Information Security Incident Response Process Development
Annotated Bibliography

Cichonski, P., Millar, T. Grance, T. Scarfone, K. (2012). Computer Security Incident Handling Guide NIST Special Publication 800-61 Rev.2). National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

NIST's document aims to guide organizations in establishing incident response capabilities, independent of hardware and software considerations, with the focus being on detecting, analyzing, categorizing and handling incidents.

The guide stipulates it's essential that organizations formalize response plans. From possible team structures, to information sharing post-incident, NIST proposes a 4 stage incident life cycle: 1/Preparation, 2/Detection & Analysis, 3/ Containment Eradication & Recovery, and 4/ Post-Incident Activity. Organizations should be ready for common attack vectors and the guide emphasizes the importance of communication with various internal and external groups throughout the cycle.

As a long-standing standards body that provides requirements for federal agencies, NIST's guide is a key, authoritative document. Though broad in scope, this overarching guide is essential to understanding the significant planning, resources, and challenges to effective preventative and reactive incident handling. While not technical in nature, it also provides several useful scenarios in an appendix which help to put some of the theory in practice and better visualize how all the pieces fit together.

Kral, P. (2011). The Incident Handler's Handbook (SANS Institute Reading Room). SANS Institute. Retrieved from https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

Kral's paper, written for a GCIH Gold Certification, breaks down the basic foundations for the creation of processes and incident handling techniques throughout the incident life cycle.

Though Kral naturally uses SANS 6 step incident life cycle versus NIST's 4, this handbook works as a distilled, nuts and bolt approach, more from the point of view of the potential incident handling technician rather than management. It's a simple to digest, straight-forward document with useful recommendations on what should be in one's jump bag, commands for both Windows and Unix environments, and checklists to make sure no step is skipped throughout the process and nothing left undocumented.

Pokladnik, M. (2007). An Incident Handling Process for Small and Medium Businesses (SANS Institute Reading Room). SANS Institute. Retrieved from https://www.sans.org/reading-room/whitepapers/incident/incident-handling-process-small-medium-businesses-1791

Pokladnik's paper, written for a GCIH Gold Certification, approaches incident handling process development through the lens of small and medium-sized businesses, taking into account their limitations in terms of budget, staff, and skill set.

The author recommends that there be a minimum number of two assigned roles, a technician and decision-maker, and suggests essential skills, training, and accessible open-source tools that he believes are mandatory to get a basic incident response team off the ground and running.

The article is a bit dated, and the recommendation to omit forensics capability might be questionable, but since more top-level guides such as NIST's *Computer Security Incident Handling Guide* are broad, technology independent, and geared towards larger entities, they're challenging to tailor to smaller organizations. Instead of picking and choosing from one of them and establishing what's feasible for SMBs where practitioners often have to wear many hats, this paper presents, through a concise, manageable, baseline approach, a good starting point for thinking about implementation while also suggesting how to expand incident response capabilities over time.

Shackleford, D. (2018). Incident Response In The Cloud. RSA Conference. Retrieved from https://www.rsaconference.com/writable/presentations/file_upload/air-w14-incident-response-in-the-cloud.pdf

In this set of slides from a presentation at a recent RSA conference, SANS Sr. Instructor Shackleford addresses the extra challenges of handling incidents in the cloud versus on-site.

Though Cloud Incident Response is deemed tougher due to a general lack of visibility and control of the data with the introduction of an external provider and virtualization, Shackleford demonstrates that cloud customers' security concerns don't necessarily match incidents' rate of occurrence. There is no growth in real incidents and breaches and, at the end of the day, the main incidents have been operational in nature and related to availability more than anything. Going through the 4 phases of NIST's classic 800-61 Rev 2. model he suggests specific ways to improve incident handling processes much of which consists in interfacing with the provider and intelligently automating processes.

While trying to research cloud incident response processes before fully grasping traditional IR might seem like trying to fly before learning to crawl, it's interesting to see what even some of the best teams have trouble with at the moment. Even though there are extra challenges and considerations, the completely unified backplane for larger organizations is a huge advantage and some recommendations can be applied locally.

Schneier, B. (2017, March 29). Security Orchestration and Incident Response. Retrieved from https://www.schneier.com/blog/archives/2017/03/security_orches.html

In this personal blog article, Schneier offers his opinion regarding the information security trend of vendors selling customers on automated solutions that aim to replace human staff.

While automation certainly is needed in incident response, he argues there is a fundamental problem with the approach in the sense that automation can only help with what is known while so much of information security is unknown regardless of the quantity of data available. Security teams need to be flexible and adaptable, something that automation is currently not necessarily suited for. Even as technology continues to advance, he believes human-centric incident response teams are what makes automation effective and not vice-versa.

Schneier is an experienced and respected voice among the security community. Whether considering understaffed incident response teams that need extra help from automated solutions or larger organizations drowning in data and threats, his direct, no-nonsense, perspective is timely and relevant with the advent of machine learning and figuring out the right balance to be struck between staff and automation.