Importance of Forensic Readiness

Almost all organizations are now dependent, one way or another, on information technology. This has led to a great deal of development as well as associated risk. Hence, various strategies have evolved (and continue to evolve as technology evolves) in a bid to minimize and mitigate the associated risk.

In the event that an organization’s business is brought to a standstill by an unwanted or unforeseen event, whether natural or man-made, the business needs to recover and continue. As a result, strategies such as incident response, awareness training, disaster recovery and business continuity planning have become basic components of organizations’ operational structure.

In addition to recovery issues, an unwanted incident can also result in other issues such as insurance claims, legal matters and regulatory issues. In the course of recovery and investigation, claims may arise against employees, third parties or even the organization, for example, pertaining to what led to the incident. Could it have been negligence, malicious intent, fraud or sabotage? Digital evidence becomes very important when such issues arise in an organization that uses IT infrastructure, even if the usage is minimal. Digital forensics tools and techniques are available for retrieving and analyzing digital evidence. Users of information systems leave digital footprints whenever they use the systems—be they computer systems, smartphones, mobile phones, tablets or networks (i.e., the Internet, intranets, phone networks).

WHAT IS DIGITAL FORENSICS?

Digital forensics is a field that is still evolving. It can be defined as the use of computer and information systems (IS) knowledge, coupled with legal knowledge, to analyze in a legally acceptable manner digital evidence acquired, processed and stored in a way that is legally acceptable. Digital forensics tends to be mainly used for investigations that are geared toward legal or law enforcement issues that are likely to end up in court; hence, the emphasis on legal acceptability. Digital evidence is extremely volatile and can be easily lost or distorted. Thus, there is a need to preserve and handle digital evidence in a manner that will ensure that it is not, and does not appear to have been, distorted or destroyed. However, digital forensics tools and techniques can also be used to recover lost files and for internal administration (such as monitoring or investigating abuse). In a nutshell, digital forensics tools and techniques can be used to trace and investigate what may have occurred or led to an incident, to retrieve lost data, and to gather evidence for use by an organization against a person or entity or to defend the organization.

Chain of custody (referred to as “continuity of evidence” in the UK) is required to provide assurance that digital evidence has been gathered, processed, handled and stored with due care such that it is not altered or destroyed, or that such cannot be inferred. Chain of custody involves documentation of how digital evidence is acquired, processed, handled, stored and protected, and who handled the evidence and why—from the point of collection to it being presented as an exhibit (e.g., in court or at a board hearing).

An organization can carry out digital investigations on its own whereby evidence is not going to court, such as for employee monitoring (where that is considered acceptable). Such a case may not necessarily require handling the evidence in a legally acceptable manner (chain of custody), but there is the possibility that such investigations could open a can of worms: Something that requires legal action may be uncovered (e.g., sabotage, fraud). In such a case, evidence being presented in court must be collected and documented in a legally acceptable manner (chain of custody), but there is the possibility that such investigations could open a can of worms: Something that requires legal action may be uncovered (e.g., sabotage, fraud). In such a case, evidence being presented in court must be collected and documented in a legally acceptable manner for admissibility. Digital forensics can also be used for audit investigations and can be very useful when investigating fraud. Auditors can use forensic tools and techniques to monitor and review compliance with organizational policies and regulatory requirements. For example, digital forensics can help discover and trace unauthorized Internet access by employees,
loopholes and vulnerabilities in the network, and malware incidents such as attacks and intrusions can be analyzed to determine how the breach occurred to prevent future attacks. Having a forensic readiness plan in place goes a long way toward ensuring such investigations and any discovery therein can be handled and presented so that the organization does not lose a case.

**WHAT IS FORENSIC READINESS?**
CESG Good Practice Guide No. 18, *Forensic Readiness*, defines 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.” Others define forensic readiness as the ability of an organization to maximize its potential to use digital evidence while minimizing the cost of an investigation.

In the course of operations, organizations generate a lot of digital data and records. Such data and records can become crucial pieces of evidence in the event of an unwanted incident. Some of this digital evidence is stored and preserved as part of disaster recovery and business continuity processes as well as document-retention policies. These could be in the form of backup files. Monitoring records (such as CCTV footage) also constitute part of digital evidence. There is still other digital evidence that may not be taken seriously, and may be required only in the event of an incident, which might not be readily available, if at all, when an investigation becomes necessary. Such evidence could be in the form of casual communication such as emails, social networking messages, and activity that was carried out on workstations and mobile devices. It is not easy to forecast when digital evidence may become necessary; furthermore, the use could be for internal purposes, regulatory or legal requirements, or other external reasons. Forensic readiness helps an organization streamline its activities so that retrieval of digital evidence becomes easy with reduced hassles. That is, digital evidence is appropriately recorded and stored even before an incident takes place, without interruption of operations. The following is a list of scenarios where digital evidence would become necessary:

- Disputed transactions
- Allegations of employee misconduct
- Showing legal and regulatory compliance
- Avoidance of negligence and breach-of-contract charges
- Assisting law enforcement investigations
- Meeting disclosure requirements in civil claims
- Supporting insurance claims when a loss occurs
- The highly volatile nature of digital evidence demands that it be treated delicately by safeguarding chain of custody. Having a forensic readiness plan in place ensures that in the event digital evidence is required, it will be readily available and in an acceptable form. This requires training of staff and having proper policies in place to ensure compliance. Forensic readiness planning complements other organizational plans and processes, including disaster recovery, business continuity and document-retention policies. Conventional disaster recovery and business continuity processes usually concentrate on low-frequency/high-impact events; a forensic readiness plan would, however, cover high-frequency/low-impact events as well. While the latter tend to appear insignificant, they could be the cause or source of a major disaster.

Forensic readiness planning is part of a quality information risk management approach. Risk areas have to be identified and assessed and measures must be taken to avoid and minimize the impact of such risk. Organizations with a good risk assessment and information security framework would find it easier to adopt a forensic readiness plan. A forensic readiness plan should have the following goals:

- To gather admissible evidence legally without interfering with business processes
- To gather evidence targeting potential crimes and disputes that could have adverse impact on an organization
- To allow investigations to proceed at costs proportional to the incident
- To minimize interruption of operations by investigations
- To ensure that evidence impacts positively on the outcome of any legal action
BENEFITS OF FORENSIC READINESS PLANNING

The benefits of forensic readiness planning include:

• **Preparing for the potential need for digital evidence.**

  In the event that an organization has to go to litigation where digital evidence is required, there will be a need for electronic discovery (e-discovery). Laws related to e-discovery, including the US Federal Rules of Civil Procedure (FRCP) and the UK’s Practice Direction 31B, require electronic evidence to be provided quickly and in a forensically sound manner when requested. Information management is the first phase (see figure 1) of the Electronic Discovery Reference Model (EDRM), which is considered a standard for going through the e-discovery process and compliance with FRCP. Information management requires, in part, that electronic evidence be collected and stored in an appropriate manner so that it is readily available when requested. Information management for e-discovery includes data retention, incident response, disaster recovery and business continuity policies—all of which are augmented by a forensic readiness policy or plan. For example, in the case of AMD vs. Intel, AMD had requested some email evidence from Intel for discovery, but Intel failed to produce it due to a faulty email retention policy and by not properly communicating the litigation hold to employees (i.e., Intel failed to properly inform employees using systems relevant to the case and their IT department that the employees’ electronically stored information [ESI] was required as evidence), resulting in severe sanctions against Intel. In 2009, Intel agreed to settle with AMD for US $1.25 billion; the company might have averted this cost if it had a forensic readiness plan in place.

• **Minimizing the cost of investigations.** Because evidence is gathered in anticipation of an incident, costs as well as the disruption of operations are minimal and investigations are efficient and rapidly completed. Because evidence is already gathered, the investigator needs only to analyze and review network logs, for example, in order to gather evidence regarding a network breach. This makes investigations faster and more efficient while also reducing adverse effects of interrupting employees’ work or production.

• **Blocking the opportunity for malicious insiders to cover their tracks.** Furthermore, because individuals become aware that evidence is being constantly gathered, they are deterred from carrying out malicious activities for fear of being caught. Constant monitoring and information gathering assist in detecting malicious insider activity. If a mischievous staff member, for example, is trying to spoof someone else’s IP address to send a nasty email to the chief executive officer or infect the corporate network with malware: Having a forensic readiness plan in place makes it easy to discover and trace such activity.

![Figure 1—The Electronic Discovery Reference Model](image)

Reducing cost of regulatory or legal requirements for disclosure of data. Having the evidence easily at hand and preserved in an acceptable manner makes it possible for it to be easily presented when and as required. As illustrated in the case of AMD vs. Intel, there is considerable financial risk when information is not properly managed. A forensic readiness plan helps augment other information security and assurance strategies such as data retention, disaster recovery and business continuity. Regulatory requirements in many countries require such strategies and polices, and lack of compliance can result in severe financial penalties. There may be instances where regulatory authorities or law enforcement may require immediate release or disclosure of certain ESI, for example, in the case of suspected terrorist activity or financing by an organization or its employees. Failure to provide such ESI in an appropriate and timely manner could result in serious adverse costs, such as loss of goodwill and regulatory sanctions, to an organization.

Showing due diligence, good corporate governance and regulatory compliance. Having good information management policies, such as a forensic readiness policy, shows an organization is on top of incident prevention and response. This helps garner goodwill for the organization, providing customers with a feeling that their transactions are secure and protected. Investors also have more confidence in an organization that has such security alertness because it ensures that threats to their investments are minimized. It also helps to encourage good relations with regulatory authorities and law enforcement since it shows that the organization goes far to ensure compliance with laws and regulations, making the job of regulators and law enforcement easier. In the case of an incident, it makes the job of investigators much easier because evidence has already been gathered prior to, during and after the incident.

Uncovering bigger cases. In monitoring acceptable usage of endpoints, malware may be discovered to have infiltrated a system and its source subsequently traced, helping to protect against such attacks in the future. This is just one example of how a potential incident may be uncovered before it becomes a security incident or detected in its infancy before it becomes a serious problem. Furthermore, greater cyberthreats can be uncovered, traced and prevented, e.g., harassment, fraud, extortion, intellectual property theft. Overall, there is increased information security.

A FORENSIC READINESS IMPLEMENTATION GUIDE
A forensic readiness plan is meant to prepare an organization for an event the occurrence of which cannot be predicted. In preparation, an organization should review and analyze security—technical controls, policies, procedures and skill sets. This can be carried out by a skilled forensic investigator, who can recommend proper amendments and action that can be taken to improve upon what is in place and ensure a good forensic readiness plan.12

The goals and objectives of the organization and its risk appetite need to be identified, the security posture analyzed, employees educated and enlightened on the forensic readiness plan, and the action plan formulated to deal with identified gaps in the status quo. Knowing the goals, objectives and risk appetite helps to determine what would be considered significant or relevant risk, what type of incidents should be expected, and how to respond to them. The current security level should then be reviewed for adequacy and to expose any potential loopholes. Employees need to be informed and educated regarding the forensic readiness plan to ensure their compliance. Finally, identified loopholes are mitigated by instituting appropriate measures.

The Carolina Crime Report offered the following 10 points for a forensic readiness checklist:13

1. Define the business scenarios that would require digital evidence. This helps to streamline where and how to concentrate evidence collection storage.
2. Identify potential evidence sources and the types of evidence.
3. Determine evidence collection requirements.
4. Establish capability for secure evidence gathering and collection in a forensically sound manner.
5. Establish a policy for proper chain of custody.
6. Ensure monitoring targets detection and deterrence of major incidents.
7. Specify the circumstances at which point the escalation of a full formal digital investigation should commence.
8. Educate and train staff on incident response and awareness to ensure that they comprehend their role in the digital evidence process and the importance and sensitivity of it.
Ensure legal review to facilitate appropriate action in response to an incident.

An IT auditor performing a forensic readiness assessment should check to see that the above points can be deduced from the forensic readiness policy of an organization.

**CONCLUSION**

Increased use and dependency on information technology for running organizations and businesses have resulted in the availability of digital footprints that can be used to unravel the what, where, how and why in the event of an unwanted incident. Digital evidence can lead to the indictment or vindication of an individual or organization. Digital evidence needs to be gathered and treated with due care, usually by applying chain-of-custody requirements, because of its high volatility.

While many organizations are currently aware of the importance and need for disaster recovery and business continuity plans, they must also recognize the need for and importance of forensic readiness planning. The tendency is to be reactive, waiting for an incident to occur then trying to handle it and carry out investigations—gathering evidence after the fact. As a result, operations become disrupted, some evidence may be altered or lost, and evidence may not be handled in an acceptable manner. Forensic readiness greatly minimizes these problems, especially as a great deal of the evidence required is available before the incident, during the incident and before investigations begin. As a result, time and money are saved, potential incidents are mitigated, and business continuity and compliance are ensured, with minimal disruption and interruption of operations. Forensic readiness also assists in ensuring employees’ compliance with the organization’s policies and regulatory requirements due to constant monitoring and review.

ENDNOTES

5. Op cit, Rowlingson, 2004
7. Ibid.
8. Op cit, Rowlingson, 2004
9. Ibid.