

TESTIMONY BY AL EDMONDS, PRESIDENT, EDS  
FEDERAL, TO THE CONGRESSIONAL JOINT  
ECONOMIC COMMITTEE ON CYBER SECURITY  
AND THE US ECONOMY  
JUNE 21, 2001

Thank you Mr. Chairman,

It is a pleasure to be with you this morning to discuss this important topic.

I am Al Edmonds, President of EDS' Federal Government-Information Solutions organization. In that position I am responsible for all of EDS' relationships with US federal, civilian and military clients.

EDS is a global services company that provides strategy, implementation and hosting for clients managing the business and technology complexities of the digital economy.

We bring together the world's best technologies to address critical client business imperatives. With over 120,000 employees in 55 countries, EDS serves the world's leading companies and governments.

The subject of this hearing is especially timely.

Monday's USA Today reports that cyberspace is the next "battlefield" and that the U.S. and other countries are hurriedly making preparations for information warfare.

While the article discusses the challenges facing our military, the prospects of global cyber security have to be of concern for all of us.

The USA Today article reminded me that I want to make a very specific point in today's hearing...*that cyber security is a global issue.* The Internet is global.

The threats to our national and economic security may come from any place in the world. Our economy and national security establishments are global, linked by business trading partners and formal governmental alliances, such as NATO.

We must be cautious not to think about these issues in only a domestic context. The future of the digital economy hinges on a secure Internet. *It is that simple.*

Our nation's national security is faced with new risks, as are public safety, law enforcement and economic security.

When I say economic security, I am referring to the security needed to protect the commercial businesses and industries that make up the U.S. economy. National security and economic security are closely related.

So, while the benefits of the Internet continue to accrue enormous benefit to U.S. citizens and businesses, we as a nation continue to face the reality that the Internet is vulnerable to attack. We saw just last year the huge costs related to a denial of service attack.

The “I Love You” virus, estimated to cost approximately \$8 billion, was just a forerunner of what we can expect as our economy and those of other countries become increasingly interconnected.

The FBI reports that 90% of 273 U.S. corporations surveyed reported security breaches in 2000, with an estimated loss of nearly \$300 million.

Although the economic cost of last year’s denial of service attack and the “I Love You” virus was considerable, I think the bigger loss was of the *trust* that individuals, businesses and governments have the reliability and safety of the Internet.

Add the threat of cyber terrorism to a daily dose of viruses, fraud, and money laundering, and it’s not hard to see that we have major issues that demand the close attention of Congress, the Administration and industry leaders. It’s clear that the Internet is a host for the “crime backbone” of the new economy.

The cost of protection is going to be high. The market analyst firm IDC predicts that spending on cyber security will increase 21% annually to \$17 billion in 2004.

I would also suggest that you don't be misled by the recent failure of dot.coms. Governments and businesses are continuing to invest in infrastructure, applications and transition to the Internet because the benefits are potentially huge.

Companies are using the Internet to develop new business models that provide lower cost and lower prices. That's good for US businesses who must find new ways to maintain their competitive edge in the global economy.

The Internet continues to be a way for businesses and government to lower costs and to reach their customers trading partners and for government, their constituents.

So, it's pretty clear to all of us that no nation can afford to have its telecommunications systems at risk.

No nation can afford to have its financial system attacked by criminals.

And none of us can afford to have our energy distribution disrupted by hackers.

This wonderful medium that will transform how we will live, work and govern will become much more valuable if it is secure, reliable and always available.

So how do we solve these cyber security issues? What role should the federal government play? What action should Congress take? What should industry do?

I have a short list of ten recommendations that I would like to run through quickly. Most of these recommendations have been well thought out and adopted by CEOs all over the world.

My Chairman and CEO, Dick Brown, has been a leader in numerous CEO groups that developed many of these recommendations.

First, Make greater investments in information assurance technology and services. There's clearly an increased need for more investment by businesses and governments in information assurance technology and services to improve cyber security and fight cyber crime.

Second: Partnership and cooperation. US industry and the federal government with law enforcement and national security must continue on the current path, to work together in close partnership. *Cooperation* and *partnership* are the keys to success, because the government cannot solve these issues alone. Nor can businesses.

Third: Industry leadership. Because the Internet is mostly owned and operated by businesses, industry leaders must take the lead in cyber security.

Industry leadership means more attention to sharing information about risks and vulnerabilities, greater investment in information assurance services and driving business-to-business security standards.

Fourth: Information sharing and analysis. This is a vital role for industry, to create industry information sharing and analysis centers (ISACs) to share information about cyber attacks, vulnerabilities, countermeasures and best practices. Several ISACs have been created. We need more.

If the federal government removes certain barriers, businesses will be more inclined to share information with government agencies.

If businesses share this kind of information with each other, and with the government, the entire community of users will be stronger and better able to fend off attacks or lower the risks of operating on the Internet.

I believe that information sharing is critical to addressing the cyber security issues.

Fifth: Lead by example. The federal government should be a model in cyber security practices and technology.

Number six: Develop federal policy in close coordination with U.S. state governments and other nations. Federal preemption will prevent a patchwork of policies that will only create barriers to success.

Seven: Shortage of skilled workers. All governments and U.S. companies need more highly trained skilled workers in security technologies and methodologies.

Eight: Avoid cost shifting. As the federal government develops policy for cyber security, avoid shifting the cost of those policies directly to the builders and users of the Internet. The cost should be shared broadly.

Nine: Privacy. Recognize that the consumer sees privacy and security as one and the same. We know that they are different in legal requirements and other areas.

And finally, regulatory oversight must be part of the equation. Regulatory bodies should refine their oversight to address cyber security issues with regulated industries. I am not suggesting *more* regulation, just greater attention to minimum actions that regulated industries should be incorporating into their businesses.

The Digital Economy has erased national borders, removed economic barriers and allowed enterprises to become truly global.

The Digital Economy has linked businesses with their customers and suppliers in ways never before imagined. It also promises great prosperity.

But we must be vigilant. The Digital Economy depends on security and trust.

Together we can provide both through a close collaboration of government and industry. Let's all make cyber space safe for all of our constituents.