Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Security Incident Handling in High Availability Environments

The telephony industry has, over time, developed very mature incident handling procedures, due in no small part to the need to manage contractual expectations and obligations on the part of both suppliers and operators. But as this industry was uniquely focused on maintaining contractually-promised Five Nines service levels, their ability to respect modern-day security-related expectations in their incident handling processes may not be possible without making some significant and much needed adaptations. This paper ...

Copyright SANS Institute
Author Retains Full Rights

AD

Security Incident Handling in High Availability Environments

GIAC (GCIH) Gold Certification

Author: Algis Kibirkstis, kibia@ethisecure.com
Advisor: Joel Esler

Submittal 2: September 8 2009

Abstract

The telephony industry has, over time, developed very mature incident handling procedures, due in no small part to the need to manage contractual expectations and obligations on the part of both suppliers and operators. But as this industry was uniquely focused on maintaining contractually-promised Five Nines service levels, their ability to respect modern-day security-related expectations in their incident handling processes may not be possible without making some significant and much needed adaptations. This paper will describe an incident handling process for high-availability systems, compare it to a popular security incident handling model, and propose to the telephony industry ways of sufficiently addressing confidentiality and integrity considerations, all while respecting their business need of maintaining high levels of service availability.

© SANS Institute 2009, Author retains full rights.

1. Introduction

Tolerance levels to various types of system outages give an interesting glimpse into what people in the Western world consider as service-level priorities. If faced with a cable television outage, the average North American would most probably be frustrated and check back in a half-hour or so, unless they were about to miss their favorite program. If there would be an electrical failure, that individual's first instincts may be to check if the neighbors are experiencing the same problem, and then hope that the power comes back within the next five minutes. Yet the average landline telephone subscriber expects to hear a dial tone within a second from when they pick up their headset, and will express concern about system problems if they don't hear that OK signal within a mere 3 seconds (Sprint, 2003).

As a result, telephony operators (telcos) go to great lengths to ensure "carrier-grade" levels of system availability (Sun 2008): design rules clearly specify that system and network availability must prevail, even in the event of billing system failures; failover and redundancy mechanisms are quick and finely tuned, so as to limit perceived availability problems; and outages trigger mature management processes at both the operator and vendor levels. Outage managers not only track progress during the managed event, but perhaps most importantly, carefully record the exact times when these events happen so that they know exactly how long their system disturbances lasted.

A typical managed outage is discovered through a telco operator's network operations center (NOC) and managed using their incident handling process. The vendor of the target system would be promptly contacted, informed of the situation, which would then trigger the assembly of a group of their own to assist in the handling the outage. Groups consisting of crisis managers, technical specialists and decision takers handle the situation until resolution.

Communications is a critical part of outage management, not only between technical staff and management, but also between peers on each side of the vendor/operator partnership. Technical specialists do what they can to bring the target system back to a standard operational state, while the management teams track progress

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

and provide guidance. The principal stakeholders, accountable for the service performance of the affected environment, need to agree on strategic decisions in order to being conclusion to incidents in a mutually acceptable manner.

System availability, commonly defined in telco circles as In-Service Performance (ISP) or as a Service Level Agreement (SLA), is generally considered to be the principal measure on which reliability of service is quantified for computing systems. In the case of telecommunications carrier systems, the fundamental guideline followed during outage or disturbance management is to bring service back to "normal" as quickly as possible. While processes are certainly followed, and record keeping is paramount, and protocol is strictly observed between operator and vendor, taking care of the effect of a disturbance or outage – the degradation or loss of service itself – is certainly more an immediate priority for both parties than determining the cause of incidents. Certainly faults get discovered during outage management and lessons are learned, but if vulnerability discovery gets in the way of problem solution, often the stakeholders will insist on bringing their systems back on-line first, and ask that discovery efforts be postponed until sometime afterwards.

Which leads into the following question: How well has the telephony industry adapted to manage the risks inherent with today's environments – the deployment of telephony systems over IP networks? Can their focus remain solely with controlling only the Availability aspect of the CIA security triad, at the expense of Confidentiality and Integrity concerns? Certainly, the closed environments traditionally associated with telephony networks helped assure high levels of confidentiality, because access to those networks was limited in a physical manner to partner operators, but the shift to using open network technologies breaks that paradigm. By strict adherence to legacy communications protocols, and through partnership agreements that determined how charging and billing would be performed (sometimes through obligatory comparison of transaction logs from both sides of each individual communication), data integrity was assured to mutually satisfactory levels, but how reliable would data transmissions become if they were exposed to remotely-executed threats that could allow people to make a mockery of billing systems?

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

And how should security-related incidents be managed? If exploited security vulnerabilities were investigated and evidence meticulously collected during outage management, then restoration of service would be delayed, resulting in longer delays before service restoration and entailing increased losses of end-user customers by the victim operator. This challenge of meeting today's security challenges in the century-old realm of telephony is a difficult fit, one that needs to take advantage of the strengths of both legacy and modern management strategies for ensuring high-availability service, in a time where telephony's relevance is challenged by today's ever-increasing reliance on messaging technologies.

Algis Kibirkstis, kibia@ethisecure.com

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

2. High Availability

In order to define a way forward for handling security incidents for carrier-grade systems, it is imperative to appreciate the challenges, needs and expectations of the high-availability marketplace.

2.1. What is High Availability?

High availability systems are broadly considered to be environments that are resistant to a variety of triggers that may lead to system disturbances (a reduction in the level of service) or outages (a complete loss of service). Also defined as Fault Tolerance (Vargas, 2000), it is attributed to a series of discrete factors contributing to an overall level of service assurance that defines a system's ISP: its ability to provide intended service in a continuous and reliable manner.

2.1.1. Component Reliability

Hardware component failure in systems can result in a disturbance or loss of service at the entire system level, but these risks can be mitigated through the use of redundant mechanisms and by procuring higher quality equipment. Hardware-level fault tolerance is commonly available from many vendors through integration of redundant power supplies, RAID disk array implementations and more stringent quality controls during component manufacturing. Failures at the hardware level are generally unnoticed by end-users if fallback mechanisms function properly.

Measurements of reliability for hardware components may be obtained from product literature. Mean Time Between Failures (MTBF) and Failure Rates are popular metrics for defining quality on the reliability scale (Vargas, 2000), and provide a way for vendors to differentiate their products for the high-availability market.

2.1.2. Architectural Redundancies

At the network level, improvements towards increased system availability can be introduced by the development of fault-tolerant network architectures: routers can be configured to send packets through alternate paths if a particular sub-network becomes unreachable; sets of load balancers manage sessions between external clients and farms

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

of back-end servers; clusters of servers are implemented in N+1 redundancy deployments, maintaining capacity of service if one system fails (Hughes, 2009); replicated environments in geographically remote locations provide "hot", "warm" or "cold" standby facilities in the event of local impacts such as fires, floods, earthquakes or malicious break-ins. Failures at this level may or may not be noticed by end-users, depending on the latency associated with the availability of the failover component.

Component-level MBTF data, together with risk assessments that predict the chances that pre-defined risks get manifested, can help towards determining the effectiveness of network-level redundancy implementations.

2.1.3. Software Robustness

Software can play a major part in the resilience of a system. A robust fault-tolerant operating system can automatically perform various types of management tasks without requiring a reboot, in order to ensure continuous system operation: watchdog programs running in memory can detect failed computing services and immediately restart them; faulty CPUs can simply be ignored in multi-processor servers during runtime (Vargas, 2000). Failures at the software robustness level often result in either increased service latency or a reduction of capacity of service, but such impacts can be mitigated through architectural redundancy mechanisms.

Operating system features, such as the Solaris Predictive Self Healing feature (Sun, 2008) and the monit Linux package (Rootninja, 2009), support monitoring of system functions as well as reactive functions to disable or restart faulty hardware and software components.

2.1.4. Recovery Capabilities

In the event of failure at the system level, the speed of a system's shutdown and startup functions impacts system availability greatly; if the startup of a system with a 99.999% stated ISP takes five minutes to fully boot, a single restart of the server would already break a contractual agreement. Similarly, system restoration from backups can be greatly hindered if the backup media cannot be quickly read into system memory.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Improving the maintainability or serviceability of systems can go a long way in improving an organization's response to discovered system faults. Minimizing the number of startup processes at boot time, or running independent startup processes in parallel, can dramatically improve response times during the last stage of system recovery; investing in regular tape drive and optical drive upgrades can provide an quicker path to recovery with minimal expense.

2.2. Quantifying Availability

With a myriad of mechanisms available for assuring improved levels of fault tolerance, problems still happen. Just as there are metrics for determining levels or resilience, there are ways to define and assess the overall capabilities of a system with respect to availability.

2.2.1. Service Level Agreements

SLAs are generally defined contractually for carrier-grade systems; a factor of availability is defined (such as 99.9%), commonly accompanied by a payment scale if the event that the SLA is not maintained. Assessments of SLA compliance are also scheduled through contract; it is not uncommon to have measurements taken monthly but assessed on a rolling yearly scale.

Costs for high-availability systems are higher than those that for those systems that do not promise levels of availability. As a result, the procurement of highly fault tolerant systems tends to be restricted to certain target market segments that can afford this expensive feature, such as the military, air traffic control, and telecommunications carriers. Essential services such as healthcare databases, oil pipelines and electrical grid management systems have client and regulatory pressures to meet defined availability expectations, making them candidates for the procurement of this type of equipment. Over the last decade or so Internet-accessible storefronts, reservation systems and remote security monitoring services have also invested heavily into availability improvements, in order to attract and keep their clientele.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

2.2.2. The Mythological Five Nines

When Wernher von Braun, director of NASA's Marshall Space Flight Center, was asked in 1967 for a reliability factor on a rocket in development, he came back with an answer that was interpreted as Five Nines. When asked by that officer how he came to that figure, his response was that he had consulted five of his German-speaking colleagues to ask if they had any problems in their areas, with each responding "nein" (Tompkins, 2005).

True story or not, this anecdote illustrates how arbitrary it can be to define levels of availability. Specifically targeting certain sectors of government and industry, vendors define levels of availability in their product documentation. Contractual agreements for telco and other sectors also include targets values for system availability.

SLA	Uptime	Downtime per year
Three Nines	99.9%	8.77 hours
Four Nines	99.99%	52.60 minutes
Five Nines	99.999%	5.26 minutes
Six Nines	99.9999%	31.56 seconds
Seven Nines	99.99999%	3.16 seconds

Five Nines has historically been held as a target objective for high-availability systems, and is commonly held as the baseline for carrier-grade systems (Shepler, 2009). An allowance of five minutes of system unavailability over a one-year period is a remarkably short amount of time, yet the vendors of today's telephony switches continue to consent to having their systems measured against this arbitrary figure.

Why is that? The answer may lie in the fact that yesterday's Five Nines promises are giving way to today's contractual demands for 100% availability. While this number jumps off the page as being unreasonable and impossible to deliver on the part of vendors, in practice this has only changed the way contracts are managed in a small way, for SLA values are fundamentally marketing tools (Tretikov, 2009). At the end of (usually yearly) evaluation periods, vendor and operator representatives meet; and if there was an outage on systems protected contractually by SLA, representatives mutually agree upon an outage period and negotiate some type of compensation for the operator. In other words, industry is moving away from the old model of aiming for SLA values and is moving all responsibility for system outages and disturbances to the vendor.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

2.3. Telecommunications and Carrier Grade Systems

The telco industry is an excellent example of a network that provides omnipresent, prompt, reliable and highly available service. Due to its current ability to support inexpensive, on-demand real-time communications across the street and across the globe, telephony remains a dependable means of communications between world leaders, business partners and family members – even with the increasing adoption of electronic message-based communications such as instant messaging (IM), voice mail and e-mail.

With the widespread adoption of telephony came increased dependency on the product. For example, emergency services quickly relied upon the telephone to receive and send out notifications. It is no coincidence that Five Nines availability is commonly known as Carrier Grade availability, as it defines a quality of service baseline that can be appreciated by the average person.

2.3.1. Benefits

High availability in modern telephony can be attributed in part to the way it is currently deployed. As one-to-one copper lines between end-users made way for shared lines using modulation techniques (Chuma, Masupe & Mbewe, 2004), and as human switchboard operators implementing physical links between subscribers were replaced by automated exchanges (Tahvanainen, 2009) capable of handling multiple simultaneous calls (telephone, 2009), costs dropped significantly. With cost savings, vendors were given the necessary financial support to develop exchanges with failover mechanisms and reboot times that supported contractual Five Nine obligations (Jonback & Schultz, 2001). Low power needs to drive landline handsets, complemented by dedicated power supplies physically distinct from the electrical power grid, made it possible for people to communicate despite power outages.

This last aspect continues to be relevant to the average consumer that is attracted to today's alternatives to landline telecommunications, such as radio-based GSM wireless telephony or voice over IP network (VoIP) options. Despite the powerful motivations behind the adoption of wireless (mobility) and VoIP (cost savings), many landline

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

subscribers maintain their subscriptions because of the availability of service during electrical power outages.

2.3.2. Expectations

Breaking contractual ISP obligations can be extremely costly not only for vendors, but also for carriers that sell a service historically associated with "always there" availability. As competition increases between telephony providers across the world, it has become increasingly possible for end-users to change telephony suppliers with relative ease; and in some places, subscribers even have the ability to retain their existing phone number when moving to a competitor's service (Government of Canada, 2005).

Applicable fines for breaking SLAs can vary greatly, depending on the contractual partnership, the types of equipment procured and the impacts of any particular disturbance. Critical exchange disturbances affecting nationwide Tier 1 carriers (Malheiro, 2008) are rumored to trigger indemnities in the range of 1000 USD a second for scheduled (maintenance) outages and of over 10000 USD for unscheduled downtime resulting from failures. According to these figures, an hour-long unplanned failure would result in a vendor outlay of 3.6 million USD, making it imperative for vendors to back up their claims of high ISP values with robust and resilient implementations and recovery techniques.

2.3.3. Residual Challenges

As described earlier, maintaining levels of high availability depends on various technical and administrative factors. When outages or disturbances do occur and require human intervention, it is imperative that the methods used to return normal service be performed in a tested, documented and timely fashion. Sensitive to customer needs and contractual expectations, telecommunications vendors and carriers have developed mature outage management procedures that carefully track and methodologically correct system faults, in order to return service back to expected levels.

Historically, and with strong justification, carriers prioritize system and network availability over all else; for after all, that is the metric against which they are contractually bound and regularly measured. But there has been a fundamental paradigm shift in the telco industry: an unstoppable and systematic migration from the trusted

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

closed network environment of the telephony network to the untrusted open network of the Internet's IP networks. As convergence brings together the realms of voice and data communications, it is reasonably taken for granted today that the telephony network of tomorrow will be purely IP based.

What to make of this new paradigm? Telephony is steadfastly moving towards open networks using open protocols, and away from proprietary hardware running proprietary software. As a result, the risk and threat levels to these environments have grown exponentially, and vulnerabilities in carrier systems have become as exploitable as any other system accessible via the Internet. Yet the priorities for telco have remained the same: maintaining high availability above everything else.

The problem is that with a strict focus on availability, there is a lesser focus on the other two fundamental aspects of information systems security: confidentiality and integrity (Tipton & Henry, 2007). With IP networks, assumptions about the confidentiality of voice communications must be quickly discarded unless cryptographic mechanisms are introduced to better ensure privacy of communications. Without tamper-proof integrity protection mechanisms such as message integrity codes (MICs) or digital signatures, billing mechanisms can be compromised and caller identities can be falsified.

And if there is a singular intent on returning system and network functionality back to standard operational levels after discovery of a disturbance or outage, how can an IP-based carrier effectively respond to network threats – particularly threats that can quickly reoccur if no new preventive, detective and corrective measures get introduced?

Although carrier outage management methods have been a key component in safeguarding "always on" service levels, they need to be adapted to adequately respond to the new risks and threats that stand before them, all while respecting the availability constraints of the telecommunications industry.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

3. Incident Handling

Many organizations have formalized processes for handling unexpected events, including unanticipated security incidents. But are these occurrences truly unexpected, or simply impossible to forecast? Is it truly possible to prepare for unexpected events in a systematic and reproducible manner? The answer is a resounding yes; and for those not yet prepared for managing eventual disturbances, there are resources available to help you reach this objective.

While some may not have yet heard about security incident handling processes, most have certainly heard about Business Continuity Plans (BCP) and Disaster Recovery Plans (DRP). Most successful businesses can possibly be categorized in two groups: those that have successfully kept their business a going concern, by triggering their tested BCP and DRP when the need arose; and those that have yet to deal with business-threatening events. By preparing strategies for dealing with potential yet unlikely situations, organizations are able to respond quickly and act appropriately, greatly improving their chances of an eventual return to normal operations.

Disaster recovery planning is the formal establishment of ground rules and best practices, for the purpose of bringing back a normal level of operations after a disastrous event such as an earthquake, fire or flood. Roles are defined, actions are detailed, backups are regularly prepared, and redundant resources are set aside for such an eventuality; and most importantly, a way forward is charted for rehabilitating business functions, quite possibly in a different geographical location. On the other hand, business continuity planning considers all aspects for efficiently and effectively managing business interruptions – through strategies such as disaster recovery plans, crisis management procedures and emergency response directives (Weil, Northcutt & Edmead, 2004).

With such plans in place, organizations are ready for a multitude of events: from plane crashes that kill all members of a company's executive; to political insurrections that can bring business operations to a complete halt; to blizzards that can keep operational and support staff away from a corporate head office for days at a time.

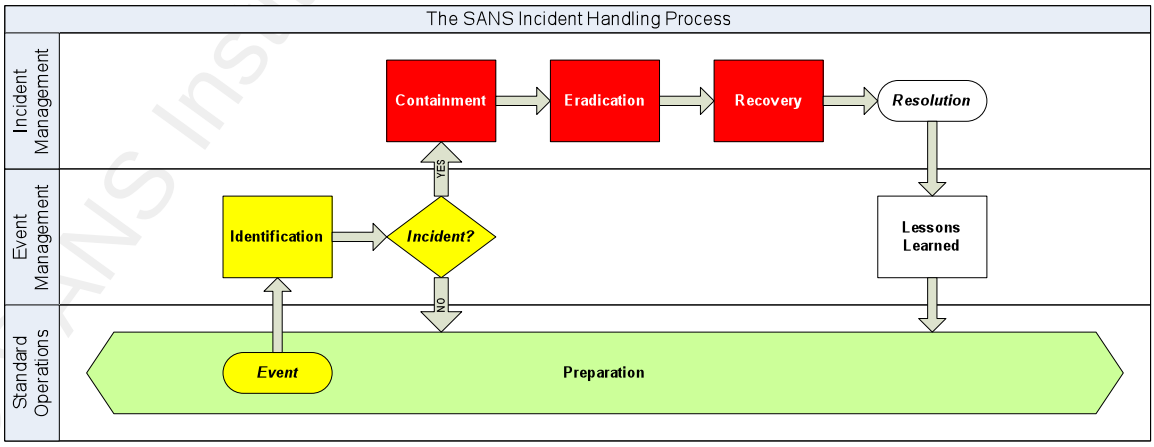
© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Incident handling is, in essence, the logical next step in organizational preparation for dealing with the unexpected and unscheduled. For while security events may not always appear to be catastrophic at discovery, the results can often bring about dramatic business impacts such as loss of service, loss of data, and loss of trust in the eyes of customers. Incident Handling (IH) processes and procedures, similarly to DRPs and BCPs, provide a methodology and framework for addressing, controlling and rectifying security-related events when they occur.

Several popular IH methodologies are available for adoption and consultation (Grance, Kent, & Kim, 2004) (Kossakowski, 1999) (Northcutt, 1998). For this discussion, the SANS six-step incident handling approach will be used as an example of an IH methodology, before moving ahead to present the specific challenges faced by telecommunications carriers in meeting availability expectations.

3.1. The SANS Institute's Six-Step Incident Handling Process

As in other popular IH techniques, the SANS Institute proposes a methodology that defines sequences of initial assessment followed by the execution of control and corrective measures; preceded by thorough preparation; and concluded with a follow-up exercise that feeds into continuous improvement of the overall process (SANS Institute, 2007). The process is defined in six distinct steps (represented as rectangles in the illustration below), which can be further categorized into three distinct handling stages (represented as rows): incident management, event management and standard operations.



© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

3.1.1. Preparation

The groundwork implemented in this initial step is critical in providing structure and guidance during times of crisis, in times when panic and emotion can cloud individual judgment and reason. In this phase policies are established, management support is enlisted, roles and teams are defined, physical resources are secured, methods are tested, and various communication interfaces are formalized (Northcutt, 1998).

With careful preparation, potential pitfalls can be avoided and negative impacts minimized during incident handling. For example, posting warning banners can provide legal protection in the event of malicious attacks. Building relationships with all members of the incident handling team, such as law enforcement and human resources, facilitates the mobilization of the team during times of need. Providing the necessary tools for handling incidents – including items such as checklists, log books, software, mobile phones and dedicated facilities (SANS Institute, 2007) – can dramatically speed up response times.

The selection of members of an incident response team is a critical step in this preparatory phase. Aside from technical staff and security specialists that have the competence to investigate and correct problems in software and hardware components, several layers of management and support staff are required to round out an incident handling team, preferably led by an experienced IH team lead to manage the event (Mandia, Prosise, and Pepe, 2003). Involvement from the following areas could prove to be extremely beneficial in certain scenarios, but may not be required in other instances: human resources, law enforcement, legal counsel, operations staff, and corporate communications to handle any interfaces to the media. Perhaps most importantly, direct involvement (or regular communication) with primary stakeholders is paramount, for they stand to be relied upon to provide business perspective and to give guidance in case there are conflicting interests to consider.

A robust IH process will clearly define the steps to take when handling incidents. In order to help efficiency, checklists should be provided to ensure that all necessary steps have been followed. With preauthorized scenarios, technical and management staff

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

have clear directives on when to call law enforcement, as well as when to "contain and clear" and when to "watch and learn" (SANS Institute, 2007).

3.1.2. Identification

The IH process is triggered when an event is discovered, usually through standard operational practices. In this "event management" stage, an assessment is made through analysis and correlation of information, followed by a determination if there was an attempt to cause harm. Opinions are then communicated through pre-approved channels, and a decision to declare the occurrence of an incident takes place (SANS Institute, 2007).

Several critical steps fall quickly into place during this phase. Once there is an indication that there may have been malicious activity, careful note taking and maintaining a traceable chain of custody for all evidence is critical for mounting successful legal campaigns against attackers. Coordination with other operations staff will greatly facilitate the investigative and assessment tasks. And once it has been concluded that the discovered events are the result of a security incident, IH team members are contacted and the incident management activity is initiated (Northcutt, 1998).

3.1.3. Containment

The core activity in containment is to "stop the bleeding" and to limit impacts on neighboring areas of the target environment (SANS Institute, 2007). The SANS process defines three sub-phases: short-term containment strategies to stop further damage to the system(s); backup generation to support legal and forensic investigation; and subsequent long-term containment activities, to further hinder the spread of the problem while attempting to maintain any current production levels.

During this first interventionist phase of the IH process, the team is deployed and actively involved with incident handling. Initial containment activities should be performed in a way that would not facilitate detection by an attacker; popular techniques to quickly limit damage and limit reactionary damage from intruders include the disconnection of network cables and the changing of passwords. By promptly harvesting backups, organizations are able to collect evidence of actual system state at time of

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

incident discovery, after which they can move more aggressively towards a full containment and subsequent eradication of the problem.

> *"One of the most difficult decisions, and one subject to extreme pressure by end-users and senior management, is what to do about the compromised system. Here you will decide whether a system should be shut down entirely, disconnected from the network, or be allowed to continue to run in its normal operational status so that any activity on the system can be monitored."* (Northcutt, 1998)

The preparatory phase of the IH plan can help organizations predefine priorities and prepare action plans for various incident scenarios, in order to facilitate decision taking for stakeholders during actual incident management.

3.1.4. Eradication

Once the administrative decisions have been made to perform corrective measures to the target environments, the technical staff is entrusted with the removal of the compromised components and the introduction of known-good replacement components. Additional investigation of the systems may reveal the causes of compromise and the methods used to perform the malicious act. Improving network defenses and testing for network vulnerabilities are also important components of the eradication phase of the incident handling process (SANS Institute, 2007).

3.1.5. Recovery

In this last phase of the "incident management" stage, the restored systems are brought back online and regression tested to demonstrate expected characteristics and functionalities. Once this has been demonstrated to the satisfaction of primary stakeholders, the systems are then returned to a production state and carefully monitored for possible re-exploitation (SANS Institute, 2007).

3.1.6. Lessons Learned

In order to reduce the possibility of future incidents, and to reap the maximum benefit from the time and effort invested in the handling of the incident, details of the incident handling activity should be promptly documented and reviewed by affected

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

members of the organization. The outputs of the review then become valuable inputs towards the ongoing tuning of the organization's incident handling process.

3.2. High Availability Concerns

At this point, carrier outage management processes have been presented and an incident-handling model has been described. Are they fundamentally different, or can the telecommunications process be adapted to incorporate critical aspects of security incident management strategies?

3.2.1. Carrier Specific Challenges

Specific challenges exist for the telecommunications industry. Recommendations to use out-of-band communications when troubleshooting computing systems are sound (Northcutt, 1998), because an intruder could intercept cleartext e-mail and IM messages. But in the case of telco systems, voice communications are an integral part of the carrier network: compromised servers could potentially flag details of call initiation, and may even provide voice call monitoring capabilities to the attacker. To adequately address this challenge, it may be a good idea for carriers to arrange reciprocal agreements with competitors for the use of their communications infrastructure, protected through a carefully crafted non-disclosure agreement (NDA) that would not tolerate the use of any compromise information for competitive advantage.

The close vendor-operator relationships that persist in telco circles can also serve to complicate incident handling strategies. When carriers detect problems with their switching equipment, vendor agreements tend to make their support staff immediately available for addressing client needs, introducing a parallel incident handling team to address the challenge at hand. When managing incidents, even the most mature outage management processes can get challenged and derailed by peers on the other side of the vendor-operator divide. While there is a generally held axiom in much of the world that "the customer is always right", the vendor may find difficulty in agreeing to pressure-driven carrier decisions that can affect the way vendors collect information and maintain stated ISP levels.

Perhaps the biggest challenge that is faced by the telecommunications industry, when considering the introduction of general security incident handling processes to their

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

telco outage management processes, lies with the fundamental differentiating factor: the need for telcos to provide high availability service. It would be absurd for carriers to put aside decades of experience and a history of dependability by taking systems offline for protracted periods of time, in order to collect sufficient evidence to get a casual intruder arrested – for they may not be in business long enough to see the issue go through the courts.

3.2.2. Maintaining Operational Redundancies

Harvesting evidence at the onset of incident discovery is paramount to successful legal proceedings against intruders; the earlier the information can be collected (through disk copies and media backups), the more reliable the evidence becomes to the judge and jury. As time elapses between incident discovery and data collection, it becomes increasingly difficult to differentiate troubleshooting activities from malicious actions in logs and on file systems.

But can telcos afford (or contractually permitted) to rip out hard drives from their systems for evidence collection and archiving, and temporarily lose their ability to tolerate physical or logical failure of their remaining hard drives? If not, standard RAID 1 (disk mirroring) or RAID 5 (disk striping with parity data) implementations (AC&NC, 2009) would be ill suited for supporting remote forensic examinations or law enforcement data collection requirements.

3.2.3. Handling Pressure Situations

There is a story in consulting engineering circles about a junior project manager getting a phone call on a Friday afternoon from the head contractor in charge of a large construction project. The head contractor informs the project manager that there's a problem: a critical piping run cannot be installed because a column stands in its way. When the project manager tells the head contractor that he needs to investigate the matter, the head contractor consents to the investigation, but not before passing on some advice: as he performs his due diligence, he will be holding up the work of nine people – the head contractor, two pipe holders, one pipe welder, one welding inspector, two scaffolders, and two pump installers interrupted from working on equipment below the scaffolding. And if he takes too long to come back with an answer, he will have to let his

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

workers go home for the weekend, and he will lose access to the welding inspector for a week, thereby introducing costly delays to the construction project.

The pressure felt by the project manager in the story above might be trivial compared to the pressure felt by those handling outages in carrier environments, due to the severe penalties associated with breaking SLAs. When faced with reoccurring security incidents, and with pressure from some stakeholders to find the cause of the repeated break-ins, how do team members react when the system owner (or some other primary stakeholder) barges into discussions and demands that the system be brought back into operation immediately?

And who is the primary stakeholder? Who should determine the way forward during incident handling for carrier grade equipment? Is it the operator's team leader, or the vendor team leader? Perhaps ultimate authority lies with system owners or technical account managers from both organizations, but what if the problem escalates to a vice-president or even the COO or CEO of one of the companies? Who takes the final decisions in those cases?

Without a policy that carefully catalogs and defines direction in handling these types of contentious scenarios, organizations may often find themselves responding to incidents according to the personal priorities of the most powerful member of the response team.

3.3. Meeting Today's Challenges

It is believed that overriding availability concerns on the part of carriers can continue to be respected, all while providing support for necessary security-related safeguards, through a combination of added investment and updated processes. Regardless if telco outage handling procedures are expanded to consider security issues or if a security incident handling method is adapted to the needs to the telco industry, improvements would have to be introduced in the following aspects:

1. Telecommunications carriers should maintain outage management processes that look for potential security violations. The discovery of security incidents should trigger specific strategies to contain and eradicate such vulnerabilities.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

2. Critical telecommunications systems should implement hard disk redundancy mechanisms that can tolerate the loss of two or more hard disks.
3. Disk cloning equipment should be made readily available so that copies of hard disks can be provided to law enforcement and forensic analysts.
4. Copies of evidence, such as hard drives and media backups, should be sealed, labeled, dated and demonstrably access controlled until submitted to law enforcement.
5. Out-of-band communication capabilities should be made available in the event of a breach in the telecommunications network. The production network (including data and voice channels) should not be used for communicating information, progress or status during incident handling.
6. Agreements should be established with each partner company to define clear and precise scenarios, with regards to which security incidents require a withdrawal of system availability and which incidents require service retention.
7. Such agreements should be agreed upon by vendor and operator senior management. Senior management, as well as law enforcement and legal counsel, should be part of the incident handling team and should sign off on the strategies defined in policy.
8. Technical staff should be required to complete their investigations, even in the event that systems were not fully remediated and kept in production. Findings and assessments should be documented and reviewed by incident handling team members and other affected members of the organization. The incident handling process should be subsequently updated if needed.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

4. Conclusion

Carrier networks have maintained mature outage management processes in order to minimize downtimes and maintain promised availability levels to a demanding marketplace. While contributors to unavailability in legacy telecommunications networks were historically limited to component failures, environmental control failures and human error (CCTA, 1992), the migration towards open systems and IP networks has introduced a need to consider the possibility of security incidents when managing outages.

In order to continue providing high availability levels in their service offerings, today's operators need to adapt their processes in order to support forensic investigation and law enforcement efforts. In addition, current support agreements between vendors and operators should be adapted so that security incidents can be investigated without immediate pressure to bring service back to promised levels.

By adopting best-of-breed security incident management strategies, carriers will be better prepared to face the security challenges of today and tomorrow, while continuing to provide service availability levels that help them maintain relevance and market share in today's "always connected" world.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

5. References

Advanced Computer & Network Corporation, (2009). RAID Tutorial. Retrieved September 7, 2009, from AC&NC Web site: http://www.acnc.com/raid.html

Agsalud, J (2009, June 1). What is a service level agreement?. Retrieved September 6, 2009, from Around Hawaii Web site: http://www.aroundhawaii.com/business/technology/2009-06-what-is-a-service-level-agreement.html

Allen, J H. (2001). *The CERT guide to system and network security practices*. Upper Saddle River, NJ: Addison-Wesley.

Beaker, (2009, June 8). The Nines Have It…. Retrieved September 6, 2009, from Rational Survivability Web site: http://www.rationalsurvivability.com/blog/?p=989

Birkholz, E P. (2003). *Special Ops: Host and network security for Microsoft, Unix and Oracle*. Rockland, MA: Syngress Publishing.

Blaauw, P (2008). BCP/DRP case study: Adapting major incident handling response frameworks to a corporate environment. *Information security for South Africa: Proceedings of the ISSA 2008 Innovative Minds Conference*, Retrieved August 6, 2009, from http://icsa.cs.up.ac.za/issa/2008/Proceedings/ISSA2008Proceedings.pdf

Buffington, J (2008). Breach notification in incident handling. *SANS Institute InfoSec Reading Room*, Retrieved August 6, 2009, from http://www.sans.org/reading_room/whitepapers/incident/breach_notification_in_incident_handling_2114

CCTA, (1992). *Availability Management*. Norwich, Great Britain: Central Computer and Telecommunications Agency.

Chuma, J M., Masupe, S & Mbewe, D (2004). Introduction to pulse code modulation (PCM). Retrieved September 8, 2009, from Washington State University Web site: http://cbdd.wsu.edu/kewlcontent/cdoutput/TR502/page13.htm

Government of Canada, (2005, December 20). News release: CRTC extends benefits of number portability to wireless consumers on a timely basis. Retrieved September 7, 2009, from Canadian Radio-telecommunication and Telecommunications Commission Web site: http://www.crtc.gc.ca/ENG/NEWS/RELEASES/2005/r051220.htm

Grance, T, Kent, K, & Kim, B (2004). Computer security incident handling guide. NIST Special Publication 800-61, Retrieved September 7, 2009, from http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Hughes Network Systems, (2009). 1:N redundancy. Retrieved September 6, 2009, from Hughes Web site: http://www.hughes.com/HUGHES/Rooms/DisplayPages/LayoutInitial?Container=com.webridge.entity.Entity%5BOID%5B894E2D23C031274DADB1219E2B500C92%5D%5D

Jonback, M, & Schultz, S (2001). Open architecture in the core of AXE. Ericsson Review, 1, 24-31.

Kossakowski, K-P (1999).Responding to intrusions. *Carnegie Mellon Software Engineering Institute*, *CMU/SEI-SIM-006 (February 1999)*

Malheiro, A (2008, January 4). Let's get to basics: Tier 1 network definition.... Retrieved September 7, 2009, from A.Malheiro::Blog Web site: http://amalheiro.wordpress.com/2008/01/04/lets-get-to-the-basics-tier-1-network-definition/

Mandia, K, Prosise, C, & Pepe, Matt (2003). *Incident response & computer forensics, second edition*. Emeryville, CA: McGraw-Hill/Osborne.

Moldes, C J. (2009). PCI DSS and incident handling: What is required before, during and after an incident. *SANS Institute InfoSec Reading Room*, Retrieved August 6, 2009, from http://www.sans.org/reading_room/whitepapers/incident/pci_dss_and_incident_handling_what_is_required_before_during_and_after_an_incident_33119

Northcutt, S (Ed.). (1998). *Computer security incident handling step by step, version 1.5*. SANS Institute.

SANS Institute, (2007). *Security 504/504.1: Hacker techniques, exploits, and incident handling: Incident handling step-by-step and computer crime investigation, V040907*. SANS Institute.

Shepler, J E. (Ed.) Telecom's Holy Grail of Five Nines Reliability. Retrieved September 6, 2009, from Enterprise VoIP Web site: http://www.enterprisevoip.com/articles/fivenines.php

Sprint (2003). *Sprint Network Outage Notification Request* (03/03 Version 1 ed.), Retrieved August 9, 2008, from http://www.sprint.com/localwholesale/docs/CLEC_forms/network_outage_notification_000.pdf

Sun OEM Platforms Engineering Group, (2008, May). Solaris The Carrier Grade Operating System. Retrieved September 6, 2009, from http://www.sun.com/servers/netra/docs/solaris_carrier_grade_os.pdf

Tahvanainen, K V. (2009). Crossbar switches replace operators. Retrieved September 8, 2009, from The history of Ericsson Web site:

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

http://www.ericssonhistory.com/templates/Ericsson/Article.aspx?id=2095&ArticleID=1380&CatID=362&epslanguage=EN

telephone. (2009). In *Encyclopædia Britannica*. Retrieved September 08, 2009, from Encyclopædia Britannica Online: http://www.britannica.com/EBchecked/topic/585993/telephone

Tipton, H F., & Henry, K (Eds.). (2007). *Official (ISC)2 guide to the CISSP CBK*. Boca Raton, FL: Auerbach Publications.

Tompkins, P K. (2005, September 9). Organizational communication as technical management: Wernher von Braun's principles and practices at the Marshall space flight center. *2005 MAPLD International Conference*, Retrieved September 6, 2009, from http://klabs.org/mapld05/presento/124_tompkins_paper.doc

Tretikov, L (2009). What's in a 100% SLA?. Retrieved September 7, 2009, from Cloudheads Web site: http://www.cloudheads.net/profiles/blogs/whats-in-a-100-sla

Vargas, E (2000).High Availability Fundamentals. *Sun BluePrints OnLine*, *November 2000*

Vinson, J (2009, May 28). Infinity Nines of Uptime. Retrieved September 6, 2009, from The Daily WTF Web site: http://thedailywtf.com/Articles/Infinity-Nines-of-Uptime.aspx

Weil, S, Northcutt, S, & Edmead, M T. (Eds.). (2004). *SANS step-by-step series: Disaster recovery and business continuity, version 2.1*.SANS Press/SANS Institute.

Wood, C C. (2008). *Information security policies made easy, version 10.0*. Houston, TX: Information Shield.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Last Updated: December 22nd, 2014

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Brussels 2015	**Brussels, BE**	**Jan 26, 2015 - Jan 31, 2015**	**Live Event**
SANS Dubai 2015	**Dubai, AE**	**Jan 31, 2015 - Feb 05, 2015**	**Live Event**
Cyber Threat Intelligence Summit & Training	**Washington, DCUS**	**Feb 02, 2015 - Feb 09, 2015**	**Live Event**
SANS Scottsdale 2015	**Scottsdale, AZUS**	**Feb 16, 2015 - Feb 21, 2015**	**Live Event**
10th Annual ICS Security Summit	**Orlando, FLUS**	**Feb 22, 2015 - Mar 02, 2015**	**Live Event**
SANS Secure India 2015	**Bangalore, IN**	**Feb 23, 2015 - Mar 07, 2015**	**Live Event**
SANS DFIR Monterey 2015	**Monterey, CAUS**	**Feb 23, 2015 - Feb 28, 2015**	**Live Event**
SANS Munich 2015	**Munich, DE**	**Feb 23, 2015 - Mar 07, 2015**	**Live Event**
SANS Cyber Guardian 2015	**Baltimore, MDUS**	**Mar 02, 2015 - Mar 07, 2015**	**Live Event**
SANS Northern Virginia 2015	**Reston, VAUS**	**Mar 09, 2015 - Mar 14, 2015**	**Live Event**
SANS Secure Singapore 2015	**Singapore, SG**	**Mar 09, 2015 - Mar 21, 2015**	**Live Event**
SANS Abu Dhabi 2015	**Abu Dhabi, AE**	**Mar 14, 2015 - Mar 19, 2015**	**Live Event**
SANS Secure Canberra 2015	**Canberra, AU**	**Mar 16, 2015 - Mar 28, 2015**	**Live Event**
SANS Security East 2015	**OnlineLAUS**	**Jan 16, 2015 - Jan 21, 2015**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**