Bennett Hall

CISC 6920

Paper 1

The Relationship Between Incident Response and Risk Management

Incident response and risk management are two relevant, important concepts in the world of information security. These two concepts both have their own individual meaning. The meaning of each concept is important to understand, but so is the relationship between these two distinct concepts. While both concepts are each individually unique and must be understood they are also intertwined, related to one another if you will. Information security is a fast moving and ever changing industry, but risk management and incident response have continued to play significant roles in the field.

Before we examine the relationship between incident response and risk management let's analyze what both concepts mean, starting with incident response. Incident response is what happens when an organization responds to some sort of security event. "It's a coordinated and structured approach to go from detection to resolution" (Luttgens, 5). Every incident is different. Some incidents are more devastating than others. Some incidents last longer than other incidents. Every action that's taken from the initial detection until the incident has been resolved is covered under the umbrella of incident response. In addition to detection and resolution this includes things like investigation, remediation, analysis, education, among others. The steps that an organization takes during incident response are critical and will have long lasting implications on the future of the organization and how it functions after the incident has been resolved.

Conversely, risk management has a different meaning, but it too is important to understand. Risk management can be defined by asking and answering some basic questions:

“ What are your critical assets? What is their exposure? What is the threat? What regulatory requirements must your organization comply with?” (Luttgens, 47). Risk management is all about the likelihood of a threat being realized and the impact that said threat will have on an organization. It’s a broad topic and in the world of information security there is an almost endless myriad of potential threats to organizations. While different organizations are more likely than others to be affected by certain threats there is also a lot of crossover. Risk management is an ongoing, never ending process that organizations must execute in order to protect themselves from attacks. Proper risk management practices can save an organization from serious threats and mitigate the impact of severe attacks. Weak, or non-existent, risk management practices will greatly damage or possibly even eliminate an organization altogether.

What is the relationship between these two concepts: incident response and risk management? We know that risk management is all about identifying threats and determining the likelihood of them being realized. We know that incident response is all about an organization's response to a security event from detection to resolution. If an organization has sound risk management policies in place they will be much better prepared to respond to an incident. Think about it: if an organization has studied a threat ahead of time and determined that a certain threat has a high likelihood of occurring then that organization can take steps to mitigate the impact that the threat will have on the business once it’s been realized. Proper preparation, via sound risk management policies, will make the incident response process much smoother. It’s like a football game. If a coach studies the opponent ahead of time he will understand the strengths that the opposing team has. He will know who the best players are, what actions the quarterback will take during play, how his opponents run their offense and defense, etc. If that coach decides not to prepare for his opponent ahead of time then he will face an unknown threat. He won’t know

who his opponents best players are or what plays they like to run. The coach and his football team will be running blind.

The same is true for attacks in the world of information security. If an organization studies its attack surface and identifies a threat that has a high likelihood of occurring, a threat that would be impactful, that organization can take steps to harden their security posture ahead of time, study the impact that the threat has had on other organizations, and even plan their potential incident response ahead of time (at least partially). Taking proactive measures better prepares the organization ahead of time to mitigate the potential threat. Being proactive also reduces the severity of the impact that the threat has on an organization, thereby significantly reducing the potential impact and damage to said organization. If an organization fails to implement sound risk management practices they will not be prepared to respond to a threat and the impact of that realized threat will be severe. Possibly a threat could be severe enough that the organization is unable to conduct business for a period of time, potentially even permanently.

As we can see it's important to understand the relationship between risk management and incident response. Understanding this relationship can encourage organizations to be proactive in their risk management practices so that they are prepared to respond to an incident when one occurs. It seems that we are hearing about new cyber attacks on a daily basis. Many of these attacks are entirely preventable and are often the result of poor risk management practices. If more organizations would practice sound risk management then they would be better prepared to respond to incidents and these attacks would be less severe. Organizations would not be caught flat footed when they are responding to an attack. Preparation can save an organization from lots of headaches, but a lack of preparation can doom an organization. This preparation, from proper

risk management, leads to an incident response that is knowledgeable about threats and better able to respond to them.

Preparation is key. One concept done thoroughly, risk management, makes the other concept, incident response, smoother and more effective when the time comes to respond to a threat that has been realized. Understanding this relationship is key to sound information security management.

Bibliography

Luttgens, Jason, Matthew Pepe, and Kevin Mandia. *Incident Response and Computer Forensics.* New York, McGraw-Hill, 2014.