ARUP CHATTERJEE
CHIEF INFORMATION SECURITY OFFICER

TAKING THE MANAGED SERVICE ROUTE TO DATA LOSS PREVENTION

WNS
Extending Your Enterprise

WNS
Extending Your Enterprise

TAKING THE MANAGED SERVICE ROUTE TO DATA LOSS PREVENTION

ARUP CHATTERJEE
CHIEF INFORMATION SECURITY OFFICER

INTRODUCTION

It is time to reorient an organization's data protection strategy towards prevention rather than detection, and protection at the source of data creation rather than merely on the network or devices where the data resides or travels

The year 2016 will be remembered for not only the big geo-political changes and economic upheavals, but also the rising threat from cybercrime that have left both corporations and individuals jittery and anxious.

Details of the Sony and Target hackings of 2014 were still tumbling out, when news came in early 2016 that cybercriminals had breached two of the most secure systems in the world – that of the US Federal Bureau of Investigation (FBI) and Department of Homeland Security. As the year progressed, it was clear that cyber criminals had upped their game, attacking, stealing and compromising the safety of millions of users' online data. The biggest such news to rock the world was towards the end of 2016 when it was revealed that one billion accounts of Yahoo were hacked.

As the incidence of cyber-attacks rises and the nature and source of a data breach take new forms, the focus is once again on building a data protection arsenal. It is time to reorient an organization's data protection strategy towards prevention rather than detection, and protection at the source of data creation rather than merely on the network or devices where the data resides or travels.

Data Loss Prevention – A Top Business Priority

With millions of dollars of business and an unquantifiable amount in brand equity at stake, Data Loss Prevention (DLP) has become an organizational priority. It's not surprising then that the DLP market is one of the fastest growing segments within the IT security space and is expected to grow to a USD 2.64 Billion business by 2020[1].

[1]http://www.prnewswire.com/news-releases/data-loss-prevention-market-worth-264-billion-by-2020-527898871.html

Rather than building it ground up in-house, organizations are looking to partner with Managed Security Services (MSS) specialists in an effort to adopt a customized DLP solution attuned to their business needs

The threat perception has moved to such a level that organizations cannot rely on a fragmented security system with chinks in the armor. Data protection is a watchdog service where there cannot be a lean hour or a minute's downtime. It must operate 24/7, cover both internal and external threats, and be all pervasive in terms of the entire lifecycle of data, from the point of creation, the network, the server, devices, and the Cloud.

How should their approach towards DLP differ from what it was a decade ago? First, look at DLP as a technology solution that is aligned to your company's processes and systems and not as a standalone software. Second, consider DLP implementation as not a one-off exercise but an ongoing one in which you are constantly reassessing what constitutes your company's sensitive data and how it must be controlled and protected. Third, make data protection an exercise in machine-human collaboration where the combined force of best-in-class technologies and analytics provides the security you need.

Rather than building it ground up in-house, organizations are looking to partner with Managed Security Services (MSS) specialists in an effort to adopt a customized DLP solution attuned to their business needs. This means that they will have access to the right DLP technology, experienced security analysts and industry best practices, thereby relieving them of the pressure to be constantly planning ahead, managing, monitoring and frequently upgrading their systems.

De-risking Data Processing: The WNS Perspective

In a Business Process Management (BPM) environment, DLP gains even more significance as BPM employees routinely handle sensitive customer data. In 2015, a fine of USD 25 Million was imposed on AT&T for a series of data thefts in its contact centers in Mexico, Colombia, and the Philippines. Contact center employees accessed without authorization the names and last four digits of the social security number of customers, and sold it to third parties.

Besides personal and financial data of customers and employees, sensitive data could be information related to a company's intellectual property, brand and business critical data, and data protected by law.

According to a study by the Ponemon Institute in 2016, the average consolidated total cost of a data breach is USD 4 Million. For each lost or stolen record of sensitive and confidential information, the consolidated cost is USD 158[2].

WNS manages over 650 simple to complex business processes for 200+ clients across the globe. We offer standardized processes across our 45 delivery centers in 11 countries. We have implemented state-of-the-art DLP technologies and laid down stringent data protection rules to de-risk the environment. As part of an enterprise-wide strategy, WNS deployed an overall DLP framework, which was segregated into individual areas that entail a high-risk for enterprise data leakage. This included endpoints, and communication channels such as e-mail and the web.

The first stage of the strategic DLP rollout involved securing the endpoints. To this end, WNS disabled USB ports on desktops to minimize the risk of endpoint data theft via a USB. This effectively narrowed down the host DLP software deployment scope to portable computing devices such as laptops that contain company data. With DLP configured on laptops, the security analysts at WNS have full visibility of all the data transferred by employees over laptops and wherever necessary can raise information security exceptions in conformance with the incident management procedures.

The second stage of our strategic DLP rollout targeted securing the web. WNS implemented a web DLP module integrated with web gateways (with SSL decryption), which makes visible all data uploads over web to untrusted destinations such as public e-mail, social media, cloud storage and the likes. This entails re-validating access control rights of employees with elevated internet rights and granting access

[2]https://securityintelligence.com/media/2016-cost-data-breach-study/

only on a need-to-have basis. This has assisted WNS to minimize the threat vector associated with data uploads on websites. The web upload monitoring for portable computing devices such as laptops (outside the office environment) was addressed with the help of the host DLP implementation which was also equipped to track web uploads. The next-generation web gateway hybrid solution from Intel Security (McAfee) comes with a cloud proxy capability which could be conditionally deployed for high-risk endpoints to limit and track web usage and uploads, replicating the internet access policies that the employee would be subject to, while within the enterprise perimeter.

WNS successfully leveraged the web DLP module as well as the endpoint DLP to secure operations for its contact center environments. The DLP tool is utilized to whitelist the transactional web applications so that employees cannot misuse the cardholder information on any unauthorized websites or save the information back for an offline misuse. All unauthorized attempts of such nature are deterred and an alert is triggered to the security analysts on the centralized Security Information and Event Management (SIEM) platform.

E-mail poses an enormous risk of data leakage and to address this, WNS implemented an e-mail DLP solution. This solution keeps a tab on the data being shared by WNS employees over official e-mail IDs to untrusted destinations. In this context, various policies have been designed to facilitate a seamless e-mail communication and reduce false positives. A whitelist of all existing client domains is created to bypass all e-mails going to trusted destinations. All other e-mails going to any other external domains apart from the client domain are detained for a stipulated period (into a live / real-time detention mail queue) for scrutiny by security analysts. Certain rules are also put in place to specifically identify employees sending out e-mails with sensitive financial information such as cardholder data.

Further adding teeth to our efforts to curb data leakage are ongoing Information Security Awareness campaigns. These highly-focused campaigns are important tools that WNS leverages to drive security awareness among its sizable workforce and familiarize them with the do's and don'ts of data portability from official computing devices.

Conclusion

The global nature of business operations today, makes corporates extremely vulnerable to cyber-attacks and data theft. Against a backdrop where miscreants are finding novel ways to mount data attacks, organizations need to remain vigilant at all times and thwart any such nefarious attempts. The focus should thus firmly remain on preventing data leakage and not merely reacting in the aftermath. This warrants a thorough risk assessment and execution of a DLP strategy that not only safeguards against risks at an organizational level, but also delivers at the individual business process level.

Developing a customized DLP solution in-house requires extensive planning, has cost implications and can run into roadblocks associated with right technology implementation and access to industry expertise. As against this, partnering with a MSS specialist implies a more cost-effective proposition, getting access to the latest and the right DLP technology, and the right expertise which are integral to de-risking the business environment.

About WNS

WNS (Holdings) Limited (NYSE: WNS) is a leading global Business Process Management (BPM) company. WNS offers business value to 200+ global clients by combining operational excellence with deep domain expertise in key industry verticals, including banking and financial services, healthcare, insurance, manufacturing, media and entertainment, consulting and professional services, retail & consumer packaged goods, telecom and diversified businesses, shipping and logistics, travel and leisure, and utilities. WNS delivers an entire spectrum of business process management services such as customer care, finance and accounting, human resource solutions, research and analytics, technology solutions, and industry-specific back-office and front-office processes. WNS has delivery centers world-wide, including China, Costa Rica, India, the Philippines, Poland, Romania, South Africa, Sri Lanka, UK and US.

To know more, write to us at marketing@wns.com or visit us at www.wns.com

WNS
Extending Your Enterprise