INCIDENTAL PAPER

Seminar on Intelligence, Command, and Control

Protecting the Financial and Payment System by Dispelling Myths
Kawika Daguio

Guest Presentations, Spring 1999
Charles J. Cunningham, Kawika Daguio, Patrick M. Hughes, Peter H. Daly, Walter Jajko, David J. Kelly, Gregory J. Rattray, Michelle K. Van Cleave, Robert T. Marsh, Randall M. Fort

June 2000

Program on Information Resources Policy

Center for Information Policy Research

Harvard University

The Program on Information Resources Policy is jointly sponsored by Harvard University and the Center for Information Policy Research.

E-mail: pirp@deas.harvard.edu URL: http://www.pirp.harvard.edu
ISBN 1-879716-63-1 **I-00-2**

Protecting the Financial and Payment System by Dispelling Myths

Kawika Daguio

In the spring of 1999, Kawika Mikaele Ka'imi'kukui Daguio became executive vice president of the Financial Information Protection Association, an organization whose mission is to provide individuals and companies well-founded assurance that their financial assets and information are protected adequately. At the time he gave this presentation, Mr. Daguio was payment systems and technology policy consultant for the American Bankers Association (ABA; URL: http://www.aba.com) in Washington, D.C. In this capacity, he addressed operations, technology, risk management, and privacy issues arising from federal regulatory management, payment system operations, payment system risk management, and telecommunications. Prior to joining the ABA, Mr. Daguio was a financial program specialist with the U.S. Department of the Treasury, Financial Management Service. He has also served in technology and financial positions in both the private and public sectors. Mr. Daguio earned a bachelor's degree in social science and social ecology from the University of California at Irvine, and holds master's degrees in business administration and public management from the University of Maryland.

Oettinger: You know our speaker today is Kawika Daguio from the American Bankers Association. You've seen his biography, so I don't need to introduce him. Before I turn it over to him, I just want to point out and remind you that the schedule this year includes a fairly mixed bag of civilian and military types. Some of you, I know, have had some queasiness or doubts as to why this was being foisted on you in a course on intelligence, command, and control. I thought, and I hope you did, that when Chuck Cunningham spoke here last week he made a pretty good case for that, by virtue of the fact that so much of the technology, so many of the problems, so many of the potential solutions are driven by or related to traditional civilian concerns. If ever there was a nice segue into what's happening here today, that was it. Next time, we will have a quintessentially military type again, so the sequence of presentations that starts today with Mr. Daguio will continue then with General Marsh, and with Pete Daly, and so on. That's my last word. Kawika, it's yours.

Daguio: I'm honored to be here, and if any of you need to find anything that I reference, I'll post it all on my Web site. The URL is www.daguio.net or www.fipanet.org.

It's a little "unbankerly" to talk about some of these issues the way we're going to talk about them. The way bankers talk about them is in the framework of risk management. If you view it at that level, of just "We're managing risks," it's very appropriate for us to talk about them. I'm going to treat this as a special occasion and so I'll stray and get down closer to the innards of the issue more than we typically do. If you're interested, I'll talk about both offensive and defensive information warfare.

The title of my talk isn't "Strategic Information Warfare in the Financial Infrastructure." It's really: "Protecting the Financial and Payment System by Dispelling Myths"—stifling lies and misdirection, and fixing things before they're broken. It's largely what we do for a living. The American Bankers Association is the oldest and largest financial trade association in the country. Some of our very earliest activities involved security—old-fashioned kinds like posting bounties on bad guys' heads. A long time ago, we used to produce code books for the teletype and telegraph days. We're the environment that produced the commercial versions of the digital encryption standard (DES) and managed test keys.

We have a history and tradition of paying attention not only to operational security issues, including information security, but also to systemic issues related to the financial security and stability of the payment system. Given that introduction to my organization, I just wanted to qualify it and say that any statements I make are not necessarily 100 percent reflective of what my management would say our policy is, and so here I'll separate and distinguish some of my personal views from the association policy and industry policy. I'll let you know when something is official industry policy

I've got a little bit of background on some of you folks, but I have some questions. I understand there are a few folks from the Kennedy School here, and you're studying public policy. How many are focused on national security-type issues? Business-economic issues—or can you separate them? How many of you work for the government and want to help us? I see a couple.

Student: Which government, and which couple?

Daguio: Any government. It's a common problem. I used to be a government employee myself and volunteered to help people all the time.

I'm going to read this part of the story so it doesn't get me into trouble, because my involvement in this area, other than actually working in the operations of payment systems, came about as a result of both some of my academic experience and where I worked at the time. I've gotten permission to tell this story if I tell it as I wrote it and got it cleared.

The very first time I wrote anything on the subject of strategic information warfare was just prior to the first war with Iraq, when I was working with the Treasury Department. At that time I focused on the federal government's direct interest in financial and payment systems. I was working for the Financial Management Service, which is a Treasury bureau responsible for government-wide financial management. It included the federal government's contracts and bank accounts with financial institutions on a worldwide basis. I was also attending the University of Maryland, doing an MBA and a master's of public management with a focus on finance. Although I was studying finance, my closest academic friends were pursuing the national security concentration in the public management school. I had previously spent a summer at the RAND Graduate School and had done some work looking at strategic nuclear warfare, and so I was well accustomed to dealing with the officers, the geeks, and the Defense Advanced Research Projects Agency (DARPA) types.

Oettinger: Is the "officers, geeks, and DARPA types" the thing that you required clearance for?

Daguio: No, it was actually the whole story, because what I did was not covered by policy at the time. Isn't DARPA the product of one of Secretary McNamara's Whiz Kids?

Oettinger: No, McNamara's Whiz Kids were Alain Enthoven[1] and the financial types. ARPA was created in 1958, in Eisenhower's second term, when Neil McElroy was secretary of defense. ARPA then reported directly to the SECDEF.

Daguio: These are really brilliant people with Ph.D.s who think and talk about stuff that doesn't often have relationships to exactly what's going on at the time. They invent cool, fun things like the Internet as byproducts, but they're not always on target, and they sometimes come from left field.

I was surprised when some "DOD" people sought me out when I was at Treasury, and asked me odd questions that led me to believe that they were trying to model the secondary impacts of an attack on a foreign financial system on ourselves and others. I responded informally with a list of arguments against attacking financial infrastructures. I took it seriously, but sometimes it felt uncomfortable taking it a little bit too seriously. So I gave them a list that said, "Attacking financial infrastructures is a bad idea for many reasons." It sets a nonacceptable precedent.

---

[1] Alain C. Enthoven, formerly assistant secretary of defense under Presidents Kennedy and Johnson and currently a professor at Stanford University, invented the concept of managed competition.

That's pretty serious. We're subject to asymmetric exposure. Frankly, we have a lot more money moving around globally than most people do, with far less granularity with respect to the ownership of the assets than is common in other parts of the world.

The arguments that really worked best for these guys come down to the fact that the U.S. government has money all over the world, and has relationships with people all over the world who owe it money. What convinced them not to ask me any other questions (I don't know whether it convinced them not to do anything) was that I was able to show them that the U.S. government had funds in financial institutions of all different kinds, on behalf of agencies all over the world, and that our trading partners and the people who owed the United States money had relationships with those institutions as well. So they actually began to understand that if you damage the financial infrastructure abroad, you could delay the movement of funds or potentially cause the loss of funds that are important to settling some kind of obligation—either an account obligation to give us back the money that is owed to us directly, or money that might be indirectly owed to the U.S. government.

Oettinger: May I comment on that? This may have fallen on more receptive ears than you might think because there is a fairly long tradition, both civilian and military, on this score that leads to thinking about things that are better left standing than demolished. In two world wars postal services were not disrupted. During the height of the Cold War era, in a whole bunch of things—among others, open skies and space—it was in the common interest of the U.S. and the Soviet Union not to interfere with each other's so-called national technical means of verification. In some of the discussions about averting nuclear warfare, the question of not destroying means of communication that would be not only warfighting but also war-terminating capabilities comes up. So I don't think this kind of reasoning that you're expounding on here is alien to military or civilian strategic thinkers. Therefore, it is an important element because sometimes it means averting an arms race or averting mutual destruction when it turns out to be in everybody's best interest, regardless of what side of an argument they're on, to keep a piece of infrastructure going. So it's a respectable argument you were making.

Daguio: At the core of my being I wanted to respond with the following, which doesn't sell well outside of my community: It's morally wrong to attack financial infrastructures. It doesn't sell well when you look at it that way. Bankers have a tradition of managing other people's assets for them, and because the infrastructure is supporting a large number of people with diverse interests, it's impossible to attack any part of that infrastructure strategically or surgically without damaging the basically 90+ percent of the activity that you have no interest in touching. So I became convinced that it's impossible and wrong to target financial infrastructures.

Student: But there has to be a group of people for whom it's morally wrong, and you're talking about its being morally wrong for bankers. Right? Because for many other people it wouldn't be morally wrong. It would be a very nice, juicy target.

Daguio: Absolutely. I believe it's morally wrong to target it if you are a developed nation engaging in legitimate defensive and offensive policy. I believe that it's proper to pick your targets carefully and not to do indiscriminate damage. But I can see how attractive financial infrastructures would be to those who are interested in destabilizing an economy or a country. In most cases, I don't think that U.S. policy is about destabilizing an entire country. It's usually about achieving a narrow goal.

Student: I don't want to bring up this subject, but in communist ideology, money is the enemy. The ideal communist society is a society where money does not exist. So for a Marxist guy at the MIT computer lab I don't think it will be a moral dilemma whether to target a financial institution or not.

Daguio: I wouldn't expect bad guys to cross us off their list of targets. My goal at the time was to make sure that most governments, es-

pecially our government, didn't set a precedent that would encourage other people to do it. There are a lot of other tools that you can use to achieve your ends more directly, and other kinds of rich targets that are probably more appropriate to pursue. I was just hoping I could take it off the table for a lot of people. But we're prepared to deal with state-sponsored organized crime, casual attackers, and insiders as they come up.

Let me conclude about where I came from and issues that I've worked on; they all come into relatively odd focus. I left the Treasury and came to work for the American Bankers Association, where I do operations automation and risk management issues. That includes helping to manage financial systemic risk, which in turn includes credit risk, operational risk, and other kinds of risks, including strategic risks. Even if there is no technical problem, but one financial institution fails because of bad management, that means making sure that the rest of the financial system can stand up to the shock of that one institution's failure.

If you look at everything that the banking system does, you'll find planning for contingency and managing risks at multiple layers. Y2K, critical infrastructure issues, managing against natural disasters, managing against insider fraud or defalcation, or fun things like that are all part of the same risk environment. The risk issues get managed basically the same way. If it poses a potential catastrophic risk to the bank, it has to be managed. If it poses a risk to the financial system, it has to be managed. When something poses a risk to the financial system, we kind of give up part of our ownership of the issue, and we share responsibility with the governments that we have to work with. That means coordinating at an industry level, coordinating within the banks, and coordinating activity among the banks, the industry, and the government. This critical infrastructure subject matter is one of those issues. The question is being asked today, "Who owns the responsibility for protecting the economy?" That's partly why I'm here following the general who spoke last week.

We have the most responsibility for protecting one of the most attractive targets that there is. We've done a terrifically good job of it for a while, but we recognize that the environment's changing. In case you didn't know, the banks have deployed cryptography and information security more broadly, and it's more integrated into banking infrastructures than in any other community except for parts of the U.S. military. We invest more in security technology and in data processing than any other industry. We are also more reliant on telecommunications than any industry other than the telecommunications industry itself. What that means is we're interdependent. We have a lot of stuff out there, and it's stuff that has to be protected.

Another question that comes up is, "Who gets to protect it, and who pays the bill?" Recognizing that we have public policy responsibilities, and because we have relationships that go back a ways, some agencies in the U.S. government have asked us to champion some of their causes for them. In cases where it would have damaged our security interests, we refused. In 1993, I ended up negotiating with the Clinton Administration on the Clipper Chip debacle (or initiative; you can call it either one) and Digital Telephony. The Clipper Chip was an approach to managing encryption keys that would have allowed the government, preferably with due process generating a piece of paper beforehand, direct access to be able to read encrypted message traffic and encrypted files.

Digital Telephony was an initiative that eventually was passed and became the Communications Assistance to Law Enforcement Act, which originally would have provided the government direct access to all of the digital networks in the country without arbitration. So, an FBI guy gets a warrant; he dials into Bell Atlantic or AT&T; gets a tap on the line; listens in; and does all kinds of fun stuff; the stuff has to be decoded; he decodes it using the Clipper keys, and the government's happy. We said, "No way in hell."

There's a mechanism called the Right to Financial Privacy Act, which allows the government to come forward with due process—to generate a piece of paper and request information about specific individuals the way they're supposed to do it, with traditional subpoenas—and we give them access to that information if we have it. So we negotiated the beginnings of a policy that had complications at the end. It says, "We're terribly good at managing our networks and managing this

information and managing our risk. You should allow us to do that, and you should make sure that in pursuing your own goals you don't cripple the security of a special infrastructure like the banking industry."

Unfortunately, when we did that, we started part of the process that led to the new thinking, which says, "As a manager of a special infrastructure that everybody else is so reliant on, you have additional obligations to the U.S. government and to the people in the name of national security." We began to hear rumblings from folks in the FBI and the defense community that said, "Hey, we're concerned that you're not managing your security well enough. We would like to help you. We don't know what you're doing, but we imagine we can tell you how to make it go better." So by setting ourselves apart, making an argument that we were special, we, to some extent, opened ourselves up to new claims being made against us. We began to hear more and more offers to help, and when those offers weren't welcomed, we began to hear rumors. Some of the least fun I've ever had in my entire life was dealing with hearings where story after story was told, all completely unfounded, where allegations were made about money disappearing and being unreported, where completely debunked stories in the foreign press (from the *London Times Observer*, for example) were being used to make claims that billions of dollars were being lost because of security holes in financial infrastructures and were going unreported.

We decided we had to respond more aggressively and become more involved in some of the national security policy debates. We began to dedicate some resources to making sure that nobody set the agenda for us, and that nobody wrested control over our risk management away from us. We strongly believe, and it's almost a mantra, that "bankers with information security risk experience are best able to determine what commercially reasonable security is, and best able to take into account information about national security and to manage those risks on behalf of both the industry and the nation."

That's a hard sell when you're sitting across from somebody who has all kinds of information and Top Secret clearances and fun things like that. That community has information that they're not allowed to share, and doesn't have a whole lot of trust in anyone. But over the last six years of sitting across from folks from the National Security Council, DOD, NSA, CIA, FBI—agencies that bankers rarely have anything to do with—we began to develop a kind of mutual respect. That respect has been earned as a result of a lot of face time and shared experiences. What I'm partly here to talk to you about is how we got where we are: to PDD 63[2] and the existence of the Critical Infrastructure Assurance Office.

A banker who runs one of my several committees, Steven Katz,[3] has been involved in a lot of these activities, and the way he characterizes what we did is that there was a lot of fear that we were hiding things. There was a lot of distrust because we hadn't seen the information that the others had. We didn't know what each community was up to. The banking industry, more than it has ever done in the past and probably ever will again, as he says, "opened its kimono." We invited investigators to come in, and we walked them through banks. We showed them operations centers. We allowed them to evaluate policy, look at maps, review practices, and to interview management and operations personnel. We pounded the pavement and interviewed people at more than 45 institutions—the most critical institutions that we could find, with the greatest amounts of traffic flowing through them and the highest visibility.

What we found was really impressive. We found no other infrastructure that remotely compared in robustness. The folks who were part of those teams from the military and from technology companies were surprised; in fact, *I* was surprised. The paranoia about operational risk that bankers have,

---

[2] Protecting America's Critical Infrastructures: Presidential Decision Directive 63 (PDD 63), May 22, 1998. Information on this document, and on the President's Commission on Critical Infrastructure Protection, can be found at www.info-sec.com/ciao.gov.

[3] Steven R. Katz is the chief information security officer at Citibank, N.A.; he also serves on the New York Clearinghouse Banks Data Security Officers Committee and is a member of, and has chaired, the American Bankers Association Information Systems Security Committee.

which comes from having so many people looking over your shoulder—your customers, your boards, regulators, and also the INFOSEC community—made these people do things that go well beyond what would be required in traditional commercially reasonable security management practices. They've gone beyond systemic risk management, and while not building the gold-plated systems that might be in place in some defense infrastructures, they've built systems that can stand up to casual attacks, internal attacks, organized crime attacks, and some state-sponsored attacks. There are examples of each in recent history that we can go over if you like. In some of them, I can't be terribly specific.

Oettinger: You said "gold-plated" military systems, and I didn't quite want to let that go by without commenting that there's an index of a significant difference in sincerely held viewpoints regarding what Kawika describes as commercially acceptable risk. Every supermarket tolerates a certain amount of pilferage because the price in lost customers and in dollars and so forth of having everybody frisked as they go in and out of the supermarket is intolerable, whereas pilferage here or there is a cost of doing business. I don't know what the threshold is for the banking industry, but my guess is that "commercially reasonable" is some measure like that. You don't frisk every customer coming into a bank. There are a number of things that you don't do because it's only money.

If you say that to somebody on the military side, it's well and good, but we are dealing with lives—in the first instance our own and those of our subordinates, et cetera, and in the second yours, dear taxpayer, and so on. Ten percent pilferage is one thing, but 10 percent decimated troops, or 10 percent decimated population, is another. So, "commercially reasonable" versus "gold-plated military" is a sometimes good-natured, sometimes ill-natured clash of perfectly reasonable goals. One wouldn't want either side to give up on the arguments, because they're reasonable, but then it brings into question that at some point a political decision has to be made. In short, in the lingo that I'm trying to thrust on you, there is a balancing act between goals that are not necessarily reconcilable. In fact, he worries me when he says they're getting so cozy, because it's not clear that from a political point of view one would want to negotiate something that may be a matter of major policy. Anyway, that's a quick reaction to what you just said.

Daguio: There is fraud. There is embezzlement in financial institutions. Financial institutions do lose money, but the one thing that every financial institution manager manages against is catastrophic risk. The one thing that he wants to protect is confidence. You can't quantify confidence terribly well. You just have to protect it. Sometimes protecting confidence requires cooperation; sometimes it requires going well beyond what other industries would consider commercially reasonable efforts. It may vary, in some cases, from country to country. It depends on the risks that you are facing. So, a large financial institution with global networks may be required to do different things than a smaller institution operating solely in Arkansas. You have to balance that, and government policy has to take that into account.

Often, policymakers ask us, "We've seen large institutions and we've seen good things. Does that mean that every financial institution in America is okay?" The answer is no. We can't know that, and even if we could know, we couldn't fix everything everywhere. But what you have to do when you're managing risks in the national security interest is to manage them reasonably. Does the U.S. government have an interest in making sure that no financial institution anywhere can lose money? Absolutely not. That's not government policy. That's an industry issue, or an individual entity issue. The U.S. government does have an interest in making sure that there's confidence in the government, there's confidence in the dollar, there's confidence in the financial system, and that the economy continues to roll on. If any security problem exists that could pose a threat to any of those interests, that becomes a matter for negotiation. It's important that it become a negotiation because it should never become a battle. Battles over relatively obscure and complicated risk issues can only

scare the general populace and damage confidence, and nobody wants to do that.

Oettinger: Another interjection here, back to last week's session and to the reading in Rattray.[4] Kawika has put his finger on some very critical questions in the last couple of minutes, but I remind you that General Cunningham said that one of the major problems is to determine what is an indicator, or an indication, of a major threat as opposed to one of the petty threats. So this boundary that Kawika is outlining in theory turns out to be conceptually somewhat difficult to figure out, and you have Cunningham's admission that he doesn't know what the indicators are. Seen in that context, Rattray's thesis is a search for criteria that will tell you when something is a large enough risk to be clearly a government concern, as opposed to being something that can be left to commercial risk management. Kawika admits that somewhere there's a handover. But the question before you here, and before the body politic, is: Where the hell *is* that boundary?

Daguio: I don't know where the boundary is, but I can give you some examples of cases in which we don't own the responsibility. Some bankers have been asked, "What is industry policy, and how are you managing against electromagnetic pulse (EMP) as a result of nuclear devices being set off?" My response is, "We don't have one. We would hope the folks in the Defense Department have taken up that issue, because it has nothing to do with traditional operations and normal economic activity." That's clearly a public sector policy determination. The industry doesn't have a position on the Strategic Defense Initiative. We shouldn't have to. There are some areas where we don't have to worry, hopefully, about whether we actually deliver answers or solutions to problems.

We have been asked how we can be sure that some of the hires we make out of MBA programs are not plants. We do rather intensive background investigations, but they don't compare to the level of a full field background investigation that you'd get if you were going to hold a Top Secret clearance. Our response was: "If you believe there are questionable people being hired into positions of responsibility in financial institutions, one would hope that you would uncover them and let us know, and/or provide us a means by which we can defend ourselves."

Then offers have been made to allow, or in some cases, require clearances for some of our people in strategic positions. I don't know how that debate comes out. I know we have a bit of a say in it, but, again, we know we're never going to be privy to all of the information that the intelligence agencies hold, nor do we expect them to share it with us. But we do expect them either to help us manage those risks or leave us alone about them.

Oettinger: Again, if I might just interject, even in that there are wheels within wheels. Let's suppose that there's an agreement between the private sector banking industry and the government as a monolith that this is a good thing. Now, who's looking after that? Folks concerned with law enforcement, like the FBI? Or folks concerned with counterintelligence, or military people? What's the nature of the threat? Let's suppose that somebody wants to steal money, but then suppose that somebody wants to steal the money as the opening of a strategic information attack in Rattray's sense. Now it sounds like a joke, but if you think about these problems of allocation of responsibility, and when you start reading the PDD 63 and look at the bureaucratic consequences of this sort of thing, again, Kawika keeps raising questions that have a lot of depth to them.

Student: I understand there's a fine line here and it's very hard to determine where responsibility comes, but I'm intrigued by the EMP example you bring up. I don't see how it could be DOD's responsibility to protect the business sector against EMP. There's nothing the Pentagon can do. It's the system's own responsibility. If you think electromagnetic radiation is a threat to you, do you really expect the Pentagon to be protecting your in-

[4] See Lt. Gen. Cunningham's presentation in this volume. See also Gregory Rattray, *Strategic Information Warfare: Challenges for the United States*, Medford, MA: Fletcher School of Law and Diplomacy, Tufts University, 1998.

house data systems against a potential breakdown because of that threat?

Daguio: I must have miscommunicated. Some people in the defense community think that EMP risk is a problem for us. We're not convinced of it yet. So our claim is that if they're convinced it is a problem for us, it's beyond our capability to manage that. It is their obligation to manage it themselves. If they believe that the only way to manage appropriately against the risk EMP poses to our infrastructures is to have a ballistic missile shield or whatever it is, or scrap every nuclear device on the planet, it doesn't matter to me. It's their obligation to manage that. If I, as an individual operator of an infrastructure, with some operations that I'm responsible for, believe that I have to build a TEMPEST shield, which protects me against electromagnetic reading from afar, or shield against EMP, I'm perfectly willing to do that if I think that's appropriate for my business case. If other people are telling me to do it, I want to see some reasons why, and I want to see some money to pay for mitigation.

Oettinger: There is also a matter of policy. The question of whether one should encourage a civil defense against EMP, or appropriate money to destroy every Iraqi nuclear plant, et cetera, is clearly an issue well beyond the banking industry or the mattress manufacturers or the universities.

Student: There's quite a difference of threat perception.

Daguio: That's why we need to spend a lot of time together: because we have such fundamentally different world views and experiences that developing a common basis for communication and experiences is critical. That's why walking people through these infrastructures and listening to all of the partners talking in their own languages, and working through "Does this make sense ... from my perspective, from his perspective?" gave us some insight. Negotiating over cryptography export control, over government access to data, over authentication infrastructures and critical infrastructure gives us more insight to how everyone operates. At some point, it may be a close enough, friendly enough relationship that some people have to worry, but there are so many bumps in the road, and we're still so early in doing this, that it's too early to call it a threat to anyone.

Oettinger: It's an absolutely vital point that he's making, and lest you think that you will get a thorough exposure to this sort of thing in this seminar, you'll note that there is nothing on the program that brings in, for example, another major player, which is the law enforcement people. The dialogue that you're hearing about here is strictly sort of civilian-military. We don't have time to bring in a third major interlocutor, and there are others as well. I urge those of you who are interested in seriously thinking about this to do some reading, thinking, and talking to law enforcement people on your own, because their perspective is very different from anything he's articulated or I'm articulating.

Daguio: There's nobody on the planet outside of some FBI officials whom I ever heard espouse some of the positions coming out of the director's office. I've talked to some of the oddest individuals you could find in the defense community, and some of the oddest people in the private sector security community. They have perfectly reasonable positions for people in those jobs to be holding, but the reason why nobody else holds positions like the FBI's is because nobody else has a collection of responsibility for law enforcement, counterintelligence, and generally for being all-around good guys who are on top of things on an international and domestic basis. They've got ownership of a set of responsibilities that makes them unique and causes them to come to unique conclusions about how the world ought to work.

We have terrific battles about whether, for example, the FBI ought to have special devices as part of our networks that allow them to monitor all the traffic flowing over them to determine whether we're under a coordinated attack on our infrastructure, and enable them to respond on our behalf. That's a decidedly odd thing to be talking about. It's also unacceptable. But it's reasonable given their perspective.

A long time ago, people thought the NSA was the enemy of commercial security. I have to say that the NSA isn't the enemy; that the relationship between the banking industry and the DOD community, and especially the NSA, goes back a long time. We're grateful that the NSA helped turn Lucifer[5] into DES; it helped turn an algorithm that didn't work right and wouldn't provide us the security and duration of use that we got from this algorithm today, and they're helping us get where we want to go. My problem is that, unlike in some areas, there are no areas that we can ever clearly define as being ours or theirs. There are no parties that we can ever say are or are not invited to the table, because conditions and technology are changing so much, and the policy issues aren't even close to being settled, that all we have before us is a long stream of endless negotiations over issue after issue. I don't believe that there is any way specifically to establish a way of evaluating anything other than the bright-line issues. All we can do is establish a mechanism and policy that enable us to communicate openly among all the various communities as transparently as possible and to help us negotiate through them one at a time. It may seem somewhat haphazard, but we're moving in that direction.

Next month there is a coordinating committee meeting with 100 financial institution information ... risk officers meeting in the White House conference center. It's a meeting that we've been calling for in various forms for a long time. Discussions first appeared in the National Security Telecommunications Advisory Council report, a beautiful paper. I have copies of it electronically that will be up on my Web site. The call for this began in the report of the President's Commission on Critical Infrastructure Protection.[6] It appears everywhere.

Clearly, the industry has some ownership over some of the issues regarding how it ought to manage its risk profile, its exposure, and how it ought to be managing public policy. Equally clearly, that forum ought to be available for the government to share its interests with the financial community. This is the beginning of a mechanism that will hopefully negotiate those policies (actually, not policies—practices) one at a time over the next few years until we have a large enough aggregate of settled issues to have some clearly white space, clearly black space, and a somewhat defined gray area to make some of these negotiations easier. These negotiations have already gotten easier for us because we have some settled issues behind us already, and hopefully they will keep getting even easier.

The chair of this coordinating committee is the sector liaison for the financial services communities, Steven Katz. He's the chair of my information security infrastructure committee. We will have the secretary of the treasury and potentially some other senior administration officers stopping by to talk about these issues. Again, there are different interests to be managed. Treasury has its own interests. The banking industry has its own interests. The defense community has its interests, and the FBI and the rest of law enforcement have their interests. You will see, as a result of anything that happens in the long term, each agency and each community of interest negotiating for the best that they can get. Quite often you will see seemingly insane exemptions, small snippets of policy that are irrational except for one thing: one party at the table needed them in order to walk away with enough chits to be able to come back to the table again so he can negotiate on another issue.

That's the odd thing about negotiating policy in this environment. You cannot win outright. If you win everything, you've lost, because somebody new will show up at the table with some new set of interests that you have to address. It all comes down to balancing things. It makes me uncomfortable to know that there will be more and more battles like this ahead of us. But I'm hoping that you bright folks will prechew through some of those issues in advance that allow us to point to papers that say, "Hey, this issue came up," or "Hey, somebody wrote about that," or "Somebody was thinking about that somewhere." My guess is that I was probably the first person that DOD ever asked, "Hey, what happens if we blow up a financial institution that we have money in? Is that a bad thing?" We'd like to have more of these things set-

[5] Lucifer was an IBM project in the 1970s that sought to implement cryptography efficiently in hardware.

[6] See note 2.

tled, more thought put into these issues, because, frankly, my community is in no position to talk about these things at the level of detail you can. Some of these subject matters aren't appropriate fodder for discussion by bankers—or they may be, but they sure as hell can't write them down and publish them, or talk about them in public. EMP, and secret moles, and Van Eck[7] freaking, and TEMPEST technology, and things like that are only parts of them.

If you start talking about the rest of the critical infrastructure issues, there are things that are really odd for bankers to be addressing: protecting power infrastructure, protecting telecommunications, protecting water supplies, and things like that. We care about those things. We're involved in the community. We try to make ourselves as independent as anybody can be from those infrastructures. But we need them, and we try to support robustness in those areas as well. But we can't let that be a diversion from our primary obligations: to make sure that our stuff works, that it's standing even if nobody else's is, and that your ATM and your bank will be there functioning even if your local hospitals, and your local law enforcement offices, and your local government agencies aren't.

Oettinger: Take him seriously on that point. Many of you don't look old enough to recall that at the height of the Cold War, when there were arguments over continuity of government and maintenance of the central services in case of nuclear attack, aside from encouragement of building concrete shelters in one's basement, the U.S. Postal Service sent out little notices you were supposed to return to them about where your mail was to be forwarded in case of nuclear attack, which always struck me as somewhat silly.

Daguio: Some of the best analogies for what might happen post disruption are previous natural disasters as unscheduled tests of infrastructures. Quite often you'll find the only lit building in the entire surroundings is the bank building. You may find one government office ...

Oettinger: The telephone building too.

Daguio: To some extent, yes. The primary, central offices will be open, but the branch offices won't. We view those as tests. Other tests include the Y2K problem, and looking at how those infrastructures will stand up. Everything that has to do with contingency management has educational lessons for those of you who are looking at strategic information warfare as either a defensive or an offensive approach. I haven't asked who of you here is particularly interested in offensive information warfare.

Oettinger: Nobody that will admit to that, anymore than bankers would admit to wanting to rob other banks!

Daguio: I think if you look around, you will find that the tools to do horrific amounts of damage are nowhere near as refined and useful as many people say. If you look at actual operating infrastructures in the wild, you will find that the chances to do cookie-cutter attacks or create any major disruption are seriously reduced by the fact that these infrastructures were built a piece at a time and cobbled together. Nobody except the people who built them or the people who are following on in those jobs really knows what's going on inside. The important lesson that you walk away with after having seen this is that the person who knows how to damage it is the person who was there, built it, and maintained it, or is the vendor. So the greatest risks we face are not from really "cool tools" on the Internet. Instead, there are people walking around with information about weaknesses and specific infrastructures that are fallible and might either turn or be turned. In the end, it mostly comes down to people and not stuff. We try to build systems to take away control and manage the risk that those people create, but you can actually never do that.

Oettinger: The risk from disgruntled employees remains still probably the major source of threat to darn near anything.

[7] A Van Eck device picks up electromagnetic radiation emanations; TEMPEST technology is designed to defeat this type of monitoring.

Daguio: Absolutely.

Daguio: I try to separate "information warfare" into offensive and defensive, and I try to separate the use of information technology tools as a mechanism for doing damage from those tools as a target. Using a bomb and a guy in a truck to blow up a data center is fundamentally different than sitting thousands of miles away at a keyboard and trying to disrupt either physical infrastructure or information infrastructure. If any of you want to talk about that, I'd be happy to deal with it. Otherwise, I'll pop up some other issues.

Student: How likely do you think it's going to be that someone thousands of miles away is going to try to strike the U.S. government and/or information systems?

Daguio: Strategically or tactically?

Student: Strategically.

Daguio: You have to separate out those two things. In RAND's "The Day After" game, they had some really interesting scenarios. The object of the exercise from the bad guy's perspective in this case was to damage U.S. stability enough so that the United States was not in a position to respond to direct conventional attacks on allied countries elsewhere in the world. So the goals were to decapitate some decision infrastructure, to cause unrest in the populace, and to give people other things to talk about than just some foreigners losing their land.

I think that kind of thing is going to be relatively unlikely. I think it's almost never going to happen unless somebody makes some really, absolutely stupid decisions, and coordinates them better than anybody else ever has in the history of the world. I don't think you can actually wage an entirely cyber war, using no physical attacks, no physical presence, no special ops guys, and things like that. I have some friends in the offensive information warfare community whom I tease because they talk about being at the pointy end of the stick. I joke about them only having bananas to fight with. There is a Monty Python skit about people using fruit to attack each other, so there's an amusing but appropriate popular culture reference there.

The very real probabilities are that there will be a significant number of coordinated, tactical uses of information technology to gain economic and/or tactical advantage. It might be interesting—and distracting—to people to have their lives and their records disrupted temporarily, but erasing somebody's identity is beyond what's possible. It is possible to disrupt things, and that's probably the most fruitful avenue for people who want to use information technology-oriented cyber-type attacks. They can be fun to talk about, and things like that have happened.

Everyone talks about the public Internet. It's not really the "public Internet." Each little piece of it is run by technologists and policymakers in that organization, and when somebody is doing damage to their part of the network, they feel obligated to do things to protect it. You have seen some minibrush wars erupt over issues that have nothing to do with the infrastructures themselves, where people hack each other's ISPs (Internet service providers) and networks in an attempt to shut their speech down and/or disable their operations. A flame war is a very mild version of it. E-mail bombing is a very mild version of it. But there are people who literally stage coordinated attacks on the servers and the ISPs that other people with less popular viewpoints use as platforms to spread their ideas. When things like that happen, the operators of the infrastructure respond by kicking the bad guys who are breaking the rules and contracts off their networks. There are some really interesting techniques that these people have used. They're not debilitating, but they can certainly be annoying and disruptive.

Far more effective than any of the cyber attacks are some of the physical attacks that we've modeled. The ones that would likely have a significant chance of causing major disruption involve capabilities that only a state would have. They're beyond the reach of most state-sponsored organizations, and they would take pretty significant special forces teams and coordination to pull off. From my perspective, if anybody ever does that, that's not cyber war, that's not informa-

tion warfare, that's war. Again, that's not my responsibility.

Oettinger: This again goes back to this matter of indications and boundaries and so on. It's an extremely important point, because much of the anecdotal evidence has to do with what Kawika describes as these minor skirmishes. It's as if you took every nut who tries to take a shot at the President of the United States, and parlayed that into the possibility of full decapitation and paralysis of the U.S. government. You'd almost have to be crazy to take a shot at the President, and the idea is almost unstoppable, but by the same token, it doesn't make a whole lot of difference. So focusing on the amount of coordination and planning, et cetera, it takes to do something that has profound effects, and differentiating that from some act of a nut, is critical in arriving at some sensible and useful understanding of the true risks. To me the stipulation is that some hacker can get into any Web server at least once. Someone can knock off anybody in this room or almost anybody anyplace else, if they are crazy enough and suicidal enough, but that is not the same as disrupting anything serious other than the life of the unfortunate victim himself.

Daguio: One wargame scenario involved the use of 20 Oklahoma City-sized weapons all at the same time in downtown New York, plus at the same time assassination of some really senior government officials and financial institution officers. Managing against that scenario is not an industry responsibility. We don't own the city of New York. One would think that if somebody were attempting that, either the FBI or the CIA would know about it, and they'd be doing something about it. My guess is that if they knew about it, we wouldn't be the first people that they would tell. So we try to balance those things. We say, "Our guys will obviously protect themselves as well as they can. We don't own the cities. We can't close off Wall Street. We can't close off all the city traffic in the downtown financial district because we don't have the right to do it. Therefore, those of you who have the ability to do those things, and who have the information about when things like that ought to be done, ought to be doing the coordination."

Sometimes we just say, "It's not our responsibility, but you're responsible for *this*, and you're responsible for *that*, and if anything bad happens and you don't talk to us, you are on record as being accountable. Everyone knows that you fell down on the job, and it wasn't us." A lot of my job involves removing obstacles in the form of regulation, and/or making people accountable for stuff that they ought to be doing already, and, in some cases, making sure we're not responsible for stuff that we don't think is ours to do.

Student: On your theme of dividing responsibility, would you be able to give us a view of how many resources a bank will deploy for defenses?

Daguio: It's hard to figure it out, because a good bit of everything that a bank deploys in terms of infrastructure is intended to manage that risk. There are pieces of it everywhere. We've got really big books of policy. We've got these cultures and traditions that get pounded into people's heads. We try to select good people, and we've got infrastructure we've built. We don't rely on the infrastructure to do the job for us. We rely more than anything on the people, first and foremost: people who are working with each other, people who are making the hiring decisions, and people who are waiting for the step in the process ahead of them. We build policies that try to do that. We've built almost an intentional inefficiency into our systems to protect the reputation of the institution, of the financial system, and of bankers in general and individually. I'll give you an example.

There's something called a control total that is dear to a banker's heart. The idea is that if three people—A, B, and C—are involved in a process, at every step information will flow out of channels that none of them can affect, to make sure that what A gets from B is what A gives to C. It's a zero trust model—trust nobody, trust nothing. If you build a system designed to do that, you can build in tolerances for losses without risking catastrophic failure.

The systems that we build are not as good as the people whom we train. The systems

that we build are the best that we can create, but quantifying investment for security is almost impossible because we use so many justifications for the expenditures. I may have two processors in two different places receiving the same information to deal with earthquakes, but they can also help me avoid a problem with an individual manager who might affect a transaction, or an individual hacker who might affect a transaction. I might have cryptography deployed for authentication and secrecy. I might have it deployed for no reason whatsoever, other than that somebody on the board read about it in *BYTE* magazine and thought it would be a good idea if we did it in a particular place. So, we're just as irrational as everybody else is, but our community is more willing and more accustomed to spending money on it than any other community. We've got $5 billion or $7 billion a year invested in R&D. It's hard to figure out where that's going because people are pursuing really diverse agendas.

I would say if you categorize what you're looking for as robustness, rather than as security, it's got to be something like 30 percent innovation, and 70 percent efficiency and robustness expenditures because we're always looking for more up time and more efficiency. This may sound weird, but efficiency helps robustness because the faster you can process transactions, the easier recovery is, and the less window there is for bad things to happen. It's kind of an odd thing to split it that way, but it allows us to double count all our expenditures and make everybody with different interests happy.

Oettinger: Sometimes it's impossible to determine what is actually a cost. Does it cost anything? My example might be hopelessly out of date; it may no longer apply. It's been years since I was involved with the banking business, but when I was, one of the cardinal rules in the banks that I was familiar with was that every employee had to take vacations, particularly tellers, because any kind of check kiting, account juggling, et cetera, is usually very time sensitive. You were always suspicious of somebody who didn't take vacations, and it was policy to make people take vacations because that was the opportunity for a scheme to collapse, or an auditor to come in and so forth and so on. When data processing equipment was first introduced, that little bit of culture was lost because programmers don't take vacations. Most software shops don't enforce a take-a-vacation policy, and so there was a period when embezzling and one thing or another by the data processing people came to light, until everybody realized that if you're a programmer in a bank, you have to take vacations just like the teller. I have no idea what they're doing today, but my guess is there are similar kinds of examples. I don't know how you put a cost on that.

Daguio: Some institutions still require everyone to take vacations. But what we've encouraged them to do is to revoke access to all systems during those vacations, because it doesn't matter in some cases whether you're in the shop or outside it if you have authorization to do interesting things on critical machines. There is no industry-wide policy surrounding vacations anymore, and it sounds odd to build an information protection policy around ritual and tradition. However, the experience of having people trying to take money from you since your industry began is very educational, and you absorb very valuable lessons through osmosis.

What we're trying to do for all the bright young people who come in with MBAs and JDs and things like that, who aren't taught to become bankers by sending them to the basement and having them spend years and years watching experienced people do stuff, is figure out why we're doing things. By figuring out for ourselves what we're trying to do, we can separate out what really still needs to be done from what doesn't help us anymore, and explain them to people who want things explained rather than being told exactly what to do. That example of cutting off people's remote access is something that the old-line bankers didn't think of. It wasn't until we thought about what we were trying to achieve by enforcing that vacation policy that we figured out we had to do some more changing.

But it's extraordinarily expensive. Let's see if we can quantify it this way. As you probably know, the data encryption standard is very mature. Test messages that were en-

crypted with DES have been broken using a lot of pretty sophisticated, expensive equipment. The way we manage our keys gives us a lot of protection that isn't evident from the way that those attacks were done, but we recognize that there is a perception that DES isn't good enough. In practice, DES isn't going to be good enough for anything at some point far off in the future, and we have to manage against that. So we're changing all of the infrastructure we have in place to support stronger encryption algorithms. That means that every point-of-sale terminal in the country and in the world, every ATM in the country and in the world, will have to support stronger encryption. I think there are on the order of 10 million point-of-sale devices. However much those cost, it takes a lot of money to replace that stuff. Replacing parts of this infrastructure may cost a couple of billion dollars in the next one or two years, and that's just in the United States. It may cost a lot more than that, and that's just for point-of-sale terminals and low-level retail transactions.

If you look at all the security technology and all the money that's being spent on public key technology, that's an extraordinarily expensive investment. The expense doesn't come from buying a certificate authority or an encryptor; it comes from hiring somebody to integrate that really cute technology with your operations to make sure it enforces a real policy meaningfully. That's where the programmers make money and the integrators make money and the recruiters make money. In the end, all that happens is that you prevent something bad from happening. No one has lost money as a result of a financial fraud from DES being broken.

If we replace the infrastructure before that happens, that's a bad-news story avoided. It's a really expensive project to avoid a bad-news story, but that's what banking and lobbying are about. It's making sure that even if you don't get credit for it (and my guys would desperately love more credit for what they do, how hard they work, and the robustness of the systems they build), in the end, you get judged on whether something interesting happened and whether it made the news. For us, a good day at the office is when nothing bad happened. That's really what we're shooting for: that at some point in time people will just discount attacking our infrastructure because it's too much work. Part of that means destroying some myths that are out there in the general culture about weaknesses in all the various infrastructures, shining lights to point out who is benefiting from propagation of those myths, and, where appropriate, opening up our infrastructures to show people what we have, fixing things that are not fixed yet and then shining a light on them, so that eventually, when everybody sees what we've got, they're not going to be interested in messing with us. We'll never get to a point where people are just going to leave us alone, but it would be nice if we could.

Student: You talked a lot about vulnerabilities in systems under attack in information warfare. What about from the other side of the equation, like the systems themselves having protection from unauthorized access that is intended just to steal information? When you look at our national security systems, whether in the military or diplomacy or intelligence, from my nontechnical point of view there's a built-in tension that comes from people who are trying to use information technology as a tool to enable people who have work to do and those people who are trying to protect the systems from unauthorized use of the information that flows through them. From your perspective, how is this built-in tension unfolding? Does any one of the factions seem to be gaining the upper hand?

Daguio: It's awkward. Bankers are not only responsible for managing assets, they're also responsible for managing information. I'm talking about confidentiality, not really about privacy, because nobody has absolute privacy anymore; about protecting financial information against illegitimate access. If we define the mission to include preventing illegitimate access by financial institution employees outside of whatever contract arrangements you have, or getting rid of unauthorized, illegitimate access by law enforcement and then by bad guys, hackers, or other people, and if you narrow it down to the information that banks have, as opposed to things that other people have, you end up with something interesting and manageable.

For us, access to information in our systems could very well enable someone to emulate you well enough to allow them to make transactions. This means not only that we have to protect your money, but also that protecting your identity and the information about you is almost the same thing as protecting your money, because if somebody steals your account information, that person could then commit identity fraud and perform transactions. So we have to protect that information as much as possible. On the other side, there's a whole part of the bank that wants to cross-sell you on all kinds of other things to make sure that we can pay for this infrastructure. The people in that part of the bank want to use your information. Under most contracts, they're allowed to use it for relationship management purposes—to make sure you have access to all of the coolest, newest financial products so you're ready for whatever you want to do with your life.

Now the problem for us is that you also want to carry out transactions with other people. It's difficult to establish credentials and capabilities for transactions that allow you to do business with people outside of our network, and still protect your privacy, our reputation, and your assets and our assets at the same time. What you've been seeing over the last 10 years is that new technologies for payment systems are being offered, which have more and more privacy protection components to them. Some of them are really amazing. Some of those will solve a lot of the problems that we face. Some of them have characteristics that could potentially be terrifically more dangerous to the system, while having major benefits for individuals in the protection of what amounts almost to their "secrecy." Balancing those interests is amazingly difficult.

One of the people whom we liberated from the Department of Energy laboratories, the national laboratories, is David Fortney. He's now working for the Integrion Financial Network. He's a really smart, good guy. He used to work on a lot of nuclear stuff. He says that the problem of protecting what basically amounts to the keys to the banks is more complex and harder to manage than the problem of managing the secrets around nuclear information and the keys to nuclear command and control, because more people are interested in getting them, they're more generally useful, kind of more fun to talk about, and the penalties are really different. We're not talking treason here. If it's against the bank, we wouldn't mind raising the penalties for abuse of trust. But people view these activities in different ways. It doesn't seem as bad to a lot of people to do one versus the other, and so it's a more difficult problem to prevent completely.

We're moving faster and faster toward that, but we've got some protection, because a good percentage of our transactions—not the value, but the number of transactions—are still on paper. They're distributed in a process where basically no part of the processing environment trusts any other part of the processing environment. It gives us relative efficiency, because we've been doing it for so long, and a lot of protection. Fraud still comes through, but the system captures activity that could pose a threat, including the capturing of financial information. No one can capture enough information from a manual, paper item flow to do anything interesting with it that will affect the system.

Now, as more and more items become electronic, there are more opportunities to play with that information, to do things, and to capture information about people's identity and things like that. Again, not all of that information is flowing solely within our borders. The greatest threat is outside of the bank's "castle" environment. It's outside in the villages and elsewhere, in the merchants. Sears has a terrific database with all kinds of financial information about customers—including their credit card numbers and expiration dates—potentially capturing people's shipping addresses, purchasing characteristics, and things like that. That is a richer target environment for low-level attacks and/or organized crime attacks than the inside of a bank, and it's far easier to get into a merchant than it is anywhere else.

Oettinger: How many of you give a second thought to using your Star Advantage card?

Daguio: What is that?

Oettinger: It's one of the usual supermarket things that gives you a slight discount in ex-

change for capturing your identity regarding every transaction you make at the checkout counter.

Daguio: It's less efficient to interfere with, which makes it a harder target to attack, either from an information capturing component or from some kind of diversion.

Student: I wonder if I can take you back to some of your comments about debunking myths about vulnerabilities, and information Pearl Harbor ideas. I don't know if I share your optimism. I guess I have a more my cynical view of the world. Could I maybe pin you down on some of your reactions to the PDD 63? Do you think that's one of those scenarios where maybe some really smart people are a solution out looking for a problem? Are they using this information sharing, kind of cutesy get-together to talk about things as a fix for that, and you're going to shine some light on that situation?

Daguio: There are people out there with whom I have spent hundreds of hours who will admit that they have empires they want to build, and they're doing it because they think it's the right thing to do. They're not terribly unhappy that it will help them get their Senior Executive Service position either upgraded or else firmly fixed, and more resources. There are people with world views that are fundamentally different than ours about what risks are tolerable and what losses are acceptable.

We want to make our systems as robust as we can reasonably make them, and some of these folks have very different views about what these technologies are capable of and how we should respond. Mind you, we hire a lot of people out of those communities into our shops. Not infrequently, we give them "Get out of jail free" cards and say, "Lead the team. Try to take us down," and they can't do it. So, when some of the loudest voices on the side that says that we're not doing a good enough job, that we're open to decapitation or general disruption, can't even begin to prove their premises, we increasingly begin to doubt them. When they do have stuff to add that we didn't know about, we build that new information into our risk management practices and policies and try to accommodate it. It's not really that we don't believe anything that they say or believe that they're doing it entirely because of agenda, it's just that we don't agree about what ought to be done, and we don't agree on what our tolerable risks are.

You might arrive at the conclusion that if you weren't able to get money out of one particular bank's ATM for a day, that's catastrophic; a really bad thing. But if you can get the money out of other ATMs, that's not a systemic problem. If it is not a widespread phenomenon that would cause a crisis in confidence, I'm not terribly concerned, because there have been days where just for operational reasons the network goes down. To me, if we have tolerances for some kinds of operational outages—natural disasters or software compilation problems—we ought to have the same leeway in the other environments. Some of the people who are involved with the National Information Infrastructure Protection Center might say that if you can do something like that at all, that's intolerable. My position would be: "If it is, if you're asking us to move beyond our business case justification, then ante up, because it's not going to happen otherwise."

I don't mean to sound flippant, but it's really hard to figure out how to do it. When we made our field visits, we walked around and we looked at central office switches, we looked at routers, we looked at fiber lines, and we looked for converging paths of all these infrastructures. We looked at geographic dispersion—are things far enough apart from each other? If you hit one target, do you get another for free? Do you have concentrated loci of control between different kinds of institutions, not only financial institutions, but infrastructures that they rely on, like telecommunications and power?

What we walked away with is that while you can cause disruptions if you try hard enough, and sometimes even if you don't try—sometimes Mother Nature does it for us, and sometimes human ingenuity, or the lack of it, causes problems—you can't hurt us enough to put us down for the count. You probably can't hurt us enough to do anything more than make us mad and slightly disrupt some people's lives. But then we'll recover fully, and we'll be back in business having learned a new lesson. We tried to set it up as

almost a biological response mechanism: you make sure the organism is healthy, make sure it has the capability to learn from things that happened to it, and then you absorb the lesson and go on.

Oettinger: It's very rare that a single cause is sufficient to get a whole systemic breakdown. Without impugning anybody's motives, I think the Armageddon view tends to look at a pure, single cause where everything goes right. But, by and large, the real world is unclean. This, again, is one of the strengths of Rattray's use of the strategic bombing analogy, although one could find fault with it. It's a good example of a single approach being very devastating in theory, but in practice, what happens? You knock off a German ball-bearing plant and forget that Sweden isn't very far, and they get ball-bearings from Sweden. You neglect to calculate some of the defensive measures, like fighter cover for your bombers. In theory, if the bombers had gotten through, they could have done *this*, but in practice, they didn't get through.

These kinds of considerations happen here as well. Kawika mentioned earlier that real-world systems are made up of God-awful little bits and pieces that their own makers don't necessarily understand. Now, if you think about intelligence preparation of the battlefield, and you think of this battlefield that is incomprehensible to its own makers, then it takes a lot of "assuming" that somebody else can take it down. Again, it's not impossible, but it's a lot harder.

Daguio: I'm not saying that we can shrug off anything. I'm saying that if you want to do something, you have to have somebody there who knows how it's working, preferably on the premises, and if you're really going to do something, you're going to have to do more than push buttons.

Student: Along those lines, I just have to ask a question about the Y2K problem. How serious do you think it is in reality, not just from the banking system perspective, but for public services and so forth? What is your assessment of the potential for perceptions alone to create a confidence issue, even though there may not be a real thing there causing serious problems?

Daguio: All of these contingency issues, especially Y2K, are interesting lessons because they enable you to dig into your systems and see how things work, and test them, and do a sensitivity analysis. "If I do this, what happens here?" Thinking is always good, and we're developing new ways of doing risk analysis. We're moving from just the risk-adjusted return on capital kinds of stuff to some really fancy stuff that literally requires rocket scientists to model.

I used to be responsible for our Y2K stuff; now I'm only responsible for testing and the actual operations stuff, and making sure that enough cash—coins and currency—and actual electronic liquidity are available. You have to discount some of what I say because I grew up in earthquake country in southern California, and so I've always had food and water. I'm fine with that. I don't have a generator. You can't use me as a touchstone, because the reason why I do risk management contingency stuff is because I'm more paranoid than most people.

I believe that there are going to be disruptions. Nobody can say that every ATM will be ready and that it will spit out cash on demand. The problem is that if you only have four ATMs and none of them is working, that could cause a perception problem about your bank. Could it cause a perception problem about the whole financial system? No. Could a shortage of cash in one community upset the entire economy and cause end-to-end civil unrest? No. If none of the Social Security checks showed up, that would be a bad thing (and won't happen!), but short of that, there is no piece of the financial infrastructure that owns enough of the machines and the software and the people that could screw up enough to cause a general disruption in our society. It's impossible for all the money to disappear.

What can happen are liquidity problems and operational problems. "I really needed to make a payment to somebody on January 3, and I couldn't because something didn't show up." In all likelihood, my guess is that there will be bad information coming into the banks a lot of times, and some information

will be incorrectly interpreted as it leaves the bank. You will see banks caught in those chains of misinformation. But we've spent so much money on this damn thing, and done so much triage, that the critical stuff is taken care of. If it's really important, we're testing it over and over again, and stress-testing it.

Student: Is there any impetus to counter incorrect perceptions? That's probably much more disconcerting for the banking industry or anybody else: the PR piece that gets out that says, "It's going to be okay." Do you do much of that?

Daguio: We're doing a lot of that. I'm glad I don't have to do that. I help them out and tell them how stuff actually works and how things will probably respond under stress. We started planning for additional cash availability three and a half years ago. In addition to the disclosed cash that's available, we have a lot more that can be lined up, pre-positioned. All we need to do is monitor the environment, and we'll have more cash and more mechanisms to distribute it.

We will have everybody out there talking to everybody at every Rotary Club meeting, every Elks meeting, even going in and talking to children in day care if necessary. But the most important thing we can do is fix things first, and then show people how they're fixed. We then ask the people who are scaring others to show us things that are broken. That's probably the only way we can win, because some people think that bankers are self interested when it comes to this issue, and question the answers we give them. The best thing we can do is prove that we're okay, that we've taken care of the most important stuff, and that whatever happens, everything will be set right, and in the end it will be okay.

It's not entirely infeasible that a financial institution (probably not a bank) will disappear. A couple of financial institutions and a few credit unions closed recently, including one that I was a member of, that kept such bad records that it was impossible to set them correct ... ever. It wasn't a Y2K problem, it was just that they couldn't find the data to set their books in order. That is such a rarity when it comes to sophisticated financial institutions that it's unlikely. In order for an institution to disappear, it would have to lose all of the old records forever, and I don't know how you can do that if you ever had your books in order. There will be mechanisms in place to make sure that those institutions' customers get taken care of, either through a merger or liquidation.

There's much attention being paid to this issue. The discount window is basically open. I think that there will be increasing reassurance coming from the Fed, the FDIC, and others in Treasury saying, "Hey, don't worry. We've been inside these banks, and looked at everything." The truth is that in some of these institutions there are full-time, never-leave-the-bank-ever teams of ADP examiners who live in that bank. They know some of those systems as well as our people do, and they're not going to let anything bad happen because then they won't get that really big cushy job in one of the big fives, or big fours, or whatever else is left when they leave. A good part of what we depend on is that everyone is protecting their own self interest. Sometimes, when you look at the steps that are taken to mitigate risk, they may be taken only to preserve an individual's reputation. As long as it is not a complete waste of money, that may be good enough for me.

Oettinger: That's slightly scary, because in the "if it ain't broke, don't fix it" tradition, messing around with software and hardware is as likely to introduce bugs as to take them out. That's what worries me a little bit.

Daguio: That's okay, but we have a tradition of operating parallel infrastructures. When we do testing, it's not, "Hey, here's an interesting set of data," it's "Build one platform on a test environment that looks exactly like your operational environment." For a long period of time, we run real-life data through it and see what happens. We find out all kinds of interesting things, sometimes scary, before it goes into production, and, God willing, we catch most of the bad stuff.

Can I take two minutes just to run through a couple of things that we didn't get to? You will find, if you're interested in payment systems, that there's a strong con-

vergence of interests among some of the anti-money laundering community, the defense community, and the banking industry about some of the technology we're using. It may have a point relevant to your privacy question earlier.

One of the ways that the banking industry builds robust systems is by auditing the hell out of everything, leaving records in a bunch of different places (all of them strongly secured), and comparing them against each other. What that produces is a lot of information that has to be protected, and the existence of that information causes it to be interesting to law enforcement. Where they have legitimate interests, they'll pursue them. One of the interesting things about having book-entry systems, with journals in a lot of places that are audited, is that it gives you a lot of robustness. It helps to protect you against insiders; it helps to protect you against outsiders; but it also makes you less efficient.

Now, one of the biggest questions that Tony and I, along with a group of others, were talking about when we were doing an R&D study was: Will the banking industry, carrying all of the burdens from regulations that it carries, as well as the operational burdens from its history and traditions, be able to compete against people who are more fleet of foot because they're less regulated and carry fewer burdens from their cultures? It's a tough question. If I have a system that's audited, auditable, robust, and slightly slower and more expensive than a system that is really efficient and free, or cheap to near free, which one deserves to survive? In the short run, the one that prospers may be the lowest-quality solution, the less robust solution. In the long run, we hope we'll win because we're trying to do a better job. But the markets don't always produce those kinds of outcomes.

Oettinger: Think of the airlines.

Daguio: The oddest market in the world is the Internet community. The decisions to deploy technology generally proceed in directions that have nothing to do with people who have the most practical experience in actually operating stuff. People are moving from robust operational platforms with good operating systems, that have proven patches for them, to products that don't work much of the time. Providers do tremendous jobs of advertising them, but they don't deliver on what they promise. The solutions that are prospering, in a great number of cases, are the lower-quality ones.

It's a tough position for us to be in. We're hoping that we can manage it, but we are also hoping that everybody takes into account, whatever they do, that we're not the only game in town, and that there are some level playing field issues out there. It's not just about making one part of the U.S. economy bulletproof. It's about making the system work, and preferably, if you can manage it, making the whole global e-commerce system work right. There's no point in building a strong, robust U.S. economy if the rest of the world doesn't exist, because eventually ours will be wound down and dragged down by the fact that the rest of the world isn't open, running, and doing business as usual.

Oettinger: We've got to wind down, but before we do, thank you very, very much for a scintillating presentation. We're grateful to you, and here is a small token of our large appreciation.

Daguio: Thank you, sir.

INCSEMINAR1999

ISBN-1-879716-63-1