IBM Global Technology Services
Security Services

Building a security incident response plan that works

A look at the top ten CSIRP (Computer Security Incident Response Plan) mistakes

IBM

Highlights

- Security breaches are virtually inevitable, and can involve thousands of data records while costing millions of dollars
- A Computer Security Incident Response Plan, or CSIRP, can help reduce the cost and mitigate the severity of breaches
- Based on experience working with hundreds of companies of all sizes, IBM offers advice for building and maintaining an effective CSIRP

Understanding the high cost of security failures

Global enterprises with hundreds of thousands of employees, small companies doing business on the web and public sector organizations of any size all have one thing in common: your networks are under almost continual attack, and your enterprise systems are at risk as well. Moreover, it is virtually inevitable that you will suffer a security breach at some point.[1]

How damaging that breach will be is influenced by many factors—one of the most important being your own preparedness. According to Ponemon Institute, having a Computer Security Incident Response Plan (CSIRP) in place is second only to a strong security posture in reducing the cost of a data breach.[2]

As a cornerstone of your defense against hackers, malware, human error and a host of other threats, a CSIRP is the map that guides your response to a successful attack. It should define the roles and responsibilities of all respondents, establish authority for making major decisions and define communications flows and notification procedures. Without a CSIRP, your incident response team can waste invaluable time and resources in figuring out what to do—leading to potentially higher costs and greater damage to your organization and your reputation.

Developing an effective incident response plan

While the basic components of a CSIRP are straightforward, crafting an effective plan requires balancing thoroughness and usability. Given the rapidly evolving threat landscape, it is not possible to build a plan that can address every potential attack—nor would you want a document that detailed and complex. Instead, you want to build flexible guidelines that can be quickly and easily applied to any type of incident.

The worst time to find out that your CSIRP is flawed is when you are in the middle of an emergency. In helping clients respond to declared incidents, IBM security experts on our Emergency Response Service teams have been able to observe what works well in a CSIRP and what does not. In this paper we share the ten most common shortcomings of CSIRPs we encounter and how you can avoid these potentially costly mistakes.

1 Making a CSIRP too complex

When designing your CSIRP, it is best to keep in mind that the audience will be reading the document during a crisis. There will be stress, chaos and, of course, urgency. Some individuals will be panicked and worried about their jobs. Executives who may or may not understand the fine technical points of what is happening will be distressed if the news media is asking questions.

CSIRPs must be crisp, clear and concise. If an employee who is unfamiliar with the document cannot quickly examine the processes described within the CSIRP, understand the chain of command and perform the necessary actions, your CSIRP may be too complex. Of course, making a CSIRP too simple is also a potential pitfall; striking the right balance between brevity and actionable direction is essential to a successful CSIRP.

Having an incident response plan in place saved U.S. organizations on average USD1.2 million per data breach in 2013.[3]

2 Overloading key personnel

Every organization has a "Joe." Joe knows everybody and every system, router, cable and coffee machine in the building. Joe is the person to whom we all look during an incident. Joe, undoubtedly, is the best person around for minor incidents and can handle them from beginning to end. When we develop CSIRPs for our customers, we quickly find the "Joe" of the organization during our standard questioning: Who is in charge of anti-virus? Joe. Who takes the lead on technical response? Joe. Who communicates with executives and regulatory authorities? Joe.

Joe is fantastic at what he does during the regular workday. However, when an incident stretches on for multiple shifts or even days, Joe can't be your go-to guy for 72 hours straight. Separating duties during an incident and distributing them across designated, trained staff is necessary if an organization does not want sleep-deprived, overloaded—and thus less effective—employees responding to incidents.

3 Treating incident response as a serial process

During a large-scale incident, multitasking is essential. Managers who look at incident response as a serial process are doomed to failure when it comes to resolving an incident in a timely manner. While each incident is unique, all incident responses are comprised of a number of short-term efforts. Pushing out new anti-virus signatures, patching systems, leading investigative efforts, informing employees and customers of your current status, fetching additional supplies of caffeinated beverages and other important tasks are all individual processes and should be treated as such. A common failure is focusing on only one of these tasks at a time and neglecting other important tasks that should be completed in parallel.

4 Failing to establish proper lines of communication

When responding to an incident, potentially many different individuals and vendors will be asked to assist. The individual responsible for managing the "'boots on the ground"—the incident manager—must be a master communicator. Communication must be orderly, efficient and follow the proper channels to ensure that all parties involved in the response are kept informed and coordinated. Within an organization, this could include technical teams as well as those responsible for physical security, human resources, compliance, regulatory affairs and risk management. External communications are also crucial, requiring that someone is clearly designated as responsible for providing timely and factual updates to your organization's public relations, media relations, customer affairs and marketing focal points. Many an organization has damaged the trust of stakeholders by failing to communicate quickly and openly about security incidents.

5 Focusing on what's easy, not what needs to be done

During almost every incident, the urge arises to focus on the easy tasks versus what needs to be done. This is akin to filling up the window washer fluid on a car when the engine won't start. While resolving a security incident, it is tempting to focus too heavily on easy tasks like static evidence gathering—for example, capturing hard drive images—rather than challenging tasks like performing analysis. But regardless of difficulty, all tasks need to be completed. Failing to focus your energy on the essential problems, whether easy or hard, will only cause prolonged headaches and prolonged incidents.

At least 50 percent of the CSIRPs evaluated by IBM security consultants show no evidence of a formal document lifecycle or a history of continual revisions.

6 Focusing on what's interesting, not what needs to be done

During some incidents, the responder will discover some bits of interesting information and become focused on a chase down an unrelated path. A common source of diversion is finding inappropriate user activity such as browsing sites that are off limits. This newly discovered information may be extremely captivating, but if it does not play a material role in the incident you are investigating, it should be set aside for later research. Endless hours can be spent on this sidetrack, consuming time that you can't afford to lose. Stay focused on resolving the incident and save the exploration for later.

Advice from IBM for first responders

Keep these dos and don'ts in mind when a security incident is declared.

DO:

- Consult and follow your organization's CSIRP
- Gather incident intelligence from multiple sources
- Ensure the proper people are involved
- Begin taking thorough first responder notes
- Activate one-time-only Incident Responder credentials
- Collect volatile data and pre-determined log files
- Safeguard systems and media for forensic investigation
- Collect network-based logs for future analysis

DON'T:

- Panic or react without a plan
- Discuss the incident with others unless directed
- Shut down, power off or back up affected systems
- Remotely access systems unless necessary
- Use common privileged domain credentials
- Install or execute any software on the systems
- Conduct anti-virus or similar scanning processes
- Attempt to retaliate against perpetrators

---

7 Abandoning the CSIRP

The urge will occasionally arise to throw out the CSIRP because it doesn't address the specific situation at hand. There is a reason why the document does not address the latest email virus or Trojan horse. The CSIRP is not meant to be an all-inclusive guide on how to confront every specific type of incident; rather, the document is a blueprint for lines of communication, roles, required notifications and steps to be taken to respond to any security breach.

Although each incident is entirely unique, a flexible and well-constructed CSIRP will allow for a response to be formulated quickly by identifying the key people who should be included, their roles, and your communication protocols. With this structure in place, the necessary steps may then be taken to address the technology behind the incident at hand.

8 Making a policy, not a plan

Always remember that the "P" in CSIRP stands for "Plans" not "Policy." Occasionally, IBM reviews a CSIRP that reads more like a policy document rather than a plan. What is the difference? A plan comprises actionable steps and roles while a policy states overarching guidelines to be applied within the organization. When an incident occurs, do you really want to be reading company policy in order to formulate a plan? Of course not. You would like a well thought out plan that tells you what to do.

9 Failing to assign an owner and keep the plan up to date

Your CSIRP has a lot in common with your garden. Both develop over time, require maintenance and attention, and should have owners responsible for their well-being. When you establish a CSIRP, an owner should be assigned to the document. This means a specific person, not a department or a position, is tasked with maintaining the document, ensuring that the personnel and procedures contained within are still relevant, and coordinating annual testing.

Without a specific owner, the document may languish, becoming stagnant and possibly causing increased response times to incidents. Moreover, to be effective, this person needs to have executive support for the ownership role or be in a high enough position to allocate resources for testing and updating.

A CSIRP should be updated regularly, at least twice a year, as well as after significant events such as completion of a merger or acquisition, major infrastructure or personnel changes, or a cyber security incident. On average in working with clients, we see CSIRPs being updated every 18 to 24 months—although in our experience it is not uncommon to see a CSIRP that has not been updated in five years. In the eventuality that an incident occurs, this out-of-date document is brought out, dusted off and the response team quickly finds that key personnel named in the plan are no longer with the company or have moved to other roles. The unfortunate end result is a delay in response—with potentially significant consequences.

10 Skipping the incident closeout process

The most valuable lessons from any incident can be learned from the after-action review. Prior to an incident being officially closed, the best practice is to hold a lessons-learned meeting where you can evaluate the effectiveness of the CSIRP (how well did it work?) and document a root cause as well as other findings.

Even if it seems like everything went as planned during an incident, it is likely that an after-action review will nevertheless bring potential improvements to light. Identifying mistakes or issues that need to be changed will only make the CSIRP stronger and more able to address your needs during future incidents. Although your response team may be eager to put the past behind them and return to normal operations, this final step should not be neglected—it is often the most important part of the incident response process.

How sound is your CSIRP?

Does your organization have a formal, documented Computer Security Incident Response Plan—and if so, when is the last time your CSIRP was updated? If your answers are anything other than "yes" and "within the last six months," you'd probably benefit from talking to an IT security expert from outside your company.

At IBM, we can help clients evaluate and improve an existing CSIRP or help you build a custom plan from the ground up. You can get started with a high-level assessment for a modest investment and, based on our findings and recommendations, decide on your next steps. This work is performed by the same security experts from the IBM Emergency Response Service team who work hand in hand with clients during actual incident response engagements. We base our CSIRP best practices on industry standards such as NIST (National Institute of Standards and Technology), ISACA (Information Systems Audit and Control Association), IETF (Internet Engineering Task Force) and ISO (International Organization for Standardization).

In case of emergency, call 1-888-241-9812

IBM Emergency Response Service (ERS) is staffed 24x7x365 by teams of incident response and computer forensic experts ready to respond globally to security incidents. ERS teams are seasoned in confronting threats facing our clients, such as zero-day malware, network intrusions and other advanced security threats.

If you are facing a serious security concern and require immediate assistance, please call the ERS hotline at: 1-888-241-9812 or +001-312-212-8034

For more information

To learn more about how IBM can help protect your organization from cyber threats and strengthen your IT security position, contact your IBM representative or IBM Business Partner, visit this website:
ibm.com/services/security

To learn more about the data breach epidemic and what you can do to prevent and respond to incidents, visit this website:
ibm.com/services/us/en/it-services/data-breach/index.html

Follow us on:



IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
January 2014

[1] IBM, *IBM Security Services Cyber Security Intelligence Index*, June 2013.

[2,3] Ponemon Institute, 2013 Cost of Data Breach Study: Global Analysis, Benchmark research sponsored by Symantec and independently conducted by Ponemon Institute, May 2013.

Please Recycle

SEE03005-USEN-01