner*  
McKenna Long and Aldridge LLP

**Leo Schenker (U.S.)**

*Treasurer*  
EastWest Institute  
*Senior Executive Vice President*  
Central National-Gottesman Inc.

## MEMBERS

**Martti Ahtisaari (Finland)**

*Former Chairman*  
EastWest Institute  
*2008 Nobel Peace Prize Laureate*  
*Former President of Finland*

**Tewodros Ashenafi (Ethiopia)**

*Chairman and CEO*  
Southwest Energy (HK) Ltd.

**Jerald T. Baldrige (U.S.)**

*Chairman*  
Republic Energy Inc.

**Peter Bonfield (U.K.)**

*Chairman*  
NXP Semiconductors

**Matt Bross (U.S.)**

*Chairman and CEO*  
WBE Hong Kong

**Robert N. Campbell III (U.S.)**

*Vice Chairman (Retired)*  
Deloitte LLP

**Peter Castenfelt (U.K.)**

*Chairman*  
Archipelago Enterprises Ltd.

**Maria Livanos Cattai  
(Switzerland)**

*Former Secretary-General*  
International Chamber of  
Commerce

**Michael Chertoff (U.S.)**

*Co-founder and Managing*  
*Principal*  
Chertoff Group



**David Cohen (U.K.)**

*Chairman*  
F&C REIT Property Management

**Joel Cowan (U.S.)**

*Professor*  
Georgia Institute of Technology

**Addison Fischer (U.S.)**

*Chairman and Co-Founder*  
Planet Heritage Foundation

**Stephen B. Heintz (U.S.)**

*President*  
Rockefeller Brothers Fund

**Hu Yuandong (China)**

*Chief Representative*  
UNIDO ITPO-China

**Emil Hubinak (Slovak Republic)**

*Chairman and CEO*  
Logomotion

**John Hurley (U.S.)**

*Managing Partner*  
Cavalry Asset Management

**Wolfgang Ischinger (Germany)**

*Chairman*  
Munich Security Conference  
*Global Head of*  
*Governmental Affairs*  
Allianz SE

**Ralph Isham (U.S.)**

*Managing Director*  
GH Venture Partners LLC

**Anurag Jain (India)**

*Chairman*  
Laurus Edutech Pvt. Ltd.

**Gen. (ret) James L. Jones (U.S.)**

*Former Advisor*  
U.S. National Security  
*Former Supreme Allied*  
*Commander*  
Europe  
*Former Commandant*  
Marine Corps

**Haifa Al Kaylani (U.K.)**

*Founder and Chairperson*  
Arab International Women's Forum

**Zuhal Kurt (Turkey)**

*CEO*  
Kurt Enterprises

**General (ret) T. Michael  
Moseley (U.S.)**

Moseley and Associates, LLC  
*Former Chief of Staff*  
United States Air Force

**F. Francis Najafi (U.S.)**

*CEO*  
Pivotal Group

**Amb. Tsuneo Nishida (Japan)**

*Permanent Representative*  
*of Japan to the U.N.*

**Ronald P. O'Hanley (U.S.)**

*President, Asset Management*  
*and Corporate Services*  
Fidelity Investments

**Amb. Yousef Al Otaiba (U.A.E.)**

*Ambassador*  
Embassy of the United Arab  
Emirates in Washington, D.C.

**Admiral (ret) William A. Owens  
(U.S.)**

*Chairman*  
AEA Holdings Asia  
*Former Vice Chairman*  
U.S. Joint Chiefs of Staff

**Sarah Perot (U.S.)**

*Director and Co-Chair for*  
*Development*  
Dallas Center for Performing Arts

**Louise Richardson (U.S.)**

*Principal*  
University of St. Andrews

**John Rogers (U.S.)**

*Managing Director*  
Goldman Sachs and Co.

**George F. Russell, Jr. (U.S.)**

*Former Chairman*  
EastWest Institute  
*Chairman Emeritus*  
Russell Investment Group  
*Founder*  
Russell 20-20

**Ramzi H. Sanbar (U.K.)**

*Chairman*  
SDC Group Inc.

**Ikram ul-Majeed Sehgal  
(Pakistan)**

*Chairman*  
Security & Management  
Services Ltd.

**Amb. Kanwal Sibal (India)**

*Former Foreign Secretary of India*

**Kevin Taweel (U.S.)**

*Chairman*  
Asurion

**Amb. Pierre Vimont (France)**

*Executive Secretary General*  
European External Action Service  
*Former Ambassador*  
Embassy of the Republic of France  
in Washington, D.C.

**Alexander Voloshin (Russia)**

*Chairman of the Board*  
OJSC Uralkali

**Amb. Zhou Wenzhong (China)**

*Secretary-General*  
Boao Forum for Asia

**NON-BOARD COMMITTEE  
MEMBERS**

**Laurent Roux (U.S.)**

*Founder*  
Gallatin Wealth Management, LLC

**Hilton Smith, Jr. (U.S.)**

*President and CEO*  
East Bay Co., LTD

**CO-FOUNDER**

**Ira D. Wallach\* (U.S.)**

*Former Chairman*  
Central National-Gottesman Inc.  
*Co-Founder*  
EastWest Institute

**CHAIRMEN EMERITI**

**Berthold Beitz\* (Germany)**

*President*  
Alfried Krupp von Bohlen  
und Halbach-Stiftung

**Ivan T. Berend (Hungary)**

*Professor*  
University of California, Los Angeles

**Francis Finlay (U.K.)**

*Former Chairman*  
Clay Finlay LLC

**Hans-Dietrich Genscher  
(Germany)**

*Former Vice Chancellor and  
Minister of Foreign Affairs*

**Donald M. Kendall (U.S.)**

*Former Chairman and CEO*  
PepsiCo. Inc.

**Whitney MacMillan (U.S.)**

*Former Chairman and CEO*  
Cargill Inc.

**Mark Maletz (U.S.)**

*Chairman, Executive Committee*  
EastWest Institute  
*Senior Fellow*  
Harvard Business School

**DIRECTORS EMERITI**

**Jan Krzysztof Bielecki (Poland)**

*CEO*  
Bank Polska Kasa Opieki S.A.  
*Former Prime Minister of Poland*

**Emil Constantinescu (Romania)**

*President*  
Institute for Regional Cooperation  
and Conflict Prevention (INCOR)  
*Former President of Romania*

**William D. Dearstyne (U.S.)**

*Former Company Group Chairman*  
Johnson & Johnson

**John W. Kluge\* (U.S.)**

*Former Chairman of the Board*  
Metromedia International Group

**Maria-Pia Kothbauer  
(Liechtenstein)**

*Ambassador*  
Embassy of Liechtenstein to  
Austria, OSCE and the UN in Vienna

**William E. Murray\* (U.S.)**

*Former Chairman*  
The Samuel Freeman Trust

**John J. Roberts (U.S.)**

*Senior Advisor*  
American International Group (AIG)

**Daniel Rose (U.S.)**

*Chairman*  
Rose Associates Inc.

**Mitchell I. Sonkin (U.S.)**

*Managing Director*  
MBIA Insurance Corporation

**Thorvald Stoltenberg (Norway)**

*President*  
Norwegian Red Cross

**Liener Temerlin (U.S.)**

*Chairman*  
Temerlin Consulting

**John C. Whitehead (U.S.)**

*Former Co-Chairman*  
Goldman Sachs  
*Former U.S. Deputy Secretary  
of State*

\* Deceased

# EastWest Institute Policy Report Series

## 2013

### **Threading the Needle**

Proposals on U.S. and Chinese Actions  
on Arms Sales to Taiwan  
Policy Report 2013—3

### **The Path to Zero**

Report of the 2013 Nuclear Discussion Forum  
Policy Report 2013—2

### **Afghan Narcotrafficking**

A Joint Threat Assessment  
Policy Report 2013—1 [EN | RU]

## 2012

### **Bridging the Fault Lines**

Collective Security in Southwest Asia  
Policy Report 2012—1

### **Priority International Communications**

Staying Connected in Times of Crisis  
Policy Report 2012—2

## 2011

### **Working Towards Rules for Governing Cyber Conflict**

Rendering the Geneva and Hague  
Conventions in Cyberspace  
Policy Report 2011—1 [EN | RU]

### **Seeking Solutions for Afghanistan, Part 2**

Policy Report 2011—2

### **Critical Terminology Foundations**

Russia-U.S. Bilateral on Cybersecurity  
Policy Report 2011—3

### **Enhancing Security in Afghanistan and Central Asia through Regional Cooperation on Water**

Amu Darya Basin Consultation Report  
Policy Report 2011—4

### **Fighting Spam to Build Trust**

China-U.S. Bilateral on Cybersecurity  
Policy Report 2011—5 [EN | CH]

### **Seeking Solutions for Afghanistan, Part 3**

Policy Report 2011—6

## 2010

### **Economic Development and Security for Afghanistan**

Increasing Jobs and Income with the Help  
of the Gulf States  
Policy Report 2010—1

### **Making the Most of Afghanistan's River Basins**

Opportunities for Regional Cooperation  
Policy Report 2010—2

### **The Reliability of Global Undersea Communications Cable Infrastructure**

Policy Report 2010—3

### **Rights and Responsibilities in Cyberspace**

Balancing the Need for Security and Liberty  
Policy Report 2010—4

### **Seeking Solutions for Afghanistan, Part 1**

Policy Report 2010—5



Founded in 1980, the EastWest Institute is a global, action-oriented think-and-do tank. EWI tackles the toughest international problems by:

**Convening** for discreet conversations representatives of institutions and nations that do not normally cooperate. EWI serves as a trusted global hub for back-channel “Track 2” diplomacy, and also organizes public forums to address peace and security issues.

**Reframing** issues to look for win-win solutions. Based on our special relations with Russia, China, the United States, Europe and other powers, EWI brings together disparate viewpoints to promote collaboration for positive change.

**Mobilizing** networks of key individuals from both the public and private sectors. EWI leverages its access to intellectual entrepreneurs and business and policy leaders around the world to defuse current conflicts and prevent future flare-ups.

The EastWest Institute is a non-partisan, 501(c)(3) nonprofit organization with offices in New York, Brussels and Moscow and Washington. Our fiercely guarded independence is ensured by the diversity of our international board of directors and our supporters.

**EWI New York Center**

11 East 26<sup>th</sup> St.  
20<sup>th</sup> Floor  
New York, NY 10010  
1-212-824-4100

**EWI Brussels Center**

Rue de Trèves, 59-61  
Brussels 1040  
32-2-743-4610

**EWI Moscow Center**

Bolshaya Dmitrovka St. 7/5,  
Building 1, 6<sup>th</sup> Floor  
Moscow 125009  
7-495-2347797

**EWI Washington Office**

1069 Thomas Jefferson St. NW  
Washington, D.C. 20007  
1-202-492-0181

[www.ewi.info](http://www.ewi.info)