Microsoft

The

Cybersecurity Risk Paradox

Impact of Social, Economic, and Technological Factors on Rates of Malware

David Burt, Paul Nicholas, Kevin Sullivan,
(Microsoft Trustworthy Computing)
and Travis Scoles
(Schireson Associates)

Introduction

Around the globe, societies are becoming increasingly dependent upon information and communications technology (ICT) which is driving rapid social, economic, and governmental development. Yet with this development, new threats to digital infrastructures have emerged.

It is therefore critical that nations understand the factors that contribute to cybersecurity at a national level so they can plan for developing their nation's digital potential. With this in mind, Microsoft recently released a set of recommendations for developing national cybersecurity strategies.[1]

Every country faces unique cybersecurity challenges. Understanding the factors that contribute to these challenges is critical, especially for developing nations. Notably, the benefits and risks of technological development are not always shared equally. By analyzing malware infection rates in selected countries, this paper highlights the disproportionate challenges that many countries face in the earlier stages of modernizing their information and communications technology. In addition, it identifies the social, economic, and technological factors that are critical to enhancing cybersecurity, and offers a set of recommendations for countries seeking to improve it.

Background

The term *cybersecurity* takes on different meanings depending on the audience. Citizens may feel that cybersecurity is related to protecting personal information, while businesses may view it as a means for providing business continuity. In the policy context, cybersecurity represents the collective activities and resources that enable citizens, enterprises, and governments to meet their computing objectives in a secure, private, and reliable manner.

Although security incidents have been (and continue to be) a frequent topic of media interest, cybersecurity, as measured by the prevalence of malware, improved between 2011 and 2012.

Given the importance of cybersecurity to contemporary societies, policymakers need measures to assess its effectiveness. In an attempt to define better metrics, Microsoft began a collaborative effort in 2013 to explore predictive cybersecurity models that could advance the understanding of the key technical and nontechnical factors that contribute to cybersecurity. The resulting study, *Linking Cybersecurity Policy and Performance*,[2] measured cybersecurity performance by tracking infection rates of malicious software (or *malware*) as a proxy for measuring cybersecurity performance. These malware infection rates are derived from the findings of Microsoft's Malicious Software Removal Tool (MSRT), which runs on more than 600 million devices worldwide every month. Microsoft publishes these findings in a semi-annual Security Intelligence Report (SIR),[3] which provides an analysis of the landscape of exploits, vulnerabilities, malware, and other intelligence data.

The SIR measures malware infection using a metric called Computers Cleaned per Mille (CCM)—the number of computers cleaned for every 1,000 executions of the MSRT. For example, if the MSRT is executed 50,000 times in a particular location in the first quarter of the year and removes infections from 200 computers, the malware infection rate for that period is 4.0 (200 ÷ 50,000 × 1,000). Lower CCM numbers equate to lower rates of malware infection, which are interpreted as higher cybersecurity performance.

1 Developing a National Strategy for Cybersecurity: Foundations for Security, Growth, and Innovation, Cristin Goodwin and Paul Nicholas, Microsoft, October 2013. (http://aka.ms/national-strategy)

2 Linking Cybersecurity Policy and Performance, Microsoft, February 2013. (http://aka.ms/securityatlas)

3 Microsoft Security Intelligence Report (SIR), Volume 15, Microsoft, October 2013. (http://aka.ms/tn7t1f)

Linking Cybersecurity Policy and Performance found that the prevalence of malware (as measured by CCM) correlates with a variety of metrics that connote the economic and social development of a nation; in general, more developed nations enjoy better cybersecurity.

Of course, malware infection rates are only one factor impacting cybersecurity, and policy plays a key role. Many nontechnical factors also affect technical cybersecurity. *Linking Cybersecurity Policy and Performance* examined over 80 different social and economic policy indicators and constructed a statistical model based on 34 of them (such as GDP per Capita, Literacy Rate, and Rule of Law) that can predict a country's rate of malware. The model created three distinct clusters of countries:

1. **Maximizers**
   Countries with effective cybersecurity capabilities that outperform the model expectations.

2. **Aspirants**
   Countries that are on a par with the model and are still developing cybersecurity capabilities.

3. **Seekers**
   Countries with higher cybersecurity risk that underperform on model expectations. Seeker countries are generally those with developing economies and lower levels of technological development.

Changes in Malware Rates Across Countries

Linking Cybersecurity Policy and Performance explored the relationship between the prevalence of malware on the one hand and socioeconomic factors and policy choices on the other. This paper seeks to understand more about the links between changes in national development and cybersecurity over time, and particularly to explore how cybersecurity is changing in Seeker countries.

Rates of malware are, of course, dynamic and fluctuate over time. Because Microsoft measures infection patterns, a single piece of malware that infects a large number of computer systems within a nation can greatly increase the rate of malware in the short term. Additionally, updates to the MSRT that detect previously unnoticed malware families can generate spikes in malware rates.

An example of this kind of volatility was observed in the Republic of Korea, where the detection of malware increased more than 300 percent between September 2012 and December 2012. This was the result of adding to MSRT the capability to detect two variants of malware that had previously gone undetected.[4] To compensate for the impact of such volatility on the models discussed in this report, quarterly malware figures have been averaged by country to generate a smoothed annual figure.

Although security incidents have been (and continue to be) a frequent topic of media interest, cybersecurity, as measured by the prevalence of malware, improved between 2011 and 2012. Among the 105 countries analyzed in this study, malware prevalence dropped from 11.2 CCM to 9.2 CCM. The majority (87.5 percent) experienced a decline in malware (improvement in cybersecurity) between 2011 and 2012, with the average decrease being 23.3 percent.

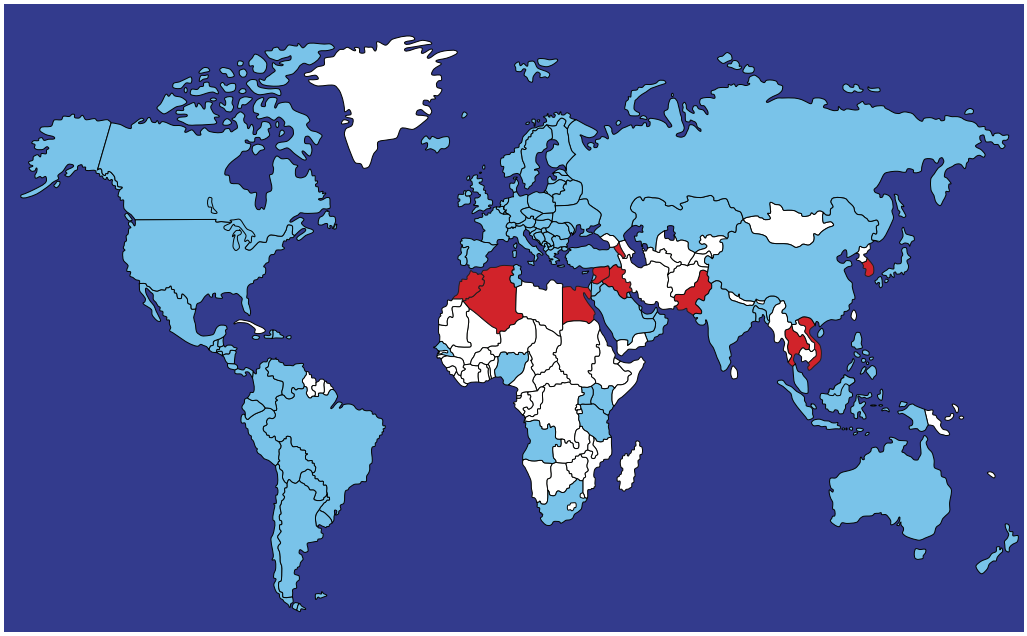
4 Microsoft SIR, Volume 14, January 2013. (http://aka.ms/SIR-v14)

Figure 1.
Comparison of the changes in malware rates.

Malware Rates: All Countries Compared to Seekers

Metric	Total	Seekers
Mean 2011 Malware Rate	11.2	18.2
Median 2011 Malware Rate	10.5	17.3
Mean 2012 Malware Rate	9.2	17.6
Median 2012 Malware Rate	7.2	14.5
Mean Malware Rate Change	-23.3%	-3.7%
Median Malware Rate Change	-26.7%	-7.4%
Percentage of Countries with a Malware Decrease	87.5%	65.5%

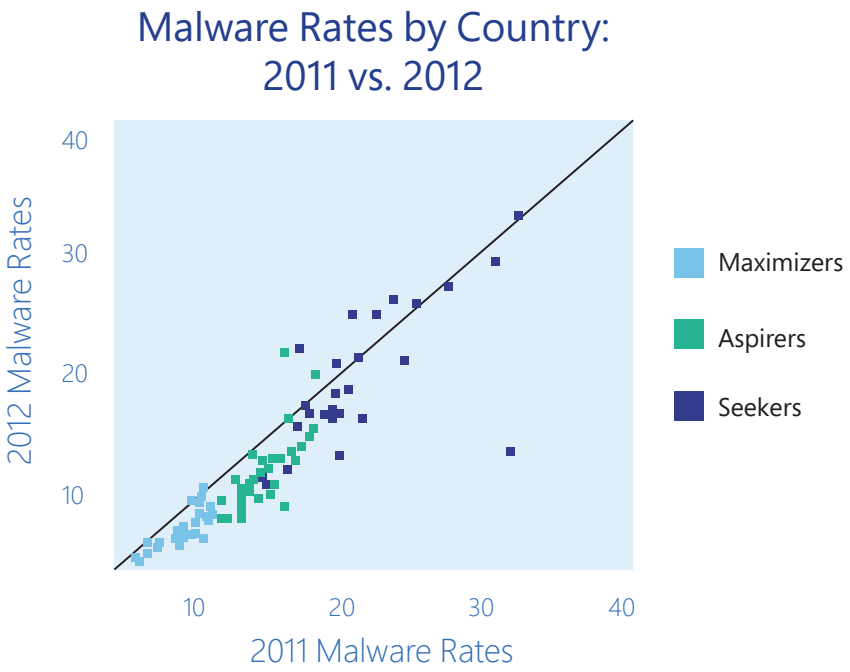
Figure 2.
Malware change by country. Blue represents a decline in the rate of malware between 2011 and 2012; red represents an increase. Countries with no data are shown in white.



In 2011, decreases in malware were more common among countries with lower malware rates, although many countries with higher rates (those with relatively poor cybersecurity) also enjoyed an improvement.

Patterns of declining malware rates in Seeker countries are of special interest. In 2011, Seekers did not have strong cybersecurity and tended to have higher malware rates overall, as well as lower economic and social development scores. Seekers are good candidates for exploring cybersecurity change because they offer the greatest diversity in the rates of change in malware–some countries are experiencing declines in malware rates and others are experiencing increases.

Figure 3.
Comparison of malware rates between 2011 and 2012. Countries above the divider line saw an increase in malware. These countries were disproportionately identified as Seekers in the previous study, *Linking Cybersecurity Policy and Performance.*



Factors that Impact Malware Prevalence

With the understanding that national development metrics can predict the prevalence of malware, and that, in general, rates of malware infection are declining (although the number of malware variants are increasing), Microsoft sought to understand why some countries showed greater improvements in cybersecurity than others. To explore this question, Microsoft created a new predictive model that attempted to explain the changes in malware prevalence between 2011 and 2012 by looking at the 34 developmental metrics previously found to predict the level of malware.[5]

Case Study:
Cybersecurity in India

India experienced an improvement in cybersecurity between 2011 and 2012. Its CCM in 2012 was 11.8, down from 15.0 in 2011—slightly less than the global average. This improvement corresponds to strong and improving Institutional Stability.

Population
1,228,127,400

Per Capita GDP
1,389

Digital Access
Below average but improving

1.1% vs 14%
Broadband penetration, like most 2011 technology metrics, was well below the mean

23%
Increase in Secure Net Servers per Million People

Institutional Stability
Relatively strong and improving

16%
Decline in corruption

Rule of Law
2.9 vs 3.3 (mean)

Demographic Stability
8 vs 5.2 (mean)

Economic Development
Below average but improving

5.7%
Increase in GDP per Capita

5 The 34 developmental metrics are derived from sources such as the World Bank Governance Indicators. (The Appendix Developmental Metrics on page 11 contains a full listing.)

The type of model[6] employed in this study is most effective when it includes as few predictor variables as possible, in order to reduce the risk of overfitting.[7]

Global Model

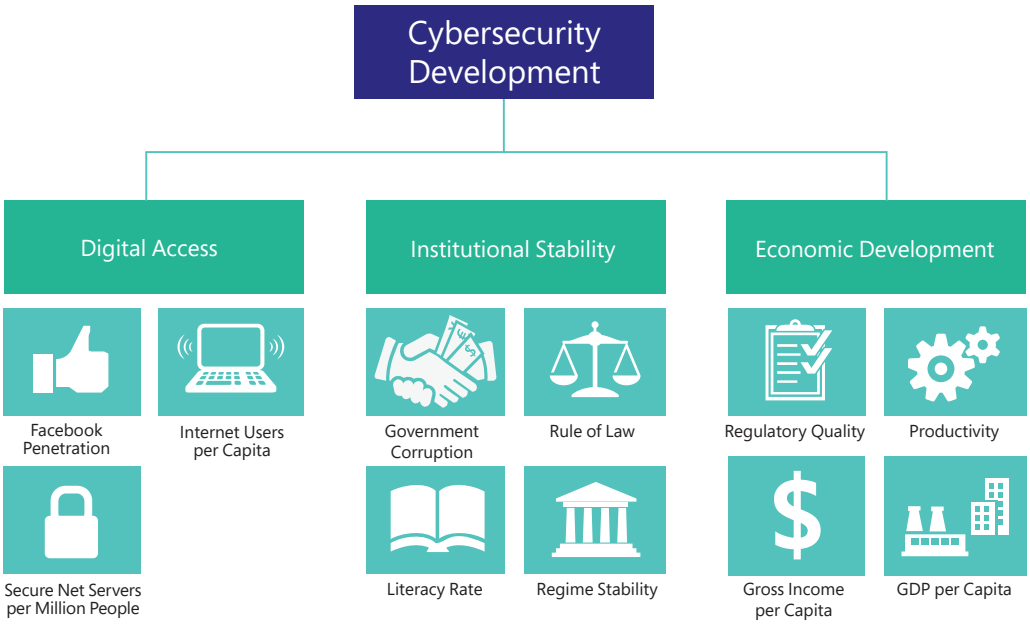
Ultimately, the model identified 11 key elements that can predict changes in global rates of malware. These predictors fall into one of three areas: Digital Access, Institutional Stability, and Economic Development. The relative ability of the predictors in each area to forecast cybersecurity change varies from country to country. As a rule, however, the model shows that countries that are above-average across these developmental areas can expect to see greater improvement in cybersecurity.

Digital Access measures both the quality and quantity of digital content being consumed; predictors include Internet Users per Capita and Secure Net Servers per Million People.

Institutional Stability applies to a group of predictors related to national, social, and human development, such as Regime Stability and Literacy Rate.

Economic Development relates to predictors that directly impact the creation of goods, income, or business operations within the country, such as GDP per Capita.

Figure 4.
This model suggests that predictors of change in malware rates fall into three main policy areas.



6 The model employed is an elastic net regression, which applies lasso and ridge penalties to all variables in an OLS framework. The lasso penalty encourages variable selection by excluding superfluous variables, while the ridge penalty lessens the impact of coefficients. This modeling technique is generally used on highly dimensional data with correlated predictors. For more information, see Zou, Hui, and Hastie, *Regularization and Variable Selection via the Elastic Net* (2005). The model was evaluated for accuracy by the mean squared error: MSE =.1.

7 Overfitting occurs when too many predictor variables give the model a false sense of accuracy by matching existing data too exactly instead of accurately identifying future prediction. As an example, if PCs in Use per Capita is highly correlated with Net-Enabled PC Ownership, the model could choose to include only PCs in Use per Capita in order to prevent overfitting the data; this does not mean Net-Enabled PC Ownership has no bearing on malware prevalence change, but instead can be interpreted in a broader sense—access to the Internet impacts degree of cybersecurity change.

Model of Seeker Countries

The global model was then applied only to Seeker countries. Because the sample was small (27 countries), the number of predictors identified by the model decreased. Three predictors were found to be significant:

1 **Secure Net Servers per Million People**

2 **Regime Stability**

3 **Regulatory Quality**

Though this model included only three predictors, they represent each of the three areas from the global model. Seekers with greater institutional stability and economic development showed larger increases in cybersecurity, similar to the effects observed in the global model. Seeker countries with increased digital access (as represented by Secure Net servers per Million People), however, had an effect opposite to what was expected.[8]

Comparing the impact of digital access predictors in both the global model and the Seeker model highlights the complex relationship between technological maturation and cybersecurity improvement. In the global model, we see increases in Facebook Penetration, a proxy for Internet access and usage, correlated with decreasing malware rates. Among Seeker countries, we see increases in Secure Net Servers per Million People, a measure of overall infrastructure development, correlated with increasing malware rates—in other words, as digital access increases for Seekers, so do regional rates of malware infection.

Case Study: Cybersecurity in Brazil

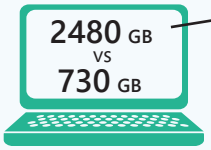
Brazil experienced an improvement in cybersecurity between 2011 and 2012 that surpassed the global average. Brazil's CCM in 2012 was 9.9, down from 17.3 in 2011, a 42% decrease. Relatively strong (and improving) Digital Access metrics, as well as solid Institutional Stability, helped Brazil realize a decrease in malware.

Population
193,741,800

Per Capita GDP
$12,798

Digital Access

Similar to the global average and improving



2011 Broadband speed: much faster than the global average

Ownership of Internet-enabled PCs

Institutional Stability

On par or above average and improving

Rule of Law

3.0 vs 3.3 (mean)

Economic Development

Below average

2.5%

Decrease in GDP per Capita

8 Ordinary Least Squares (OLS) Regression. MSE = .03. OLS was employed in lieu of elastic net due to the extreme impact of the ridge penalty on the limited case values obscuring coefficient impact on the model. Variable selection was conducted by analyzing the statistical significance of the predictors in a variety of models determined via both stepdown and heuristic methods. All predictors are significant at 5 percent.

The Paradox of ICT Modernization

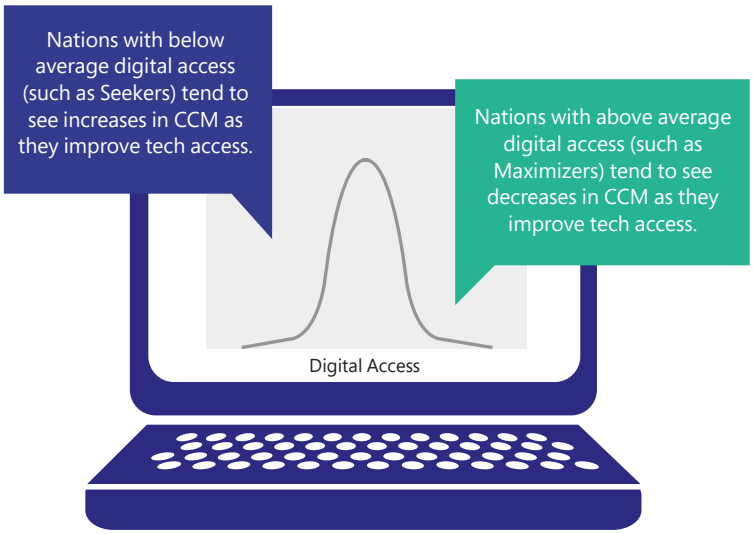
There is a paradox that stems from the modernization of ICT. While increased Internet access and more mature technological development is correlated with improvement in cybersecurity at the global level, it has the opposite effect among Seeker countries. To explain this effect, this study hypothesizes that there exists a tipping point in digital maturity after which increased access ceases to encourage the growth of malware and begins to reduce it.

This hypothesis suggests that countries with a developing level of ICT may be unprepared to secure their ICT infrastructure commensurate with the increase in citizen use of computer systems, which provides greater opportunity for malware to spread unchecked. Seeker countries are typically less mature in their security capabilities for newly deployed technologies, which explains why regional malware infection-rate increases are observed as digital access increases.

However, there appears to be a certain level of technology maturity at which countries develop enough technological sophistication that they can curb the growth of malware. Improving digital access after that point correlates with improved cybersecurity—the effect observed in more technologically mature countries.

Figure 5.

Hypothesized effect of maturing technology development on cybersecurity.



This hypothesis can be indirectly tested by correlating various technology development metrics with changes in the prevalence of malware, both in those countries whose adoption of technology is relatively low and in those countries where it is relatively high, using the model created in *Linking Cybersecurity Policy and Performance*.

This model shows a negative correlation in the more technologically mature countries between factors signifying ICT maturation and malware prevalence, suggesting that further maturation encourages improvement in cybersecurity. The correlations for those same predictors are positive among Seeker countries, supporting the notion that initial increases in digital access have a negative influence on cybersecurity among countries whose technology development is less mature, as depicted in Figure 6.

These correlations support the main tenets of the hypothesis. It is also important to note that this phenomenon does not suggest that less technologically mature countries with less digital access should decrease investments in ICT. On the contrary, crossing the tipping point is critical to both long-term improvements in cybersecurity and realizing the other benefits of expanding an information society.

Figure 6.
Correlation of Digital Access predictors with changes in the regional rates of malware infection in Seeker and Maximizer countries.

Figures are correlation coefficients, with values of 1 and -1 representing perfect correlation, and 0 representing no correlation.

For example, the table shows that as Broadband Penetration increases, Maximizers (countries that are more technologically mature) experience a decrease in malware (-.33), while Seeker countries (that are less technologically mature) experience an increase in malware (.68).

2011 Predictors of Digital Access	Technologically Mature Countries (Maximizers)	Seeker Countries
Secure Net Servers/Million People	.19	.86
Broadband Penetration	-.33	.68
Mobile Internet Penetration	-.19	.58
Internet-Enabled PC Ownership	-.34	.20

To help address these challenges, global ICT baselines can provide guidance for building cybersecurity capacities. These capacities include software development, the ability to respond to cybersecurity incidents, creation of supportive policies, and risk management. Microsoft's recent paper on national strategies for cybersecurity offers a good overview of some of these capacities.[9]

Building cybersecurity capacity in Seeker countries is critical to the long-term future of the Internet. The United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security recommended in its 2013 report that:

> States working with international organizations, including United Nations agencies and the private sector, should consider how best to provide technical and other assistance to build capacities in ICT security and their use in countries requiring assistance, particularly developing countries.[10]

Collaboration on capacity-building will benefit the global ICT ecosystem in several ways. First, increasing cybersecurity in Seeker countries expands opportunity for development, trade, and engagement between nations. Cybersecurity contributes to better critical infrastructure performance, as well as greater trust and stability in information systems. Increased trust in turn helps spur greater economic transactions and growth.

Second, increased cybersecurity also helps Seeker countries better manage risks, both internally, for their governments and citizenry, and internationally, by helping to ensure that the new ICT investments of the Seeker country do not become platforms for cybercrime. Focused capacity-building efforts around cybercrime policy development and law enforcement training can further equip Seeker countries to navigate the increased challenges of new ICT investments.

Third, increased cybersecurity expertise in Seeker countries helps the public and private institutions in these countries participate in the broader community of security experts and engage in a full range of protection, detection, and response and recovery activities. This participation helps contribute to global stability and the security of cyberspace.

Cybersecurity concepts may apply around the world, but they should be advanced with an appreciation for societal and cultural differences. It is essential to understand how the broad range of factors explored in this paper shape the cybersecurity environment.

9 Developing a National Strategy for Cybersecurity, Goodwin and Nicholas, 2013.

10 Report of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, page 10, June 2013. (http://aka.ms/GGE-Report)

To explore the question of how different countries approach cybersecurity, Microsoft recently developed a report, *Hierarchy of Cybersecurity Needs: Developing National Priorities in a Connected World*,[11] which looks at how countries seek to maximize the benefits of the Internet by matching their cybersecurity priorities to the needs of their citizens.

Conclusion and Recommendations

As information and communication technology continues to grow in importance, it is imperative for individual countries to make the needed investments in cybersecurity so they can fully realize its benefits. Though cybersecurity is contingent on a variety of factors that vary by country, nations can best position themselves for future improvement by focusing policy on areas that improve technological, social, and economic outcomes to benefit all citizens.

This paper reviews quantitative evidence to show that the fundamental underpinnings of ICT policy and cybersecurity are linked to other areas of development. And though those countries most in need of cybersecurity gains may experience early struggles in their digital journey, they can eventually come to enjoy positive outcomes, including the innumerable benefits of greater ICT development.

Microsoft urges governments to consider policies that support continued growth in ICT sophistication, access, and security, and as a crucial first step, to adopt a national cybersecurity strategy.

Microsoft recommends these seven practices as the basis for a national strategy.

1. **Develop a risk-based approach.** Assess risk by identifying threats, vulnerabilities, and consequences, and then manage it through mitigations, controls, costs, and similar measures.
2. **Set priorities.** Adopt a graduated approach to criticality, recognizing that disruption or failure are not equal among critical assets or across critical sectors.
3. **Coordinate threat and vulnerability warnings.** The strategy should recommend that government and the private sector partner to create a threat-and-vulnerability warning model.
4. **Build incident-response capabilities.** Establish incident-response practices for the most critical and significant cybersecurity incidents.
5. **Educate the public.** Developing a knowledgeable, sophisticated cybersecurity work-force is critical to reducing national cybersecurity risk.
6. **Invest in research and technology.** A research and technology agenda to promote advances in cybersecurity, cryptography, applied mathematics, and related fields is critical.
7. **Think globally.** Integrate international standards to the maximum extent possible, keeping the goal of harmonization in mind wherever possible.

Microsoft looks forward to engaging with government policymakers and sharing its perspectives on the critical challenge of strengthening national approaches to cybersecurity.

11 Hierarchy of Cybersecurity Needs, Oxford Analytica, 2013. (http://aka.ms/hierarchy-of-needs)

Appendix: Developmental Metrics

Indicator	Description	Source
Broadband Penetration	Fixed broadband connections per 100 people	International Telecommunication Union **aka.ms/ITU-Broadband-Stats**
Broadband Speed	The contracted capacity of international connections between countries for transmitting Internet traffic	World Development Indicators **aka.ms/WorldBank-Dev-Indic**
Corruption	Corruption perceptions index relates to perceptions of the degree of corruption as seen by business people and country analysts, and ranges between 10 (highly clean) and 0 (highly corrupt).	Transparency International **www.transparency.org/cpi2012/results**
Demographic Stability	Pressures on the population such as disease and natural disasters make it difficult for the government to protect its citizens.	Failed States Index **ffp.statesindex.org**
Facebook Usage	Number of Facebook users	Internet World Stats **www.internetworldstats.com/facebook.htm**
GDP per Capita	Gross domestic product per capita, current prices	International Monetary Fund **aka.ms/IMF-Data-2012**
Government Type	The extent to which a society is autocratic or democratic	Polity IV **www.systemicpeace.org/GlobalReport2011.pdf**
Internet-Enabled Computers	Percentage of households possessing a broadband Internet-enabled computer	Euromonitor International **www.euromonitor.com**
Literacy Rate	Adult literacy rate	Euromonitor International **www.euromonitor.com**
Market Size	Domestic consumption plus country exports minus country imports	World Development Indicators **aka.ms/WorldBank-Dev-Indic**
Mobile Broadband	Active mobile-broadband subscriptions per 100 inhabitants	International Telecommunication Union **aka.ms/ITU-Broadband-Stats**
Population	National estimates	Euromonitor International **www.euromonitor.com**
Productivity	Refers to labor productivity, that is, the output of goods and services in the economy per employed person	Euromonitor International **www.euromonitor.com**
Regime Stability	The number of years since the most recent regime change	Polity IV **www.systemicpeace.org/GlobalReport2011.pdf**
Regulation	Measures the extent of regulation within the business sector and captures general regulation with respect to investment and competition	World Bank Governance Indicators **aka.ms/WorldBank-Dev-Indic**
Rule of Law	The extent to which individuals within a society respect property rights, the police, and the judiciary system, as well as the quality of police and legal safeguards	World Bank Governance Indicators **aka.ms/WorldBank-Dev-Indic**
Secure Net Servers	Secure Internet servers per one million people	World Development Indicators **aka.ms/WorldBank-Dev-Indic**