

Information Security and Privacy In Emerging Economies.

Implications for Global Competitiveness



Prepared by:

Brian Fitzgerald
RSA, the security division of EMC Corporation

Introduction

It has become almost cliché today to note that the internet and the digital technologies that comprise it have transformed the world around us. The ability to manipulate, share and manage information has changed the ways in which we live, work and play—and continue to change them at an accelerating rate.

The internet and World Wide Web have created a digital world without borders. Our tendency is to think of the impacts of the internet age on us as individuals: both positive, such as increased access to information, easier communication and simpler commerce, and negative, such as the erosion of privacy, or the threats of online fraud, identity theft or the outsourcing of jobs to far-away lands. But the impact of the digital revolution is just as telling on nations as it is on individuals. This new hyper-connected world offers huge opportunities for developing nations: new access to ideas and capital, and new opportunities for commerce, education and global relevance. However, this world without borders is also a world without privacy or ‘separation’ for nations and economies. Only a few generations ago, a nation could develop a nascent industry to maturity, forge an ideology and nurture the education of its young, all in relative isolation, separated by the world’s oceans, mountain ranges and by the limits of our transportation infrastructure. Today we live in a crowded global village where worldwide competition is a reality from ‘day one’ of a new industry and where thought processes, educational strategies and ideological debates are exposed to a global influence almost from their moment of creation.

These phenomena have especially significant impacts on emerging nations and economies. Unlike today’s developed nations, these emerging economies are not afforded the luxury of separation in any form. They must develop their means to create wealth in the shadow of a pervasive global influence. And they must evolve their approaches to privacy, intellectual property, and commerce in light of the requirements of the global, interconnected community in which they must live.

The Evolution of Trust in the Digital World

The digitization of commerce, communication and collaboration, and the blurring of borders and boundaries it entails, drive change in some of the most fundamental aspects of interaction between people and between nations. One of those aspects is the nature of trust itself. This paper will explore the various dimensions of trust as they apply to the digital realm, and how those dimensions apply to the strategies and needs of nations that are emerging into prominence on a global scale.

“Trust is essential to the efficient activity of an economy or other social system; without it a system is burdened by skepticism, uncertainty, and friction, all of which constrain and may even destroy it.”

Timothy Grayson

Why Does Trust Matter?

Trust, while amorphous in some ways, is a crucial lubricant to the machinery of society. Trust in the privacy of communication is key to the honest sharing of ideas. Trust in the intentions and actions of others is the key to trade and commerce. And trust in the safety of our bodies and property is the key to nearly every form of social behavior. As Timothy Grayson wrote, “Trust is essential to the efficient activity of an economy or other social system; without it a system is burdened by skepticism, uncertainty, and friction, all of which constrain and may even destroy it.”

In the non-digital world, humans had thousands of years to develop the senses, systems and frameworks that enable trust to be assumed between people, governments and corporations. Those systems of trust enabled global trade, freedom of speech, and open sharing of ideas and information. While not perfect, these systems of trust were sufficient to grease the wheels of our society, facilitating trade, collaboration, invention and education.

The rapid rise of the digital infrastructure has strained many of these systems of trust for even the most developed economies. The acceleration of trade and communication on a global basis via electronic means has broken down many of the systems and even customs that had stood us well for thousands of years. Even only a few decades ago, nearly all business had a major face-to-face dimension, every deal negotiated over multiple sit-downs, and sealed with a ‘handshake’ between individuals.

Today companies and individuals communicate over public networks, with their most private information stored in servers in locations they may never know. Massive volumes of trade occur between automated systems with no human intervention. Ideas and creative work product become easily fungible in their digital form, and easily stolen by competitors and perhaps aggressive nation-states.

The result is a growing contradiction: even as the rate of global trade and online communication grow, the levels of trust in the safety of the digital realm often decrease due to fraud, exposure of personal information, misuse by governments, and increasing media coverage of these forms of malfeasance.

Much as certain countries gained global reputations for trust and privacy in financial dealings, and thus became the bankers to the world, opportunities exist for countries to become global brands in the trustworthiness of their infrastructures for collaboration, commerce and communication.

Emerging economies are faced with a double challenge: building their infrastructure to compete globally, and establishing credibility on a global stage for their ability to be trustworthy stewards of digital economy. High levels of trust will lead to increased collaboration with trading networks, drive increased innovation and invention, and speed the development of scholarship and rich communication. Low levels of trust will result in the opposite; a citizenry that cannot leverage the productivity benefits of the internet and the tools it has produced, and a business community that finds it difficult to conduct profitable trade on a global scale.

Emerging economies also are presented with a significant opportunity. The rapid transformation to a digital economy and global society has leveled the playing field in many ways. By creating the right policies and infrastructure for trust in a digital world, they have the chance to become world leaders in this area. Much as certain countries gained global reputations for trust and privacy in financial dealings, and thus became the bankers to the world, opportunities exist for countries to become global brands in the trustworthiness of their infrastructures for collaboration, commerce and communication—the ‘Switzerlands’ of the digital economy.

The Hyper-extended Enterprise and the Hyper-extended Nation

Over the past decade a new kind of enterprise has evolved. We have defined this as the 'hyper-extended enterprise'. This new form of enterprise marketed by its massive interconnection and extension along four dimensions:

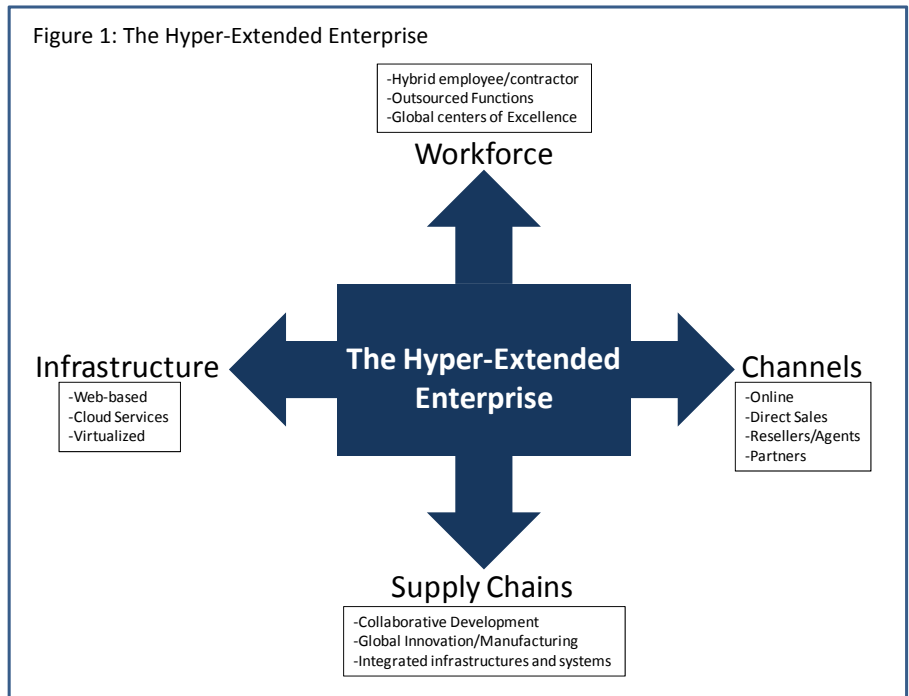
Workforce: the hyper-extended enterprise has blended workforce of employees, contractors, outsourcers and even partners, all of who participate fully in the value chains of product development, service, sales and business operations.

Channels: these hyper-extended enterprises reach their customers or constituents through many channels, from direct touch and online interfaces to distribution partners, agents or subcontractors.

Supply Chain: these enterprises count on a long global supply chain, not only for raw materials and products, but for ideas and best practices.

Digital Infrastructure: these enterprises are leveraging advances in technology ranging from mobile devices and social media to cloud computing and virtualization. They have blurred the boundaries of their own digital infrastructure to create agile IT infrastructures for communication and collaboration.

A recent report by International Data Group and RSA, the security division of EMC Corporation, identified the following: "Businesses are rapidly embracing new tools and technologies including cloud computing, social networking, virtualization, and mobile communications, the breakdown of the traditional boundaries that surround organizations and protect their data assets. The result is the "hyper-extended enterprise." Although this evolution is helping companies achieve strategic goals such as cutting costs, boosting innovation, and improving internal and external communications, it's also potentially exposing them to information security risks." (IDG MarketPulse Report, "As Hyper-Extended Enterprises Grow, So Do Security Risks").



Enterprises have become ‘hyper-extended’ to leverage the benefits of digital technologies and to compete effectively on a global basis. Nations are now undergoing the same transformation.

The dynamics of the hyper-extended enterprise are instructive for nations seeking to be bigger players on the global digital stage. Nations also are becoming hyper-extended along many of these same dimensions. This is occurring not just in commerce, where their domestic corporations and industries become hyper-extended to compete and thrive globally. Collaboration, communication, and education also are becoming hyper-extended. This phenomenon creates great opportunity and efficiency, but also exposes national policies and infrastructure to the same requirements and risks with which today’s hyper-extended enterprise are already contending.

So just as today’s global enterprises have had to develop sound policies, practices and technologies for ensuring security, privacy and ‘trust’ in a hyper-extended digital environment, today’s nations must do the same to be effective competitors and contributors on a global scale.

Just as today's global enterprises have had to develop sound policies, practices and technologies for ensuring security, privacy and 'trust' in a hyper-extended digital environment, today's nations must do the same to be effective competitors and contributors on a global scale.

Ensuring Trust for the Hyper-extended Nation

Nations that excel in taking advantages of the opportunities of 'hyperextension' can thrive. They can lower their costs, increase rates of innovation, and provide the environment for their industries and citizens to thrive. So what are the key attributes of trust for the hyper-extended nation? There are three that will be considered in this paper: Digital Policy, Digital Infrastructure, and Digital Culture.

Digital Policy:

The hyper-extended nation must develop policies for the protection of information, ideas that encompass the unique challenges and requirements of a digital world. Legacy policies and laws often constrain the productivity and innovation benefits possible in a digital economy. Modern concepts such as cloud computing for example, promise to lower the costs of computing by moving information processing and storage fluidly around the globe to balance workloads and lower costs. In many nations however, these capabilities run headlong into decades or centuries-old laws that require physical 'possession' of certain kinds of information by companies and governments. In a paper-based world, information could easily be defined by a physical location. In a digital world, physicality becomes moot, and new thinking is required to construct policies that can protect privacy, but enable the productivity gains of innovations such as cloud computing.

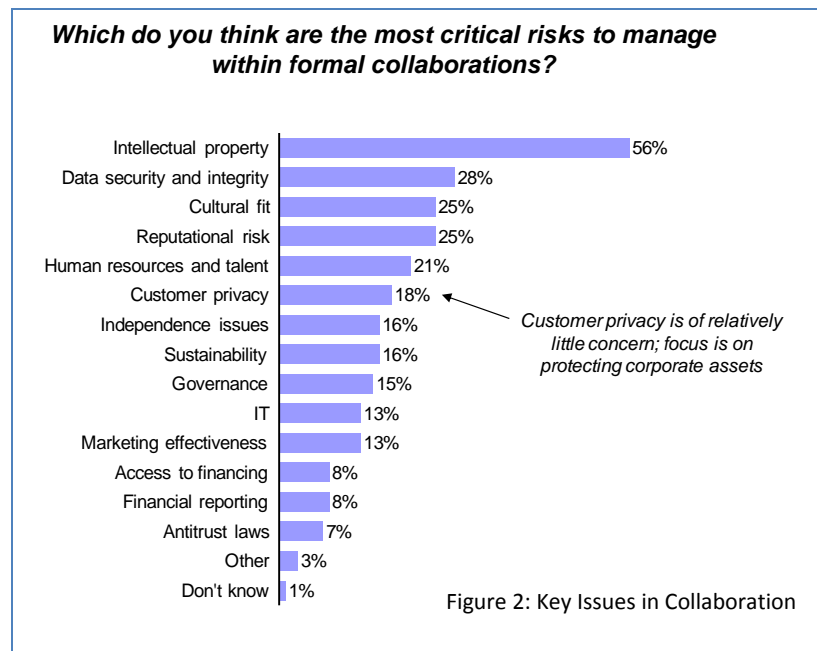
These issues are not just issues for emerging economies. The French Data Protection Authority (La Commission Nationale de L'informatique et des Libertes) fined Tyco Healthcare France, the French subsidiary of a large U.S. multinational corporation, 30,000 Euros in connection with its use of a global human resources database to transfer employee data from France to the United States.

While this action was taken in the interest of enforcing French privacy laws, clearly this sort of restriction can put a damper on the efforts of corporations to do business in certain countries where such laws are too onerous. For larger developed or emerging economies, the financial benefits most often outweigh

the risk or added costs associated with such regulations. But for emerging economies without large, attractive consumer or commercial bases, policies and laws constructed with the mobility of digital information in mind can make a nation a more favorable location for multi-national corporations looking to expand their operations and facilities. Just as taxation has often been a key consideration for companies researching new locations, digital privacy laws and the ease of leveraging modern technology is emerging as another important factor.

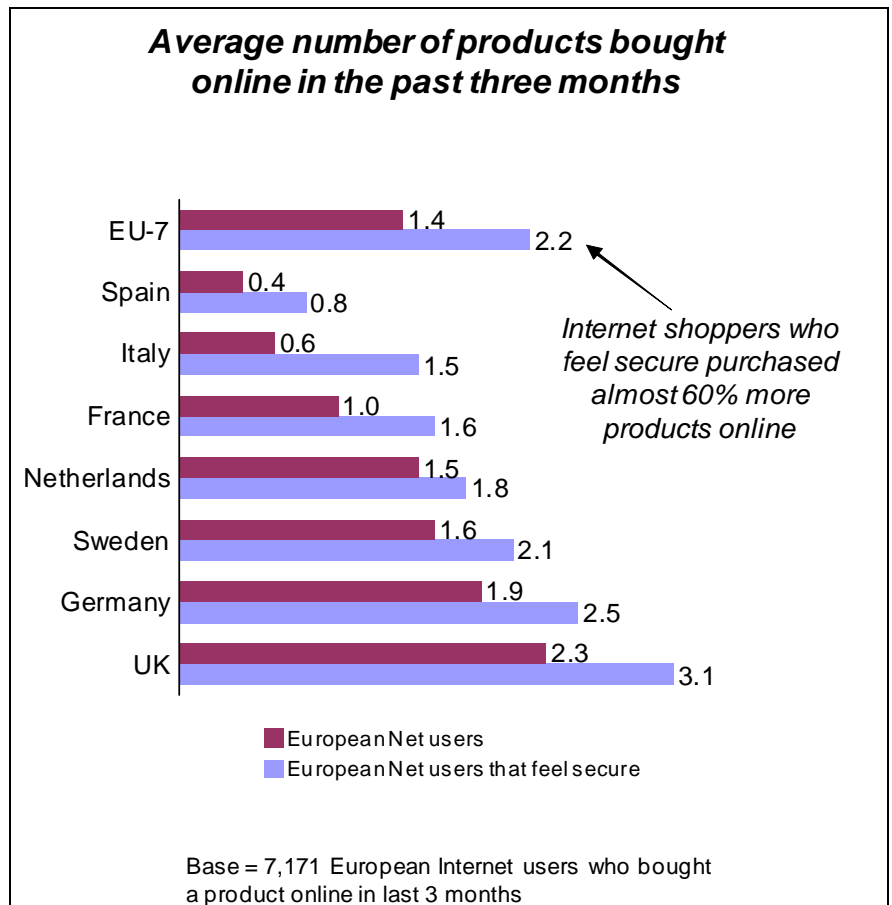
Conversely the hyper-extended nation also can benefit from laws that protect privacy and ownership of digital information in ways that promote innovation, collaboration and commerce. Digital information can easily be replicated and modified. This malleability and mobility becomes a challenge in enforcing intellectual property protection and copyright law. As organizations look to extend their collaboration networks globally, they must consider the extent to which the nations in which they operate protect the intellectual property created by this global collaboration. Laws protecting intellectual property and the global innovation networks that will create it can become important factors in establishing a nation as a trusted part of a global supply chain or innovation network.

Laws protecting intellectual property and the global innovation networks that will create it can become important factors in establishing a nation as a trusted part of a global supply chain or innovation network.



In a Survey of 158 senior executives of large enterprises protection of intellectual property and data security are seen as key concerns for those considering formal collaborations. (Source: PriceWaterhouse Coopers).

In the face of increasingly-sophisticated online fraud occurring globally, trust is essential for citizens of any nation to transition their personal behaviors and practice to the digital domain with confidence. Participation in the global digital community and its benefits, whether it is for online banking, social media, education or communication, will be limited unless nations create effective laws and promote the knowledge and technology adoption needed for safe use of the internet by its citizens. Research by Forrester Research has shown a correlation between confidence in the security of online commerce and the amount individuals will spend online. Logic would hold that the same relationship applies to use of social media tools and other internet-based capabilities. Unless emerging nations are able to help their citizens gain the technologies and skills to use these capabilities with confidence, they will suffer a decided disadvantage over time.



Source: Forrester Research

Figure 3: The Impact of Online Trust on E-Commerce

Protecting Intellectual Property and Enabling Collaboration: A Technology Snapshot:

Promoting the use of advanced technologies for Data Loss Prevention (DLP) can serve to help enterprises gain reputations for trusted collaboration. DLP technologies identify sensitive information within a data center or personal computer, or traveling over a network, and implement controls to ensure that policies governing that information are enforced. Using DLP technologies, information such as employee personal data, credit card numbers or even computer-based engineering diagrams can be protected from accidental disclosure or intentional theft, while still enabling sharing of the information by trusted parties for collaboration or commerce.

Protection of ideas and communication is a key element of education and scholarship. In modern economies, there are increasing ties between educational infrastructure and industry. Digital economies depend on a steady flow of highly educated workers. But they also increasingly collaborate with educational institutions for basic research and innovation. Building a culture of scholarship and free flow of ideas is crucial to enabling this sort of virtuous circle. Policies and infrastructure that enable the free flow of ideas in a climate of trust and privacy is a crucial foundation to a success in an emerging digital economy.

Digital Infrastructure:

Hyper-extended nations must provide the digital infrastructure that enables this sort of global collaboration. Digital infrastructure must support massive information flows, ensure high availability, and be agile enough to evolve at the speed of the internet.

But the digital infrastructure itself, like the policies that impact it, must be designed to enable the elements of privacy, security and trust described above. Some nations today continue to restrict the use of technologies, such as encryption, in ways many believe are efforts to ensure their ability to monitor communication within their nations. Such restrictions on technology destroy this environment of trust and serve to create massive friction in the ability to conduct trade or collaboration, and limit the attractiveness of these nations to the larger global economy. In order for enterprises and nations to be able to compete and

Strategies for ensuring trust based on personal contact or cultural similarity for example, are no longer as relevant in a world where collaboration and commerce can happen between individuals thousands of miles apart, who may never meet and who come from radically different cultural backgrounds.

collaborate globally, all other parties must be able to work in an environment of trust and assurance of confidentiality.

The technologies for ensuring privacy and security in the digital domain exist today. Nations that not only permit broad use of these technologies but build reputations for excellence in their use will gain tremendous advantage in their ability to attract talent, foster innovation and enable their industries to compete successfully in the global digital economy.

Ensuring Privacy with Shared Devices: a Technology Snapshot:

In emerging economies, digital infrastructure (PC's, internet access points) are often shared by multiple people. How then does one ensure privacy and confidentiality for students and researchers using shared devices for schoolwork or innovation? Desktop virtualization offers a solution. With virtualization, the computing environment a person is using is no longer tied to a physical device such as a PC or server. Virtualization allows many applications or individuals to share a computing platform, with each perceiving that they have sole access to the device and its resources. With desktop virtualization the computer 'image' that a person uses—his or her preferences, applications and data—are not stored locally but are retrieved when needed from a centralized, highly secure server. This means when a student logs onto a shared device, they can use secure credentials (passwords, private phrases, and other forms of security) to retrieve the 'image' and do their work. Upon completion of their work, they log off the system, and the image disappears from the local device, ensuring no following users can access the information, logs or other data with which that student had been working. Desktop virtualization can enable many shared users of physical devices, while maintaining privacy and personalization for each individual, making it an ideal technology for education and research in locations where technology such as PC's is scarce.

Without a cultural mindset and objectively-determinable understanding accepted behavior, the trust environment becomes opaque to digital systems and processes, making trade and collaboration difficult at best.

Digital Culture:

The cultures and practices of today's societies must in some ways evolve to more easily embrace the somewhat abstract and 'impersonal' nature of the digital world. Strategies for ensuring trust based on personal contact or cultural similarity for example, are no longer as relevant in a world where collaboration and commerce can happen between individuals thousands of miles apart, who may never meet and who come from radically different cultural backgrounds. The nations who can preserve their culture while learning to adapt certain traits to be successful in a digital environment serve to gain a global advantage.

China can serve as an example of the conflict between traditional approaches to determining 'trust' and the methods required by a digital economy. In a paper titled Relationship-based e-commerce: theory and evidence from China, Maris G. Martinsons writes: "The inability to rely on universal rules and impartial courts, especially when state agencies are involved, has forced the Chinese to rely greatly on guanxi (Xin & Pearce, 1996; Seligman, 1999). Guanxi are relationships or connections between two or more people (or organizations) in which each can prevail on the other(s) for help. The Chinese 'do not (particularly) love guanxi' (Li & Li, 2000), but they must depend on it in the absence of systematic rules. Institutional deficiencies encourage people in China to do business with those that they know and trust – family, friends, classmates and others in their in-group or guanxiwang (network of connections). Guanxi lubricates the early stages of business and provides psychological comfort in dynamic and uncertain environments. New business partnerships commonly result from informal recommendations by existing in-group members. Those making recommendations have strong incentives to be reliable and accurate because their personal reputation is at risk."

Martinson goes on to point out that in China "Trusted partners can rely on 'handshake agreements' in lieu of formal contracts. Since those with the right guanxi can break or at least bend written rules (Seligman, 1999, p. 35), business conduct in China is often judged in terms of being reasonable, 'heli', rather than strictly legal – 'hefa'".

Trust will be a currency that is traded by individuals, enterprises and nations, as they look to further their aims on the global stage

Guanxi, and the concept of 'reasonable' vs 'legal' works well in localized economy where relationships can be personal, and where large bodies of past shared experience can be used to build trust and determine what is 'reasonable'. But in a global, digital economy where those factors do not exist, new cultural mindsets, and new standardized means for creating trust, must be developed. Without a cultural mindset and objectively-determinable understanding of accepted behavior, the trust environment becomes opaque to digital systems and processes, making trade and collaboration difficult at best.

One can imagine mergers of technologies such as social media with classic relationship concepts such as guanxi to enable shared experience and personal connect to be created between people that may never meet personally. But a marriage of those technologies and a culture that enables trust in a more abstracted digital environment will be essential to nations looking to evolve to become leaders in the hyper-extended global economy.

Establishing Trust in Online Interactions: A Technology Snapshot

Humans use a variety of methods to establish trust with other individuals or organizations. We rely on personal experiences, references from trusted sources, and inspection of the behavior of the other party for its appropriateness to the situation as just some of those methods. Technology today can reproduce some of those methods to ensure trust in digital interactions: Risk-Based Authentication and Adaptive Authentication technologies create risk scores based on many factors such as familiarity of the identity, consistency of behavior and even the geographic location from which someone is trying to access a system or sensitive information. High risk scores trigger more in-depth security controls. Transaction monitoring capabilities can look at actions of a person on a website and determine if those actions fit their usual course of behavior. Unusual behaviors (such as trying to transfer funds to an offshore account) would also trigger increased security. And technologies such as digital certificates can help make sure devices such as PC's and PSA's have legitimate privileges to the systems they are trying to access.

Conclusion:

Commerce, collaboration and communication have, throughout time, been enabled or hampered by the environment of trust, security and privacy in which they occur. In an increasingly fluid, interconnected global community, the ways in which we create trust, ensure privacy and provide security must evolve, and must take advantage of available best practices and advanced technologies. Trust will be a currency that is traded by individuals, enterprises and nations, as they look to further their aims on the global stage. And the ability of a nation to ensure these factors in a rapidly advancing digital environment will in part determine its success in creating wealth, prosperity and significance for its citizens and itself.

Three major factors will be important to earning that currency for nations in the digital realm: policies that enable free flow of information while protecting ownership and confidentiality; technologies that enable information protection, prevent fraud and ensure confidentiality; and a cultural mindset that can evolve its traditional values and means of ascertaining trust to function effectively in the abstracted world of the internet.

The rapid digitization of communication, collaboration and commerce can level the playing field between nations. The nations that most effectively take advantage of this opportunity by developing excellence on the factors described above can become leaders in the global economy, and create massive value for their citizens and the world community.

###