Hari Mukundhan, CISA, CISSP, has more than 13 years of extensive information security, IT audit, IT operations, and project and program management experience across a wide range of clients and businesses. He is currently a cybersecurity program manager in a leading private organization. He can be reached at *harimukundhan@yahoo.com.*

A Business-integrated Approach to Incident Response

With the significant increase in the rate of cybersecurity incidents worldwide, the financial impacts due to these incidents have also soared. From 2013 to 2014, the total number of security incidents has increased by 48 percent to 42.8 million incidents, and the number of companies reporting losses of US $20 million or more has almost doubled over the same period.[1] In addition, the number of aggressive business disruption attacks that impact the network core is expected to increase significantly over the next three years.[2] Recent high-profile attacks on various large retail and financial organizations are cases in point.

A Poneman Institute study revealed that only 14 percent of companies surveyed said that their executive management takes part in the incident response process, and "as a consequence of this lack of involvement and awareness, incident managers may not only find it difficult to prioritize incident handling, but may also find it difficult to obtain the resources from business leadership to invest in the skills and technologies necessary to deal with future security incidents,"[3] which are expected to increase significantly. Therefore, incident handling as a function requires strong integration with operational risk management processes in a more systematic manner, so that the impact to business can be better understood and the prioritization of incidents can be more accurate.

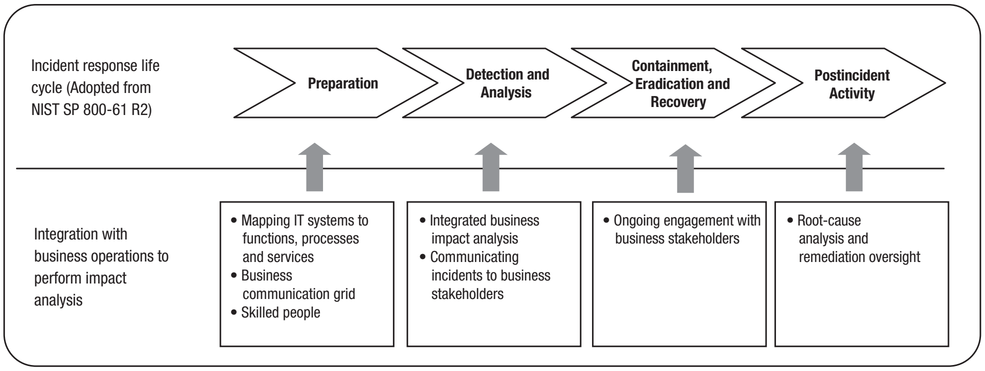
AN INTEGRATED APPROACH TO INCIDENT HANDLING

The US National Institute of Standards and Technology (NIST) "Computer Security Incident Handling Guide"[4] has been leveraged to emphasize the potential integration points between the security incident management process and operational risk management process and to provide a framework for incident managers and business managers to engage each other effectively. This article reviews each phase of the NIST process flow guide, identifies the integration points with business stakeholders and provides guidelines on how to operationalize those in a practical way (**figure 1**).

INCIDENT PREPARATION PHASE

The IT system infrastructure should be mapped to the business processes it supports, the governing functions and, ultimately, the client services delivered. This helps the incident managers estimate the overall business impact rapidly once they are reasonably confident about the accuracy of the incident precursor and indicators, which typically affect the infrastructure components (e.g., UNIX hosts, file transfer servers). Identifying the potential areas of impact is probably one of the most important and challenging parts of the incident response process.[5] But maintaining an evergreen map of how the system functions, processes and is

Figure 1—Incident Response Life Cycle and Business Integration


Incident response life cycle (Adopted from NIST SP 800-61 R2)
Preparation
Detection and Analysis
Containment, Eradication and Recovery
Postincident Activity
Integration with business operations to perform impact analysis
• Mapping IT systems to functions, processes and services
• Business communication grid
• Skilled people
• Integrated business impact analysis
• Communicating incidents to business stakeholders
• Ongoing engagement with business stakeholders
• Root-cause analysis and remediation oversight

Source: Hari Mukundhan. Reprinted with permission.

serviced provides organizations a significant advantage when they race against time to recover and respond to an incident.

In large organizations, documenting every process can be a time-consuming and costly exercise, but it does not need to start from scratch. There are some existing documents that could potentially be used to build the map, for example:

- US Sarbanes-Oxley Act of 2002-related process walk-through documents and test sheets can provide information on the process and supporting systems.
- Business impact analysis (BIA) and recovery time objective (RTO) documents can provide insights, albeit at a high level in many cases, on the functions, processes and services that may experience outages and estimates on how long systems may be unavailable.
- Risk and control assessment programs typically strive to map the business components to the systems to identify the operational risk to business due to the identified system risk factors.

An unfolding security incident, depending upon its scope, could create confusion and panic to both staff and customers. To proactively mitigate such confusion, incident managers should provide clear, precise, relevant and targeted information to various audiences. For the business stakeholders, the message should be as nontechnical as possible and must point to potential business impacts so that stakeholders can calibrate the responses on their side. The incident manager role in the information security organization has the best vantage point to provide such information. The incident manager should be prepared up front with the communication grid, i.e., what information should be communicated to which business stakeholders and during which life cycle stage of the incident. Appropriate templates, email distribution lists and call trees should be created up front in partnership with the business. Where possible, a dry run should be performed to fine tune the effectiveness of the communication channels and vehicles. **Figure 2** is an example of a communication grid.

As with many things, people make the difference between a good process and a great process. Staffing the incident management process with the right people with the right skill sets, especially at the integration points with business, helps in navigating the response to a more successful outcome. Ideally, such staff should have a good mix of technical, business and communication skills and be equally comfortable dealing with the technical teams and the business teams.

DETECTION AND ANALYSIS

Risk is typically a function of the adverse impact that arises if the circumstance or event occurs and the likelihood of occurrence.[6] Therefore, if the impact to business is unclear, the risk due to the incident is also unclear. This situation can potentially lead to incident response teams incorrectly prioritizing incidents. That is, it may outwardly appear that one incident is more critical than another, but, in fact, this may not be the case. For example, an externally facing web site that is being impacted by a denial-of-service (DoS) attack may appear more critical than the unavailability of a single sign-on (SSO) server that services many internal applications. But in the case of a web site with a commonly used SSO server, for example, its unavailability could cripple business operations. Obviously, in such a case, the SSO server incident needs to be prioritized ahead of the DoS attack incident. Because of situations such as this, quickly understanding the business impact in partnership with business managers is vital. The following are some of the business impacts that require analysis:

> “If the impact to business is unclear, the risk due to the incident is also unclear.”

- **Financial impact**—Both a financial loss and an inappropriate financial gain to an organization due to an incident should be considered when determining the financial impact. Based on the capital requirements and the risk appetite, organizations should identify a threshold value beyond which a formal chief financial or risk office review is required. An inappropriate financial gain is still considered a financial impact that requires investigation, analysis and eventually corrective action. For example, a man-in-the-middle attack on an end-of-day net transaction file sent by a client may show that the client owes money to the firm rather than the other way around.
- **Legal and regulatory impact**—The impacts regarding legal concerns, such as contractual issues, regulatory fines and penalties, and breach of service level agreements (SLAs), must also be considered. Given the heightened regulatory environment after the global financial crisis, the potential impact to statutory and regulatory requirements needs to be given special attention.

Figure 2—Example of a Communication Grid

Information required for the communication grid:

1. Identify relevant stakeholders associated to various key processes and systems in the organization.
2. Pre-establish communication channels and contact details:
   a. Identify audio and video conference numbers. Preferably, maintain a separate conference line for senior management.
   b. Create email distribution lists.
   c. Create call tree(s) to broadcast message to business users.
   d. Where possible, obtain dedicated rooms with both video and audio conferencing facilities.
   e. Maintain key stakeholder official contact information.
3. Create email, call tree, etc., communication templates.
4. Create a communication grid to determine 'what should be communicated to whom' with clarity on what MUST (mandatory) vs. what SHOULD (recommended) be communicated to whom. In other words, mandatory vs. recommended.

Key Incident Management Actions	Relevant Stakeholders					Communication Channel
	Technology and IT Security Managers	Business Manager	Senior Management	Functional Heads (Business and Administrative)	Business Users	
Complete initial notification of potential business-impacting incidents.	Must	Must	–	Should	–	Email distribution list
Evaluate business impact on a continuous basis.	Should	Must	–	Should	–	A/V conference/contact list/ In-person
Perform periodic executive updates.	–	–	Must	Should	–	Senior management A/V conference lines
Communicate business impact.	Should	Must	Must	Must	Should	Email distribution list
Evaluate and finalize containment, eradication and recovery options.	Must	Must	Should	Should	–	Email distribution list
Communicate actions and relevant information around the finalized option.	Must	Must	Must	Must	Must	Call tree
Perform periodic recovery updates.	Must	Must	Must	Must	Must	Call tree

Source: Hari Mukundhan. Reprinted with permission.

- **Operational impact**—A partial or full inability to run the day-to-day business operations of an organization needs to be considered. Depending on the type and scope of the incident, an impact to business operations may or may not impact customer service. It may or may not impact finances. It can be organizationwide or can be limited to a certain section. However, a sustained impact to operations typically leads to a cascading financial, regulatory and/or reputational impact.
- **Reputational impact**—Reputational impact occurs when negative publicity regarding an institution's business practices leads to loss of revenue or litigation.[7]

Typical incident documentation tends to delve deep into the technical details related to the incident (e.g., the IP addresses impacted, details of the system log files, the network layer in which the incident occurred). However, as noted in the incident preparation stage, the incident manager should keep the message nontechnical and focus on the potential impacts to the business in a plain and simplistic fashion. The communication templates created during the incident preparation stage can be utilized to get the key messages out as soon as possible via email distribution lists, call trees or conference calls.

The following are some of the key aspects to be taken into consideration while documenting and communicating the incident:

- Determine the incident types and the severity level at which business engagement is required. Note that not every incident warrants a business engagement. Also take into consideration the sensitivity of the information before sharing.

- Develop templates and guidance to create a high-level, nontechnical executive summary articulating the scope and depth of the incident. Target this toward the executive business leaders.
- Develop templates and guidance to create a detailed, nontechnical write-up articulating the impact to IT systems and, thereby, the potential processes and services that could be impacted. Such communication is typically targeted toward the function heads, managers and staff.
- Maintain email distribution lists, call trees and other possible communication channels that can be used for communication during the incident.
- As required, train incident managers on the important aspects of business communication.

CONTAINMENT, ERADICATION AND RECOVERY

For incidents that have a business impact, the incident manager and the business manager have to work closely to ensure that business response is timely and adequately calibrated. If the incident and the business impact is an evolving one, the incident manager may have to invite the business manager to brief, periodic touch-point meetings to appraise the current state of the incident's scope and depth and how it is being contained and eradicated. The business manager, depending upon the evolving state of the incident and its containment or eradication success rate, would, in turn, be expected to constantly reassess the impact and respond accordingly. For example, if a network worm has brought down only a small number of desktops used by operations staff and the incident response teams are able to successfully contain, eradicate and restore services quickly, then the impact to customers may not be significant and the business may have to simply wait for the rest of the desktops to be up and running. On the other hand, if the network damage is spreading fast and is outpacing the incident response team, the business managers may have to consider other options, such as activating a disaster recovery site, transferring work to a different location or shifting to a manual option.

Periodic engagement with the business manager during this phase has the following advantages:

- Provides a constant feedback mechanism to the incident managers on the priority level of an incident
- Provides feedback on the effectiveness of the business continuity plan, thereby improving the resilience of the organization and its functions
- Assists in proactively managing news media, social media, regulators, vendors and other third parties
- Manages client expectations accordingly
- Prepares the business proactively for legal and other contractual impacts
- On a long-term basis, aligns the cybersecurity agenda with the business strategy

POSTINCIDENT ACTIVITY

The postincident activity section of the NIST guide[8] provides excellent insights on how to arrive at lessons learned and how to improve the incident response process in general. Performing a root-cause analysis for impactful incidents and following it up with remediation measures is important. In simple terms, the incident manager should be able to document the relationship between the incident's root causes and the business impact and how the incident was contained, eradicated and recovered. A joint lessons-learned session should, at a minimum, focus on the following:

- Identify accountable parties to the incident root cause and assign ownership to remediate.
- Determine if the incident has recurred along with a recurring financial impact. If the probability of the incident occurring in the future is also high, consider whether additional capital needs to be allocated to cover for future potential losses.
- Update the system's function-process-service map and other documentation, if required.
- Determine whether the business impact was calculated accurately and what needs to be done to improve the calculation.
- If the disaster recovery site was activated, check whether the recovery plan requires an update. Interface with business continuity managers to carry forward the update.
- Constant oversight should be provided by business managers to ensure that root-cause owners are remediating the root causes on time and business management is kept updated.

CONCLUSION

To help keep the cybersecurity agenda consistently aligned with business priorities and to provide a practical and effective mechanism for prioritizing incidents, an integrated approach to incident management is vital. Response and recovery can be more targeted and more efficient. Additionally, incident managers may find themselves in a better position to obtain resources to invest in skills and technologies that are required to deal with future incidents.

ENDNOTES

[1] PricewaterhouseCoopers, "Global State of Information Security Survey: Key Findings and Trends," 2015, *www.pwc.com/gx/en/consulting-services/information-security-survey/key-findings.jhtml*

[2] Gartner, "Gartner Says By 2018, 40 Percent of Large Enterprises Will Have Formal Plans to Address Aggressive Cybersecurity Business Disruption Attacks," 24 February 2015, *www.gartner.com/newsroom/id/2990717*

[3] Ponemon Institute, "Cyber Security Incident Response: Are We as Prepared as We Think?" January 2014, *www.lancope.com/sites/default/files/Lancope-Ponemon-Report-Cyber-Security-Incident-Response.pdf*

[4] Cichonski, P.; T. Millar; T. Grance; K. Scarfone; "Computer Security Incident Handling Guide," NIST Special Publication 800-61, August 2012, *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf*

[5] *Op cit*, Cichonski

[6] National Institute of Standards and Technology, "Guide for Conducting Risk Assessments," NIST Special Publication 800-30, USA, September 2012, *http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf*

[7] Federal Financial Institutions Examination Council, *IT Examination HandBook*, InfoBase, USA h*ttp://ithandbook.ffiec.gov/it-booklets/retail-payment-systems/retail-payment-systems-risk-management/reputation-risk.aspx*

[8] *Op cit*, Cichonski