FORENSIC

Legal Informatics and Multimedia

Forensic Analysis for Computer Systems

Plan of the course:

1. Introduction
2. Evolution of Computer Forensics
3. Computer Forensics Process
4. Types of Computer Forensics
5. Forensics Readiness

Course 5: Forensics Readiness

5.1 Introduction

5.2 Goals of Forensic Readiness

5.3 Forensic Readiness Steps

5.4 Benefits of Forensic Readiness

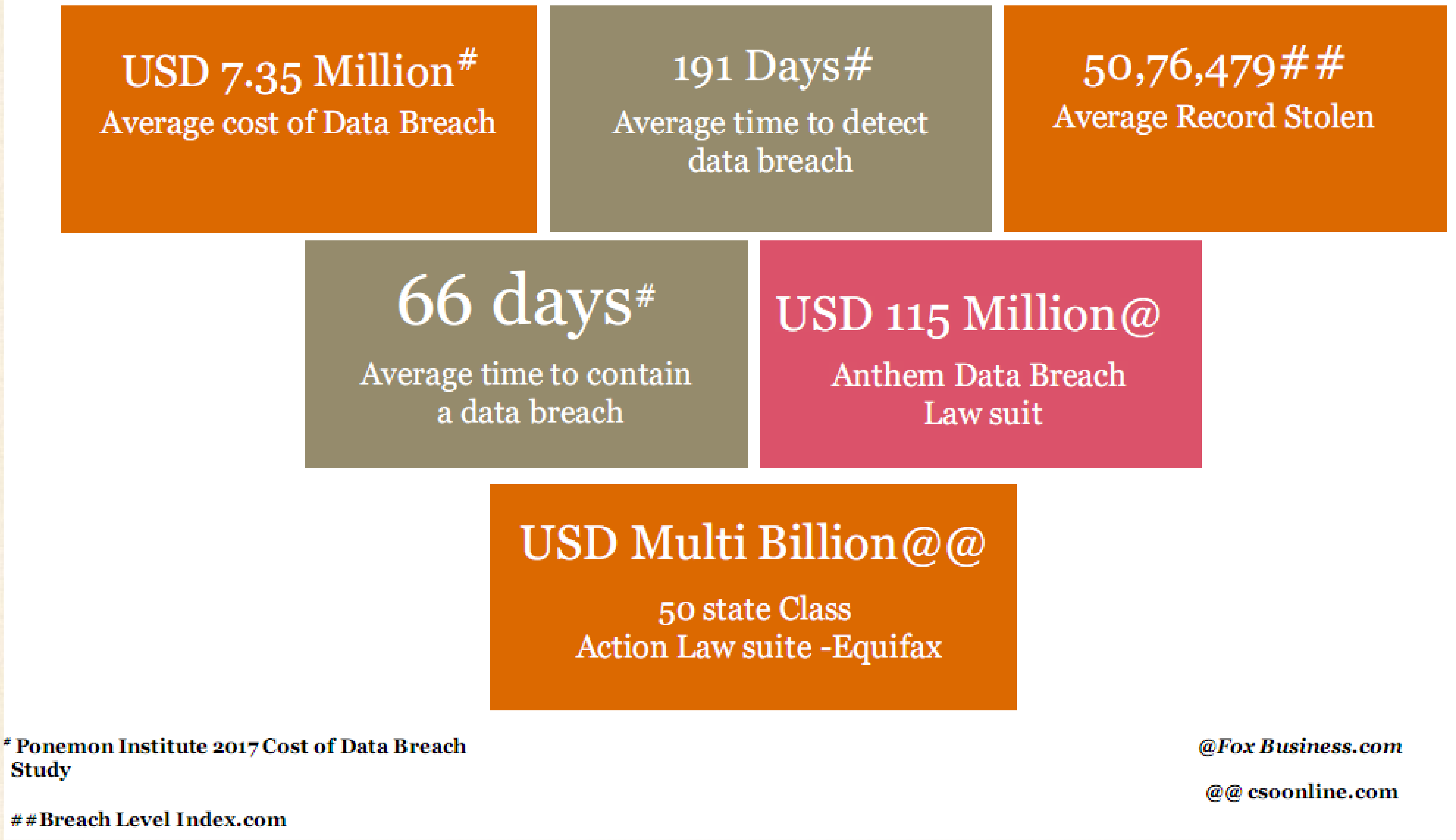
5.5 Forensic Readiness features

5.1 Introduction

Modern digital technologies not only present new opportunities to business organizations but also a different set of issues and challenges that need to be resolved.

With the rising threats of cybercrimes, many organizations, as well as law enforcement agencies globally, are now establishing proactive measures as a way to increase their ability to respond to security incidents as well as create a digital forensic ready environment.

5.1 Introduction



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

5.1 Introduction (cont)

Forensic readiness is the ability of an organization to maximize its potential to use digital evidence* whereas minimizing the costs of an investigation.

Forensic readiness as: “*The achievement of an appropriate level of capability by an organization in order for it to be able to collect, preserve, protect and analyse 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”*.

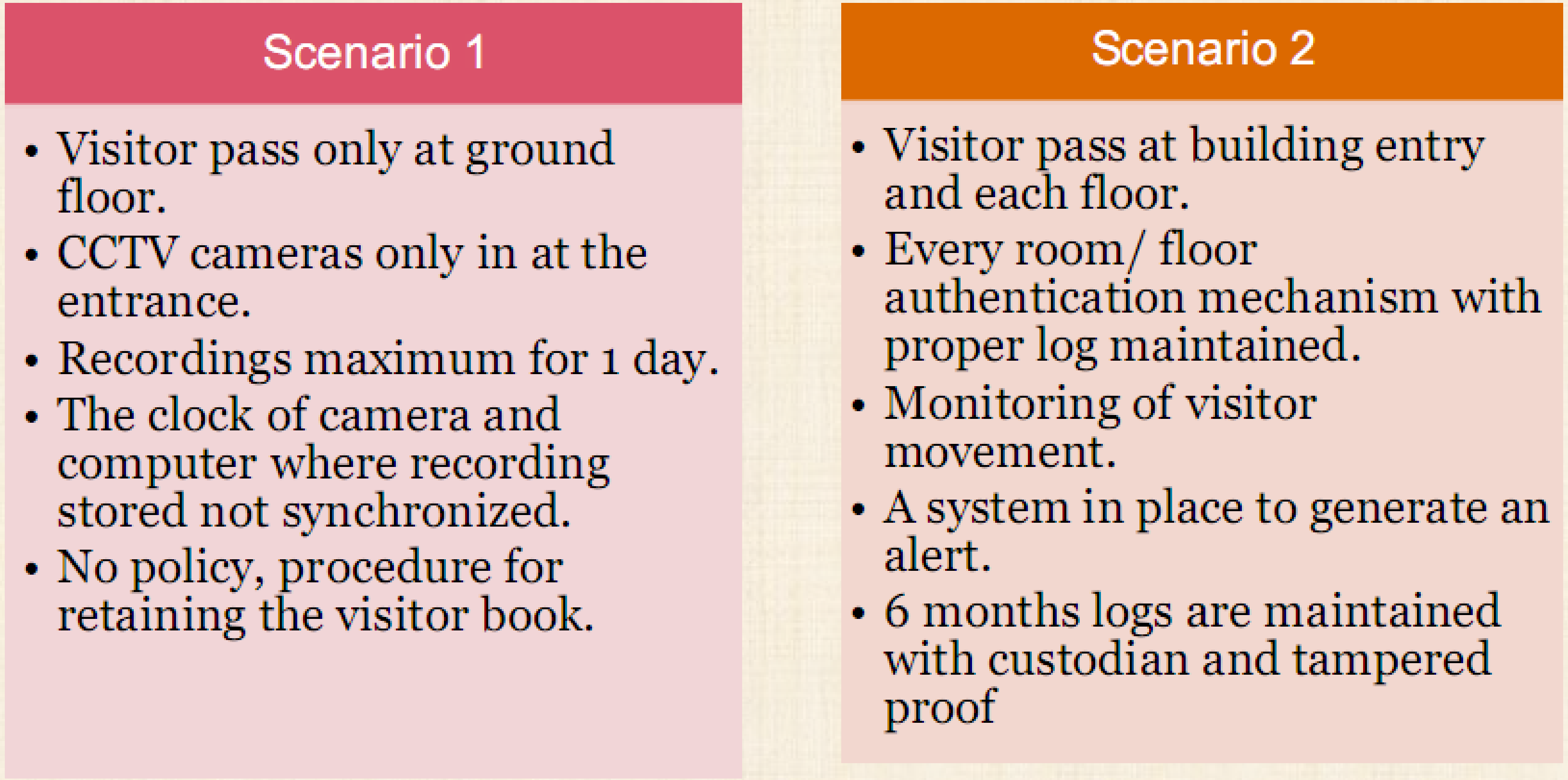
Forensic readiness as defined by Mohay as the extent to which computer systems or computer networks record activities and data in such a manner that the records are sufficient in their extent for subsequent forensic purposes, and the records are acceptable in terms of their perceived authenticity as evidence in subsequent forensic investigations.

*Digital evidence can be in the form of log files, emails, back-up disks, portable computers, network traffic records, and phone records etc.

5.1 Introduction (cont)

- 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.

Which scenario is better?



Scenario 1

- 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.

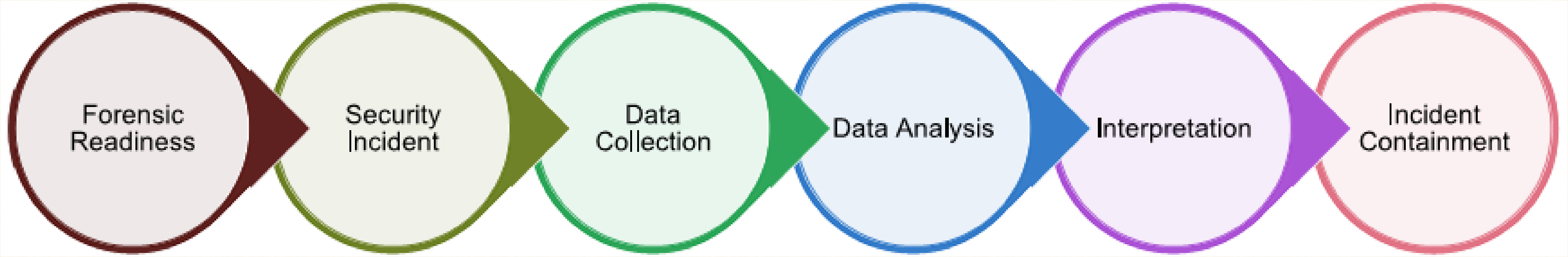
Scenario 2

- 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

5.2 Goals of Forensic Readiness

Some of the important goals of forensics readiness are:

- To gather admissible evidence legally and without interfering with business processes;
- To gather evidence targeting the potential crimes and disputes that may adversely impact an organization;
- To allow an investigation to proceed at a cost in proportion to the incident;
- To minimize interruption to the business from any investigation; and
- To ensure that evidence makes a positive impact on the outcome of any legal action.



Identify
Protect
Security Governance
Detect
Recover
Respond

5.3 Forensic Readiness Steps

The following ten steps describe the key activities in forensic readiness planning:

1. Define the business scenarios that require digital evidence:

The first step in forensic readiness is to define the purpose of an evidence collection capability. The rationale is to look at the risk and potential impact on the business from the various types of crimes and disputes. What is the threat to the business and what parts are vulnerable?

2. Identify available sources and different types of potential evidence:

The second step in forensic readiness is for an organization to know what sources of potential evidence are present on, or could be generated by, their systems and to determine what currently happens to the potential evidence data. Computer logs can originate from many sources.

5.3 Forensic Readiness Steps (Cont.)

3. Determine the evidence collection requirement:

The purpose of this step is to produce an evidence requirement statement so that those responsible for managing the business risk can communicate with those running and monitoring information systems through an agreed requirement for evidence. One of the key benefits of this step is the bringing together of IT with the needs of corporate security.

4. Establish a capability for securely gathering legally admissible evidence to meet the requirement:

At this point the organization knows the totality of evidence available and has decided which of it can be collected to address the company risks and within a planned budget. With the evidence requirement understood, the next step is to ensure that it is collected from the relevant sources and that it is preserved as an authentic record.

5.3 Forensic Readiness Steps (Cont.)

5. Establish a policy for secure storage and handling of potential evidence:

The objective of this step is to secure the evidence for the longer term once it has been collected and to facilitate its retrieval if required. It concerns the long-term or off-line storage of information that might be required for evidence at a later date.

6. Ensure monitoring is targeted to detect and deter major incidents:

In addition to gathering evidence for later use in court, evidence sources can be monitored to detect threatened incidents in a timely manner (suspicious events detection). This is directly analogous to Intrusion Detection Systems (IDS), extended beyond network attack to a wide range of behaviors that may have implications for the organization.

5.3 Forensic Readiness Steps (Cont.)

7. Specify circumstances when escalation to a full formal investigation:

Some suspicious events can be system generated, such as the rule-base of an IDS, or the keywords of a content checker, and some will be triggered by human watchfulness. Each suspicious event found in step 6 needs to be reviewed. Either an event will require escalation if it is clearly serious enough, or it will require enhanced monitoring or other precautionary measures, or it is a false positive. The purpose of this step is to decide how to react to the suspicious event.

8. Train staff in incident awareness:

So that all those involved understand their role in the digital evidence process and the legal sensitivities of evidence, The aim of this step is to ensure that appropriate training is developed to prepare staff for the various roles they may play before, during and after an incident. It is also necessary to ensure that staff is competent to perform any roles related to the handling and preservation of evidence.

5.3 Forensic Readiness Steps (Cont.)

9. Document an evidence-based case describing the incident and its impact:

The aim of an investigation is not just to find a culprit or repair any damage. An investigation has to provide answers to questions and demonstrate why those answers are credible. The questions go along the lines of who, what, why, when, where and how. Credibility is provided by evidence and a logical argument. The purpose of this step is to produce a policy that describes how an evidence-based case should be assembled.

10. Ensure legal review to facilitate action in response to the incident:

At certain points during the gathering of the cyber-crime case file it will be necessary to review the case from a legal standpoint and get legal advice on any follow-up actions. Legal advisers like attorney should be able to advise on the strength of the case and suggest whether additional measures should be taken; for example, if the evidence is weak is it necessary to catch an internal suspect red handed by monitoring their activity and seizing their PC ?.

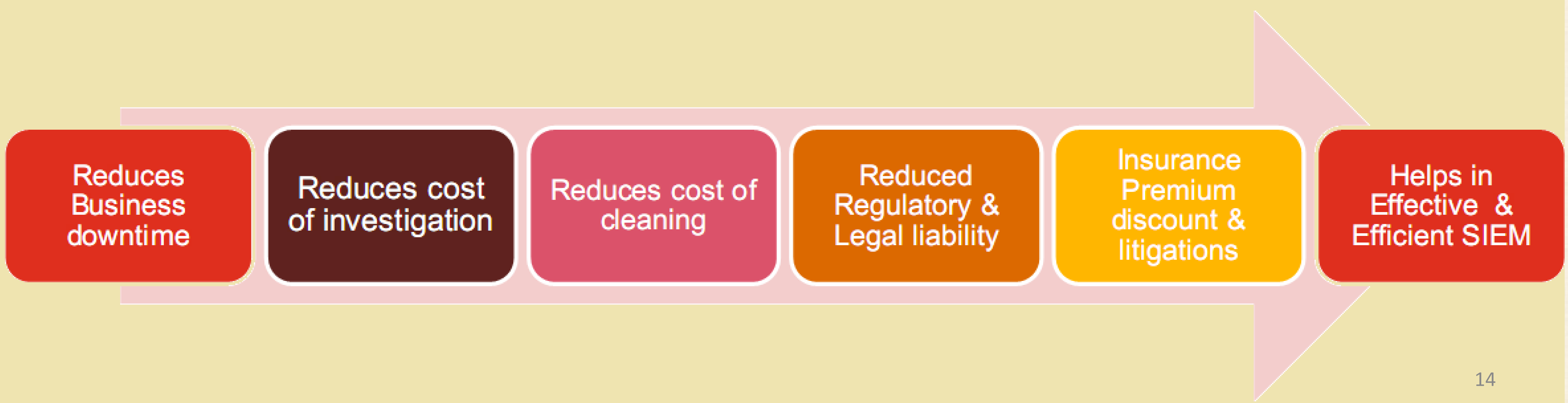
5.4 Benefits of Forensic Readiness

Forensic readiness can offer an organization the following benefits:

- evidence can be gathered to act in an organization's defense if subject to a lawsuit;
- comprehensive evidence gathering can be used as a preventive to the insider threat.
- in the event of a major incident, an efficient and rapid investigation can be conducted and actions taken with minimal perturbation to the business;
- a systematic approach to evidence storage can significantly reduce the costs and time of an internal investigation;
- a structured approach to evidence storage can reduce the costs of any court-ordered disclosure or regulatory or legal need to disclose data (e.g. in response to a request under data protection legislation);

5.4 Benefits of Forensic Readiness (Cont.)

- forensic readiness can extend the scope of information security to the wider threat from cybercrime, such as intellectual property protection, fraud detection, extortion etc;
- it demonstrates due diligence and good corporate governance of the company's information assets;
- it can support employee sanctions based on digital evidence (for example to prove a violation of acceptable use policy)


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

5.5 Digital Forensic Readiness features:

it is required for:

Regulatory Compliance

- GK Recommendations
- Cyber Security Framework

Business Impact analysis

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

Legal

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

Threat detection & Monitoring

- To enhance SIEM capability
- Log correlation, Interpretation

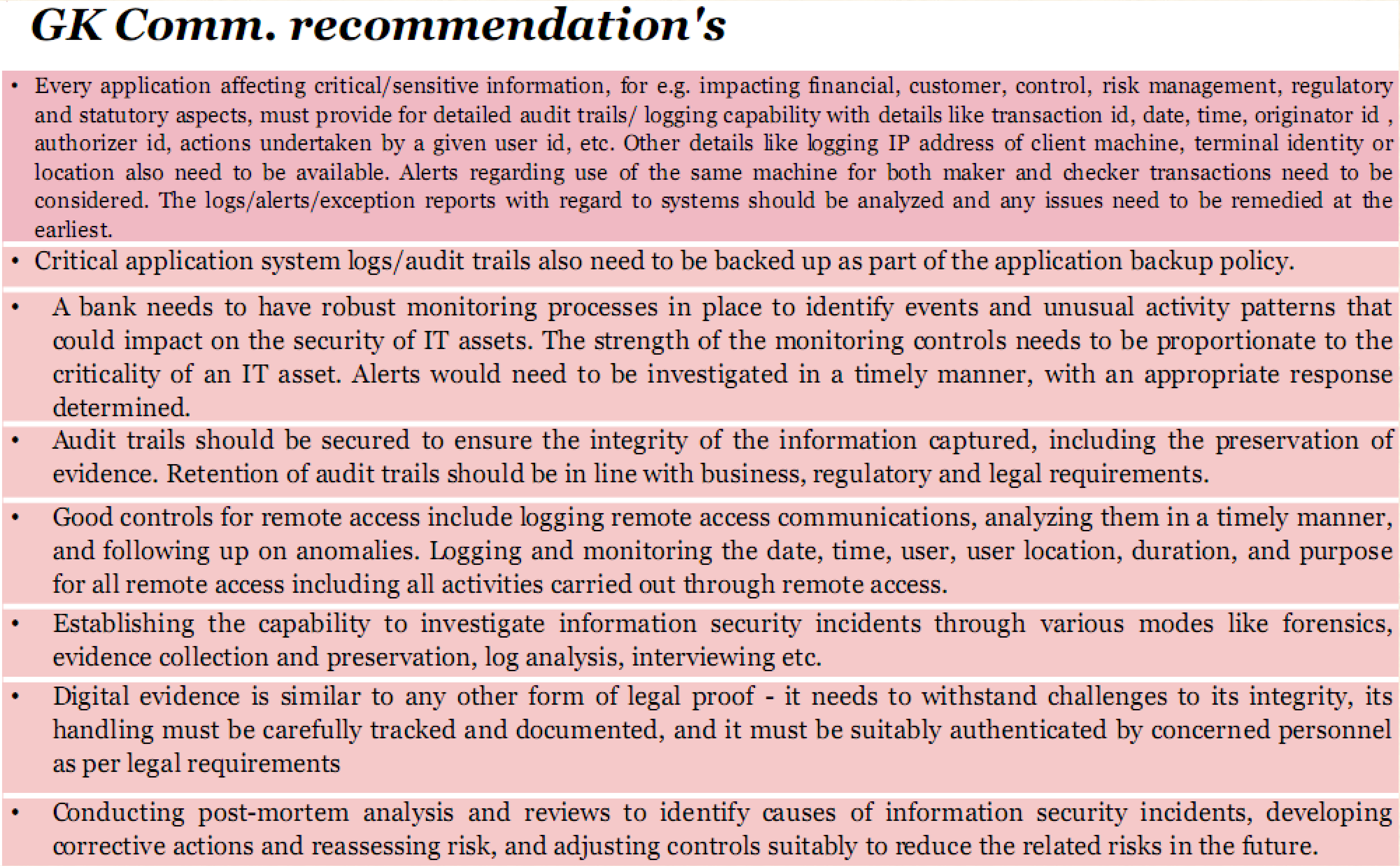
Employee Misconduct

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

Insurance claim

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

5.5 Digital Forensic Readiness features:



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.

5.5 Digital Forensic Readiness features (Cont.)

The checklist

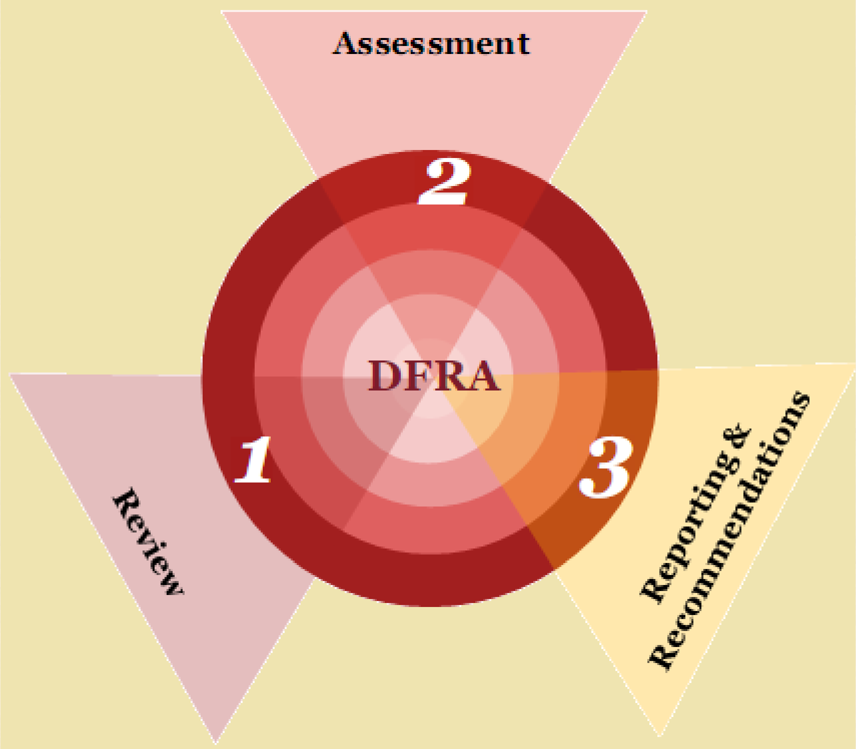
- Identify the business scenarios and various threats both external and internals.
- Identify potential sources and types of data – devices, applications, data bases
- Map the sources of data with threat.
- Identify the collection and retention requirement – Legal, Regulatory compliance
- Test and improve 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.

ISO 27037	ISO 27041	ISO 27042	ISO 27043
Guidelines for identification, collection, acquisition and preservation of digital evidence	Guidelines on assuring suitability and adequacy of incident investigation method	Guidelines for analysis and interpretation of digital evidence	Guidelines for incident investigation principles and processes

5.5 Digital Forensic Readiness features (Cont.)

Assessment -Approach

- 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

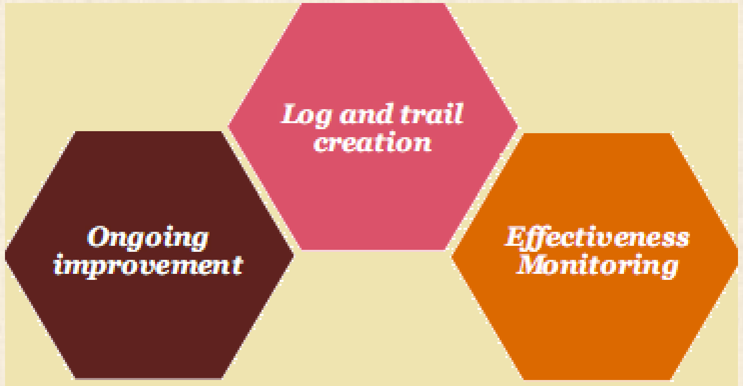


- Effectiveness of log collection & retention in tracing & tracking the security incident;
- Effectiveness of log monitoring & analysis
- Effectiveness of existing controls in detection, prevention of attacks;
- Effectiveness of incident response such as handling, coordination & resolution;
- Effectiveness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

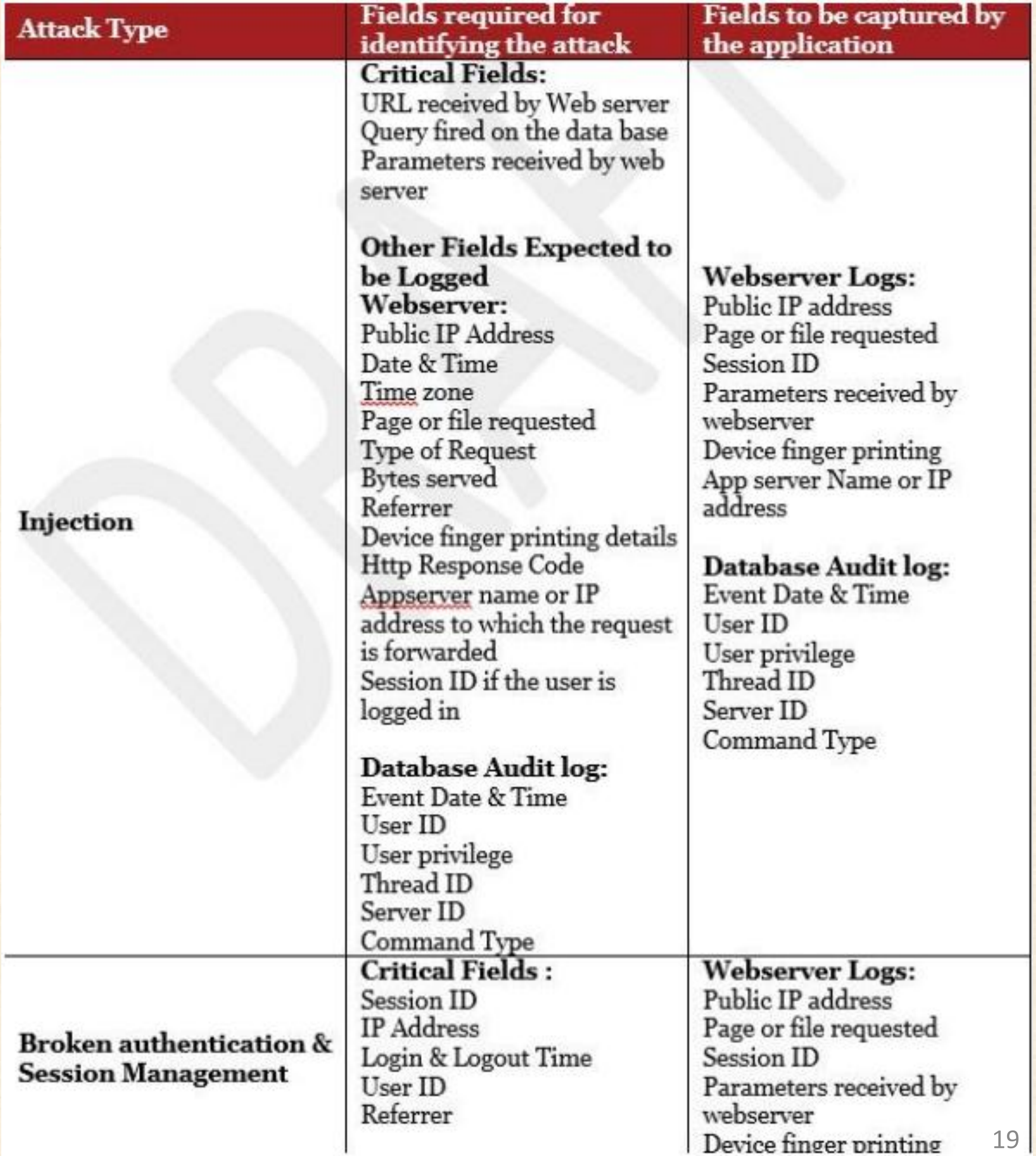
- Gap analysis for existing vs Standards such as ISO 27037, 27041,27042,27043 , 27001, RBI cyber security framework, Gopal Krishnan committee.
- Recommend framework, policy, procedures for digital Forensic readiness
- Recommend enhancements to existing process & technology to support forensic readiness

5.5 Digital Forensic Readiness features (Cont.)

Guidelines



- 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