Securing Indian Cyber Space

'Issues and Challenges'

Indian Computer Emergency Response Team (CERT-In)
Department of Information Technology
Ministry of Communications and Information Technology
Government of India
Tel: 011-24363138, Web: http://www.cert-in.org.in, E-mail: info@cert-in.org.in

"In security matters,

there is nothing like **absolute** security"

"We are only trying to build **comfort levels,** because security costs money and lack of it costs much more"

"Comfort level is a manifestation of efforts as well as a realization of their effectiveness & limitations'

Cyber Security – Why is it an issue?

Because…..although the threats in cyber space remain by and large the same as in the physical world (ex. fraud, theft and terrorism), they are different due to 3 important developments

- automation has made attacks more profitable
- action at a distance is now possible
- attack technique propagation is now more rapid and easier

Cyber Security – Why is it an issue?

In addition to the 3 important developments, there are 3 more trends that make an enterprise transparent and vulnerable

- Internet enabled connectivity
- Wireless networking
- Mobile computing

"Good recipe for trouble – E-Commerce+M-Commerce +Critical sector plus well known brand-name"

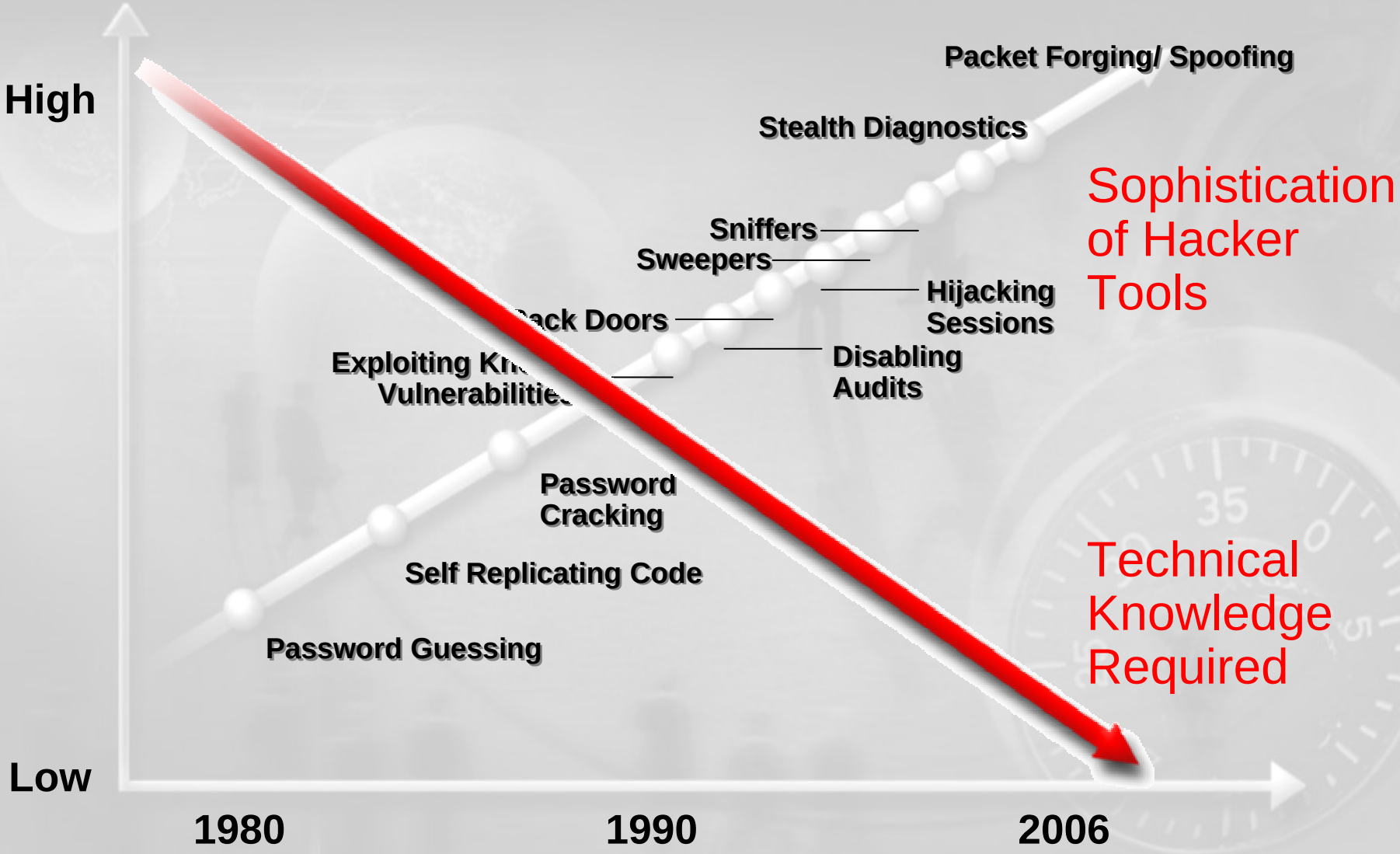
Today's Enterprise – Struggle for balance

Today, the enterprises need to balance the four requirements simultaneously

- Sensible investments and reasonable ROI
- Compliance with legal requirements
- Facilitate business with secure access to information and IT resources
- Keep intruders at bay

An improperly managed & vulnerable IT infrastructure can upset the balance

Information Security – General trends



Active bot net work computers per day

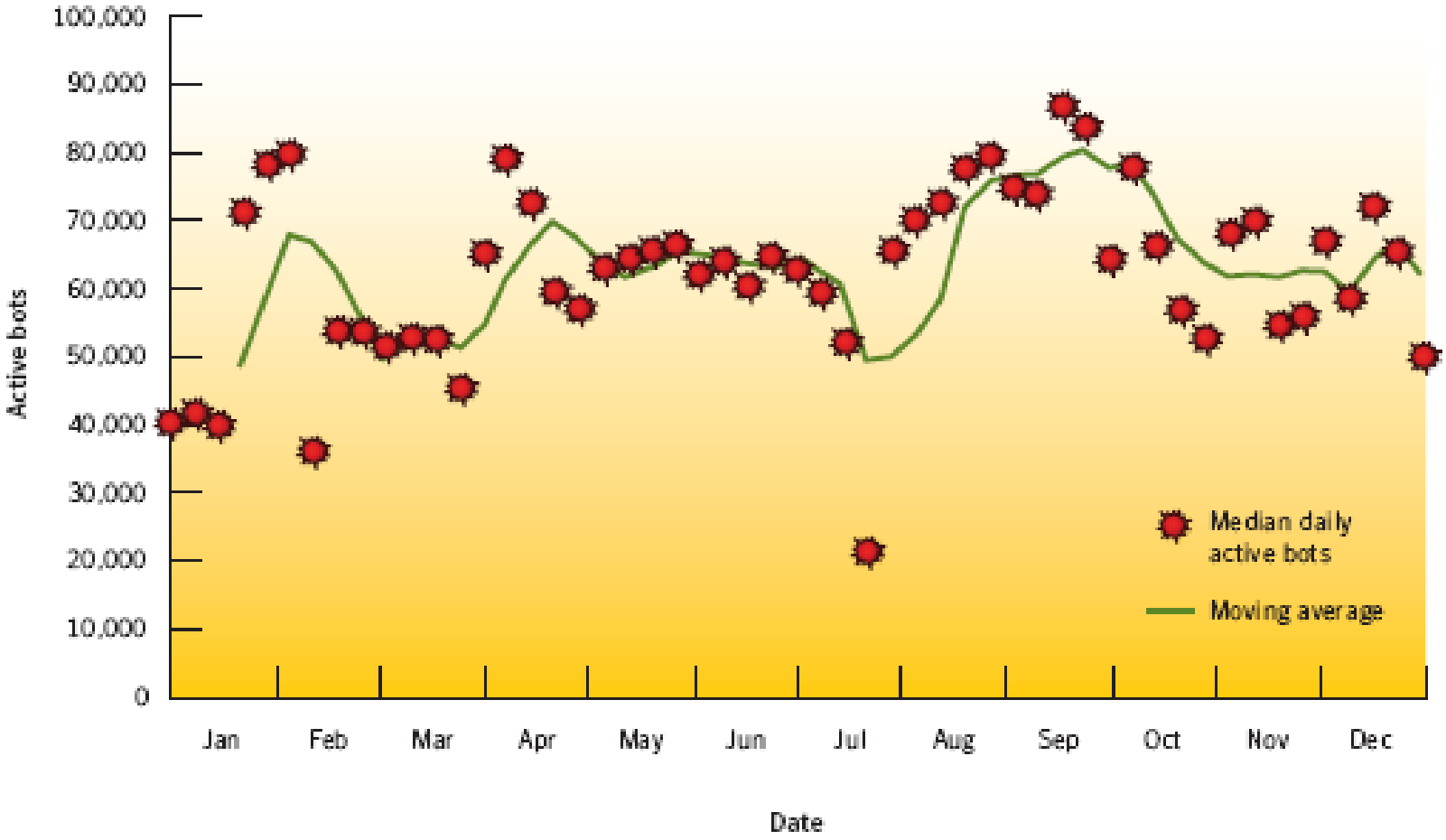


Figure 11. Active bot-infected computers per day
Source: Symantec Corporation

Top countries by bot-infected computers

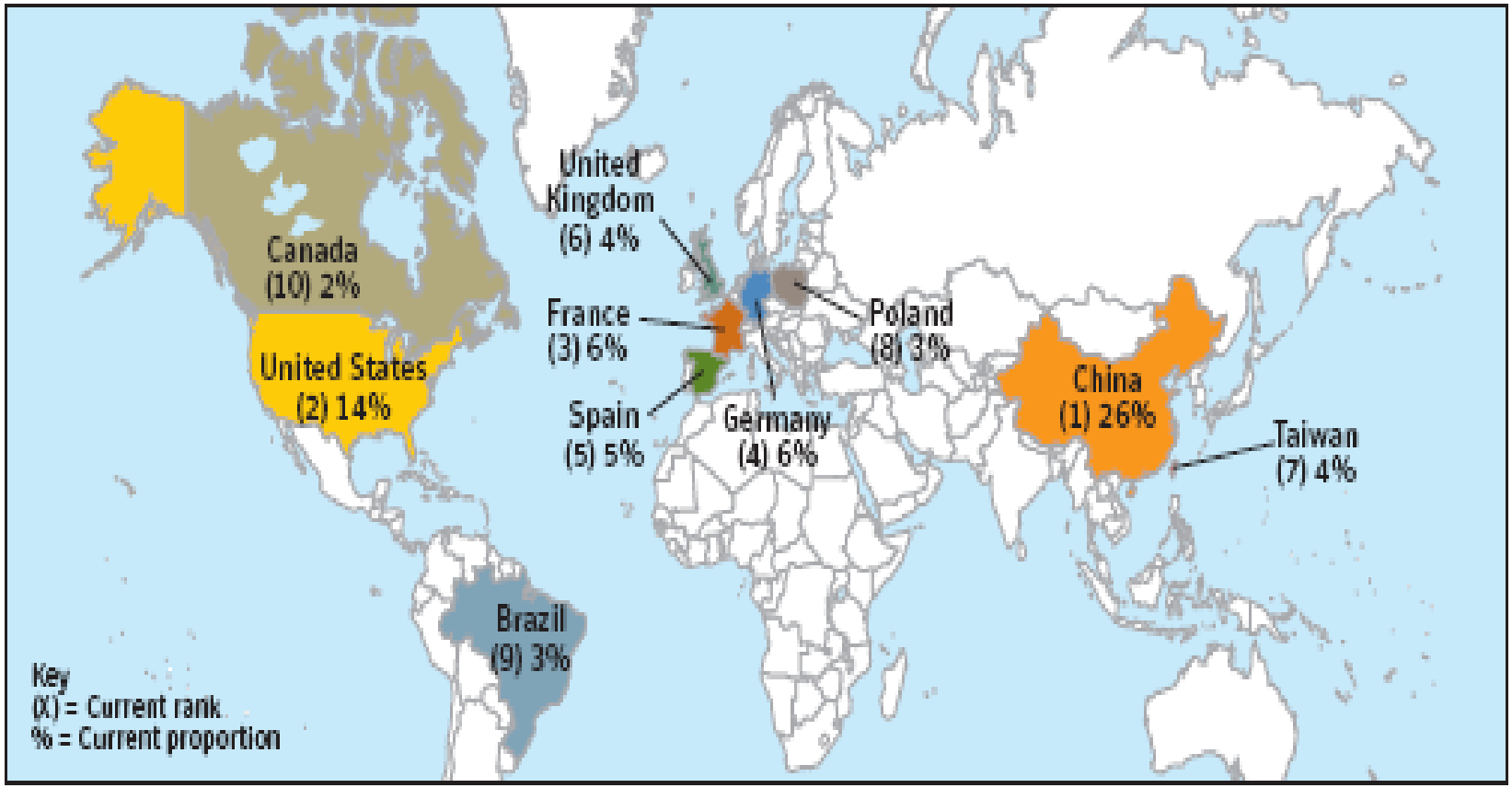


Figure 12. Bot-infected computers by country

Source: Symantec Corporation

Denial of service attacks per day

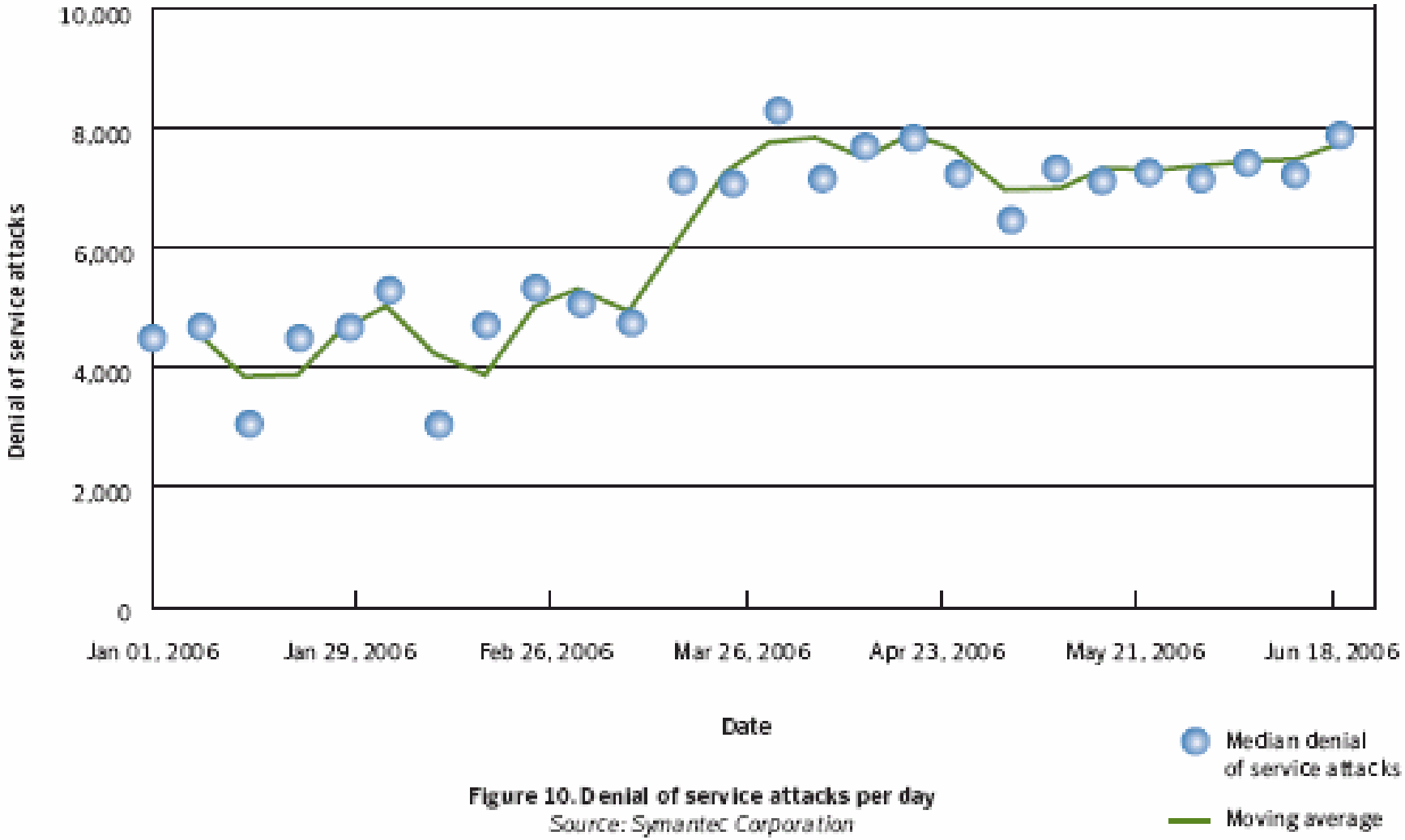
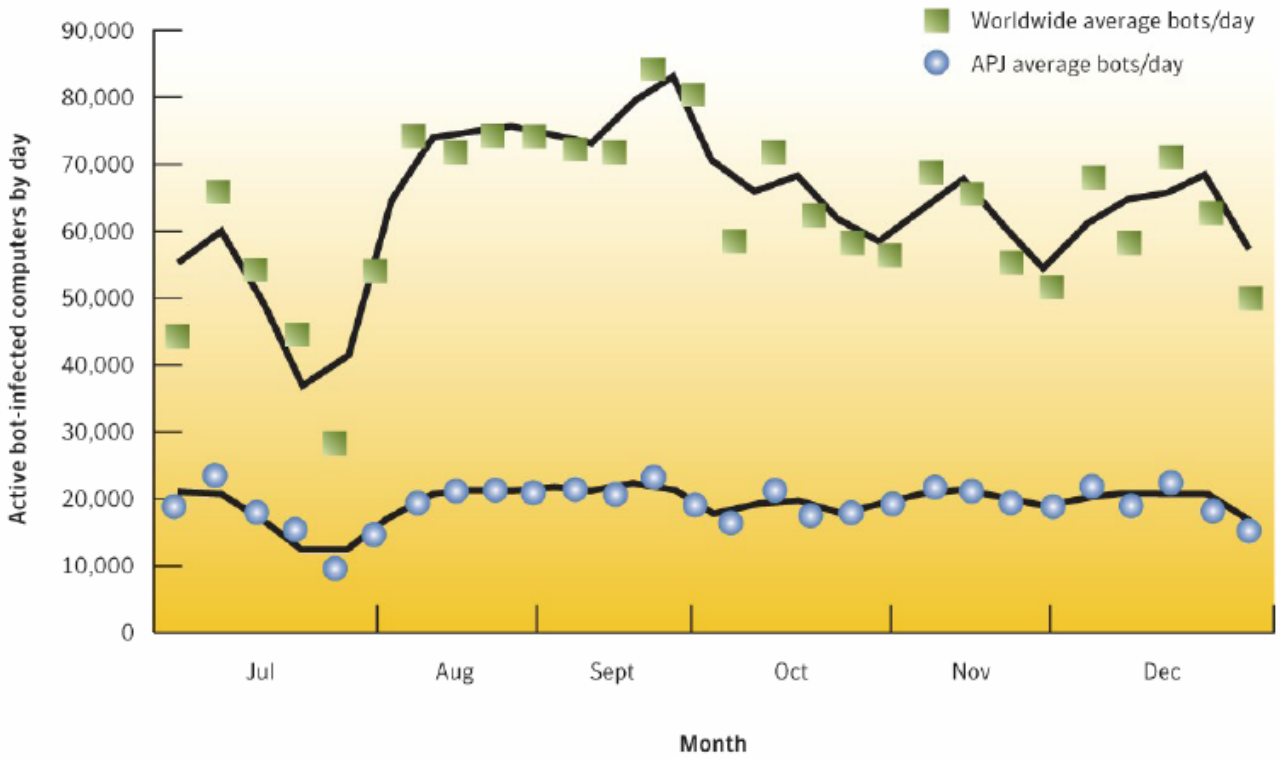


Figure 10. Denial of service attacks per day
Source: Symantec Corporation

Active bot infected computers per day

- Symantec observed an average of 19,095 active distinct bot-infected computers per day in the APJ region.
- Symantec detected an average of 277 active bot-infected computers per day in India. .

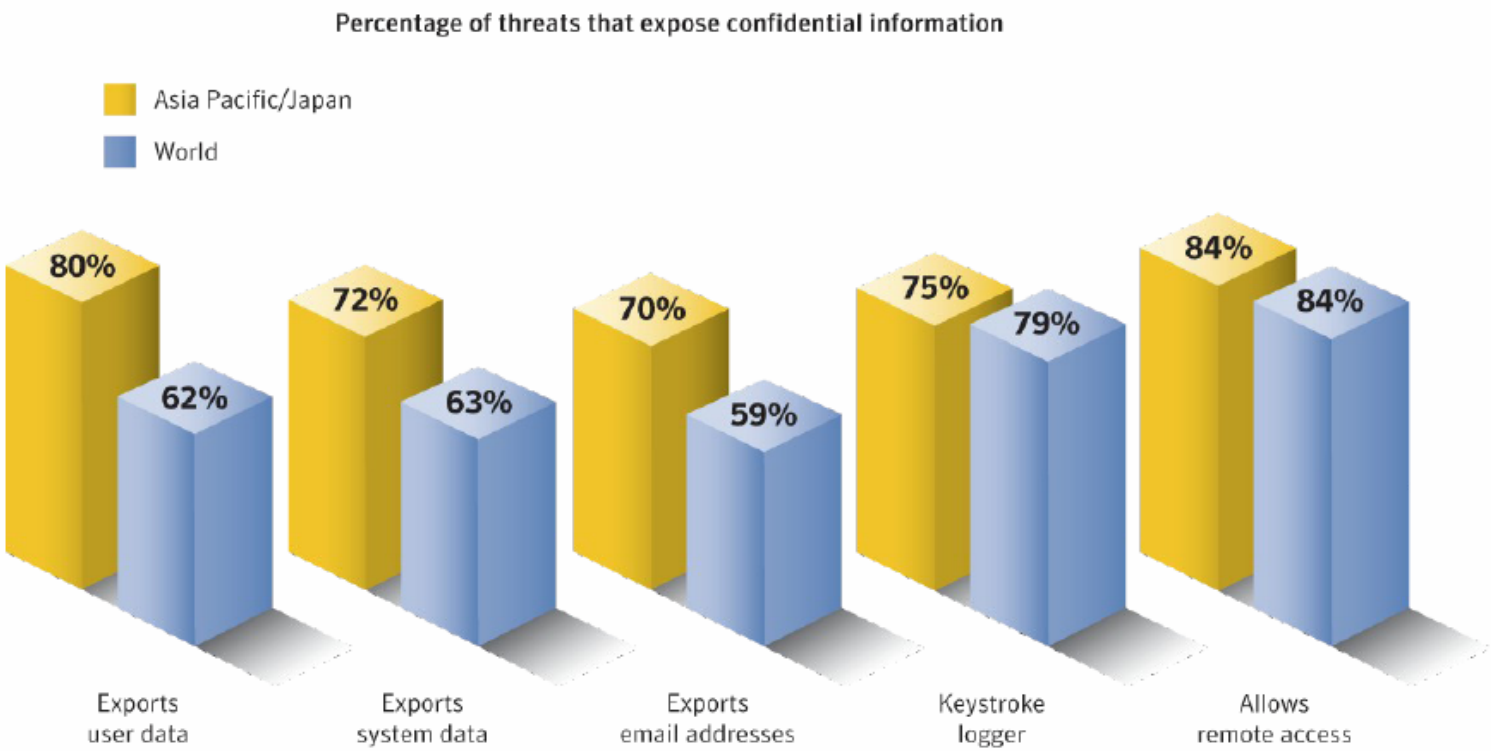


SPAM in India

- Spam originating in India accounted for one percent of all spam originating in the top 25 spam-producing countries making India the eighteenth ranked country worldwide for originating spam.
- A high percentage of email originating in India constituted spam. Of the messages originating in India 76 percent were considered spam

Threats to confidential information

- 60% of the top 50 malicious codes reported in India contained threats to confidential information
- 84% of confidential information threats by volume allowed remote access



Global Cyber Trends – The next wave

Recent studies reveal three major findings:

- Growing threat to national security - web espionage becomes increasingly advanced, moving from curiosity to well-funded and well-organized operations aimed at not only financial, but also political or technical gain
- Increasing threat to online services – affecting individuals and industry because of growth of sophistication of attack techniques
- Emergence of a sophisticated market for software flaws – that can be used to carry out espionage and attacks on Govt. and Critical information infrastructure. Findings indicate a blurred line between legal and illegal sales of software vulnerabilities

Mischievous activities in cyber space have expanded from novice geeks to organized criminal gangs that are going Hi-tech

Threats to National security

Internet has become an weapon for political, military and economic espionage

- Organized cyber attacks have been witnessed in last 12 months
  - Pentagon, US in June 2007
  - Estonia in April 2007
  - Computer systems of German Chancellery and three Ministries
  - E-mail accounts at National Informatics Centre, India
  - Highly classified Govt. computer networks in New Zealand & Australia
- The software used to carry out these attacks indicate that they were clearly designed & tested with much greater resources than usual individual hackers
- Most Govt. agencies and companies around the world use common computing technologies & systems that are frequently penetrated by criminal hackers and malware
- Traditional protective measures are not enough to protect against attacks such as those on Estonia, as the complexity and coordination in using the botnets was totally new. National networks with less sophistication in monitoring and defense capabilities could face serious problems to National security

There are signs that intelligence agencies around the world are constantly probing others' networks and developing new ways to gather intelligence

Threats to Online services

Online services are becoming prime targets for cyber criminals

- Cyber criminals continue to refine their means of deceit as well as their victims In summary, the global threats affecting users in 2008 are:
  - New & sophisticated forms of attacks
  - Attacks targeting new technologies, such as VoIP (vishing – phishing via VoIP & phreaking – hacking tel networks to make free long distance calls) and peer-to-peer services
  - Attacks targeting online social networks
  - Attacks targeting online services, particularly online banking services
- There is a new level of complexity in malware not seen before. These are more resilient, are modified over and over again and contain highly sophisticated functionality such as encryption (Ex. Nuwar also known as 'Zhelatin' and 'Storm' worm' – with a new variant appearing almost daily)
- As a trend we will see an increase in threats that hijack PCs with bots. Another challenging trend is the arrival of self-modifying threats

Given the exponential growth in social networking sites, social engineering may shortly become the easiest & quickest way to commit ID theft

Hi-Tech crime: A thriving economy

The market is growing for zero-day threats & tools for cyber crime

- With so many PCs now infected (around 5 % of all global machines are zombies), competition to supply botnets has become intense. The cost of renting a platform for spamming is now around $ 3 - 7 Cents per zombie per week
- A budget as little as $ 25 to $ 1500 USD can buy you a trojan that is built to steal credit card data and mail it you. Malware is being custom written to target specific companies and agencies
- Computer skills are no longer necessary to execute cyber crime. On the flip side malware writers today need not commit crimes themselves. People can subscribe to the tools that can keep them updated with latest vulnerabilities and even test themselves against security solutions (Ex. MPACK or Pinch include support service)
- The black market for stolen data (Ex. Credit cards, e-mails, skype accounts etc) is now well established and the cost of obtaining credit cards is upwards of $ 5 USD
- Another black market that is causing alarm to Govts is that of Zero-day exploits. In Jan 2006 a Microsoft WMF (windows meta file) exploit was sold for $ 4000 USD

Competition is so intense among cyber criminals that ‘customer service’ has now become a specific selling point

Future Challenges

Trends suggest an increase in safe havens for cyber criminals and hence the need for International cooperation arrangements

- It is an inevitable reality that some countries will become safe havens for cyber criminals and international pressure to crack down won't work well
- It is believed that in next few years Govts are likely to get aggressive and pursue action against the specific individuals/groups/companies, regardless of location
- It is also likely that Govts will start putting pressure on intermediary bodies that have the skills and resources, such as banks, ISPs and software vendors to protect the public from malware, hacking and social engineering
- We may see industry sector codes of practice demanding improved security measures, backed probably by assurance and insurance schemes
- Greater connectivity, more embedded systems and less obvious perimeters
- Compliance regulations will drive upgrades and changes and also increase system complexity and legal wrangles – increase in civil suits for security breaches
- Massive data storing patterns that ensure data never goes away – a boon to law enforcement agencies

As of now, cyber criminals seem to have no real threat of prosecution. Our job is to create a climate of fear of effective prosecution, as in other types of crime

Securing Indian Cyber Space

role of

Indian Computer Emergency Response Team (CERT-In)

CERT-In: Mission and Mandate

Established in 2004

Mission: 'Alert, Advice and Assurance'

'Ensure security of cyber space in the country'

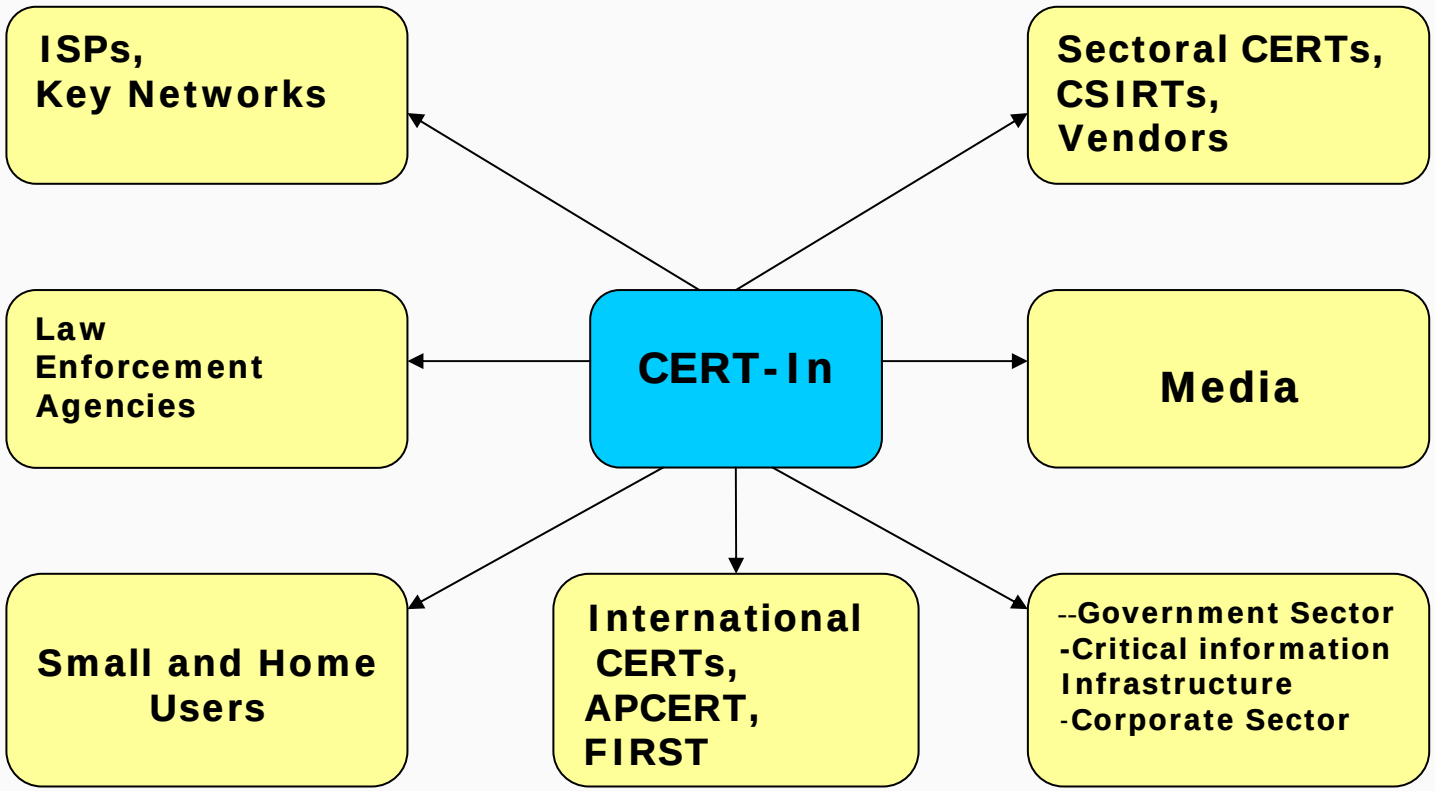
by

'Enhancing the security of communications and Information infrastructure'

through

'Proactive action and effective collaboration aimed at security incident prevention, prediction & protection and security assurance'

Information Sharing: Stakeholders



CERT-In is the nodal agency to coordinate all cyber security related matters in India

CERT-In - Cyber Security Focus

It has four enabling actions:

- Enabling Govt. as a key stakeholder in creating appropriate environment/conditions by way of policies and legal/regulatory framework to address important aspect of data security and privacy protection concerns. *Specific actions include – National Cyber Security policy, amendments to Indian IT Act, security and privacy assurance framework, crisis management plan (CMP) etc.*
- Enabling User agencies in Govt. and critical sectors to improve the security posture of their IT systems and networks and enhance their ability to resist cyber attacks and recover within reasonable time if attacks do occur. *Specific actions include – security standards/ guidelines, empanelment of IT security auditors, creating a network & database of points-of-contact and CISOs of Govt & critical sector organisations for smooth and efficient communication to deal with security incidents and emergencies, CISO training programmes on security related topics and CERT-In initiatives, cyber security drills and security conformity assessment infrastructure covering products, process and people*

CERT-In - Cyber Security Focus

- Enabling CERT-In to enhance its capacity and outreach and to achieve force multiplier effects to serve its constituency in an effective manner as a `Trusted referral agency'. *Specific actions include – National cyber security strategy (11th Five Year Plan), National Cyber Alert system, MoUs with vendors, MoUs with CERTs across the world, network of sectoral CERTs in India, membership with international/regional CERT forums for exchange of information and expertise & rapid response, targeted projects and training programmes for use of and compliance to international best practices in security and incident response.*
- Public Communication & Contact programmes to increase cyber security awareness and to communicate Govt. policies on cyber security.

Cyber Security – Strategic objectives

- Prevent cyber attacks against the country's critical information infrastructures
- Reduce national vulnerability to cyber attacks
- Minimise damage and recovery time from cyber attacks

Security Assurance – Actions at Country level

- Policy directives on data security and privacy protection - Compliance, liabilities and enforcement (ex. Information Technology Act 2000)
- Standards and guidelines for compliance (ex: ISO 27001, ISO 20001 & CERT-In guidelines)
- Conformity assessment infrastructure (enabling and endorsement actions concerning security product – ISO 15408, security process – ISO 27001 and security manpower – CISA, CISSP, ISMS-LA, DISA etc.)
- Security incident - early warning and response (National cyber alert system and crisis management)
- Information sharing and cooperation (MoUs with vendors and overseas CERTs and security forums).
- Pro-active actions to deal with and contain malicious activities on the net by way of net traffic monitoring, routing and gateway controls
- Lawful interceptions and Law enforcement.
- Nation wide security awareness campaign.
- Security research and development focusing on tools, technology, products and services.

Security Assurance – Actions at Network level (ISP)

- Compliance to security best practices (ex. ISO27001), service quality (ISO 20001) and service level agreements (SLAs) and demonstration.
- Pro-active actions to deal with and contain malicious activities, ensuring quality of services and protecting average end users by way of net traffic monitoring, routing and gateway controls
- Keeping pace with changes in security technology and processes to remain current (configuration, patch and vulnerability management)
- Conform to legal obligations and cooperate with law enforcement activities including prompt actions on alert/advisories issued by CERT-In.
- Use of secure product and services and skilled manpower.
- Crisis management and emergency response.

Security Assurance – Actions at Corporate level

- Compliance to security best practices (ex. ISO27001), and demonstration.
- Pro-active actions to deal with and contain malicious activities, and protecting average end users by way of net traffic monitoring, routing and gateway controls
- Keeping pace with changes in security technology and processes to remain current (configuration, patch and vulnerability management)
- Conform to legal obligations and cooperate with law enforcement activities including prompt actions on alert/advisories issued by CERT-In.
- Use of secure product and services and skilled manpower.
- Crisis management and emergency response.
- Periodic training and up gradation of skills for personnel engaged in security related activities
- Promote acceptable users' behavior in the interest of safe computing both within and outside.

- Maintain a level of awareness necessary for self-protection.
- Use legal software and update at regular intervals.
- Beware of security pitfalls while on the net and adhere to security advisories as necessary.
- Maintain reasonable and trust-worthy access control to prevent abuse of computer resources.

Cyber Security – Why is the reluctance?

- May be, the stakeholders including customers have not yet started insisting on an assurance
- Many organisations would not want to implement strong security measures thinking that they do not have anything that others would want – probably what they do not realize is that they could become launch pads for attacks on others (Need to be a good neighbour)

Cyber Security – Why is the reluctance?

- Quite possibly, there could be other pressing issues of survival that relegate security to an afterthought
- Sometimes, there is a confusion – Is it Confidentiality, Integrity & Availability or the other way?
- Besides this, there is a very difficult choice between convenience and security measure
- Or simply, their cyber space is empty

Cyber Security Assurance

It is certainly not true that organisations are not interested in security.

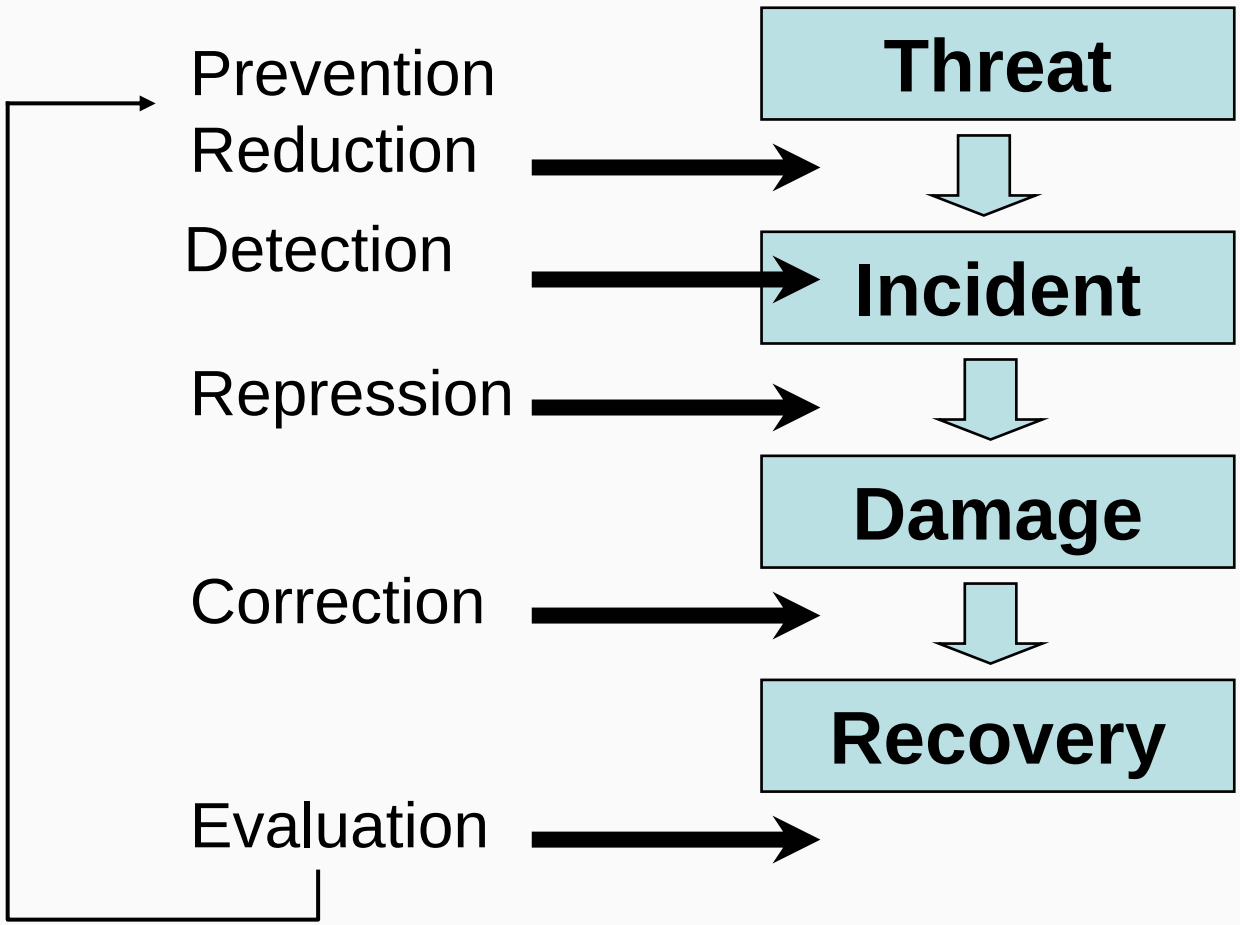
…….Then what is holding them back?

Security Assurance - Expectations

"To determine how much is too much, so that we can implement appropriate security measures to build adequate confidence and trust"

"To derive a powerful logic for implementing or not implementing a security measure"

Security Assurance - Outcome



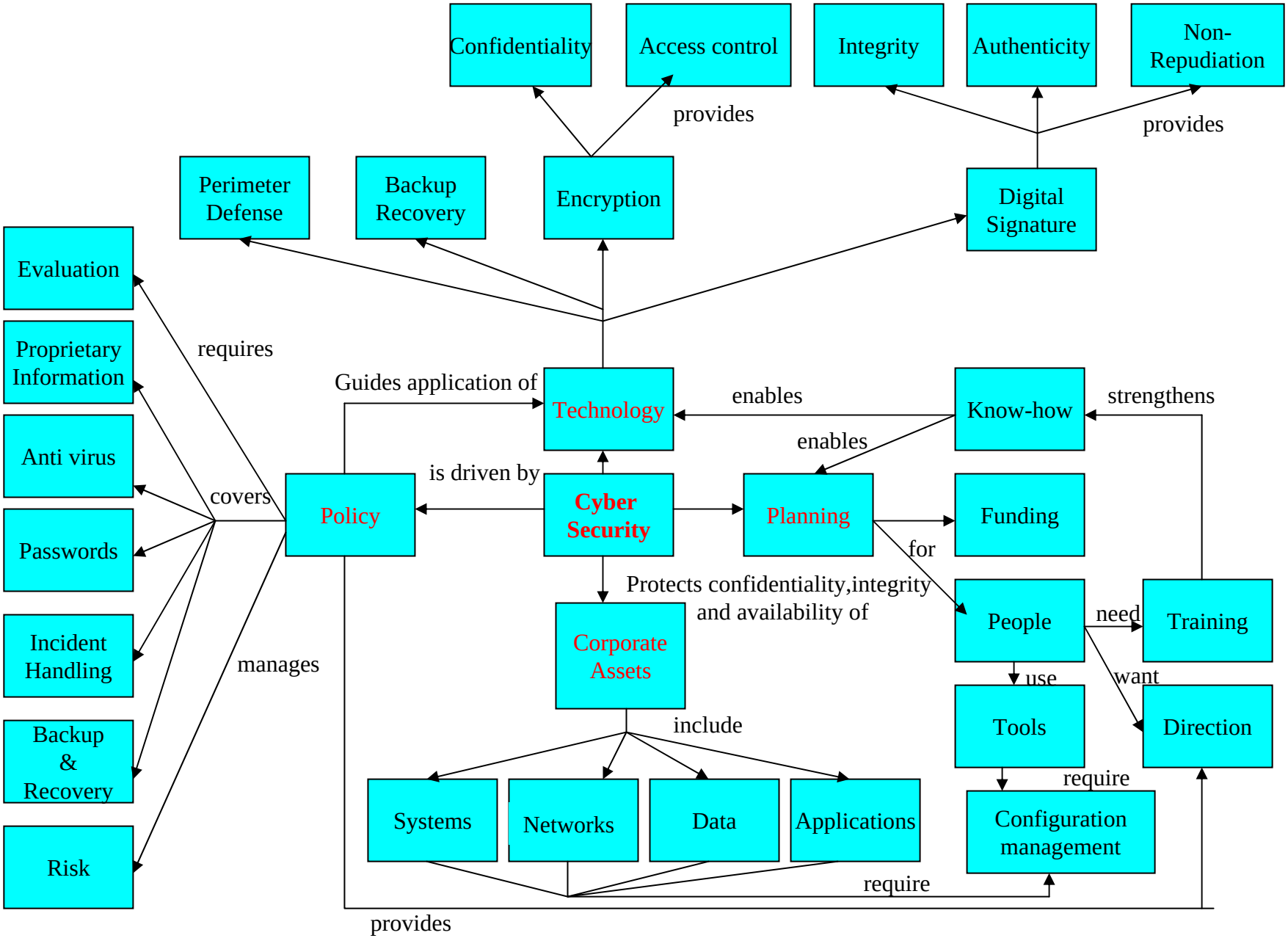
Security Assurance - Emphasis

With security assurance, we are not intending to make the system ‘hacker proof’, but devise a mechanism which can, to a large extent

- Anticipate potential problems
- Pre-empt through proactive measures
- Protect against considerable damages
- Ensure recovery and restoration

‘It is all about the ability to **expect the expected** before we are ready to **expect the unexpected’**

Cyber Security Assurance - Focus



Security Assurance @ National level

"National Information Security Assurance Program (NISAP)"

for

Government and Critical Infrastructure Organizations

Security Assurance Framework – Concept

It has four elements

- Mandatory compliance requirement – *in the form of a legal/regulatory framework*
- Mandatory compliance efforts – *to ISMS standards like ISO/IEC 27001/IS 15150/BS 7799 etc*
- Mandatory compliance verification – *of security technical, managerial as well as operational controls including ISMS assessments, penetration testing, vulnerability assessment, application security testing etc*
- Mandatory compliance reporting – *to CERT-In as a notified entity on a periodic basis*

Security Assurance Framework - Highlights

- Covers three kinds of web & networking environment, depending on types of risks & related business impact
  - **Low risk -** *In general, the environment caters to providing information to users*
  - **Medium risk -** *In general, the environment caters to providing information to users and allowing some amount of interaction including non-commercial transactions*
  - **High risk -** *In general, the environment caters to providing information to users, allowing interaction and commercial transactions including on-line payments*

Security Assurance Ladder

- Security control emphasis depends on the kind of environment
  - Low risk : ***'Awareness'*** *– know your security concerns and follow best practices*
  - Medium risk*:* ***'Awareness & Action'*** *– Proactive strategies leave you better prepared to handle security threats and incidents*
  - High risk*:* ***'Awareness, Action and Assurance'*** *– Since security failures could be disastrous and may lead to unaffordable consequences, assurance (basis of trust & confidence) that the security controls work when needed most is essential.*

Cyber Security - Final Message

"In security matters

Past is no guarantee; Present is imperfect and Future is uncertain"

"Failure is not when we fall down, but when we fail to get up"

“We want you Safe”

Thank you