COGNIZANT

Coordinating Security Response and Crisis Management Planning

Proper alignment of these two critical IT disciplines can mean the difference between an efficient response and a prolonged disaster.

Executive Summary

Too often, information security incident response plans, disaster recovery and business continuity plans are not aligned with the overall corporate crisis management process. Now, more than ever, an organization must be able to quickly respond to a security breach, with both a tactical response and a strategic corporate message. The global village really is upon us, and with international businesses being supported by partners and outsourcers now the rule rather than the exception at many organizations, time is literally money. Web sites cannot be down, or customers will go elsewhere. With global services providers of all types supporting a profusion of company data, effective security is hypercritical. More stringent security standards (such as PCI for credit cards), penalties and compliance requirements all amplify the need for robust and tested response programs.

This white paper discusses the benefits of, and an approach to, integrating the security response process into the overall corporate crisis management plan and the pitfalls to avoid during this implementation.

Similar efforts go into building, managing, exercising and maintaining security incident response plans and overall corporate crisis management plans. For most organizations, the escalation, notification and decision-making process is similar, regardless of the incident. The struggles organizations encounter, while developing these plans, also tend to be similar. Building awareness, understanding roles and responsibilities and allocating time and resources (financial and human) can all be impediments to sound response plans.

Better plans can be developed by integrating elements of both initiatives to overcome these shortcomings.

Creating a Security Emergency Response Team

There are two types of security emergency response teams (SERTs) within an organization, a strategic team and a tactical team. The strategic team focuses on the overall company direction. It is notified by the tactical team about every incident and determines whether executive management needs to be notified. If the incident impacts a large percentage of the company (e.g., a distributed denial of service attack), the strategic team will be notified and the head of that team will alert the executives.

Cognizant

The strategic SERT team comprises the following members:

- **Chief information officer (CIO):** The CIO typically reports to executive management on the status of an incident. The escalation process should define when executive management will be notified (e.g., at the start of the incident, during or after), and what will be reported. The CIO's overall responsibility is to provide executive management an overall picture of what is happening within the organization. This reporting process must be appropriate to the audience, and the individual presenting it must know how and what to communicate to help executives make the correct decisions. The executive management team makes the final decision on how to respond to the incident based on the CIO's input.
- **The chief information security officer (CISO) or IT security director:** Overall IT security for the organization is the primary responsibility of this person. The CISO typically develops the strategic SERT plan for the company. In devising the plan, he must ensure every type of incident and its associated reaction is addressed. For the plan to be successful, it must have executive support. The plan must become a living document where changes and maintenance are encouraged on a regular basis. It needs to be tested regularly as well (whether once a quarter, twice a year, etc.), via a tabletop walk-through exercise with strong representation from both the strategic and tactical teams so that everyone understands their roles and responsibilities. Such steps ensure that the plan becomes part of an organization's overall security program and remains valid and up to date.

The CISO has a role on both the strategic and tactical SERT teams. As a member of both teams, he can report to the CIO on the progress made combating the incident.

The one group most SERT plans overlook is the business units. This ties back to the linkage of the SERT with an organization's existing crisis management plan. Integrating these two initiatives helps ensure that executive reporting and management is in place and that individual business areas are better prepared to respond to any form of incident or business interruption, be they cyber, man-made or natural.

Within each business unit, a director or higher-level person is typically appointed to the strategic team. As the security team within the organization evaluates what incidents to track and how to do so, the BUs then notify the SERT team how the incidents affect or impact business applications or processes. While information security may think a particular incident is a priority-1, adding the response from the BU may lead people to better understand that the incident is actually only a priority-3, or lower. Thus, BUs become an integral part of the SERT team and the evaluation process. Considering that most incidents affect a business application, BU representatives are the ones best equipped to inform the CIO organization when the application is functioning correctly again. BU representatives also make assessments and add value when creating an incident matrix. Figure 1 (on following page) depicts a security incident matrix that can be used when strategic incidents occur.

During an incident, the strategic team typically sets up a conference call as part of a preliminary response. During this call, each team member will identify themselves. The call will take place within the allotted time frame. During the initial call, the type and potential severity of the incident is identified, including impacted systems and applications. This call helps determine if the incident is spreading within the company. During subsequent calls with the team, initial response effectiveness is gauged. If these initial actions aren't effective, the strategic team will change the tactical team's direction.

It is important that the strategic team clearly sends only one message to the executive team as well as to the employees. If there is more than the one message, confusion could ensue across the company. Also, only executives or identified personnel are allowed to speak to the media about the incident.

It is difficult to create a matrix that will cover all types of incidents, but it is helpful if a SERT team can hold brainstorming sessions with everyone. By doing this, organizations receive direct buy-in from the BUs rather than working within an IT vacuum, as often happens. Once this matrix is created, it is presented to a director-level executive for approval.

The functions of this team are to:

- Make a preliminary assessment of the damage.
- Notify senior management on the current status, impact to business and plan of action.
- Declare the disaster, if necessary.
- Initiate the emergency situation plan.

Illustrative Incident Matrix

Category	Event Priority		
	Single Workstation	Multiple Workstation/ Single DMZ Server	Multiple Servers/PCI
Category I: Unauthorized Root/Admin Access	P3-2	P2-1	P1-1
Category II: Unauthorized User Access	P3-3	P2-2	P1-1
Category III: Attempted Unauthorized Access	P3-4	P2-2	P1-2
Category IV: Successful Denial of Service Attack	P2-1	P1-2	P1-1
Category V: Poor Security Practice or Policy Violation	P4-4	P2-x	P1-2
Category VI: Reconnaissance/Probes/Scans	P3-3	P3-2	P2-3

NOTE: If there is a fast-spreading new worm or virus, do an immediate callout. Malicious code includes bots, Trojans, worms and viruses. There is a thin line between a probe/scan and attempted or unauthorized access.

Figure 1

- Organize a control command center as a central point of recovery efforts.
- Organize and provide administrative support to the recovery effort.
- Administer and direct the problem management function.

Once the incident is closed, a root cause analysis (RCA) is performed. Key points of this analysis include:

- The CISO is responsible for ensuring timely completion of the RCA report.
- An RCA is mandatory for all critical situations.
- Capture the inputs from all the stakeholders within <N> business days after the root cause is identified.
- The draft RCA report is reviewed with all the stakeholders within the next <N> business days after problem resolution.
- The RCA document is made available at a common location.
- The RCA report should clearly capture lessons learned and action items.
- After its review with all stakeholders, the final RCA report should be formally accepted by the customer (BU leader) within <N> weeks.

The Importance of Crisis Management Planning

Crisis management plans allow organizations to respond quickly and efficiently to an event. While emergency response deals with evacuation and staff safety, crisis management takes the next step beyond the initial emergency and deals with the escalation and decision-making process that executives and operations require to protect the organization at the time of the incident.

Crisis management provides the means to integrate and coordinate an organization's overall response. This process links emergency response management to business continuity/technology recovery. This process provides companies with:

- An incident response organizational structure, such as:
  - Internal crisis management: providing consistent communication flow.
  - Greater response planning: alerting appropriate company management.
  - Interfacing with external entities such as customers, analysts and media.
- Linkage to alerting (emergency response).

- Assessment and decision-making: pulling in appropriate management, executives, operations and vendors needed to support the incident.
- Structure for initiation and ongoing monitoring/management of a situation.
- Processes and tools to support determining crisis status escalation and de-escalation.

Recent history is full of examples of organizations that have responded well (think Odwalla Juices) and not so well (Exxon) to business emergencies.

Integrating information security into the crisis management process, and further into business continuity and disaster recovery, better prepares an organization to respond effectively.

Odwalla acted quickly, took responsibility, addressed the problem and rebounded as an organization. It spent millions, including a product recall and process improvements, and was hit with the largest fine ever assessed by the FDA. Yet, this is an incident that today is not widely discussed or remembered.[1]

The Exxon Valdez issue is an example of a crisis that was handled poorly, including mismanaged media communication. Moreover, the cleanup of the oil spill was slow, as was Exxon's acceptance of culpability. This ended up costing Exxon billions of dollars in fines and even more in reputation loss.[2]

Pulling It All Together

There are similarities in the security response and crisis management plans. Linking them will help pull the pieces together to better prepare an organization to respond to any incident. Integrating information security into the crisis management process, and further into business continuity and disaster recovery, better prepares an organization to respond effectively.

Our recommendation: start with a plan that can be tested with a walk-through exercise. This helps the organization understand all the moving parts and which vendors and partners should be included. From there, develop a plan that:

- Matches the organization, culture and partner relationships.
- Lays out the framework and strategy; familiarizes the team (internal and external) with the concepts, etc.
- Is based on the charter, as an action-oriented guide.
- Includes a one-page guide, to serve as the main tool, with contacts, roles and responsibilities and flow.

Make sure to hold a walk-through/tabletop to validate the organization, process, timing, decision-making and communications processes. Then finalize the plan and have vendors and partners participate in the walk-through/tabletop exercise. Vendors love to take an opportunity to meet with executives and can add valuable insight to your response assumptions.

The Importance of Linking Processes

SERT plans sometimes hit the wall when bringing business units into the planning process. BUs can help security teams better understand and validate the impact of security and/or IT outages and their input should be actively encouraged and embraced.

Coordinating the activities of crisis management and SERT planning with the business units is critical.

Many organizations let minor incidents turn into major events because their initial response is weak. Delays and confusion at the front end of an issue can mushroom into a much worse incident. To prevent this from happening, your organization must link its incident responses into a comprehensive action plan that pulls in executive, operational, technical and third-party support that can quickly respond to any event.

Remember:

- Integrated planning builds an integrated and accurate communication process.
- Combining efforts ensures more successful business area buy-in.
- Business unit involvement makes the assessment process more accurate.
- Maintaining the plans better prepares your organization to respond to any outage, event or incident.

Footnotes

[1] http://www.mallenbaker.net/csr/crisis05.html.

[2] http://iml.jou.ufl.edu/projects/fall02/susi/exxon.htm.

About the Authors

Martin Welsh, CBCP, MBCI, leads Cognizant's Disaster Recovery and Business Continuity Practice. As the Practice Lead, he is responsible for the development and support of DR/BC methodology, products and service delivery. As a DR/BC expert, he has product management, business development and hands-on experience developing IT and business recovery programs, strategies and services for Fortune 500 clients. Marty can be reached at Martin.Welsh@cognizant.com.

Acknowledgement

We would like to thank Keith Taylor for his contribution to this paper.

About Cognizant

Cognizant (NASDAQ: CTSH) is a leading provider of information technology, consulting, and business process outsourcing services, dedicated to helping the world's leading companies build stronger businesses. Headquartered in Teaneck, New Jersey (U.S.), Cognizant combines a passion for client satisfaction, technology innovation, deep industry and business process expertise, and a global, collaborative workforce that embodies the future of work. With over 50 delivery centers worldwide and approximately 171,400 employees as of December 31, 2013, Cognizant is a member of the NASDAQ-100, the S&P 500, the Forbes Global 2000, and the Fortune 500 and is ranked among the top performing and fastest growing companies in the world. Visit us online at www.cognizant.com or follow us on Twitter: Cognizant.

World Headquarters
500 Frank W. Burr Blvd.
Teaneck, NJ 07666 USA
Phone: +1 201 801 0233
Fax: +1 201 801 0243
Toll Free: +1 888 937 3277
Email: inquiry@cognizant.com

European Headquarters
1 Kingdom Street
Paddington Central
London W2 6BD
Phone: +44 (0) 20 7297 7600
Fax: +44 (0) 20 7121 0102
Email: infouk@cognizant.com

India Operations Headquarters
#5/535, Old Mahabalipuram Road
Okkiyam Pettai, Thoraipakkam
Chennai, 600 096 India
Phone: +91 (0) 44 4209 6000
Fax: +91 (0) 44 4209 6060
Email: inquiryindia@cognizant.com