



ARETE Consultants
UNDERSTANDING *you*. YOUR *business*.

FINANCIAL DATA & ITS SECURITY THREATS, ISSUES AND PREVENTION FOR CORPORATE

Apurv Kansal,
DIRECTOR,
Arete Consultants Pvt. Ltd

T : 91 11 2625 6363
F : 91 11 2626 1973

E : contact@aretecon.com
W : <http://www.aretecon.com>



ARETE Consultants

UNDERSTANDING *you*. YOUR *business*.



TOP SECRET

T : 91 11 2625 6363

F : 91 11 2626 1973

E : contact@aretecon.com

W : <http://www.aretecon.com>



Apurv Kansal

From: impsoftwares@googlegroups.com on behalf of Sunaina L [sunaina.k1987@yahoo.com]
Sent: Wednesday, May 05, 2010 2:49 PM
To: impsoftwares@googlegroups.com
Subject: Surf Internet Safe & Secured. Now You can watch seamless Cricket.

Hello Members,

Get the worlds fastest browser from Microsoft. Surf Internet Safe & Secured. Now You can watch seamless Cricket.

[Download Here for Free](#)

Regards,
Team Best Software's.



ARETE Consultants

UNDERSTANDING *you*. YOUR *business*.



T : 91 11 2625 6363

F : 91 11 2626 1973

E : contact@aretecon.com

W : <http://www.aretecon.com>

WHAT IF ?

- A Laptop is **HACKED** with data like
 - Customer Names and Contact Details
 - Project Reports
 - Supplier and Costing Details
 - Credit Card Information
 - Raises Good Questions:
 - Should The Data Be On The Notebook?
 - Should It Be Locked Down On A Server In The Data Center?
 - Do We Need To Store All The Information About Our Customers That We Do?



ASK ?

- Are The USB Ports Protected ?
- If A User Downloads Information To Any Portable Device, Can We Detect It ?
- Does Your Policies Cover Storage Of Protected Information On Workstations And/Or Mobile Devices ?
- Testing IT Systems With Live Data ?
- Is The Data Ever Encrypted ?
- Do You Allow Cell Phones In The Office That Can Take Pictures ?
- Are our employees' background verified ?



DATA SECURITY

- Securing corporate and personal data in computer and communication systems against accidental or intentional attacks to maintain the confidentiality and integrity of data
- Attacks can be external or internal, by insiders or outsiders
- Even the most robust information security programs can't prevent physical attack or theft of data
- Hackers are compromising systems faster than information security professionals can patch them
- Hackers, unsatisfied employees, malicious software, unauthorized usage of data storage devices (usually infected) etc can be potential threats to information security



20% Do not have anti-virus software suites such as Norton or Trend Micro on every desktop/laptop



37% No company-wide SPAM filtering on the e-mail



51% No new passwords administered periodically



61% No enforced policies regarding downloading software and apps to company PCs/laptops



67% No VPN or remote access client such as Citrix or Cisco



71% No Web filtering (restricts access to high risk Web sites)



Common Methodologies

- Botnets
- Distributed denial of service (DDoS)
- Phishing
- Vishing
- Virus
- Spam
- Malware
- Crimeware
- Ransomware



Issues

- The Internet connection offers a way to communicate with millions of people globally, but is difficult to control due to its complex and dynamic nature. A wide range of attacks are possible: eavesdropping, identity spoofing, denial of service.
- Connections to vendors/partners are often not secured enough, due to lack of time/resources, or belief in security through obscurity. They can be used as an attack point by Partner organisations (Partners don't always stay partners...) and also for attackers who have already penetrated the Partner's network.
- Sensitive information, if not securely disposed of, will yield a valuable resource to attackers. The main threat is unauthorised access to information.



Issues

- Wide area networks are used to extend the corporate Intranet to many remote areas. The cabling probably passes through public zones. The complexity of Wide Area Networks can serve as a deterrent to attackers, but is it enough?
- Social engineering can be used to trick personnel into divulging information or providing access. Helpdesks may also be subject to social engineering, providing modem numbers, passwords etc. unwittingly to unauthorised persons.
- Many people who are not employees, will have access to buildings in one way or another. Threats include theft, damage and copying.
- Other physical threats include laptop theft, natural disasters and loss of media during transport.



Issues

- Security policies and technology are not in sync with organisational changes
- Continued vulnerability of key technology products
- Exponential increase in data traversing through networks
- Decrease in requirement of technical skills to hack into a system



ARETE Consultants

UNDERSTANDING *you*. YOUR *business*.

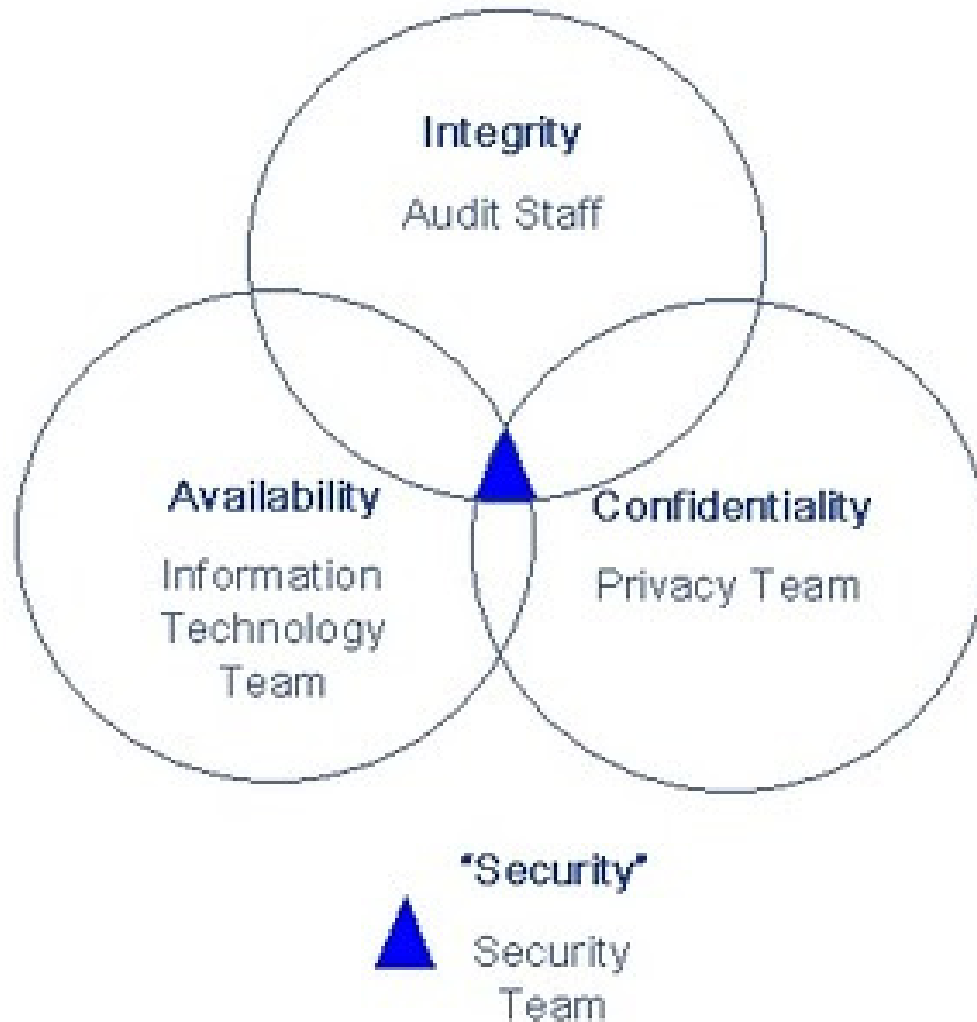


T : 91 11 2625 6363

F : 91 11 2626 1973

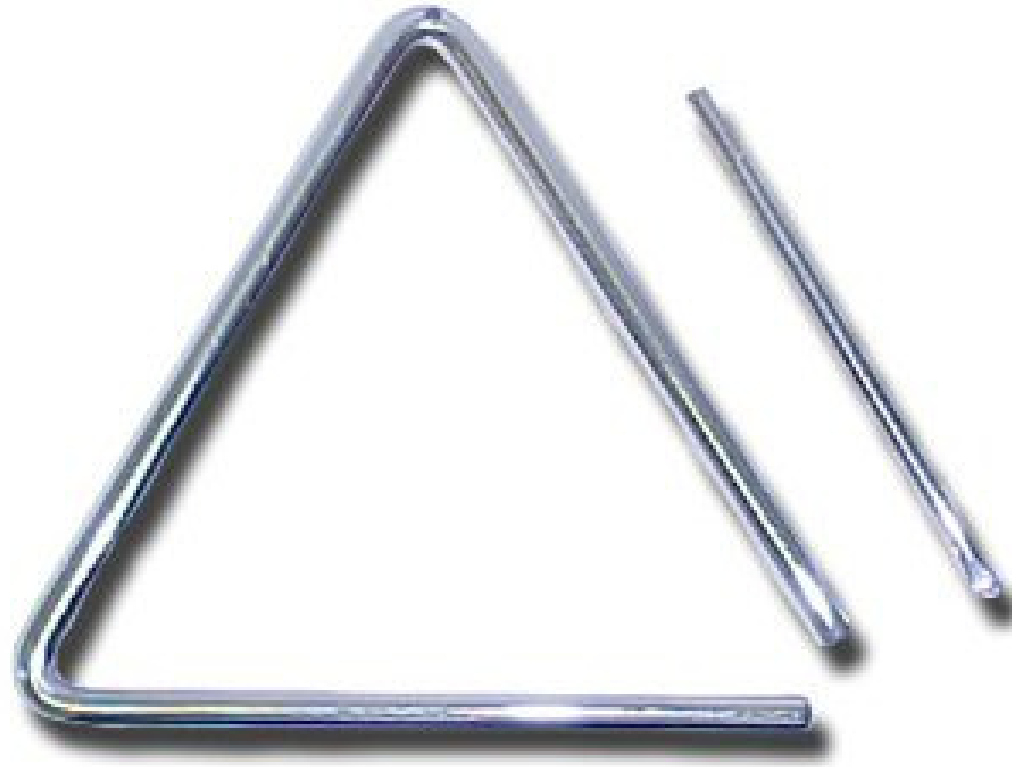
E : contact@aretecon.com

W : <http://www.aretecon.com>





Time



Resources

Functionality



Risks

- **Inherent Risks:**
 - Nature of Business
 - Geographical spread of Institution
 - Management's approach towards Information Security
- **Control Environmental Risks:**
 - Physical Access to the Information System
 - Improperly defined User roles & authorizations
- **Other Risks:**
 - Inappropriate incident handling
 - Insufficient Security Measures
 - Irrational access of Information System of vendors, consultants etc

Parameters for selecting safeguards

- **The nature of the threat:** The attackers resources (financial, technical, time), degree of motivation and ease of access should all be considered. For example, most would expect frequent attacks from the Internet, so firewalls between the Internet and Intranet are frequent.
- **Information lifetime:** How is information generated, stored, processed, copied, printed and destroyed?
- **Information aging:** How does time affect the information? e.g. a new pricelist might be sensitive before publication and would published to the world subsequently. A new pricelist replaces an old one, becomes useless.



The Information-Centric Security Lifecycle





Prevention

- Ownership – Assign ownership to information
- Classification of Information
- Access Controls – Set access controls for the users
- User Identification & Cryptography – Initiate an employee identification system and encrypt the sensitive data.
- Disposal – dispose off sensitive information safely and properly



Must Haves

- Top Management Support
- Legal & Regulatory Compliance (HIPAA, GLBA, PCI DSS, Sarbanes-Oxley, ISO 27001)
- End User Awareness, Training & Continued Education
- Robust Information Security policies
- Disaster Recovery and Business Continuity Planning
- Periodical audit of IT systems and software



A Few Tips

- Don't store sensitive data unnecessarily. Shred documents regularly
- Don't store sensitive data in plaintext
- Keep a copy of data offsite
- Beware of Wi-Fi
- Use Public Computers judiciously
- Use a firewall
- Look at your infrastructure
- Stay on top of security releases and anti-virus updates
- Treat security as an ongoing activity



ARETE Consultants

UNDERSTANDING *you*. YOUR *business*.



Apurv Kansal
apurv@aretecon.com
+91-9811-500-506

T : 91 11 2625 6363

F : 91 11 2626 1973

E : contact@aretecon.com

W : <http://www.aretecon.com>



ARETE Consultants
UNDERSTANDING *you*. YOUR *business*.

Contact Us

Arete Consultants Pvt. Ltd. INDIA

302, South Ex. Plaza I,
NDSE Part – II,
New Delhi – 100 049, India.

M : 91 11 2625 6363

E : contact@aretecon.com

W : <http://www.aretecon.com>,
<http://www.aretesoftware.com>

View our portfolio at: <http://www.aretesoftware.com/>

THANK YOU!!

T : 91 11 2625 6363

F : 91 11 2626 1973

E : contact@aretecon.com

W : <http://www.aretecon.com>