Chapter 11
Turning Weakness into Strength:
How to Learn From an IT Security Incident

Randy L. Burkhead
Capella University, USA

ABSTRACT

In today's culture organizations have come to expect that information security incidents and breaches are no longer a matter of if but when. This shifting paradigm has brought increased attention, not to the defenses in place to prevent an incident but, to how companies manage the aftermath. Using a phenomenological model, organizations can reconstruct events focused on the human aspects of security with forensic technology providing supporting information. This can be achieved by conducting an after action review for incidents using a phenomenological model. Through this approach the researcher can discover the common incident management cycle attributes and how these attributes have been applied in the organization. An interview guide and six steps are presented to accomplish this type of review. By understanding what happened, how it happened, and why it happened during incident response, organizations can turn their moment of weakness into a pillar of strength.

INTRODUCTION

A 21st Century individual must confront a new aspect of modern life – that information security incidents will happen and it could be anyone's fault. Anyone could be the person who loses a thumb drive, gives away someone's username and password, or anybody's identity might be the one someone steals. What happens when this happens? How can organizations respond to these various events? The research conducted in "A Phenomenological Study of Information Security Incidents Experienced by Information Security Professionals Providing Corporate Information Security Incident Management" (Burkhead, 2014) details how private companies located in the Pacific North West of the United States respond to these issues from a human perspective. Participants discussed experiences that ranged from working with small business clients to global firms dealing with threats large enough to take down the Internet around the world.

DOI: 10.4018/978-1-5225-7113-1.ch011

This chapter is designed to provide the reader with two essentials lessons to be learned. The first lesson is to inform the reader about this modern threat that can affect anyone around the world and how it is possible to assess and analyze a crisis situation in order to learn, mature, and grow over time. The second lesson is providing a moldable framework for conducting phenomenological research in various fields. Phenomenology models are designed to describe rather than explain experiences (Creswell, 2012). The focus of phenomenology is on the lived experiences of participants. The experiences, when analyzed, form a structure that reflects the essences of the phenomenon experienced. The media has remarked that security incidents are no longer a matter of if but a matter of when. This change makes what comes after an incident just as important, if not more so, than the protections placed around data to keep it safe.

The first part of this chapter is designed to provide the reader with some background information on the subject of information security incident management. Several terms are provided so that readers without an IT security background may have a better understanding of information security incidents. Once all readers have a common understanding of the terms used in this subject area, the results of some previous research using a phenomenological model are presented to provide the reader with a framework for the processes, procedures, and lessons learned in incident response. This common understanding of terms and pervious research is important in order to understand the processes and procedures involved in conducting reviews of information security incidents.

The second part of this chapter is designed to provide the reader with an explanation for conducting similar research. Prior to conducting a study it is important to establish the scope of the project. Once the scope has been established there are six steps to conducting an after action review using a phenomenological approach. Step one is to leave personal baggage at the door as it is important not to form biased opinions. Step two is to collect the data through interviews and technical analysis. Step three is to breakdown the data into its simplest components. Step four is to reconstruct the data in order to understand the themes that span all sources. Step five is to identify the essences of the reconstructed data in order to provide a strong basis for the final step. Step six is to recognize the conclusions and build recommendations. The end result of this assessment processes will allow organizations and individuals to learn from information security incidents.

PREVIOUS RESEARCH

There is a lot of existing research on the topic of cyber security ranging from war applications to criminal activities. There are published standards for IT security including industry regulations like the Payment Card Industry Data Security Standard (PCI-DSS), government sponsored standards like United States National Institute for Standards and Technology (NIST) special publication 800-53, laws and regulations such as the Health Information Privacy and Accountability Act (HIPAA), and international cyber security standards such as International Standard Organization (ISO) 2700 and Information Technology Infrastructure Library (ITIL). Each of these standards has processes and procedures for incident response; but they each have only limited instructions for how to build an incident response program. There is very little research into the phenomenon of IT security incidents and incident management in the field.

Despite being a problem that has existed for well over three decades most research has been focused on the attack methods, actors, and vectors rather than the actions, decisions, processes, and procedures used during information security incident management. A phenomenological model is uniquely suited for research designed to address this gap. In “A Phenomenological Study of Information Security In-