INCIDENTAL PAPER

Seminar on Intelligence, Command, and Control

Managing Your E-Business: Electrifying Reality
Albert J. Edmonds

Guest Presentations, Spring 2000
Charles E. Allen, Albert J. Edmonds, John J. Garstka,
Timothy G. Hoechst, Hans Mark, Dale W. Meyerrose,
Mark C. Montgomery, Scott A. Snook

May 2001

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 1-879716-74-7 **I-01-1**

May 2001

PROGRAM ON INFORMATION RESOURCES POLICY

Harvard University **Center for Information Policy Research**

Affiliates

Anonymous Startup
AT&T Corp.
Australian Telecommunications Users Group
BellSouth Corp.
The Boeing Company
Booz•Allen & Hamilton, Inc.
Center for Excellence in Education
CIRCIT at RMIT (Australia)
Commission of the European Communities
Critical Path
CyberMedia Convergence Consulting
CyraCom International
DACOM (Korea)
ETRI (Korea)
eYak, Inc.
Fujitsu Research Institute (Japan)
Hanaro Telecom Corp. (Korea)
Hearst Newspapers
High Acre Systems, Inc.
Hitachi Research Institute (Japan)
IBM Corp.
Korea Telecom
Lee Enterprises, Inc.
Lexis–Nexis
Lucent Technologies
John and Mary R. Markle Foundation
Microsoft Corp.
MITRE Corp.
Motorola, Inc.
National Security Research, Inc.
NEC Corp. (Japan)
NEST–Boston
Nippon Telegraph & Telephone Corp (Japan)
NMC/Northwestern University
PDS Consulting
PetaData Holdings, Inc.
Research Institute of Telecommunications and Economics (Japan)
Samara Associates
SK Telecom Co. Ltd. (Korea)
Strategy Assistance Services
United States Government:
  Department of Commerce
    National Telecommunications and Information Administration
  Department of Defense
    National Defense University
  Department of Health and Human Services
    National Library of Medicine
  Department of the Treasury
    Office of the Comptroller of the Currency
  Federal Communications Commission
  National Security Agency
  United States Postal Service
Upoc
Verizon

Managing Your E-Business: Electrifying Reality

Albert J. Edmonds

March 9, 2000

Lt. Gen. Albert J. Edmonds, USAF (Retired) is president of the Government Industry Group of EDS. He joined EDS in February 1998 as president of the Military Systems strategic business unit in the Government Services Group, and assumed his current position in January 2000. As president of TRI-COR Industries, Inc., from June 1998 to January 1998, he directed daily operations and managed all new business development. In his last position on active military duty, General Edmonds was director of the Defense Information Systems Agency from June 1994 to June 1997, where he also served as manager of the National Communications System and directed the President's National Security Telecommunications Advisory Committee. Earlier, he served as director of Communications-Electronics in Strategic Air Command's 3rd Air Division and as commander, 27th Communications Squadron. In January 1985, he became deputy chief of staff for Communications-Computer Systems, Langley AFB. He later served as director of the C4 Systems Directorate, U.S. Central Command, from July 1988 to May 1989. In September 1991, he was appointed director for C4 Systems, Joint Staff, Washington, D.C. His military awards and decorations include the Defense Distinguished Service Medal, Defense Superior Service Medal, Legion of Merit, Meritorious Service Medal with three oak leaf clusters, and Air Force Commendation with three oak leaf clusters. General Edmonds earned a bachelor of science degree in chemistry from Morris Brown College and a master of arts degree in counseling psychology from Hampton University. He is a distinguished graduate of the Air War College, and has completed Harvard University's National Security Program. In 1996, the Career Communications Group recognized him as Black Engineer of the Year.

Oettinger: Our guest today has to make a five o'clock plane, and I've got to get him out of here by 3:30, so we want to take maximum advantage of his presence here. Let me say a word or two about General Edmonds. If you've looked at the list of previous speakers, he has been here three times before: once as the director of the J-6 in the Joint Chiefs of Staff, and twice as director of the Defense Information Systems Agency (DISA), and he's gracious enough to come back this time in his private sector capacity as an officer at EDS. He's also an alumnus of our National Security Fellows Program. It's a delight to have him here with us once again. Thanks a lot.

Edmonds: Thanks, Tony. It’s a pleasure for me to come here today. I have a couple of things I want to tell you. I know some of you have military backgrounds, and some have civilian backgrounds, so I’m going to try to give a little bit of something for everybody.

I spent 33 years in the Air Force. I was doing computer programming before most of you were born. It was Boolean algebra, punchcards, breadboards, and the like, and technology evolved like a good wine. It got better with age.

I’ve come here before to talk about some things, but first I’ll tell you a little bit about myself. As Tony just told you, I ran DISA right before I retired in 1997. You probably have seen a little bit of information on the Defense Information Infrastructure (DII) that we were trying to create, with messaging, command and control, transmission, and combat support. That was my “house,” as I called it: the house that Al Edmonds built, the DISA house.

When General Meyerrose comes next week, ask him about it. Raise your hand and say, “General Meyerrose, can you tell me about the DII?” Question two, ask him about the Global Command and Control System and what a fused picture of the battlespace really means, because he was one of my disciples during those days and he worked on this with and for me. If he doesn’t give you the answer, let me know, and we’ll take good care of him. Question three: “What is the Global Combat Support System supposed to do for people?” The fourth question to ask him: “How would a coalition partner—meaning an ally, another country that we were trying to do something with—work together with us if the United States were trying to help somebody out, for instance after an earthquake, or in a contingency such as Bosnia, or whatever. How would another country participate? Would there be a system there to allow them to play this or not? What are you doing as an active duty guy now to make sure that can happen when you conduct coalition activities?” Those are the questions you should ask General Meyerrose, and see how many he can answer to your satisfaction. Give him a grade, and I’ll ask Tony how he did. So I just set him up, right?

I spent 33 years in the military working those kinds of issues, and believe it or not, industry has the same kinds of problems. The CEO, the chairman of the board, wants to have a fused picture of his battlespace every day, whether it’s EDS with 140,000 workers in 57 countries and all the states in the United States, or whether it’s a small company of $5 million a year with 100 workers doing whatever. The CEO, or the chief operating officer, wants to know: “How is my battlespace? How is shipping, how is invoicing, how is finance, how are operations?” Those chief executives want to know that every day, and if they’re really on top of their game, they want to be able to push a button on their personal computer (PC) and pull up some type of metrics or some kind of management system to get that data. The harder it is for them to get that information, the more sour they’re going to be dealing with their workers during the course of the day, because they don’t have a picture of the battlespace.

This means that you need good solid communications. You have to have some kind of messaging capability, whether it’s e-mail, or Microsoft Exchange, Lotus Notes, or whatever, and you’ll need some kind of support stuff: PCs, cell phones, Palm Pilots, whatever you’re using.

You’ve got to have some way to know that your systems are green, red, or yellow—operational, down, or whatever—because your customer is going to let you know. If you haven’t got a way to see it for yourself, your customer will call on the phone and say, "Get over here, Al. If you can't fix my business for me, you're out of here. Every minute I'm out, Al, I lose millions of dollars." That's how they talk in industry. They don't talk about putting people's lives in harm's way. They talk about, "Every hour I'm down, I lose this many dollars." When the call center that's supporting MCI goes down, the chairman and CEO of MCI picks up the phone and calls our chairman, Dick Brown, and says, "Dick, we've been out for 15 minutes. What are you doing?" If Dick doesn't know that MCI has been out for 15 minutes, someone else is going to get in trouble, because Dick wants a fused picture of his battlespace. He cannot afford not to have one.

At our headquarters down in Plano, Texas, we have an underground control room, about as large as the control room in the Pentagon where the Defense Department monitors its networks, where we can look at our data centers worldwide, and see how they're operating. We can go down to the circuit board in the back of it, read the card number of whatever is red or inoperable, and see there's a ticket open to let us know somebody's working on it and what they're doing about it. We have to do that for our business customers, because to our customers it's dollars and cents. For some of our military customers, it's life and death.

Do any of you military guys have an ID card? They come from DEERS, the Defense Enrollment Eligibility Reporting System. We've been running that system for 20 years for DOD. Now, we've evolved into the SmartCard.

This technology is going to evolve right along with what's happening in our midst, so it is absolutely no different. I changed my uniform, but the work I'm doing is about the same. I've been at EDS for a couple of years. I started off with military systems, doing just defense systems, and, believe it or not, I worked on the same stuff I was working on before. We were doing security in the data centers and all those kinds of things.

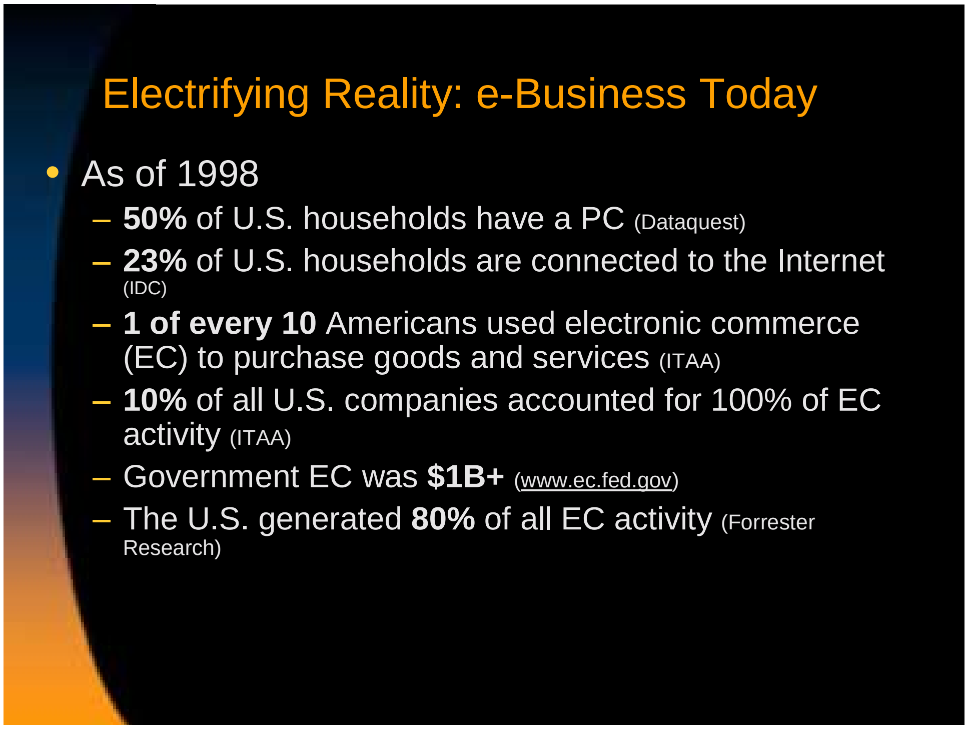
DISA pays the president of the United States out of Columbus, Ohio, from the data center there that DISA runs. When I got to DISA, I could go in there and check on his pay system because it wasn't secure. I fixed that. I got out and found that EDS was the contractor who fixed that for me.

Now, let me tell you why I'm telling you all this, because I'm going to talk about something very different from what you would think I would talk about coming in as a retired military officer. I want to talk about electronic kinds of stuff. I'm going to go through some slides. Stop me if you like, and I'll talk about anything you want to talk about in these slides. I want to stimulate your thought process to ask me about whatever you have on your mind, because this is a technological vintage that doesn't take 18 months, or 12 months, to ripen; it's 6 months or 3 months. As a matter of fact, every time you pick up the *Wall Street Journal*, another 25-year-old or 35-year-old got a great idea that's going to change the world.

People think you just go out into industry for money. That's not it. What I like most about my job today is that I do global government—that's state and local, federal, and international—because I honestly believe in my altruistic heart that what government does for its people should be good for all mankind. It's absolutely my belief. So, I believe that if we, EDS, or we, Harvard, or we, the United States, or we, China, or we, the Philippines, can provide better service to our citizens, our citizens will be better world citizens and they can communicate with each other better in common terms that we all understand and respect. To me, this information technology world is going to facilitate that.

You can't show me one mother on the face of this earth whose heart doesn't go out to a child who is hurt. You can't find me a father worth his salt whose heart won't ache when he sees a child hurt. Those kinds of feelings are common to the whole human race and, as a matter of fact, to the animal kingdom as well. Dogs, or elephants, or any part of the animal kingdom have those kinds of emotions, those kinds of common bonds. This type of technology is going to take that to another level: respect for your fellow persons, respect for individual rights and freedoms, individual aspirations, individual everything. That's what's good about this. That's what's so good about Harvard. That's what's so good about this kind of class, because we bring people from all parts of the world together and share our common thoughts and debate them, and we all go away as better people.

Let me go through my slides really quickly. Interrupt me any time you want. I have what I call a provocative title here: Electrifying Reality (**Figure 1**). The reason I do this is because I've been doing computer programming since 1964, though in a different form. Everybody thinks this is new technology, new everything. I have evolved with this stuff, and so, when I used to push STOP or START RUN on my computer, I thought that was starting the computer. Now they call it booting the system. I've been booting the system for a long time, but this is what I want to talk about.



Electrifying Reality: e-Business Today

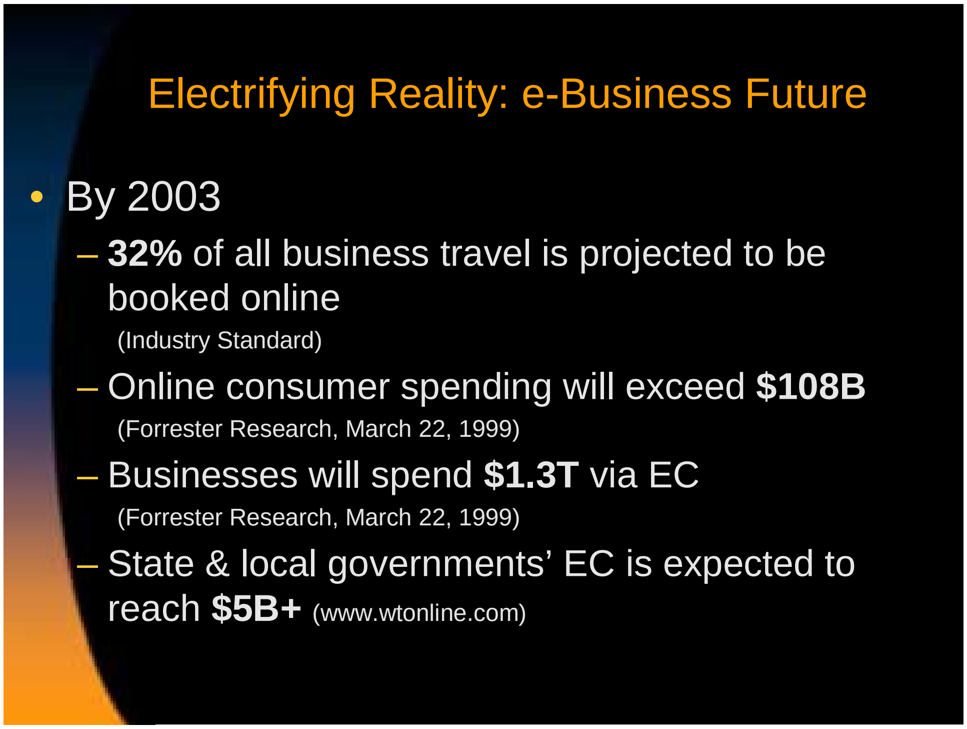
- As of 1998
  - **50%** of U.S. households have a PC (Dataquest)
  - **23%** of U.S. households are connected to the Internet (IDC)
  - **1 of every 10** Americans used electronic commerce (EC) to purchase goods and services (ITAA)
  - **10%** of all U.S. companies accounted for 100% of EC activity (ITAA)
  - Government EC was **$1B+** (www.ec.fed.gov)
  - The U.S. generated **80%** of all EC activity (Forrester Research)

Figure 1

I also do this because I want you to think like entrepreneurs. I want you to think that when you leave here, regardless of what you're doing, you can become wealthy one day, not because you went to Harvard but because you can take this electrifying reality and do something with it. Today, everybody worth his salt who wants to be elected to something, or wants to be in charge of something, will tell you, "I am going to go into some kind of e-business: e-government, e-trade, e-toys, e-billing, e-whatever, because that sells."

The president of the United States put out an edict to all those government activities that fall under the executive branch and gave them some specific tasks: by the year 2002 they should have so many of *this*, so many of *that*, and some of *this*. All those government activities now are building their budgets around doing those things they've been tasked to do, including on-line voting and on-line taxes. By the way, we at EDS do a lot of that stuff electronically right now for the U.K. and for Australia.

If you go through this list and look at what people anticipate is going to be happening in 2003 (**Figure 2**), I will just tell you that it's going to happen before that, because if you can conceive of this in 2000, what are you going to be doing for three years while you're waiting for it to happen? Everybody who sees this chart and this kind of information will say, "I'll bet that this 32 percent has already been booked." I haven't had a paper ticket for airline travel for about a year and a half now. I walk in, open my wallet, show my driver's license, and I get my ticket, and I can negotiate for a good seat. If they have my seat back at row 10, I get row 2. If they have any



Electrifying Reality: e-Business Future

- By 2003
  - **32%** of all business travel is projected to be booked online
    (Industry Standard)
  - Online consumer spending will exceed **$108B**
    (Forrester Research, March 22, 1999)
  - Businesses will spend **$1.3T** via EC
    (Forrester Research, March 22, 1999)
  - State & local governments' EC is expected to reach **$5B+** (www.wtonline.com)

Figure 2

seats in first class, I ask if they can stick me up there. I don’t want to have a paper ticket with my boarding card for row 22! I haven’t sat in the back of the plane for a long time now, because I do electronic ticketing.

On-line consumer spending, this good and great activity, is growing every day because of confidence. Business and state and local governments— every Governor I’ve read about—are telling the people, “We’re going to have government services on-line. I want every classroom to have the Internet. All the libraries are going to have the Internet.” When it gets dark, you can make speeches for governors, mayors, or heads of state on the Internet. “Every classroom will have Internet access. Every library will have Internet access. In San Francisco, we’re going to send the report cards home on-line over the Internet. No longer will you not know what your kid’s grades are.” This is the reality.

I have some figures on what I call “the global marketplace” (**Figure 3**). These numbers are really distorted for a very basic reason. Even in my company, we call a lot of activities “outsourcing.” It’s electronic business, but we like that nice term. What it really means is that we take the government’s business and we do it for them.

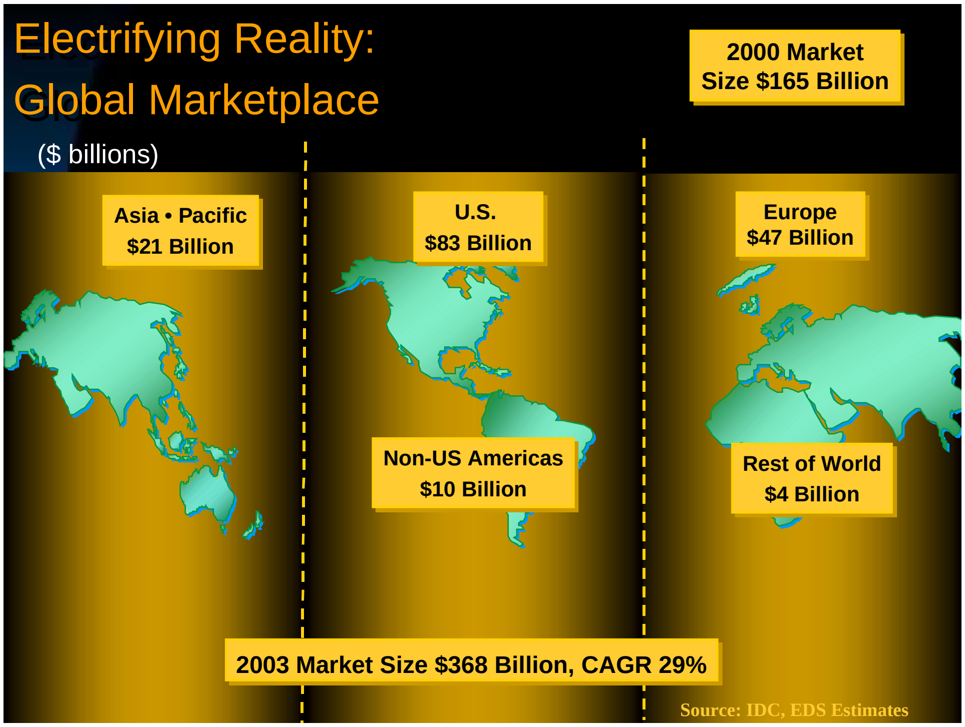
I’m going to talk quickly about market trends, enablers, and implementation issues. I’m going to talk a lot about information assurance, because my bottom line to you, and my thesis to you, is that we have to build a trusted business environment. It doesn’t make any difference if you’re talking about government, industry, or schools; you want a trusted business environment. You want to make sure that when I get something from you I have a pretty good feeling, like 99 percent confidence, that I’m getting it from you, and not from somebody else.

Then there are what I call market trends and business drivers (**Figure 4**). I won’t spend a lot of time on them. There’s also miniaturization. The world is getting smaller, what with air travel and the Internet. You can connect to anyplace you want to connect to on the face of the earth. All you do is tune your spot, and I can find it on the Global Positioning System (GPS). You put your earth station there; I can plop it down, I can put it in a suitcase or on my back, and I can put you right in here with no problem. Digitization gives higher quality throughput.

Ease of use is essential. Nobody wants to do a lot of typing. I never learned how to type. I’m up to about six fingers now, but I used to use one. But everybody wants to click and shoot, and everybody wants to reduce costs, increase value, and improve customer service. Whether you’re in the military, or in a bakery serving your customers, or whether you’re at Harvard and have students, you want to do those things, and it’s important to do them.

The reason for that is that everybody has tight budgets (**Figure 5**). We all know how to hang onto our money. If you have kids, you give them an allowance. You have tuition to pay, you have car notes to pay, you have a mortgage to pay, and you want to make sure that you give all of the public better services. We call it “improved citizen services.”

My mother-in-law does not want to put her check into the bank electronically. She wants to get it in the mail, and she wants to take it down to the bank and get it cashed. My mom was the same way. She got robbed one time in broad daylight. The thief watched her go into a store and



Electrifying Reality:
Global Marketplace

($ billions)

2000 Market Size $165 Billion

Asia • Pacific $21 Billion

U.S. $83 Billion

Europe $47 Billion

Non-US Americas $10 Billion

Rest of World $4 Billion

2003 Market Size $368 Billion, CAGR 29%

Source: IDC, EDS Estimates

CAGR = compounded annual growth rate

Figure 3

Market Trends and Business Drivers

Business Drivers

- Globalization
- Competition

Trends & Indicators

- Dis-intermediation
- Re-intermediation
- Micro-segmentation

Consumer Expectations

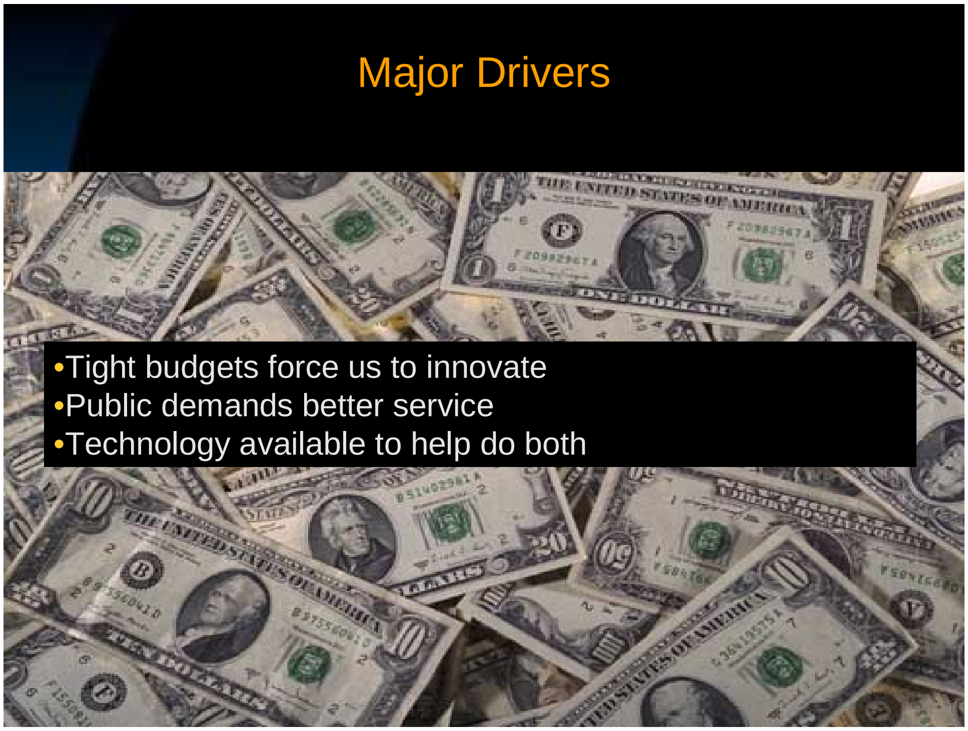
Technology Catalysts

- Universal connectivity
- Digitization
- Ease of use

Desired Business Results

- Reduce cost
- Increase value creation
- Improved customer service

Figure 4



Major Drivers

- Tight budgets force us to innovate
- Public demands better service
- Technology available to help do both

Figure 5

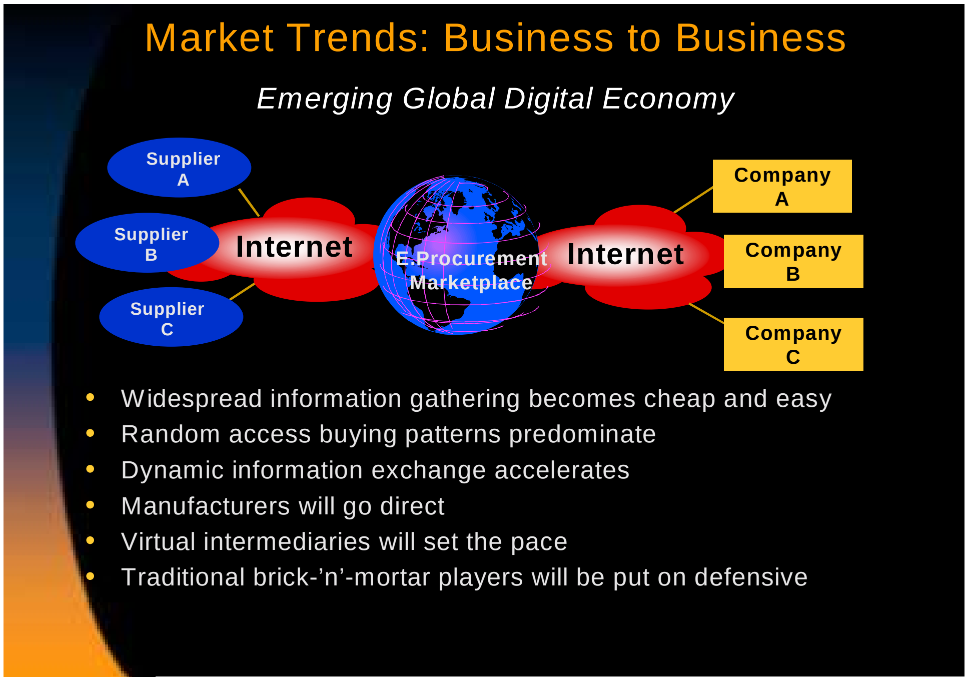
get her check cashed. She had her purse and was coming down the street with a bag of groceries, and he came up behind her and said, “Don’t turn around.” He grabbed her purse out of her hand, and she never went back to that store again to cash a check. She got electronic deposit right after that.

So people want better services. They also want to know what their Social Security entitlements are. They want to get their driver’s licenses. You can order a sporting license over the Net, and print it out at your home. You can go on-line down in North Carolina and say, “I want a hunting license or a fishing license,” and they will send it to you. You can give them your credit card number and they will take the money out of your account.

People don’t want to stand in lines. If you want to register your car in Washington, D.C., there’s one place in the whole city and you have to stand in about three lines. You have to stand in one line to get a form, another line to fill it out, and another line to tell you that you have the wrong form. I know, because I had a Washington, D.C., license plate for one year. I said, “Lord, if you will let me get through this one year, I will never get one again,” and I didn’t, because in the Pentagon, where I worked, in Virginia, they had a counter line to walk through and get your license plate easily, just like that. So being a military guy, I got a Virginia license plate. I don’t want to go to that one place in Washington and stand in a line. The services for the citizen are not very good.

Let me just tell you the kind of things that you’re going to be hearing. I did this on purpose, because I wanted to make sure you hear the things that you’re supposed to hear before you go back home. You will hear a lot of stuff about “B2B.” That’s business-to-business: businesses doing business with other businesses electronically (**Figure 6**). I need something; you have it; and we want to do business without somebody coming in between us. That means I don’t have a salesman coming to see me, or I don’t have to do something else. Suppose you’re my provider of routers; you’re Cisco, and I’m AT&T. Rather than have somebody come to try to sell me routers, I now have connectivity to you electronically through the Internet. So, when I need routers, I punch in my code, tell you “five,” and you tell the computer to take the order, pack it up, and send it to where I need it to go, B2B.

Suppliers and buyers can interact with each other through the Internet. Company C can go to Company A. As a matter of fact, in the Department of Defense, where I worked right before I retired, I put 500,000 companies in a database at the Defense Logistics Agency (DLA), which is DOD’s big buying agency. So when customer A or B wants something, all he has to do is go on-line and say, “I want to buy five tanks, or five boxes of toilet paper.” It gets out into the e-procurement marketplace in the middle of the picture, and all the companies that sell those things get this on their machine. They have a timeline. They can go back and say, “I will provide you five tanks, or five water fountains, for this price.” The buyer says, “Hmm, I have five proposals here. What do I want? I want proposal #2.” They accept proposal #2 and tell proposals #1, #3, #4, and #5, “Thank you very much, but no thank you,” and they tell #2, “Send it to me.” The seller ships the items and sends an invoice electronically, and the buyer transfers the money to them electronically. That’s electronic commerce.



Market Trends: Business to Business

Emerging Global Digital Economy

Supplier A

Supplier B

Supplier C

Internet

E-Procurement Marketplace

Internet

Company A

Company B

Company C

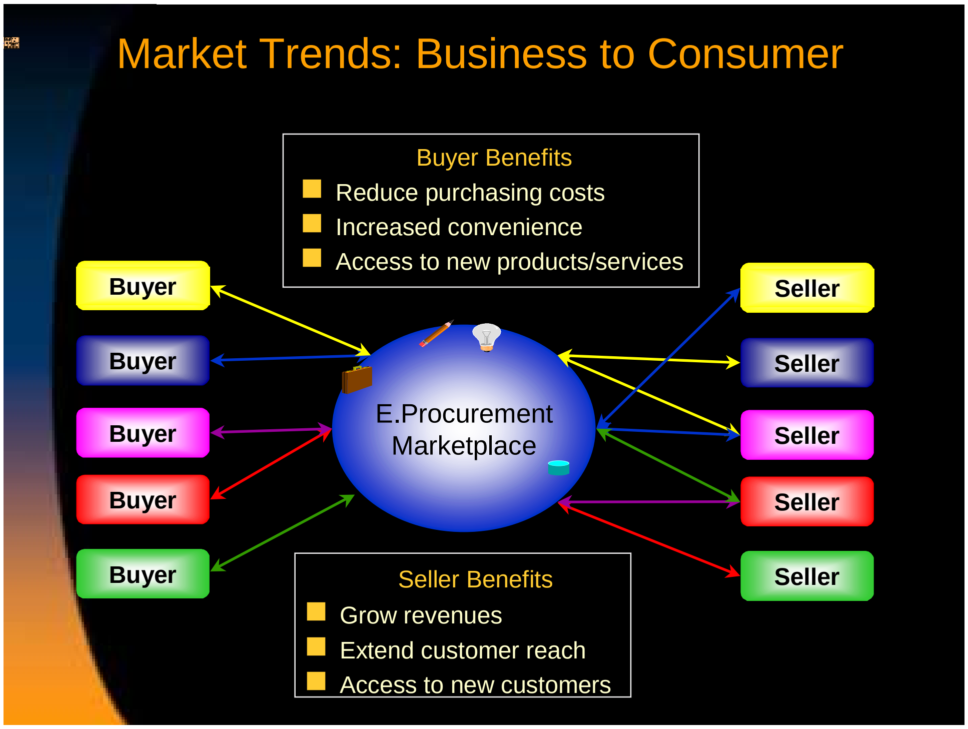
- Widespread information gathering becomes cheap and easy
- Random access buying patterns predominate
- Dynamic information exchange accelerates
- Manufacturers will go direct
- Virtual intermediaries will set the pace
- Traditional brick-’n’-mortar players will be put on defensive

Figure 6

One of the values of this is that you can get rid of en masse disbursement (**Figure 7**). We have a tremendous problem in the Department of Defense today with what we bought and what we paid for and the differences. This marketplace is a reality today. There is business-to-business, and there is business-to-customer. The real benefits here are that the guys who sell something will get their money fast. They don't worry about 45 days or 180 days before they get paid. The organizations that buy stuff can now reach more than 500,000 sellers, and those people, who never had all of those folks available to them before, now have a whole department they can sell stuff to. We registered them with DLA. That's the new environment. That's the market trend.

Student: You gave the example that the buyer can choose. In that case, do you think the market will reverse itself, in the sense that buyers will have more power because you'll have so many sellers? In other words, that it will be more of a buyer's market?

Edmonds: It's happening like that right now, as a matter of fact. One of the complaints that some of the sellers have today, and one of the reasons why people are changing their businesses, is that the buyers are in the driver's seat right now. For example, there was a time when you wanted a Dell computer or a Compaq computer or whatever, and you knew what it cost, and you might go to two or three different places to compare costs. Now you can sit in your office and say, "I want to buy 500 computers to do these kinds of things," and you can actually auction against Dell, Sun, Hewlett-Packard, or Gateway until you get the price that you want for what you want to do.



Market Trends: Business to Consumer

Buyer Benefits

- Reduce purchasing costs
- Increased convenience
- Access to new products/services

Seller Benefits

- Grow revenues
- Extend customer reach
- Access to new customers

Figure 7

As a matter of fact, it's so much so now that at EDS we don't even bid hardware anymore. We bid leasing the hardware for you, or we'll just auction it for you. We tell you that we'll do the auctioning for you and get you the best price for that capability from any of these sellers. But we recommend to our clients that we won't even buy the computers anymore; we just lease them for three years, with a three-year warranty. So we get all the maintenance done for free, and when those three years are up, you get another bunch of leases. Companies that can do that have a real advantage from a competitive point of view. That's exactly what's happening. You have to build Dell computers cheaper or faster or something, or with some "gee whiz" on them, because "commodities" like hardware are no longer a real factor in the marketplace. Your intellectual property has now become the most important thing: your flexibility to integrate all this stuff.

This is definitely the whole idea, and from a government point of view, which is what I was interested in, I wanted to put the government in that powerful position. I wanted to save taxpayers' money. The sellers don't like it. The more convoluted and complex the process, the more money they make, because they charge you for each step. They have to pack it up and get someone to ship it to you, and some of it gets lost or it's late getting there. You buy two or three, even though you need only one, because one might fail. When you get just-in-time kind of delivery, you get just the number that you need and this warranty, rather than owning something. You turn it in when it doesn't work. That's what you want. I have to say, I'm on the sellers' side most of the time, in that I do this kind of work for a living. But I represent the buyers a lot as an integrator at EDS.

Student: What did you mean by "making intellectual property more valuable"?

Edmonds: You'll buy a product from those folks who have good ideas and can solve your problems faster, or in a flexible way to allow you do more than one thing, and that costs a lot of money. They make a lot of profit from that. So you have to be a thought leader: you understand how to provide health care better, or you understand government. For instance, I consider myself a government person, and I can leverage government ideas around the world for EDS at a better price than somebody who doesn't know government very well.

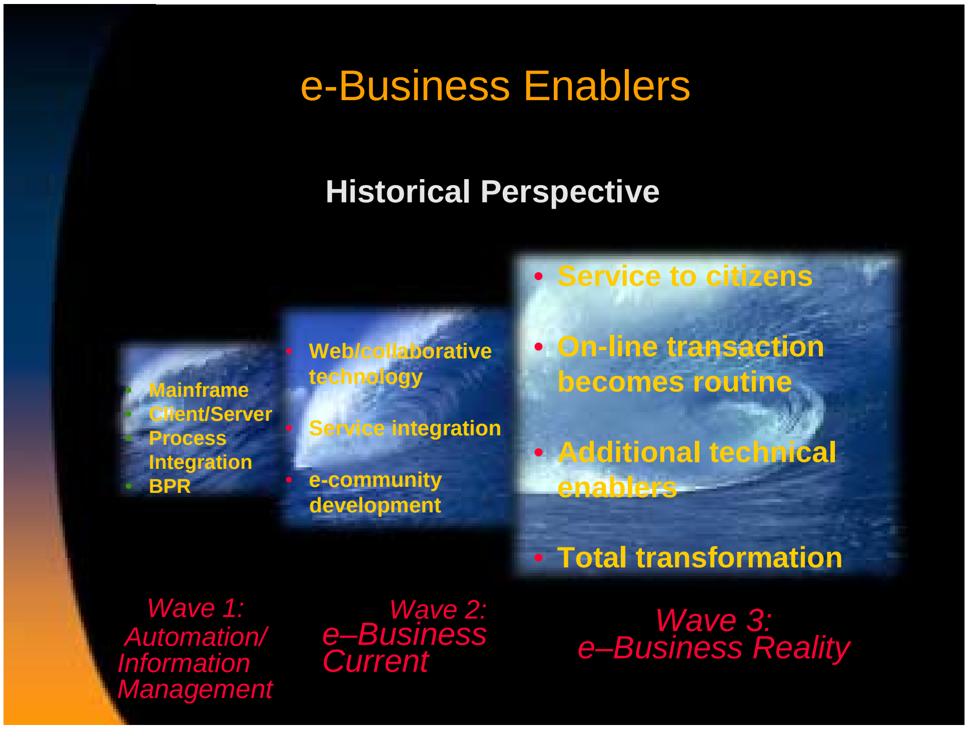
People in Amsterdam wanted to know how to do local government, how to do taxation, and how to do command and control systems, so I went to Amsterdam and talked to them about my command and control system background. What I talked to them about was the same command and control system that the U.K. has, because I know it very well. If I can sell them an 80 or 90 percent solution, and I only have to deliver another 10 percent to do that unique stuff, I have just made a lot of money. Most buyers won't select the company that has to sell them a brand new system to get that 100 percent, and start from scratch, and won't even get there for three or four or five years, because I have a solution here that will solve most of their problems. That's intellectual property, because that's your thought process, your brain power.

With hardware, you can take his box, your box, any one of these briefcase-sized computers, put it on the desk here, and we all can use it. You might not know how to boot it based on his password, but you know how to use it. So those things will become nonentities in terms of the competitive environment, because you can get better prices on-line at auction.

Let me give you a little bit of historical perspective (**Figure 8**). You might already know this, but this bottom line says it all. We had a mainframe environment: client/server, process integration, and basic business process re-engineering. It was all big stuff. We did that. Right now we're doing Web collaboration technology, service integration, and e-community development. But the third wave shows my focus on things like service to citizens: on-line transactions for people, additional technical enablers, and all kinds of enablers.

Wireless is going to change the world. We'll be doing other business: the telephone lines, the fiber that we've been so ecstatic about, are going to go away. The wireless people are coming, and they're going to come in big time. We're coming in with a wireless communications capability. As a matter of fact, if you have a Palm Pilot 7 (I have a Palm 5), you can do your emails on a Palm computer. Every 30 minutes your stuff gets enabled, so you can go back to your email server, wherever it is, on a Palm 7, which has a little antenna on top of it, and you can download your email wireless.

The transformation I'm talking about is going to be the electronic business reality. Delta Airlines will be able to give you a discount if you order your ticket on-line. If you're going to take a vacation with your family and you get a 10 percent discount because you have a $3,000 or $4,000 bill, that's not shabby! I'm going to take the family to San Jose in April, and it's about $5,000 for all my crew to go. Add it up: 10 percent of that is significant. I can rent a car for a week. So this is not just technology for technology's sake; it's happening.



e-Business Enablers

Historical Perspective

- Mainframe
- Client/Server
- Process Integration
- BPR

Wave 1: Automation/ Information Management

- Web/collaborative technology
- Service integration
- e-community development

Wave 2: e–Business Current

- Service to citizens
- On-line transaction becomes routine
- Additional technical enablers
- Total transformation

Wave 3: e–Business Reality

BPR = business process re-engineering

Figure 8

Let me talk a little bit about some of the implementation issues facing government and business. I want to deal with them a little bit more, because these are the controls that you were talking about earlier. They are also the realities that are going to keep haunting us as we go through this transformation.

Taxation and customs are really important. You can go in and out of the United States pretty easily right now. The Customs folks are looking for technology more than anything else: “What are you smuggling, technology or drugs?”

I don’t have my INPASS card, but if you’re a business person going in and out of the United States, you can now get a card called INPASS that we at EDS provide to the Immigration and Naturalization Service. You go through a little aisle and snap your card through, and if you put your hand in it, the biometrics gets your fingerprint, handprint, and eyeball print, and you can just walk through the line. People are moving technology and stuff so rapidly that this taxation and customs part is a big issue.

The government has put a three-year moratorium on taxing the Internet, but this electronic payment business is going to be booming. Everybody is afraid of putting out too much cash, giving you a check for $1 million instead of $10,000. But electronic payment systems are happening.

Intellectual property protection we talked about: This is *my* software. *I* developed this. This is *my* idea. I’m working for *this* company.

We are trying to create a uniform commercial code (UCC) for electronic commerce as a de facto commercial way of doing business. Corporations will do this rather than government. We’re evolving those codes.

Student: Is this being conceived of as an international UCC?

Edmonds: Yes.

Student: What is a commercial code?

Edmonds: We’re trying to create a commercial code for how we’re going to do electronic business among industries. At one time, the government was involved in it, and they just couldn’t get started. You’ll find that people like Bill Gates and Larry Ellison, especially some of the big software development companies like that, spend a lot of time in Europe and in the Pacific trying to get their counterparts to agree on some uniform codes for commercial businesses.

Student: I’ve got to believe that governments are going to want a big piece of this international electronic UCC. It’s going to shape how businesses, how economies, grow for the next dozen years.

Edmonds: They do. The only problem is that when the governments do it, the bureaucracy tends to get you a five-hump camel.

Student: How do you overcome this? How do you keep government from smothering this?

Edmonds: As a matter of fact, I know personally that Lou Gerstner from IBM, Bill Gates of Microsoft, and Larry Ellison from Oracle have been working with other industry people in countries around the world. They say, "Let's not let the government capture this." Now, having said that, I will tell you that the U.S. government embraced those same people to try to make sure that they understand what the U.S. equity is in that.

Student: What is meant by U.S. equity?

Edmonds: U.S. equity is what is good for U.S. business; in this case, what is good for U.S. business from this code.

Student: And government is trying to point out their view of what that is?

Edmonds: No, from the U.S. point of view, what is good about this code? When it goes to the U.K., Tony Blair and his government will tell the same people, "Here's what the U.K. thinks." For the rest of Europe, the Euro-dollar kind of thing, a lot of the economy has changed, and the big issue in Europe is the European economic environment. How are they going to function as one? One of the big areas of concern is, "If we've got to do this electronic commerce in Europe, are we going to do it as one entity, as one European environment, or as individual sovereign countries—as Germany, Spain, or the U.K.?"

Student: How about the Asian environment: Japan, China, Thailand, Indonesia, and India?

Edmonds: Yes. As you keep evolving this, as we said at lunchtime, the World Trade Organization (WTO) becomes important, because it gives you a framework in which you can work because they have some rules already. What you try to do is make the rules you already have evolve, or transform them into something that you want them to be.

Student: What you're envisioning is going to overtake the WTO. It will make the WTO virtually obsolete on this.

Edmonds: It will make the WTO pro forma rather than active. Right now it's active.

Oettinger: That's the dream. There are other folks with other views, and so there will be umpteen years of *Sturm und Drang*.

Edmonds: Absolutely.

Student: How would it overtake the WTO?

Edmonds: What the WTO does now is sit down and negotiate rules of trade: how we're going to trade with each other, how we're going to sell things and buy things from each other. They have those rules established. They deal with things like copyright laws, trademarks, service marking, all those kinds of things. Once you get a uniform code for electronic commerce and you start doing your business electronically and those things become uniform and universal, it becomes kind of a moot point to sit down and negotiate more of them, other than when they have changes.

Student: And this is different because this is folks just focusing on electronic commerce?

Edmonds: Try to think of electronic commerce as a medium. Commerce is commerce. We've had commerce since the beginning of human history. It evolved from bartering. You trade one X for my one Y. What's happening now is that we can move stuff faster. We can pay for stuff faster. We create new stuff faster, and, by the way, people create different things. Do you remember when I showed you the buyers and sellers (**Figures 6** and **7)**? Think about those as nations rather than people. If we could do those same kinds of things with the Internet and you've got a community based on these rules, that's what we're talking about. But we're taking it from a people-to-people thing to nation-to-nation, or hemisphere-to-hemisphere, or industry-to-industry: automobile-to-automobile, automobile parts-to-automobile parts, health care-to-health care. Just think of anything. I can go on-line to buy what I want with my PC, and if I'm a nation, I'm going to permit my people to do this using these rules of engagement.

Student: The UCC would be more businesses sort of defining what the rules are, but with the WTO it's more nations sort of defining them?

Edmonds: Yes.

Oettinger: Then, depending on who gets annoyed, either with respect to those corporate entities or with respect to the WTO, you might have the kinds of events that you had in Seattle where some folks suddenly said, "The WTO and all that are not speaking for me." That's why I said that's the dream. Details of what will happen have yet to play themselves out, because you've got different stakeholders who would rather have the WTO make the rules, others who would rather have a bunch of companies make the rules, and some who say "a plague on all their houses" and want it to go away.

Edmonds: Exactly.

Student: Is this going to become like a giant operating system for world commerce? If your program doesn't run on the operating system, nobody's going to want to deal with it.

Student: I think that could be a danger.

Edmonds: What would be dangerous about it?

Student: One could argue in terms like the idea of public space, where you could have people who don't hook into the overall structure. Some people may be excluded, because they are saying something or doing something that doesn't fit into the overall structure of the architecture.

Edmonds: Let me take that in a pure sense, rather than in a social sense. In a pure sense, you're absolutely right, because that's exactly what you want. You have a code of conduct, and if you're not governed by that code of conduct, you don't show up. One code of conduct, for example, is that you wear clothes when you come to school. If you decide you don't want to wear clothes, you can't come to school, because you just violated the code of conduct. Do you see what I'm saying? That's the pure sense.

In a social sense—and this is probably a better position—that's the issue of the digital divide: namely, leaving part of the world out of this whole process. That's why we are all interested in making sure that countries, as well as the people of countries, are included in this process, so that you don't have a good chunk of humanity not participating in this environment.

Oettinger: You might try to put it another way. It is very useful to have a common currency, because trading without a common currency goes back to barter. It is extremely inefficient. Now, having a common currency does not necessarily guarantee the elimination of the divide between the rich and the poor. It's the same thing here. Instead of talking about paper currency, you're talking about procedures that work on an electronic basis. Whether that's good for the rich or the poor is another question. They're obviously related.

Edmonds: Let me flip through a couple more of these slides, and we'll come back to that. I've got some privacy stuff to talk about. Privacy is important, because all people want to think their conversations, their transactions, are theirs and nobody else's. This is one of the threats to what we're trying to do, because you can always find some people who will make you wonder if this is good or not because they've had their privacy violated.

Telecommunications infrastructure and information technology are becoming so good and so pervasive that they have become a nonissue. EDS has just made a bid on a Navy/Marine Corps job for several billions of dollars, and I can tell you, we're basically giving this technology away. We're not talking about circuits or telephone lines anymore, or making you pay $25 for your telephone. We're talking about 500,000 dial tones, because those dial tones are riding on the technology that is doing all this other stuff. We're not buying these things separately anymore. We're now ("we" being EDS and MCI and all the other companies) trying to move the government and eventually companies away from thinking about "I need to buy five telephone lines" to "I need multimedia. I want video. I want voice. I want data. I want all of them, and I can get the widgets to provide me the wherewithal to multiplex it and do what I want to do with it."

Content is really critical. Who is going to manage the content of the stuff you're using? In the Bosnia operation, one of the biggest problems we had was managing the information that we were putting out there. We had so much information—intelligence, operations, weather, and all that. Who was going to manage how much stuff you gave the boss on the ground? Who was going to manage the information the boss or the CEO got in his office in the morning?

You know about technical standards and efficiency. You want to do it the best way.

I'm going to talk more about security and information assurance, because this is important. It's a foot stomper. This is on the test. This is what you're going to find on your final examination. As we worked all through 1998 and 1999 on Y2K, this thing called information assurance was probably the biggest problem. Security is the most significant impediment to talking advantage of the explosive potential of e-business. These threats are real, and they're evolving. They're not necessarily threats because there are belligerents out there trying to make problems for people. The threats are real because it's fun. It's neat! There's a commission for hackers, and you must have hacked into two major systems to be invited to join.

In my last life, I had about 50 guys and gals in one group, and what they did was continually probe and check my systems to make sure that they were okay. I never ever said they were all okay. They never are. I made that analogy in the Pentagon. The Pentagon has about 5,555 windows. You can close 5,554 of them. If you leave one window open, you can still get in. That's the way this stuff is. If you bring one disk with a virus on it to the office, you can boot everybody else's machine. If you send a photo with one pixel in it that will allow me to come back and get read/write capability for your software, I can control your system. If I get root access to your system, I can control whatever the system does.

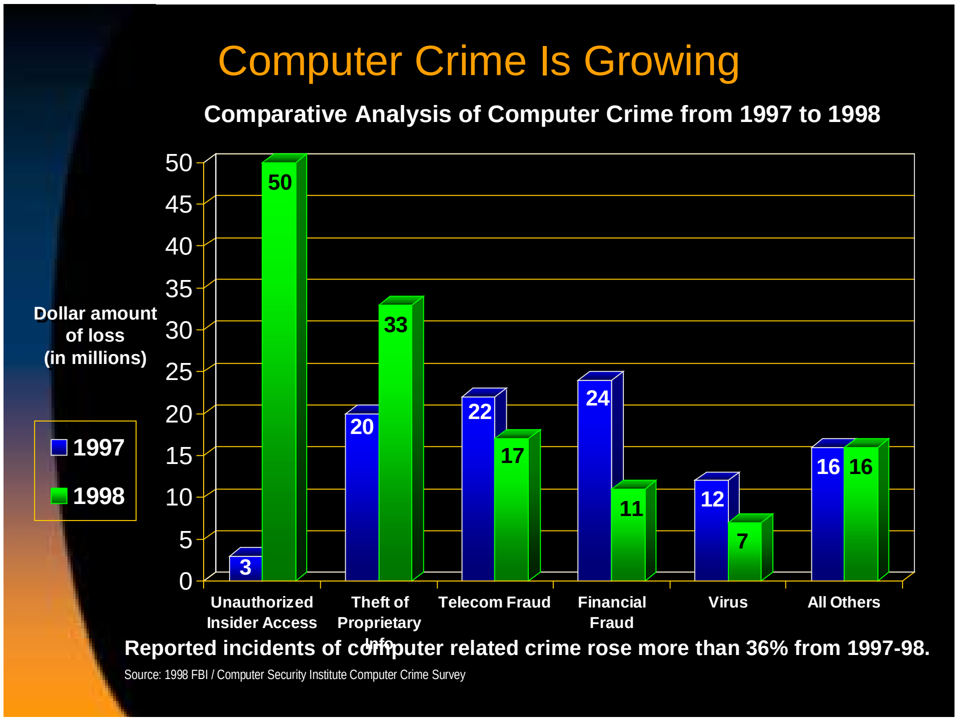
Let me show you a good example of what's happened over the years (**Figure 9**). The blue, or left, bars are 1997; the green, or right, bars are 1998. These are incidents of computer crimes: financial fraud, telecommunication fraud, theft of property, unauthorized access. There are so many free tools on the Internet that you can just download and use them. The other part of the problem is that companies like mine, or banks and financial institutions like credit unions and insurance companies, have no interest whatsoever in telling the world that we are under attack or have had our information exposed or violated, because it undermines public trust in our entities.

So, we have a dilemma. The dilemma is that we don't want the government involved, but the government has the wherewithal to help us. But we won't tell the government, which is willing to fix the problem. There are two or three entities around, and I've participated in two of them, that are trying to work this problem for the United States and to a lesser degree for the world: how to create confidence in these systems for information assurance.

What is information assurance? First of all, you need a security architecture for your systems, whatever they are. I don't put my banking stuff on my computer at home. My EDS computer at my house is separate from my home computer. My home computer runs my household; and, frankly, it's my wife's computer. I just use it to say hello to my friends. I personally don't put them together, because I've got a particular kind of capability on each one and I don't want to mix or cross them. I don't want to manage them every day. I don't have anybody at my house now who will do that for me anymore. I have to do it myself. So my architecture is a very simple one: I split my two systems. One has real firewalls and stuff on it; and the other one doesn't have anything on it but my password and whatever, and I change it once a year. I need to make sure that I don't violate the EDS environment I'm working in. Information assurance provides confidence in the security architecture and in security policy, implementation, and enforcement. It encompasses the active assessment of the business and regulatory environment, systems, people, and processes.

You've got to have continuous, proactive defensive operations. You can never fix all the problems. The day you think you fixed your system, you think you're okay, you're riding off into the sunset, and *pow!* I'll tell you that the next day all your systems will have problems again.

Some of the superb encryption products offer free privacy, triple DES (data encryption standards) policy features, but most of them do not. What you're really trying to do here, whether you're in business or whatever, is to maintain a trusted business environment. I need to know that I am getting information or data from the person who is who he says he is and if he sends it to me, I can almost look at it and say it's correct.


Computer Crime Is Growing

Comparative Analysis of Computer Crime from 1997 to 1998

Reported incidents of computer related crime rose more than 36% from 1997-98.

Source: 1998 FBI / Computer Security Institute Computer Crime Survey

Figure 9

Are any of you old enough to know what a slide rule is, besides Tony and me? One of the basic premises of a slide rule was that you had to have an idea of what the answer was going to be. You couldn’t do your SATs with it, because they gave you the choice of 1, 10, 100, or none of the above. If you didn’t have an idea of which it was, your slide rule would give you the 1, and you could put as many zeros as you wanted after it. If they asked you how many ohms there were in something—6, 60, or whatever—unless you had a clue, the slide rule didn’t help you. You were in trouble.

This is the same thing. You’ve got to have a trusted environment. You’ve got to have an idea of what your environment should look like. You have to have an idea of what the information you’re receiving should look like. If you don’t, you don’t know what you have. It’s easy to masquerade. It’s easy for him to intercept my message when I try to communicate with you, and to look like me when it comes to you. By the time he’s done it twice, he has everything he needs.

Student: That’s in order to do business.

Edmonds: Government or business, it doesn’t make any difference. Suppose I’m in business, and I’m dealing with General Motors, and I want 25 cars delivered to my showroom, and I want them by Good Friday because I want to have an Easter sale on cars. If Tony intercepts my message and tells GM to send them in May, I’m going to have this Easter sale with no cars. That’s doing business.

If I go on the military side and I say, “Meet me on Trolley Hill number 505 in Korea at 0500,” and you get there at 0500 but the enemy has intercepted my message and sends some lowflying airplanes over that same hill at 0510, you're in trouble. You've been exposed because they intercepted the message. It's the same thing. You've got to have a trusted environment.

The difference is that the military guys will put a piece of encryption on it to make sure it's safe. NSA, the National Security Agency, will buy a crypto to make sure that message is what it's supposed to be. They have some authentication at the bottom with funny little codes on it. In the commercial world, the business world, we have a tendency to be a little more lax and to say, "Oh, I don't have time to get involved with that stuff. It costs money. Here's my bottom line." What we don't really understand is that it will hurt our bottom line worse if we don't do something.

Do you recall when the Indian government fired off the nuclear missiles and Pakistan did the same thing? Everybody got excited, and we were going to embargo their trade and do all that stuff. The one real problem that we had was that a lot of what was embargoed was software development, because a lot of U.S. corporations have their software developed in India. So I had this discussion one day. "What about this? Does this impact you guys?" The industry guy said, "Yes, it does, but most of the stuff was transmitted over a communication line." So my next question was, "You're not worried about that?" He said, "No, not really." I said, "What you ought to do is put information assurance software on there to make sure you get the software the way you're supposed to." He said, "I don't put anything on it." I said, "Why don't you put anything on it?" He said, "It's a just lot of data and gobbledygook."

If you think about that for a moment, if you're a software development company, you get your software developed in India, and you transmit it in the clear, and you don't protect it, you might get anything back. So we told that company, "We recommend you use at least some privacy systems to make sure your system is trusted."

Student: Sir, has your view of secure encryption, or hard-to-break encryption, changed since you moved from government to industry?

Edmonds: To tell you the truth, it has probably gotten stronger. If I were transmitting that software from India back to here, I'd protect it as much as I would protect command and control from the military, because it gives me a commercial advantage.

Student: I guess where my question is coming from is that the government was interested in having something like the Clipper Chip, where there is perhaps a back door for the NSA or something of the sort, whereas industry was vehemently opposed to that. Has your view changed?

Edmonds: Yes, it has changed to some degree. I think there are better ways of doing that. You've got to allow U.S. companies to sell and compete in the international market, because if you don't, you lose your competitive advantage. There are other entities that can offer the same capabilities and you're at a bigger disadvantage. So I think that is an extreme position that is not very practical or very viable, and it becomes less practical every day. I know that the government is trying to move away from that to some degree.

Student: Did you think that when you were in DISA?

Edmonds: I had the same logic about it, but sometimes where you stand is where you sit. If you serve in the government, you've got to support the government's policy positions. Once you're not in the government anymore, you can still have your position. The only question you have is one of integrity. So my integrity reasoning says that the position I took was okay, because at the time we didn't have the flexibility that we currently have in technology. The issue was more black and white yesterday; today there are some shades of gray, and those shades of gray tell me that I can protect my systems, not with encrypted things, but with a privacy feature that is good enough for the industry that I support.

As a matter of fact, I designed all my systems with that in mind. I would put the family jewels in a network called SIPRNet (Secure Information Protocol Router Network), and encrypt the whole darned thing. Those things that were not the family jewels I put in NIPRNet (Nonsecure Information Protocol Router Network), which is an unclassified net, and didn't encrypt it. People went in now and then and messed up a Web page and did things to it and all, but those were the rules I made because I didn't have the luxury of the shades of gray in the middle. I made that very hard decision, and that's the way I testified all the time.

Oettinger: One of the tradeoffs there is that if you are on the one system and not on the other, you've got too many boxes on your desk and they can't talk to each other, and it becomes a pain in the neck.

Student: Exactly. That's something I was going to ask you about a little bit later. For the last several years I worked in the J-2 staff in CINCPAC. One of the issues we dealt with was multilevel access, which was always just around the corner. That would mean that you could sit down at a computer box in the command center and if you had a CONFIDENTIAL clearance, you would only get CONFIDENTIAL, or if you had a high-level clearance, you could get access to everything that your clearance allowed. Of course, if you are working intelligence, where you are constantly dealing with high-level clearance stuff as well as unclassified stuff, you don't want to have 12 different boxes, and that is really what you'll find in those intelligence places—all kinds of different boxes having different categories of information.

Oettinger: This is one of the places where the limits of technology, and the desires for assurance and so on, are still in a state of evolution.

Student: So it's still out there. Are we getting closer?

Edmonds: That's a good question, and I'll tell you two things about it. I had breakfast this morning with Mike Brown from Litton, who has been in this business a long time. He's also in the shipbuilding business. I recall that about 10 years ago Litton invested a lot of its own money in a multilevel security terminal. Then Honeywell invented the HoneyMacs, and we at DOD contracted with them to do that. They developed them, but it took so long that when they got there we didn't want them anymore.

You've got Scott Air Force Base in a J-2 environment, and they still have a few HoneyMacs in there for multilevel security with nothing running on them because they're doing what you said. They're going system high, because that's easier. I made the same decision on the SIPRNet and the NIPRNet. I said, "I don't have time to be bothered with this CONFIDENTIAL security or

TOP SECRET, et cetera. I'm going to go system high and put all this stuff right here and all unclassified stuff over there."

Student: Even there, you've lost the whole intelligence community, which is on Intelink.

Edmonds: That's what I was going to tell you. I didn't lose them because of Intelink. I lost them because of culture. The intel guys did the same thing I did, but they took all that intelligence stuff and classified it SECRET. They've got all this funny stuff, so they can let everybody have it on a Web kind of basis called Intelink. I could have taken all of the Intelink and put it right on the SIPRNet so that the operators could have both, but the intel world wanted to have its own thing. They built Intelink just at the same time we put all the classified material on the SIPRNet. So that's a cultural thing, rather than a technology thing.

When I was the J-6, I went to CINCCENT down at MacDill. I walked into the intelligence room, and there was the SIGINT stuff, the COMINT stuff, and the other stuff—about three or four different INTs. Three of them came from NSA, and they were on different terminals, different networks, because the community said they had to be separated. So you won't get rid of those things until a J-2 or a JCS chairman or a CINCCINC says, "I will not have that anymore."

Oettinger: The intelligence argument, of course, is that the reason is that if I have delicate sources, I want to be able to control who sees the information, and you're not going to blow my X years of investment by changing it. So, again, these are not good and evil or white and black, et cetera. They are nasty little tradeoffs where people see different ways, and they're hard problems.

Edmonds: Yes, by definition, they're compartmented. As a matter of fact, down at CENTCOM, our CINC was so desperate about this that he had individuals who worked each of those compartments, and nobody knew what the other compartments did.

Student: That's just it. I don't want to talk about these expensive boxes, but each of those boxes has a person attached to it because the CIA will only let a CIA guy have access to it.

Oettinger: Don't just flog the government. I'll give you another instance, because this is a universal problem. You know my crazy thing about balances. If you try to look at this in an all-or-nothing kind of way, you won't get anywhere. If you're running a bank or an insurance company, or some kind of financial institution, one of the reasons you may have to have umpteen terminals is that you cannot have the same clerk selling insurance who is doing banking transactions because the Glass–Steagall Act prevents that. Last year there was a big lobbying push, and for the first time since the Depression, Congress passed revisions to the Glass–Steagall Act that regulated financial services.[1] It's still under litigation. This affects the whole question of how many terminals you need to handle financial transactions in a manner that to a customer would look like, "What the hell, I don't care about those banking rules. I want to deal with one person." The answer used to be: "Sorry, but if you deal with only one person, you're breaking the law."

Edmonds: Let me tell you, we do it in industry also. I won't take a long time on this point. In EDS, we have four lines of business. One is high-level consulting, A. T. Kearney. These guys are

[1] President Clinton signed the Gramm–Leach–Bliley Act, or Banking Modernization Bill, on November 12, 1999.

thought leaders. They cost big bucks. We have what we call Information Solutions: they provide solutions that integrate the garden-variety information technology, communications, and automated data processing. It's a big group. We have a group called Business Process Management. They're the ones who do claims processing on Medicaid or Medicare. Then we have a group called E-Solutions that does all electronic stuff.

These are four lines of business, all King and Queen Kongs, and they're big masters. Now, any given customer might have all four of those folks providing services to him. The biggest issue we wrestle with every day is: "Whose customer is this? Is it E's, B's, I's, or A's? Let us look at this thing." Some days it's: "Who's the toughest person on the block?"

I went to the U.K., and we were bidding on their Social Security system. The issue was that the Social Security thing was an I-Solutions effort, but the E-guys said, "I'm going to be doing all this on-line stuff. This should be mine." Then the U.K. was doing an electronic commerce deal, and we were bidding on it to get some French company. Again, E said, "It's mine," and the other guy said, "But this is all mine because this is the business process here," and so on.

In industry, unlike the military, woe be unto the person who walks into his boss's office and says, "We have a problem here, Tony. Will you referee between the two of us on what we're going to do?" We'd both get shot. So we end up having to go back and say, "Okay, somehow we've got to solve this problem." Then we talk about it in a way that kind of resolves it from an issue point of view. Sometimes I say, "You had the last one, so I get this one." In industry no CEOs will sit down and referee between two people who report directly to them and let them keep their jobs. They just won't do it. If you have a problem, just suck it up and go solve it. The CEOs don't want your problems. They want you to make some more money, sell some more business, or do something, but not to give them your problems.

Let me hit this and then I'll let you guys ask some questions for the last few minutes here. These are key questions to consider in connection with building a trusted business environment. If you're running a business, military or otherwise, do you know how many times your system has been compromised or someone has attempted to compromise it today? You ought to know if somebody is trying to get into your system. You ought to have something in your system that will give you an indicator immediately if somebody tries to get in there. We used to do it for security purposes. We would leave our calling card. It would say, "We've been trying to get into your system. We were unsuccessful." We'd leave that right in your system.

Who is responsible, and what is the impact on your business? What happens if they do get in there? I got into an unclassified military system and nosed around with the chief of staff sitting right next to me. We had already called the commander down there and told him, "This is what we're going to do. You're not in trouble if we break in there, but we're going to show the chief of staff what we can do." This was an unclassified system, because it didn't have any protection on it. We found some things on the system that were not classified but kind of embarrassing, like the promotion list for the two-star generals, which was going to be released the next day. We found people who were getting passports processed, and we could figure out that there was something going on in a particular place because a lot of guys were going there. But you have to make a conscious decision whether to protect that or not. Maybe it's cost prohibitive, maybe you don't care; but at least you make a conscious decision.

Do you regularly assess your systems to identify potential threats and vulnerabilities? The national labs have always been vulnerable. Everybody keeps going to the labs to try to get stuff out of them. Hackers like to get into the Pentagon simply to say they got into a Pentagon system. They like that because it's good press. They broke into the Pentagon health and welfare system and found that somebody announced he had a ticket to sell to the basketball game, but they got in there and they're happy.

What systems are most critical to your operation, and what kind of strategy do you have to protect them? That's what you need to ask yourself if you're in charge of something anywhere.

There are several kinds of things that I look at when I'm evaluating a system. Do you have information security items on your agenda? Does management participate in information security services and enforce the rules? If you look at the agenda for most meetings on any subject that you go to for the next six or nine months, unless the subject is information assurance, they won't even talk about trusted systems. Somebody may come to me and say, "I'm worried someone could break into this," but they don't have this on the agenda. If they do, the boss won't talk about it. I can't get the insurance company down in Hartford, Connecticut, to talk about it. I can't get the financial guys down in New York City to talk about it, until one day somebody will say, "We just had $40 million transferred out of our account." Then they will say, "Ssh, don't tell anybody! Come over here! What happened?" Then you start working the problem. You solve the problem, but you still don't talk about it, and you don't share it with other financiers or the banks, either. You just clean it up and go.

I recall we got a phone call once from the White House to help a bank. That was when I was on active duty. I said, "We can't help you because we're government, but I can tell you the name of a company that can." So I called that company and told them, "This guy's going to call," and the company did help them, but in part of the company's report they said, "We helped the bank and the bank cut us off. They went solo and did the job themselves."

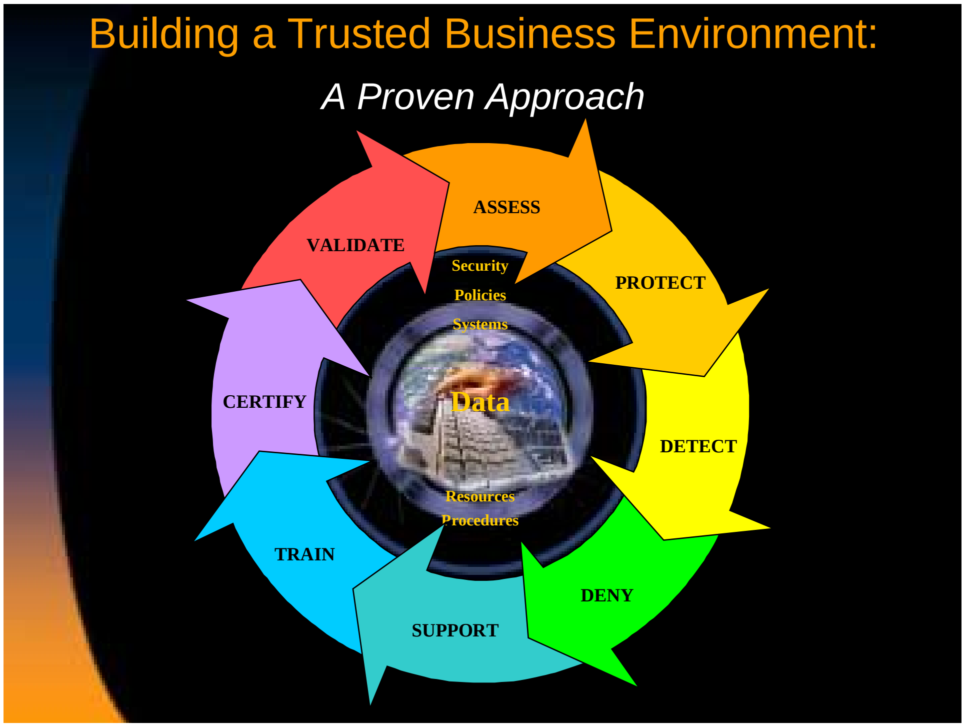
Oettinger: Let me just interject. When you read the assignment on the President's Commission on Critical Infrastructure Protection and listen to John Tritak and the stuff seems Byzantine to you, figure out why they seem to be scratching their left ear with their right hand. It's because they're walking on these eggshells. On the one hand, folks want protection; but on the other hand, they don't want to admit that they need it. In a situation like that, it gets very hard to help out.

Edmonds: That's right. It's very hard to help anybody.

Here are some more issues to consider. Are the information assets regularly classified as to who owns them, and are there identified business-line information owners? Who owns this machine? Who owns this room here? Who is the responsible person for this organization? Who is responsible for training? Who is the system administrator for this stuff? How long has that person been there? Have the staff been changed out? Did they go PCS (permanent change of station)? Did they bring somebody else in? Have they been trained? Usually they take an administrator, probably the least computer literate person, and they put that person in charge of this stuff. Is information security really integrated into your business units, and is there a response team in case you get into trouble? Who is accountable? When something happens, what do you do, and who cares? Who wants to know? Where do you turn? Does somebody know how to fix it? Do you keep them on-line to try to tell where they're coming from?

This I'm a little bit proud of. This is my food chain (**Figure 10**). I created this about ten years ago, and I call this the life cycle of a trusted business environment. I now have taken this and put it into EDS, and we sell it as a product. We can sell any part of this. The reason I call it the food chain is because it never stops. You can assess your problem. If you call up and say, "Come in and tell me how bad I am," I will come and assess you. I say: "I will tell you privately how bad you are. Do you want me to protect you or not? I can protect your system. I can get the products and do things for you. I can sit here in the future, and I can detect if anybody tries to get into your system. If you want me to, I can deny them access, or I can let them in and then watch them so I can find out who they are and report them to the FBI. I will provide support to you by coming here and maintaining your systems to make sure they're good. I'll continue assessing them. I'll train your people on good security, and I'll train your system administrators so they can detect the problem themselves if you don't want me to do this for you. I'll come back to you every six months or twelve months, however often you want, and certify that your system is still good, or I can do it on-line. I can do it routinely: monthly, weekly, however you want me to do it. I'll validate it and give you a certificate every time I do it as of the date you chose."

We did this for the Air Force one Friday, and a contractor came in on Saturday and loaded some new stuff, and on Sunday they got hacked. Their whole Web page got a lot of pornography put on it. They said, "You guys just validated this and certified that it was good!" We went


Building a Trusted Business Environment:

A Proven Approach

Figure 10

back and assessed the thing again, and we found they loaded some new software and opened up the doors we closed. There's no endgame. It is a continuous cycle, and it continues to go.

We do this on-line, full time, routinely, in Reston, Virginia. One is for a distance learning network. We do this on-line, because one person can watch multiple networks. When I was at DISA, I did it for the DII. I had a contractor sitting there, who just watched these bits and bytes all day long. He'd say, "Oh, there's a problem," and it would start flashing. We'd call the team and start working on it. We would find out what it was, isolate it, and let the right people know, and sometimes we would pass it to the appropriate government agency, sometimes to the local police, sometimes overseas. That life cycle of information assurance is very important.

We're coming down the stretch here. Information assurance reduces vulnerability. You can make sure that you prevent unauthorized use of information, unauthorized access to information on a company or its customers, and fraud. The biggest problem for companies is fraud—not external, but inside a company. People who have access to all the systems can do things to you. In fact, there are some people who give themselves pay raises or bonuses fraudulently. This is really important, and will always be big in this country.

Privacy and confidentiality are very important. People can steal your identity. They can tamper with data, they can repudiate transactions, and they can also disrupt business.

Student: Can you go over the difference between information assurance and trusted systems? I think you mentioned something else. Are those all the same things?

Edmonds: Let me just differentiate between them. Information assurance is basically a general term that means I am going to assure that the information that you're going to get is what it is supposed to be. I will certify that information.

Student: Like information integrity?

Edmonds: Yes, like information integrity. I use the term "trusted business environment" in kind of an inclusive way: it doesn't have to be just a network, or just a computer system, but whatever environment I'm working in. The term means that because that environment has so many different parts, when you put it together as a whole, it will stand the test of scrutiny.

For instance, when I put this package I just bought from you out on the flight line to get shipped someplace, it has a barcode on it. That barcode gives you the information that this is in fact the thing you ordered and that I put it on the airplane. This could be tracked back from the original order, or it could go to the destination. This is a trusted business environment, so everybody in this environment here has trust in it because we looked at the components of it and we know that each piece does meet the test we want it to meet. So, we conclude that this is trusted for us. We'll keep doing business in this environment until that trust is broken.

I use that terminology because I don't like to differentiate between government and business. We have the same concerns that you have in government. I want to make sure that I can trust this is what it is. This is not a fake. So I use that to differentiate between information assurance and security. I’m talking about information integrity, meaning that it is good quality data.

Student: And you want to protect against unauthorized use.

Edmonds: Yes. Use, or interception, or masquerading.

Student: So “information assurance” is more against unauthorized use, but trusted environment is more for...

Edmonds: ...the environment itself, which might be very large.

Student: But it’s basically the same thing.

Edmonds: They’re closely related.

The other things here are the starting points for information assurance. These are foot stompers. This is not an information technology problem; it’s a business problem. The biggest problem we have in business is getting the boss to say, “Yes, this is my bottom line. If I can’t deal with Citibank in New York for a day I’m out of business, or if I can’t deal with the Metropolitan Life Insurance Company for whatever reason—because the data are corrupted or the system is down—I’m out of business.” You actually have to demonstrate that to people. The way I got money for this problem is that I brought the secretary of defense and the chairman of the Joint Chiefs of Staff and two service chiefs to my building and I showed them how I could interrupt the business of the Defense Department. They said, “Here’s some money. Go fix the problem.”

Security is a business enabler, not a stand-alone objective. You should not do it as a separate activity. It should be built in as a part of your everyday business. E-business efforts will fail unless we engineer security concurrently with applications and infrastructure. If we don’t do this, e-business won’t make it, because once I get your credit card number I can go out and buy stuff as though I were you. So you’ve got to have some assurance that the data you’re using are correct.

In summary, e-business is the new generation of business. Computer crime and losses are widespread and growing. E-business and extended environments extend the vulnerabilities to computer crime and multiply the vulnerabilities. Information assurance regarding the data you send or receive is an effective enabler, and maintaining a trusted business environment is an integral part of any business. If I’m at EDS, I want my 144,000 people in EDS to work inside EDS in a trusted environment. We have firewalls. We have products. We have things to make that happen. We do business inside EDS among ourselves in a trusted environment, and I can’t violate that environment. A comprehensive approach that has a good architecture and good policies is critical, and this all should be based on good practices.

That’s my bottom line to you: that this information technology environment we’re in today must be trusted to be effective. The people who use it, especially when there are big bucks and lives involved (and that’s kind of the military and the civilian perspective: lives and bucks) have got to believe that they can operate in this environment in a trusted way or they won’t use it.

That's why today the military and some of these businesses are still using old processes and still doing things in an old-fashioned way, because they don't trust the environment. That's because we, the technologists, haven't given them a good enough foundation and driven them to understand this business.

I could talk about this for a long time. Let me stop here, because I told you I would stop for you to ask questions about this or anything else.

Student: With your J-6 hat on, what are those trust issues? If we're looking through the battlespace at the operational and tactical levels, one of our big trust problems is power generation. We can make command and control as electronic as we want, but we still have the same number of personnel over there doing this in analog format because we can't trust power generation. The same 1960-vintage generators are powering all of our tactical operations centers. What did you see, from up at J-6, that we are doing about fixing that problem? Just the battery weight problem unhinges the whole system.

Edmonds: I look at that as a major failure. I hate to push it off on the civil engineers, because that's one of the biggest mistakes we made with power. We give it to the civil engineers to do, and it should be more aligned with operations than civil engineering. Then you'd find that we would do the R&D to get light weight (the new chief of staff of the Army[2] is always talking about light weight) and long-lived, replenishable power generation, and we just haven't done a good job on that. We have not put our best minds on it. This is a major fault, not just of the military, but in general.

Student: We're doing that, but if the generator turns off, you're done.

Edmonds: You're in trouble. You're absolutely right. That's an area that I think needs some good, hard-core R&D. It's a big problem.

If you don't want to talk about this stuff, you can ask me a question about anything else. Any questions about command and control?

Student: In e-technology environments and trusted environments, maybe the behavior of people, or of companies, or of countries will change. I just want to know your views on the country-to-country issues, and also the effects on the security or authority of foreign countries.

Edmonds: I think that's an excellent question. I think a trusted business environment, which is a trusted national environment, will improve the relationships among countries. I have to tell you that I felt that way when we put the hotlines in between Moscow and Washington, D.C., so we wouldn't have any mistakes on nuclear weapons. Although we were still in the Cold War, I think that we had created somewhat of a trusted environment in that we were going to call each other before we did something. History has proved that it was right, because, whether it was by accident or not, we didn't do it. I think the more we can provide a trusted environment to exchange information between nations, the more we're going to operate and deal in different and better ways that will allow us to do things better on this earth.

[2] Gen. Erik K. Shinseki became Chief of Staff of the U.S. Army on June 22, 1999.

I believe that, I really do, because the biggest problem, the biggest threat to safety and security and peace, is misinformation and misunderstanding. A lot of those misunderstandings are not because you say yes and I say no; some of them are cultural. What is it that you want out of this deal, and what do I want out of this deal? They may not be too far apart. It may be that all you want to do is make a public announcement. I might want a piece of land, or I might want the water rights, but we both can get what we want if we can operate and negotiate in a trusted environment.

When we used to have those diplomatic negotiations, you might have seen on television that the government people had to walk out in the woods or someplace to have a trusted conversation. Those weren't trusted environments, so they were all trying to do one-ups on each other and kind of outdo each other. If they had a trusted environment, they could negotiate in a way that all of them could get what they want. I think it's better. That technology has a lot of good implications for the future because information is power. I'll tell you, it is power.

I recall the days when we had those pouches with locks on them. The guy with the pouch with the lock on it with the real hot information was a powerful guy, and that was the general's favorite person. When he walked in at seven o'clock every morning and unlocked that pouch and noted two or three things and then locked that thing back up, that was power. It's no different. This power has been unleashed now in so many different ways.

Student: Yes, but even when you have twelve different boxes, you still have the guy with the pouch. The CIA guy will only talk to the Pope. He won't talk to any of the lesser beings.

Edmonds: Sure, but that's the culture thing. Let's kill that.

Student: In the present world, the United States has more power versus other nations, so it is rather asymmetrical.

Edmonds: Let me tell you something about that. A warrior never unsheathes his sword until he gets ready to use it. The power aspect of it is the certainty of having power. Often times, it leads you to a point where you don't have to use it. There are different forms of power. For instance, I think that information is power. When the people of the world become informed on things, they will become more powerful.

Let me give you another view, a sociological view. A nation of 500 million people who are all healthy, have good jobs, are happy, and play golf in the afternoon every Wednesday with a lot of money in their pockets is pretty powerful. I recall that in the 1980s or whenever there was a tremendous economic boom in Japan. Everybody was buying cars and all that stuff from Japan. Japan was probably one of the most powerful nations on earth at that time, and they had a very small military. So, there are different forms of power. This power had been unleashed through the Japanese people, who were working in harmony in those plants and producing products that the world wanted, and their economy was booming. There are so many ways to transform power, and so many different definitions. A country like Switzerland or Sweden, with a good economy, where people are healthy and vibrant, I call a sleeping giant.

But, in this case, the information technology I'm focusing on is a way to share this power with the whole human race. Knowledge is power. If you have a family member with cancer, you can go on the Web and find out things about it. I mean if you are in Beijing, Bangkok, Saigon, or Paris, there is no way anybody can keep the power of the knowledge on the Web from you. That's the human power that you don't ever want to forget about.

Student: I see a huge problem coming out from a lot of this. If I can draw an analogy, the Law of the Sea was basically established by Britain when Britain was in a position to establish such things. Britain ruled the seas at that time, and, basically, the Law of the Sea that we have today is kind of inherited and derived from that. Countries that have only recently come to the table, China for instance, have accepted the Law of the Sea as it stands, but they say, "That law was developed when we weren't at the table. We're not 100 percent comfortable with it." Now this UCC, which I think will become extraordinarily powerful, is being developed right in front of the eyes of countries like China, India, and a good part of East Asia, and if they don't feel like they have a piece of how this thing is put together, they're going to be terribly resentful of it.

Edmonds: That's one of the reasons why the administration is trying to get China in the WTO right now, because China is a very large country, with a large part of the human race, and China needs to be at the table. China needs to be involved. As a matter of fact, although I don't think he's doing it for the same reason, the President is trying to get Africa and Latin America involved in the same way. We have a large place on the globe, but it's kind of like I tell folks, "You can eat an elephant a bite at a time, but you can't wait until everybody gets ready to eat at the same time." So, you keep pressing on, but you're going to try to bring the other folks along with you. I think that's one reason why the President is really adamant about trying to get China in the WTO and those other kinds of organizations, so that you don't leave them behind. I think it's the right thing to do. You have to start someplace.

The other thing is that you aren't going to stop the revolution. This is the revolution of this century, and you want to bring everybody in it and let them flail away a little bit.

Student: My father does a lot of e-business, as you showed on the slides, and he does get his clients through e-mail, or they visit his Web site or things like that. But he never closes a deal without actually meeting them in person. Do you find that a lot even with all this technology?

Edmonds: Oh, yes.

Student: It comes down to that human connection.

Edmonds: I have that bias. It took me a long time to do e-mail. I refused to do it for a long time because I was a commander and my command instincts told me I commanded by walking around and eyeballing people. I would take your handshake, look you in the eye, and I could tell whether I liked you or not, and those kinds of things. So, even today with all that stuff—and I'm a part of this—I want to see the person. I want to know that when you gave me your word, that's your word, and I will hold you to it. All this other stuff is good, but there is nothing that will ever replace that personal element for me because that's just golden.

Thank you for your time, and I hope some of this has been worthwhile for you. I tried to pick kind of a different subject for you, a little provocative. I could have talked about anything else you wanted to, but this is what I wanted to share with you. I'm going to talk to a bunch of folks down in Washington about the same thing next Wednesday night at the Software Symposium, with Dr. Hamre,[3] as a matter of fact, because nobody wants to talk about the uglies. They want to talk about, "Oh, it's coming, and we're going to make big money!" This is the uglies. Thank you very much.

Oettinger: We do have something for you to remember us by. Thank you so much for a wonderful presentation.

[3] Dr. John J. Hamre was deputy secretary of defense from 1997 until March 2000.

Acronyms

B2B	business-to-business
CEO	chief executive officer
CIA	Central Intelligence Agency
CINC	commander in chief
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DLA	Defense Logistics Agency
DOD	Department of Defense
EDS	official name of company; formerly Electronic Data Systems
NIPRNet	Nonsecure Information Protocol Router Network
NSA	National Security Agency
PC	personal computer
R&D	research and development
SIPRNet	Secure Information Protocol Router Network
UCC	uniform commercial code
U.K.	United Kingdom
USAF	United States Air Force
WTO	World Trade Organization

INCSEMINAR2000

ISBN-1-879716-74-7