Event-Based Assessment of Cyber Security and Digital Forensic Readiness

TREO Talk Paper

Andrés Díaz López
University of Mississippi
alopez@bus.olemiss.edu

Abstract

DFR is the state of preparedness to obtain, understand, and present digital evidence when needed. Measures taken to be prepared for digital forensics are, in big part, measures of cyber security readiness. However, the objectives of DFR can be at odds with those of cyber security. While, cyber security measures aim to keep systems integrity, confidentiality and availability, forensic readiness objectives are defined as “maximizing the environment’s ability to collect credible digital evidence, and minimizing the cost of forensic during an incident response” (Tan 2001). Therefore, while the responsible of cyber security rushes to stop the breach, the DFR expert is gaining insights from it.

The problem in measuring DFR is that regardless of the actions taken to be prepared to respond to an incident requiring the collection, analysis and presentation of digital evidence, such response can only be assessed after a real incident occurs. And even if it occurs, the incident will be unique in antecedents, circumstances, manner, and consequences. It is unlikely that another incident in the same or a different organization will share those same conditions. Once an incident occurs, that experience affects the awareness and knowledge of the actors involved and the expectations against which to measure future reactions to new events. Therefore, comparisons are difficult.

According to Mouhtaropoulos, Grobler, & Li “Digital forensic readiness is often ad hoc and no consistent application or framework exists globally” (2011). After a wide review of the literature in DFR, the present research has found that this assertion remains true to these days and provides grounds for a research question: how can organizations assess their level of digital forensic readiness (DFR) in absence of a widely accepted standard of its application? In answering this question, one can think of two different approaches separated by a critical point in time: the moment of the realization of an incident. To evaluate the preparation before an incident, organizations can compare what they have, know and are doing to what experts suggest that they should have, know and be doing. However, the artifact proposed here is based on the chronology of events considered after the incident has occurred. These events include the the opening of a vulnerability, being aware of it, preparing safeguards, suffering an incident, awareness of the incident, start investigating, solving the security issue, and closing the investigation. Put this way, the digital investigation process unveils several opportunities of assessment and improvement of firms’ DFR based on the timing of these critical points and the distances in time among them.

In summary, this article proposes an event-based model that uses the chronology of critical points in the timeline of events associated to an incident as an artifact for the assessment of DFR and cybersecurity readiness. A visualization tool of the artifact and examples of possible DFR and cybersecurity key indicators will be presented. The TREO session can provide insights for the betterment of the artifact and its feasibility, as well as for the appropriate research methodology to validate the contribution and the direction that future research on this topic should take.

References
