GREATEST CYBER THREATS OF 2015
How to Avoid the Disparate Infrastructures Where They Fester
The security measures protecting your network are always there but are never visible. Although your company is diligently fighting to keep the bad guys out, it is often difficult to determine exactly where your systems are vulnerable. In the age of the cyber-attack, safeguarding data and systems has never been more important.

The year 2013 – known by many network security specialists as The Year of the Mega Breach – saw over 552 million data breaches.¹ The 2014 hacks on Home Depot, J.P. Morgan, and Gmail compromised the identities of 282,000,000 people.²

The age of hacker is upon us, and organizations of all sizes must equip their security teams to battle these malicious threats accordingly. The first step is understanding what your company is up against.
Although there are new cyber threats that hit the World Wide Web every second, here are two attacks that have gained enough momentum to become serious threats to businesses of all sizes:

**CryptoLocker Attacks**
As one of the latest cyber threats to emerge, the CryptoLocker cyber-attack gets its name from the data and files that it encrypts and holds at ransom, forcing companies to fork-over the hacker’s desired price if they ever want to see their files again. As a botnet, this malicious program spreads through and feeds on networks of virus-infected companies. SMBs are a major target of CryptoLocker scams.

Gameover Zeus, one of the most prevalent of the CryptoLocker malware, has attacked over 1 million computers and has cost victims over $100 million dollars. In the first month that this malware was launched, it claimed around 200,000 victims in the United States alone.³

**Phishing Attacks**
Phishing Attacks are not new to the world of cyber threats, but they have become more intricate and tricky to catch. Disguised as legitimate sources, phishing emails and messages are meticulously crafted by spammers to get users to click links that will unknowingly hijack information and network access from victims.

For businesses, this means compromising sensitive employee and company data. These threats are also difficult to detect as they alter router, network, and firewall settings to perpetually harvest data. In a 2014 report, Google announced that it discovers more than 90,000 phishing sites and over 50,000 malware-infected sites every month.⁴
Both CryptoLocker and phishing attacks are designed to penetrate firewall, malware, and other network defenses. So, the question becomes: How do I keep my data safe? There is no one true answer, but one thing is certain: Companies must develop security controls within their architectures. Unfortunately, security controls become complex and hard to monitor with disparate, siloed systems.

Identifying and managing IT risk has become even more challenging as server sprawl cases from virtual environments continue to increase. Traditional infrastructure management tools lack the scalability and ability to perform at rates needed to manage server sprawl. In a large enterprise environment, for instance, IT admins can spend a week or more updating server firmware across all environments.5

And then there are other complications that go hand-in-hand with disparate systems, including:

» **Difficult Compliance Management** – As the number of tools and admins needed to manage an IT infrastructure increases, more task forces are required to sort through the complexities and ensure compliance mandates are being met.

» **A Lack of Business Agility** – Companies are unable to reallocate application resources, which limits performance and compromises visibility across the entire IT environment.

» **Performance and Security Concerns** – As a group of connected servers and systems, an entire infrastructure is only as formidable as its weakest link. Performance, security, and availability are all affected factors.
Overall, companies need to find new ways to resolve server sprawl complexities and security issues that can be found in new virtualized environments. It differs for every company, but many are turning to converged infrastructures to better connect their systems and avoid siloed operations. With designs that are fully-tested to prevent security vulnerabilities, converged infrastructures connect entire virtual machine environments to eliminate server sprawl and mitigate endpoint penetration threats.

According to the IDC Worldwide Quarterly Integrated Infrastructure and Platforms Tracker, the worldwide integrated infrastructure and platforms market increased revenue 33.8% ($2.4 billion) in 2014.6

One answer for why so many companies have moved to converged infrastructures can be found in the business benefits that tend to radiate throughout an organization. For instance, another study performed by the IDC found that converged infrastructures helped companies:7

» **Reduce Infrastructure Maintenance and Management Costs** – IT infrastructure costs were lowered by over $45,000 per 100 users, and the average annual datacenter costs was lowered by around 68%.

» **Reduce Staff and Deployment Costs** – IT staff could configure, deploy, and test infrastructure 75% faster and at a 30% reduction in system integrator costs.

» **Reduce End User Downtime** – Annual user productivity losses due to outages were reduced, saving companies an average of $9,000 per 100 users per year.
CONCLUSION

Proper security measures have become essential to survival in today’s ever-changing world of cyber threats, and new breakthroughs in IT infrastructures (like converged methodologies) are helping companies simplify to combat the chaos.

To gain a more in-depth exploration of converged infrastructures and how they can help protect and empower business, reach out to the HP Partner Community today to scout out a best-fit consultant in your area.