Considerations for Implementing a Next-Gen Incident Response Process

John McDonald, Senior Consultant,

IT Risk Management and Security

October, 2015

OPENSKY
A TÜV Rheinland Company

Table of Contents

Table of Contents

© OpenSky Corporation

Introduction

The constant bombardment of breach reports in the news recently has many organizations asking the question, “Are we prepared?”. The last few years have seen dramatic shifts in IT, with cloud solutions, mobile devices, social networking and virtualization dramatically expanding the scope and complexity of the typical IT infrastructure, making that question much more difficult to answer. As IT and security staffs are being tasked with tracking, managing and securing assets within and without an increasingly amorphous perimeter, attackers and the tools they use are growing in complexity, sophistication and scale. According to The Enterprise Strategy Group’s ‘Tackling Attack Detection and Incident Response’ report (April 2015), the rate of security investigations across all types of organizations continues to grow:

	All Survey Respondents	Less than 999 Employees	1,000 to 4,999 Employees	More than 5000 Employees
Average number of security investigations	78	31	41	150

(The Enterprise Strategy Group, 2015)

70% of these attacks were general “shotgun-style” of attacks, not targeting a specific organization; however, more telling is the fact that almost 30% of these attacks were targeted at a specific organization, significantly increasing the probability that they will succeed in penetrating the defenses. The impact of these trends is that organizations are realizing that it’s no longer a case of “if” they are penetrated, but “when” they are. It’s not uncommon for organizations to find themselves handling dozens, if not hundreds, of security incidents per year. As a result security teams are being forced to reevaluate their traditional approach of devoting virtually all their efforts and resources primarily to preventative controls, and adopting a more balanced allocation between prevention, detection & response.

This whitepaper provides an overview of how organizations will need to approach incident response and management in the face of an ever-growing number of attacks and penetrations. Note that it is not meant as a step-by-step guide on how to implement an incident response/management strategy, but rather to provide ideas and guidance on what should be considered.

© OpenSky Corporation

Foundation

In most organizations, security incident management has solely been the domain of the IT Security team and has been executed primarily as a highly technical, discrete process, with minimal interaction or input from the rest of the organization. While this approach worked when an organization only had to worry about one or two incidents a year, it tends to exceed an acceptable level of business impact when dealing with dozens or hundreds of such incidents in the same timeframe.

For example, consider a scenario where the IT Security team has discovered a penetration that has distributed malware to several internal servers. The team may spend several days identifying, isolating and manually cleaning up the infected systems. In today's business climate, where downtime can be measured in thousands to millions of dollars per hour, or real impact to human health and safety, such an extended approach to incident management is no longer acceptable.

In order to deal with today's business and risk climate, the foundation of any incident management process must be the development and integration of business risk requirements, not just technical drivers. Allowing (or even worse, requiring) the IT Security team to make all of the decisions when managing a security incident will most likely result in an increasing rate of unacceptable negative business impacts that will only get worse as the threat environment becomes more increasingly hostile.

What is an 'Incident'

The first (and one of the more difficult) steps when defining an incident response/management strategy is to define what the organization considers to be an 'event' and an 'incident'. Two of the more popular definitions are provided by the NIST SP 800-61 standard and ISO ISO/IEC 270035:2011 standard. These are as follows:

	Definition of Event	**Definition of Incident**
NIST SP 800-61	*An event is any observable occurrence in a system or network. Events include a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt. Adverse events are events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data.*	*A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.*

© OpenSky Corporation

ISO/IEC 27035:2011	*An information security event indicates that the security of an information system, service, or network may have been breached or compromised. An information security event indicates that an information security policy may have been violated or a safeguard may have failed.*	*An information security incident is made up of one or more unwanted or unexpected information security events that could very likely compromise the security of information and weaken or impair business operations.*

Both sets of definitions are reasonable, and can either be used as-is or as a foundation for the creation of organization-specific definitions. Other than the terms of 'event' and 'incident', organizations may also wish to define additional basic terms, such as:

- Attack
- Penetration
- Denial of Service
- Breach

Regardless of what is defined, the definitions should be clearly communicated to all personnel directly and indirectly involved in the incident management process.

Beyond the basic definitions, a classification schema also needs to be developed. The schema can incorporate factors such as the scale or scope of the incident, the potential impact to the organization, etc. A basic schema can be something as simple as a sliding scale between 'L0' and 'L5', with L0 being initial discovery of unusual activity and L5 being a major breach of sensitive assets; provisions should also allow for incidents to be re-classified as more information is uncovered. This will allow the organization to ensure that the impact of any given incident can be clearly understood at any step of the process by all personnel involved.

As indicated earlier, documenting and communicating all incident-related taxonomies to all personnel involved is critical to ensuring an efficient and consistent approach to handling incidents. This includes everyone from an IT admin who may be asked to delete a file during an incident to senior-level executives who may need to understand the phrasing of status updates.

The Process

While describing an incident management process itself can be simple, ensuring it encompasses all of the concepts, interactions and capabilities described in this whitepaper can be difficult. The NIST 800-61 and ISO 27035:2001 standards both provide excellent examples of generic processes which can be used as-is or as a foundation for developing a custom process.

© OpenSky Corporation

However, there are a number of factors that must be considered when developing such a process:

- It must encompass all concepts, interactions and components for the environment it supports.
- It must be flexible enough to allow for any type of incident the organization may encounter.
- It must be documented, communicated and trained on by all personnel that may need to support it like any other business process. Simply emailing a PDF document out that describes the process is not sufficient.
- It must be updated when the IT infrastructure, the organization, the threat landscape or any other factor that may impact the process changes. Such updates must be communicated to all impacted personnel.
- It must contain specific detailed procedures that are specified for each aspect of the business and infrastructure that may require unique handling.

Finally, once the process has been developed a software tool capable of supporting the entire process and all of its related components and interactions must be implemented. While emails, phone calls, spreadsheets and whiteboards may suffice for a once-a-year process, implementing incident management as a structured business process requires tools that are specifically designed to support such a process.

People & Expertise

While incident management has typically been the domain of the IT Security team, anyone that has ever been involved in such a process in the real world realizes that 'it takes a village' to successfully execute and conclude. In the past, IT Security has typically been forced to phone, email and cajole the resources they need to handle the full scope of an incident, resulting in wasted hours or even days. In order to take incident management to the next level, those resources will need to be an integral part of the incident management process planning and implementation. Such resources and their roles include:

- **IT Security** – the team that plans, execute & coordinates the process initially.
- **IT Operations** – provides infrastructure support, expertise and information.
- **Backup/Recovery team** – provides the ability to rapidly recover impacted assets.
- **Disaster Recovery team** – supports failover if local recovery isn't possible and ensures all supporting components remain available throughout the process.
- **Legal** – provides guidance during the process and takes more direct control when legal issues are involved (e.g. breach)

© OpenSky Corporation

- **Application Owners/Lines-of-Business** – provide the process with an understanding of the potential business impact of their specific assets.
- **Executives** – provide input, guidance and support for the process and maintain an on-going awareness of all incidents and their potential risk impact.
- **Physical Security** – provides support for incidents involving a physical component/penetration or internal employees/contractors.
- **Marketing** – provides guidance on communicating the process to customers, partners, etc.
- **Public/Press Relations** – creates and maintains templates and releases for use when required as part of an incident.
- **External Coordinator** – coordinates interactions with any necessary external government and/or regulatory agencies. This role may be supported by various teams within the organization, depending on the specific external agency involved.

The roles and responsibilities for each resource should be developed and documented. Primary and secondary contacts for each role should be identified and trained on their role in the process and kept up to date on any relevant changes.

One of the most critical and often overlooked aspects of identifying resources and assigning roles and responsibilities is the need to have clearly defined and agreed-to authority assigned to each role. Consider a scenario where, during an incident response process, the team identifies a critical server that has just come under attack, but if they can isolate that server quickly a breach could be prevented. However, if they have to go through multiples levels of request and approval before they can isolate it, the attacker may succeed in breaching it before approval is received.

Tools & Technologies

While whiteboards and spreadsheets may have worked for an occasional incident process, moving to incident management as a business process requires a much more robust and capable set of tools and technologies. These include:

- **Automated Process Tool** – The successful implementation and execution of an incident management process needs to be supported by an automated tool set that provides the integration, communications and tracking capabilities required to support all of the aspects of the process. Each additional tool or communications channel necessary to support the process adds complexity and risk. The selected tool should also be capable of acting as a central repository for all information, notes and documents related to incident handling and recovery, providing the foundation for a comprehensive 'post-mortem' review.

© OpenSky Corporation

- **Integrated Event Log System** – The majority of time responding to an incident is spent reviewing event logs to understand what is happening and how. Lack of an integrated system that collects and correlates all event logs for all infrastructure and security components, forces the team to spend time gathering the necessary information from multiple sources and manually correlating it, increasing response time and increasing the risk that the team will miss some critical piece of information.
- **Infrastructure Documentation** – One of the single biggest time sinks in any incident response process is the acquisition of information regarding the infrastructure. Effective and timely incident management requires accurate, comprehensive and up-to-date documentation on all systems, networks, users, devices and any other component in the environment.
- **Threat Intelligence** – No infrastructure exists in a vacuum, and having a good understanding of the types and details of threats that currently exist can significantly reduce the amount of time necessary to handle an incident. If a given attack methodology or tool has been previously discovered and the team has access to that information, analysis time can potentially be reduced from hours or days to minutes.
- **Network Session Data** – Virtually every modern cyber-attack incorporates a network communications component, and tools are available that allow all network communications in an infrastructure to be recorded, stored and analysed. While a talented analyst might be able to eventually piece together most aspects of an attack based on event logs, the ability to re-play its associated network communications can provide a complete picture almost instantly.
- **Communications** – In many instances an attacker may seek to disrupt or monitor network communications in order remain undetected and in operation for as long as possible. The incident management team needs to have a secondary communication channel available that is not part of the organization's regular network and is not publically associated with the organization in order to perform functions such as access threat intelligence, communicate with law enforcement, etc. during an attack.

Recovery

While every attack is different, the single common factor among all attacks is that they seek to make changes to the infrastructure's configuration or contents. These can range from the installation of malware to the creation of a new user account, and may impact a single system or dozens of systems. Regardless of the changes and their scope, the incident management process must include a component that restores the infrastructure to a known good state. This is frequently accomplished with standard backup and recovery tools that are implemented and managed by part of the IT team, based on requirements defined by the application owners. However, in most instances, recovering from a security incident was not considered when these

© OpenSky Corporation

tools were implemented, which may render them less effective than necessary when recovering from such an incident. For example, there have been several publicized attacks where the attacker sought to delete the data they stole as well as the backup copies in order to cover their tracks (these are frequently referred to as 'wiper-class events'). In that instance, an organization may never be able to completely recover from the attack.

Effective recovery typically requires a range of solutions that support a variety of asset criticalities. This may include a mix of tools such as continuous data protection for the most critical systems, hourly snapshots for secondary system and daily backups for non-critical systems.

In addition to having appropriate recovery tools, having an effective recovery process is critical to a timely response. For example, consider an environment where getting a system restored requires the submission of a help desk ticket, which is scheduled and handled on a first-come, first-served basis by the backup team. If an incident infects 10 servers and the incident management team must submit 10 separate tickets and wait for them to be processed, recovery could take days, which may allow the attacker to re-infect the environment.

Lessons Learned

Every action, every person, every tool and every communication has a potential impact on the incident management process. However, in most environments much of that information is lost once the event is concluded, virtually guaranteeing that any mistakes will occur again in futures incidents. Like any good process, an organization should seek to maintain a cycle of continuous improvement within their incident management process. After each incident, all data should be reviewed and all personnel should provide input in order to improve the process.

Axioms

In support of the considerations that have been discussed in this whitepaper there are a number of axioms that should be kept in mind when building out a next-gen incident management capability. These are:

#1 – After 24 hours the impact of an unresolved incident begins to increase geometrically
#2 - Incident management must be about getting the business back up and running at an acceptable level of risk
#3 - If it's not documented and signed off on by management, it probably won't happen the way you need it to
#4 - Phone calls and meetings have a geometrically progressive negative impact on incident management and recovery time
#5 - There is a direct correlation between information access time and incident response time
#6 – Those who fail to remember the past are doomed to repeat it

© OpenSky Corporation

Conclusion

As with most aspects of IT security, today's rapidly evolving IT and threat landscape are forcing organizations to reconsider how they approach managing security incidents. While a war room full of empty coffee cups, stale pizza and tired security analysts might have sufficed in the past, today's rapid-fire attack threats are mandating a more structured and business-oriented approach to incident management. As a result, organizations are realizing that security in general, and security incident management in particular, can no longer be the sole domain of a single technical team, but needs to incorporate resources from across the organization in order to effectively manage the risk such incidents represent.

Additional Resources

The following table provides a list of additional resources that may be of interest to the reader.

Source	Title	Link
Carnegie Mellon University Software Engineering Institute	Handbook for Computer Security Incident Response Teams (Free)	http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=6305
National Institute of Standards and Technology (NIST)	NIST 800-61, Computer Security Incident Handling Guide (Free)	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
ISO	ISO/IEC 270035:2011 Information security incident management ($)	http://www.iso.org/iso/catalogue_detail?csnumber=44379
SANS	Multiple Documents (Free)	http://www.sans.org/reading-room/whitepapers/incident
Netflix	Fully Integrated Defense Operation tool (Free)	http://techblog.netflix.com/2015/05/introducing-fido-automated-security.html

© OpenSky Corporation