

# Putting Military Security Techniques to Work in the Commercial Market



*John Droge*  
*Vice President*  
*Business Development*  
*jdroge@mykotronx.com*

**May 13, 2004**



## Abstract

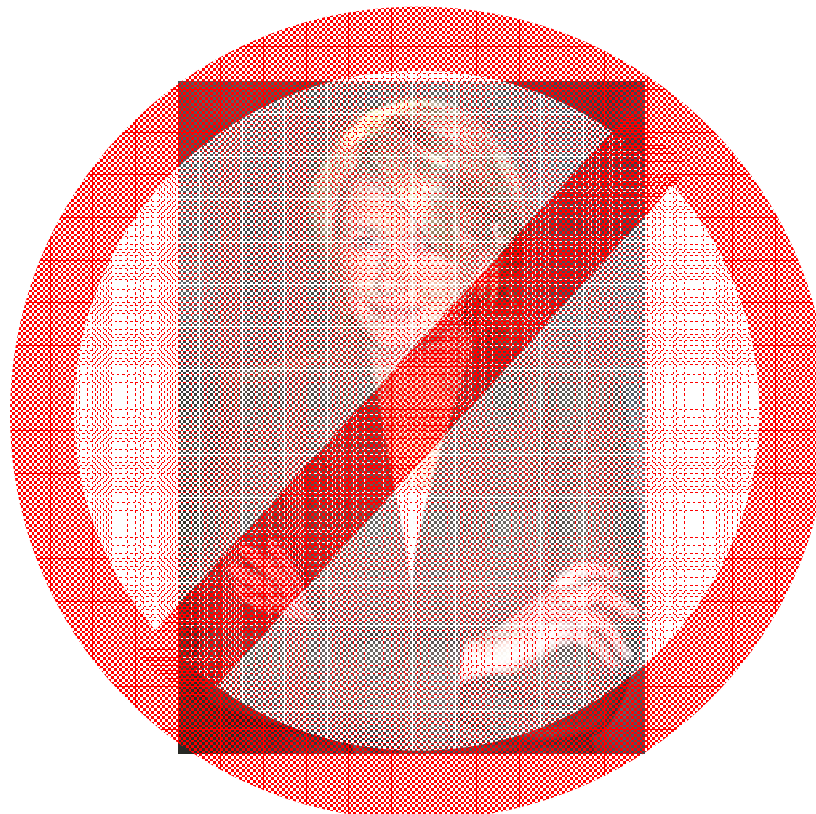
- Everyone has their ideas about what kind of cryptographic technology protects the President's "red phone" and how America guards its military satellites from attack.
- But few people know the real truth to those questions like the experts at the Mykotronx division of SafeNet Mykotronx, the company responsible for more NSA-endorsed products than any other company in the field.
- While John Droge, VP of business development, SafeNet Mykotronx, will not be revealing any state secrets in this presentation, he will discuss how the needs of high-assurance industries such as financial and healthcare and applications like wireless are driving the transfer of military cryptographic technologies to the private sector.
- His discussion will cover such topics as the increasing demand for higher levels of encryption and FIPS level security in commercial fields; the availability of tamper-resistant and tamper-detection packaging and enclosures that were once associated only with government products; and the transfer of satellite uplink encryption techniques to commercial communications.
- He will address how companies can make a decision to employ custom cryptographic solutions versus off-the-shelf products for various applications and consider the tradeoffs.
- It will be an insider's look at high-level security.

# Agenda

- **Introduction**
- **US Government information security technology**
  - The cryptographic technology that protects the President's “red phone”
  - How America guards its military satellites from attack
  - US Government cryptographic requirements
  - US Government cryptographic trends
- **Commercial information security technology**
  - The transfer of satellite uplink-encryption techniques to commercial
  - The increasing demand for higher levels of encryption and FIPS-level security
    - When is it needed
    - How to be successful
- **USG and commercial comparisons**
- **Practical advice**

## Now, for Anyone Expecting to Hear About Government “SECRET Stuff” ...

- **Sorry .. I will not be sharing any classified secrets**



# Information Security Techniques

---

- What are the techniques?
- What makes sense and what doesn't?
- Why?
  
- What are the needs of the US Government?
- What are the security needs in the commercial marketplace?
  
- Unique (never before released) industry survey results
- Quiz or two ...

My presentation is only 25 minutes, so hopefully ...



Courtesy of [www.fm99.com](http://www.fm99.com)

# Secure Phone

- Digital and analog
- Programmable Crypto Module (PC Card)



# FORTEZZA Plus

- This is the cryptographic “engine” for the President’s secure phone
- To date, we have produced approximately 150,000 FORTEZZA Plus PC cards
- Programmability features of the FORTEZZA Plus card have enabled five (5) new models to choose from



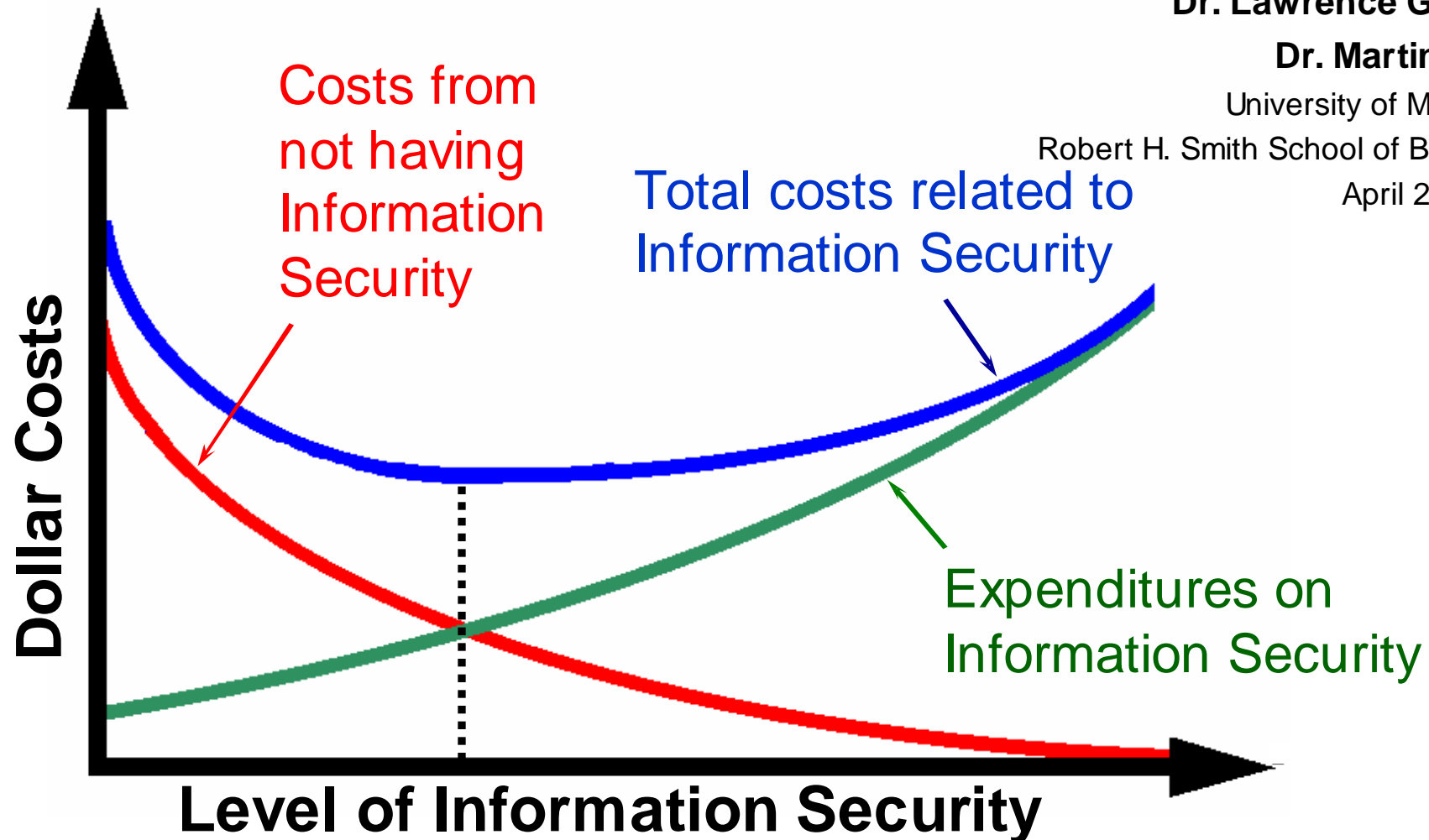
## The Truth Behind the President's Phone

- Developed and produced in secure facilities
- Hardware-based cryptography
- Classified algorithms
  - Key exchange, confidentiality, digital signatures, randomizer
- Programmable
- Special anti-tamper features
- High-assurance, trusted platform (phone) called the Secure Terminal Equipment (STE)
- The card is programmed (initialized) by a Government controlled trusted key management center
- Two-factor authentication – the card and a PIN
- It is a COMSEC Controlled Item (CCI)
- But would you pay \$3,500 for a secure phone?

# CENTCOM Headquarters – Quiz #1



# Economic Aspects of Information Security



Dr. Lawrence Gordon

Dr. Martin Loeb

University of Maryland

Robert H. Smith School of Business

April 26, 2001

# Satellite Command Links are Protected

*National Information Assurance Policy for U.S. Space Systems*

- NSTISSP No. 1 (17 June 85)
  - National Policy on Applications of Communications Security to U.S. Civil and Commercial Space Systems
- NSTISSP No. 12 is the follow-on policy to NSTISSP No. 1
  - *Government or Government contractor use of U.S. civil (Government-owned but non-DoD) and commercial satellites launched five years from the date of this policy shall be limited to space systems using accepted techniques necessary to **protect command/control uplink**.*
  - *The Director, NSA, ... shall provide approved protection techniques and guidance.*
  - ***NSA endorsed INFOSEC hardware** ... is available as Contractor Furnished Equipment ...*



# Essential Properties of Good Security

## 1. Ease of:

- Use
- Deployment
- Management
  - Service
  - Support

## 2. Convenience

- Flexibility
- Portability

## 3. Robustness

- Crypto strength
- Independent evaluation

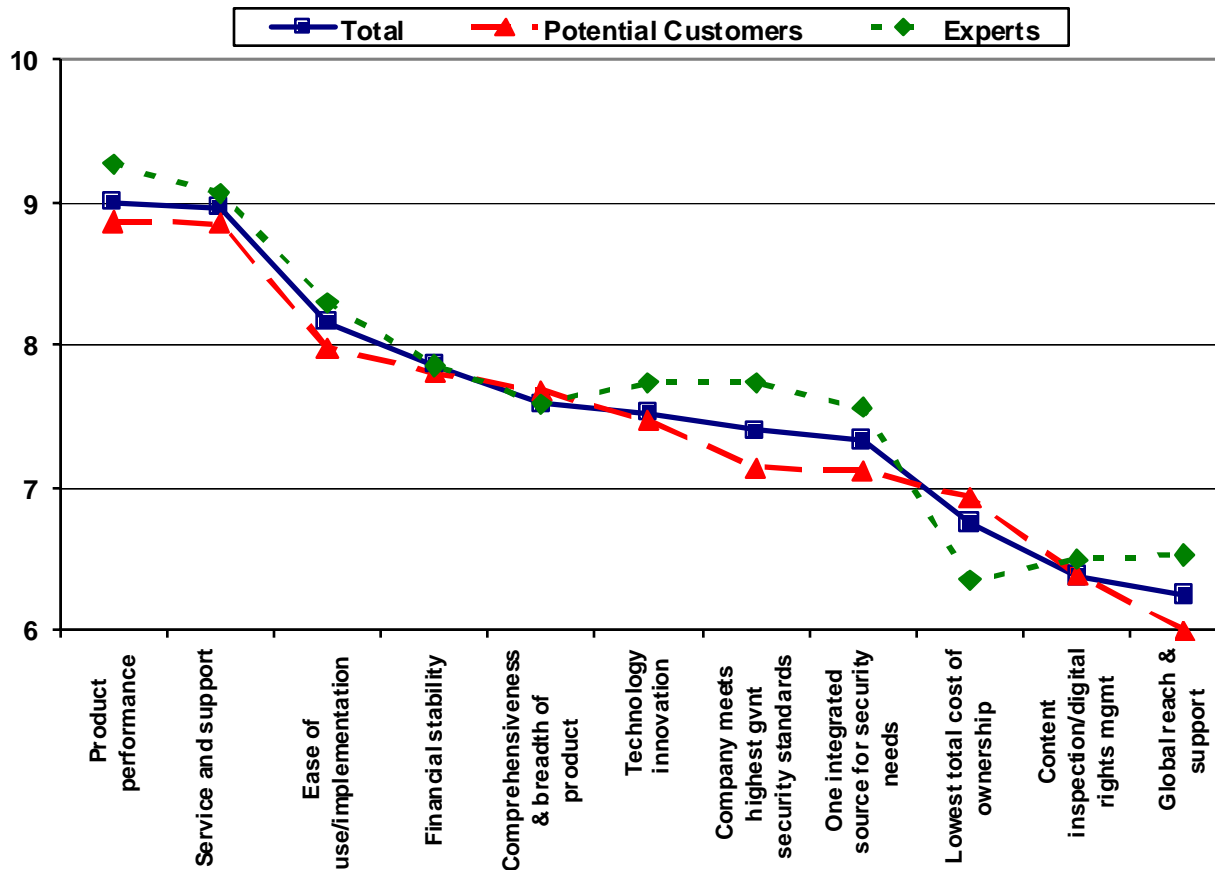
## 4. Scalable

## 5. Compatible

## 6. Performance

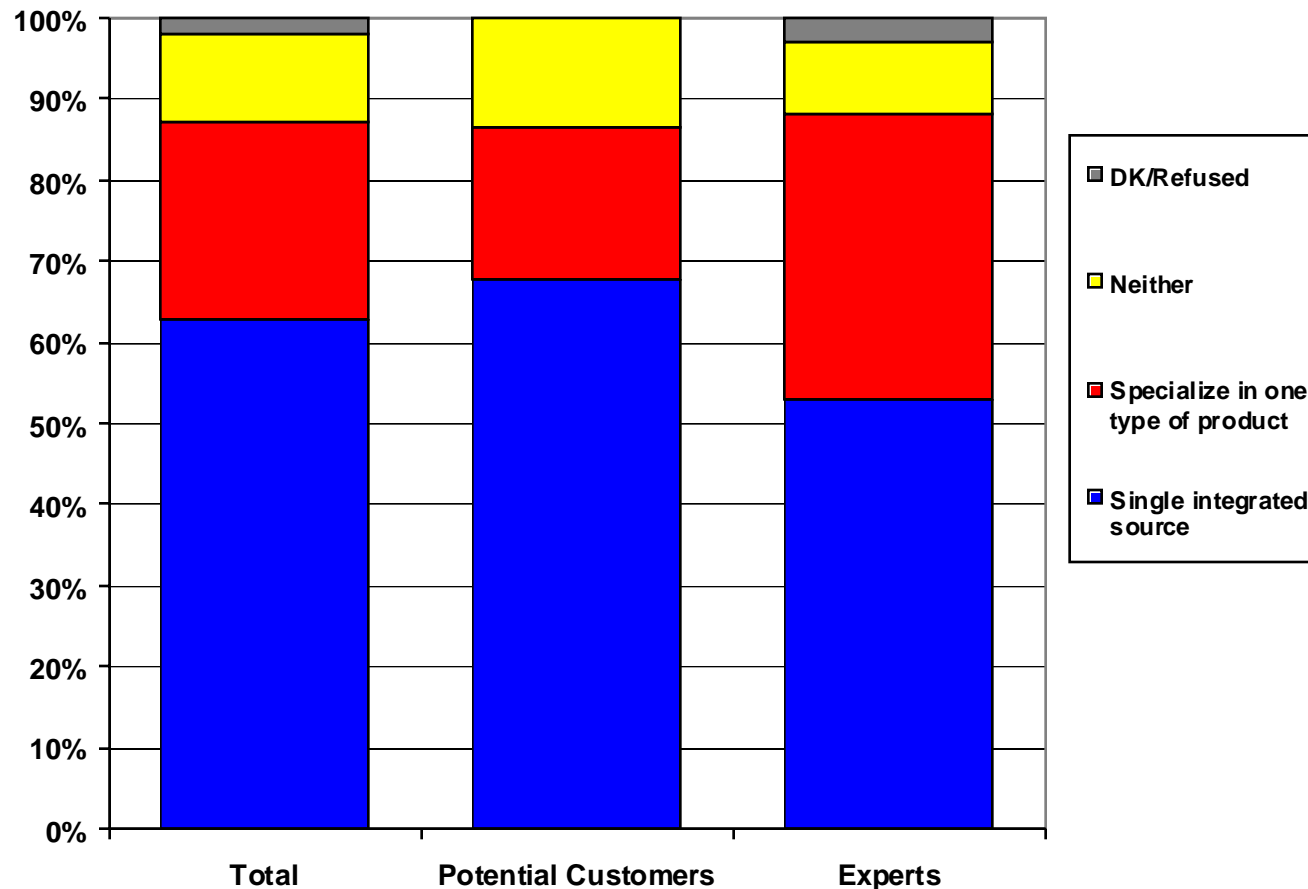
## 7. Cost

When selecting a security partner or provider, please rate the importance of each of the following attributes. Rate your response on a 0-10 scale where 0 equals “not at all important” and 10 equals “extremely important.”



Products' performance, the service and support provided by the security company, and the ease of use and implementation are regarded as the 3 most important attributes.

## Which of the following types of vendors do you prefer more?

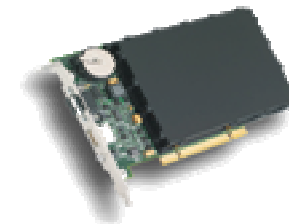


Although most respondents (68%) prefer single integrated source vendors, Experts favor vendors that specialize in one type of product more than customers/potential customers.

# Migration of Security Technologies

- **The following commercial security technologies migrated from Government / military products**

- Hardware-based crypto
- Tamper technologies (hardware security modules)
  - Tamper switches, tamper wraps, labels/decals
- Robust cryptographic algorithms
- Importance of authentication in addition to encryption
- Cryptographic System On a Chip
- Fault (failure) analysis
- Public key acceleration (needed for PKI)
- Assurance – trust in the device



- **The following Government / military security technologies migrated from commercial products**

- High Assurance IP Encryption (HAiPE)
  - Derivative of IPsec

# Information Security Comparisons

	Legend
Very Important	
Somewhat Important	
Usually Not Considered	

## Trends

Increasing = ↑

Decreasing = ↓

**Focus on these**



## Information Security Techniques

	US Government	Commercial
Policy / Regs / Mandates		↑
Confidentiality - Link	Classified	
Confidentiality - Network	Classified	Standards ↑
Confidentiality - Voice	Classified	
Confidentiality - Data at rest	↑	↑
Authentication / Identity	Tokens / biometrics ↑	Tokens (2 factor) ↑
Key Management	Classified	Standards ↑
Assurance / Certifications	NSA / CC / FIPS ↑	FIPS ↑
TEMPEST	OCONUS only	↑
TRANSEC	Military apps	
Physical security of electronics		↑
Algorithm Selection		Standards based
Defense in Depth		↑

# Passwords

## 1. High management cost

- ❖ Resetting forgotten passwords
- ❖ Difficult to extend trust to other domains

## 2. Insecure

- ❖ Easily guessed or obtained

## 3. Inconvenient

- ❖ Frequent change
- ❖ Requirement for uniqueness per service

**This is your enemy!**



## Security Seen as a Nuisance by Many

- The one basic security mechanism we have all used for more than two decades is client logon
  - Userid with a password
- For more than a decade, the major Operating Systems we use offer us a “convenient” way to (using a checkbox) bypass the one basic security mechanism
  - Having to type in that pesky little password is an inconvenience
- Security solutions need to be valued for their convenience and ease of use

# Client Authentication

- **Authentication tokens**

- 2 and 3 factor
  - Shared secrets
  - PKI
  - Rolling codes
  - Biometrics
- Form Factors
  - USB
  - Smart card
  - Fob



- **Used for**

- Network logon
- Virtual Private Networks (VPN)
- Web-based security solution
- Workstation logon

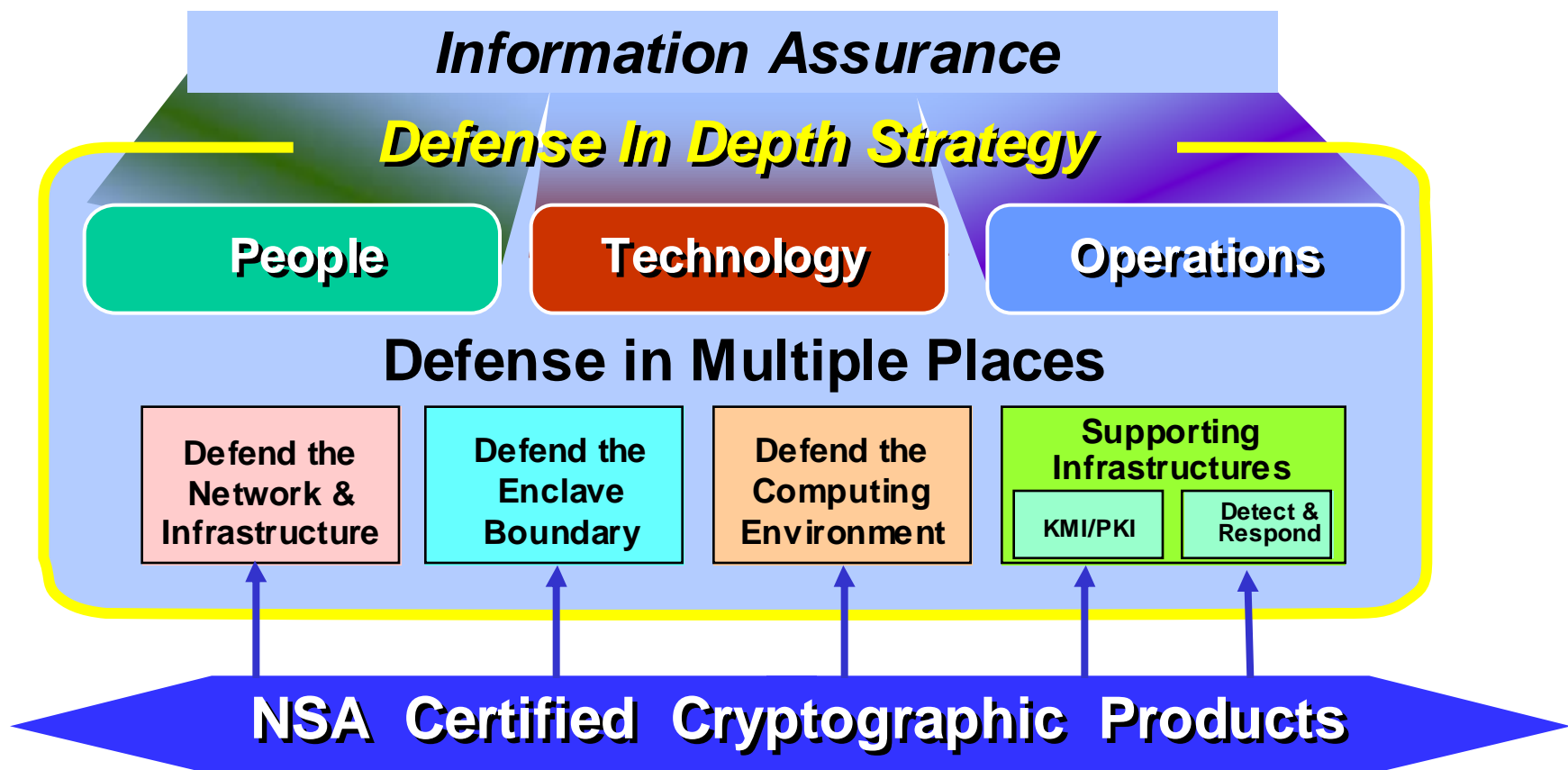


## A New Vulnerability – Data at Rest

- **Airport lost-and-found counters report being flooded with jewelry ... and especially laptops left behind at checkpoints since enhanced screening**
  - Seattle-Tacoma: Screeners turned in 115 laptops left at checkpoints in three months. That compares with three laptops turned in during the same period one year before.
  - Denver. Ninety-six laptops were recovered at security checkpoints over two weeks the previous year.
- **Stricter airport security is producing an unwelcome byproduct: a rash of lost laptop computers**
- **Hard drive mirroring ... an interesting story**

# “Defense in Depth”

*Don't put all your eggs in one basket*



## Information Security Characteristics

	US Government	Commercial
Ease of use / convenience	Green	Red
Transparency	Green	Red
Cost / ROI	Green ↑	Red ↓
Reliability	Red	Red
Upgradeable / future cap	Yellow ↑	Yellow ↑
Maintainable	Red	Red
Non-replicable	Red	Yellow ↑
Manageability	Red	Green ↑
Interoperability	Green ↑	Yellow
Robustness	Red	Yellow ↑
Branding	Green	Yellow
Large deployments / scale	Yellow	Yellow

## Information Security Usage

	US Government	Commercial
Web access	↑	↑
Dial up / remote connectivity / mobility	↑	
IDS	↑	↑
Firewalls		
Network logon	↑	↑
Workstation logon	↑	↑
Wireless		↑
Cell phones		
Cryptographic acceleration		
PDA's	↑	↑
High speed	↑	

# Personal Electronic Devices (PEDs)

- PEDs are problematic
- Over 300,000 PDAs will be lost at airports this year
- Government PDA directions
  - Upgrade COTS
  - Develop Sensitive But Unclassified (SBU) and Type 1 solutions



The screenshot shows a news article from MSNBC's Technology section. The article is titled "PDA's prone to hacker attacks" and is attributed to Reuters. The text of the article reads: "WASHINGTON, Aug 16 — Handheld computers such as those using the industry leading Palm Inc. operating system are increasingly vulnerable to hacker attacks and should not be trusted to store 'any critical or confidential information,'".

## DOD To Issue New Policy On Use Of Handheld Communication Devices Inside The Pentagon

June 27, 2002

DOD To Issue New Policy On Use Of Handheld Communication Devices Security officials are expected to issue next month a new policy that will restrict the use of wireless communications devices at the Pentagon, sources say. The "Pentagon Area Common Information Technology Wireless Security Policy" is in final coordination; John Stenbit, the assistant secretary of defense for command, control, communications and intelligence, is expected to sign the directive.

## Other Information Security Products / Issues

	US Government	Commercial
Insider Threat	↑	↑
Aligning security objectives to business case		↑
Virus / Worms / Spam	↑	↑ ↑ ↑



# Addressing Homeland Security

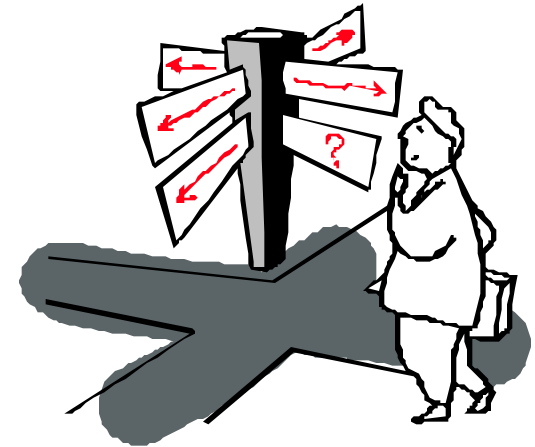
# Homeland Security

**Only 1 in 5  
people take  
Critical  
Infrastructure  
Protection  
seriously ...**

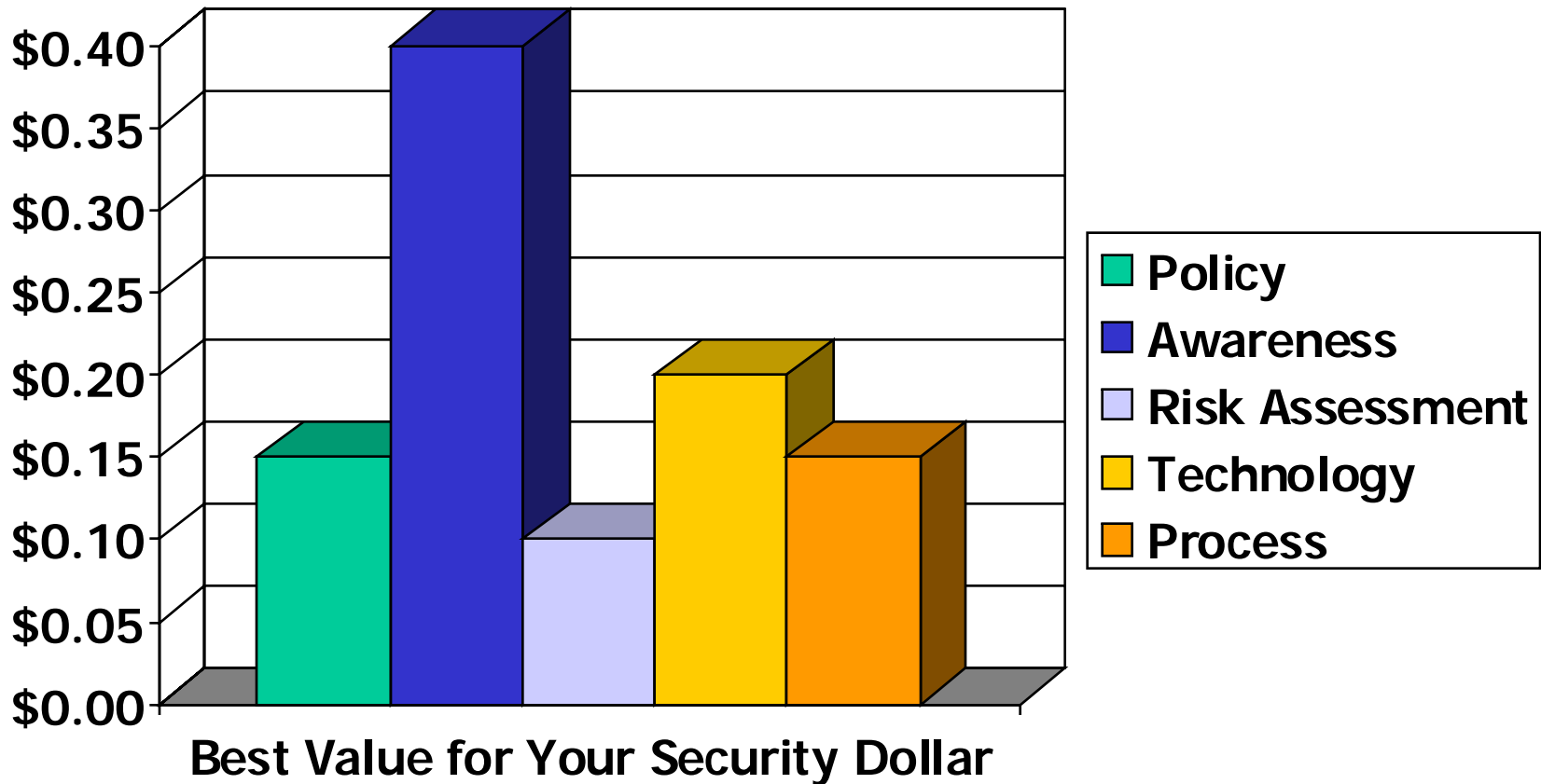


# Roadmap to Security

- **Assessment and planning**
  - Develop a Standard of Due Care
    - Industry and business specific
  - Perform Network Analysis
    - Architecture, Protocol and Application
- **Prevention (deploy and test)**
  - Deploy a Network Infrastructure
  - Deploy Secure Components and Applications
  - Perform Penetration Testing and Q/A
- **Detection, Response and Maintain**
  - Monitor and Maintain for Continued Security



# How to Spend a Dollar on Security

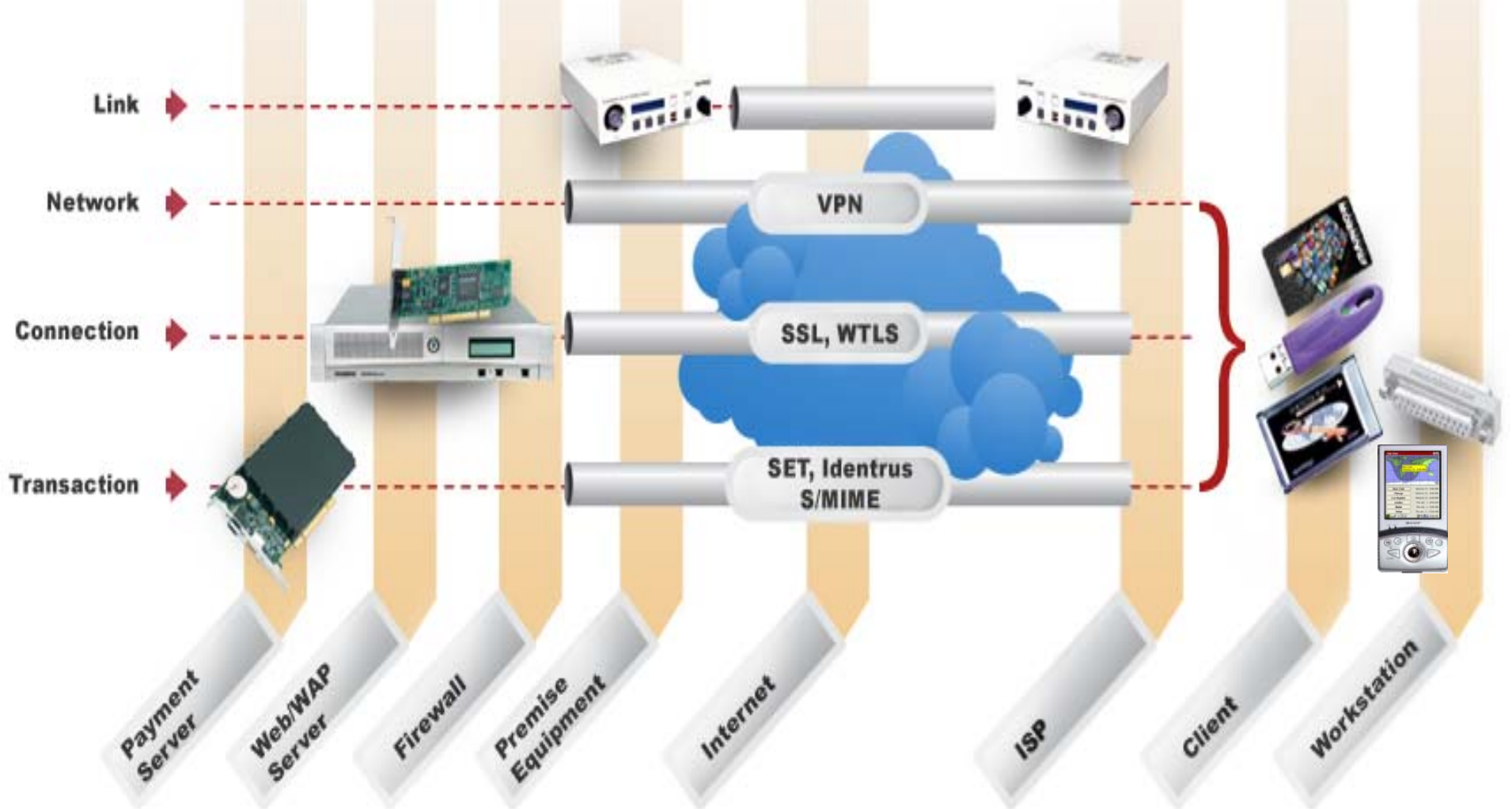


Source: 11/2000 ComputerWorld Article

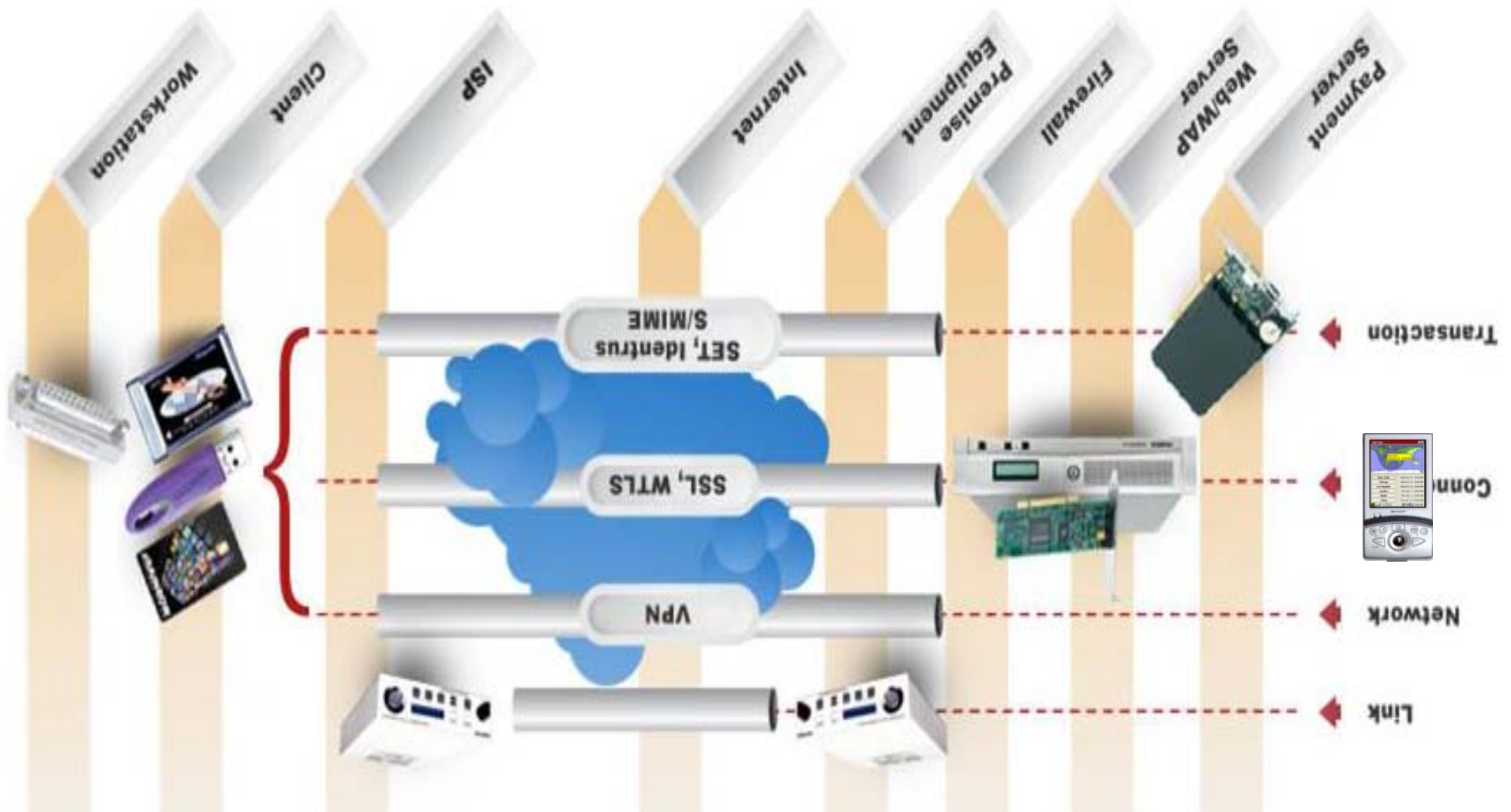
# End-to-End Security Mechanisms

- **Hardware-based encryption**
  - SSL, VPN, Link, Storage, High Speed
- **Data at rest encryption**
- **Multi-factor authentication**
  - Access control tokens
- **Digital signatures**
- **Transparent crypto**
- **Key Management**
  - PKI, digital certificates
- **Instant Private Web**
- **NSA, NIST, and other certifications**

# Security Solutions Overview



# Security Solutions Overview

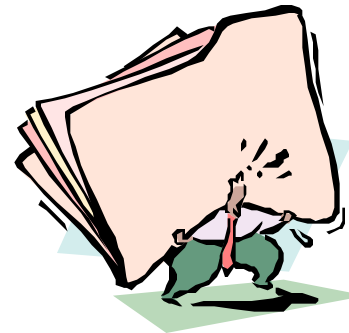
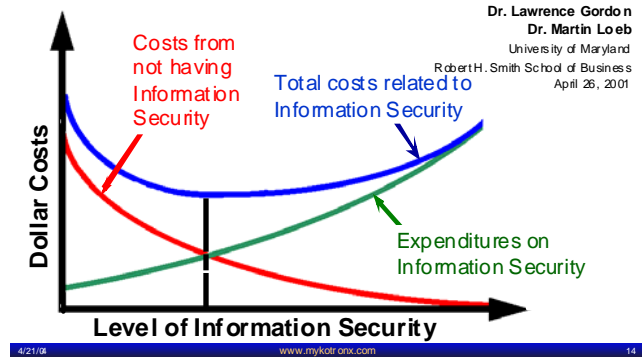


# Solution Evaluation Criteria

- **Ease of:**
  - Use
  - Deployment
  - Management
- **Convenience**
  - Flexibility
  - Portability
- **Robustness**
  - Crypto strength
  - Independent evaluation
- **Scaleable**
- **Compatible**
- **Performance**
- **Cost**



## Economic Aspects of Information Security



## Conclusions

- There is a concentrated effort by the bad guys
- There will be a mix of security products similar to the products on your network
- Identity: the cornerstone of security with tokens / devices making the security real for authentication
- “Defense in Depth”
  - **Don't rely on a single security solution**

*Cryptography needs to provide security AND convenience and performance*

# Questions?

*John Droge*  
*jdroge@mykotronx.com*

*www.mykotronx.com*  
*www.safenet-inc.com*