# Chapter 12
# Forensic Readiness and eDiscovery

**Dauda Sule**
*Audit Associates Ltd, Nigeria*

## ABSTRACT

*In a bid to discover, uncover, and stamp out digital crime while ensuring information security and assurance, there is a need to investigate the crime once it has taken place. This will help trace the criminals and also secure an organization against future attacks. Forensic readiness entails that an organization be at alert in terms of digital evidence collection and storage – that is, collecting and storing such evidence constantly in a forensically sound manner, not just when the need for such evidence arises. In the event litigation arises or is anticipated, digital evidence may need to be reviewed by the opposing parties prior to court proceedings to assess quality of the evidence; this is eDiscovery. This chapter explores eDiscovery and forensic readiness. Digital evidence for eDiscovery needs to be forensically sound and provided in a timely and efficient manner - forensic readiness helps to ensure this. This chapter seeks to establish how forensic readiness is relevant to the eDiscovery process.*

## INTRODUCTION

In this digital age, issues pertaining to information security and assurance abound; and with increased technological advancements, criminals are also improving on their skills and causing more and more havoc. Digital forensic investigations are one way of ensuring information assurance and security; in that it can lead to discovering how a digital crime was committed and possibly tracing and apprehending the perpetrators. Knowing how a digital crime was committed can also assist an organization strengthen its defenses as it reveals weaknesses and lapses in the organization's information security and assurance measures. Forensic readiness requires that an organization be on its toes as regards gathering, storing and analyzing digital data in a forensically sound manner – such data has the potential of serving as digital evidence in the event of an incident or litigation. Such digital evidence can be used by an organization to trace how an incident happened, defend itself or indict a party, also to show regulatory compliance and best practices. With forensic readiness, investigations can be carried out faster and more efficiently with minimal disruption to normal operations, and it also reduces the cost of such evidence gathering. Electronic evidence is constantly gathered and stored until something occurs whereby it would be required to serve as evidence or used for backup and recovery – it is like saving for a rainy day. Therefore in the event of an

DOI: 10.4018/978-1-4666-6324-4.ch012

incident that requires investigation, the evidence only has to be presented, as it is already collected and stored in a forensically sound manner. This helps make evidence presentation and investigation much faster and allows for business continuity with minimal disruption to normal operations, which would have arisen if investigators had to gather the evidence after-the-fact. It also helps ensure that an attacker does not cover his tracks after an attack as evidence is collected before, during and after the breach – collecting evidence after the breach could afford an attacker time to wipe out his tracks before evidence gathering and investigations begin.

eDiscovery on the other hand comes up when there is litigation or litigation is anticipated, requiring opposing parties in litigation to possibly review each others' digital evidence to assess its quality prior to court proceedings. eDiscovery may also be viewed as the sum total of the processes involved in a digital investigation including evidence gathering and analysis. Seigle-Morris (2013) considered the whole point of eDiscovery to be reduction of data volume that requires review into a manageable and easily reviewable form, extracting only that which is relevant to the case at hand. eDiscovery can be a very delicate issue, its rules and guidelines have to be safeguarded by both parties in litigation. The digital evidence has to be forensically sound, timely, relevant, and in the format required by the requesting party; failure to meet up with the rules and guidelines can result in severe consequences for the erring party. In the case of *AMD vs. Intel (2005)*, Intel failed to provide digital evidence as requested by AMD in good time, resulting in heavy costs to Intel at the end of the day.

From the point of view of eDiscovery being litigation requirements for digital evidence review prior to court proceedings and the view that eDiscovery is the process of digital investigations, there is the need to have digital evidence collected in a forensically sound manner and for it to be provided in a timely and efficient manner. In order to achieve this, it would be best to collect and store such evidence constantly, not only when the need for it arises – that is forensic readiness. Forensic readiness ensures constant collection of digital evidence in a forensically sound manner making the eDiscovery process much easier and efficient. Forensic readiness goes a long way in ensuring that an organization is adequately prepared for eDiscovery.

## BACKGROUND

The field of digital forensics is still an emerging one – there are not really any firmly established principles for it yet, although there are guidelines available. Digital forensics is an important aspect of information security especially in this digital age, it is used to investigate and establish proof of crimes committed using IT resources and platforms. Every activity carried out using IT systems and platforms leaves a digital footprint and tends to be stored in the form of Electronically Stored Information (ESI). A review of ESI can reveal a lot about what had occurred on the system and/or platform.

Sule (2013) defined digital forensics as the use of computer and information systems knowledge, coupled with legal knowledge to analyze in a way that is legally acceptable digital evidence acquired, processed and stored in a legally acceptable manner. This definition takes into cognizance that digital forensics is where technology and the law meet. There is an emphasis on legal acceptability of evidence as it is usually the case that digital evidence will end up being used for civil or criminal court proceedings, bearing in mind that legal acceptability varies from country to country, and jurisdiction to jurisdiction. The most important thing is to ensure that the evidence is collected, stored and analyzed in a forensically sound manner to provide reasonable assurance that the evidence was not tampered with or damaged and also not giving room for anyone to claim such. Others have a more open definition of digital forensics without much emphasis on legal acceptability, as