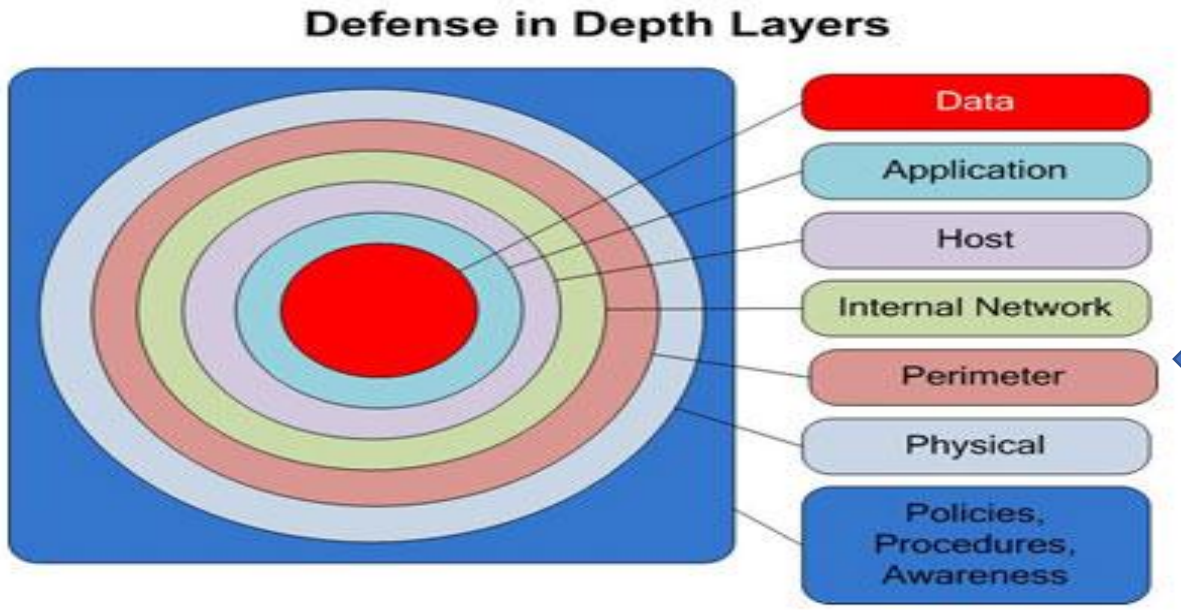
Latest Trends of in Cyber Hygiene

Defence in Depth and Still Vulnerable!!!!!



When it comes to Organisational cyber threat, employee, partners and vendor must be taken as seriously as WE DO it for our own personal security

KRATIKAL
SECURE FOR SURE

Increase in Cyber threats

- More than 4,000 ransomware attacks have occurred every day since the beginning of 2016 – Barkly
- Cybercrime damages will cost the world $6 trillion annually by 2021 - Cyber Security Ventures
- India witness one cyber crime every 10 minutes - NCRB Reports
- 90% of the Cyber Attacks take place due to the employees of the organisation – Kaspersky
- It seems Back door is implemented everywhere to harness the individual dat
- 2 Million Cyber Security Professionals needed in the world by 2019 – Forbes

KRATIKAL
SECURE FOR SURE

Where Does the Threat Arise?

Traditional Threat Vectors
System / Devices etc
Desktop Applications
USB / Mounted Media
Browser
Email Security
Security Over Websites
Data Security

Modern Threat Vectors
Mobile Phone / Tabs
Mobile apps (utility)
Phone / SMS
Chat Messengers
Resources: Camera, Microphone
Theft
Data Security

KRATIKAL
SECURE FOR SURE

Desktops/Laptops Hygiene

Threat

- Malware Attacks
- **Ransomware**
- Device Theft
- Data theft
- Zero Day Vulnerabilities
- Data Privacy
- Backdoors

Case in point

- A recent Zero day vulnerability in Microsoft Office rendered all versions post Office 2010 susceptible to hacking.
- The vulnerability involved unsuspecting users downloading a .hta file, renamed as a .rtf file. This file, upon execution, ran a VBScript which provided a *Remote Code Execution*

Traditional Hygiene

- Good Antivirus
- Regular Updates of the OS
- Using user account instead of admin account
- Configuring firewalls to block connections
- Uninstall stale applications
- Avoiding Piracy and Cracking

Modern Hygiene

- Covering camera with a Post-It/Sticky
- Disabling microphone while not in use
- Virtual Assistants: **Cortana, Siri, Alexa**
- BIOS Passwords
- Group Policies
- Active Directories
- Microsoft Account*

KRATIKAL
SECURE FOR SURE

Removable Media

Threats

- Vectors for Malware Attacks
- Data Theft
- USB Dropping in the parking lot
- Rubber Ducky: Is your USB drive actually a USB drive ?
- Killer USB: https://www.youtube.com/watch?v=X4OmkBYB4HY

Traditional Hygiene

- Blocking of Removable Storage
- Antivirus Engines

Modern Hygiene

- Physical port blocking
- Blocking external input devices
- Testing against Power Surges

KRATIKAL
SECURE FOR SURE

Web browsing

Threats

- Malicious Links
- Malicious JavaScripts
- Malvertisements
- Form Autofill data
- Stored Credentials
- Browser Cache and History

Traditional Hygiene

- Antivirus
- Private Browsing
- Master Passwords

Modern Hygiene

- Light Beam
- Adblockers
- Web of Trust
- Dr. Web Link Checker
- JSGuard

KRATIKAL
SECURE FOR SURE

E-Mail Security

Threats

- Phishing attempts
- Spam Mails
- Mail Spoofing/Fake Mails
- E-Mail Privacy
- E-Mail Compromise
- E-Mail Confidentiality

Traditional Hygiene

- Spam filters
- Malware filters
- Email Fingerprinting
- Email Access Policies
- Blacklisting

Modern Hygiene

- 2 Factor Authentication
- E-Mail Encryption (Pretty Good Privacy)
- Suspicious email tracing
- Behaviour fingerprinting
- Avoid opening links on Mobile devices
- Whitelisting

KRATIKAL
SECURE FOR SURE

Desktop Data Security

Threats

- Data theft
- Data loss
- Device Damage
- Insider Threats
- Corporate Espionage
- Naïve Employees
- 3rd Party Applications
- Cloud Storage
- Malware
- **Ransomware**

Case Study

1. Food delivery start-up Data breach
2. Telecommunication data breach

Traditional Hygiene

- Antimalware Solutions
- Usage Instructions and SOPs
- Access Controls
- Data Backups and Encryption Policies

Modern Hygiene

- Advanced threat detection engines
- Vulnerability Management
- N-factor authentication
- Compliances and Risk Assessment
- **Employee Risk Assessment**
- Regular Identity Re-Certification

KRATIKAL
SECURE FOR SURE

Case in point -> Different Approach to Data Security

zomato

2 months ago

Security Notice

[Update] 60% of our users use third party OAuth services (i.e. Google and Facebook) for logging in to Zomato. We don't have any passwords for these accounts - therefore, these users are at **zero** risk - both within Zomato, as well as on Google and Facebook (and any other services where the same Google/Facebook ID is being used to log in). For all our other users, as a safety measure, we strongly advise changing your passwords on other services where you might have used the same password as Zomato - we are also sending emails to such users prompting them to do the same as we speak.

—

Over 100 million users visit Zomato every month. What binds all of these varied individuals is the desire to enjoy the best a city has to offer, in terms of food. When Zomato users trust us with their personal information, they naturally expect the information to be safeguarded. And that's something we do diligently, without fail. We take cyber security very seriously - if you've been a regular at Zomato for years, you'd agree.

Zero day confirmation

The Indian EXPRESS

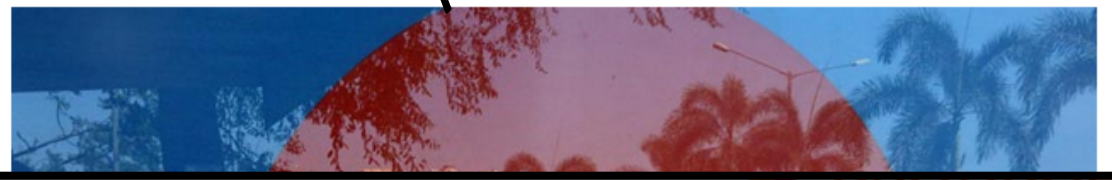
Reliance Jio Data Breach: Accused used own debit card to make payment for web space, say police

He also used his own computer to set up the website, based on which he was eventually arrested. As per cyber cell officers, cyber criminals normally pay via bitcoins and use proxy servers in similar cases of security breach, to remain below the radar.

3 SHARES

Facebook Twitter Google Plus

Written by **Mohamed Thaver** | Mumbai | Published:July 14, 2017 1:50 am



7 days after confirmation

SECURE FOR SURE

Social Media Security

Threats

- Ease of information gathering
- Check-ins, Location tagging, likes, interests, Tweets and media share
- Publicity stunts
- Social Media apps

Hygiene

- Reduce social media fingerprint
- Avoid sharing information over Social Media
- Website, LinkedIn, Wikipedia and other social accounts can be juicy sources of information
- Avoid using unverified and untrusted apps
- Green Padlock: ***Is it secure ?***

KRATIKAL
SECURE FOR SURE

Mobile Device Security

Threats

- Over privileged Apps
- Digital Privacy
- Device Theft
- Hardcoded Apps
- Rogue Apps
- Backdoors

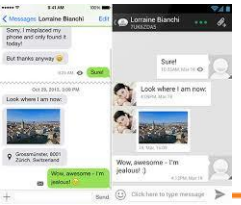
Hygiene

- Antivirus
- Device Administrators
- Data Backup
- Device Encryption
- Permission Management
- Uninstalling stale applications
- Scanning for hardcoded applications
- Cloud Backups: **Boon or Bane ?**

Case in point

1. Over 40 applications blacklisted by Intelligence Bureau

KRATIKAL
SECURE FOR SURE



Messaging Apps

Threats

- Hoaxes
- Social Engineering attempts
- Bullying
- Dissemination of Objectionable Content
- Dissemination of Malwares
- Circulation phishing links
- Problems of screen size

Modern Hygiene

- Intrinsic Antivirus
- **Awareness about Cyber Security**
- Deterrence via Law

Case in point

- Hoaxes

KRATIKAL
SECURE FOR SURE

Sample Hoax

KRATIKAL
SECURE FOR SURE

RBI to issue ₹2000 Rupees Notes coming February 2017

Not just a piece of paper There is much more in this note Read the full content of this message

India is all set to add one more denomination to its currencies shortly. The Reserve Bank of India (RBI) will be issuing Rs 2,000 currency notes, the highest to come into circulation, even as some experts feel7 high-value denominations should be discontinued to curb black money.

The Rs 2000 currency is designed keeping in mind to eradicate the black money issues using state of the art indigenous nano technology, every Rs. 2000 currency note is embedded with a **NGC (Nano GPS Chip)**

SECURE FOR SURE

People Security

Threats

- Social Engineering
- Weak Passwords
- Insecure browsing habits
- Human nature
- Respond to catchy messages, mails and calls
- Easy to trust
- Ransom (people in exchange of data)

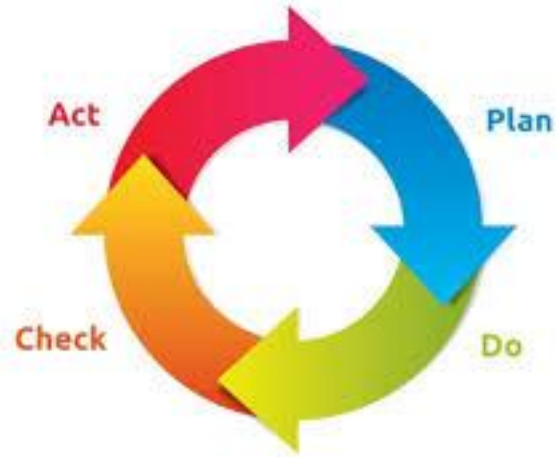
Modern Hygiene

- Cyber Insurance
- People Risk Assessment

Case in point

- One of the biggest accounting firms of the world were recently hacked due to negligence on the part of the employee

Net Net



- Data, Device and People continued to be Targets, Protect them
- Create cyber security culture
- Take good care employees during on-boarding, employment, exit and post exit
- Enable controls and have a rigor in follow through
- Security is a team work and responsibility of all
- Aware, Aware, Aware
- Implement whistle blower policies
- Use analytics to your advantage

There is no substitute for common sense

There is no Patch for human stupidity

Questions ??