TechTips Newsletter

tech hero

Insider Tips To Make Your Business Run Faster, Easier And More Profitably

June 2017

This monthly publication provided courtesy of Richard Lynn, VP Sales & Marketing, Tech Hero

Our Mission: To build a community of successful minded entrepreneurs that inspires excellence, encourages collaboration and expands the capacity of all members to achieve great things.

Is a Digital Geneva Convention in our future?

Malicious hacking and cyberattacks have been all over the news lately, from the dangers of Internet of Things products to the allegations of Russian intervention in the U.S. presidential election.

This danger of cyberattacks has always been present. Now, though, there are more computers to attack, leading to more potential destruction. Also, hacking a personal computer can be more than simply annoying and costly; the consequences are getting ever more dangerous. This was evidenced with the hack of Ukraine's power grid.

Because of the shift in the types of cyberattacks, Microsoft called for a type of Digital Geneva Convention at this year's RSA conference in February. For those who hadn't heard of it before, the RSA conference is, according to their site, the world's largest provider of security events with the motto, "Where the world talks security."

The original Geneva Convention, which took place shortly after the end of World War II, set humanitarian and other guidelines that all nations are supposed to follow to protect citizens during times of wars and conflicts.

Why now?

The growth of cybercrime in new avenues (like the IoT) isn't actually what Microsoft is most worried about. Instead, the proliferation of these attacks garnered by or against both for-profit companies and governments demonstrates a shift from previous offenses.

Microsoft acknowledged on their blog that there isn't a single step that will counter this large problem, but working toward a solution is a necessity at this point. They ask for a "Digital Geneva Convention that will commit governments to protecting civilians from nation-state attacks in times of peace."

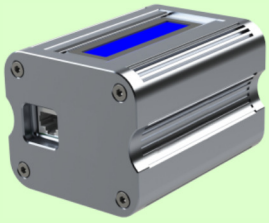
They also compared the involvement of the Red Cross to the assistance of technology companies. Called "the Internet's first responders" by Microsoft, these companies must protect against nation-state cyberattacks as a "neutral Digital Switzerland that assists customers everywhere and retains the world's trust."

How big is the problem?

As many people in the IT security field know, it's a huge problem that is only growing. According to ISACA, they anticipate that 74 percent of businesses around the world will be hacked each year. Even more, "the estimated economic loss of cybercrime is estimated to reach $3 trillion by 2020."

Yet, Microsoft believes the real problem lies beyond the economic downfalls. Instead, the most worrisome attacks now are those performed by nation-states, citing the Sony attack by North Korea in 2014 as a turning point.

Latest Network Security Device: "NetDefender"



Vulnerability Management Solution

The new NetDefender Vulnerability Management Solution enhances security by proactively identifying, monitoring, and notifying businesses of potential vulnerabilities in their networks—all with breakthrough simplicity and affordability.

Utilizing proprietary software and the compact NetDefender Sensor, NetDefender works in three phases:

1. Identification

The user's network is continuously scanned to locate and identify every connected device with an IP address, from computers and smartphones to printers and smart devices

Includes scanning of external-facing IPs to provide a 360-degree view of network vulnerabilities

2. Monitoring

All connected devices are then scanned 24x7 for vulnerabilities such as missing software patches

3. Notification

All scan information, including vulnerabilities, is displayed in an easy-to-read dashboard, including instructions for remediation

A proprietary "SPF" (Security Protection Factor) scoring system makes it easy to understand the network's health

Users and their IT security providers can be alerted to critical issues via email or text

For more information on this solution please contact your Tech Hero representative at (800) 900-8234 (option 2)

This differed from previous cyberattacks because it was simply revenge for a movie — Seth Rogen's "The Interview" — that made fun of North Korea leader Kim Jong Un. The attacks have progressed, and Microsoft (perhaps in a bit of an exaggeration) stated that now "nothing seems off limits to nation-state attacks."

Regardless whether Microsoft's statements can be considered excessive or not, it's undebatable that there is a new battleground on the Internet that users, companies, and nation-states must pay more attention to.

One of the most difficult aspects of determining how to combat these attacks is the fact that "cyberspace in fact is produced, operated, managed and secured by the private sector." While the government obviously has a role to play, these attacks are often done on private citizens and companies.

Client Spotlight

Baker Barrios

Our philosophy centers around design stewardship. We see design as a vehicle to influence the way people use space, by creating environments that are both accessible and adaptable and that provoke inspiration and connection. Clients rely on us as strategic business partners – as well as for the creativity, technical precision and independent thinking we apply to every project. Understanding each client's objectives, culture, personality and values is critical to achieving excellence in architecture, interior design, planning, landscape architecture, structural engineering, branding and communications.

Would you like your company highlighted here in our "Client Spotlight"? Then give us a call today at: 1-800-900-8324 x8840.

What is Microsoft doing?

Of course, Microsoft used this conversation to discuss what they are doing to protect consumers from these attacks, spending $1 billion annually in developing and implementing new security features throughout the technology stack.

One way to protect users is by educating them, especially about email phishing attacks, considering that "an estimated 90 percent of all hacking begins with an email phishing attack."

However, security administrators know that average users cannot always be relied on for protecting themselves from scams or bear the sole responsibility for this. Microsoft themselves plugged their Advanced Threat Protection for Microsoft Exchange Online, which identifies and stops malware and suspicious code patterns in emails.

This feature is one of Microsoft's many implementations meant to ward off attacks, as numerous other tech companies are doing as well. Security-related product features must work together with data analytics and machine learning in order to uncover nation-state attacks.

Microsoft explained how they have a three-part partnership across their company, working with the Microsoft Threat Intelligence center to search through over 200 cloud services and third-party feeds, creating a real-time understanding of potential threats.

Threats are forwarded to the Cyber Defense Operations Center, which is staffed around the clock, taking immediate action. Next, the Digital Crimes Unit takes legal action across these threats, including those performed by nation-states.

However, Microsoft admits that this is something that they, or any other tech company, is unable to do alone.

Is it up to the government or private sector?

In a short answer, both.

One action that Microsoft sees as the first step is up to the governments; they should decide on and implement international cybersecurity rules (aka a Digital Geneva Convention) in order to protect average people online.

In fact, there are already foundations for international rules in place, such as cybersecurity norms for nation-states recommended by governmental experts from 20 different nations in 2015. These were "aimed at promoting an open, secure, stable, accessible and peaceful ICT environment."

Additionally, China and the U.S. came to an agreement that cyber-enabled theft of intellectual property would not be performed by either country's government, something that Microsoft believes should also happen between the U.S. and Russia so all civilians are protected.

This allowed the initial 20 nations to more adamantly push for their previous recommendations. These recommendations should move from norms to actual global rules that avoid "cyberattacks that target the private sector or critical infrastructure or the use of hacking to steal intellectual property."

Not only this, but the tech company also believes that governments should be required to aid the private sector in its attempts to detect, contain, respond to, and recover from such events. Another issue with the way the government handles these attacks is that, according to Microsoft, it stockpiles, sells, or exploits them, rather than reporting the vulnerabilities to vendors.

So, it is clear that the future of Internet security does not lie firmly in the hands of either the private or the public sector; instead, this Digital Geneva Convention should feature an independent organization with representatives from both to determine and share which countries were involved in the nation-state attacks.

"Only then," Microsoft adds, "will nation-states know that if they violate the rules, the world will learn about it."

vmware® PARTNER

PROFESSIONAL SOLUTION PROVIDER

Free Consultation to review your VMware Licensing!

Contact your Tech Hero sales representative to schedule a FREE review of your VMware licensing.

Find out ways to save money, ways to receive free upgrades, and a better understanding on the VMware license models.

tech hero

1-(800) 900-8324 (option 2)

Sales@TechHero.com

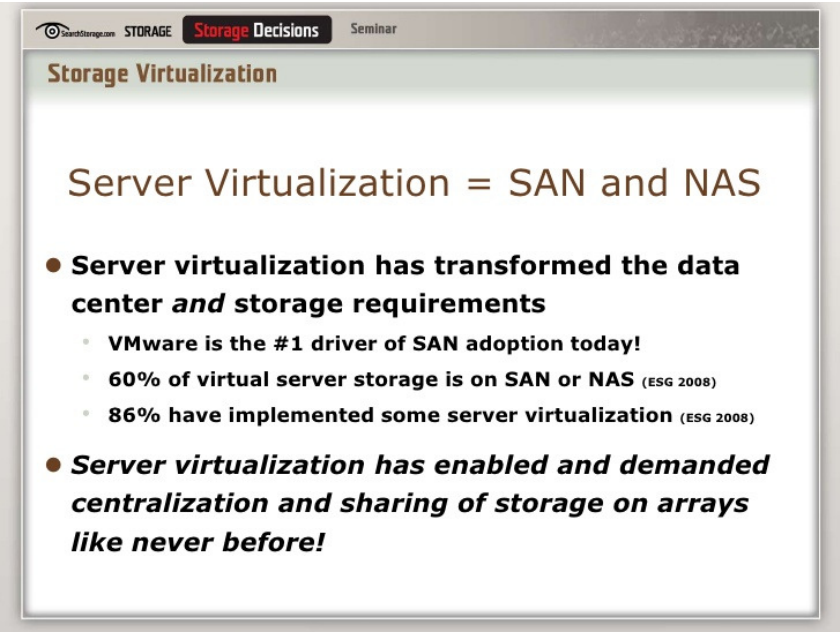
How the new state and future path of storage virtualization will transform the enterprise

What is storage virtualization? Well, it's a combination of physical storage devices used as virtual storage. Software-defined storage has been years in the making. It is particularly relevant for datacenters.

As far as datacenters go, to have storage infrastructure controllable by software is a commonplace; storage virtualization takes it to a whole new level. With the explosive growth in data and networked storage over the past decade, storage virtualization satisfies a critical imperative to avoid server and storage sprawl by providing an efficient and salient way to access storage.

For enterprises, the tangential priority is to also boost utilization, rein in capex and operational expenditure incurred on such sprawling facilities while continuing to meet all relevant service-level agreements (SLAs). Such factors are the key drivers behind the growth of storage virtualization.

Current state and enterprise advantages



These are some of the key advantages of storage virtualization as noted by IDC in one of their research reports:

- Storage provisioning is simplified, and capacity expansion across different types of storage systems is well enabled.
- Data protection is also well provided for.
- Utilization levels for storage assets increase by 20 percent-70 percent.
- Storage virtualization enables seamless movement of data across different types of systems, which enables systems administrators to be able to automatically have data migrated to less expensive storage levels, thus cutting costs significantly

Drivers for enterprise adoption

These are some of the other drivers for implementing storage virtualization, as identified by HP in one of their white papers:

Organizations are continuing to provision individual storage units manually while buffer capacity remains trapped, and unable to be shared.

Siloed management and data services also inhibit storage virtualization — each storage pool, device, and service needs to be handled separately, which causes ineffective management, thus driving up costs.

Four infrastructure gaps

There are a few gaps that need to be addressed to effectively implement storage virtualization. They are:

Explosive growth in data constrained by stranded capacity and storage silos

For many years, organizations have been experiencing extraordinary growth in data requirements. IDC has estimated that even during the 2009 recession, the annual rate of growth in networked storage was around 41 percent. As the economy has rebounded, leading to new applications and the increased adoption of digital media by enterprises, IT departments must prepare themselves for higher rates of data growth and specific data storage requirements.

In the past, IT departments have responded to such explosions in data by adding more storage devices.

However, this action led to the creation of storage silos and stranded capacity, which made it very difficult to do sharing of storage capacity, shift capacity to other applications as needed, or repurpose the underutilized storage capacity in any other form. Such challenges call for storage tiering, consolidation, effective data migration, and storage virtualization.

Inability to scale or pool storage

There are several ways in which an IT infrastructure made up of stranded disks and silos of storage increase the cost of storage.

- Acquiring, managing, and deploying separate, disconnected storage pools.
- Low levels of utilization waste the investment in storage.
- It is costly and inefficient to manage separate pools of storage.
- The inability to repurpose storage capacity reduces flexibility while forcing the purchase of more unnecessary storage.

Storage virtualization reduces the stranded capacity and at the same time, enables the pooling of all resources. Thus, storage virtualization is able to provide smooth storage capability, which is as easy as simply attaching additional disk capacity.

Piecemeal approach to management inhibits automation and optimization

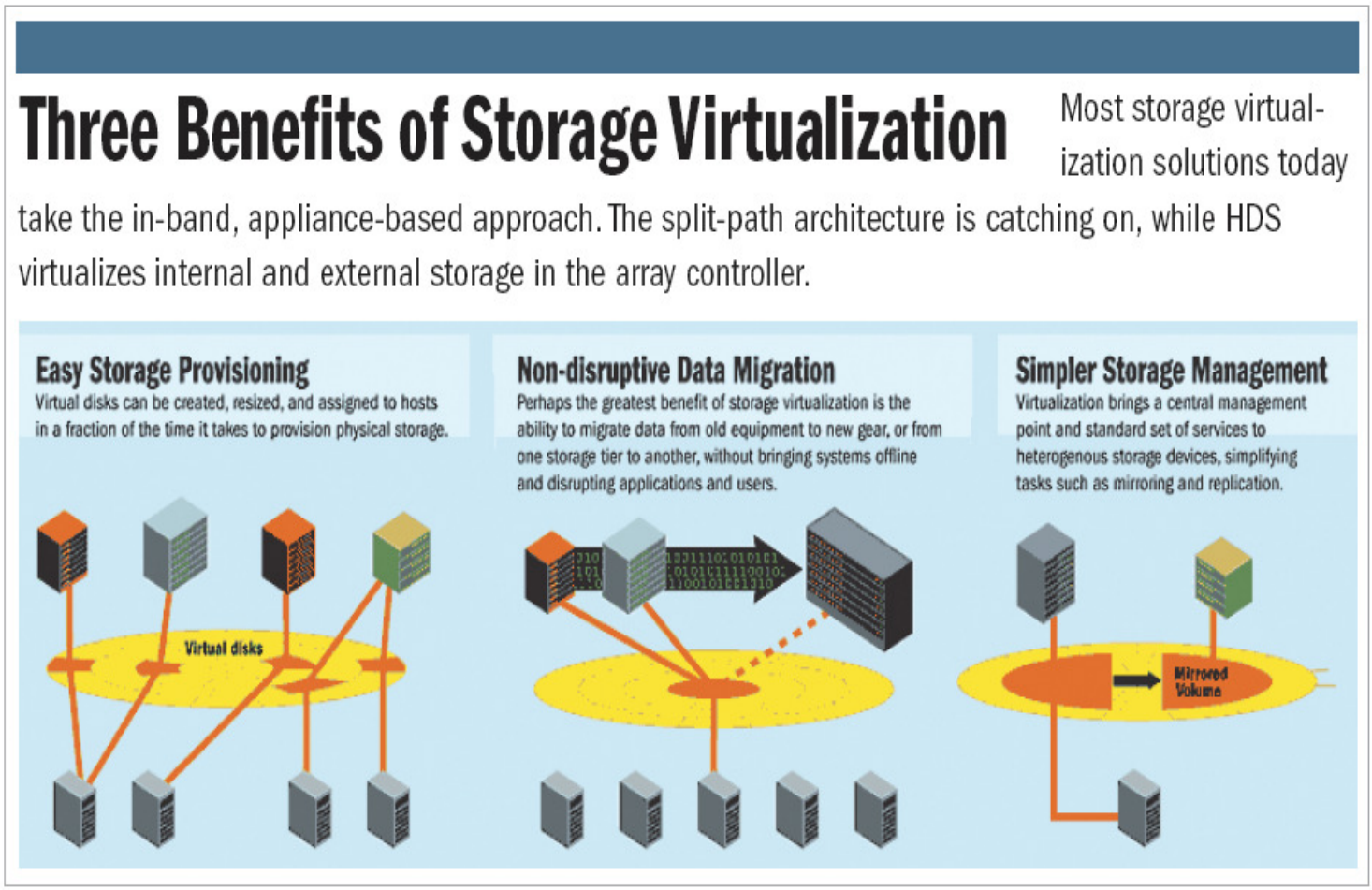
It's only when the storage is managed as a single, logical pool that effective automation and storage optimization can be implemented. In the absence of this, each storage silo would need to be automated and optimized as its own separate island of storage.

This kind of disconnected approach renders futile any efforts at load balancing, dynamic capacity management, or performance tuning. Optimization can be best implemented when administrators are able to work at a higher logical level of abstraction across the entire range of storage devices and physical storage pools.

This kind of piecemeal management is also inefficient and increases costs in many ways. Being slow, it requires the administrators to handle each device or storage silo (no, this silo has nothing to do with the agriculture industry or missiles either!) separately.

This approach also forces systems administrators to work at the lower device level, which demands more specialized skills. Consequently, the organization starts needing more administrators with varied skills. As a sum total of all the outcomes, administrators handle much fewer TBs on a per-administrator basis.

Separate domains hinder the provision of unified data services



THECHANNELCO.
CRN
MSP 500
2017

Tech Hero

has made the Pioneer 250 list of CRN's 2017 Managed Service Provider 500 List!

The 2017 MSP 500 list recognizes companies in North America whose approach to delivering managed services is one innovative step ahead.

The MSP Pioneer 250 is a list of channel companies with business models weighted toward managed services and largely focused on SMB market.

The presence of unified data services capability allows administrators to operate at higher levels of abstraction where they can logically move storage across different vendors, arrays, and storage domains. Unified data services are inclusive of:

Replication: The ability to move data synchronously or asynchronously to other capacity by using data-mirroring techniques.

Snapshots: The partial, fast backup performed for a large dataset, usually for data protection in the interim.

Intelligent tiering: This uses policy-driven tools to automatically store data on the right storage device based on the required level of storage and protection, age, frequency of use, and other such attributes.

Cloning: A fast, partial backup of a large dataset, similar to snapshots function. It is generally used for interim data protection or for load balancing.

Mirroring: An exact copy of a dataset made on a block by block basis when the data is written to disk for the first time (synchronous mirroring) or at a later time (asynchronous mirroring).

Thin provisioning: This is a form of storage provisioning whereby the actual physical capacity blocked for an application is less than the amount that has been provisioned logically, with the specific intent that more physical capacity can be allocated later when needed.

A well-implemented set of unified storage data services enables the IT division to reduce costs as well as provide capabilities such as migration, tiering, and cross-array consolidation in a fast, effective, and tremendous manner. Overall, this results in faster storage provisioning, better data protection, and more effective storage deployment.

tech hero