

“Five Mistakes of Incident Response”

Anton Chuvakin, Ph.D., GCIA, GCIH, GCFA

All organizations have to care about security incident response! Unlike detection and prevention, the response is impossible to avoid. While it is not uncommon for the organizations to have weak prevention and detection capabilities, response will have to be there since the organization will often be forced into response mode by the attackers (be it the internal abuser, omnipresent ‘script kiddy’ or the elusive ‘uber-hacker’). The organization will likely be made to respond in some way after the incident has occurred.

This article presents five mistakes that companies make regarding security incident response.

1 Not having a plan

The first mistake is simply not creating an incident response plan before incidents start happening. Having a plan in place (even a plan that is not well-thought) makes a world of difference! Such plan should cover all the stages of incident response process from preparing the infrastructure to first response all the way to learning the lessons of a successfully resolved incident.

If you have a plan, then after the initial panic phase, (‘Oh, my, we are being hacked!!!’) you can quickly move into a set of planned activities, including a chance to contain the damage and curb the incident losses. Having a checklist to follow and a roster of people to call is of paramount importance in a stressful post-incident environment.

To jump-start the planning activity one can use a ready-made methodology, such as SANS Institute 6-step incident response process (described here <http://www.sans.org/sans2005/description.php?cid=437> and in other SANS materials). With a plan and a methodology your team will soon be battle hardened and ready to respond to the next virus faster and more efficiently. As a result, you might manage to contain the damage to your organization.

2 Failing to increase monitoring and surveillance

The second mistake is not deploying increased monitoring and surveillance after an incident has occurred. This is akin to shooting yourself in the foot during the incident response. Even though some companies cannot afford 24/7 security monitoring, there is no excuse for not increasing monitoring after an incident has occurred.

At the very least, one of the first things to do after an incident is to crank up all the logging, auditing and monitoring capabilities in the affected network and systems. This simple act has the potential to make or break the investigation by

providing crucial evidence for identifying the cause of the incident and resolving it. It often happens that later in the response process, the investigators discover that some critical piece of log file was rotated away or an existing monitoring feature was forgotten in an 'off' state. Having plenty of data on what was going on in your IT environment right after the incident will not just make the investigation easier, it will likely make it successful.

Another side benefit, is that increased logging and monitoring will allow the investigators to confirm that they indeed have followed the established chain of custody (explained here http://en.wikipedia.org/wiki/Chain_of_custody as “document or paper trail showing the seizure, custody, control, transfer, analysis, and disposition of physical and electronic evidence.”)

#3. Being unprepared for a court battle

The third mistake is often talked about, but rarely avoided. Some experts have proclaimed that every security incident needs to be investigated as if it will end up in court. In other words, maintaining forensic quality and following the established chain of custody needs to be assured during the investigation.

Even if the case looks as if it will not go beyond the suspect's manager or the human resources department (in the case of an internal offense) or even the security team itself (in many external hacking and virus incidents), there is always a chance that it will end up in court. Cases have gone to court after new evidence was discovered during an investigation, and, what was thought to be a simple issue of inappropriate Web access became a criminal child pornography case.

Moreover, while you might not be expecting a legal challenge, the suspect might sue in retaliation for a disciplinary action against him or her. A seasoned incident investigator should always consider this possibility.

In addition, following a high standard of investigative quality always helps since the evidence will be that much more reliable and compelling, if it can be backed up by a thorough and well-documented procedure.

#4. Putting it back the way it was

The fourth mistake is reducing your incident response to "putting it back the way it was". This often happens if the company is under deadline to restore the functionality. While this motive is understandable, there is a distinct possibility that failing to find out why the incident occurred will lead to repeat incidents, on the same or different systems.

For example, in the case of a hacking incident, if an unpatched machine that was compromised is rebuilt from the original OS media, but the exploited vulnerability is not removed, the hackers are very likely to come back and take it over again. Moreover, the same fate will likely befall other exposed systems. Thus, while returning to operation might be the primary goal, don't lose sight of the secondary goal: figuring out what happened and how to prevent it from happening again. It feels bad to be on the receiving end of the successful attack, but it feels much worse to be hit twice by the same threat and have your defenses fall in both cases.

Incident response should not be viewed as a type of "firefighting" although you'd fight plenty of fires in the process. It can clearly help in case of a fire, but it can also help prevent fires in the future.

#5. Not learning from mistakes

The final mistake sounds simple, but it is all too common. It is simply not learning from mistakes! Creating a great plan for incident response and following it will take the organization a long way toward securing the company, but what is equally important is refining your plan after each incident, since the team and the tools might have changed over time.

Another critical component is documenting the incident as it is occurring, not just after the fact. This assures that the "good, the bad and the ugly" of the handling process will be captured, studied and lessons will be drawn from it. The results of such evaluations should be communicated to all the involved parties, including IT resource owners and system administrators.

Ideally, the organization should build an incident-related knowledge base, so that procedures are consistent and can be repeated in practices. The latter is very important for regulatory compliance as well and will help satisfying some of the Sarbanes-Oxley requirements for auditing the controls to information.

[Anton Chuvakin, Ph.D., GCIA, GCIH, GCFA](#) is a Security Strategist with netForensics, a security information management company, where he is involved with designing the product, researching potential new security features and advancing the security roadmap. His areas of infosec expertise include intrusion detection, UNIX security, forensics, honeypots, etc. He is the author of a book "Security Warrior" (O'Reilly, January 2004) and a contributor to "Know Your Enemy II" by the Honeynet Project (AWL, June 2004) and "Information Security Management Handbook" (CRC, April 2004). In his spare time he maintains his security portal <http://www.info-secure.org>