

---

---

# *Information Systems Security Directions and Challenges*

John Adams

Sr. Vice President of Engineering  
Security Dynamics Inc.

---

---

SecurityDynamics

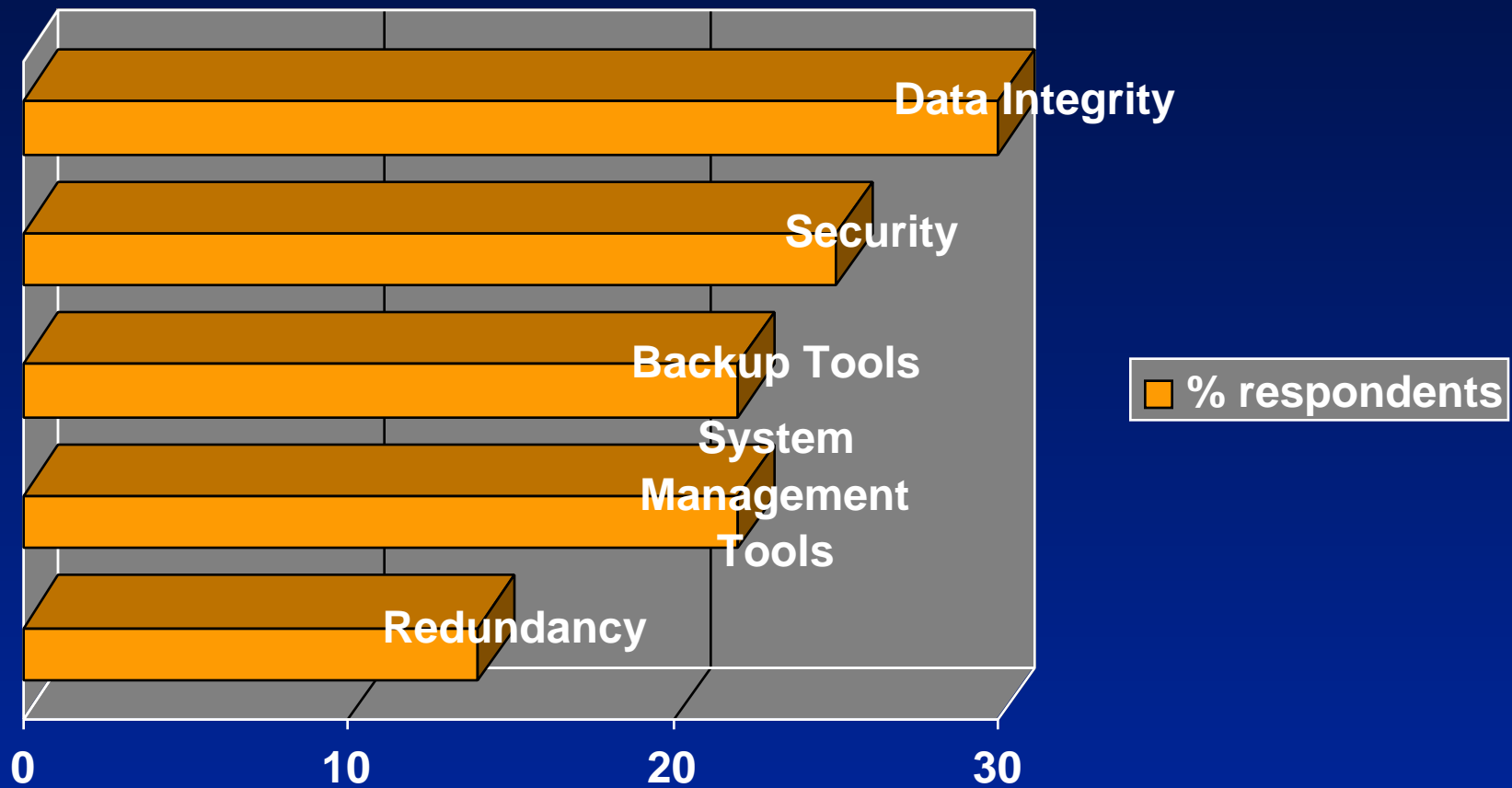
---

---

# *Security Dynamics Inc. Profile*

- Focused primarily on commercial market
- Largest “pure” security company
- Defacto standards for:
  - User “two factor” authentication (SecurID)
  - Public Key Cryptography (RSA)
- Over 1,250,000 users of SecurID technology
- Over 80,000,000 copies of RSA BSAFE tool kits
- Accelerated growth

# What IT managers worry about



Source: Information Week 9/25/95

---

---

# Enterprise Security Market Drivers

- ***Sharp growth in Remote & Internet access to database, electronic mail and network files.*** Worldwide remote access market CAGR of 80% through 1998 (IDC 1995). The need for email and information security and privacy will continue to follow this growth
- ***The number one and two priorities for IT managers are: Data integrity and information security (Information week, 9/25/95)***
- ***Existing infrastructure operating in a broad range of network and platform environments.*** Companies are looking for solutions that span their heterogeneous networks. Customers need multi-platform, enterprise wide security solutions
- ***Companies are integrating network administration with tools that minimize administrative overhead and maximize productivity.*** The “more with less” philosophy will continue to drive the integration and consolidation of administration and management

---

---

# *Information Security Market Drivers*

- Rise of public data networks leading to a sharp growth in remote & Internet access to DBs; Email; Net Apps
- Media exposure is at an all time high (Internet/Intranet)
- Existing infrastructure operating in a broad range of network and platform environments

---

---

# *Information Security Market Drivers*

- Internet technology rapidly being applied to the enterprise (Intranets)
- Increasing demand for integrated network administration to:
  - minimize overhead
  - maximize productivity

---

---

## *So why isn't it here today?*

- Standard, interoperable security solutions are not yet pervasive
- People frequently are not sensitive to security issues (until they get burned that is)
- Security technology is in a state of transition
- Industry has not led in terms of defining a set of acceptable business practices around security

---

---

## *The issues involved*

- You need to know who you are dealing with (Strong Authentication)
- You need to keep private things private (Encryption)
- You need to bind information to people (Digital Signatures)
- You need to assure that people don't cheat (Non-Repudiation and Auditing)

---

---

## *How does the lack of strong security effect things?*

- Lets say you have an electronic contract which you need to distribute to another party over the Internet
- With existing Internet tools like WWW and Email you lose a lot compared with paper
  - No assurance that the contract was signed
  - No guarantee that the contract is authentic
  - No assurance of the source of the contract
- Basically, it's worth the paper its printed on!

---

---

# Challenges

- Internet solutions (TCP/IP, The Web, Email ....) to the corporate Intranet have greatly expanded the reach and exposure of corporate networks
- Proprietary, non-interoperable security solutions are evolving to a standards based open security model based upon public key cryptography

---

---

# Challenges

- SDI is in the middle of this change
  - The leading vendor in token based authentication based upon a proprietary security solution
- RSA brings key technology to the table
  - RSA is recognized as the leader in public key cryptography
  - RSA is driving the development and use of common standards for public key crypto
- The joint company spans both areas

---

---

# *Standards are the key*

- Standards at multiple levels are necessary for pervasive, easy to use, common security solutions
  - Application layer standards
  - Standard certificate and key management systems
  - Standards based, easy to use security administration
  - Shared profiles to set common key sizes, encryption algorithms

---

---

## *How things stand*

- Industry is dominated by a large number of proprietary solutions
- Microsoft & Netscape (others) have formed consortia developing key defacto standards
  - *A few bigger groups fighting this out is better than lots of smaller skirmishes*
- RSA continues to be a focal point for defacto standards development, and is commonly viewed as a neutral partner

---

---

## *How things stand*

- Academia and industry are working well
  - RSA and others host joint conferences and development efforts between academia and industry
- Government and industry are getting closer, but still have fundamental differences
  - Key escrow remains an issue
  - Current regulations in key length cause U.S. developed products to not be competitive with non-U.S. products

---

---

## *Example of emerging standards*

- Secure Email providers appear to be converging on a set of defacto standards
  - PGP and PEM have some popularity, but are hampered by the lack of consistent policies around keys and certificates
  - S/Mime seems to have this under control
    - » Agreements on key length and crypto algorithms
    - » Many vendors are agreeing to support
      - Netscape, Microsoft, Lotus, Banyan, ....

---

---

## *Example of emerging standards*

- IPsec allows the creation of Virtual Private Networks over the Internet
  - including employees working securely from home or on the road over ISPs
  - Router and firewall implementations allow entire networks to be secured without changing any end system software
  - IPsec works without application changes
- IPsec is an IETF standard and could well overtake SSL in the market

---

---

# Smart Cards

- Smart Cards are a key enabler for the practical deployment of public key systems
  - They provide secure private key storage
  - They support on-board cryptographic operations
  - They are a convenient, portable media for certificate storage

---

---

# Smart Cards

- Smart Cards can support multiple applications
  - Physically, the Smart Card can act as an employee badge, printed with a picture and company identification
  - Cryptographically, the Smart Card can act as an authentication device, access control to secure rooms, a digital signature device, and the employee key store

---

---

# Smart Cards

- How big a wallet do you need to carry your Smart Cards?
  - It would be nice to merge multiple applications on a single Smart Card, but there are technical, political, and usage issues which make this unlikely for the near future
  - There are opportunities to merge several related applications onto a single card however

---

---

# *Mixing multiple SC applications*

- Technically, current Smart Card processors and operating systems do not support multiple independent security domains within a card
- Politically, who do you trust to program the last application on the card; who is responsible if the first application is compromised?

---

---

# *Mixing multiple SC applications*

- From a usage point of view, short lived SC applications like a debit card are incompatible with long lived applications like an authentication card
- Classes of applications which are related, have similar lifetimes, and which can be programmed by a single provider can live together

---

---

# *A Security Smart Card*

- A single RSA based Smart Card with the following characteristics makes sense:
  - I&A process based on RSA
  - Secure Private Key storage for all user associated private keys
  - Digital Signature support
  - Certificate storage for the user's certificate, and for frequently used certificates
  - The employee badge

---

---

# *The Security Smart Card*

- Some open issues exist:
  - There is a need for a high quality, secure, and easy to manage enterprise CA
    - » Owned, secured, and operated by the corporation
    - » Supplied as either a service (e.g. VeriSign) or a product
  - Standardization needs to occur around how applications allocate certificates, allocate CRLs, and interface with Smart Cards
    - » Significant progress is happening here

---

---

## *Single Sign-On*

- Single Sign-On has been something that the industry has needed for a long time, but a common, vendor neutral solution has not emerged
- A short lived certificate which certifies an authentication 'cookie' seems to be a promising idea
  - The interaction with authorization privileges needs to be worked out

---

---

## *In closing*

- The emergence of new defacto and dejure standards is enabling interoperable, scaleable, multi-vendor solutions to evolve
  - *We need to keep this momentum going*
- We must continually try to unify the directions of industry, academia, & government

---

---

## *For more information...*

- Security Dynamics home page; “<http://www.securid.com>”
- RSA Labs home page; “<http://www.rsa.com/rsalabs/>”
  - An excellent public key crypto FAQ
  - Free Software
- For information on Secure WAN (IPsec); “<http://www.rsa.com/rsa/SWAN/home.html>”
- For information on Secure Mime (S/MIME); “<http://www.rsa.com/rsa/S-MIME/home.html>”
- For information on Secure Sockets Layer; “<http://home.netscape.com/newsref/std/SSL.html>”
- For information on Secure HTTP; “<http://www.eit.com/projects/s-http/>”
- A starting point on Smart Cards is:  
“<http://www.smart-card.com/>”