Critical Challenges to Information Security & Guidelines to use Responsive Service Now Platform

Chandra Sekhar Maganty, K Sai Prasanthi, G.V. Priyanka, K. Harsha Reddy, Kuna Srinidhi

Abstract: ***Encroachment of data constantly threatens the modern business. The risk was increasing from 222.5 million in 2009 to 4.1 billion in 2019 over the past 10 years. The main aim of this paper is to track the risk, make security comparisons in Traditional approach vs Modern approach and reasons to choose service. Knowledge on service tool, use of right platform and it's working in real life.***

Index Terms: Analysis, Data breach, Performance, Reporting, Responsive platform Risk tracking, Runbooks,Security comparisons, Service Now.

I. INTRODUCTION

Infringements of information constantly threaten the modern business. And the risk continues to increase: the total number of identities exposed by data breaches rose to 4.1 Billion Records in first six months of 2019.Time-to-time compromise is measured in minutes, and data expiration arises in days.

Worse yet, it may take months to detect a breach, with an ever age of 201 days to discover. Organizations are at risk of exposing valuable data and confidential information that are unable to respond quickly. The recovery process can be incredible costly and incalculable damage to the reputation of the business. Why is it that detecting and responding to threats takes long? One key culprit is pointed out by defense and IT profession also: the disconnection between protection and IT devices.

Traditional approaches impede effective alignment of incident- response across organizations:

- Numerous, disjointed systems produce thousands of un prioritized warnings cumulatively.
- Lack of coordination leads to wasted hours on manual processes
- Organizational complexity means the right contacts are difficult to track
- Numerous, unsecured data sets and security runbooks make it impossible to ensure that everyone is on the same page. Including inefficiency, many challenges were caused by manual processes associated with typical securityresponses.

Spreadsheets are quickly obsolete, and messages frequently end up in the wrong inboxes. In both cases, it can be incredibly difficult to define and track performance metrics. And all too often, these manual procedures pressure highly trained professionals to work on low-level tasks.

How would you rate the ability of your organization to respond to threats and vulnerabilities to security? Use this short checklist to evaluate what your business might be enhanced by the right security operations solution. Are you knowledgeable that the right solution can allow your security team to:

1) Do you rely on a single source of protection and IT truth?All stakeholders are required to access the latest data. A centralized system allows responses to be coordinated by security and ITteams.
2) All security incidents and vulnerabilities should be prioritized?

The best way to handle an alert overload is to prioritize it immediately based on its potential impact on your company. Analysts need to know exactly which systems are affected and any possible consequences for related systems.

3) Reconfiguring the basic tasks ofsecurity?

Both incident and vulnerability information was drawn into a single system. Analysts have all the information they need to protect by correlating threat intelligence data with security incidents

4) Integrating the server for configuration management (CMDB)?

Analysts can identify compromised systems their locations, and how vulnerable they are to multiple attacks efficiently with CMDB integration.

5) Safeguard your securityrunbook?

Workflows are essential to ensure that your security runbook is adhered to. Predefined mechanisms enable Tier 1 workersto

undertake actual security work, while more experienced security professionals focus on tracking complex threats.

6) Identify authorized approvals and experts on the subject quickly?

Identifying approved approvers and experts must be straightforward and conflicts quickly escalate if service-level agreements (SLAs) are not met.

7) Detailed metrics are extracted to track SLAs, undertakepost

-incident feedback and enable process improvements?

You must be able to track SLAs and collect review statistics.

Revised Manuscript Received on January 15, 2020

Chandra Sekhar Maganty,**Konerulakshmiah** Education Foundation,Guntur,India.Email:Chandu1207@Gmail.Com

K Sai Prasanthi, Konerulakshmiah Education Foundation,Guntur,India.Email:Prashsru@Gmail.Com

K.Harsha Reddy, G.V.Priyanka Is Currently Pursuing Bachelorsdegree Program In Computer Science & Engineering In K L University, India. PH-6281202334, 7093517479. Email:gudisevenkatapriyanka999@gmail.com,harshakosna@gmail.com

T he solution for security operations generates complete, up-to- date timelines for all practices and approvals automatically.

There are several ways in which an organization can respond when a high-profile vulnerability arises Contrast an organization's response with one using an integrated approach framework using a conventional, disjointedmethod.

Traditional Approach:
The security team scrambles to handle it once a threat is detected. The CISO is learning about it and wants to know if it impacts the organization Group races to analyze applications and determine who should approve any emergency patching. Many processes are manual, so analysts are struggling to gather the information necessary to provide an accurate impact assessment to the CISO. Critical systems can be vulnerable, causing a data breach in the sector.

Proposed Approach:
In contrast, the company could respond immediately to the vulnerability using an integrated response platform This activates the following steps quickly:

Next, information is automatically transferred from their vulnerability management system to the security operations system. Security analysts quickly find out this is a significant loophole, with a high likelihood that information privacy, reliability, and availability will be completely lost if exploited. Relevant information is immediately made available to the security team to remedy the situation.

Hundreds of vulnerable items are then integrated with the CMDB and prioritized based on the effect of business service, resource criticality, and vulnerability risk rating. The next measures are taken care of by built-in workflows, ensuring analysts follow the security runbook.

The system automatically generates requests for sensitive compromised products to accept emergency patches. The changes are evaluated by an additional inspection. Once the essential things are patched, protection and IT can use a single solution system to create a plan to resolve the remaining vulnerable objects. Automated workflows help to route requests from security analysts to the right IT people. The common platform ensures that information is shared on a secure "need to know" basis, eliminating the need for organizational structure memorization. Now, the CISO is briefed, and a post-incident analysis with accurate metrics is automatically generated by the security operations solution. The CISO is happy and secure for the company.

To respond to the growing number and sophistication of today's threats and vulnerabilities, an innovative security operations solution is essential. Security and IT departments can effectively collaborate with all stakeholders to analyse and resolve challenges with full transparency in disruptive issues.

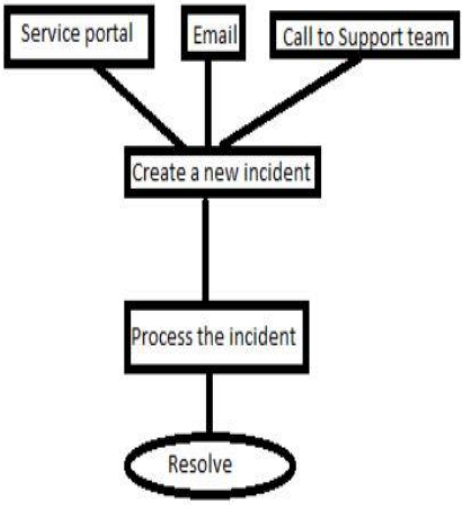
REASONS TO CHOOSE SERVICENOW:
One of the biggest challenges for information security leaders is to respond effectively to security incidents. That is why it is so important to choose an integrated response platform.
The most effective approach for security response is ServiceNow Security Operations. This provides a single forum to resolve incidents and vulnerabilities across security and IT and will improve the performance of your organization to respond to incidents with additional intelligence.

With a great solution for security operations in place, the team can make efforts to recognize threats and vulnerabilities, fix them and manage them more effective. Automation allows respondents to concentrate more easily on more complex issues. And you can have accurate data at your fingertips to constantly assess the safety posture of your company.

SERVICENOW IN A NUTSHELL:
ServiceNow keeps changing people's way of working. ServiceNow encourages the modern organization to run faster and be more flexible than ever before with a product orientation towards the operations, tasks and processes that make up the daily working life. Customers use our service model to describe, organize and automate workflow, eliminate email and spreadsheet dependencies to turn the company's service delivery and management. ServiceNow enhances service management for all business departments including IT, security, human resources, services, field service, and more. With ServiceNow business cloud, we provide a ' light-out, light-speed ' experience – designed to handle everything as a platform.

II. METHODOLOGY

Incident Management:
An occurrence is raised when assistance isn't working appropriately or when it is in unusual condition, with the goal that the proposed group (Administration work area/Backing group) will take a shot at it to re-establish to ordinary conditions. Model: Exceed expectations sheet isn't working appropriately. The client who raised an issue can follow it, include remarks and request reports on the ticket until it is settled. Group will chip away at the issue dependent on need thusly dependent on effect and desperation.



Problem Management:

In the event that there are any related episodes announced as often as possible about an issue, an issue ticket is raised. At the point when an issue ticket is raised, it implies the group will discover the underlying driver of the blunder bringing about the stoppage of these kinds of mistakes later on. Issue the executives target expelling the issues for all time from the IT foundation. Model: Email server is down.

Change Management:
It is raised when there is new change (expansion/adjustment/erasure) in the item with no unsettling influences in the IT administrations. Model: Overhauling a product. There are three sorts of predefined changes in ServiceNow – Standard, Crisis and Ordinary.
• Standard Change: Normal and determined procedures that are as of now approved i.e., no compelling reason to sit tight for Change Warning Board (Taxi) endorsements, will go under standard changes.
• Crisis Change: It is a high need issue that legitimately goes to Taxi for approval as it ought to be actualized quickly.
• Ordinary Change: The progressions which are not standard or crisis change will go under typical change. This procedure includes every one of the procedures like endorsements, usage, audits and afterward finishes with a shutting state.

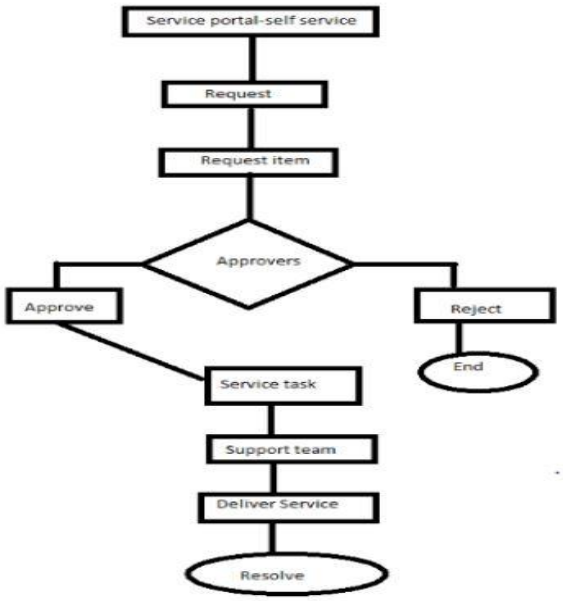
Configuration Management Database (CMDB):
It is the focal area where one can discover information on every one of the advantages and business administrations of an association, for example, PCs, system, programming, etc as tables.

Knowledge Management:
It contains articles with data on the most widely recognized issues, which the clients can resolve without anyone else. These will be appeared to clients when they raise a ticket with comparable issues or they can experience the information base. In the event that the article encourages them, there is no compelling reason to rise a ticket, empowering the help group to deal with other high need issues. There are various classifications of articles in information the executives.

Asset Management:
It includes every one of the parts of the IT resources of an association. Resource The executives incorporate every one of the benefits just as CIs (Design Things). CIs incorporate the administrations accessible in an association and resources incorporate the money related following of the properties of an association. This module shows gadgets indicating CIs and their sorts, PCs and so forth. It likewise shows all the pending resources.

Connect Chat:
This is a talk apparatus that encourages clients to visit with singular client or with bunches for sharing documents and refreshing a record. We can include or evacuate individuals in the gatherings. Records can be refreshed straightforwardly from these discussions under work notes and remarks.

Service Catalog:
It is where we can get every one of the administrations/items that are accessible in an association. It acts such as Self Help
for the workers with the goal that they can demand accessible things as per their needwhich makes an
Assistance List task.



Workflow:
It is a bit by bit stream to mechanize the work procedure in ServiceNow. There are some predefined work processes and it additionally empowers us to make new work processes according to our necessity. The work process contains exercises like creating new records, warnings, endorsements, and so on. It enables us to include conditions and contents that make designers present an easy to use process.

Reporting:
This includes creation and dispersion of reports that show the present status of information in our occasion (for instance, number of open episodes or number of settled occurrences) as pie-diagrams, structured presentations,

records or schedule based perspectives. As a matter of course, announcing alternative is accessible for every one of the tables. We can likewise show reports as landing pages to know our group execution. There are additionally some predefined reports accessible in ServiceNow.

HR Service Delivery:
This gives all the HR benefits via computerizing them and makes them effectively accessible to every one of the representatives of an association. It manages all the documentation, request, solicitations and onboarding of a representative. It goes about as a solitary stage comprising of the considerable number of administrations required for the representatives which thus improves in general productivity of the firm. Model: Payrolls, benefits, contracting, arrangements, etc.

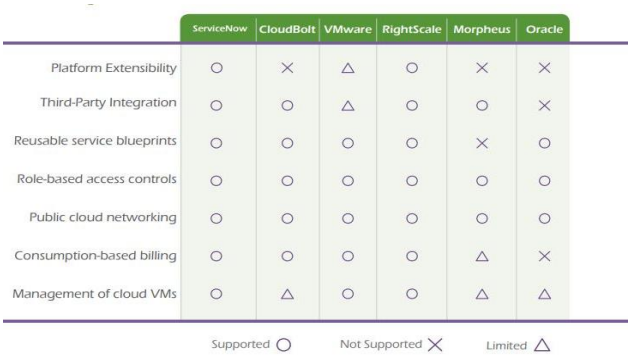
Virtual Agent:
This enables clients in finishing the normal errands without trusting that help from the help will group by a computerized operator and completes the work quickly, improving client support and diminishing the outstanding burden. Clients can check the status of their tickets/cases and update their remarks if the clients are discontent with the virtual operator they can demand for a live specialist, so they are diverted to the accessible operators or will be added to the line of the operator's rundown. Predefined conversational points are accessible, including new themes utilizing virtual operator originator according to our necessities is additionally conceivable.

Agent Intelligence:
It helps in foreseeing estimations of fields and auto-populating them while making a record dependent on a short depiction, classification, etc. This computerizes work processes and predicts results utilizing AI calculations. As per the preparation of models, work will be steered dependent on past related records which help in the decrease of goals time. We can utilize predefined arrangements or make new answers for occurrence and client support the board. These arrangements will be accessible just once the operator knowledge module is enacted.

III. ANALYSIS

ServiceNow is the best fit for organization sizes and sectors Despite the rich features of ServiceNow and its hierarchical system structure, you should be mindful that the pool of enterprises that can benefit from the platform is restricted to mid-sized and large organizations. ServiceNow cost calculator has 500 as the smallest number of employees in a company that, with the aid of the app, could render imaginable savings. And the reason is simple: if a corporation is smaller than that, its internal business processes are not typically sufficiently complicated and convoluted to leverage the dynamic features of ServiceNow.
It can be pretty much anything about the sectors where ServiceNow can come out of use. ServiceNow implementation specialists see that some sectors are more likely to use it than others, but the usage field is still impressive.

IV. RESULT



Service now has many features when compared to other platforms. So it is recommended to use service now and also it's features can be extended by using JavaScript

V. CONCLUSION

The major advantage of service now tool is it can be hosted in cloud. All the applications in service are delivered via internet using SaaS and PaaS cloud models. It is based on ITIL (Information Technology Infrastructure Library) and also reduces ITSM (Information Technology Service Management) cost by 60% to 80%. ServiceNow is customizable and also provides services based on the on-demand IT Service Management. It provides information privacy, transparency and enhanced administrative monitoring. Process consistency, customer self service and effective reporting makes ServiceNow more advantage to users. This to improve processes with agility and low risk and we need not choose between upgrading and configuring

REFERENCES

1. https://www.securonix.com/web/wp-content/uploads/2018/03/Securonix_ServiceNow_Solution_Brief-1.pdf
2. http://s3.amazonaws.com/idgcampaigns/documents/uploaded_data/ab2/378/63-/original/ebk-get-started-building-servicenow-custom-apps.pdf?1572612821
3. http://s3.amazonaws.com/idgcampaigns/documents/uploaded_data/c13/583/9a-/original/ebk-now-platform-reference-guide.pdf?1572612528
4. http://s3.amazonaws.com/idgcampaigns/documents/uploaded_data/600/0ee/4f-/original/ebk-the-future-of-accounting-is-now.pdf?1572537775
5. http://s3.amazonaws.com/idgcampaigns/documents/uploaded_data/f17/985/ad-/original/servicenow-ebook-now-platform-campaign.pdf?1572611992
6. https://acadpubl.eu/hub/2018-119-14/articles/1/3.pdf
7. https://www.ijrcar.com/Volume_2_Issue_11/v2i1130.pdf https://www.ijser.org/researchpaper/Cloud-Computing-Security-Breaches-and-Threats-Analysis.pdf

AUTHORS PROFILE

Mr. Chandra Sekhar Maganty is working as Assistant Professor in department of CSE in Koneru Lakshmaiah University. His research area is IOT and Network Security. He has published several papers in area of Network Security and IOT. He is having around 12 years of experience in teaching Area of interest in subjects are Network Security, Enterprise Programming, Web Technologies, OOPS through java, etc

Mrs. K Sai Prasanthi is working as Assistant Professor in department of CSE in Koneru Lakshmaiah University. Her research area is IOT and Network Security. She has published several papers in area of Network Security and IOT. She is having around 11 years of experience in teaching Area of interest in subjects are Network Security, Operating Systems, Computer Architecture, Computer Network, etc.

G.Venkata Priyanka from Computer Science and Engineering Department, Koneru Lakshmaiah Education Foundation student located

K.Harsha Reddy from Computer Science and Engineering Department, Koneru Lakshmaiah Education Foundation student located at Vaddeswaram,Guntur.