The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

Sponsor Firm:

Hewlett Packard Enterprise
Nathan Hall
Director of Solutions Architecture

Hewlett Packard Enterprise
Vinay Jonnakuti
Sr. Manager, Technical Marketing and Solutions

Partner Firm:

VLP Law Group LLP
Melissa Krasnow
Partner

Thank you for logging into today's event. Please note we are in standby mode. All Microphones will be muted until the event starts. We will be back with speaker instructions @ 11:55am. Any Questions? Please email: info@theknowledegroup.org

Group Registration Policy

Please note ALL participants must be registered or they will not be able to access the event.
If you have more than one person from your company attending, you must fill out the group registration form.

We reserve the right to disconnect any unauthorized users from this event and to deny violators admission to future events.

To obtain a group registration please send a note to info@theknowledgegroup.org or call 646.202.9344.

The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

- Please note the FAQ.HELP TAB located to the right of the main presentation. On this page you will find answers to the top questions asked by attendees during webcast such as how to fix audio issues, where to download the slides and what to do if you miss a secret word. To access this tab, click the FAQ.HELP Tab to the right of the main presentation when you're done click the tab of the main presentation to get back.

- For those viewing the webcast on a mobile device, please note:

  - These instructions are for Apple and Android devices only. If you are using a Windows tablet, please follow the instructions for viewing the webcast on a PC.
  - The FAQ.HELP TAB will not be visible on mobile devices.
  - You will receive the frequently asked questions & other pertinent info through the apps chat window function on your device.
  - On Apple devices you must tap the screen anywhere to see the task bar which will show up as a blue bar across the top of the screen. Click the chat icon then click the chat with all to access the FAQ's.
  - Feel free to submit questions by using the "questions" function built-in to the app on your device.
  - You may use your device's "pinch to zoom function" to enlarge the slide images on your screen.
  - Headphones are highly recommended. In the event of audio difficulties, a dial-in number is available and will be provided via the app's chat function on your device.

The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

- Follow us on Twitter, that's @Know_Group to receive updates for this event as well as other news and pertinent info.
- If you experience any technical difficulties during today's session, please contact our Technical Support @ 866-779-3239. We will post the dial information in the chat window to the right shortly and it's available in the FAQ.Help Tab on the right. Please redial into the webcast in case of connectivity issue where we have to restart the event.
- You may ask a question at anytime throughout the presentation today via the chat window on the lower right hand side of your screen. Questions will be aggregated and addressed during the Q&A segment.
- Please note, this call is being recorded for playback purposes.
- If anyone was unable to log in to the online webcast and needs to download a copy of the PowerPoint presentation for today's event, please send an email to: info@theknowledgegroup.org. If you're already logged in to the online Webcast, we will post a link to download the files shortly and it's available in the FAQ.Help Tab

The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

- If you are listening on a laptop, you may need to use headphones as some laptops speakers are not sufficiently amplified enough to hear the presentations. If you do not have headphones and cannot hear the webcast send an email to info@theknowledgegroup.org and we will send you the dial in phone number.

- About an hour or so after the event, you'll be sent a survey via email asking you for your feedback on your experience with this event today - it's designed to take less than two minutes to complete, and it helps us to understand how to wisely invest your time in future events. Your feedback is greatly appreciated. If you are applying for continuing education credit, completions of the surveys are mandatory as per your state boards and bars. 6 secret words (3 for each credit hour) will be given throughout the presentation. We will ask you to fill these words into the survey as proof of your attendance. Please stay tuned for the secret word. If you miss a secret word please refer to the FAQ.Help tab to the right.

- Speakers, I will be giving out the secret words at randomly selected times. I may have to break into your presentation briefly to read the secret word. Pardon the interruption.

- We need your insights -- We are conducting some special research to improve The Knowledge Group for you. Give us ten minutes on the phone and we will give you three months of FREE CE webcasts. Please click this link to sign up and participate: https://knowgp.org/2q1zI3b We look forward to hearing from you.

The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

Sponsor Firm:

Hewlett Packard Enterprise

Hewlett Packard Enterprise (HPE) is a technology company with a comprehensive portfolio spanning from cloud to the data center to workplace applications. HPE hyperconverged technology and services help customers around the world make IT more efficient, more productive, and more secure.

In 2017, Hewlett Packard Enterprise (HPE) acquired SimpliVity and now offers HPE SimpliVity hyperconverged systems, complete hardware-software solutions that are designed, built, and supported by HPE. HPE SimpliVity hyperconverged technology lets organizations simplify IT. The infrastructure combines compute, storage services, and networking in a single 2U appliance, and incorporates all of the traditional IT functions: WAN optimization, unified global VM-centric management, data protection, cloud integration, deduplication, built-in backup, caching, and scale-out capabilities. Inline deduplication, compression and optimization are applied to all data at inception, reducing resource consumption (storage and CPU) while increasing application performance.

HPE SimpliVity 380 is a turnkey hyperconverged solution built on an HPE ProLiant DL380 compute platform. Systems can be clustered to form a shared resource pool that delivers high availability, mobility, and efficient scaling of performance and capacity.

Partner Firm:

VLP LAW GROUP LLP

Founded in 2008, VLP is a business and transactional law firm that delivers top quality legal services from experienced attorneys through an efficient platform. VLP's broad practice includes high tech, life sciences, clean tech, retail, consumer products, edtech, and real estate. VLP's clients range from from individual executives and early-stage startups to Fortune 500 companies, including public and private corporations, venture capital investors, private equity funds, educational institutions and companies, nonprofits and individuals. VLP provides general corporate, licensing, contract, intellectual property protection and counseling, securities regulation, financing, merger and acquisition, real estate, commercial lending, tax, employment and other legal services.

The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

Brief Speaker Bios:

Hewlett Packard Enterprise
Nathan Hall
Director of Solutions Architecture

Nathan leads the Hybrid IT field engineering organization for HPE North America which includes HPE's Hyperconverged (SimpliVity) and Composable (Synergy) product lines, as well as HPE's container and orchestration technology portfolios. Prior to the HPE acquisition, Nathan held various leadership roles at SimpliVity over his three year tenure, and was directly involved in a range of key company initiatives ranging from revamping enterprise marketing messaging, to margin improvement, to utility/consumption pricing and metering models to better compare and compete with AWS. Prior to SimpliVity, Nathan was the global CTO for one of EMC's largest accounts, and led the architecture and technical team for delivering a novel on-premise cloud solution with utility AWS-like metering and pricing for one of the world's largest companies, which ultimately led to the largest end-user transaction in EMC's history prior to the Dell acquisition. Nathan has also held several other notable roles in the technology industry, including co-founder and Chief Architect of ColdStor Data, where he led the design, was awarded patents, and brought to market the world's first purpose-built for archive cloud storage service.

Hewlett Packard Enterprise
Vinay Jonnakuti
Sr. Manager, Technical Marketing and Solutions

Vinay brings in 10 years of experience working on Data Center technologies. As a leader in the technical marketing organization he currently manages a team of technologists and engages with customers to bring the feedback to make HPE Products better. He comes from SimpliVity acquisition into HPE, where he architected and built a platform to provide a cloud based infrastructure to showcase SimpliVity technology across the globe. Prior to SimpliVity, he has 7 years of experience working at EMC in various roles specializing on replication technologies.

The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

Brief Speaker Bio:

VLP Law Group LLP
Melissa Krasnow
Partner

Melissa Krasnow is a partner at VLP Law Group LLP whose practice encompasses domestic and cross-border privacy and data security, technology transactions and mergers and acquisitions.

She advises companies on responding to data breaches (HIPAA, FERPA, financial services regulatory and PCI DSS), preparing written information security programs, devising incident response plans and facilitating tabletop exercises. Melissa counsels boards of directors and executive officers on privacy and data security risk oversight and developments and reviews cyber liability insurance policies. She advises companies on responding to regulatory inquiries and complying with state, federal and international privacy and data security and related laws. Melissa is a Certified Information Privacy Professional/US (CIPP/US) and a National Association of Corporate Directors Board Leadership Fellow.

The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

Ransomware is a type of malicious software that can slow down or even immobilize a user's computer access and then attempt to exact money to cure the problem. It can range from rogue security and tech support, to screen lockers that claim illegal activity has been detected, and most dangerously to malware that steals and encrypts the user's files – literally holding them for ransom.

One of the most prevalent forms of cyberattack today, ransomware is aimed not only at individuals but also at businesses and institutions. Antivirus and antimalware software are essential weapons for the defensive arsenal, but larger organizations may need to take more sophisticated measures to prevent costly data corruption or loss, and to combat ransomware when it attacks.

This LIVE Webcast by The Knowledge Group will give a thorough overview of the ransomware epidemic and offer insights and practical tips on how to implement an effective cybersecurity strategy.

Some of the major topics that will be covered in this course are:

- Ransomware Types
- Prime Targets of Ransomware
- Business Operational Risks and Legal Pitfalls
- Risk Identification and Mitigation
- Best Practices and Recommendations

The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

Hewlett Packard Enterprise

SEGMENT 1:
Nathan Hall
Director of Solutions Architecture
Hewlett Packard Enterprise

Hewlett Packard Enterprise

SEGMENT 2:
Vinay Jonnakuti
Sr. Manager, Technical Marketing and Solutions
Hewlett Packard Enterprise

VLP LAW GROUP LLP

SEGMENT 3:
Melissa Krasnow
Partner
VLP Law Group LLP

► *For more information about the speakers, you can visit: https://theknowledgegroup.org/event-homepage/?event_id=2061*

The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

Hewlett Packard Enterprise

SEGMENT 1:
Nathan Hall
Director of Solutions Architecture
Hewlett Packard Enterprise

HPE SimpliVity 380

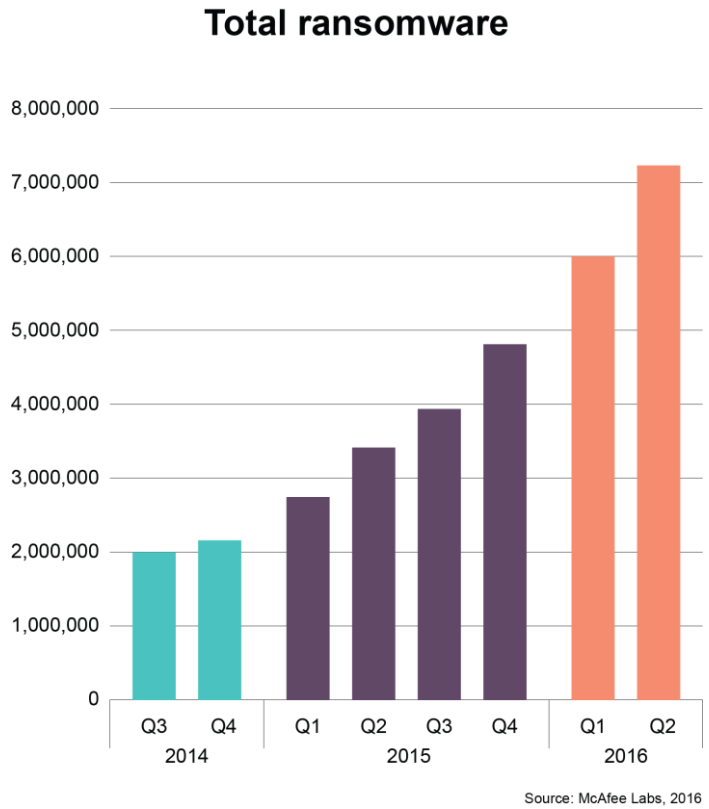
Defeat ransomware with built-in data protection

The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

Hewlett Packard Enterprise

SEGMENT 1:
Nathan Hall
Director of Solutions Architecture
Hewlett Packard Enterprise

The ransomware scourge



The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

Hewlett Packard Enterprise

SEGMENT 1:
Nathan Hall
Director of Solutions Architecture
Hewlett Packard Enterprise

The WannaCry ransomware attack

The attack has hit more than 200,000 victims in at least 150 countries, says Europol

200,000
Victims

150
Countries

Source: intel.malwaretech.com

The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

Hewlett Packard Enterprise

SEGMENT 1:
Nathan Hall
Director of Solutions Architecture
Hewlett Packard Enterprise

Cost of ransomware

Ransom fees are typically between

$200 and **$10,000**

Source: Gartner*

7,694 ransomware complaints totaling

$57M since **2005**

Source: Internet Crime Complaint Center

Cost of downtime

$7,900 per **minute**

Source: Ponemon Institute

*Use These Five Backup and Recovery Best Practices to Protect Against Ransomware, Robert Rhame, Roberta J. Witty, 8 June 2016.

The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

Hewlett Packard Enterprise

SEGMENT 1:
Nathan Hall
Director of Solutions Architecture
Hewlett Packard Enterprise

Gartner's take on planning for a ransomware attack

Gartner cites the following key challenges:
Antivirus software cannot be relied upon to detect and stop all ransomware.
A single infected client can encrypt file shares, potentially including cloud storage locations.
Once files are encrypted, organizations have two choices: restore from a backup or pay up.

Use These Five Backup and Recovery Best Practices to Protect Against Ransomware, Robert Rhame, Roberta J. Witty, 8 June 2016.

Ransomware is generating huge revenue and causing significant damage. It should be expected that these attacks will continue to intensify in volume and sophistication.

The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

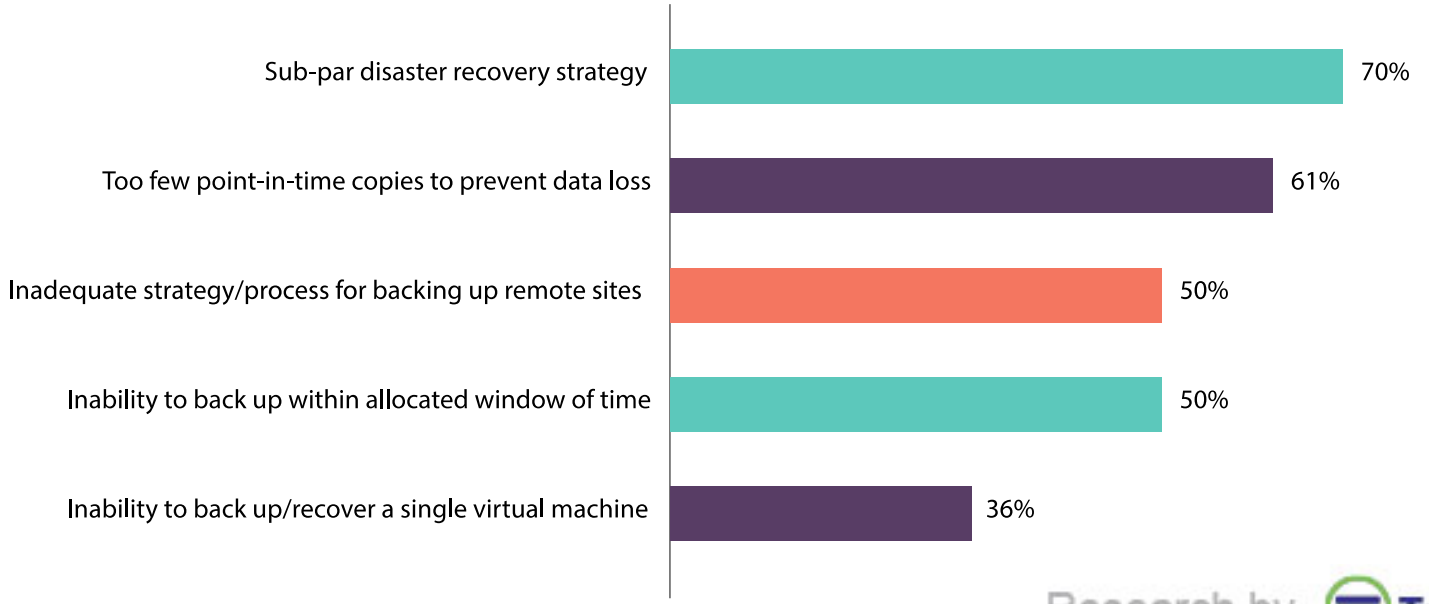
Hewlett Packard Enterprise

SEGMENT 1:
Nathan Hall
Director of Solutions Architecture
Hewlett Packard Enterprise

Ransomware problem compounded by poor data protection

Data protection challenges

Before deploying HPE SimpliVity hyperconverged infrastructure, which of the following data protection challenges did you experience?



Research by TechValidate

The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

Hewlett Packard Enterprise

SEGMENT 1:
Nathan Hall
Director of Solutions Architecture
Hewlett Packard Enterprise

If ransomware strikes, are you prepared?

- How many different backup and disaster recovery (DR) solutions are required to meet your current service level agreements (SLAs)?
- How long does it take to manage backup policies?
- What recovery time objectives (RTOs) and recovery point objectives (RPOs) can you achieve today?
- **How soon could you recover in the case of a disaster?**

The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

Hewlett Packard Enterprise

SEGMENT 1:
Nathan Hall
Director of Solutions Architecture
Hewlett Packard Enterprise

Credit union streamlines disaster recovery with HPE SimpliVity

Challenge

- Refresh data center hardware with a solution that aligns to virtualization
- Provide for integrated disaster recovery, shorten recovery times
- Simplify management, allowing for a small team
- Shrink infrastructure footprint

Solution components

3 HPE SimpliVity systems

- Refreshed and reduced data center equipment
- Minimal impact on operations
- Integrated disaster recovery set solution apart

Outcome

- Automated and cost-effective disaster recovery
- Enhanced flexibility for improved overall performance
- Seamless data-center-in-a-box implementation
- Simple solution and simplified management without sacrificing performance or scalability

The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

Hewlett Packard Enterprise

SEGMENT 1:
Nathan Hall
Director of Solutions Architecture
Hewlett Packard Enterprise

Profile of a CryptoLocker attack

Ransomware attack holds Central One Federal Credit Union data hostage

3:30 p.m. First signs of trouble

– First noticed problem when employee couldn't process large file from the Federal Reserve

– At first, thought it was a problem with core application vendor

– Vendor identified corrupt file as possible root cause

6:00 p.m. Attempt to copy folder from another branch location

– Attempted to copy the folder from another branch location

– WAN connection only 1.5 Mbps took about two hours to process

8:00 p.m. Discovery of CryptoLocker ransomware demand

– After transfer, file was still not able to process

– Team then identified the root cause as CryptoLocker

The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

Hewlett Packard Enterprise

SEGMENT 1:
Nathan Hall
Director of Solutions Architecture
Hewlett Packard Enterprise

Recovering from CryptoLocker with HPE SimpliVity

- A recovery point from prior to the infection was selected
- HPE SimpliVity restored the 500 GB virtual machine (VM) in seconds
- Database was operational in minutes
- Subsequent transactions recovered and processed

8:30 p.m. The team left the office

No data lost.

No ransom paid.

The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

Hewlett Packard Enterprise

SEGMENT 1:
Nathan Hall
Director of Solutions Architecture
Hewlett Packard Enterprise

Solving data protection

- ✓ Reliable data protection that's easy to manage
- ✓ Instant backup and recovery of data
- ✓ Simple and highly efficient offsite disaster recovery
- ✓ Highly resilient architecture to maximize uptime and prevent data loss

The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

Hewlett Packard Enterprise

SEGMENT 1:
Nathan Hall
Director of Solutions Architecture
Hewlett Packard Enterprise

HPE SimpliVity Data Virtualization Platform

Guaranteed data efficiency

- Always-on compression and deduplication
- All data at inception, globally
- Offloaded to HPE OmniStack Accelerator
- Guaranteed 90% capacity savings across primary storage and backup

40:1

HPE SimpliVity customers average **40:1 data efficiency** and half see greater than 50% performance improvements

TechValidate

The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

Hewlett Packard Enterprise

SEGMENT 1:
Nathan Hall
Director of Solutions Architecture
Hewlett Packard Enterprise

HPE SimpliVity Data Virtualization Platform

Built-in resiliency, backup, and disaster recovery

- Full logical backups with near zero overhead
- Guaranteed 60-second restore of 1 TB virtual machine
- Granular RTOs and RPOs from hours to seconds
- Simple, affordable offsite DR
- Redundant array of independent nodes (RAIN) and RAID protection of data

51%
of customers using HPE SimpliVity built-in data protection **retired existing third-party backup or replication** (IDC)[1]

70%
improvement in backup/recovery and DR reported by HPE SimpliVity customers (IDC)[1]

57%
of HPE SimpliVity customers **reduced recovery times** from days or hours to **minutes** (TechValidate)[2]

TechValidate

IDC Analyze the Future

[1]IDC white paper, "HPE SimpliVity Hyperconvergence Drives Operational Efficiency and Customers are Benefiting," June 2017
[2]2016 TechValidate survey of HPE SimpliVity infrastructure customers

The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

Hewlett Packard Enterprise

SEGMENT 1:
Nathan Hall
Director of Solutions Architecture
Hewlett Packard Enterprise

HPE SimpliVity Data Virtualization Platform

Global VM-centric management and mobility

- Policy-based, VM-centric management
- No logical unit numbers (LUNs), shares, or volumes
- Right-click operations
- Native tool integration
- Single view of all data centers and ROBOs

81% **increase** in time spent on new projects

IDC Analyze the Future

The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

Hewlett Packard Enterprise

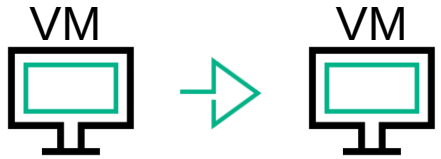
SEGMENT 1:
Nathan Hall
Director of Solutions Architecture
Hewlett Packard Enterprise

Instant backup and recovery of data - guaranteed

HPE SIMPLIVITY HYPERGUARANTEE

HyperProtected

60 seconds or less on average for local backup or restore of a 1 TB VM



- Powered by HPE SimpliVity infrastructure's unmatched data efficiency
- Full logical backups in seconds
- Application-aware backups and file-level restore
- RPOs of minutes, RTOs of seconds

For detailed information about the HPE SimpliVity Guarantee, including conditions and limitations please see HPE SimpliVity Guarantee

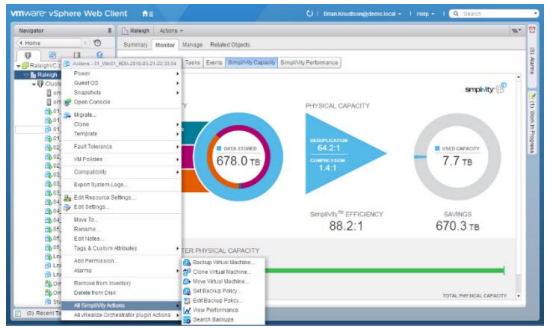
The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

Using HPE SimpliVity user interface—you only need three clicks

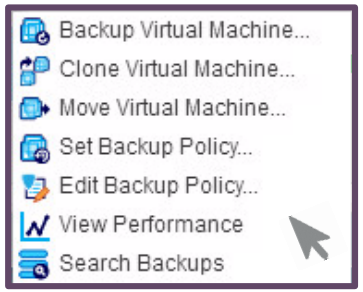
SEGMENT 1:
Nathan Hall
Director of Solutions Architecture
Hewlett Packard Enterprise

HPE SIMPLIVITY HYPERGUARANTEE

HyperSimple



Just three clicks



- Simple, intuitive interface
- No LUNs, shares, or volumes
- Empowers IT generalists and VM admins
- Familiar tools and interfaces like vCenter, vRealize, and UCSD

Over half (57%) of customers benefitted from an average of

53%

increase in **staff productivity**

For detailed information about the HPE SimpliVity HyperGuarantee, including conditions and limitations, please see HPE SimpliVity Guarantee
IDC white paper, "HPE SimpliVity Hyperconvergence Drives Operational Efficiency and Customers are Benefiting," June 2017

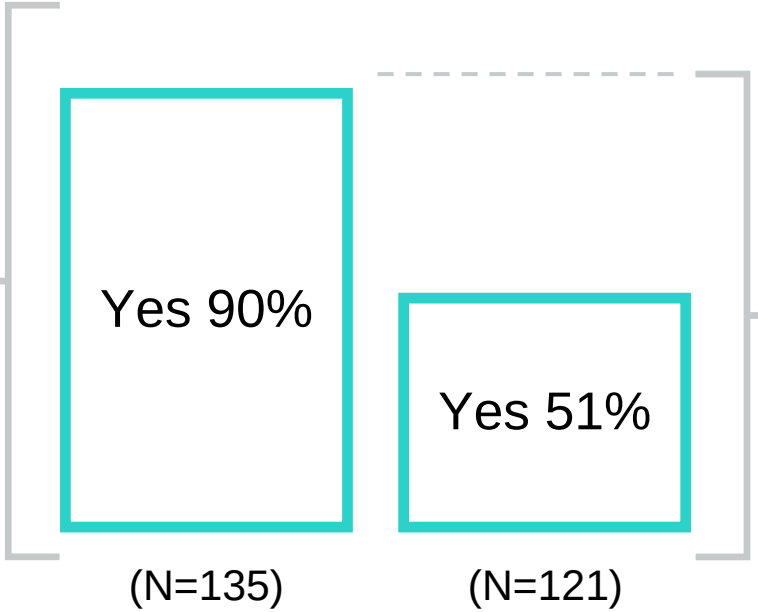
The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

Hewlett Packard Enterprise

SEGMENT 1:
Nathan Hall
Director of Solutions Architecture
Hewlett Packard Enterprise

Displacing third-party backup and replication at ROBOs

90% of HPE SimpliVity customers use the built-in backup/recovery



51% of HPE SimpliVity customers retired existing third-party backup / replication software in lieu of HPE SimpliVity's data protection features

IDC white paper, "HPE SimpliVity Hyperconvergence Drives Operational Efficiency and Customers are Benefiting," June 2017

The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

Hewlett Packard Enterprise

SEGMENT 2:
Vinay Jonnakuti
Sr. Manager, Technical Marketing and Solutions
Hewlett Packard Enterprise

Talking Points

- Showcase how you can easily recover after Ransomware with HPE SimpliVity
- HPE SimpliVity provides Reliable data protection that's easy to manage
- HPE SimpliVity provides Highly resilient architecture to maximize uptime and prevent data loss

The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

SEGMENT 3:
Melissa Krasnow
Partner
VLP Law Group LLP

What is Ransomware?

Ransomware is a form of malware targeting both human and technical weaknesses in an effort to deny the availability of critical data and/or systems. Ransomware is frequently delivered through various vectors, including phishing and Remote Desktop Protocol (RDP). RDP allows computers to connect to each other across a network. In one scenario, spear phishing emails are sent to end users resulting in the rapid encryption of sensitive files on a corporate network. When the victim organization determines they are no longer able to access their data, the cyber actor demands the payment of a ransom, typically in virtual currency such as Bitcoin. The actor will purportedly provide an avenue to the victim to regain access to their data. Recent iterations target specific organizations and their employees, making awareness and training a critical preventative measure. In 2016, the IC3 received 2,673 complaints identified as ransomware with losses of over $2.4 million. Source: FBI Internet Crime Complaint Center 2016 Internet Crime Report at https://pdf.ic3.gov/2016_IC3Report.pdf

The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

SEGMENT 3:
Melissa Krasnow
Partner
VLP Law Group LLP

How is Ransomware Delivered?

Ransomware often arrives through e-mail phishing campaigns, which typically require the user to take an action such as clicking on a link or downloading a malicious attachment. Other campaigns use drive-by downloads, where a user visits a malicious website or a site that has been compromised, and the act of loading the site causes the ransomware to automatically download onto the user's computer. In addition, ransomware is delivered through "malvertising" campaigns, where malicious code is hidden in an online ad that infects the user's computer….Attackers also have exploited server-side vulnerabilities to deliver ransomware payloads by searching for networks that had failed to patch known vulnerabilities. Source: FTC Business Blog at https://www.ftc.gov/news-events/blogs/business-blog/2016/11/ransomware-closer-look

The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

SEGMENT 3:
Melissa Krasnow
Partner
VLP Law Group LLP

Federal Trade Commission's Recommended Steps

- Keep software up-to-date - download security updates as soon as they are available – no matter what operating system.
- Back up important files routinely.
- Think twice before clicking on links or downloading attachments and apps. Source: FTC Business Blog at https://www.ftc.gov/news-events/blogs/business-blog/2017/05/wannacry-worries-update-now

The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

SEGMENT 3:
Melissa Krasnow
Partner
VLP Law Group LLP

Federal Trade Commission Remarks About Ransomware

A company's unreasonable failure to patch vulnerabilities known to be exploited by ransomware might violate the FTC Act….businesses play a critical role in ensuring that they adequately protect consumers' information, particularly as security threats like ransomware escalate.
Source: Opening Remarks of FTC Chairwoman Edith Ramirez, Fall Technology Series: Ransomware at https://www.ftc.gov/system/files/documents/public_statements/983593/ramirez_-_ransomware_remarks_9-7-16.pdf

The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

SEGMENT 3:
Melissa Krasnow
Partner
VLP Law Group LLP

Department of Health and Human Services Guidance

When electronic protected health information (ePHI) is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the information), and thus is a "disclosure" not permitted under the HIPAA Privacy Rule. Source: FACT SHEET: Ransomware and HIPAA at https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

[An] increase in HIPAA violations includes breaches due to ransomware events, such as WannaCry, and other cyber attacks….could have been prevented by an informed workforce trained to detect and properly respond to them. Training on data security for workforce members is not only essential for protecting an organization against cyber attacks, it is also required by the HIPAA Security Rule. Source: Train Your Workforce, so They Don't Get Caught by a Phish! at https://www.hhs.gov/sites/default/files/july-2017-ocr-cyber-newsletter.pdf

The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

VLP LAW GROUP LLP

SEGMENT 3:
Melissa Krasnow
Partner
VLP Law Group LLP

Department of Homeland Security US-CERT Alert Regarding WannaCry

Recommended steps for prevention.

Recommendations for network protection.

Recommended steps for remediation.

Defending against ransomware generally. Source: US-CERT Alert (TA17-132A) at https://www.us-cert.gov/ncas/alerts/TA17-132A; note that this Alert is referenced in https://www.sec.gov/files/risk-alert-cybersecurity-ransomware-alert.pdf

The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

SEGMENT 3:
Melissa Krasnow
Partner
VLP Law Group LLP

What Steps Does the FBI Recommend Taking?

Isolate the infected computer immediately, and remove infected systems from the network as soon as possible to prevent ransomware from attacking network or share drives.

Isolate or power off affected devices that have not yet been completely corrupted.

Immediately secure backup data or systems by taking them offline, and ensure backups are free of malware.

Contact law enforcement immediately.

Collect and secure partial portions of the ransomed data that might exist if available.

The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

SEGMENT 3:
Melissa Krasnow
Partner
VLP Law Group LLP

What Steps Does the FBI Recommend Taking? (con't)

Change all online account passwords and network passwords after removing the system from the network if possible, and change all system passwords once the malware is removed from the system.

Delete registry values and files to stop the program from loading.

Implement security incident response and business continuity plans.

The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

SEGMENT 3:
Melissa Krasnow
Partner
VLP Law Group LLP

What Steps Does the FBI Recommend Taking? (con't)

Conduct a post incident review of the response to the incident, and assess the strengths and weaknesses of the incident response plan. Source: FBI brochure at https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view

The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

SEGMENT 3:
Melissa Krasnow
Partner
VLP Law Group LLP

Reaching Out to the FBI / Filing a Complaint

The FBI requests that victims reach out to their local FBI office and/or file a complaint with the Internet Crime Complaint Center at https://www.ic3.gov/default.aspx
Source: FBI public service announcement at https://www.ic3.gov/media/2016/160915.aspx

The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

SEGMENT 3:
Melissa Krasnow
Partner
VLP Law Group LLP

Should the Ransom be Paid?

The FBI does not support paying a ransom to the adversary because it does not guarantee the victim will regain access to their data. In fact, some individuals or organizations are never provided with decryption keys after paying a ransom. Paying a ransom emboldens the adversary to target other victims for profit and could provide an incentive for other criminals to engage in similar illicit activities for financial gain. Although the FBI does not support paying a ransom, it recognizes that executives, when faced with inoperability issues, will evaluate all options to protect their shareholders, employees, and customers. Source: FBI public service announcement at https://www.ic3.gov/media/2016/160915.aspx

The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

SEGMENT 3:
Melissa Krasnow
Partner
VLP Law Group LLP

No More Ransom!

NEED HELP unlocking your digital life without paying your attackers*?

* The general advice is not to pay the ransom. By sending your money to cybercriminals you'll only confirm that ransomware works, and there's no guarantee you'll get the decryption key you need in return.

Source: https://www.nomoreransom.org/en/index.html

The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

SEGMENT 3:
Melissa Krasnow
Partner
VLP Law Group LLP

FBI on Prevention and Continuity Measures

Regularly back up data and verify the integrity of those backups.

Secure your backups and ensure backups are not connected to the computers and networks they are backing up.

Scrutinize links contained in e-mails and do not open attachments included in unsolicited e-mails.

Only download software – especially free software – from sites you know and trust. When possible, verify the integrity of the software through a digital signature prior to execution.

The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

SEGMENT 3:
Melissa Krasnow
Partner
VLP Law Group LLP

FBI on Prevention and Continuity Measures (con't)

Ensure application patches for the operating system, software, and firmware are up to date.

Ensure anti-virus and anti-malware solutions are set to automatically update and regular scans are conducted.

Disable macro scripts from files transmitted via e-mail.

Implement software restrictions or other controls to prevent the execution of programs in common ransomware locations, such as temporary folders supporting popular Internet browsers, or compression/decompression programs, including those located in the AppData/LocalAppData folder.

The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

SEGMENT 3:
Melissa Krasnow
Partner
VLP Law Group LLP

FBI on Prevention and Continuity Measures (con't)

Enable strong spam filters to prevent phishing e-mails from reaching the end users, and authenticate inbound e-mail using technologies like Sender Policy Framework, Domain Message Authentication Reporting and Conformance, and DomainKeys Identified Mail to prevent e-mail spoofing.

Scan all incoming and outgoing e-mails to detect threats, and filter executable files from reaching end users.

Configure firewalls to block access to known malicious IP addresses.

Consider disabling Remote Desktop Protocol if it is not being used.

Conduct an annual penetration test and vulnerability assessment. Source: FBI brochure, Ransomware Prevention and Response for CISOs, at https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view

The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

SEGMENT 3:
Melissa Krasnow
Partner
VLP Law Group LLP

FBI on Prevention and Continuity Measures (con't)

Focus on awareness and training.

Patch all endpoint device operating systems, software, and firmware as vulnerabilities are discovered.

Manage the use of privileged accounts by implementing the principle of least privilege.

Configure access controls with least privilege in mind.

Use virtualized environments to execute operating system environments or specific programs.

The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

SEGMENT 3:
Melissa Krasnow
Partner
VLP Law Group LLP

FBI on Prevention and Continuity Measures (con't)

Categorize data based on organizational value, and implement physical/logical separation of networks and data for different organizational units.

Require user interaction for end user applications communicating with Web sites uncategorized by the network proxy or firewall.

Implement application whitelisting. Only allow systems to execute programs known and permitted by security policy. Source: FBI public service announcement at https://www.ic3.gov/media/2016/160915.aspx

The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

SEGMENT 3:
Melissa Krasnow
Partner
VLP Law Group LLP

Additional Considerations

Organizations also should conduct a cyber-security risk analysis of the organization and have and test an incident response plan. FBI brochure at https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-ceos.pdf/view

Take into account insurance coverage, namely cyber-liability/cyber-extortion coverage.

See article on kidnap insurance and ransomware at http://www.reuters.com/article/us-cyber-attack-insurance-idUSKCN18F1LU

The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

SEGMENT 3:
Melissa Krasnow
Partner
VLP Law Group LLP

Additional Considerations (con't)

After….[the]….devastating global ransomware attack, now known as WannaCry, directors will once again be questioning management teams to make sure the company is protected. The challenge is that most directors do not know what questions they should be asking.

If I were sitting on a board, this attack would prompt me to ask questions about the following three areas: End of Life (EOL) software; patching; and disaster recovery. Source: https://blog.nacdonline.org/2017/05/questions-to-ask-after-the-wannacry-attack/

Public company disclosure:

We do not have cyber or other insurance in place that covers this attack.

Source: FedEx Corporation Quarterly Report on Form 10-Q at https://www.sec.gov/Archives/edgar/data/1048911/000156459017018835/fdx-10q_20170831.htm

The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

SEGMENT 3:
Melissa Krasnow
Partner
VLP Law Group LLP

National Institute of Standards and Technology (NIST)

The National Institute of Standards and Technology (NIST) Guide for Cybersecurity Event Recovery at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf includes an example of a recovery plan in the form of a playbook for a ransomware attack. While the guide applies to US federal agencies, it should be useful to any organization.

Constant threats of destructive malware, ransomware, malicious insider activity and honest mistakes create the imperative for organizations to be able to quickly recover from an event that alters or destroys data. The National Cybersecurity Center of Excellence (NCCoE), together with members of the business community and vendors of cybersecurity solutions (Hewlett Packard Enterprise is a Technology Partner/Collaborator), released the draft NIST Cybersecurity Practice Guide, *Data Integrity: Recovering from Ransomware and Other Destructive Events*, SP 1800-11. Public comments on this draft will be accepted through November 6, 2017.
Source: https://nccoe.nist.gov/projects/building-blocks/data-integrity

The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

SEGMENT 3:
Melissa Krasnow
Partner
VLP Law Group LLP

Resources

Ransomware Guidance at https://www.irmi.com/articles/expert-commentary/guidance-on-ransomware

Cyber-Security Event Recovery Plans at https://www.irmi.com/articles/expert-commentary/cyber-security-event-recovery-plans

Directors and Cybersecurity at http://www.vlplawgroup.com/wp-content/uploads/2017/01/M.Krasnow-Bloomberg-Article-1-2017.pdf

The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

Q&A:

Nathan Hall
Director of Solutions Architecture
Hewlett Packard Enterprise
nathan.hall@hpe.com
646-704-3540

Vinay Jonnakuti
Sr. Manager, Technical Marketing and Solutions
Hewlett Packard Enterprise
vinay.jonnakuti@hpe.com
(508) 948-3292

Melissa Krasnow
Partner
VLP Law Group LLP
MKrasnow@vlplawgroup.com
(312) 350-1082

► *You may ask a question at anytime throughout the presentation today. Simply click on the question mark icon located on the floating tool bar on the bottom right side of your screen. Type your question in the box that appears and click send.*

► *Questions will be answered in the order they are received.*

The Increasing Risks of Ransomware: What Your Business Needs to Know and Do

ABOUT THE KNOWLEDGE GROUP

The Knowledge Group is an organization that produces live webcasts which examine regulatory changes and their impacts across a variety of industries. “We bring together the world's leading authorities and industry participants through informative webcasts to study the impact of changing regulations.”

If you would like to be informed of other upcoming events, please click here.

DISCLAIMER:

The Knowledge Group is producing this event for information purposes only. We do not intend to provide or offer business advice.

The contents of this event are based upon the opinions of our speakers. The Knowledge Group does not warrant their accuracy and completeness. The statements made by them are based on their independent opinions and does not necessarily reflect that of The Knowledge Group‘s views.

In no event shall The Knowledge Group be liable to any person or business entity for any special, direct, indirect, punitive, incidental or consequential damages as a result of any information gathered from this webcast.