A Guide On Cyber Security Automation

For Banks, Financial & Insurance Business

How to Manage Cyber Threats, Increased Regulations Using Risk Management & Automation

Seconize.co

SECONIZE

Table of Contents

1

CHAPTER ONE

Introduction – Cyber Threats For FSI (Banks, NBFC, Insurance)

Introduction

Cyber Threats For FSI (Financials, NBFC, Insurance) Industry

Organizations are increasingly turning to hybrid public and private clouds to ensure uptime, accelerate innovation, and meet customer service demands. BFSI industry is the torch bearer for digital transformation.

All financial services are today being made available at the click of a button. No wonder that it is one of the highest attacked industry too, and the cyber-attacks are only going up.

With the migration to the cloud, the attack surface is only increasing and getting sophisticated. Even so, institutions must migrate to the cloud to stay competitive.

Cyber-attacks for financial services industry can be particularly hard. For financial services, data quite literally is money, and companies are especially vulnerable to reputational damage. What's worse is that no organisation, however big or small, is immune.

"In January of 2019, the State Bank of India, the country's largest bank, leaked financial data of millions of customers."

The industry has responded to this, as it is critical for their business. The regulator is making sure that the customers interests are protected. This is leading to more stringent regulations from RBI, SEBI and IRDAI.

2

CHAPTER TWO

Regulations & Industry

Key take away on Cyber Threats & Remediation

Regulations & Industry

What is key take away on cyber threats and remediation?

If one analyses and understands the core of what the regulations are stating, they are saying, be **more smart, automate and report.**

Being smart is, to classify the assets, like externally/internally facing, critical assets and have appropriate measures to manage them accordingly.

- *Follow a risk management approach* – You have to find all the issues, you may not be able to address all of them, so prioritize and manage them based on the risk they pose to the organization.
- *Assess frequently* – Gone are the days when audits used to be done yearly or at best biannually. The attacks are all automated, so should the response. Regulations call for a more continuous assessment.
- *Report the security posture* on a quarterly basis, with the findings, and what has been addressed, and an assurance plan of what is going to be addressed within a given time frame.

Cyber risk management can be effective only when the information it is based on is accurate. Yet cyber risk reporting at many companies is inadequate, failing to provide executives with the facts they need to make informed decisions about countermeasures.

Because of the information gaps, managers often apply a standard set of controls to all company assets. As a result, low-priority assets can be overprotected, while critical assets remain dangerously exposed.

Regulations & Industry

What is key take away on cyber threats and remediation?

What does the Industry ask?

DSCI and PwC 2021 report on evolving Cyber security priorities.

- Threat management with risk-based vulnerability prioritization is currently the topmost priority of Indian executives.
- Of the 68% of the executives who selected ‘improving threat management capabilities’ as one of their top three cyber security priorities, 50% have chosen ‘risk-based vulnerability prioritization’ as a measure to do so.
- Over 21% selecting ‘automated intelligent remediation’.

.

3

CHAPTER THREE

Focus on Risk Management & Automation

Focus on Risk Management & Automation

Why and what of Risk & Automation?

The regulators and industry echo 2 key themes. That is the

1. Risk based Vulnerability Prioritization

2. Automated Intelligent Remediation

Let us explore why these two are critical for businesses today

Risk Based Vulnerability Prioritization

" Research has shown that organizations suffer 80% less breaches by adopting a Risk Based Vulnerability Management model.
- Gartner"

The potential for loss, damage, or destruction of an asset as a result of a threat exploiting a vulnerability. Risk is the intersection of assets, threats, and vulnerabilities.

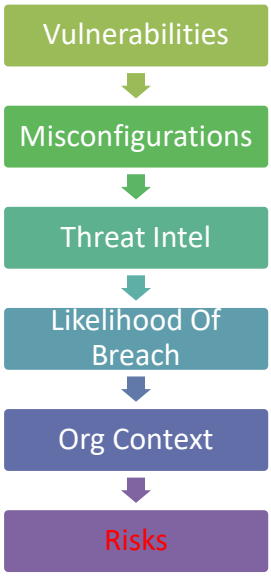
"Risk is not the enemy – too much of it is. But very importantly, so is too little of it. Between recklessness and complacency, there is a Goldilocks Zone of risk – not too much, not too little – just right.

Rohit Ghai - President, RSA"

Focus on Risk Management & Automation

Why and what of Risk & Automation?

Identification of risk involves a 5-step process that starts with Identifying vulnerabilities across the organization, model the risk for the identified weakness, prioritize them, and start remediating the top risks – thereby given the same time and effort, the organizations is de-risking themselves optimally



The top 5 advantages of risk-based vulnerability management is,

- It is automated and Continuous enterprise IT risk assessment product which
- It helps evaluate the business risk for an organization vs just issues
- It's follows data driven approach enables easier to prioritize
- Organization's gets achieves an acceptable risk level and increase security posture
- It is Near real-time holistic view vs point in time

Focus on Risk Management & Automation

Why and what of Risk & Automation?

Automated Intelligent Remediation

We have understood so far on benefits of risk based vulnerability prioritization. But another critical element required today of organization who have cloud and on-prem assets is the intelligent automated remediation.

"Hybrid environments are becoming the norm in financial services companies, In this mixed environment, manually monitoring systems for security and compliance becomes more difficult and, in many cases, impossible."

says ***Dr. Sashank Dara, CTO and Co-founder of Seconize.***

Fortunately, an automation strategy can help improve the security and compliance of an organization and reduce the overall risk to the business.

Benefits of Automation

Automation doesn't just help institutions manage security and compliance more comprehensively and efficiently.

- It helps them avoid human errors by automating the configuration of systems and software patches.
- Provides is visibility and control of the entire mixed environment, getting everyone in the enterprise on the same page regarding security and compliance.
- Visibility information about system configurations and software updates and security patches, which is crucial.

4

CHAPTER FOUR

Checklist – How to assess solution for cyber security threat management & Automation?

4-Point Checklist

How to assess solution for cyber security threat management & Automation?

Despite all the benefits of risk based vulnerability and automation , the challenge of choosing the right solutions can delay deployment.

In this chapter, we provide 4 point checklist that will help you assess your needs in the area of security, risk and compliance automation and enable you to make informed choices.

The 4-point checklist includes,

1. Centralized Visibility & Control
2. Security
3. Compliance
4. Reporting

#1 Centralized Visibility & Control

Today's complex, mixed-hybrid-cloud infrastructures present significant challenges to getting a big-picture, centralized view of the security and compliance status of enterprise systems.

In addition, many legacy security tools do not work in the cloud or in hybrid cloud environments.

54% of the organizations surveyed were adjusting their cloud strategies to meet evolving regulations.

4-Point Checklist

How to assess solution for cyber security threat management & Automation?

Ensure the systems and tooling that you evaluate provide centralized visibility and control, along with centralized automation capabilities for all of your critical systems—whether they're on-premise or in private and public clouds.

#2 Security

As a financial institution, you want to minimize security risks to your business. Choose security automation accordingly.

"Seconize DeRisk, for example, automatically monitors systems and provides the ability to prioritize the risks and fix the security patches at scale as soon as they are available. "

Any solution you choose should be able to perform both functions—security scanning for both vulnerabilities and regulatory compliance, and automated patching—without manual effort. Automation should also enable administrators to reliably and repeatedly provision secure systems.

#3 Compliance.

Besides scanning for security vulnerabilities, solution should also scan for compliance issues across hybrid cloud environments, including checking for compliance with a range of standards relevant to the financial services industry.

4-Point Checklist

How to assess solution for cyber security threat management & Automation?

"Seconize RBCM (Risk Based Compliance Management) provides the ability to scan and remediate vulnerabilities and security compliance baselines. The tool adheres to increasing NBFC regulatory requirements and compliance practices such as ISO 27001, OWSP Top 10 and 15+ others"

#4 Reporting

Advanced solutions allow for robust and feature-rich reporting on systems to aid in compliance audits and enhance security. Reports should be centralized and provide easy access to anyone who needs them.

That includes team members whose job it is to provide evidence of compliance to internal or external auditors.

"Many security standards have hundreds of security controls," observes Shashank Dara. Co-Founder, Seconize

"You want to make it as easy as possible to prove to the auditor that you are passing the requirements of any relevant standard or custom security policies that are specific to the organization."

In addition, compliance reports should clearly indicate how to fix the failed security controls and ideally provide native tooling to automatically remediate the failed security controls for any given security standard.

CHAPTER FIVE
Conclusion

Conclusion

How to assess solution for cyber security threat management & Automation?

In previous chapter we talked the 4-point checklist.

But at the same time, it is important to remind, no set of tools, however capable, will solve all of an organization's security and compliance needs.

Security isn't a product. Instead, it's a continual process that requires the participation of everyone in the organization.

A consistent risk based automation strategy, using an automation language that all the disparate teams in the organization speak, is key to powering this participation.

Essentially, automation extends the possibilities in to

Identify -> Prioritize -> Auto-remediate

If we have to summarize, here's what to look for in risk based automated solutions,

- Visibility into all automation workflows, including information about who is running what automation and when
- The RBI/SEBI/IRDAI controls are automatically mapped on a continuous basis.
- Centralized automation logs documenting which automation scripts have run where, by which person(s), and on which systems

6

CHAPTER SIX

Seconize DeRisk Solution

For Risk & Compliance Management

Seconize DeRisk Product Enables BFSI institutions to better manage their cyber risk and also the compliances as demanded by the regulator.

DeRisk Center product, assesses all the assets and applications of the organization. Assets are classified based on their criticality, exposure and scans are performed on a continuous basis.

Risk prioritization is done from the vulnerabilities identified, so that the organization can focus and optimize their efforts towards reducing the exposure.

Better still, using the auto remediation feature, issues can be addressed, this helps greatly to reduce the mean time to remediate.

Quarterly and periodic reports are generated which gives details of the issues identified, addressed, and which are planned to be addressed, in the format as needed by the regulator.

The RBI/SEBI/IRDAI controls are automatically mapped on a continuous basis. One can export the report, which serves as a internal gap audit report. This is data driven and saves enormous time and effort for the organization.

Next Steps

With a hybrid IT environment, across on prem and cloud, it is becoming more complex, and relying on limited resources one cannot fix all the vulnerabilities given by the current set of tools.

Risk based Security and compliance automation not only helps reduce the security risks associated with human errors, it can also relieve the pressure on beleaguered IT departments, freeing them up to focus on business operations and innovation.

Automation and risk based vulnerability management solutions from Seconize can help enterprises, startups and medium sized businesses meet the security & regulatory challenge in hybrid cloud environment by providing visibility, control, and security across a hybrid environment while aiding compliance, all with the help of automation.

And by adopting a risk management model, you get to achieve savings of 60% on resource requirement.

> *“Seconize DeRisk helps us to improve our security posture and give us overall visibility.”*
>
> **K Karthikeyan, CTO KreditBee**