CAFRAL WORKSHOP ON TRENDS IN CYBER ATTACKS, INCIDENCE RESPONSE & DIGITAL FORNSICS

September 4, 2017, Mumbai

TAKEAWAYS FROM CAFRAL WORKSHOP ON TRENDS IN CYBER ATTACKS, INCIDENCE RESPONSE & DIGITAL FORNSICS: September 28-29, 2017

Takeaways from session by Dr Sanjay Bahl, Director General, CERT-In

Objectives of Cyber Security

- The key objective of Cyber Security is the protection of information and its critical elements, including the systems and hardware that create, use, store, transmit and delete that information.
- There are four levels of security. Desktop, Transport, Network, Web applications. Antivirus for desktop, encryption for transport of data, firewall for illegal access and patching for perversion is required.
- Through the selection and application of appropriate safeguards, Cyber security helps the organization's mission by protecting its physical and financial resources, reputation, legal position, employees, and other tangible and intangible assets.
- It is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.
- **Tracks Description of cyber security**
    - Network Security: to protect networking components, connections, and contents from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure.
    - Application Security: to protect various applications or the underlying system (vulnerabilities) from external threats or flaws in the design, development, deployment, upgrade, or maintenance.
    - Data Protection and Privacy: to prevent unauthorized access to computers, databases and websites and protect data from corruption. It also includes protective digital privacy measures.
    - Identity and Access Management: to enable the right individuals to access the right resources at the right times for the right reasons by authentication and authorisation of identities and access.
    - Cyber Assurance / GRC: to develop and administer processes for Governance, Risk and Compliance
    - Digital Forensics: To collect analyse and report on digital data in a way that is legally admissible. It can be used in the detection and prevention of crime and in any dispute where evidence is stored digitally.
    - Incident Management: to manage information security incidents and identify, analyse, and correct hazards to prevent a future re-occurrence
    - BCP/DR: to develop and administer processes for creating systems of prevention and recovery to deal with potential threats to a company thus protecting the protecting an organization from the effects of significant negative events
    - End Point Security: to protect the corporate network when accessed via remote devices such as laptops or other wireless and mobile devices. Each device with a remote connecting to the network creates a potential entry point for security threats.
    - Security Operations: to monitor, assess and defend enterprise information systems (web sites, applications, databases, data centres and servers, networks, desktops, etc.)
    - Industrial Control Security: to secure control systems used in industrial production, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other smaller control system configurations such as programmable logic controllers (PLC) often found in the industrial sectors and critical infrastructure

The organisations and job roles in Cyber Security fall under the following categories:

- **User Organizations**: These organisations manages security of their infrastructure, applications and data. They often use InfoSec services & products to safeguard their Cyber security Assets. They could be from various other sectors like Banking, Healthcare, Telecom, Retail, IT-ITES, etc. e.g CapGemini, Tata TeleServices, HSBC, Apollo Healthcare, etc.
- **IT Services Organizations:** InfoSec services firms help user organizations manage the aspects of their information security program by consulting, developing, implementing, administering, monitoring, maintaining and troubleshooting for InfoSec solutions. e.g FIS, TCS, WIPRO, etc.
- **Consulting Organizations:** Consulting firms guide organizations in their strategies, initiatives and compliance with standards and regulatory requirements and also help them ensuring protection of their network and critical IT assets, and that their staff is fully equipped to address external and internal threats. e.g Pwc, KPMG, Deloitte etc.

Takeaways from session by Sidharth Vishwanath, Price Waterhouse Coopers

Changes in Cyber Security Strategy in the Context of recent Cyber Attacks:

The Banking ecosystem of the past was a closed one, with brick and mortar branch, with highly human interfaced banking where you knew your customers and cash intensive. As the digital channel in financial services continues to evolve, the threat surface has grown multi-fold. Thus, reforming the cyber security strategy is need of the hour. Between April to August 2017, the attacks seem to follow a trend for the banking sector: Malware (40%) , Account Hijacking (20%) & Data Breach (20%) have been the top 3 attacks faced by the banking sector. DNS Hijacking (6%), Domain squatting (7%) and RCE Vulnerability (7%) are other types of cyber attacks. (Source : Hackmageddon)

Re-Strategizing Security		
Custom Malware, Phishing, Account hijacking, Campaign Connections with Command and Control Systems, Ransomware , Data Breach	Require five pronged strategy	1.Redefine Crown Jewel protection program
		2. Managing Third-party connections
		3. Advanced Malware Detection Capabilities
		4. Advanced Cyber Testing
		5. Innovative awareness program

The new strategy for Cyber Security has to Redefine Crown Jewel protection program of the bank beyond just Data protection: It should include 1. Real Time monitoring of Mission Critical asset needs to be established 2. Ongoing review of hardening/ Correlating events with change requests Advanced Use Case – Correlating events with application and transaction alerts 3. Differentiated thresholds 4. Lower alert resolution timelines

Managing Third-party connections is important. It can be done by 1. Inventorying all network connections to understand the threat exposure 2. from each connection 3. Risk Assessment of all connections to ascertain the right mix of controls 4. for each connection 5. Logging andMonitoring for early identification of compromise enabling for quicker respond and recovery initiatives

Advanced Malware Detection Capabilities can be built by investing in advanced capabilities like 1. Endpoint Detection & Response 2. Honeypots and Sinkholes 3. Anti-APT with Sandboxing 4. Develop pattern recognition and anomaly detection capabilities 5. Invest in Security analytics in order to leverage long term correlation

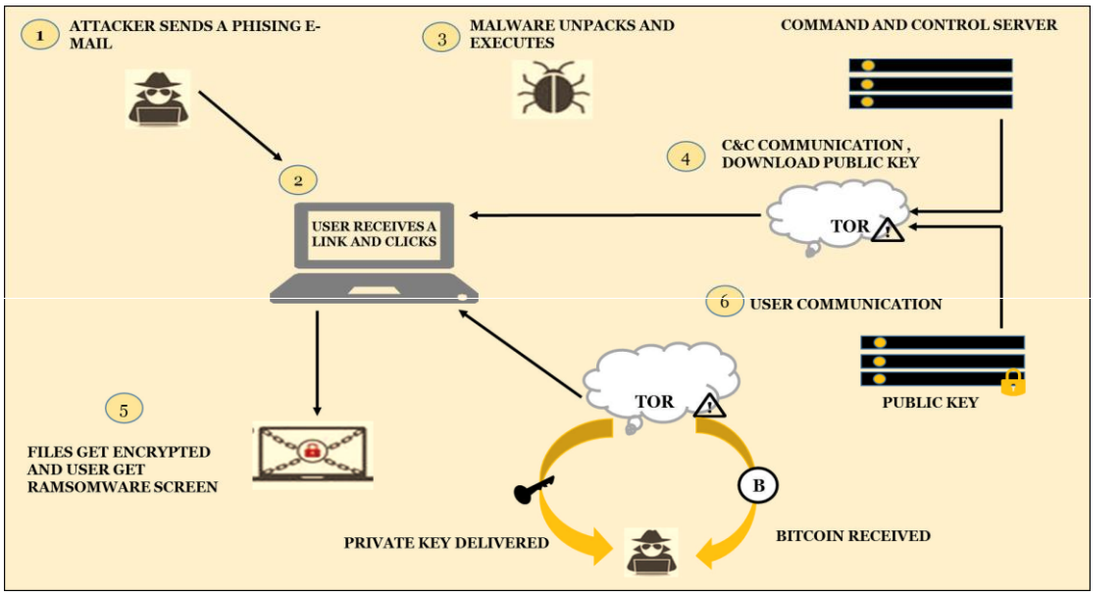
Advanced Cyber Testing can be done by 1. Red Team exercise to mimic real-life attacks 2. Move from point-in-time to continuous testing of defense 3. Multi-Vector attack scenarios to act as catalyst for evolving controls 4. Blue team to root cause and strengthen the defense

Innovative awareness program can be taken up by 1. Creating in-house advocacy group for championing awareness 2. Not limiting to classroom /presentation – use “show n tell” 3. Using

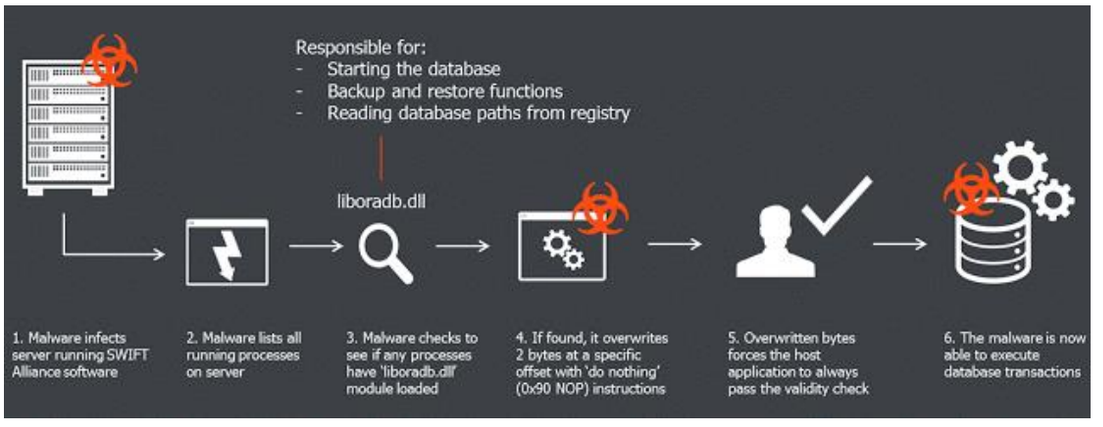
Gamification and Simulation to bridge awareness gaps

CASESTUDIES:

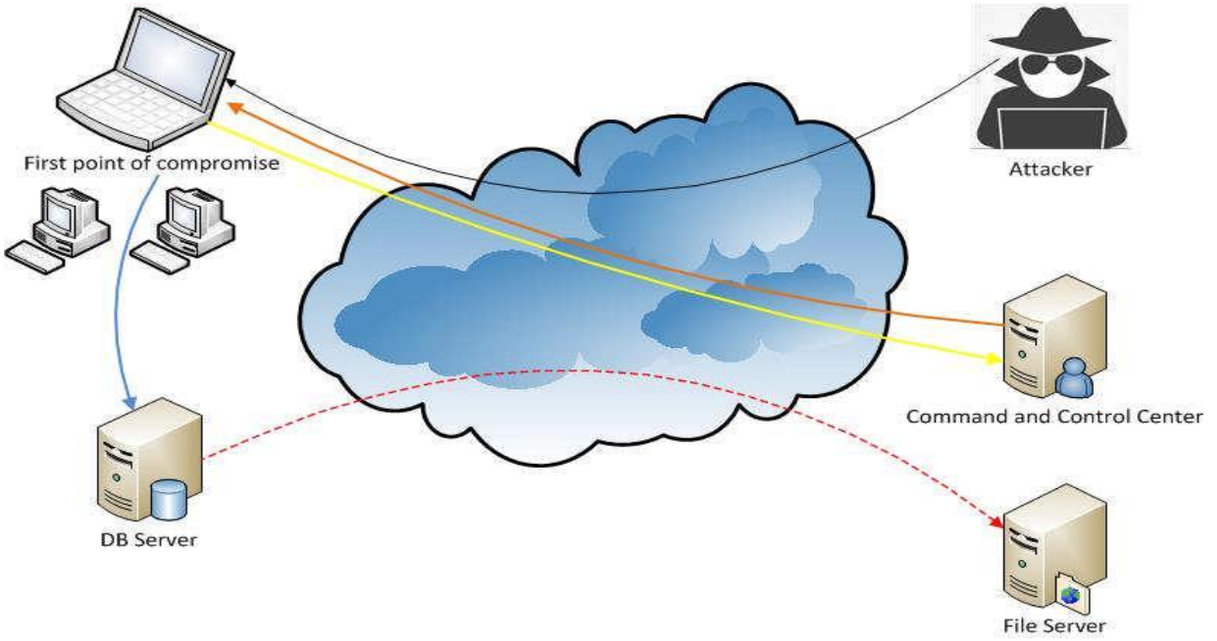
Case Study 1-A recent Ransomware attack: Characteristics and targets: 1. Phishing campaign leading to Malware injection 2. Cross industry exploiting similar vulnerability 3. Assets were required to be formatted



Case Study 2-A recent ransomeware attack: Characteristics and targets -1. Deep product knowledge, Custom Code and use of privilege ID 2. Designed for banking industry with specific target in mind 3. High value transactions



Case Study 3 – A recent Data Leakage incident: Characteristics and targets-1. End user identity compromise – successful malware injection 2. Lateral movement to reach Database 3. Exfiltration of data from database server



Case Study 4– A recent DNS Hijacking: A Characteristics and targets-1. All customer traffic rerouted to fake sites 2. Customer details are acquired by the hacker through the fake sites 3. Banks were unable to communicate to the employees through email Turn user traffic from Real Server to Fake Server

Takeaways from session by Sangram Ghyal, Price Waterhouse Coopers

Building Advanced Security Operations Centre (SOC)

Next Generations Security Operations Centre needs to change from being proactive to being predictive. Security imperatives have rapidly evolved over the years with changes in technology and business models. Evolution of Operational Risks and Types of Security Focus:

1995-Virus protection focused on ensuring that IT systems and devices performed as expected

2000-2003-IT and network security focused on the protection of the device and the information assets passing through the network

2003-2010-Cyber Security and assurance has taken a more comprehensive system, data and mission assurance role

2010 onwards-Rapid change in Technology adoption esp. cloud, IoT and mobile along with evolving threat and landscape

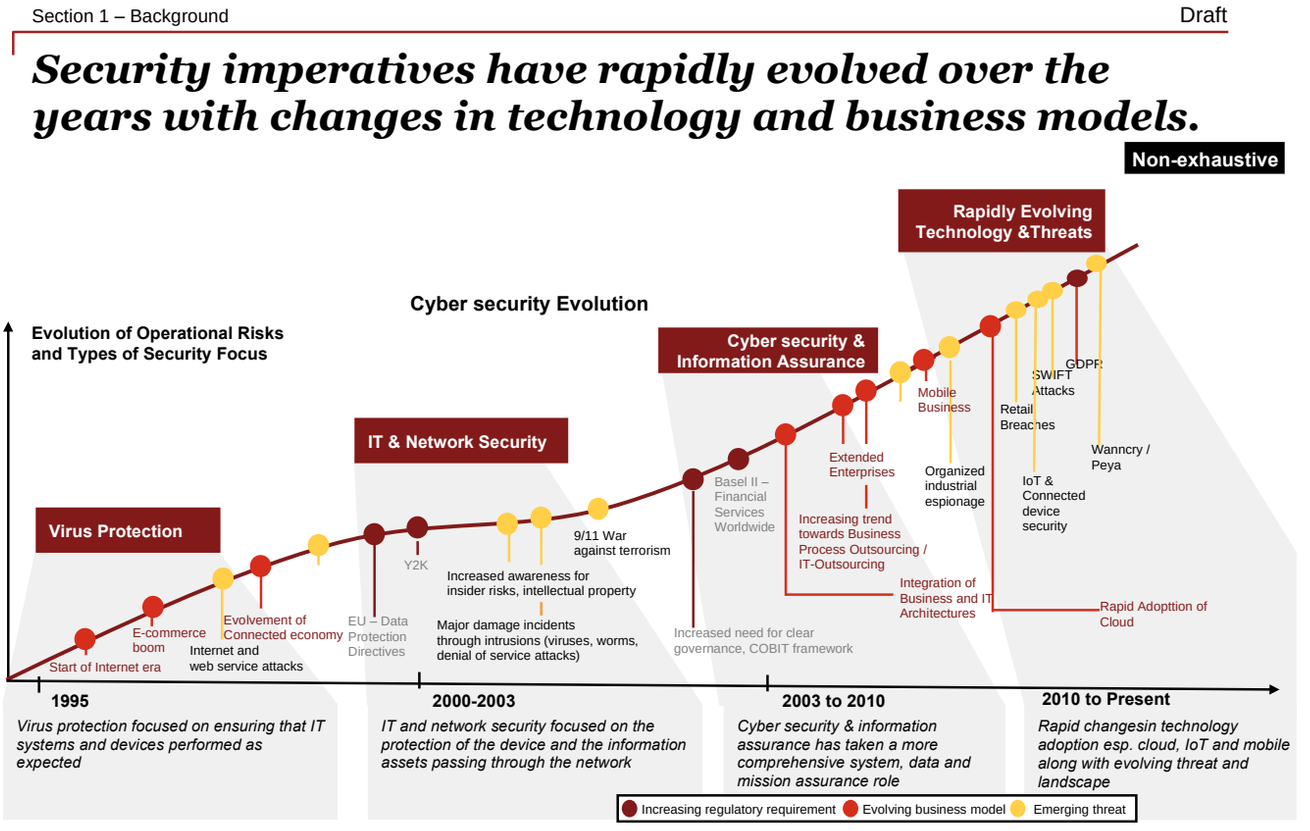


Diagram: Change in the nature of attacks

How has the nature of attacks changed?: Nature of attacks changed from Traditional Information Security involving the people, process, and technology measures to support information and systems confidentiality, integrity, and availability to Cyber Security involving assumed state of compromise. The term has evolved to take on new meaning and seriousness today given the characteristics of the threats and impact of compromise.

Characteristics of cyber security perpetrators have five characteristics:

Act on behalf of nation states: Many attacks originate from state-sponsored groups, acting in the name of patriotism and using information in place of traditional warfare weapons.

Use sophisticated and persistent methods of attack: Breach analysis shows criminals perform considerable reconnaissance and adopt both high and low tech tactics to achieve access into a network.

Target information for long-term strategic gain: Attackers are seeking valuable corporate intellectual property; terrorist activities against governments, and defacement of corporate brand/organizational reputation.

Are global and multi-national: Many of the largest attacks have come from Eastern Europe, China, Russia, and South America, with many groups having a multi-national component.

Are organised: Cybercrime syndicates ("hacktivists"), such as Anonymous, coordinate attacks through their thousands of members across the globe.

The question today is not 'Can I be breached?' but 'Can I detect and defend effectively?' Therefore, defending is not a passive activity. One needs to actively hunt, contextualize and respond to threats. Nature is full of anti-fragile systems. The human muscles are a good example of anti-fragile system. The more they are subjected to bouts of stress, the stronger they grow (quote from the book 'Antifragile by Nicholas Taleb'). SOC needs to codify the principles of 'antifragility' in cyber security Advanced SOC operating model. The right strategy is early discovery, rapid response and threat resistance-all on the

basis of data sharing. This calls for a Security Operations Centre model which is capability driven. From Traditional SOC with disconnected service capabilities and tightly coupled technology components (Logging & Monitoring, Security incident management, Threat/Vulnerability Management, compliance management) to **New Generation SOC with Integrated service capabilities and loosely coupled technology components** (with Incident response, Ivestigation, Attack surface management, Digital Brand Protection, Enginnering and operations and Cyber intelligence and hunt team services). Next Generation SOC is about orchestration of capabilities to deliver early detection, rapid response and threat resistance.

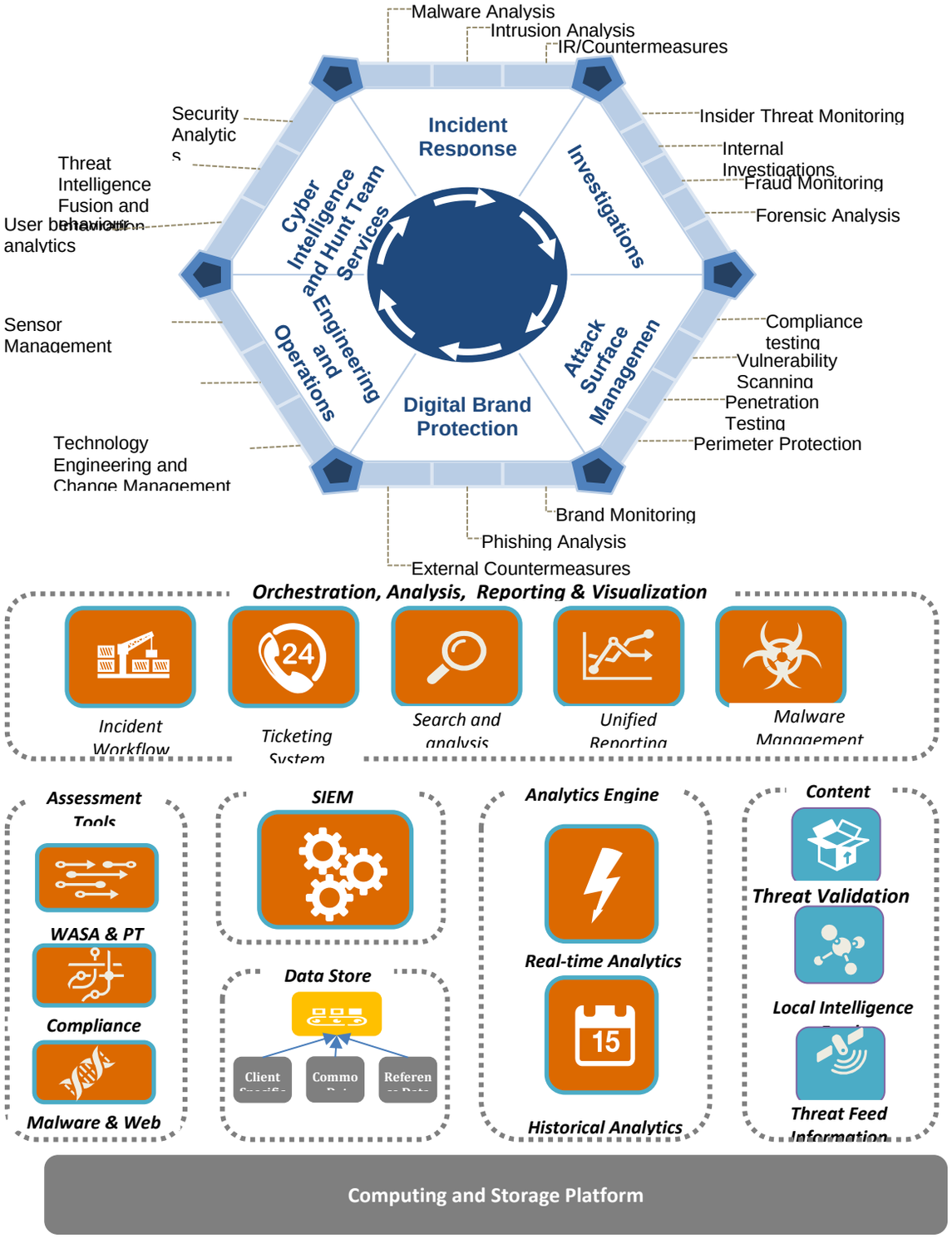


Diagram: Schematic of SOC build up on computing and storage platform.
Diagram of New Gen SOC (The Technology Schemeatic of new generation SOC)

Main Focus Areas for for threat intelligence in next Generation SOC are Threat intellingence, Anaytics and machine learning.

1) **Threat Intelligence- Where do you get the Threat Intelligence?:** Hash values, IP addresses and Domain names are easy targets fro the attackers where Indicators of Compromise provided by most OEM's and Anti-virus providers. A number of Open-source and Commercial Feeds are available.

System Artifacts, Tools and TTPs are pain points fro hackers for which Indicators of Compromise Have to be developed by Cyber Threat Intelligence team. System Artifacts Develop from known malware behaviour. TTPs and Tools are developed by analysing malware to understand variants, families, CnC domains and threat actors. Technical & Tactical Threat Intelligence is by Looking at the indicators. Well Written Yara Rule for protecting Files and Exact command channel structure for protecting Network.

2) **Analytics: Analytics is not about Data – Analytics is about knowing what to look for!**

1. Behavioural Analytics for Malware Detection using DNS Activity (DGA)
2. Statistical analysis for malware detection (C2 activity) through DNS Tunnelling (increased entropy method)
3. Statistical Analysis for malware detection (C2 activity) through Web proxy analysis (increased entropy method)
4. Unusual network activity – statistical analysis of net flow information
5. Detection of C2 connections through Threat Intelligence fusion with outbound connections and DNS queries
6. Data Leakage / Network activity analysis based on geo-spatial distribution

3) **Machine Learning:** What is Machine Learning? Traditional programming is where Computer is fed with data and program to give output. But Machine Learning, we feed data and output to get a program!

The two most useful use cases of Machine Learning in Security are

1) User and Entity Behaviour Analytics –

Connections

- Logon / log off
- Application usage
- Data usage
- Time / Space distribution

2) Network Behaviour Analytics

- Protocol profiling
- Ports and frequency
- Packet sizes and entropyy
- Beaconing and signalling

Adversarial Machine Learning is the new way to fight and threat intelligence tool.

Takeaways from session by Ravi Kumar, Chief General Manager, CSITE, Department of Banking Supervision, Reserve Bank of India

Takeaways: from presentation by Department of Banking Supervision Reserve Bank of India on Cyber Security Framework -
Implementation in Banks & Regulatory Observations on Cyber Risk and Customer Protection
Cyber Security Framework in Banks -June 2, 2016 -Expectation from Banks - **Comprehensive assessment & securing the banks' IT systems from cyber threats**

Board approved Cyber-security Policy	**Cyber Crisis Management Plan to strengthen Incident Handling and Response**
Continuous Surveillance -Emphasis on setting up of SOCs	**Cyber Security Preparedness Indicators**
Conducive IT architecture	**Reporting to RBI**
Comprehensive Network and Database security	**Organisational Arrangements**
Protection of Customer Information	**Cyber-security Awareness**

Inter-disciplinary Standing Committee on Cyber Security is established on February 28, 2017 pursuant to Monetary Policy announcement on February 8, 2017. Its mandate is as under;
It will be headed by Executive Director overseeing Banking Supervision with inter-departmental heads; External members include CERT-In, experts from Academia, industry and CEO of RBI's IT subsidiary

•**Terms of Reference:**
•Review the threats inherent in the existing/emerging technology
•Study adoption of various security standards/protocols
•Interface with stakeholders
•Suggest appropriate policy intervention
•The Standing committee will operate through a framework of sub-groups on various domains. Three sub-groups constituted.

Major Systemic Cyber Security Concerns
•DMARC -Domain-based Message Authentication, Reporting & Conformance –for email authentication –Government and Financial Sector including all the regulators;
•ATM –Several issues –unsupported software; hardware issues; ATM management arrangements; physical security;
•Security Operations Centre –effectiveness –concentration in few vendors
•TELCO related –cloning of SIMs, re-issue of numbers; mobile hardware standardisation; Vishing;
•Aadhaar seeding –issues for banks
•Adoption of cloud infrastructure for seemingly non-critical applications
•Dependence on outsourced IT vendors –vendor risk management
•Increasing sophistication of attacks;

Major Cyber Security Concerns For Banks
•-Need for Directors / Top Management with knowledge on IT / Cyber Security aspects
•-Lack of cyber hygiene –anti virus, inventory, patch, port, password and configuration management
•-Lack of sensitivity on cyber incidents impacting customer confidence
•-HR issues –CISO / Non-specialisation/ lack of qualified and skilled resources
•-Budgetary constraints
•-On going monitoring / reconciliation / application testing before roll out / multiple vendors
•-Difficulty in procurement –CVC requirements / Dependence on consultants for RFP etc.
•-Some banks have concern on VAPT carried out by private players;
•Risk Management not having a handle on cyber risk and underestimating the risk.

Way forward
•RBI continuously strengthening the monitoring / supervision of banks
•Assessment of banks and communication of concerns;
•Scope to be expanded to other regulated entities
•Strengthening RBI engagement with other Regulators for best practices
•Continue coordination with various Government Agencies proactively –WG on Fin-CERT –recommendations finalised –report submitted; Digital Security Committee – RBI a member –work in progress;
•Continuing engagement with CERT-IN, Fin-CERT as and when established; Setting up of a Sectoral CERT;

•-Need for all the stakeholders to remain vigilant and alert about threat landscape and impact; situational awareness; address HR side of the issue;
•-Round the clock surveillance of banks' systems –at different time slots;
•-Skill and awareness building –Concerted efforts needed at national level with Government's support
•-Need for a robust Data Security Standard
•-Need for articulating Secure Coding Practices / improving application security
•-Need for bringing in specialisation in IT / Cyber Security areas at all levels
•-Collective action by banks could help (SOC, Threat Intelligence etc.)

International Developments
•Standard Setting Bodies concerned –various initiatives
•IMF Working Paper WP/17/185 on Cyber Risk, Market Failures, and Financial Stability –2017
•IOSCO –CPMI paper on Cyber Security
•G-7 declaration on Cyber Security
•FSB –conducting surveys and working on standards
•CBEST of BoE, CFI of HKMA, …
•NIST, ISO 27001, Critical Security Control for Cyber Defense, OWASP, Finconet(Canada), …

CSITE Cell of DBS RBI Our Experience of IT Examination…**Most of the banks do not seem to have robust systems and controls that would meet regulatory expectations –**
Incidents of wallet, SWIFT, misuse of cards, Ransomware, DDoS, etc.

Challenges in IT Governance of banks –
Absence of directors with expected knowledge of IT, lack of broader vision for a secure IT architecture, routine submission of status reports with very limited directions, review of policies not keeping pace with the developments.

CISO needs empowerment –
CISO function needs to be strengthened, be it in staffing or in having due say over security matters. Inappropriate reporting lines of CISO, not in alignment with the principle of second line of defense

Staff with necessary IT skills is a major issue
Availability of skilled staff is not adequate
No succession planning in many banks
Dependency on a few staff
Technology compliance framework meeting security standards not noted
Use of Legacy & Unsupported Systems/Applications -
Issues in integration with the latest applications , security weaknesses and service efficiency

No proactive action from banks regarding systems which are past/approaching End of Life

Perimeter security needs strengthening –
Ports are kept open with limited monitoring
Internal links also exposed

Poor oversight over the outsourced activities –
Assessment delayed / perfunctory
Prompt Corrective steps not monitored
Application of patches & Configuration -
System/Application Patches and updationsof anti-virus/anti-malware solutions were neither comprehensive nor timely.
Vendor staff had unbridled access for configuration and administration of systems, network equipment, etc.
Banks did not have data leakage prevention policies & procedures for the laptops/mobile devices issued to their staff.
Security Operations Centre –
SOC was either not yet established by some banks or outsourced elsewhere with only limited monitoring by their personnel.
Inadequate monitoring of logs of operations, traffic and transactions by SIEM
Dearth of security analysts to make meaningful analysis
Consortium of banks may explore the possibility to jointly establish SOCs to address the issue

Application bugs; Reconciliation issues
Selection of vendors, testing of s/w; business taking precedence
Reconciliation of transactions delayed/not done
Many banks did not have Risk Based Transaction Monitoring systems
Lack of situational awareness : The vital need for threat intelligence should be recognized and acted upon. The amount of awareness that the cyber criminals have is phenomenal. Subscription to national/international threat intelligence feeds is essential; SOC alerts; CISO Forum
Incident Response: Delayed/deficient response, investigation; unpreparedness of outsourced service providers. Hypothetical scenarios to be devised for all the critical systems at the minimum and playbooks are developed appropriately. To participate in/conduct cyber drills
Appropriate communication strategy: Coherent, responsible communication by the industry as a whole is necessary particularly when a security incident or perceived risks can have wider ramifications like risk of losing public confidence.
Timely reporting of cyber security incidents: Reporting to IBCART has not been satisfactory. Reserve Bank has instructed banks to report within 2-6 hours of unusual cyber security incidents. Laxity noted
Preventing execution of un-authorized software: Whitelisting/blacklisting of applications in end-point devices was not implemented.
Network, Mobile Management and Security: Automated network discovery and management, WIPS, MDM solution was not implemented.
Secure Configuration: Regular review of Secure Configuration Documents (SCDs) was not observed. In a few banks SCDs were not present for Database, End-point OS.
Application Security Lifecycle: OWASP guidelines/other global standard security practices was not followed
User Access Control Management: Privileged Identity Management (PIM) Solution to monitor access to critical servers was not being implemented.
Advanced Real-time Threat defence and Management: Anti-APT solution was not implemented to prevent zero-day attacks. Deep scan of network packets was not ensured. Regular review of websites access provided through proxy was not done.

Reasons for Cyber Incidents include •**Anti-virus solution not updated** •Weak administrative passwords configured on servers, applications and database. •Internet Access on critical servers •Patches not updated •Spoofing attack •Fund Transfer based on email advise •**Microsoft Patch-Wannacry (MS17-010)** •**Weak vendor oversight –remote access to vendor not monitored, vendor activities not audited** •**Lack of validations –wallet to payment gateway** •**Inadequate testing (UAT) –UPI (transaction status, error code)** •**Webserver compromise –poor coding practices** •USBs enabled
Recommended Practices Inventory Management of Business IT Assets Preventing execution of un-authorized software Network Management and Security Secure Configuration Application Security Lifecycle Patch/ Vulnerability & Change Management User Access Control Management Secure Mail and Messaging System Vendor Risk Management
Cyber Incidents…which have occurred in recent times in Indian banks SLA Breach by Vendor: The prepaid card vendor had done some database alterations to increase the balance in prepaid cards Phishing Attack Rogue Mobile Application: A mobile application (.apkfile), similar to bank's mobile application was found on some website. UPI APP: without debit to certain customer accounts which were not having sufficient balances, beneficiary were found to be erroneously credited DDOS: A UDP flooding at magnitude of 30.15 Gbps was observed by the bank Malware: ATM switch of a service provider was affected by a malware compromising details of cards processed through the switch Ransomware: "Wannacry" & "Petya" -PCs got shutdown and after restarting, message demanding Ransom to decrypt the files of the systems was shown which were encrypted to some unknown format. SWIFT: PCs in Treasury Zone got compromised by malware through which fraudulent SWIFT transaction were initiated

Takeaways from Mobile Device Management Challenges and Drivers: K K Mookhey, Network Intelligence

Mobile forensics will continue to become more important in almost all investigations.

With the addition of innovation devices and other industry leading OS's, overall platforms and carriers has proliferated over the past few years, creating additional challenges for IT organizations. Bring Your Own Device (BYOD) is complex, expensive, and dangerous especially for Data Security. Increase in mobile and mobile Internet usage will increase security risks. If employees are using their own devices, legitimate questions include:

- How can IT protect the corporate data from corruption, misuse, or theft?
- How can efficient use of company-owned applications be supported on a device with non-standard configuration?
- How can the employee install a needed application even when their device uses a different operating system or operating system version?
- Who is responsible for taking care of his or her asset;

- How can the organization protect centrally located data if it can't ensure that a device is properly secured?

Key Drivers for Mobile Device Management are as under;

- ❖ Management of mixed platforms/devices
- ❖ Carrier Agnostic
- ❖ Protect Email
- ❖ Provisioning Device Protection
- ❖ Application Management
- ❖ Device Monitoring
- ❖ Policy Enforcement and Notification
- ❖ Usage Management
- ❖ Analysis and Reporting

Mobile Device Artifacts are as under;

- Browser
- GPS data
- Call records
- Contact list
- Email Gmail
- Cache
- Backup of the device (/sdcard)

Artifacts to location are a sunder;

- SMS and MMS location :
- SD Card data
- WhatsApp
- WeChat
- Line
- BBM
- Etc.
- Etc…

Risks occur in following areas:

Insecure apps, malicious apps
Bring-your-own-device at work
Value-added services
Apps that don't respect your privacy and security

Tools for Android Phones: Setup Pentesting Platform-Tools which can be used in Android phones for testing:

- Drozer
- Android Developer Tools
- dex2jar
- apktool
- JD-GUI
- Burp Suite
- Genymotion Emulator

One can install these individually by yourself or can download android application testing frameworks like AndroidTamer, Appie, Santoku-Linux .To individually install each tool, please go through the documentation of the respective tools on their websites.

Tools for iOS Application Security: iOS application security assessment and how to setup these tools and overview of these tools. An iOS application typically runs on an iPad, iPhone, or an iPod touch and is written in Objective-C programming language. The iOS app is stored in an .ipa file that is an iOS application archive file. Dedicated machine for Hackentosh can be built by using any iDevice-iPhone , IPod, IPad etc. or MacOS by installing MAC OS in virtual machine, tutorials are available on the internet. Software (Tools) include;

- Itunes.
- iPhone explorer
- iPhone config utility
- hex editor

- Burp Suite
- class dump-z.0.2
- Cycript
- Snoop-it
- And many more

Methodology for cyber investigation of iOS mobiles : The entire security testing of an iOS application can be divided into the following phases:

1. Static Analysis: static analysis is done by testing and evaluation the application by examining the code, configuration file, local storage and class dump of the application without executing the application.
2. Dynamic Analysis:
   In dynamic analysis testing we will evaluate of an application during runtime, by hooking application with interception with some dynamic tools Burpsuite Cyscript, Snoopit.

Care for mobile users for cyber security:

- Keep your phone's operating system updated
- Do not download apps from untrusted sources – only the official app stores
- Use a difficult-to-guess unlock code
- Keep your device physically secured
- Double-think before posting online and educate your family as well!

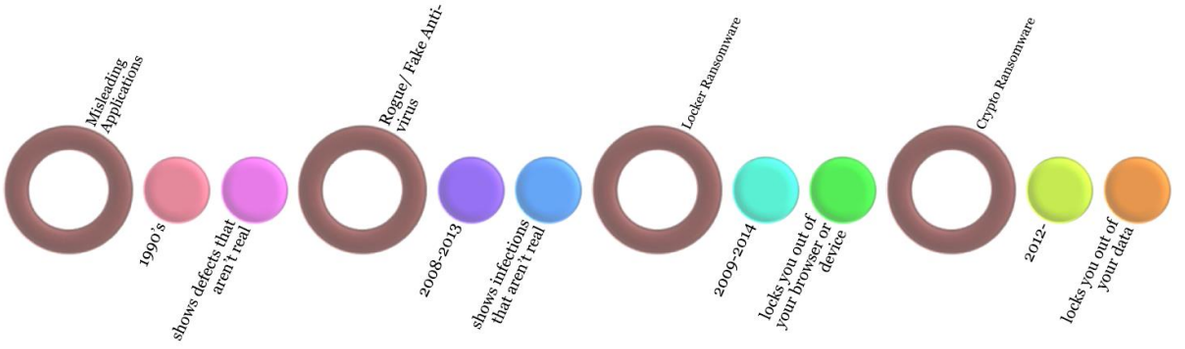
Takeaways from Strategies to mitigate and importance of digital forensic readiness: Krishna Sastry Pendyala, Executive Director, PwC

What is Ransomware?

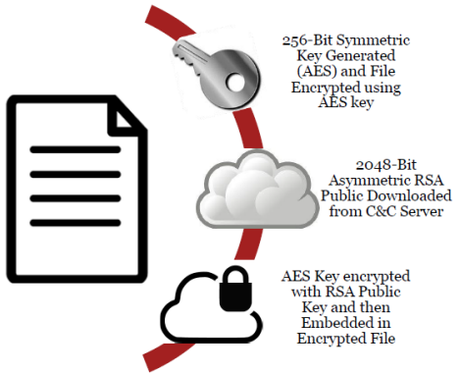
- Currently the biggest threat organizations are facing.
- Ransomware: malicious software
  - ✓ Revenue Generation Malware
    - ✓ For whom?

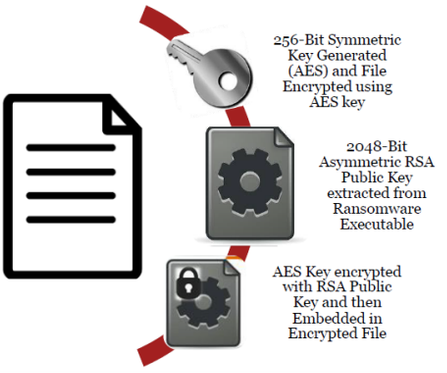
- Ransomware exploits vulnerable systems, applications and users
- Executable's delivered via:
  - ✓ Attachments or web links in phishing emails,
  - ✓ Malvertising on innocuous web pages,
  - ✓ Drive-by downloads (e.g. fake antivirus).
  - ✓ Arriving via a macro-enabled Word (*.docm*) or Excel file (*.xlsm*), ransomware can also be downloaded by link (*.lnk*), JavaScript (*.js*) or VB script (*.vbs*) files.

Evolution of Ransomware



Asymmetric Cryptography

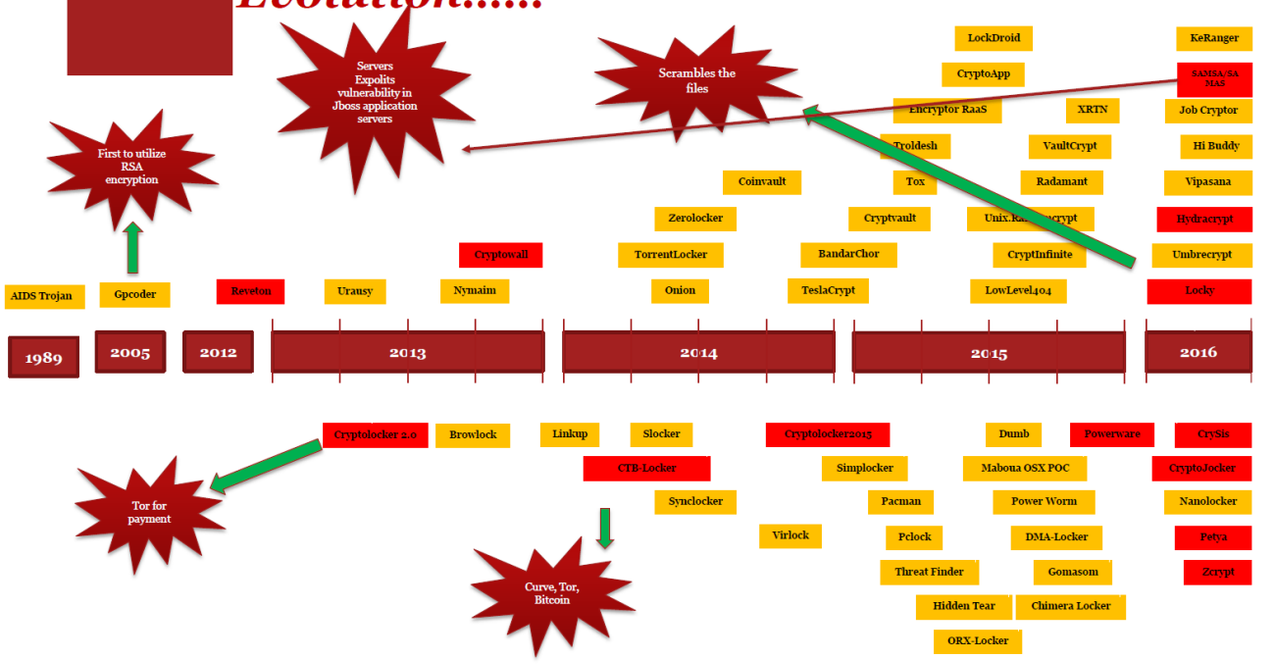




Ransomware has to download a Public Key before encryption begins from Command & Control Server: : CryptoDefense

Ransomware can begin encrypting without contacting a server first as it already has a Public Key embedded in the executable: CTBLocker

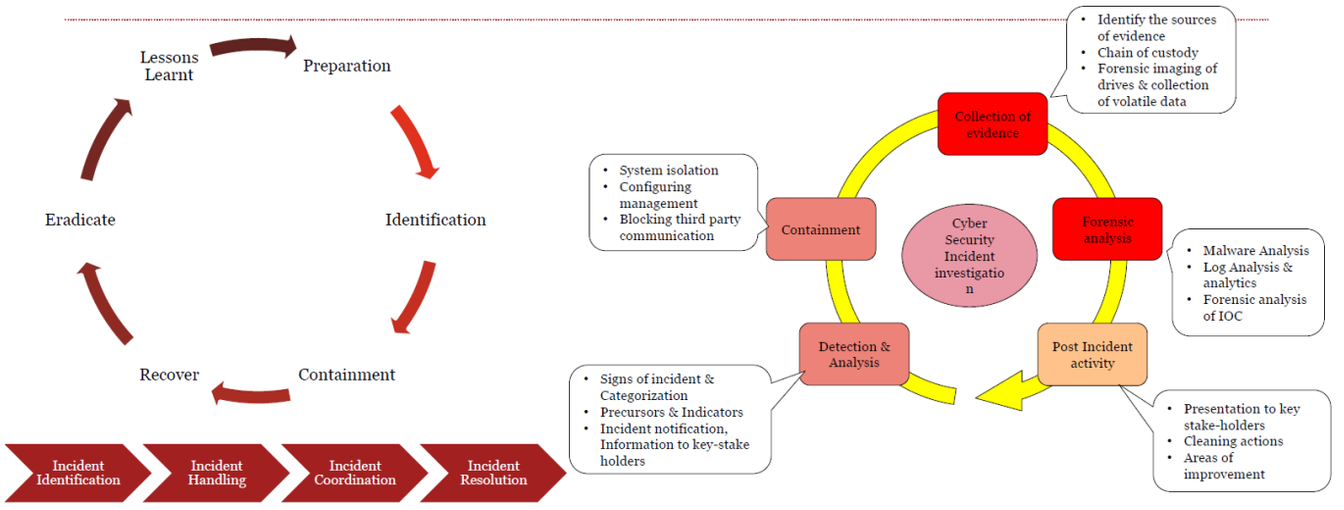
Evolution.....



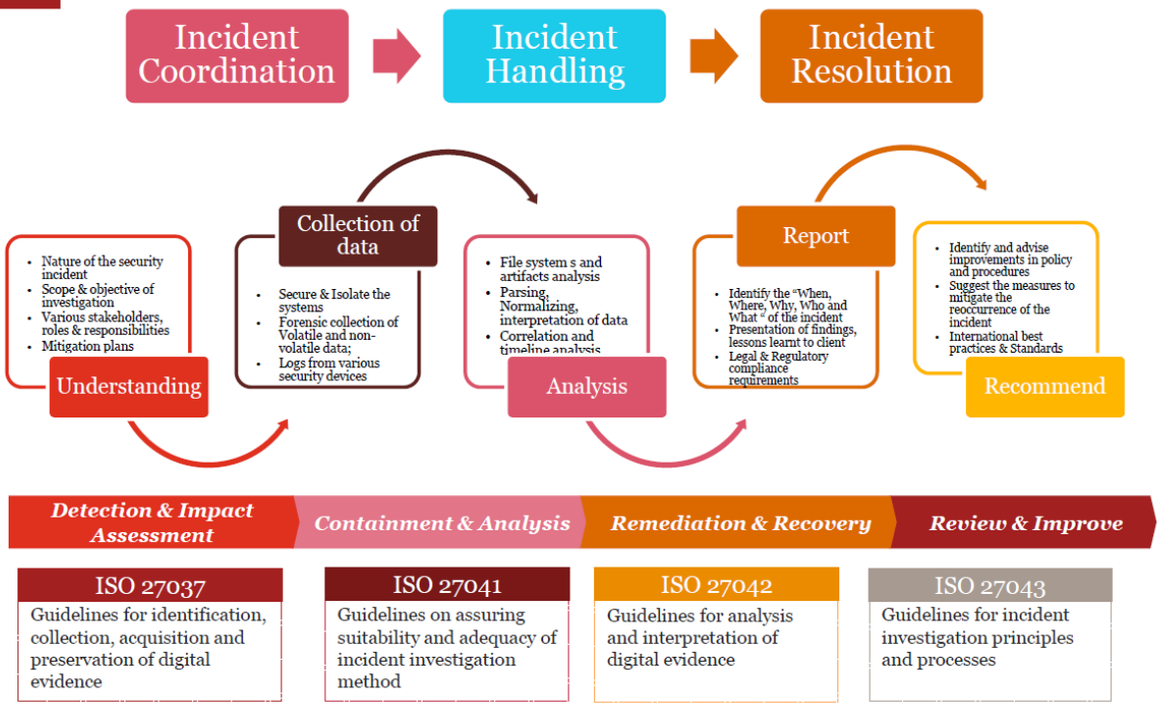
Ransomware infection with Advanced Persistence Threat (APT)

1. Start with automatic reconnaissance
   - ✓ JexBoss + J Boss remote shell installed + Nmap
2. Gain access to credentials
   - ✓ 'M64.exe' application, a recompiled version of Mimikatz
3. Use credentials for back door entry
   - ✓ ABPTTS.jsp' created a HTTP based tunnel into the network
4. Install Ransomware
   - ✓ Scanned the network for RDP open ports, Used 'psexec' command to execute the Ransomware (Carnavio2.exe)
5. Execute Remotely
   - ✓ Used 'psexec' command to execute 'vssadmin' to delete the volume shadow copies
   - ✓ Deleted publickeyxml files
6. Erase the tracks & Demanded Ransom

Incident Response Management – crucial Part of Crisis Management



Approach



We are infected…what to do?

- Disconnect the infected system(s) from network.
- Keep at least one system in switch–on mode.
- Collect the RAM Dump & Image the drive (FTK Imager free)
- Conduct the timeline analysis of files.
- Analyze the registry, Identify the batch/Exe etc.,
- Preserve the Logs – AV, Firewall, Proxy
- Use public sources: Identify the strain/variant of Ransomware
  - To identify the type of Ransomware infected, the IR team can use a free online service called ID Ransomware which can detect up to 54 infections, available at http://www.thewindowsclub.com/id-identify-ransomware.
  - If you are able to identify the ransomware, check if a ransomware decrypt tool is available for your type of ransomware. The list of ransomware decryptor tools are available at http://www.thewindowsclub.com/list-ransomware-decryptor-tools.
- Evaluate your responses
  - Restore from back-up, Volume shadow copies.

How to minimize the Impact of Ransomware attack

- Change your cyber security strategy
  - **"Prevent, Respond, Detect" to "Detect, Respond, Prevent"**
    - Detect, Prevent, Recover
- Validate/ Review back-up process
  - **Recent back-up offsite… "Air-gapped"**
- Review network permissions and End-user, Administrator user privileges
  - **Principle of least privilege to minimize the impact**
  - **Disable RDP**
- Develop Incident Response Plan - Ransomware specific
  - Develop good Communication plan, Checklists, SoP's
    - Table-top exercise, Cyber Drills
- End-user awareness

How to prevent Ransomware attack

- Controls at
  - Distribution Phase, Infection Phase, Communication Phase, Encryption Phase
- Validate/ Review Patch management process
  - OS/ Application patches
- Disable Macros using AD group policy
  - Office 2016 –Administrator can block Macros
- Monitor inbound traffic/ Spam filter/ Malware protection
  - End-point Protection, Whitelisting of applications…

Tech solutions…..not limited to..

- Use web-gateway/URL filtering (block access to C&C servers)
- Deploy antivirus protection
- Use HTTPS filtering
- Block spam and filtering
- Use a sandboxing solution
- Block risky file extensions (javascript, vbscript, chm etc…)
- Password protect archive files
- Use HIPS (host intrusion prevention service) & other signature-less technologies

Should I pay Ransom…

Lost resort…

- When everything fails…VSS, Backup, (Forensic) Recovery….

Is it Legal to purchase Bitcoins?

- Yes…

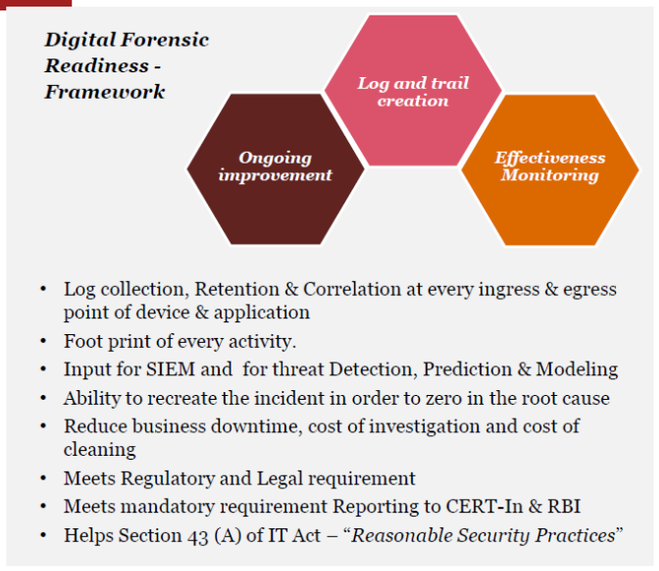
Payment of Ransom

- Illegal

Can I file a compliant ….

Harassment, memo's…..

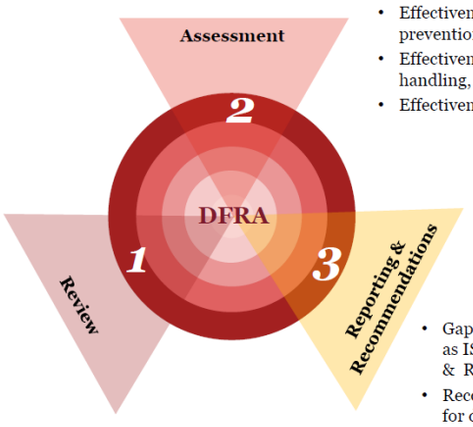
Digital Forensic Readiness Assessment



- Log collection, Retention & Correlation at every ingress & egress point of device & application
- Foot print of every activity.
- Input for SIEM and for threat Detection, Prediction & Modeling
- Ability to recreate the incident in order to zero in the root cause
- Reduce business downtime, cost of investigation and cost of cleaning
- Meets Regulatory and Legal requirement
- Meets mandatory requirement Reporting to CERT-In & RBI
- Helps Section 43 (A) of IT Act – "*Reasonable Security Practices*"

Digital Forensic Readiness Assessment -Approach

- Existing Forensic readiness Policies, Framework, Governance;
- Existing log collection & retention policies of critical business applications, Firewall, IPS, router, load balancer, SIEM tools etc.
- Cyber Security Incident Response policy & framework
- Legal & regulatory compliance requirements



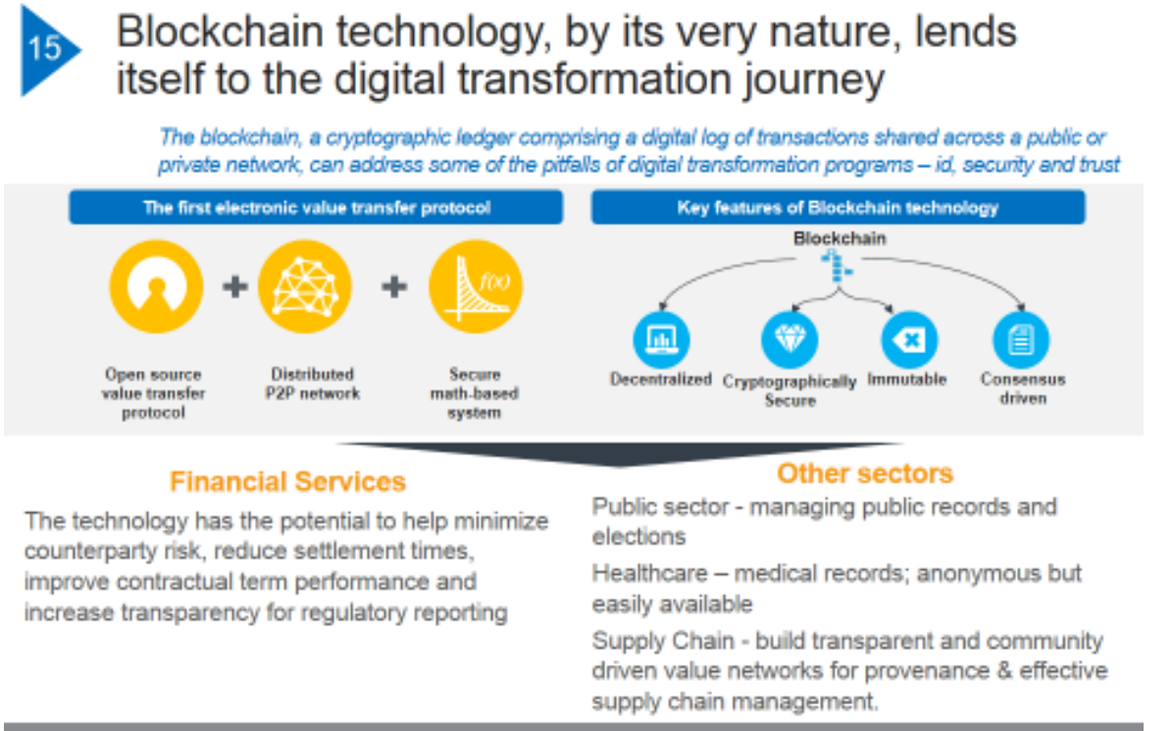
- Effectiveness of log collection & retention in tracing & tracking the security incident;
- Effectiveness of log monitoring & analysis
- Effectiveness of existing controls in detection, prevention of attacks;
- Effectiveness of incident response such as handling, coordination & resolution;
- Effectiveness of evidence preservation, collection

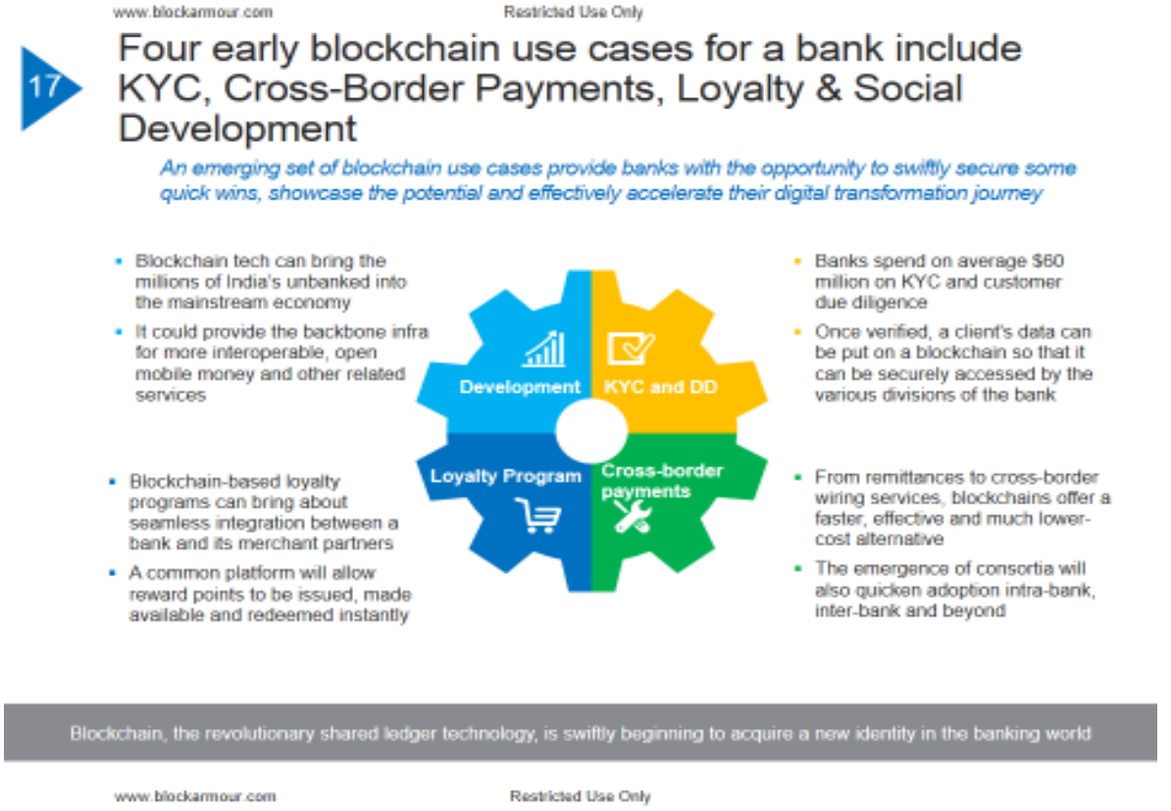
- Gap analysis for existing vs Standards such as ISO 27037, 27041,27042,27043 , 27001) & RBI/IRDA policies;
- Recommend framework, policy, procedures for digital Forensic readiness
- Recommend enhancements to existing process & technology to support forensic readiness

Takeaways from session on BLOCKCHAIN IN CYBER SECURITY by Narayan Neelakantan, Co-founder & CEO. Block Armour

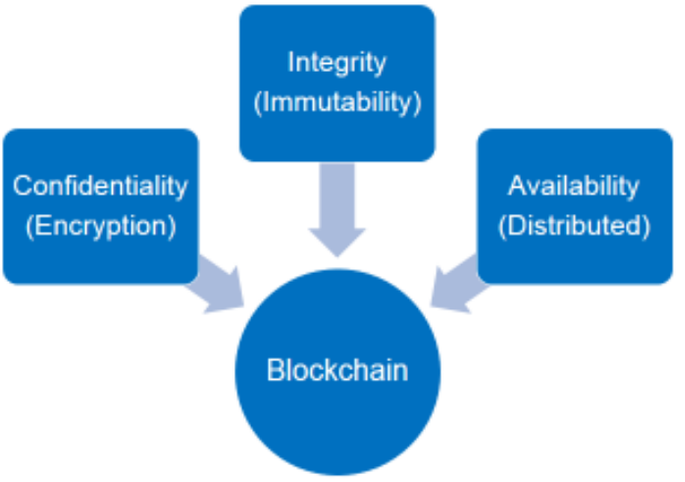
Defined Perimeter: Next-gen Security architecture which implements the Zero Trust Model BDP uses the blockchain-based digital signatures to authenticate humans, devices and data

BDP delivers a secure extended perimeter using private permissioned blockchain and TLS technology. Leveraging BDP, organizations can ring-fence critical systems securely providing access to authorized users and devices

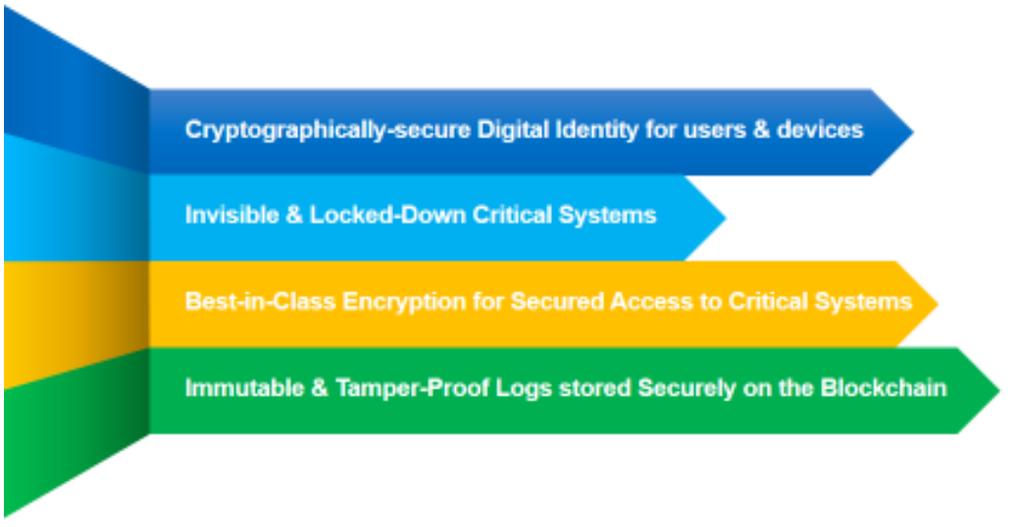




21 The inherent characteristics of blockchain can be used for building cyber-security use cases



27 The Result: Next-gen cyber security capabilities to protect critical systems against evolving cyber threats



Its time we reclaimed cybersecurity using emerging technology!

(Summary prepared by Ravi Sangvai: Program Director: CAFRAL)