WEI INSIGHTS TECH BRIEF

ENTERPRISE SECURITY IN A HYBRID IT WORLD

75% of IT Decision Makers say they are facing challenges implementing a hybrid IT model.[1]

Predicted costs pertaining to cybercrime damage will hit $6 trillion by 2021. In order to combat this rampant destruction, Gartner expects worldwide spending on cybersecurity to top $1 trillion over the next five years. It is hard to dismiss these disturbing numbers when scanning the recent headlines.[2]

- The largest ransomware to date was paid in June of 2017 by a South Korean web hosting company. The final negotiated payment was approximately $1 million.
- After being hit with the Petya malware attack this summer, several globally recognized companies reported that the elongated suspension of critical business operations would impact corporate earnings. These notices led to the sharp declines in their stock prices.
- According to a global study compiled by IBM and the Ponemon Institute entitled, The 2017 Cost of Data Breach, the total cost of a data breach is $3.62 million on average. The average cost per data record is $141. The United States is the most expensive country with an overall cost of $7.35 million.

The role of internal IT today begins and ends with cybersecurity. It may in fact be the most important function of IT today, for in the absence of cybersecurity, there may be nothing left to protect. The responsibility to protect

The role of internal IT today begins and ends with cybersecurity. It may in fact be the most important function of IT today, for in the absence of cybersecurity, there may be nothing left to protect.

confidential, personal and proprietary data proves even more challenging in this new era of cloud computing. Meeting this challenge is one of the motivating factors in choosing Hybrid IT as your enterprise platform. One of the principles of Hybrid IT is that companies have differentiating levels of security mandates concerning their data; which can limit the types of data that can be migrated to third party data centers. Here are a few examples:

- Companies that have proprietary data that if lost or compromised, would significantly impact the company

WEI

- Companies that belong to certain industries such as healthcare or deal with credit card transactions must follow strict compliance regulations when it comes to the hosting and protection of data
- Issues of data sovereignty may create a nebulous gray area concerning governance and privacy of data hosted on cloud platforms that incorporate multiple regions of the globe
- Company politics and status quo practices may prohibit data from residing outside of the firewall perimeter

WHERE SHOULD I STORE MY DATA?

The beauty of Hybrid IT is that it offers the best of both worlds: the controllability and governance of on-premises along with the scalability of the public cloud. Just as Hybrid IT allows you to pair each workload with the optimum platform, it allows you to match data with the appropriate store location based on its security parameters and preferences. To accomplish this, IT must conduct a risk assessment to determine the data locality of all files and databases. The risk assessment must also review all industry and government compliances as some may forbid the hosting of data with third parties or offshore locations. Data should never be migrated until it passes a security and compliance litmus test.

5 SECURITY RECOMMENDATIONS FOR HYBRID IT

While Hybrid IT offers the flexibility to manage different data types and sources by distinct security policies, it does present distinct challenges as your existing staff must manage, monitor and enforce security for multiple locations. Below are five recommendations to shore up the security of your Hybrid IT enterprise.

1. It is important to demand transparency from your cloud service providers. Ask a CSP to demonstrate their security controls up front. They should have clear documentation concerning policies for the accessing, modification, replication and deletion of data. A public CSP should be able to establish how information is segregated between customers and that they have proven experience and knowledge concerning compliancy audits. Have your CSP specify the physical geography where your data will reside as well. Make sure that all of these parameters are detailed in your SLA.
2. One of the advantages of the cloud is that users can access the digital services they need from anywhere. It also means that hackers and unauthorized users can attempt to infiltrate those services from anywhere, opening up your enterprise to credential stuffing attacks. These can be thwarted by implementing multifactor authentication. A survey conducted at the Black Hat Conference in Las Vegas in 2017 showed that 38% of hackers considered MFA the toughest security system to beat.[3] The era of protecting accounts and resources by a single password are over.
3. Any type of data hosted in the cloud that contains confidential, sensitive or proprietary information should be encrypted, both in transport and at rest. This should include log files, backups and other data sources that can be of benefit to a hacker. Users should always connect to cloud resources through a secure connection that is encrypted by a certificate assigned by a trusted certificate authority in order to prevent session hijacking and man-in-the-middle attacks.
4. As mentioned, increasing the number of involved locations through multiple public clouds can obviously complicate the security role of your IT staff. IT personnel must be provided the training and tools to actively monitor all of the involved data centers. The idea of securing that which you cannot visibly see can be an uncomfortable thought. This is why it is important to obtain detailed visibility of your entire infrastructure. The ability to manage all computers through a single security management console regardless of location is critical.

It should be able to capture data from both cloud and on-premises systems to help quickly identify, contain and mitigate threats. Cloud admins should be able to roll out security policies as quickly as they can spin up additional servers and resources. Security controls should be directed at the macro domain level as well as individual service containers.

5. Even when proper security systems and protocols are in place, data can still be compromised because of user carelessness. A confidential document is wrongly forwarded to an unauthorized party or sensitive data is mistakenly included in a slide presentation used for a business conference. Selecting a cloud provider with integrated information protection or a rights management system will help prevent user oversights. These systems classify your stored data and then implement policies that pertain to the assigned classification. An example of this is Azure Information Protection, which allows you to track and control how your confidential data is used.

There is a lot to absorb from a security perspective when it comes to Hybrid IT. Fortunately, Hybrid IT allows you the ability to transform your enterprise in a calculated, systematic fashion in order to ensure that your enterprise is secure down to the most granular level. With Hybrid IT, agility, scalability and security can work in cohesion.

TALK TO WEI TODAY

Talk to the cloud security experts at WEI today.

Sources:
1. IDG Research commissioned by WEI, June 2017.
2. Top 5 cybersecurity facts, figures and statistics for 2017. Steve Morgan, CSO Online, Oct 19, 2017. http://www.csoonline.com/article/3153707/security/top-5 cybersecurity-facts-figures-and-statistics-for-2017.html
3. Hackers Say Humans Most Responsible for Security Breaches. Kevin Townsend, Security Week, August 11, 2017. http://www.securityweek.com/hackers-say-humans-most-responsible-security-breaches

ABOUT WEI

WEI is an innovative, full service, customer centric IT solutions provider.

Why WEI? Because we care. *Because we go further.*

At WEI, we're passionate about solving your technology problems and helping you drive your desired business outcomes. We believe in challenging the status quo and thinking differently. There are a lot of companies that can take today's technology and create a great IT solution for you. But we do more. We go further. And we have the customer, vendor and industry awards to prove it. WEI is a premier technology partner, who always puts our customers first while providing the most innovative solutions for over 25 years.

WEI Dedication meets innovation.

info@wei.com
www.wei.com
43 Northwestern Drive | Salem, NH 03079
800.296.7837