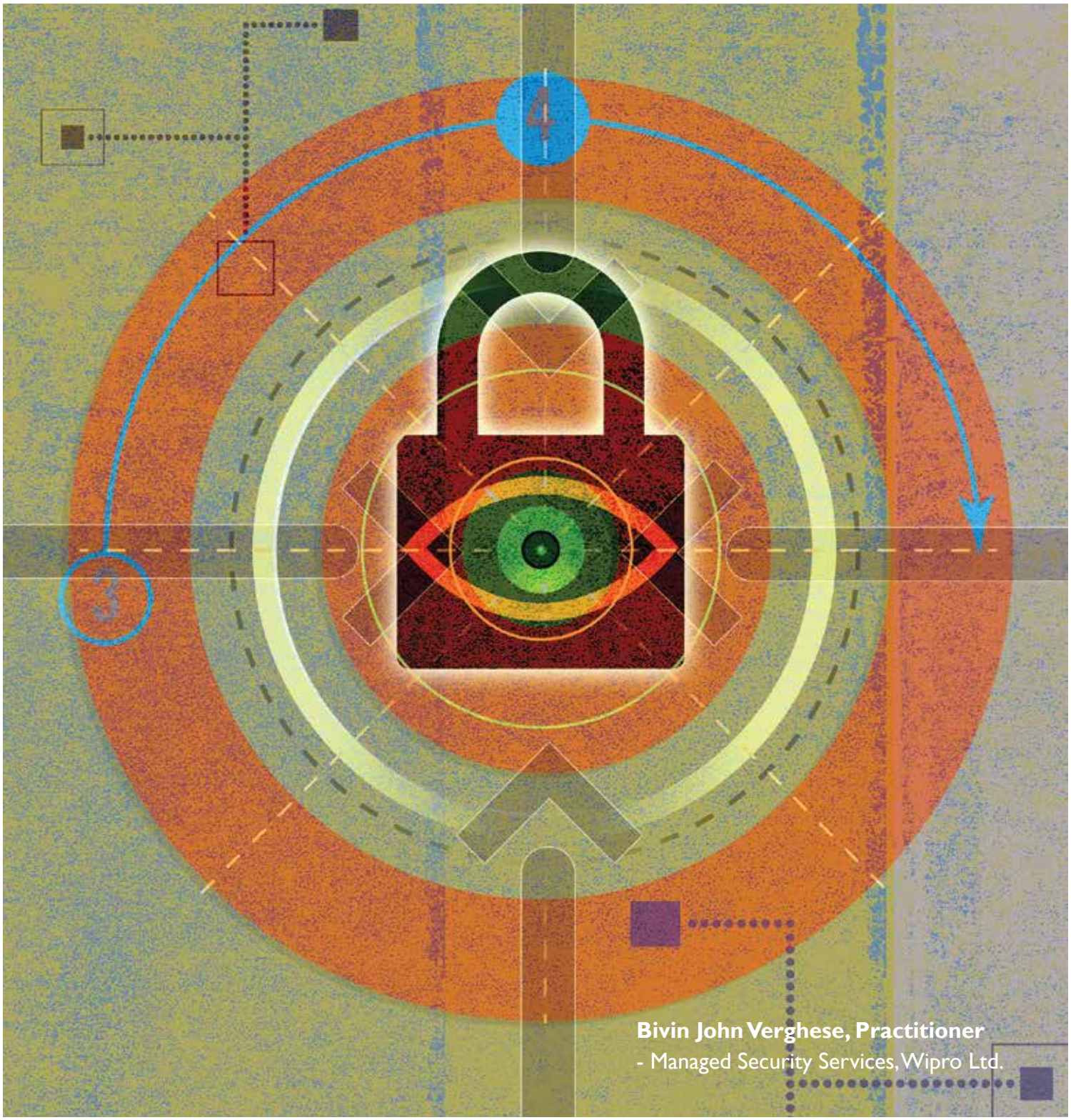
www.wipro.com

WIPRO
Applying Thought

CYBER SECURITY, A GROWING CIO PRIORITY



Bivin John Verghese, Practitioner
- Managed Security Services, Wipro Ltd.

Contents

Abstract

The information era has furnished us with a plethora of data empowering enterprises to provide tailored, differentiated and an enhanced experience to customers through newer channels. In parallel, such developments have also given rise to cyber criminals who attack systems and cause major damages and losses to organizations and their customers. Cyber-attacks orchestrated, often surpass the sophistication levels of technology solutions adopted by companies. CIO's today must therefore gear up to protect their organizations from such hostilities.

This paper explores the challenges and possible security measures available to organizations that seek the ability to fend off such attacks and ensure data security.

Introduction

According to the 2014 Worldwide Threat Assessment Report, cyber threats top the list of concerns for securing confidential data . Instances of cyber breaches are reported frequently and from across the world. While banks are common targets, there are instances of cyber-attacks aimed at compromising personal data, reported by universities, corporations and governments too.

Despite the frequency of such incidents, organizational response to these attacks remains lukewarm and inadequate. Many CIO's underestimate the risk and fail to make adequate investment in cyber threat intelligence systems.

It is therefore imperative to drive home to this segment, the need to invest in cyber security to buttress the organization's safety. Efficient cyber security initiatives must be capable of evaluating BYOD for security risks and policies while balancing data privacy and sharing. The initiatives should also be towards evaluating and auditing enterprise applications that have social and collaboration capabilities and are deliverable on the cloud. In addition to monitoring knowledgeable insiders who could be potential threats a good security system must also, monitor cyber risks from board level executives and have third party service and solution audit capabilities.

Cyber security – A top concern for CIO's

With increasing instances of cyber breaches being reported, studies reveal greater focus on security measures across organizations today .Enterprises and C-level executives must therefore focus on understanding better the implications of cyber security, and the drivers and the challenges in formulating cyber security before implementing a solution. Improving cyber security is emerging as the top priority of Chief Information Officers (CIO's) for several predominant reasons:

- The large volumes of data requiring data analytics, and increased complexity of the cyber-attacks/breaches
- Increased data migration to online services increasing the vulnerability of data
- BYOD and cloud services enable access of enterprise applications via personal devices increasing susceptibility of systems. Unauthorized users can easily hack company networks once they crack devices
- Tightly integrated supply chains (customers-vendors-organizations) increase risk from the weakest link
- Cybercrime has become a service and hence it is difficult to trace malware
- Lack of preparedness to make quick changes in business processes and policies, in case of a cyber-attack. This is an essential skill particularly in case of a highly sophisticated attack, which has the ability to bypass detection until after cyber attackers have breached the company defenses

Apart from gauging the readiness of the business leaders towards owning this issue and identifying teams responsible for developing and maintaining enterprise approach to cyber security measures, it is also for the CIOs to look into the following:

- Identify information assets that are most critical, and evaluate the "tangible and intangible value at stake" in the event of any breach
- Convey commitment to security of data to external vendors, partners and customers. Understand the roles of cyber security in customer value proposition and determine the organization level actions to keep data secure
- Analyze technology, business processes, and other initiatives used by the organization and perform competitive analysis to implement industry best practices
- Monitor relevance of the organization's cyber security approach and business processes at all times
- Ensure regional/national level compliance with legal issues related to cyber security. Big Data analytics can help enterprises remove the false alarms in the existing monitoring systems, pull information from internal and external data, and correlate high-risk alerts across monitoring systems and the data coming from social media and mobile devices

Demand for a 360-degree view – the way forward

Most businesses react to security breaches after they occur as the usual approach to security is based on threats and vulnerabilities identified based on past incidents.

Organizations must shift their approach to a 360-degree view of cyber intelligence focusing on the study of architecture, process, practices and technology to reveal possible vulnerabilities. They need to identify the source (internal or external) of the malware and correlate the data with other threats to predict future vulnerabilities and deal with security issues in a proactive manner.

An effective cyber security framework covers:

- **Threats directed to response** - Smart analytics tools identify and correlate breaches across various platforms (internal and external) that have compromised information assets to build predictive patterns of imminent vulnerabilities and strategies
- **Prioritize based on severity, criticality, and business impact** – The intelligence system prioritizes the criticality of breaches occurring annually, quarterly, monthly or weekly
- **Establish KPIs** – Establish KPIs of cyber security strategies and tactics that IT specialists, auditors, cyber intelligence analysts, and security officials can share. Changes in cyber security monitoring and control can close security gaps (if any)
- **Constant monitoring** – Constant monitoring helps test for vulnerabilities and validate cyber security strategy

1 http://www.dynamiccio.com/2014/02/cyber-security-tops-intelligence- communitys- 2014-threat-assessment.php
2 http://www.coresecurity.com/system/files/attachments/2013/04/ RickHollandFiveStepstoBuild.pdf
3 http://www.itbusinessedge.com/slideshows/top-security-priorities-for- cios- in-2014.html

- **Automation** – Automating cyber security measures to achieve frequent, timely and reliable measurements in adherence to compliance, legal policies, and metrics

A good case in point where cyber intelligence can make a marked difference is the banking and financial services industry. Frequent and sophisticated cyber-attacks in banks subject them not only tor serious threat of monetary loss but also loss of credibility.

Incidences of attacks in banks is higher because of data being distributed across multiple devices, the complicated IT infrastructure and reliance on IT resources outside company's firewall. According to a report published by Longitude research in 2013, four in five banks have faced cyber-attacks; most commonly spam attacks, closely followed by phishing and Distributed Denial of Service (DDoS) attacks.

The solution to such threats lies in effectively exploiting the large volumes of data in the banking sector to build threat intelligence strategies by developing insights. Frequency of security events, categorizing breaches and incidents as spam, phishing, DDoS, hacking, categorizing of attackers and establishing motivation of attacks is part of the process of improving cyber security efforts.

The benefits

Cyber security measures are essential to prevent unauthorized access to networks, computers and data. Other equally important benefits include:

- A strong and effective safety set-up guarantees information security and promises no disruption in business operations
- Reliable cyber security control system enhances the credibility of the organization
- Stringent security checks increases stakeholder confidence in the company's data
- Recovery time in case of disruptions is less with a cyber control system in place

Implementing a robust cyber security strategy

For an effective cyber security posture, enterprises must look into the following:

- Taking up cyber security at a C - level, as it is business centric
- Identifying business processes or assets that are vulnerable to malicious attacks, rather than uncovering technological weaknesses
- Performing a cyber-risk profile across the value chain to address security concerns with the business partners
- Shifting from protecting enterprise perimeter to securing sensitive data as corporate information can be accessed using public Wi-Fi or cloud services
- Creating and frequently updating intelligence threat strategies by simulating the cyber attacks or evaluating security measures before entering a new geography

Conclusion

There is an overarching need for comprehensive cyber security and controls to defend high-value corporate data. Such a crisis not only requires high-tech cyber security and intelligence monitoring systems, but also a cultural shift at the organizational level with C – level participation.

Cyber security of the future will rely heavily on intelligence and insights. To derive most from cyber security measures, enterprises must develop an intelligence mindset, invest in cyber intelligence technology, and take a 360-degree view of cyber intelligence. Cyber intelligence comprises a spectrum of cyber threat management; tactics that enable organizations to use proactively, smart analytics and monitoring tools. For cyber security and intelligence to work together, enterprises need an organized approach to cyber security, integrating C-level participation, risk management and governance, human factors, business processes, systems, change management, legal and compliance policies, coordination with external entities (customers, vendors, or partners).

Moreover, cyber security concerns do not stop once the organization has set up the charter, processes, systems, and change management. Continuously monitoring and frequently updating processes, systems, and response mechanisms in line with compliance and policies are the key. Finally, in depth understanding of the expectations of the stakeholders in the value chain will enable better coordination to share accurate data (internal and external) by taking an integral path.

Author Profile

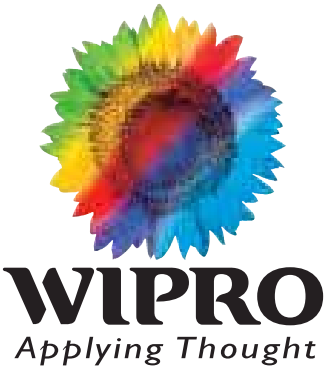
Bivin John Verghese has been part of Wipro for the last 8 Years focusing on Managed Security Services. He has been instrumental in evangelizing about the cyber threats & the need to move towards a Cyber Intelligence Center across customers in India & ME. Has been a speaker in the CISO forum on Next Gen Cyber Intelligence Center and has been an active contributor to the Cyber Security think tanks.

About GIS

Global Infrastructure Services (GIS), a unit of Wipro Limited, is an end to end IT infrastructure & outsourcing services provider to global customers across 57 countries. Its suite of Technology Infrastructure services spanning Data Center, End User Computing, Networks, Managed Services, Business Advisory and Global System Integration. Wipro, is a pioneer in Infrastructure Management services and is amongst the fastest-growing providers across the world. GIS enables customers to do business better by enabling innovation via standardization and automation, so that businesses can be more agile & scalable, so that they can _nd growth and succeed in their global business. Backed by our strong network of Integrated ServiceNXT™ Operation Centers and 11 owned data centres spread across US, Europe and APAC, this unit serves more than 500+ clients across with a global team of 23,800 professionals and contributes to over 30% of Wipro's IT Services revenues of Wipro Limited.

About Wipro Ltd.

Wipro Ltd. (NYSE:WIT) is a leading Information Technology, Consulting and business Process Management company that delivers solutions to enable its clients do business better. Wipro delivers winning business outcomes through its deep industry experience and a 360 degree view of "Business through Technology". helping clients create successful and adaptive businesses. A company recognized globally for its comprehensive portfolio of services, a practitioner's approach to delivering innovation, and an organization wide commitment to sustainability, Wipro has a workforce of over 140,000 serving clients in 175+ cities across 6 continents. For more information, please visit www.wipro.com.



DO BUSINESS BETTER

WWW.WIPRO.COM

CONSULTING | SYSTEM INTEGRATION | BUSINESS PROCESS SERVICES

WIPRO LIMITED, DODDAKANNELLI, SARJAPUR ROAD, BANGALORE - 560 035, INDIA TEL : +91 (80) 2844 0011, FAX : +91 (80) 2844 0256. email : info@wipro.com

IND/MADINC/JAN2014-JAN2015