Digital Forensic Readiness

Krishna Sastry Pendyala
Executive Director,
Incident Response & Digital Forensic Services

January, 2018

pwc

Agenda

1. Setting the Context
2. Case Studies
3. Lesson's Learnt?
4. What is Digital Forensic Readiness?
5. Scenario's & Benefits where Digital Forensic Readiness required?
6. Digital Forensic Readiness assessment - approach
7. Questions


Setting the Context

Few Statistics

USD 7.35 Million#
Average cost of Data Breach

191 Days#
Average time to detect data breach

50,76,479##
Average Record Stolen

66 days#
Average time to contain a data breach

USD 115 Million@
Anthem Data Breach Law suit

USD Multi Billion@@
50 state Class Action Law suite -Equifax

 # Ponemon Institute 2017 Cost of Data Breach Study

##Breach Level Index.com

@Fox Business.com

@@ csoonline.com

Few Cases…

Hack to cost Sony $35 million in IT repairs

Deutsche Bank to Pay $220 Million to U.S. States Over Libor

Bangladesh Bank drops $81m cybertheft investigation due to cost of probe

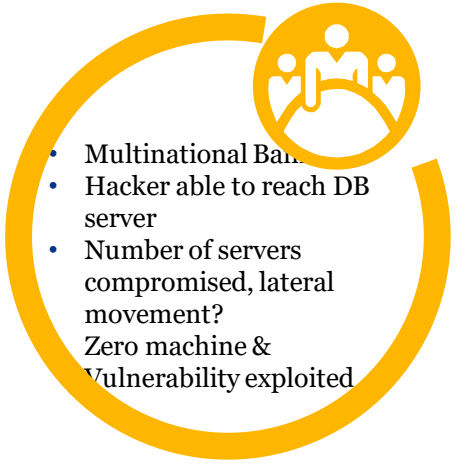
Epic Systems Case: US court halves fine on TCS to $420 million

Case Studies

Case Studies

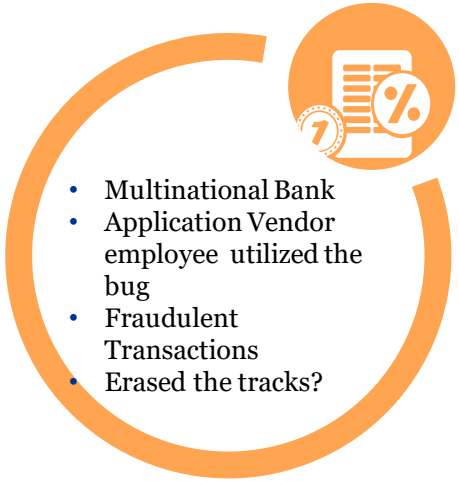
Forensic Investigation : When, Where, Who, What and Why

- Manufacturing Company
- WannaCry Ransomware Attack
- AV and Firewall Logs
- The Zero Machine
- Why anti-virus could not quarantine?



- Multinational Ba
- Hacker able to reach DB server
- Number of servers compromised, lateral movement?
  Zero machine & Vulnerability exploited

- Cyber Insurance Claim dispute
- Insurance company not willing to pay – Fraudulent Claim
- The extent of damage and source of attack.



- Multinational Bank
- Application Vendor employee utilized the bug
- Fraudulent Transactions
- Erased the tracks?

- Cost of investigation/cleaning?
- Source of attack?

- Firewall Logs – Configuration
- Allowed IP not logged, only denied
- Application Logs?

- Patch Management?
- AV updates
- Firewall logs

- Database logs?
- Application logs?
- Backdoor entry for the application

Lessons Learnt

What is missing?

- What logs each device, application etc., will generate?
- What type of logs are required to investigate a security incident?
- What type of logs are required to be captured for the type of attack?
- What type of logs are to be fed into SIEM for threat alert/modeling?
- What format they should be collected?
- How to preserve the logs (data)?
- How long they should be retained?
- What is the Legal & Regulatory requirements?

Which scenario is better?

- Mr. ABC returned to office after 25 days on 28th, June 2017 and found HDD missing from his Desktop computer System.
- Mr. ABC occupies cabin 3, in 5th floor of 7 storied building.

Scenario 1	Scenario 2
• Visitor pass only at ground floor. • CCTV cameras only in at the entrance. • Recordings maximum for 1 day. • The clock of camera and computer where recording stored not synchronized. • No policy, procedure for retaining the visitor book.	• Visitor pass at building entry and each floor. • Every room/ floor authentication mechanism with proper log maintained. • Monitoring of visitor movement. • A system in place to generate an alert. • 6 months logs are maintained with custodian and tampered proof

What is Digital Forensic Readiness?

Basics

Definition

- *Application of science for Legal Problems*
- *Admissible evidence - reliable*
- *Repeatable and reproducible*

Forensics

Definition

- *Information of any probative value…0,1 – Data, logs etc.,*
- *Section 79 (A) – IT Act – Electronic Evidence*
- *Highly Fragile - Tampered*

Digital Evidence

ISO 27037
Guidelines for identification, collection, acquisition and preservation of digital evidence

ISO 27041
Guidelines on assuring suitability and adequacy of incident investigation method

ISO 27042
Guidelines for analysis and interpretation of digital evidence

ISO 27043
Guidelines for incident investigation principles and processes

What is Digital Forensic Readiness?

Definition

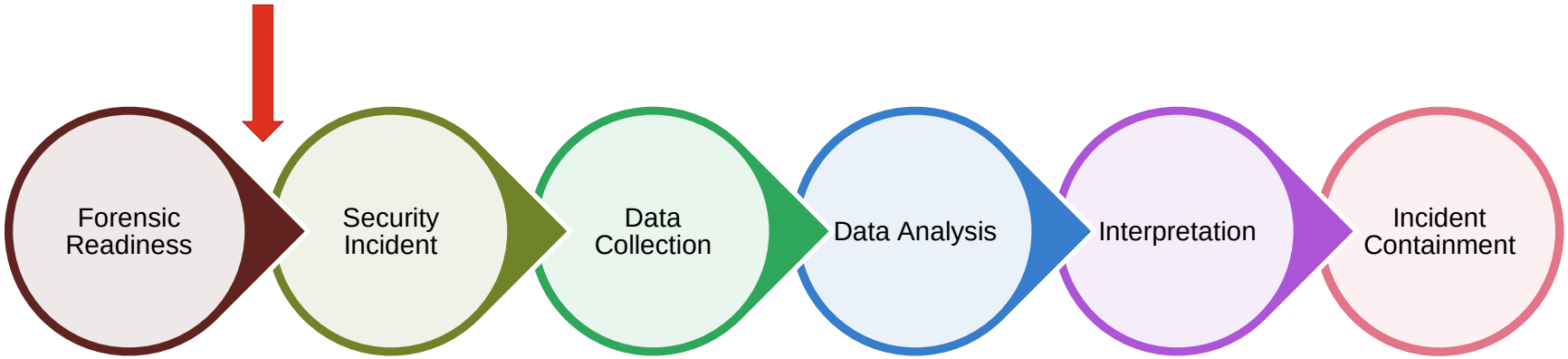
- *The achievement of an appropriate level of capability by an organization in order for it to be able to collect, preserve, protect and analyze digital evidence so that this evidence can be effectively used in any legal matters, in disciplinary matters, in an employment tribunal or court of law.*

Is it reactive?

Definition

- *the ability of an organization to maximize its potential to use digital evidence while minimizing the cost of an investigation.*

Proactive And Predictive



Scenario's where Digital Forensic Readiness Required?

Regulatory Compliance

- GK Recommendations
- Cyber Security Framework

Insurance claim

- Both insured & insurer
- Fraudulent claim or Genuine claim
- Extent of damage

Legal

- Reasonable Security Practices – 43 (A) of IT Act
- Civil/ Criminal Disputes

Threat detection & Monitoring

- To enhance SIEM capability
- Log correlation, Interpretation

Employee Misconduct

- Corporate Policy Violations
- Un-authorized access of systems and Fraud

Business Impact analysis

- Extent of damage
- Business downtime, extent of penetration, cost of cleaning etc.,

GK Comm. recommendation's

- Every application affecting critical/sensitive information, for e.g. impacting financial, customer, control, risk management, regulatory and statutory aspects, must provide for detailed audit trails/ logging capability with details like transaction id, date, time, originator id , authorizer id, actions undertaken by a given user id, etc. Other details like logging IP address of client machine, terminal identity or location also need to be available. Alerts regarding use of the same machine for both maker and checker transactions need to be considered. The logs/alerts/exception reports with regard to systems should be analyzed and any issues need to be remedied at the earliest.
- Critical application system logs/audit trails also need to be backed up as part of the application backup policy.
- A bank needs to have robust monitoring processes in place to identify events and unusual activity patterns that could impact on the security of IT assets. The strength of the monitoring controls needs to be proportionate to the criticality of an IT asset. Alerts would need to be investigated in a timely manner, with an appropriate response determined.
- Audit trails should be secured to ensure the integrity of the information captured, including the preservation of evidence. Retention of audit trails should be in line with business, regulatory and legal requirements.
- Good controls for remote access include logging remote access communications, analyzing them in a timely manner, and following up on anomalies. Logging and monitoring the date, time, user, user location, duration, and purpose for all remote access including all activities carried out through remote access.
- Establishing the capability to investigate information security incidents through various modes like forensics, evidence collection and preservation, log analysis, interviewing etc.
- Digital evidence is similar to any other form of legal proof - it needs to withstand challenges to its integrity, its handling must be carefully tracked and documented, and it must be suitably authenticated by concerned personnel as per legal requirements
- Conducting post-mortem analysis and reviews to identify causes of information security incidents, developing corrective actions and reassessing risk, and adjusting controls suitably to reduce the related risks in the future.

Benefits of Digital Forensic Readiness

- Reduces Business downtime
- Reduces cost of investigation
- Reduces cost of cleaning
- Reduced Regulatory & Legal liability
- Insurance Premium discount & litigations
- Helps in Effective & Efficient SIEM

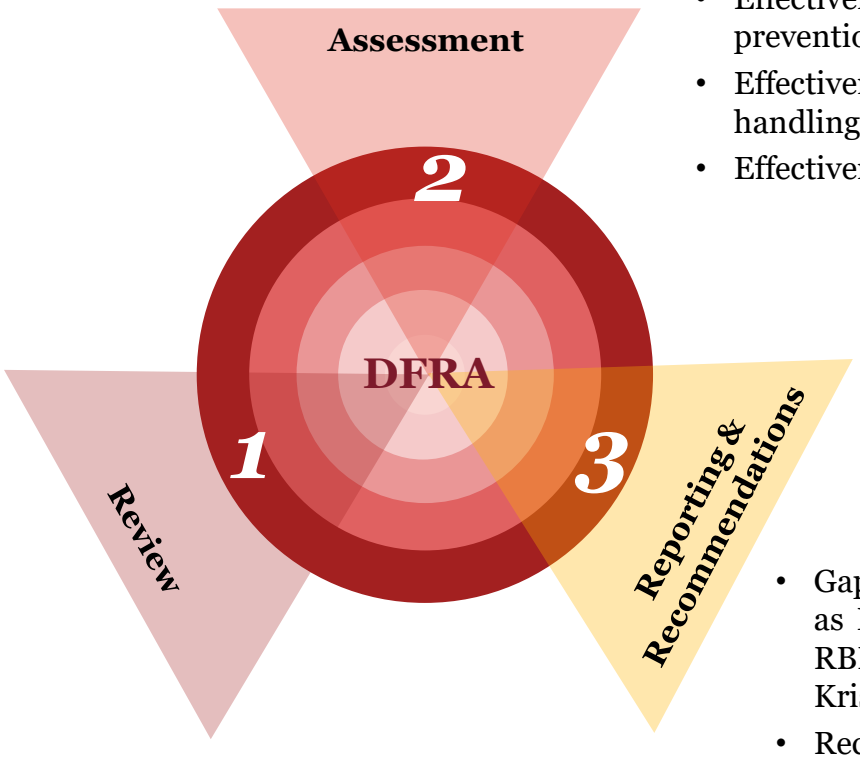
Digital Forensic Readiness Assessment - Approch

Are you ready - Digital Forensic Readiness checklist

- ✓ Identify the business scenarios and various threats both external and internals.
- ✓ Identify potential sources and types of data – devices, applications, data bases
- ✓ Map the sources of data with threat.
- ✓ Identify the collection and retention requirement – Legal, Regulatory compliance
- ✓ Test and improve the forensic preservation, collection and chain of custody capability
- ✓ Awareness of SoC and IR team forensic capability
- ✓ Document evidence-based cases, describing the incident and its impact.
- ✓ Ensure legal review to facilitate appropriate action in response to an incident
- ✓ Test the sufficiency at regular intervals.

Digital Forensic Readiness Assessment -Approach

- 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



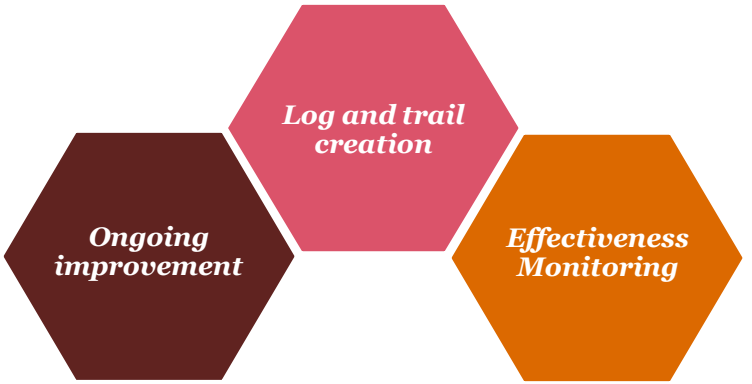
- Existing network architecture, applications, process owners, Governance;
- Type of threats external & internal for each application etc.,
- Existing log collection & retention policies of critical business applications, Firewall, IPS, router, load balancer, SIEM tools etc.
- Cyber Security Incident Response policy & framework
- Legal & regulatory compliance requirements

- Gap analysis for existing vs Standards such as ISO 27037, 27041,27042,27043 , 27001, RBI cyber security framework, Gopal Krishnan committee.
- Recommend framework, policy, procedures for digital Forensic readiness
- Recommend enhancements to existing process & technology to support forensic readiness


Closing thoughts

Closing Thoughts

- Digital Forensics – No longer Reactive - Proactive, Predictive
- Foot Printing of every activity – Log collection, retention, preservation at every ingress & egress point of device & application.
- Input for SIEM - for threat Detection, Prediction & Modelling
- 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.



Attack Type	Fields required for identifying the attack	Fields to be captured by the application
Injection	**Critical Fields:** URL received by Web server Query fired on the data base Parameters received by web server **Other Fields Expected to be Logged** **Webserver:** Public IP Address Date & Time Time zone Page or file requested Type of Request Bytes served Referrer Device finger printing details Http Response Code Appserver name or IP address to which the request is forwarded Session ID if the user is logged in **Database Audit log:** Event Date & Time User ID User privilege Thread ID Server ID Command Type	**Webserver Logs:** Public IP address Page or file requested Session ID Parameters received by webserver Device finger printing App server Name or IP address **Database Audit log:** Event Date & Time User ID User privilege Thread ID Server ID Command Type
Broken authentication & Session Management	**Critical Fields :** Session ID IP Address Login & Logout Time User ID Referrer	**Webserver Logs:** Public IP address Page or file requested Session ID Parameters received by webserver Device finger printing


Questions?

Krishna Sastry Pendyala

Executive Director, Cyber Security

Mobile: +91 94904 33296

Email: sastry.pendyala@pwc.com

Thank you