A Guide for Aspiring CISOs to Have the Ability to Prioritize and Triage Incident Response and Vulnerability Remediation in a Calm, Balanced Manner

ISM 6100 Group Project

Authors:

Chris Jarko, csjarko@yahoo.com

John Dittmer, jdittmer@prosol1.com

Advisor: Stephen Northcutt

Abstract

Incident response and triage is possibly the most stressful situation a Chief Information Security Officer (CISO) can face, yet the CISO must remain calm. The surest way to remain calm is to be prepared; the CISO must start with a sound approach to risk management, and knowledge of their enterprise's networks, sensitive data, and key people. Techniques and procedures for incident handling must be documented in plans and policy and rehearsed on a regular basis. Also, the CISO must build (or outsource) an incident response team with the right mix of skills and experience. After an incident (or audit), the CISO will undoubtedly be left with a list of vulnerabilities to mitigate. This mitigation effort will require the CISO to make prioritization recommendations to senior executives and must maintain a balance between securing the enterprise and ensuring the enterprise can still meet the organization's business needs.

How to Prioritize and Triage Incident Response and Vulnerability Remediation (In a Calm, Balanced Manner)

First things first: Stay Calm. Relax. Focus. Breathe. You got this…

As the CISO, you are responsible for making sure cyber incidents are handled completely and immediately. You might even be required to personally lead the effort if your Information Security department is small. But how does one efficiently lead an incident response, especially if it's the first time? Effective leadership, no matter the context, requires the individual in charge to remain calm. Calm comes from confidence, and confidence comes from preparation. This section will show aspiring CISOs how to prepare for incidents, as well as the vulnerabilities that will inevitably become revealed by them.

Start with a sound foundation.

To be successful in a crisis, any leader must rely on a sound foundation. While crisis situations will often require flexibility and even creativity in solving problems, the foundation of any information security program is its overall approach to risk. This approach is not just a methodology for categorizing risks, vulnerabilities, and threats – although that is indeed a critical part of it. Rather, the organization's risk management approach should be a manifestation of its risk appetite. The CISO and the rest of the organization's executives must clearly understand and share this appetite. With a common understanding of how much risk the organization is willing to accept, the CISO can rest assured that their best efforts will be in line with the organization's goals, and can function on the task at hand.

Beyond that, there are a few key elements to any successful incident response program. Sharita Knight, Incident Response Lead at a major U.S. Department of Defense agency, offered this: "There were three things we needed to have: First, you have to know your network." Knowing your network, both its hardware and software, is so important that the Center for Internet Security (CIS) lists this knowledge as the top two of its 20 Critical Security Controls for Effective Cyber Defense (Center for Internet Security, 2016). "Second, you need to have your procedures down," Sharita continues, "Not only what each of your team members need to do, but who you need to report to, and who you need information from. Third, you need the right mix of skills on your incident response team. Initial responders, malware reverse engineers, network experts, forensics people – a broad mix that can handle all aspects of the situation. Once we had all three of those things, I felt a lot less stress going into incident response situations (Knight, 2016)."

Have a plan, and rehearse it regularly.

Many excellent classes teach incident response, such as the SANS Institute's SEC 504, *Hacker Tools, Techniques, Exploits and Incident Handling*. Regardless of where you turn for instruction, incident handling typically boils down to six phases. SANS identifies these as: *Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned* (Skoudis & Strand, 2015); following this sequence will serve you well. The actual technical means of incident response are beyond the scope of this guide, so our discussion will be primarily limited to the first phase: Preparation. Preparation means much more than identifying who will be on the incident response team, where they will work, how they will communicate (and how you will communicate to your senior executives), what equipment they will use, and other practical aspects of responding to a cyber breach. It also means documenting these preparations in writing as an organizational policy, but perhaps more importantly, in an actual incident response plan, or IRP.

Having an IRP is critical. While it may only serve as a point of departure the first time it's executed in earnest, having the plan captured in writing and approved at the highest level possible will provide assurance of executive buy-in. This buy-in will become crucial during the incident response when it's time to lock down specific user accounts or possibly even work with law enforcement officials should criminal prosecution become necessary. Moreover, restricting knowledge of ongoing incident investigations is essential in cases of employee misconduct, i.e., "insider threat" scenarios. This secrecy, as well as other actions resulting from the investigation, will inevitably lead people to gossip. Support from other C-level executives and Directors (who were consulted during plan approval) can help tamp down the firestorm of loose talk which could otherwise only complicate your efforts.

Creating this plan from scratch may seem like an overwhelming task, but fortunately, there are many places to turn for help. Several U.S. Government agencies have published or are in the process of publishing guidance on preparing for and responding to cyber incidents. Some of these, such as the one produced by U.S. Department of Justice's Cybersecurity Unit, are very broad-based and easily digestible (U.S. Department of Justice, 2015). The recommendations made in this document are very sound (the document itself is titled "Best Practices for Victim Response and Reporting of Cyber Incidents"), but these recommendations are given more at the "macro" level. At the other end of the spectrum, the National Institute of Standards and Technology (NIST) recently published the second revision to its Special Publication 800-61 (NIST SP 800-61 Revision 2). This 79-page document, written for CISOs and CIOs, contains more detailed information on how to create an incident response team, planning and rehearsing for cyber incidents, and there is even a checklist for incident response (National Institute of Standards and Technology, 2012).

Practicing your plan: War Gaming

But simply having an approved plan on the shelf is not enough. Ideally, the plan should be read by all members of the incident response team at least quarterly and should be practiced at least every six months, incorporating lessons learned into a revision of the plan. This schedule of reading, rehearsal, and revision is more demanding than it may sound, but there are very meaningful reasons for this. First, cybersecurity professionals often have high turnover rates (Seals, 2016); if a CISO is not careful, he may find himself with a response team made up of individuals who have never seen the IRP until they are required to execute it in a real-world situation. Second, the technical skills used during incident handling are not necessarily the same as those used to architect a secure network or to perform continuous monitoring. Incident handling requires expertise in such things as digital forensics and evidentiary procedures, which are not necessarily a standard part of cybersecurity coursework. Finally, networks change over time. A change in architecture may require a modification in the tools used during incident handling, or at the very least, the information security team must understand the effect their tools may have on the network. Breaches are bad enough; a self-induced Denial of Service is obviously something to be avoided. By rehearsing regularly, your incident handling team will gain confidence in their ability to perform, and their confidence will inspire you as well. You will project this confidence to your superiors in the way you carry yourself during the crisis and will make it easier for you to request financial support for any needed fixes once the crisis is over.

These incident rehearsals do not necessarily need to involve physically going through the steps of deploying the incident response team and their gear, although that is a good idea to do after the IRP is initially published, as well as after any major revision. A physical walk through can highlight deficiencies in planning, such as not having enough computer cables or hard-cases to transport the team's gear to the site of an incident. Once you have physically validated your incident response plan, you can conduct the majority of your plan rehearsals on paper, in the form of a "War Game." A War Game (usually called a Table Top Exercise or “TTX” in U.S. Government circles) is typically conducted in an informal setting and led by a facilitator (U.S. Department of Homeland Security, 2016). War Game participants should include everyone with a role in your incident response plan. (Executing a cyber incident response presumes there is a "victim" in your organization. This individual can be represented by either the War Game facilitator or by another member of your enterprise.)

During the War Game, the facilitator uses a predetermined scripted scenario, presenting information as it would appear chronologically during a real cyber incident. As each piece of the event is revealed, War Game participants discuss how they would respond and can ask questions of others. This cross-talk not only helps validate your incident response plan but also helps create a uniform level of shared situational understanding among the players in a real cyber incident.

A word of advice on choosing a facilitator: Many organizations find it beneficial to hire a facilitator from outside the organization. Warren Fish, a Manager of IT Audit, suggests that this has been a “Best Practice” for his organization. A third-party facilitator can be impartial and is less likely to be intimidated by your Executive or Senior Vice Presidents, or other senior executives such as the COO or CEO (Fish, 2016).

Executing your plan: Triaging cyber incidents.

Once you have built your incident response team and written and rehearsed your incident response plan, you will be as prepared as any CISO can be during a cyber incident. From there it is a question of when (not "if") you will need to execute your plan. But what if your incident response is triggered by multiple indications? This scenario is not as unlikely as it may seem; sometimes an organization doesn't realize its enterprise is under attack until several cybersecurity events are correlated. If this is the case, you may find yourself in a situation where the incident exceeds your incident handling capacity, and you must prioritize your team’s actions.

As with risk management in general, there are several approaches to this task, and CISOs should not feel the need to “reinvent the wheel.” The U.S. Government has published several invaluable guides on the subject of incident prioritization. One such guide is the National Cybersecurity and Communications Integration Center (NCCIC) Cyber Incident Scoring System (NCISS). The NCCIC, the cybersecurity operations center of the U.S. Department of Homeland Security, based the NCISS on NIST SP 800-61r2, so there is a natural tie-in, should you choose the NIST SP as the basis for your incident response program. The NCISS uses weighted mathematical scores to prioritize incident handling, but "is *not* [emphasis in original] intended to be an absolute scoring of the risk associated with an incident" (United States Computer Emergency Response Team, 2016).

There are other resources available to the aspiring CISO. In 2014, researchers from the (U.S.) Naval Research Laboratory (NRL) published "*A Framework for Event Prioritization in Cyber Network Defense*." This framework is focused on determining the potential damage caused by a given event and uses several complex mathematical equations to arrive at an answer (Kim, Kang, Luo, & Velazquez, 2014). Outside of the U.S. Government, the International Organization for Standardization (ISO) produced a standard for Information Security Management, ISO 27001. Within the ISO 27001 standard is an appendix for Information Security Incident Management, Appendix A.16 (Kosutic, 2016).

Whichever of these resources you use, you should understand that there will always be some degree of subjectivity involved since you must prioritize your organization's sensitive data. Regardless of what this sensitive data is – intellectual property such as trade secrets, financial data, credit card numbers, or patient health records – this data requires more protection. Also, there is no "one size fits all" answer. Each organization is different, and what works well for one might not work at all for another. Still, if your incident response capability is based on a sound framework, documented in plans and policy, and practiced and understood by all involved, you will be in a better position to handle a breach.

Another key factor in your decision process will be how your organization classifies its sensitive data. Having a multi-tiered classification scheme will allow you to use weighted criteria to prioritize your actions. In many cases following a cyber incident, an organization might not know exactly what information has been exfiltrated from their enterprise; they only know that a data breach has occurred. Data classification groups information by how much risk an organization incurs with its loss and provides a scheme for segmenting the network. Armed with the knowledge of where different classifications of information are stored on the network, you can evaluate the *apparent* risk to your organization based on the initial details of a particular cyber incident. The term "apparent" is used here because the *actual* risk can't be fully appreciated until you understand the full scope of a breach. Still, you can use the following question as a quick litmus test: "What can I do to avert as much damage to my company as possible?" Until a breach is contained and its source eradicated, reduction of risk will almost certainly outweigh any other considerations, with the possible exception of a complete denial of service.

One final note on incident response capabilities: There is another option to consider with regards to your incident response team. Many organizations outsource their incident response to third-party Managed Security Service Providers such as Solutionary or Verizon Enterprise. Warren's employer, a global provider of electronic payment and banking solutions, also outsources its incident response capability. "We lack the staff capabilities," he said, and outsourcing your incident response is "way cheaper." (Fish, 2016)

Remediating vulnerabilities: Balancing risk with security.

Once the dust has settled after an incident response, an enterprise is often faced with previously undiscovered vulnerabilities. In all likelihood, however, most of the vulnerabilities on your enterprise's IT will have been identified through your IT audit program. Whichever the case, these vulnerabilities need to be remediated. In a perfect world, these remediation efforts will fit within your department's budget and won't adversely impact your enterprise's operations. Unfortunately, we do not live in an ideal world, and you will almost certainly have to prioritize your department's time and money to get the best return on investment. Here are some thoughts on how to approach this:

They've already stolen your data.

The easiest decisions will probably come about as the result of a breach. Being able to show the Board of Directors the tangible effects of cybersecurity vulnerability couches your remediation efforts in terms all non-IT executives understand: impact to the bottom line. Moreover, the immediacy of the breach will probably heighten emotions as well. Use this to your advantage, but do not abuse it. If you use a security breach as justification for money and personnel to fix *all* of your problems, you probably won't get what you ask for, and you may engender mistrust of your efforts and motivations in the future. In the aftermath of a breach, do your due diligence to uncover the root cause of the breach and solicit your leadership's support to fix the problem. If there are underlying deficiencies that indirectly but *legitimately* contributed to the breach, it is fair to ask for help on these also, but it is a very prudent idea to have supporting evidence when you make your pitch to the Board.

Some problems can't be fixed right away.

Sometimes, vulnerabilities may arise from the use of legacy hardware or beyond end-of-life software. While this may seem like a simple problem, often an immediate upgrade is not possible. One possible scenario is this:

Your company uses a proprietary software solution for a critical business process. This software is only compatible with Windows XP, which is no longer supported with security updates. You can't stop using the software right away because stopping this business process means stopping all business operations, and your company will go out of business. As it turns out, this particular software application is Internet-facing, and also touches one or more internal servers, so you can't isolate it from the rest of your network or the Internet. The application developers can rewrite (i.e., "port") the application to run on a modern version of Windows, but that will take a significant amount of time, since the original developer (the only person who truly understands how the application works) retired years ago and is no longer available.

In the scenario above, the only things you can do are: a) Increase monitoring of traffic to and from the proprietary software (i.e., place additional security controls to reduce risk by decreasing your detection time); and b) Direct the owner of the affected business process to come up with a "get well" plan and a timeline to port the software to run on a fully-supported operating system. (If you do not have the authority to direct this, escalate the matter to somebody who does.) Once the timeline is established, the residual risk is accepted (often called a "risk exception" in audit terms) and is "out of scope" for further audit and vulnerability assessment until the end of the timeline. The only action remains for you to do is to ensure the additional monitoring is accomplished and track the timeline to make sure the original problem is not "forgotten" (Fish, 2016).

Some things will get you (or your boss) fired, or worse.

Sometimes the nature of your business will require compliance with certain regulatory frameworks, such as the Payment Card Industry Data Security Standard (PCI-DSS). PCI-DSS applies to “any organization, regardless of size or number of transactions, that accepts, transmits or stores any cardholder data.” Fines for non-compliance with PCI-DSS can be “catastrophic” (Control Scan, Incorporated, 2016). This being the case, you probably won’t have to wait for a breach to get what you need to fix the problem. If an internal audit identifies a vulnerability that makes your organization non-compliant with any applicable data security standard (PCI-DSS or otherwise), remediate that vulnerability immediately.

Not all vulnerabilities are created equal.

Vulnerability scanning is an essential part of any worthwhile IT audit program. There are numerous tools for this, both open source and commercial. Some vulnerability scanners also perform asset discovery, making them an excellent choice if you do not already have a good baseline of your enterprise (Fish, 2016). All scanners categorize vulnerabilities, either in terms of severity or risk. While these categories are not perfect, they do provide the best means for prioritizing vulnerabilities not already identified as a risk exception. Start at the top of the list and work your way down. For each item on the list, collaborate with the affected system and business process owners to assess whether to remediate the vulnerability or accept the risk in order for your organization to function. It's important to note here that as the CISO, you won't be the one making the final decision. Your responsibility will be to make the business owner aware of the risk, and to document it.

An endless task?

As a new CISO, you might not have ever seen the results of a vulnerability scan. The results may shock you; it is not uncommon for vulnerabilities to number in the thousands, tens of thousands, or even more for a large enterprise. There will be one item for each *instance* of a vulnerability, meaning that if there is a vulnerability on a particular version of the Windows 7 OS, and you have a thousand hosts running that version, you will have a thousand items on the scan report just from that one issue. These one thousand items can be treated as one issue for remediation purposes, and will effectively reduce the number of vulnerabilities needing prioritization. Excluding vulnerabilities for which there is a documented risk exception will further lessen the number. Also, you may find a number of vulnerabilities pertaining only to a specific segment of your network, such as software development. An examination of the vulnerabilities and network segment in question may generate a high number of risk exceptions, reducing your list even more. Ultimately, however, it is unlikely you will ever remediate (or make a risk exception for) everything on your list. Your goal should be to reduce your list to a level that is manageable both in terms of your information security program's capacity as well as in terms of risk to your organization's business operations. If you find that difficult to accept, remember this: Your organization doesn't exist solely for the purpose of keeping its information secure. It exists to provide a service or produce a product.

A final note on remediation: It's not just about the hardware and software.

There is more to an IT audit than vulnerability scans. An audit identifies and reports on risk to the enterprise. Much of this risk comes from vulnerabilities in hardware and software, but there is another significant source. The people operating the systems and the processes they use can't be fixed with a hardware upgrade or software patch. Human-induced risk must be mitigated through clear and concise policy and procedures. Furthermore, these policies and procedures must be kept up to date and published so the people in your organization can understand and follow them. As with risk exceptions, the CISO won't be the final authority; rather, as your organization's top information security professional, your input will be critical in formulating policies and procedures that are both realistic and reasonable.

Conclusion

Being the CISO during an incident response situation is nerve-wracking, but the stress can be managed through diligent preparation. Know the enterprise, build (or outsource) a competent incident response team, and capture incident response procedures in officially approved plans and policy. All of these things will help the CISO make the right prioritization decisions during an incident. After an incident (or even after an audit), there will almost always be more vulnerabilities than resources to remediate or mitigate them. Recognizing the vulnerabilities will also force prioritization decisions, and a CISO must also weigh the need to secure the enterprise with the business requirements of the organization. The decision calculus for this is never simple, but such things as taking a practical approach to what can and cannot be done, grouping vulnerabilities by network segment (when possible), and external factors such as compliance requirements can help the CISO make recommendations that allow senior executives to make informed decisions about risk.

References:

Center for Internet Security. (2016, August 31). *CIS Controls for Effective Cyber Defense.* Retrieved from Center for Internet Security Web site: https://www.cisecurity.org/critical-controls.cfm

Control Scan, Incorporated. (2016, December 17). *Frequently Asked Questions*. Retrieved from pcicompliance.org Web site: https://www.pcicomplianceguide.org/pci-faqs-2/#1

Fish, W. (2016, December 15). Interview with Warren Fish. (C. Jarko, Interviewer)

Kim, A., Kang, M., Luo, J., & Velazquez, A. (2014). *A Framework for Event Prioritization in Cyber Network Defense.* Washington, D.C.: Naval Research Laboratory.

Knight, S. (2016, December 13). Interview with Sharita Knight. (C. Jarko, Interviewer)

Kosutic, D. (2016, December 11). *Overview of ISO 27001:2013 Annex A*. Retrieved from ISO 27001/ISO 22301 Knowledge base : http://advisera.com/27001academy/knowledgebase/overview-of-iso-270012013-annex-a/

National Institute of Standards and Technology. (2012, August). *NIST SP 800-61 Revsion 2, Computer Security Incident Handling Guide.* Retrieved from NIST Publications: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Seals, T. (2016, December 10). *High Cybersecurity Staff Turnover is an 'Existential Threat'*. Retrieved from Infosecurity Magazine: http://www.infosecurity-magazine.com/news/high-cybersecurity-staff-turnover/

Skoudis, E., & Strand, J. (2015, June). Incident Handling. *Hacker Tools, Techniques, Exploits & Incident Handling*. Bethesda, Maryland: The SANS Institute.

U.S. Department of Homeland Security. (2016, December 11). *Exercises*. Retrieved from Ready.gov: https://www.ready.gov/business/testing/exercises

U.S. Department of Justice, C. U. (2015, April 30). *Best Practices for Victim Response and Reporting of Cyber Incidents.* Retrieved from U.S. Department of Justice Web site: https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/04/30/04272015reporting-cyber-incidents-final.pdf

United States Computer Emergency Response Team. (2016, June 6). *NCCIC Cyber Incident Scoring System.* Retrieved from US-CERT Web site: https://www.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System

Checklist: Incident response and vulnerability remediation prioritization

- Know your organization's approach to risk acceptance and its risk appetite, and make sure your bosses share the same understanding.
- Know your enterprise:
  - Hardware
  - Software
  - Sensitive Data (and how your organization classifies it)
- Have clear procedures for incident response:
  - Individual responsibilities
  - Reporting responsibilities and data sources
- Have the right mix of skills on your incident response team, or consider outsourcing incident response altogether.
- Document your incident response procedures in an Incident Response Plan (IRP).
  - If necessary, refer to external guidance for suggestions:
    - U.S. Government
    - Industry best practices
  - Conduct at least one physical walkthrough of your IRP.
  - Have all incident response team members read the IRP quarterly.
  - Validate your IRP with an incident response War Game every six months.
    - Use a facilitator, ideally from an external source.
    - Conduct an out-of-cycle War Game after any significant changes to your IT architecture.
  - Incorporate lessons learned (either from War Games or real-world incidents) into your IRP.
- Choose a method for incident prioritization.
  - Examples: NCISS, ISO 27001, etc.
  - Modify as necessary based on lessons learned and evolving best practices.
- Prioritize vulnerability remediation:
  - If a breach occurs, conduct a root cause analysis to identify remediation needs.
    - Do your due diligence; be thorough but timely.
    - Use extreme caution in asking for resources to fix problems unrelated to the breach.
  - Have a process for legacy hardware or end-of-life software that cannot be discontinued.
    - Place additional security controls to mitigate risk, focusing on detective rather than preventative capabilities.
    - Request a risk exception.
    - Request a plan (including a timeline) to port software or replace hardware.
    - Consider the affected system "out of scope" until the timeline ends, but track timeline progress.
  - Address non-compliance issues (e.g., PCI-DSS) immediately.
  - Utilize your vulnerability scanner's categorization features to assist prioritization.

  - Group vulnerabilities in order to better understand the true state of your enterprise’s security posture.
    - Vulnerabilities unique to a particular OS, application, or hardware appliance.
    - Consider a risk exception for vulnerabilities unique to a particular network segment.
    - Exclude from audit (i.e., place “out of scope”) vulnerabilities with approved risk exceptions for the duration of the exception. (This may exclude entire systems or network segments.)
- Remember:
  - You’ll never get down to “zero” vulnerabilities.
  - Your organization doesn’t exist solely for the purpose of keeping its own information secure. It exists to provide a service or produce a product.