WHY INCIDENT RESPONSE PLANS ARE CRITICAL FOR IT

Data center downtime is a reality. The 2016 Ponemon Institute research report titled 'Cost of Data Center Outages' found that the cost of data center downtime averages over $740,000 in the enterprise segment. These incidents may have roots to power system failures, technical glitches, human errors or perhaps more concerningly, cyber-attacks. Organizations therefore need to craft an effective Incident Response Plan (IRP) in order to reduce the risk of IT service downtime due to cyber intrusions, particularly involving on-premise infrastructure for which the internal IT is entirely responsible to maintain optimal operations, high availability and security.

Incident Response Plan refers to a documented strategy and guideline that works as a systematic mechanism to manage risk in response to an IT incident, particularly involving a cyber-attack. If the security incident is not managed, the risks can escalate exponentially, causing significant losses to the target. It is therefore critical to be prepared for both the apparent threats as well as unforeseen security risks that may emerge from financially motivated cybercrime underground rings, hacktivists or even state-sponsored cybercriminals.

The Incident Response Plan is a guideline containing industry-proven best practices and protocols necessary to bring the compromised systems back alive and running at optimum performance. Specifically, for organizations in the healthcare, financial and defense industries subject to stringent compliance regulations, creating and maintaining an effective, up-to-date and practical Incident Response Plan is a critical requirement. The guidelines encompass three key components of the incident response strategy: the people, the processes and the tooling. The IRP identifies and informs appropriate personnel of their relevant duties; defines the processes that must be take at various

stages once an incident has occurred; and the tooling that must be capable of proactively taking preventive action to keep the risk from spreading across the enterprise.

How to Create an Incident Response Plan for your Organization?

SANS Institute highlights six key components of the Incident Response Plan. Here's how to proceed with each stage of the IRP for your enterprise:

1. **Preparation:** This stage of the IRP covers activities that would allow the organization to respond to a security incident effectively. The preparation activities may include establishing policies, deploying technology solutions, laying out procedures, devising governance mechanism and facilitating collaboration between appropriate personnel. Strategies for employees with different roles and hierarchies should be document and available with convenient access to appropriate users. Workforce training and education is a critical requirement to ensure effective preparation. To make it easier for employees to comply, the guidelines should involve simple checklist items to help them go through subsequent phases of the IRP.
2. **Identification:** This stage covers the investigation activities where appropriate IT staff members are required to identify the cause, scope and priority of a potential security incident. It may take advanced security solutions to determine a cyber-attack incident. Organizations may need to identify patterns within network traffic to determine anomalous behavior and correlate each incident with risk factors to determine the scope of a potential attack. These threats may come from the unauthorized use of access privileges by internal employees or network intrusions by external actors. Organizations cannot afford to invest significant resources on every incident notification and should therefore deploy systems that help navigate through the noise of false alerts while identifying the most prevalent threats proactively. Based on organizational policies, business requirements and compliance regulations, organizations can devise an IRP that would help them tackle the incidents accordingly.
3. **Containment:** Once the target has learned about a security incident compromising their network, appropriate steps must be taken in order to reduce the damages. It may not be resource efficient or an optimal approach to fight the security attacks immediately. This phase involves isolating the compromised systems such that the risks don't spread beyond the point of incident origination. The damage limitation strategy may be as simple as disconnecting the compromising systems from the network or isolating the hardware and migrating the workloads to failover servers. The next step should involve backup and disaster recovery protocols to make sure that the necessary data is secure and available for immediate or later use. Once the temporary solutions are practiced, the organization can evaluate long-term solutions such as identifying the root cause, negligence or intentional malpractices by employees, as well as investing in additional resources as necessary.
4. **Eradication:** This phase relates with the immediate efforts to eradicate the source of the breach. The documented IRP should provide guidelines on accurately evaluating the root cause and calculating the true cost of eradicating the risk. For instance, the cost of reimaging a set of compromised storage components may be different from replacing the hardware and applying the necessary disaster recovery protocols to regain access to critical information. Additionally, the organization must perform the necessary measures to ensure that similar attacks don't compromise the systems again. This may require reevaluation of vulnerable

software components, hiring experts with the necessary IT skills, workforce training and education, or even firing rogue insiders involved in facilitating security incidents.

5. **Recovery:** Once the problems associated with the originating root cause and security incidents are resolved, the organization is expected to bring systems back into production environment. The faster the organization reaches and completes this phase, the lower is the downtime and users can leverage the IT-enabled business products and services faster. Systematic testing and verification procedures should be documented to ensure that the production systems are fully functional once restored to the pre-incident phase.
6. **Lessons Learned:** Finally, organizations should help the workforce learn from every security incident. If the workforce or technology demonstrates the same patterns of behavior that led to the original incident, chances are that similar incidents will follow. The cost of reworking and fixing compromised systems repeatedly may not be affordable for small and midsize business firms. On the other hand, the valuable feedback received during a real-world security incident may provide invaluable information in making the network and business more secure.

Cyber-attacks are inevitable. Data breaches are a real threat. If the organization is not adequately prepared to respond to a security incident, the IT downtime resulting from frequent security incidents may run organizations out of business. Research finds that 93 percent of the organizations that faced downtime for over 10 days eventually filed for bankruptcy later in the year. An effective Incident Response Plan will help prevent your organization from reaching that fate.