Executive UPDATE
CUTTER CONSORTIUM
Access to the Experts
BUSINESS TECHNOLOGY & DIGITAL TRANSFORMATION STRATEGIES

# Security Incident Response: Preparation Is Key

*by Aurobindo Sundaram*

Most organizations will experience a large security incident at some point. The difference between an organization that survives and thrives following an incident versus one that flounders can be summed up in one word: *preparation*. Athletes, emergency responders, performers, and many others practice for hours before the main event. So why do organizations not do the same for security incidents? Urgent timelines, high stress, uncontrollable events, and scrutiny from customers, regulators, press, and investors are surely good reasons to put better preparation practice in place. While many organizations have a disaster recovery and business continuity (DR/BC) plan, few focus on preparing specifically for a large security incident. In this *Executive Update,* we outline a multipronged approach for best practice organizations that focuses on continuous process improvement (detailed below in Sections A, B, and C):

- Create a strategic incident response plan (IRP) — Section A
- Test the plan with executives — Section B
- Adjust the strategic plan and build operational plans — Section A
- Test the operational plans — Section B
- Test the plan with both internal and external resources and make enhancements to the IRP — Sections B and C
- Continue this improvement process periodically — Section C

## Section A: Preparation of an IRP

Incident response on the fly will never work. Period. During a large security incident, dozens of stakeholders must make hundreds of decisions in real time, all in some undetermined order. This is a recipe for disaster unless you have the following strategic and tactical steps documented:

The *Executive Update* is a publication of Cutter Consortium's *Business Technology & Digital Transformation Strategies* practice. ©2018 by Cutter Consortium. All rights reserved. Unauthorized reproduction in any form, including photocopying, downloading electronic copies, posting on the Internet, image scanning, and faxing is against the law. Reprints make an excellent training tool. For information about reprints and/or back issues of Cutter Consortium publications, call +1 781 648 8700 or email service@cutter.com. ISSN: 2470-0932.

- **Roles and responsibilities.** During an incident, everyone has an opinion, but only a few stakeholders that can/should make decisions. Are you clear on the responsible, accountable, consulted, and informed (RACI) matrix for your IRP? For example, who decides whether to contact law enforcement? Who decides whether to make a press statement? Who decides on hiring external counsel? Who decides when to notify the board of directors? These are all important questions, and for many, there may be obvious answers, but in the heat of an incident, they can be forgotten. I strongly recommend that businesses take the time to define a RACI matrix for key decisions.

- **Form responses.** There are many stakeholders (e.g., customers, consumers, press, regulators, law enforcement, and internal staff) that you must communicate to during an incident. Do you have form responses ready and available for different incident types?

- **Operational playbooks.** Have you ensured that for every feasible major incident, you have a playbook that addresses the necessary tasks (what), the timing (when), the roles and responsibilities (who), and how tasks are performed (how)? This is critical to ensure that there are no gaps during the response (see Figure 1).

- **Third-party support.** Do you have contracts with all the third parties you may wish to use during an incident (e.g., outside counsel, law enforcement, forensics support, consumer and call center support, crisis management, and translation services)?

- **Key decisions matrix.** This may not be in the first iteration of your IRP, but as you run through simulations, ensure that you are war-gaming decision points and making decisions that you anticipate having to implement in the future. As a simple example, for a denial-of-service attack lasting longer

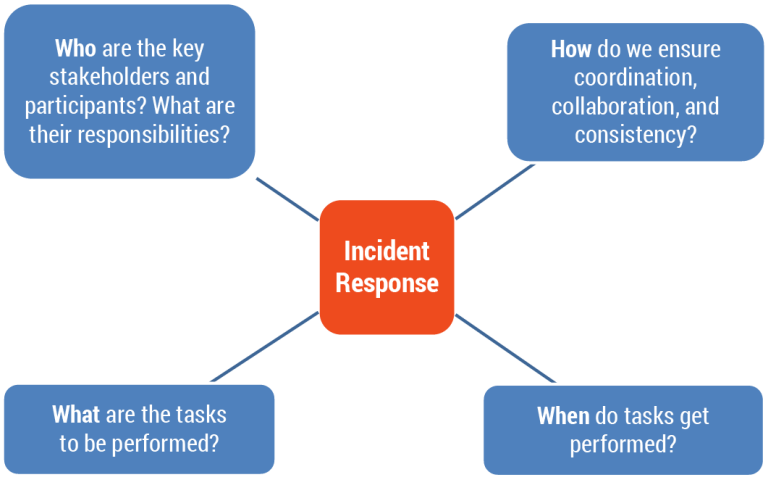


Figure 1— IRP in a nutshell.

than 12 hours, you may choose to always issue a press release and give a usage credit to your customers. These "pre-decisions" lead to cost, resource, and operational implications that you can prepare for in advance.

*Key recommendation:* most organizations should begin their incident response journey by creating a high-level strategic plan, then a set of operational buckets, and finally start documenting each in order of criticality.

## Section B: Execution of an Exercise

This section is intended more for the facilitator of an exercise, although it will be of use for anyone involved in the response process. To have a successful, valuable exercise, the facilitator must:

- **Create realistic scenarios.** Use your industry and business knowledge to create a realistic, bad-case scenario that is relevant to your organization. Use industry events as a base (e.g., a ransomware attack, a data breach, or public privacy troubles) and adapt them to your organization.
- **Use resources already available.** Seek our scenarios from information security experts that you can adapt quickly for your own use.
- **Decide on the methodology.** Decide on how to run the exercise. For instance, ensure you answer such questions as: Are the parties already trained or are they walking blind into an exercise? If pretrained, do they get a copy of the exercise beforehand to prepare? How much time do you want to devote to the exercise and why?
- **Split the exercise into manageable modules.** Every incident follows a logical path from discovery to investigation to response to remediation to communication. It is smart to split the incident into modules that roughly reflect this path so it is easier to manage, summarize, and learn from. A "big bang" exercise benefits no one. During an exercise, you will likely need to segue between modules as a real incident response does not always follow a straight-line path from investigation to communication.
- **Speak little but guide a lot.** A facilitator moderates the discussion and guides the executive team toward collaboration, lessons learned, and activities of interest. The facilitator is not there to teach the team. That comes later. Lead with such questions as: Have you thought of X? In the XXX case, this happened. How does that influence your decision? What are the implications of notifying your entire customer base in this form? Remember that the executives will have to make the decisions during an actual incident — you're there to train them to know how to make the right ones.

*Key recommendations*:

- Train executives on the IRP (one hour) a week or two prior to the exercise.
- Provide executives with the full IRP as a pre-read document.

- Create a five-module exercise.
- Perform the exercise in person if possible.
- Devote two and half hours to the entire exercise, with each module being 20 minutes long (with some deviation permitted for discussion and transitions).
- Allot 20 minutes following the exercise for a debrief and ask for improvement ideas.
- Follow up within a week with a summary of actions, owners, and timelines.
- Follow up periodically as required.

## Section C: Follow Up and Continuous Improvement

Most organizations will start with a shell of an IRP and then start filling in the operational details. Typically, this effort begins with a security incident where the response goes horribly wrong; on occasion, it can be from the results of an exercise, such as one performed above. Even with a fully fleshed out IRP, every security incident is different. The best way to manage an IRP is to iteratively make improvements to it, rather than attempt a "big bang" comprehensive plan.

On completion of an exercise, here are the task areas that add the most value to an organization:

- **Post-incident action areas.** Immediately following the exercise, the facilitator should give his or her impression on key areas of enhancement. The facilitator should also invite feedback from the participants. This feedback should be broad-brush feedback, not specifically action-oriented (that comes later). For example, a facilitator might say, "We had no contingency plan to work through a million-consumer notification, and we'll need operational plans to address that"; "We noted a key conflict between Communications and Legal on press statement timing"; or "We noted that technology has a robust plan to isolate the network during an incident."
- **Areas of conflict.** During an incident, there are bound to be conflicts and differences of opinion. The keys to handling them are: (1) create RACIs for key decisions before an incident; and (2) tease out conflicts in exercises, resolve them offline, and feed them back into the IRP. I cannot stress enough how important it is to allow conflicts to occur (and be resolved) in safe exercise situations, so that you're not having arguments in the heat of an incident. I've been in far too many of these.
- **Quick fixes.** There will be findings that are obvious and quick to fix. These should be prioritized for implementation, as they likely give you significant value with low effort. Often, they involve resourcing and clarification of responsibilities (e.g., "We need a retainer with outside counsel with expertise in countries X and Y").

- **Strategic planning tasks.** There will be strategic focus areas that need to be addressed. In your first exercise, those will likely be around roles and responsibilities, playbooks for specific incident types, and public statements on the incident (e.g., "We need to be ready with a communications strategy for a large personal data breach with media monitoring, public statements, stakeholder training, and notification of individuals and regulators"). These are broad priorities that will need multiple teams to coordinate implementation.

- **Operational planning tasks.** Strategic priorities will decompose into associated operational tasks. These are far lower-level tasks and typically are handed off to operational teams to address. They are substantial in terms of work effort though (e.g., "How can we scale up to handle 1,000 calls a day when normal call volume is 20 a day?"). This is where your IRP succeeds or fails, so don't take these tasks lightly or assume things will work out. They won't.

*Key recommendation:* Organizations will serve themselves well by populating the task areas above following every incident response exercise or security incident. The lessons learned and continuous improvement process are integral to the success of an IRP.

# Conclusion

This *Update* makes it clear that an organization without a security IRP is at high risk during a security incident. Yes, you can wing it, but even the best-prepared organizations struggle during a significant incident. What makes you think you can never practice and then go out and hit a home run when an incident occurs? Organizations must prioritize their immediate future efforts in accordance with the key recommendations outlined in Sections A, B, and C of this *Update*. As organizations develop their IRPs, they should ensure that all efforts answer one of the key questions: *who, what, how*, and *when*.

# About the Author

*Aurobindo "Robin" Sundaram is the Head of Information Assurance & Data Protection at RELX Group, an FTSE 100 listed company. Mr. Sundaram is responsible for creating and developing security and risk management policies, procedures, and standards; collaborating with chief information security officers (CISOs) to implement these policies; creating and enhancing fraud-detection technologies; investigating and responding to security incidents; and ensuring compliance with information security frameworks. He regularly reports on information security to RELX Group's board of directors, CEOs, and CTOs. Previously, Mr. Sundaram spent seven years at Schlumberger, a leading oilfield services corporation, where he implemented its information security program. During his tenure, objectives reported to the board were set for information security across the 50,000+ strong organization for the first time in Schlumberger's history. Mr. Sundaram was also closely involved in the design of the technical security architecture for the 2004 Summer Olympic Games in Athens, Greece. His thought leadership has led to several published papers in the security field, and he was recognized as a finalist for Information Security Executive of the Year in 2007 for the southeast region of the US. Mr. Sundaram holds a master of science degree from Purdue University and an MBA from Emory University. He can be reached at aurobindo.sundaram@relx.com.*