

◆ WSJ NEWS EXCLUSIVE | BUSINESS

Colonial Pipeline CEO Tells Why He Paid Hackers a \$4.4 Million Ransom

Joseph Blount says he needed to quickly restore service after cyberattack threatened East Coast supply

THE COST OF A MALWARE INFECTION?
FOR MAERSK, \$300 MILLION

Backups in the Age of Ransomware

Nik Simpson (Gartner)
October 20, 2021

SECURITY

The WannaCry ransomware attack left the NHS with a £73m IT bill

22 Texas Towns Hit With Ransomware Attack In 'New Front' Of Cyberassault

Alert: Further ransomware attacks on the UK education sector by cyber criminals

The NCSC is responding to further ransomware attacks on the education sector by cyber criminals.

World's biggest meat producer JBS pays \$11m cybercrime ransom

Brazil-based giant paid ransom in bitcoin after ransomware attack shut down operations across world

2020 Was Bad!

5400

Companies surveyed

37%

Hit by ransomware

\$170,404

Average payout

65%

Data recovered

2021 Is Worse!

State and Local Government is a Target

An Overview of the Texas Ransomware Attack and What You Can Learn from It

A Coordinated Ransomware Attack Hit 22 Texas Municipalities in 2019. Here's What You Can Learn from It.

<https://heimdalsecurity.com/blog/texas-ransomware-attack/>

Alaska Health Department Services Affected by Malware Attack

Latest in a String of Incidents at Public Health Agencies Globally

Marianne Kolbasuk McGee (HealthInfoSec) • May 20, 2021

<https://www.govinfosecurity.com/alaska-health-department-services-affected-by-malware-attack-a-16708>

Louisiana Suffers Another Major Ransomware Attack



Lee Mathews Senior Contributor

Cybersecurity

Observing, pondering, and writing about tech. Generally in that order.

Follow

<https://www.forbes.com/sites/leemathews/2019/11/20/louisiana-suffers-another-major-ransomware-attack>

Incident Of The Week: Alabama Hit By 2nd Ransomware Attack In As Many Months

User Awareness Potentially Thwarts Threat

<https://www.cshub.com/attacks/articles/incident-of-the-week-alabama-hit-by-2nd-ransomware-attack-in-as-many-months>

Cyber criminals executed attack on Bristol police computers

David McGee Jul 27, 2021 Updated Sep 9, 2021 0

https://heraldcourier.com/news/cyber-criminals-executed-attack-on-bristol-police-computers/article_c69c24f2-e320-5d74-9134-52129a50f447.html/

Information Posted Online After N Carolina Ransomware Attack

Officials in a North Carolina county say an investigation into a cyber attack on its computer network showed personal information posted for sale on the "dark web."

<https://www.usnews.com/news/best-states/north-carolina/articles/2021-02-16/information-posted-online-after-n-carolina-ransomware-attack>

A large, ancient stone castle with multiple towers and battlements, set against a clear blue sky. The castle is built on a grassy hill. The text is overlaid on the right side of the image.

Backups are the last line of defense!

If backups are lost or damaged during the attack there is no plan B.

But Backups are Under Attack



Drive-by
attacks

Backup not specifically targeted
Backup storage exposed or unpatched
security flaw in backup system



Targeted
attacks

Backup system specifically targeted
Backup storage, or Backup
Administrative console breached

**Encrypted or deleted backups means:
Lost Data... Lost Time...Lost Revenue...Lost
Customers... Lost business**

How can I Protect Backups?



Protect The Backup Storage

- ✓ Audit write permissions on backup storage
- ✓ Use non-interactive accounts for backup
- ✓ Apply security patches promptly
- ✓ Don't use obsolete infrastructure

Protect The Backup Console

- ✓ Require MFA for all logins to the console
- ✓ Use RBAC to limit “blast radius”
- ✓ Restrict console access locations
- ✓ Talk to your backup vendor!!!

**Attacks target more than
just data and backups!**

Protect Critical Infrastructure

 Active Directory

 DNS, DHCP configurations

 DNS, DHCP configurations

 Storage array/NAS configuration

Protect Critical Infrastructure



Application build environments



Switch & Router configurations



Gold system images



Firmware images

How can I recover from backups?



Multiple Challenges



When the
attack started

When was your last “good” backup?

Can you accept the data loss inherent in using the last good backup?



Infected
backups

Unencrypted doesn't mean uninfected

Any changes made over the course of the attack are captured in backup



Endpoint
strategy

When was your last “good” backup?

Can you accept the data loss inherent in using the last good Backup?

Recovering Applications (1)

1

Operating system,
application code,
and data recovered
from backup to the
isolated recovery
environment

2

Operating system,
application code,
scanned for
malware in Isolated
recovery
environment

3

Cleaned application
promoted back to
production network

Strengths & Weaknesses

Strengths

- Standardized process for all workloads

Weaknesses

- Can't guarantee to catch everything
- Doesn't scale well without automation
- Require significant hardware resources, especially for physically-hosted workloads

Recovering Applications (1)

1

Only application data
recovered from backup

2

OS and application
recovered from vaulted
“Gold images” or
installation media

3



Reconstituted application
and data restored to
production network

Strengths & Weaknesses

Strengths

- High-degree of confidence that workload is clean after restoration
- Can leverage existing automation of provisioning

Weaknesses

- More complex for physically hosted workloads
- May require changes to the way applications are deployed

Next Steps



Follow backup vendor's best-practices



Investigate immutable storage & vaulting



Develop recovery plan & infrastructure



Conduct ransomware recovery exercises



Request an analyst call

Recommended Research

Detect, Protect, Recover: How Modern Backup Applications Can Protect You From Ransomware

G00733304

How to Protect Backup Systems From Ransomware Attacks

G00757692

Innovation Insight for Leveraging Isolated Recovery Environments and Immutable Data Vaults to Protect and Recover From Ransomware

G00748659

Magic Quadrant for Enterprise Backup and Recovery Software Solutions

G00733940

Critical Capabilities for Enterprise Backup and Recovery Software Solutions

G00733943

VITA SERVICE TALKS

Let's continue the conversation



LET'S CONTINUE THE CONVERSATION

VITA is offering customers an opportunity to expand upon the discussions that were started today. These service talks will either be one-on-one (agency/supplier) or in open group settings and will provide agencies the opportunity to ask more detailed questions about the services and how they can be applied to their organizations.

PLEASE VISIT THE VITA WEBSITE, VIRTUAL SERVICES FAIR PAGE, FOR INFORMATION ON JOINING THE GROUP SESSIONS AND SIGNING UP FOR 1:1 SESSIONS:

[HTTPS://WWW.VITA.VIRGINIA.GOV/TECHNOLOGY-SERVICES/SERVICES-FAIR/](https://www.vita.virginia.gov/technology-services/services-fair/)



The following VITA service talks have a capacity of 500 attendees:

- **Cloud services**

- Tuesday, Nov. 9: 9 – 10:30 a.m.
- Tuesday, Nov. 16: 1 – 2:30 p.m.

- **Messaging services**

- Thursday, Oct. 21: 1 – 2:30 p.m.
- Thursday, Nov. 4: 9 – 10:30 a.m.

- **Voice and data services update**

- Monday, Oct. 25: 1 – 2:30 p.m.
- Monday, Nov. 15: 9 – 10:30 a.m.

Questions can be submitted in advance by emailing businessreadiness@vita.virginia.gov. Please include the topic in the subject line. For example: Question for messaging service talk

One-on-one service talks are available first come, first served. Please coordinate with your team and sign up your agency for one session only.

- **Application integration services (AIS)**

- Wednesday, Oct. 27: 9 – 10:30 a.m.
- Wednesday, Nov. 10: 1 – 2:30 p.m.

- **ePen**

- Thursday, Oct. 28: 9 – 10:30 a.m.
- Wednesday, Nov. 3: 1 – 2:30 p.m.

- **Box**

- Monday, Nov. 1: 9 – 10:30 a.m.
- Friday, Nov. 12: 9 – 10:30 a.m.

- **Robotic process automation (RPA)**

- Tuesday, Oct. 26: 9 – 10:30 a.m.
- Monday, Nov. 8: 1 – 2:30 p.m.