DATACOM SYSTEMS INC

Developing an Effective Incidence Response Plan

A guide for converged networks

A DATACOM SYSTEMS WHITE PAPER

Vital Data

Information Technology management has historically been plagued by after-hour calls, to attend to an urgent network crisis. Improved cabling, device stability and end-user education has improved uptime in most networks. With improvements in technology and reliability, the dependence on networked systems has increased. Converged systems carry vital data applications, e-commerce, and voice traffic on a single network.

As organizations continue to migrate to a true converged cable plant in the Voice Over Internet Protocol (VOIP) environment, the responsibility of network professionals to prevent minor traffic congestion will escalate. Security concerns and increasing malware replication speeds require well-prepared, coordinated and timely responses to any type of incident. A fast, efficient, comprehensive response plan is necessary for organizations to ensure they maintain critical business processes and customer confidence.

Incident Response can be defined as a specific process developed and designed to ensure an approved and appropriate response to a variety of events. An incident response plan prepares for the occurrence of an unintended event. The plan will analyze the events impact on the organization, collect data, and suggest a response. When the business processes have returned to their normal state, the Incident Response (IR) plan reviews the process and response of the event in order to improve the plan.

Incident Response is defined as a specific process developed and designed to ensure an approved and appropriate response to a variety of events.

An IR plan is a small part of the total planning and preparation documentation required for an organization to respond properly to an event. Additional documentation may include Disaster Recovery, Business Continuity and Communication Plans. Some businesses consolidate the documents described, into a single plan. This single document is difficult to understand, maintain and use during an event. Multiple documents are easier to maintain, use and get approved by senior management. A brief overview of supporting documentation is required to understand the role of the IR plan.

A Disaster Recovery (DR) plan organizes the process of declaring an emergency or event. Responsible parties are identified that have the authority to notify, engage and approve resources, declare the emergency and perform damage assessments. The communication between departments to conduct these tasks is identified under the DR plan.

Once a disaster has been declared, a process is initiated to contact specific individuals, internal or external within the organization. The process may be in either the DR or Business Continuity (BC) plan, depending on the scope of the event. Contact information is in the Communication Plan. Contact information is required for both internal and external resources. For example, in the case of a Security Breach, law enforcement may be involved. In the case of an application failure, the software vendor maintenance contract may be activated to support the recovery of the program or data.

The Communication Plan will provide contact information for all responsible agents in the organization, and third party or supporting companies. The communication plan will include Customer, Account, Authorization Numbers or passwords to allow the individual contacting agency to authenticate itself with approved vendors. These confidential numbers will not normally be made available to everyone who gets a copy of the communication plan. Multiple versions or appendices of the Communication Plan may exist to restrict access to sensitive information.

The Business Continuity (BC) plan prioritizes applications or systems based upon function, financial or public impact to the organization. This will mandate system priority and focus for any recovery techniques.

The BC plan organizes recovery strategies for specific components or functions and considers external support such as insurance and external vendor selection. Focus is upon maintaining the business function, and fully recovering the function when appropriate. An example may include the loss of the order processing function. If an order processing function, or access to the system goes down, an Application Service Provider may be engaged to provide emergency order processing services, from a facility outside of the geographic area, which has the authority to redirect e-commerce traffic, and possibly DNS or MX tables.

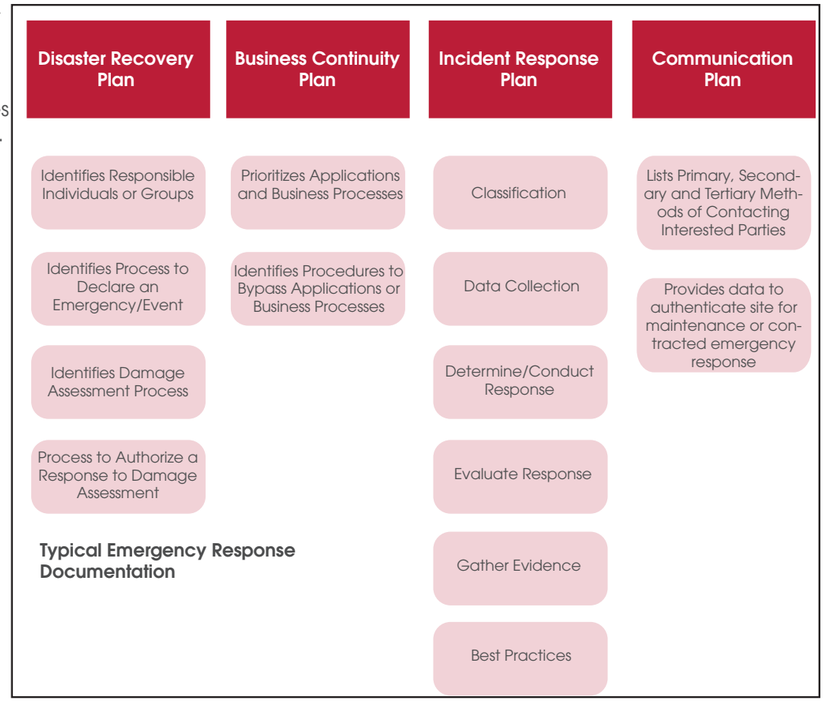
Effective response

Each company is going to organize their disaster planning documentation according to their business model. The below figure identifies disaster planning documents. This allows each document to be specifically focused on key areas, while referring to other documents for specific details related to an event.

Departments or groups will maintain and update each plan on a regular basis. For example, the Communication Plan will be updated frequently, since it will contain Names, Phone Numbers, Email Addresses and Authorization Codes. The DR plan would change less frequently and would probably not mention specific names, but titles when referring to responsible parties.

Once the goal of each document is understood, their function and use during an event becomes clear to the individuals involved. The process of a damage assessment, declaring an emergency/event and authorization for a response, is contained in the DR plan. The damage assessment process will authorize an appropriate level of response. The DR processes require data and response recommendations provided from the IR plan. An example in this document clarifies the relationships between the documents.

The detail of collecting, organizing and recommending a response is within the scope of the IR plan. The IR plan will provide information to and receive guidance from the other plans. Once notified of an event, the IR plan will determine how many systems are affected and provide that information back to the appropriate executive to declare an emergency or event. This IR process begins during the Classification phase.



Typical Emergency Response Documentation

Effective response to an incident requires that it is properly classified.

Classification

Effective response to an incident requires that it is properly classified. While there are numerous natural and unnatural events, the key is to quickly classify the type of event, and systems that it can or will affect. Identify responses under categories, based upon the level of impact to the core business processes of the organization, for example:

Response Classification Name	Impact
Alpha	Impacts one or more critical business processes
Bravo	Degrades one or more critical business processes
Charlie	Degrades a non-critical business process
Delta	No business processes are impacted, response required for legal or informational purposes

The response classification may dictate how fast the IR team responds, who makes up the team, or how fast they notify specific executives, employees or media outlets. Authority may be granted to specific individuals to purchase equipment, coordinate services, contact third party support, or activate disaster recovery sites or vendors as needed.

Sustaining critical business systems evolves from an understanding of how the systems work, interrelate and are restored. Knowing critical process vulnerabilities is the first step to securing them. System security reviews, help you identify points of failure and leads to a risk assessment. The risk assessment provides a guideline of the common attack vectors and areas at risk to the organization.

Attack vectors dictate the type of Intrusion Prevention to deploy and method of Eradication. When a system has been compromised, pertinent attack vectors, allow an IR team to quickly conduct a damage assessment, to determine the extent of system degradation. Running down the list of attack vectors quickly identifies what type of containment is necessary to prevent the issue from spreading to other systems. A quick review of the pertinent information about each critical system can assist during the classification process. The following triage table is provided as an example:

Critical System Triage Table	Email	Web
Server Name		
Server IP		
OS		
OS Patch Level		
AV Patch Level CPU Utilization		
Memory		
Disk Space		
Date/Time		
Orders		
VOIP		
Finance		

Data collection

Do not force your IT personnel to gather data for the first time during a crisis.

The classification process is a triage type method to quickly determine if a business process is at risk, and quickly provide that information to the appropriate business owner.

Data Collection

Collecting data across multiple devices and network segments is critical during an emergency. Gathering network analysis data quickly and effectively across multiple network segments during an outage or security breach is usually difficult to correlate, even with advanced tools.

A variety of methods and tools can be used to accomplish this process. Some items that may need to be collected or reviewed would include: network management software, log files, intrusion detection systems, application monitoring devices, and firewall, router or Ethernet switch logs, RADIUS or TACACS logs, critical server system logs, VOIP Server logs, or access attempts into protected folders or files.

Understand what type of information is required for each type of incident. Know how you are going to collect that data, and which tools are required. Who has the appropriate access to the tools or the systems the tools collects data from. Many IT professionals use "jump kits" which are preloaded backpacks that have a variety of software, tools and supplies to analyze their network remotely. The "jump kit" is prepared so that it can be carried by someone that is on-call over the weekend, or grab on their way out the door, in the event of an evacuation of the facility. A sample "jump kit" is shown below:

MIS Emergency Jump Kit

Item	Function	Last Updated/ Tested
Access Control		
Key to Data Center	Unlocks Main Door to Facility	
ID card	Access to Backup Facility	
Network Tap	Provides access to Network Links where RADIUS or Router/Switch Access is unavailable.	
Software		
MS Windows	OS for Servers 1-5	
Redhat Enterprise Linux	OS for Server for Eng. App.	
Oracle Database Software	Database for R&D Group	
VOIP Analysis Software	Determine delay/jitter	
Media		
Blank CDs	Backups	
Backup Data, or access to off-site backup data	Used to recover systems	
Network Tap	Provides access to Network Links where RADIUS or Router/Switch Access is unavailable.	

MIS Emergency Jump Kit

Item	Function	Last Updated/ Tested
Analysis/Troubleshooting		
Laptop (Patched)	Remote Access (Analysis Tools Preloaded), Utility CD included, Dialup or remote account for internet access preloaded	
Tools	Tools to remove equipment from racks, open computer cases, remove cable, etc…. (Flashlight Incl.)	
Cables, Various	Used for Password Recovery, Server access, i.e. EIATIA568, Cross-over,T1	
Documentation / Communication		
Communication/ Incident Response/ Business Continuity/ Disaster Recovery Plans	Lists all Emergency Processes and Forms	
Paper/Pencil/ Forms	For notes, process etc…	

Practice with these tools on a variety of systems is increasingly important. Do not force your IT personnel to gather this data for the first time during a crisis. Practice using these tools and accessing different systems from a variety of locations, on a regular basis.

The requirement to collect, review and analyze information across multiple systems has become complicated enough to require multiple skills, experience and abilities. The individuals reviewing the information may need to have a significant level of access to critical systems. This type of access is not usually held by a single individual in an organization. A designated backup should be available for each critical system.

Specific problems result from the analysis of VOIP systems. A number of skill sets and tools are required to appropriately analyze a VOIP issue. If the server operates on a Windows or UNIX type operating system, skill sets with troubleshooting and analyzing that system are required. Specific log files, security patches and anti-virus updates must be completed and validated regularly.

VOIP issues can be the result of network congestion, quality of service (QOS) configuration, network routing or security problems. Network analysis for VOIP is often done with clients or devices placed around the network to determine delay, latency and jitter. Access to these devices may require out of band access to ensure availability during network outages. The use of network taps to gather this information will guarantee that accurate timing is received by the analysis software and prevent dropped packets for security software. The use of taps eliminates the need to access network devices and configure port mirroring to gather data.

Baseline information about your network and familiarity with analysis tools and access methods is necessary to provide accurate information during an event.

Depending on the type of problem, forensic information, log files, backups or trace files may need to be collected and used for prosecution or best practices analysis. Chain of custody issues with this type of information needs to be understood and followed so that data is admissible in court, or valid for remediation or security

Appropriate response

enhancements in the future. Training for individuals that collect this data is highly recommended, and offered by several agencies.

Determine/Conduct Response

Once the problem has been identified and a damage assessment performed, per the DR plan, a response can be determined. An example of some responses and their associated actions are identified below:

Response	Action	Approval Authority for Action
Evacuate Facility	Activate Hot Site	CEO or Exec. VP
Shutdown Process	Activate Shutdown Procedure	VP Operations or equivalent
Gather Data	Gather data about the system effected	Director Level, Operations, IT or Security
Isolate devices or effected areas	Take systems offline; disable new logins; lockdown network segments	VP level or equivalent
Modify Systems	Apply patches, security fixes, security updates, restore from backup	VP MIS or VP responsible for the Application

Note that Executive Approval is required for most actions. While obvious responses, like evacuating the facility in the case of a fire or bomb threat is obvious, the decision to activate the company's hot site, is a financial and business decision. If the main facility may be reoccupied in less than 24 hours, it may not make sense to activate the hot site, which is why this decision needs to occur at the highest levels. The IR plan is important, since it indicates the approval authority for each action and identifies appropriate responses.

Evaluate Response

After invoking the appropriate response, the effected systems and processes must be evaluated. If systems are still affected, more data collection, analysis and another response must be made. This is an ongoing action, and the key identifiers, logins, log files, cpu utilization, etc… must be closely observed and recorded by the IR team. As a result of this analysis, another action, or the associated timeline with the recovery process may change. The IR teams' role is to process this information and provide it back to the executive team, which may change the damage assessment. The damage assessment will determine other actions necessary in conjunction with timeframes, media coverage, utility responses, etc.

Gather Evidence

If the problem is eliminated, all information associated with the event is collected, stored, and reviewed to improve the overall IR process. If legal action is required, this information will be used as evidence.

Evidence may need to be collected and stored on removable media, or on special purpose systems. Organization and presentation of the evidence should be organized and determined ahead of time, to permit faster analysis and recovery times.

Best Practices

Any process centric approach needs to be maintained and updated on a regular basis. A best practices phase helps identify problem areas after an event, and allows appropriate groups and individuals to take corrective action.

Do not force your IT personnel to gather data for the first time during a crisis.

Item	Yes/No	Action
Preparation		
Were there gaps in the IR preparation process?		
Was the documented process followed?		
Did the IR plan link appropriately with other documentation?		
Classification		
Was the event properly Classified?		
Were all attack vectors or system vulnerabilities identified to provide the team with the information to formulate an appropriate response?		
Data Collection		
Was appropriate data collected?		
Was any piece of data overlooked?		
Was the IR team properly equipped?		
Was the IR team properly trained?		
Did the IR team communicate effectively both internally and externally?		
Was data properly stored?		

Item	Yes/No	Action
Determine/Conduct Response		
Was the appropriate response carried out in a timely manner?		
Was corrective action approved by an approved authority?		
Did the actions taken, contain the event or limit its' spread to other systems?		
Evaluate Response		
Was the action evaluated?		
If the response did not solve issue, was new data collected to update the damage assessment?		
Gather Evidence		
Was all of the appropriate evidence gathered?		
Was evidence gathered appropriately to submit in a court of law?		
Best Practices		
Was an IR process review conducted?		
Was an IR process review recommendation process updated as a result of the review?		

Best practices

When using log files for evidence, timestamps are used to track packets through the network. Unfortunately, most network devices and servers clocks are not synchronized, which may make such evidence inadmissible in court. Using a network tap allows you to capture raw data without a network device timing or retiming the packet. Centralized storage devices can be used to save and protect historical network traffic for review at a later time.

Review current forensics tools and methods frequently, and ensure that the IR staff is trained in collecting and storing this information. The companies' legal department or local law enforcement agencies may have additional insight into forensics issues.

Best Practices

A process review meeting is held to determine quality of the event procedures and processes, and where improvements can be made. Data and forms used during the entire process are valuable to review and analyze. Each action or communication should be recorded and time-stamped. This requirement often dictates that someone is available for note taking and communication, especially in large organizations or where multiple contractors may be involved, or where tracking software is unavailable.

Schedule when recommendations and changes to the emergency management plans will be complete after an event. This ensures that the next event will be run more effectively.

Emergency documents should be concise with defined goals. They should be written to accommodate a variety of issues.

The importance of planning

While our reliance on networked computer systems has increased, so has our susceptibility to outages. A comprehensive and process centric plan to work through these events is mandatory to maintain business resilience and customer confidence. Increasingly, government regulations require that businesses provide documentation related to Disaster Recovery and Business Continuity processes.

Organization, planning and testing are the key elements to a worthwhile process centric system. Staff should train and test the processes regularly to confirm that each individual understands their specific roles and are capable of performing additional duties if required.

Remediation and data collection tools and equipment should be tested and updated. A variety of open source tools are available to augment commercial software, since open source tools may not meet admissible data collection requirements for some courts.

Emergency documents should be concise with defined goals. Detailed information that changes frequently should be consolidated in appendices or individual documents, which make them easier to update. Overall, plans should be generic and written to accommodate a variety of issues. Maintaining this process is challenging in today's fast-paced environment, but the savings on downtime, customer confidence and business resilience are worth the investment.

Datacom Systems Inc.

9 Adler Drive
East Syracuse, NY 13057

250 Park Ave.
7th Floor (Suite 7072)
New York, New York 10177

Datacom Systems Inc. UK
107 Cheapside
London
EC2V6DT

Enquiries
US & Canada: +1 315 463 1585
Europe: +44 (0)20 7397 3795

www.datacomsystems.com