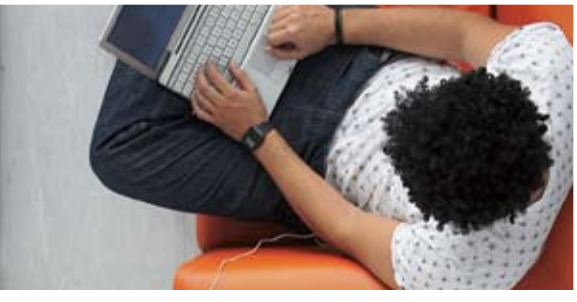
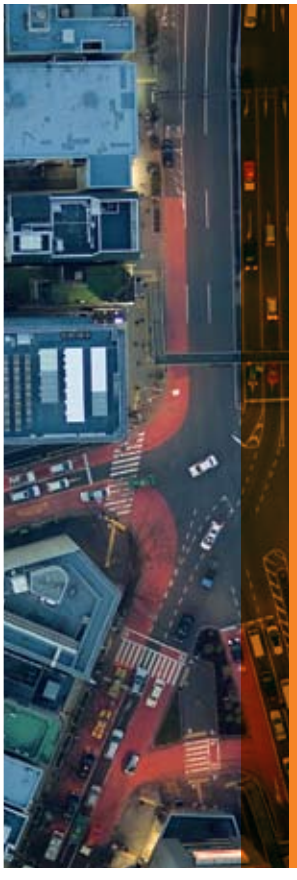
Security & Society





A GLOBAL
INNOVATION
OUTLOOK
REPORT

Nicholas Donofrio
IBM Executive Vice President
Innovation and Technology

It is one of the great paradoxes of the digital age. Tremendous advances in technology provide businesses, governments and individuals with an unprecedented capacity to ensure their safety and security. At the same time, the tools and methodologies available to disrupt society and to compromise assets have never been greater.

So it comes as no surprise that security is an inconvenient but fundamental fact of life. Practicing good security takes time, discipline and money. Little wonder that securing the physical and digital assets of our clients, business partners and employees has been a significant part of IBM's business for decades.

But providing security in this era of globalization takes more than one company, or even one government. Security in the 21st century requires a concerted, collaborative effort between businesses, governments and individual citizens. It requires that we push intelligence out to every edge of these networks, gather and analyze information in real time and react faster to all threats. In short, providing security today requires that we all get smarter.

The good news is that we have the technology and tools to do just that. Cultural and bureaucratic barriers aside, the ability to quickly capture, analyze and cross-reference security data of all varieties exists today and is already making a difference in the world. Take the example of the Operational Riskdata eXchange Association (ORX), a group of 42 banks from 14 countries that share operational risk data to improve their planning and prediction of risk. To feel comfortable sharing this sensitive information, the banks use powerful anonymization technology to protect their identities from each other.

Throughout the pages of this report, you will see many examples like that of ORX, where businesses, governments and individuals are doing their respective parts to improve global security. You will also read about many areas in which security is still inefficient and in dire need of innovation. Indeed, there are many opportunities to get smarter about security.

The Global Innovation Outlook is designed to facilitate collaboration and openly share the many insights from its participants. But this report is only the beginning of the conversation. We hope the essays in this report spark new ideas, businesses and partnerships going forward that endeavor to solve the world's most vexing security problems. The real work starts now.

Nicholas Donofrio
IBM Executive Vice President
Innovation and Technology

Security & Society

Society owes its very existence to the basic human need for collective security. In this way, security and society are synonymous. Without one, the other ceases to be.

But the relationship between security and society has grown increasingly complex and dynamic over the last two decades. Never before has the balance between the two been more in flux, as globalization, interdependence and digital technologies have literally reshaped the foundations of society, challenging every accepted approach to its security.

Today, we are a truly global society, traveling freely and conducting business without borders over a communications network that connects virtually every person on the planet. The speed with which this change has taken hold has created unprecedented opportunity, both legitimate and otherwise. As business models and lifestyles have migrated from the physical world to the digital world, so too have criminal elements and other destabilizing forces.

It's all part of the inevitable security power struggle and the reason why truly complete security is not an attainable goal. Perhaps this is why many believe that security strategies should focus more on resiliency, or the ability to absorb and respond to attacks, rather than hardening perimeters and securing boundaries. Or that society needs to take a more distributed approach to security, empowering and enabling each of the world's security stakeholders to take more responsibility for the collective.

On the following pages, you will find a more detailed description of the concept of distributed security, as well as further insights culled from a series of six brainstorming sessions, or "deep dives," that IBM convened around the world in 2008. These meetings brought together business leaders, government officials, entrepreneurs, academics and nonprofits to ask the hard questions about the future of security.

The end result of this effort is not, of course, a solution to the world's security problems. This report is instead a collection of innovative security strategies for a globally connected world, strategies in which every government, business and citizen has a role to play.

"Society moves faster and is more complicated today than ever before. We expect access to communications and information anytime, anywhere, on any device. And security threats are constantly attempting to undermine these services. That's why it takes a monumental effort to secure the infrastructure that supports that capability. And why it's monumentally important that we do it well."

—Ken Silva
Chief Technology Officer
VeriSign, Inc.

MORE THAN 1.2 MILLION LEGAL AND ILLEGAL IMMIGRANTS SETTLE IN THE UNITED STATES EACH YEAR.

The Network Effect

Tapping into the power of distributed security

Globalization has supplied us with a new breed of security threat: those that know no geographical boundaries. Online attacks can emanate from anywhere, and target anyone. Geographical borders are easily crossed. And global communications are cheap and easy. In this new era of global interdependence, the amount of damage that one individual can do is far greater than at any time in history.

IN 2007, THE GOVERNMENT OF ESTONIA WAS GROUND TO A HALT BY MASSIVE DENIAL-OF-SERVICE ATTACKS.

THE RUSSIAN BORDER IS 57,792 KILOMETERS IN LENGTH AND COMES IN CONTACT WITH 14 DIFFERENT COUNTRIES.

FIVE UNDERSEA CABLES WERE CUT IN EARLY 2008, AFFECTING COMMUNICATIONS SERVICES TO MILLIONS. CAUSE IS STILL UNKNOWN.

INTERNET USAGE IN BRAZIL INCREASED BY 1,000 PERCENT SINCE 2000, WITH 50 MILLION USERS ONLINE THIS YEAR.

It is called **the network effect**, in which the harmfulness of a single threat is exponentially proportional to the number of people exposed to it.

To date, the network effect has worked in favor of the bad guys. They have harnessed and exploited this new digital reality, and they themselves have become a network of formidable strength and speed. For example, 94 percent of all browser-related online exploits occur within 24 hours of a vulnerability being disclosed. These so-called "zero-day" attacks provide further evidence that the traditional centralized, command-and-control approaches to security are no longer sufficient in this fast-paced, constantly changing networked environment.

But there is a simple and powerful notion taking hold among the security elite that may finally turn the tide. "To fight a network, you need a network," says Katharina von Knop, Assistant Professor, University of the Armed Forces, Munich.

And why not? After all, there are presumably more "good guys" in the world than bad. By empowering these individuals, businesses or governments with the knowledge and technology necessary to share the responsibility of good security, thousands of threats could be mitigated and security costs could be dramatically reduced. By moving flexible and adaptive security intelligence out to the edges of the network, you achieve something we are calling "**distributed security**." And whether you work in government, the private sector or are just a regular tax-paying citizen, it's a critical step toward crafting new security strategies that are more aligned with the digital era.

GLOBALLY CONNECTED

1.4 billion people use the Internet.
More than **1 billion** people travel internationally each year.
More than **$12.5 trillion** in global trade changes hands every year.

"To fight a network, you need a network."

—Katharina von Knop
Assistant Professor
University of the Armed Forces, Munich

REGIONAL VIEW:
MOSCOW GIO DEEP DIVE
55°45′N 37°37′E
POPULATION: 10,382,754
AREA: 1,081 KM² (417 SQ MI)

In Moscow, participants felt that Russia had many valuable lessons on global security to share with the world. This was the first location where the idea of community-based security was broached, and the idea that towns, villages, families and individuals all have a role to play in improving security. Also, many participants felt that the responsible and innovative management of Russia's vast energy supplies would be the greatest contribution the country could make to global security.

Common Law

Considering the Internet is only a few decades old, it's not surprising that the security systems that guard this digital realm are less evolved than those that govern the physical world. In fact, many of the terms used to describe Internet security are still borrowed from the lexicon of physical security: firewalls, backdoors, patches and so on.

But for a medium as distributed and populist as the Internet, putting up walls hardly seems an appropriate response to the rapidly evolving security threats that plague it. That's why many GIO participants advocate the idea of **community-based security**, in which online groups that share a common interest police themselves, sensing and responding to threats as needed.

"Could there be a time in the future when bad behavior is punished by the community?" asks Pat Conley, Senior Vice President of Product Development at VeriSign. "On a very small scale you see this in forums and other online communities already, and this kind of self-imposed punishment is a way in which the community lays down the law."

For better or worse, the idea conjures up images of the puritanical village in Nathaniel Hawthorne's novel ***The Scarlet Letter***. But these communities can take a variety of forms: a company; a political party; a social network. And in the digital world, communities are even more fluid and self-selecting. The only requirement is that the group share a common set of values.

To some, being judged and policed by a group of peers is a more appealing option than being policed by governments or local law enforcement agencies. But even some advocates of the idea have serious reservations. "I like the idea of community-based security and having many eyes and ears," says Hiroshi Maruyama, Director of IBM's Tokyo Research Laboratory. "But can we trust a community? Do they have real wisdom? Or are they just a mob?"

Q&A

Gunter Ollman_Chief Security Strategist

IBM Internet Security Systems

It's easy to be skeptical about self-policing. How does it work?

"In World of Warcraft, for example, players assign each other rankings based on reputation and contribution. If someone insists on being disruptive and not playing by the rules, they will find themselves quickly ostracized by the group. There are even organized "vigilante" groups that will track down chronic abusers of the rules, regardless of changes in their in-game identities, and publicly post records of their behavior as a warning to others. Once you build up a bad reputation, it becomes very hard to escape it."

Wireless Watchdogs

When it comes to empowering individuals to assume security responsibility for themselves and their community, perhaps no single device holds more potential than the mobile phone. Never before has such a powerful and versatile tool been placed in the hands of billions of people around the world, in both developed and developing regions. They are personal, location-aware and able to send and receive invaluable security information. This unique blend of characteristics makes the billions of wireless devices around the globe a **massive untapped arsenal** in the battle for good security, both physical and digital.

> "The mobile phone can be a key instrument for enabling secure transactions."
>
> **—Ingo Noka**
> Head, Visa Payment Security in Asia Pacific, Visa

Already mobile phones are being used to receive regional security alerts. In March, when a dangerous criminal escaped from a maximum security prison in Singapore, the government sent alerts and photos of the man to all mobile phone subscribers in the area.

In addition, mobile phones will soon become powerful tools for verifying a variety of financial transactions. "The mobile phone can be a key instrument for enabling secure transactions," says Ingo Noka, Head, Visa Payment Security in Asia Pacific, Visa, who is based in Singapore. "They are always connected to the network, they have processing power and practically everyone has one. In fact there are 3.3 billion mobile phones in the world today, compared with 1.6 billion Visa cards. Mobile phones are also ideal as another authentication tool as they are capable of dynamic passwords, and you can use them to alert consumers of the possibility of a fraudulent transaction."


There are more than 3 billion mobile phone subscribers worldwide...


FINGERPRINT CAPTURED
GOVERNMENT BUILDING // 3:56 PM
BANK TRANSACTION VERIFIED
BANK ATM // 7:15 PM
...and each one of them has the potential to play a role in improving security.
IDENTITY AUTHENTICATED
BANK // 12:03 PM
LICENSE PLATE CAPTURED
STREET CORNER // 10:15 AM
TERRORISM ALERT RECEIVED
APARTMENT COMPLEX // 8:03 AM


RADIATION DETECTED
SUBWAY TUNNEL // 7:58 AM
RADIATION WARNING RECEIVED
REALTY BUILDING // 8:00 AM
VOICE AUTHENTICATED
INSURANCE COMPANY // 4:04 PM
MOBILE TRANSACTION VERIFIED
AUTOMOBILE // 11:30 AM
CREDIT CARD TRANSACTION VERIFIED
HOTEL // 2:34 PM

But it's the mobile phone's ability to sense and send information that has the security community most energized. With audio and video capability built into most new smartphones, the average citizen could potentially record suspicious activity and send it to the authorities. When hooked up to a CCTV network, mobile devices can offer remote security monitoring of your home or business. And looking further into the future, GIO participants suggested mobile devices could be equipped with miniature Geiger counters that constantly sense for radiation and relay the location information to anti-terrorist agencies, all without the active participation of the end user.

Some of the ideas are more fantastic than others, but the possibilities are endless. Of course, it's not all upside. Mobile devices bring with them certain security concerns of their own. They are easily lost and compromised. And the same characteristics that make them so valuable in fighting crime make them a useful tool for committing crimes. But perhaps the most disconcerting quality of mobile phones is that the security technology used to protect them is many years behind that used to protect PCs.

Mobile payments are expected to hit **$300 billion** by 2013.

The Secure Supply Chain

For the past two decades, businesses large and small have embraced the economic efficiency of global supply chains, spreading their operations to wherever the work gets done best. The savings have been immense. But there is a downside to the ever-lengthening global supply chain: it is complex to manage and nearly impossible to secure.

"The fragmentation of these supply chains has been so severe, the number of variables entering the system has become overwhelming," says Athol Yates, Executive Director at the Australian Homeland Security Research Centre. "Your company may have a full understanding of its own system, but not of the whole system. And there isn't one individual in the group that has that capability."

That's why Yates advocates more evenly distributing security responsibilities throughout the supply chain, increasing transparency from start to finish, and easing the burden on the customer-facing unit. By cultivating stronger vendor relationships and encouraging each link in the chain to shoulder a proportionate load, overall security can be increased, and costs can be decreased. One way to accomplish this would be to **make the supply chain smarter**, by having each vendor feed regular risk data into a central analysis engine, developing a kind of vulnerability dashboard to direct security resource allocation.

> "Your company may have a full understanding of its own system, but not of the whole system."
>
> **—Athol Yates**
> Executive Director
> Australian Homeland Security Research Centre

Of course, the shorter the supply chain—and more local—the easier it is to develop these relationships. Many companies are already beginning to reconsider the length of their supply chains over fears of so-called "resource nationalism," or the potential for part or all of their supply chain to be compromised because of foreign political action. And in the face of rising global transportation and manufacturing costs, the cost arbitrage that made big supply chains attractive in the first place is diminishing. All of which begs the question: Are small supply chains the next big thing?

Q&A

Athol Yates_Executive Director

Australian Homeland Security Research Centre

What is the state of security in the world's industrial supply chains?

"Security of supply chains is extremely variable, which reflects the fact that they are comprised of a variety of commercial, governmental and international organizations with quite different objectives. Just-in-time management, policies to reduce supply numbers and other factors which reduce the redundancy and flexibility of supply chains mean that a disruption in supply chains can quickly create serious economic consequences for individual companies, industries and even entire countries. Each organization needs to determine the correct balance of supply chain efficiency and security robustness."

The Sandwich Supply Chain

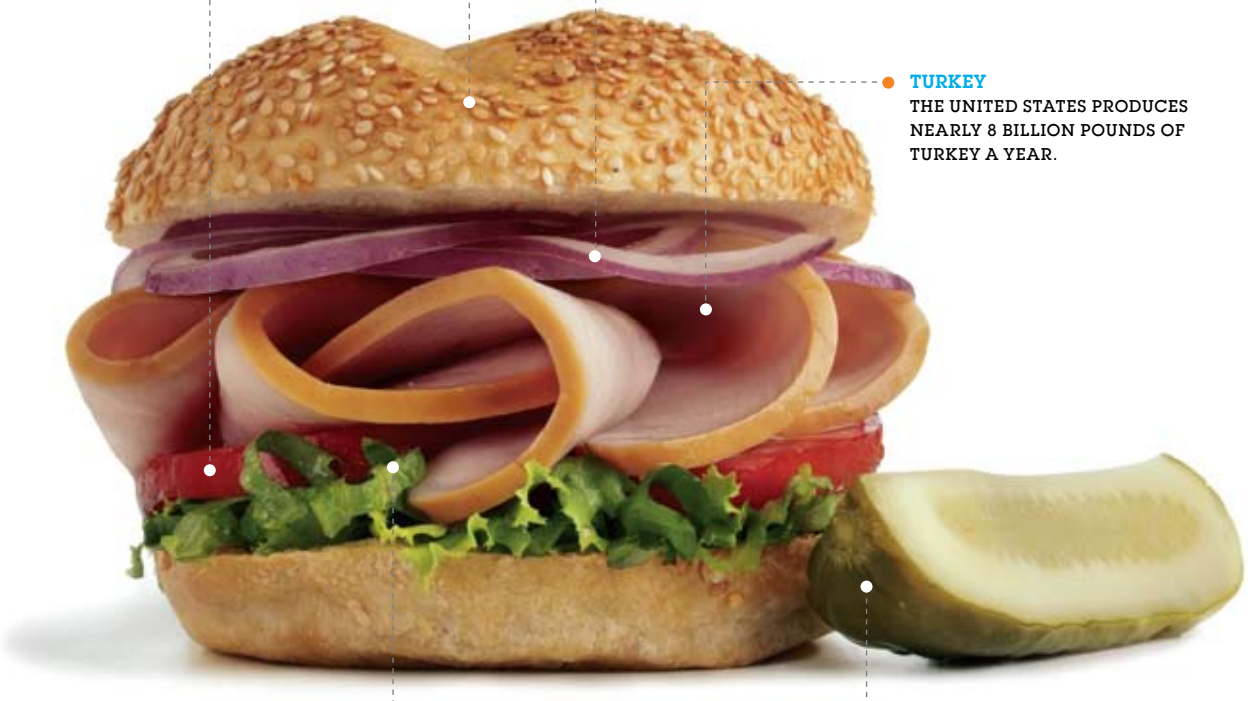
EVEN A SIMPLE DELI SANDWICH HAS FAR-FLUNG ORIGINS THESE DAYS.

SESAME SEEDS
70 PERCENT OF THE WORLD'S PRODUCTION OF SESAME SEEDS IS DONE IN ASIA.

TOMATO
CHINA PRODUCES 32 MILLION TONS OF TOMATOES EVERY YEAR.

ONION
ONIONS ARE PRODUCED AND EXPORTED FROM SIX DIFFERENT CONTINENTS.

TURKEY
THE UNITED STATES PRODUCES NEARLY 8 BILLION POUNDS OF TURKEY A YEAR.



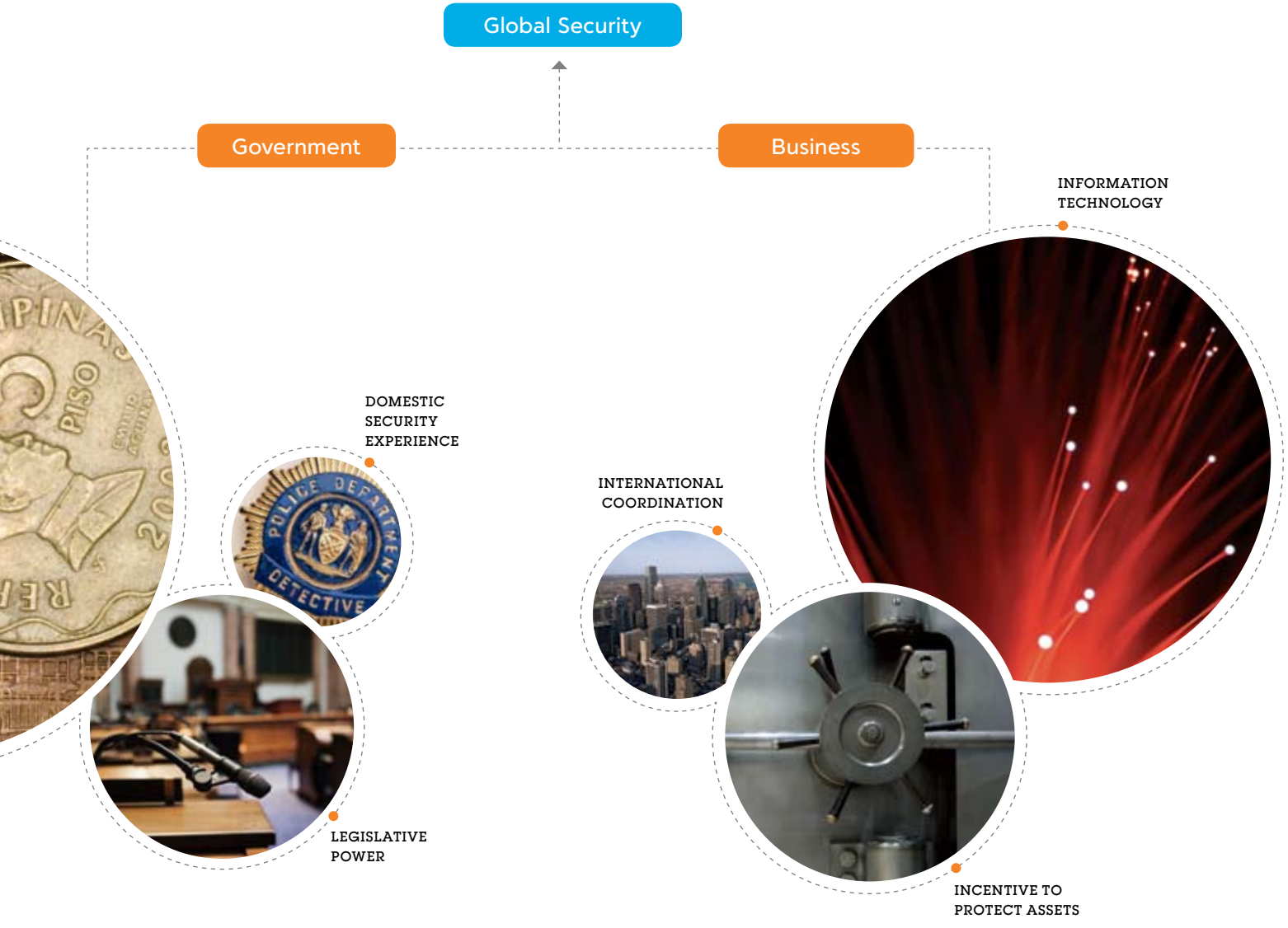
LETTUCE
LETTUCE IS EXPORTED FROM THE UNITED STATES, CHINA, MEXICO, EUROPE AND CANADA.

PICKLE
INDIA EXPORTS MORE THAN 65,000 TONS OF PICKLES A YEAR.

The New Roles

How governments and businesses must adapt to the new security reality

Traditionally, government has been the primary provider of security to its citizens. In fact, security has always been one of the most basic functions of government. But in a truly global society in which international business, travel and crime are de rigueur, both local and national law enforcement agencies are increasingly challenged in providing comprehensive security.



"The private and nonprofit sectors, communities and individual citizens, as well as federal, state, local and tribal governments, all share common goals, responsibilities, and accountability for homeland security."

—David Trulio
Special Assistant to the U.S. President and Executive Secretary
Homeland Security Council at the White House

REGIONAL VIEW:
BERLIN GIO DEEP DIVE
52°31′N 13°25′E
POPULATION: 3,416,300
AREA: 892 KM² (344 SQ MI)

Sustainable security, used in the same sense as "sustainable energy," was talked about at length in the Berlin deep dive. The concept suggests that to achieve truly sustainable security, society must first root out the very causes of instability and conflict, such as resource scarcity, wealth disparity, oppressive government and the like.

"Security cannot be solely a governmental enterprise—to try to make it one would simply not work," says David Trulio, Special Assistant to the U.S. President and Executive Secretary of the Homeland Security Council at the White House. "Our Natural Strategy for Homeland Security is premised on the notion that homeland security is a shared responsibility built upon a foundation of partnerships. The private and nonprofit sectors, communities and individual citizens, as well as federal, state, local and tribal governments, all share common goals, responsibilities and accountability for homeland security."

This is a sentiment that is widely held among GIO participants and one that falls in line with the thinking around distributed security systems. After all, it's not hard to see that business and government both benefit from a safe and secure citizenry. For instance, there are already many examples of governments working with retailers to monitor and secure vital shopping districts.

The only question remaining is: What roles should the private sector and government play in this new vision? And as crime migrates from the physical world to the digital, how will the responsibilities for pursuing and eliminating security threats be shared between the two?

Q&A

Howard Stoffer _ Director, Management and Administration

Counter-Terrorism Committee Executive Directorate, United Nations

Why are global standards important in the fight against terrorism?

"So that every State understands what it must do in this struggle. Terrorists are well organized and they know what to do to commit terrorist acts. States need the UN and other international organizations to standardize ways to strengthen borders, protect air and seaports, make terrorism a crime in every country and prosecute, extradite and imprison terrorists. This is what my office does. We coordinate with States and scores of international law organizations around the world to promote cooperation on standards that are beginning to stop terrorists from exploiting weak links in the international system. As a result, we are saving innocent lives and putting limits on terrorist activities."

Good Security, Good Business

No single entity in the security triumvirate of government, business and individuals has a stronger natural incentive toward strong, global security than the private sector. In a macroeconomic sense, secure markets breed more confident consumers. More specifically, the global retail industry loses somewhere between 1.6 percent to 2 percent of its revenues every year to fraud, theft and organized crime. And the costs of cybercrime, and the expense of protecting against it, are ballooning daily.

"I think the role of the private sector is increasingly important, because when we talk about globalization, we are talking about economic globalization."

—**Nandkumar Saravade**
General Manager of the Financial Crime Prevention and Risk Management Group
ICICI Bank, Mumbai

Indeed, **good security is expensive**, but bad security can be even more costly. The question is, what portion of security resources should companies spend on defending against threats, and what portion should they spend pursuing them? Over the course of the deep dives, there were many calls for businesses to go on the offensive, to leverage the powerful global networks and business partnerships they had forged to track down, identify and prosecute threats.

Using its experiences with the SARS outbreak of 2003, Taipei participants seized on the immune system metaphor for global security. The basic idea is that if global security worked like the human immune system, it would allow threats to enter the system, but quickly mount responses and bolster defenses for future attacks of the same nature.

REGIONAL VIEW:
TAIPEI GIO DEEP DIVE
25°2'N 121°38'E
POPULATION: 2,630,191
AREA: 272 KM² (105 SQ MI)

"I think the role of the private sector is increasingly important, because when we talk about globalization, we are talking about economic globalization," says Nandkumar Saravade, General Manager of the Financial Crime Prevention and Risk Management Group at ICICI Bank in Mumbai. "Political systems are still very nationalistic, very domestic oriented. They don't understand what's happening in the economic sphere. That's where the transnational companies who have seen the problems in many countries, and have a better grip on the problem, are in a position to make a difference."

To do that, companies are beginning to share information about threats, vulnerabilities and security best practices on a large scale. Typically the private sector has been loath to divulge such sensitive data. But anonymization technology is a powerful tool for allowing companies to pool risk data without revealing their identities.

"Of course data has to be protected, especially in a bank," says Paolo Campobasso, Senior Vice President and Chief Security Officer at UniCredit Group in Milan. "But if security is going to improve, the first thing we have to do is open ourselves up and share information. Because **security is not a competitive sector**."

ANONYMIZATION

HISTORICALLY, COMPANIES HAVE BEEN RELUCTANT TO SHARE INFORMATION ABOUT SECURITY THREATS, VULNERABILITIES AND BEST PRACTICES BECAUSE OF COMPETITIVE CONCERNS. BUT BY USING ANONYMIZATION TECHNOLOGY, EVEN THE FIERCEST OF COMPETITORS CAN BENEFIT FROM EACH OTHER'S SECURITY EXPERIENCE. THOUGH IT MAY SEEM A SIMPLE PROCESS, ANONYMIZATION ACTUALLY REQUIRES A COMPLEX SET OF STEPS TO ELIMINATE THE POSSIBILITY OF BACKTRACKING A PIECE OF DATA TO ITS ORIGINAL SOURCE.

The Legal Vacuum

Globalization has come on fast, remaking the world's business landscape in a matter of years. And while corporations have been quick to adapt, the legal infrastructures and law enforcement agencies have been struggling to keep up. Prosecuting international crimes, especially those of a digital nature, has been particularly troublesome.

Courts of law are dangerously out of touch with the digital criminal landscape.

"There are two disincentives to robbing a bank: the first is the vault, which makes it hard to do; the second is that you go to jail for a long time if you get caught," says Lynn Batten, Director of the Information Security Group at Deakin University in Melbourne. "In the Internet age, businesses have been hard at work developing the digital equivalents of the former, but where is the government analog for the latter?"

Batten argues that, in general, courts of law are dangerously out of touch with the digital criminal landscape. As a result, they develop an over-reliance on expert witnesses, which leads to poor conviction rates. There is also no precedent for sentencing, which is often ad hoc at best, and rarely fits the crime. In short, there is very little reason for cyber criminals to fear the consequences of their actions.

To address this challenge, the private sector may need to mount a concerted campaign, on a local and global level, to lobby for thoughtful, specific legislation around digital crime. In return for tougher laws, the security experts from within the private sector could help educate and guide the government agencies responsible for investigating and prosecuting these crimes.

Businesses must guide governments wisely, however, and avoid pushing for laws with unintended consequences. In an attempt to mitigate online banking fraud, the Singaporean government recently mandated two-factor authentication for all online bank transactions in the city-state, a move that pushes the onus for security squarely back onto the private sector.

Q&A

Francis Yeoh_Chief Operating Officer

National Research Foundation, Singapore

How do some nations develop a culture of security?

"A culture is not something that can be legislated—it is something that evolves slowly over time. So it is possible for governments to create a culture of security-consciousness by having programs over a sufficiently long period of educational activities, political speeches and media messages that remind citizens of the importance of security in their lives. This has been done quite effectively by governments in many countries in a number of areas such as environmental protection, city cleanliness and healthy living."

Built-In Security

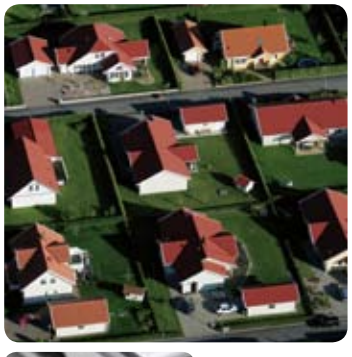
Another way the private sector can effect positive change is by **embedding security** into the products and services it brings to market. Sometimes natural market forces will drive these decisions, like built-in car alarms, insurance discounts for home security systems or embedded security tabs for DVDs and other media. Other times the government can legislate, regulate or litigate the change.

"If you buy a car, and get hurt because of a design flaw, the manufacturer has a strong safety liability in that case," says Ting-Peng Liang, National Chair, Professor, and Dean of the College of Management at National Sun Yat-Sen University in Kaohsiung, Taiwan. "But if you get hacked because your system or software is poorly designed, the vendor has no security liability. You're left on your own to secure data and equipment you know nothing about."

When building security into products, however, companies must carefully consider the trade-offs consumers are willing to make against convenience or cost. GIO participants pointed out that Apple has been widely criticized for not including more security measures in its popular iPod music players. But a big reason for the iPod's success has been its simplicity and ease of use, something that burdensome security requirements could undermine. Alternatively, participants pointed out the self-contradictory behavior of consumers who clamored for improved security features in Microsoft's Vista operating system, then complained incessantly about the same features upon release of the product.

"'**How much security is enough?**' is a question I grapple with every day," says Ingo Noka, Head, Visa Payment Security in Asia Pacific, Visa. "My biggest fear is that we are so concerned about security that we destroy the valuable things the Internet has to provide. I don't want the Internet to require consumers to hold three different security tokens to exchange information or make transactions, or require users to have to attain permission from multiple bodies just to post a simple comment on an online public forum. It will become like TV, which is not interactive. It's important to remember that the value of security is crucial in helping to build trust among users. You must be careful not to destroy that which you are trying to protect—in this case the interactivity and potential of the Internet."

PC SECURITY
IT TAKES 20 MINUTES FOR AN UNPROTECTED PC TO GET INFECTED WITH A VIRUS ON THE INTERNET.



IDENTITY THEFT
IN 2007, 127 MILLION PERSONAL RECORDS WERE LOST OR COMPROMISED.

HOME SECURITY
A HOME WITHOUT A SECURITY SYSTEM IS TWO TO THREE TIMES MORE LIKELY TO BE BURGLARIZED.

MOBILE SECURITY
83 PERCENT OF WIRELESS OPERATORS HAVE BEEN HIT BY MOBILE DEVICE INFECTIONS.

FLASH DISK SECURITY
10 PERCENT OF EMPLOYEES REPORT FINDING A FLASH DRIVE UNATTENDED IN A PUBLIC PLACE.

AUTO SECURITY
CAR THIEVES STRIKE EVERY 26.4 SECONDS.

Security or Convenience

Best Behavior

Using incentives to change bad habits

When it comes to security, disincentives are easy. If you steal something, you might get caught and go to jail. If you leave your office unlocked, your laptop may not be there when you get back. Indeed, there is no shortage of negative consequences for insecure behavior. And while these consequences are well known, people and businesses still put themselves, and others, in harm's way with bad habits like lazy passwords and lax security.

> Strictly Business
> The Threat Within
> Convenient Truth

40 PERCENT OF PASSWORDS CAN BE CRACKED WITHIN ONE HOUR.

63 PERCENT OF ONLINE USERS USE THE SAME PASSWORD FOR ALL ACCOUNTS.

That's why distributing responsibility throughout the security food chain requires more than just knowledge and technology at the so-called "edges" of the network. Empowerment will only get you so far. For real behavioral change, incentives can also be a powerful tool.

"Incentives are the key," says Pierre Noel, Worldwide Enterprise Risk Management and Information Security Specialist at IBM. "If you want people to take responsibility for their own security, and protect themselves, you have to give them a good reason to do so."

But incentives are hard. They require imagination, creativity and true innovation. The best ones are easy to understand, immediate, compelling and relevant. And whenever possible, they should pay for themselves.

"We see a lot of innovation from the bad guys, but we don't see so much innovation from the people who want security, and they are just as smart," says Pat Conley, Senior Vice President of Product Development at VeriSign. "Perhaps that's because they have not yet been motivated in the same way. I believe in economics, that people will do what they're motivated to do. So we have to create an economic environment in which people are motivated to innovate on the positive side of the security equation."

84 percent of network attacks are considered preventable with simple security measures.

"We see a lot of innovation from the bad guys, but we don't see so much innovation from the people who want security, and they are just as smart."

—Pat Conley
Senior Vice President of Product Development
VeriSign, Inc.

THE GREEN MARK VODKA WAX CAP DESIGN RETURNED CONFIDENCE FOR VODKA CONSUMERS AND WITHIN FIVE YEARS, THE BRAND BECAME THE TOP-SELLING VODKA IN RUSSIA.

Strictly Business

The most powerful incentive for changing behavior in the private sector, for better or worse, is money. There are already well-established businesses bringing in billions from the provision of security products and services. And for years the insurance industry has rewarded consumers with discounts for securing themselves and their belongings. But **where is the business opportunity if security is not the product you are selling?**

Marketing security requires a perfect blend of innovation and timing. One example of this is the vodka business in Russia. Counterfeit vodka in Russia is a growing problem, one that is costly for the beverage industry and dangerous for consumers. As a result, beverage makers often struggle to secure their supply chains and ensure that the product that ends up on store shelves is legitimate.

Five years ago, the makers of a relatively unheard of brand called Green Mark, decided to secure their product with a unique, distinctive-looking and totally tamper-proof cap modeled after the wax caps of the 1940s. The cap guaranteed the security and safety of the product, and in just five years, Green Mark became the top-selling brand of vodka in Russia.

Q&A

Tony Murphy_Chief Operating Officer

Daon Inc.

Biometrics seemingly holds so much promise for improving security. Why hasn't this technology been more widely adopted?

"With most innovative and disruptive technologies, adoption begins slowly and builds over time. In the case of biometrics, the early adopters lacked clear standards with which to establish interoperability. But, as standards have been developed, the pace of adoption of biometrics has actually been impressive even to seasoned security professionals. Also, the cost of biometric devices is coming down, with some types of sensors becoming a commodity, which will drive faster adoption. Finally, new technologies are often "tested" in large-scale government deployments before being adopted in commercial applications. Some of the larger government projects now involve more than 50 million biometric records in a secure environment."

"It offered a new level of protection to customers, who are extremely sensitive to buying counterfeit products," says Nikolai Ermochkine, Vice President of Strategy at Industrial Investors, the company that owns Green Mark. "But it also enhanced the image of the product enormously."

> "It's very important when marketing security that the technology is integrated into the product."
>
> **—Nikolai Ermochkine**
> Vice President of Strategy
> Industrial Investors

Shortly after, another brand of vodka took the concept a step further, laser engraving each bottle with a unique number that can be text messaged to confirm the legitimacy of the product. While this new approach is compelling to some consumers, the only drawback is that the onus (and cost) for confirming whether the product is secure falls back on the customer. "It's very important when marketing security that the technology is integrated into the product," says Ermochkine. "And it must be effortless for the consumer."

The Threat Within

Insider threats come in many shapes and sizes, with a whole spectrum of motivations. Whether you are dealing with a careless employee, a vindictive IT worker or a greedy executive, the damage these insiders can do is significant. Carnegie Mellon University estimates that a third of insider attacks cause immediate damages in excess of $500,000, some in the tens of millions. And that doesn't include the impact on business operations and reputation.

Thwarting insider attacks is no easy task, but by recognizing the warning signs and providing the right incentives to employees, organizations can minimize the likelihood of an event ever taking place. According to the Insider Threat Study from Carnegie Mellon, 92 percent of insider attacks are precipitated by a **negative work-related event**, as opposed to opportunism. These events could include everything from insufficient bonuses to demotions to restricted Internet access. And 97 percent of saboteurs exhibit clear signs of behavioral concern prior to committing an attack, such as inappropriate purchases on company accounts, dress code violations, tardiness or diminished performance.

While it's not realistic to think that any organization could prevent insider attacks entirely, there are some basic steps they can take to limit the damage. Monitoring online behavior, eliminating unknown access paths and tightening procedures around demotion and termination are some of the concrete steps organizations should take. But there are many other "soft incentives" that are critical in addressing the potential for insider threats as well. Properly setting expectations and positive intervention through the use of employee assistance programs fall into that category, as does cultivating a sense of loyalty and responsibility to the organization.

Carnegie Mellon University estimates that a third of insider attacks cause damages in excess of **$500,000**.

There was clear concern in Japan that this island nation was gradually losing its reputation for being one of the safest and most secure countries on Earth. In particular, the effects of globalization are making it harder for Japan to maintain its culture of security, allowing destabilizing forces, both physical and digital, into the country.

REGIONAL VIEW:
TOKYO GIO DEEP DIVE
35°41'N 139°46'E
POPULATION: 12,790,000
AREA: 2,187.08 KM²

"Systemically, culture and ethics are important, but employees also need to know what they can share, and when they can share it."

—Charles Meister
Executive Director, Institute for Critical Information Infrastructure Protection and Center for Systemic Security Management at the University of Southern California

One GIO participant told of how his retail company gathers employees 30 days before they open a new store, participating in team-building exercises and "culturalization." Through this process, which includes a number of unorthodox techniques—such as throwing pies in each others' faces—the employees build trust and expectations of each other, understand the brand they are representing, and feel ownership in the success of the branch.

Ironically though, this technique can sometimes backfire if company policies or procedures are not properly communicated. When employees are highly engaged, they also tend to feel ownership in the enterprise, which is normally a very good thing. "But when people feel like they *are* the company, they may also feel free to share information inappropriately," says Charles Meister, Executive Director, Institute for Critical Information Infrastructure Protection and Center for Systemic Security Management at the University of Southern California. Meister believes that the right blend of cultural direction and procedural instruction is the key to striking a balance. "Systemically, culture and ethics are important, but employees also need to know what they can share, and when they can share it."


THE BANK OF TOKYO-MITSUBISHI UFJ, LTD. USES VEIN PATTERN RECOGNITION IN THEIR ATM MACHINES TO VERIFY IDENTITIES AND ALLOW BANK CUSTOMERS TO WITHDRAW GREATER AMOUNTS OF MONEY.

Convenient Truth

Security is most often associated with inconvenience. Forgotten passwords, long lines at the airport and faulty car alarms are all good reasons to curse the very need for security measures. In fact, these inconveniences are quite often the reason why many people abandon good security practices to begin with. But **can practicing good security actually make your life more convenient?**

As it turns out, convenience can be a powerful incentive for consumers to alter their security behavior for the better. "People will do all kinds of things for the littlest convenience," says Larry Ponemon, Founder of the Ponemon Institute, a research consultancy. "They'll give up their personal information for things that, on the surface, seem like an unreasonable gain."

At the Bank of Tokyo-Mitsubishi UFJ, Ltd., customers who submit their biometric data—in this case a mapping of the veins in their hands—are allowed to withdraw greater sums of money from ATM machines. The bank gets tighter security around its ATM transactions and customers get the advantage of higher withdrawal limits.

Convenience is so powerful, in fact, that some people will actually pay to improve overall security. In airports, for example, many travelers pay an annual fee to submit their personal data for prescreening privileges that let them speed through airport security.

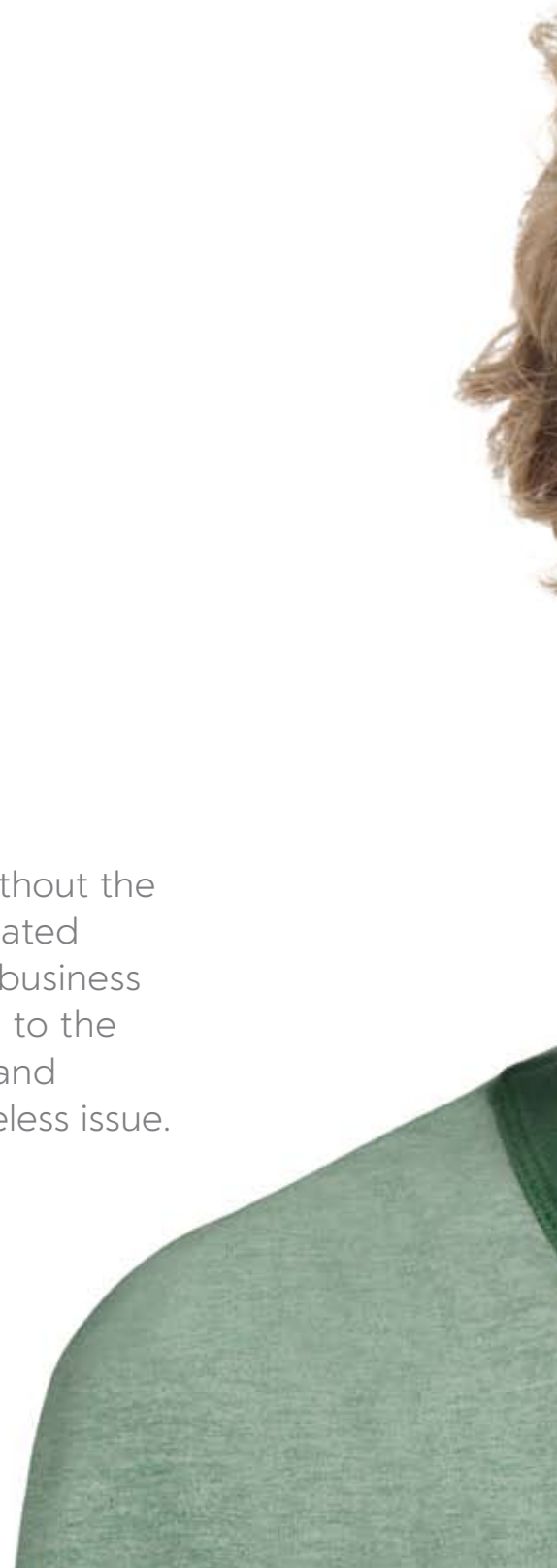
Offering customers too much convenience can lead to some unintended consequences, however. Visa's Zero Liability policy, which absolves cardholders from illegitimate purchases on their card, does not improve consumer security behavior. "Is that an incentive?" asks Chackan Lai, Business Leader, Payment System Risk Assessment at Visa. "Yes in that it encourages cardholder transactions. But at the same time, it does take away their incentive to protect their information. So, sometimes, incentives can be a double-edged sword."

Getting to Know You

The evolving relationship between security and privacy

They are often talked about as if you can't have one without the other. But privacy and security have a far more complicated relationship than that. And as human relationships and business interactions increasingly move from the physical world to the digital world, the nuances of data collection, identity and anonymity are reshaping the way we approach this timeless issue.

> The Master Token
> Reputation Reconnaissance
> Reclamation Project



MonkeyWing
FireNikon
SerialInflux83
Psychogeek1337
RichMahagony
DentedMango
GarbageCompactor
GhostRnrOn2nd
JesseSpano
TillerDoppelganger
WitfilledCharmer
CheeseburgerDreams
JeterBuiltMyHotRod
RegisteredDumDum
OliveTintedMonster
GaryGnu
HobbitLove
GoduckSoup
Zectron
StrangerInTheAlps
Listerfiend
DrStrange
Toetapper78
InternetCrazies
LazyEyed_UrbanPoet
BitofaRembrandt
SatisfiedDork
SpazPride1336
LovestruckDoofus
ResIpseLoquitur
DRGonzoVegas
TheRocketSurgeon
CelticIceWolf3000
MrsBadcrumble
PrecociousReggaeFan
Libatius
BFMoran
DebbieDownerNYC
CorwinMarmot
RaccoonDiner
Client_9
IntellectFist
NitrogenBull
BaaderMeinhofGang
EyeBay13

Cali_Tattoo
volunteerjack
MadDandy
Roger_Roger_1001
Bronx_Son
Floppingaces9
13thbeing
misterGOfast
aclockworkOJ
riverrat&y
mr_natural
hendrixguy89
octobrthundr
wideyes17
carlitoswhey
gamblegoon
wind_denial
touchofirish
SonoftheSouth66
FantomPhiend
Man_o_Warrior
BadHairDaySpa
LoneStar11
Cypher Soldier
Chubbycubby
BermudaRectangle
DukeRaoul
buchannonite
Bluebeard
buffalo_soul
aztlanchica
gawker00
derbyfan
leftcoaster10
wennershop
MercuryOutlaw
Boswellington
Highandoutside
Jxer1991
desert_okie
glimmergoddess7
experimentfail
AmericanDreemer1
benz_studio
Uber_Sorcerer

ghostrider
greenmyst87
snowglobetrotter
heartbrkr94
MrBryteSide
savedbythebell21
CarribeanQueen
Jackofhearts
Lilly21
SlimJim99
RozeMary
OLDminer
delaCroix
SevereMercy
Prince_casper
blackforestcake
strongisland96
jersey_g
tha_croaksta
badmascara
dontfakethefunk
thewholebag
snozzberryDC
JKinHK
wtcremember
attaboy
guytalent
StealthH4x0r

theroyalwii
moohound
y_cant_tori_leet
tha_ville_kru
EliteMonkey
overthelime
unbranded1
bartonfinklestein
StixNStonez
Brightknight12
EarthData
Golf_Dad55
Sarge99
highfalutin
macmurpheee
petescandy
sanandreasgangsta
Lyono78
ManualError
bluetoothless
Flobotflo
Greenlantern61
UrbanAchiever99
no_metronome
rocktheMike87
ninasimoneNYC
thatsnotaknife
masked_avenga

bshade2005
THEguitarhero791
futurelevel
GooseIsland
0donutlover0
777samurai
iwouldprefernotto
ckallie01
functionorform
genevieve
tr3ats
happyaynsley
linyee555
hellokevo
djtannerr
replicanthunter
whirledpeas
brrrgerbelle
ell1ebell1e
screenname004
pepi6400
theholbrooklyn
trotsee
skellington31
LOTRranger
SilentDragonfly
klikbeep
5w3371im3

Online identities are easy to accumulate, but difficult to authenticate.

BlackPhantom
marathonerHI
FiberInferno
SARAHnbd
lizinchi
gotophilk
leonsphinx
thebartthe
MemoryNikon
tenderbarfly
keithmoonraker
FrequencyX
slowyerroll
maude_lebowski

blue_gray_sky
DantheMann
ZeroPulsar
L33tness
Bman7841
cardinalbird7
Edge165
Gomer74791
hipn91
Geniusburger
Ryuken_81
Speed86
PACMAN1179
jBauer24

TheDarkPenguin
Brando47
demolitionMN
DiscoStew
thisismusic
lemonhead75
linuxgrl
mrabc123
chnkngxprss
01ympiad
shutterbug35
boaf85
flowerlady
AgentCooper

REGIONAL VIEW:
CHICAGO GIO DEEP DIVE
41°52'N 87°37'W
POPULATION: 2,833,321
AREA: 237 SQ MI (606 KM²)

Privacy was the key theme in the Chicago dive. Participants, for the most part, agreed that privacy and security can not only peacefully coexist, but thrive in tandem in the digital age, through careful application of technology and policy. It was also noted that in developing countries, privacy is not yet a security concern.

"I think that privacy is too often juxtaposed with security, and it's assumed that security means that you're giving up privacy," says Chris Kelly, Chief Privacy Officer at Facebook. "But I think you can have a great deal of control over your personal information and still maintain a secure environment. In fact, having that control can result in a more secure environment."

This concept is called "informational self-determination." It means the online world should be no different than the physical world in that individuals have the right to decide what information about themselves is communicated to others and under what circumstances. That means businesses and governments would have less latitude in the collection and dissemination of customer data.

> "I think that privacy is too often juxtaposed with security, and it's assumed that security means that you're giving up privacy."
>
> —**Chris Kelly**
> Chief Privacy Officer
> Facebook

It all seems reasonable enough, but does that mean that individuals retain the right to determine whether their identity is revealed and to whom? Or maintain multiple identities? Because that would not mirror the physical world, and it would be hard to argue that anonymity and false identities are not powerful enablers of the criminal element.

"If we could create a world in which you can't do anything without proving yourself to the other party, then we'd have a lot less to worry about," says Shohei Kimura, Chairman of SECOM Co. Ltd., the largest private security company in Japan. A world that absolute is probably not realistic, and for some not even desirable. And as the Internet continues to muddy the waters between privacy and security, the debate over issues like these rages on.

The Master Token

To some, the problem of crime and insecurity has a simple and absolute answer: biometrics. In fact, the human body's unique identifiers—including fingerprints, voice, veins, retinas, even DNA—are sometimes referred to as the "master tokens." But while biometrics is an undeniably powerful tool for holding people accountable for their actions, it is not yet a perfect security solution.

For one thing, there is significant, though abating, resistance to giving up this valuable information. The fear is that because this information is so powerful and so personal, if it is stolen, counterfeited or misused in some way, it would be a devastating violation of the victim's privacy and identity, and the reclamation process would be extremely burdensome.

"People think that if you use biometrics, that's it—you give up any hope of privacy," says Ann Cavoukian, Information and Privacy Commissioner for the Province of Ontario, Canada. "It's not true. You can actually design biometrics to be privacy protective and offer a very high level of security. I call this 'Privacy by Design'."

Along those lines, there are some promising technologies that could mitigate the absolute nature of biometric authentication. An emerging field called "**cancelable biometrics**" holds particular promise. It works like this: Instead of enrolling with your true fingerprint (or other biometric), the fingerprint is imaged and intentionally distorted in a repeatable manner, and this image is used as the identifier. If this image is stolen or otherwise compromised, a new fingerprint can be issued by simply changing the parameters of the distortion process.

Technology like cancelable biometrics provides enhanced privacy for the user because his or her true fingerprint is never used anywhere. And because different distortions can be used for different types of accounts, it precludes the possibility of various organizations cross-referencing your print and sharing profile information.

Increasingly biometrics is being used for everything from financial transactions to airport security. Many times, participants don't have an option to opt out. But when it comes to the possibility of biometrics for national or international identification systems, solutions like cancelable biometrics can help make widespread adoption more politically and culturally palatable.

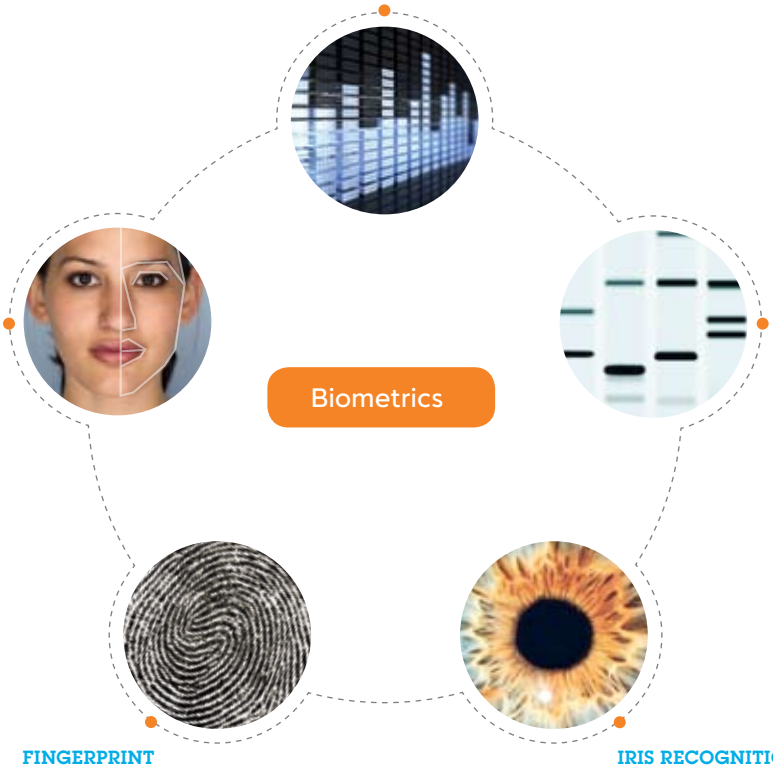
Q&A

Harriet Pearson_Vice President, Regulatory Policy and Chief Privacy Officer

IBM Corporation

What can employers do to help employees improve their personal security and privacy?

"Employers can do a lot by educating employees—keeping the issues on the proverbial radar screen. But even the best-intentioned employees sometimes don't practice good security behavior. So we recommend that employers architect corporate policies and an environment that makes secure and trusted behavior the obvious choice. For example, in 2005 IBM adopted a first-ever global policy that classifies genetic information as the most sensitive information we handle and crafted policies that strictly limit disclosure and use of that kind of information. Further, we specified that genetic information can't be used by IBM to make employment decisions or to deny basic health insurance coverage. What does that have to do with security? A lot—employees should not have to worry that information about them, that has nothing to do with how well they can contribute, may be used against them."


VOICE RECOGNITION
GREAT POTENTIAL FOR MOBILE PHONE TRANSACTIONS.
FACIAL RECOGNITION
NEW TRENDS INCLUDE 3-D TECHNIQUES AND SKIN TEXTURE ANALYSIS.
Biometrics
DNA
CHANCES OF TWO INDIVIDUALS SHARING THE SAME DNA PROFILE IS LESS THAN ONE IN A HUNDRED BILLION.
FINGERPRINT
ONE OF THE OLDEST FORMS OF BIOMETRICS. IT HAS BEEN USED FOR MORE THAN 100 YEARS.
IRIS RECOGNITION
FALSE MATCH RATES ARE BELOW 0.000000000001 PERCENT.

Reputation Reconnaissance

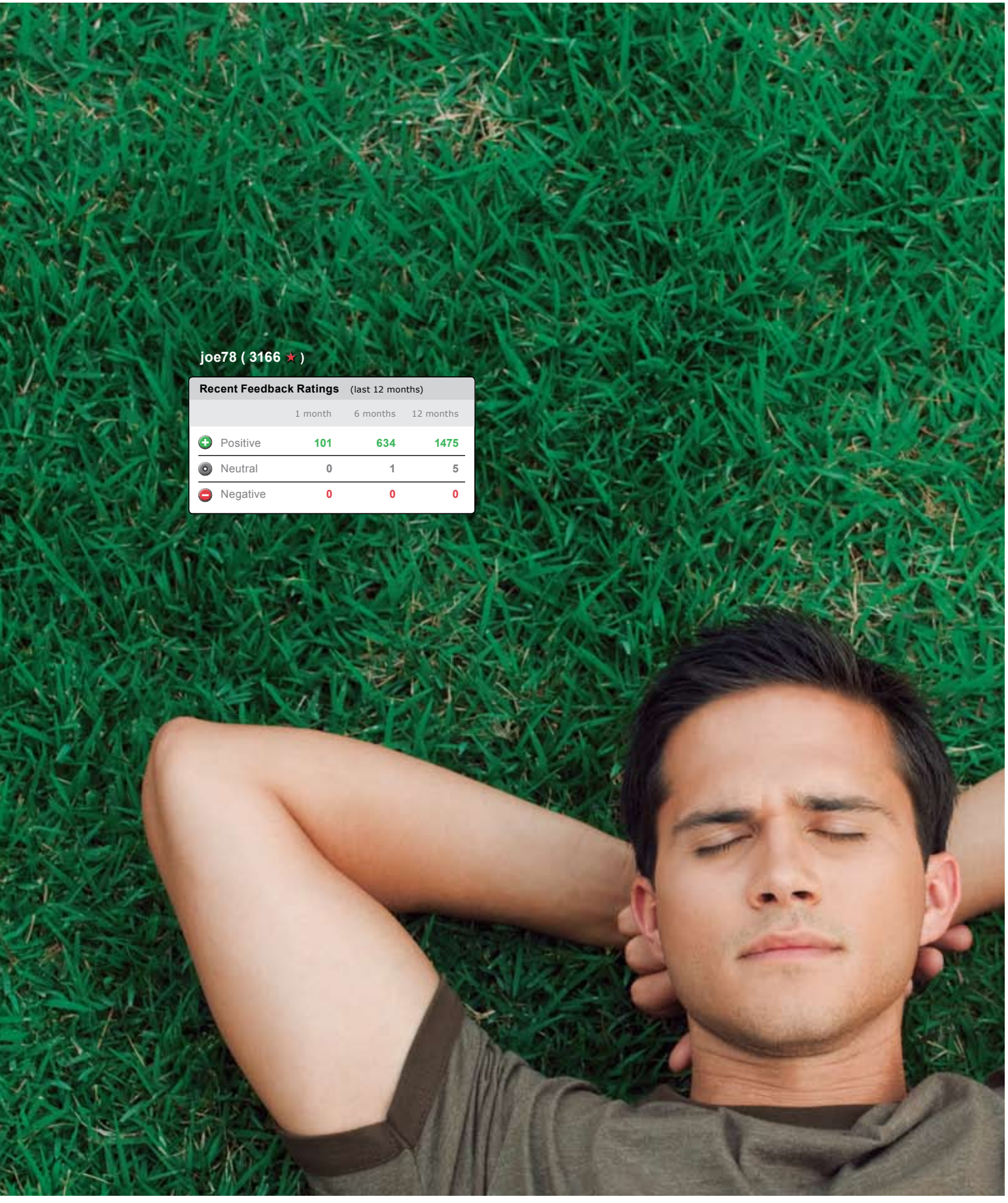
Authenticating people's identities is a critical part of providing any secure environment. But this is a particularly vexing problem online, where traditional means of verifying one's identity give way to the veil of anonymity.

"In the physical world, you would be pretty surprised if you saw an unfamiliar or unsavory character come to your front door, and you certainly wouldn't let them in," says Phil Zimmermann, the creator of Pretty Good Privacy (PGP). "But our e-mail inboxes fill up daily with unsavory characters, easily slipping past the electronic front door and sitting down in our living rooms."

Multiple identities are not always a bad thing, however. One of the truly compelling aspects of online communities is that individuals can escape their physical identity, try on different personas and interact with others in a way they could not in the physical world. This freedom from being tied to a single identity is one of the defining characteristics of the Internet.

With that in mind, many GIO participants advocate the development of **peer-to-peer based online rating systems**. Similar to the idea of community policing or the reputation networks found in eBay's seller ratings, the concept revolves around individuals assigning both each other and the Web sites they visit a security rating. If people frequent Web sites with low security ratings, or consistently misrepresent themselves, their individual rating would suffer as a result, and so on. These ratings would apply to however many identities an individual assumed.

Others favored ratings that more closely mirrored credit ratings, which are aggregated from various data points and brokered through a third-party organization. The question there, of course, is who that third party would be, and how they could be trusted. In the end, it may be a combination of the two that proves the most reliable way to judge online interactions.


joe78 (3166 ★)
Recent Feedback Ratings (last 12 months)
1 month
6 months
12 months
Positive 101 634 1475
Neutral 0 1 5
Negative 0 0 0

REGIONAL VIEW:
VANCOUVER GIO DEEP DIVE
49°15'N 123°6'W
POPULATION: 650,869
AREA: 115 KM² (44 SQ MI)

The issue of online identities dominated the conversation in Vancouver, and participants put forth a number of innovative ideas about how to manage and control personal information online. Also, the group came to a complete consensus that a delicate balance of centralized and distributed security solutions is the right way to address global security.

Reclamation Project

There's no question that the more widely available your personal information is, the more vulnerable you become to both physical and digital attacks. And the Internet has made that information appallingly easy to obtain. Home addresses, phone numbers and birth dates are often a simple Google search away.

That's why the idea of identity reclamation services may be a burgeoning opportunity. With so many social networking profiles and other sources of personal information proliferating online, people are finding it increasingly difficult to put the proverbial genie back in the bottle. "Electrons are very patient," says one GIO participant. "I mean, once it's out there, it's out there. That's why being able to take it back would be an enormously useful service."

Technically speaking, this kind of digital tattoo removal service is nearly impossible due to the fantastically distributed nature of the Internet. But that's not to say that there aren't other strategies that would help alleviate the problem.

Data tethering is the notion that organizations should be able to ensure copies of information are accurate and up to date. Tethering ties the original record, or master copy, to all subsequent copies of the data. In this manner, one change in the master copy is then reflected throughout the information sharing chain. "Non-tethered systems in national security and law enforcement settings are especially problematic as there can be real privacy and civil liberties consequences resulting from organizations operating on incorrect data points," says Jeff Jonas, Chief Scientist, Entity Analytics, IBM Corporation. "And this leads to a real waste of resources to boot."

84 percent of Internet users claim they never give out personal information online. **89 percent** actually do.

Q&A

Sadie Creese_Director of e-Security

The University of Warwick Digital Laboratory

How does giving end-users more control over their personal information make them more secure?

"We know that empowering people to take responsibility for their own assets is an important part of delivering security; users are part of the system and so will inevitably have a positive or negative effect on vulnerability and exposure to threats. By enabling people to take effective control over their personal information we can begin to limit the level of vulnerability they have to identity theft and associated crime. This in turn has benefits for wider society as it will help to prevent fraudulent access to corporate assets and citizen services, and play a part in fighting organized crime and terrorism."

GIO contributors include representatives from the following companies and organizations:

Aeroflot
Allen & Buckeridge
Alticor Inc.
Amadeus Capital Partners Limited
ARBURG GmbH + Co KG
Australian Homeland Security Research Centre
Best Buy Canada Ltd.
Capgemini Sverige AB
Central Bank of Russia
Clientron Corp.
Computer Network Limited
Counter-Terrorism Committee
Executive Directorate, United Nations
Daon Inc.
Dartmouth College
Deakin University
Debix Identity Protection Network
Department of Industrial Technology,
Ministry of Economic Affairs, Taiwan
E.Sun Financial Holding Co., Ltd.
EC Network
Euro-Asian Association of Security Goods and
Services Manufacturers
Eurotechnology Japan KK
ExxonMobil
Facebook
FoeBuD e.V./BigBrotherAwards Deutschland
Free Software Foundation Europe
Gas Natural SDG, S.A.
Georgia Institute of Technology
Gobi Partners
Goldman Sachs International
Honeywell
Hung Capital Management Ltd.
IBM Corporation
ICICI Bank Ltd.
Idealgovernment.com
Identity Theft Resource Center
Indian Statistical Institute
Industrial Investors
Industrial Technology Research Institute
InformZaschita, Inc.
iNovia Capital
Institute of the Information Society
i-Sprint Innovations
JK&B Capital
John Jay College of Criminal Justice
Kaiser Permanente
Metropolitan Electricity Authority, Thailand
Ministry of Economy, Trade and Industry, Japan
Ministry of Internal Affairs and
Communications, Japan

Movimentos em Rede
National Research Foundation, Singapore
National Sun Yat-Sen University
National Tsing Hua University
NEC Laboratories Europe
Nissan Motor Co., Ltd.
Nokia
Openwall, Inc.
PayPal
PGP Corporation
Ponemon Institute, LLC
Province of Ontario
Quadnetics Group plc
Queensland University of Technology
RBC Financial Group
Russian Academy of Sciences
SanDisk Corporation
Science and Technology Advisory Group of the Executive Yuan, Taiwan
Science Council of Japan
SECOM Co., Ltd.
Sennheiser electronic GmbH & Co. KG
Simon Fraser University
Small and Medium Enterprise Administration, Ministry of Economic Affairs, Taiwan
Social Technologies
Sun Life Financial
Telecom Information Sharing and Analysis Center Japan
The ABB Group
The Bank of Tokyo-Mitsubishi UFJ, Ltd.
The Homeland Security Council at the White House
The IA Group
The Kroger Company
The University of Warwick Digital Laboratory
Toyota Motor Corporation
TPO Displays Corporation
Tyco Fire & Security
UniCredit Group
Unisys
United Way Taiwan
University of Southern California
University of the Armed Forces, Munich
Valiant Technologies Pvt. Ltd.
Ventures West
VeriSign, Inc.
Virginia Polytechnic Institute and State University
Visa Inc.
Western Payments Alliance

The goal of achieving higher security on a global basis requires ambition and patience. It also takes teamwork.

Through the Global Innovation Outlook, IBM is working with multiple constituencies, from both the public and private sectors, on market initiatives and thought-leadership projects to enhance security in both the physical and digital worlds.

If you or your organization would like to get involved, don't hesitate to contact us at **www.ibm.com/gio**.

IBM would like to thank VeriSign, Inc., its Global Innovation Outlook Partner, for its thoughtful contribution in every aspect of the GIO cycle.

About the GIO

In early 2004, IBM took an unprecedented step: We opened up our annual technology and business forecasting processes to the world with the first Global Innovation Outlook.

The GIO is rooted in the belief that the very nature of innovation has changed. Today, the greatest innovations come from multiple sources, working together, solving common problems. And that means the truly revolutionary innovations of our time—those that will create new markets, redefine old ones, and maybe even change the world for the better—will require collaboration on a global scale. With that in mind, the GIO challenges some of the brightest minds on the planet—from the worlds of business, politics, academia and nonprofits—to collaboratively address some of the most vexing issues on Earth, and identify opportunities for business and societal innovation.

This collaboration begins with a series of open, dynamic conversations called "deep dives." To date, nearly 50 GIO deep dives on five continents have brought together more than 650 influencers from dozens of countries. These free-form conversations, fueled by a diverse mix of expertise and perspectives, are inevitably candid and spirited. Collectively, they result in an explosion of ideas that spark new relationships, policy initiatives and market opportunities for all involved. Previous topic areas have included the environment, health care and transportation. To order copies of reports from previous GIOs at no charge, please visit www.ibm.com/gio/order.

International Business Machines Corporation
New Orchard Road, Armonk, NY 10504