VMsources Group Inc.

# Intelligent Information Security

A Comprehensive Approach to security for Organizations

# Agenda

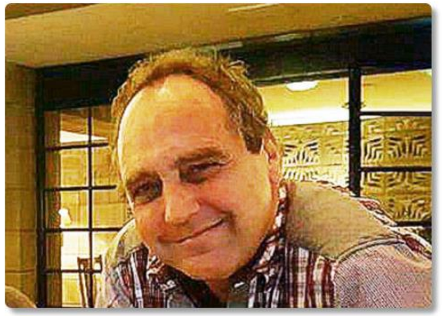
- Introductions
- “Where's the Beef?”
- Identify the Challenges
- Intelligent Information Security: Training, Prevention, Remediation (TPR)
  - **Training** – Educating users to avoid malware
  - **Prevention** – Preventing issues before they happen , utilizing active technologies to stop hackers before they hit gold
  - **Remediation** -- Being able to recover quickly & quietly when events do happen

# The VMsources Core Team

Real people with real experience

John Borhek
John is the CEO and Lead Solutions Architect and IT Director at VMsources Group, Inc.

Elizabeth Salazar
Elizabeth Salazar es nuestra especialista de mercado LATAM (América Latina y el Caribe).



Sean McMahan
Sean is all about making things work intelligently and helping intelligent people.

David Uihlein
Dave is our CTO and a fully trained and certified IT Specialist with over 30 years experience.

Ron Watkins
Ron is our director of Facilities Management and is responsible for upkeep of our facilities.

Jeff Marshall
Jeffrey Marshall, CPhT-ADV is a specialist in digital healthcare information management including electronic medical records, pharmaceutical studies, imaging, and patient care.

# The Challenges

## Ransomware

Network and security flaws allow Ransomware to spread through an Organization like fire

## Theft

Hackers are using new attack vectors to steal Organizational data and demand payments

## Identity Verification

Organizations encourage bad security by using obsolete policies and authentication methods

## Phishing

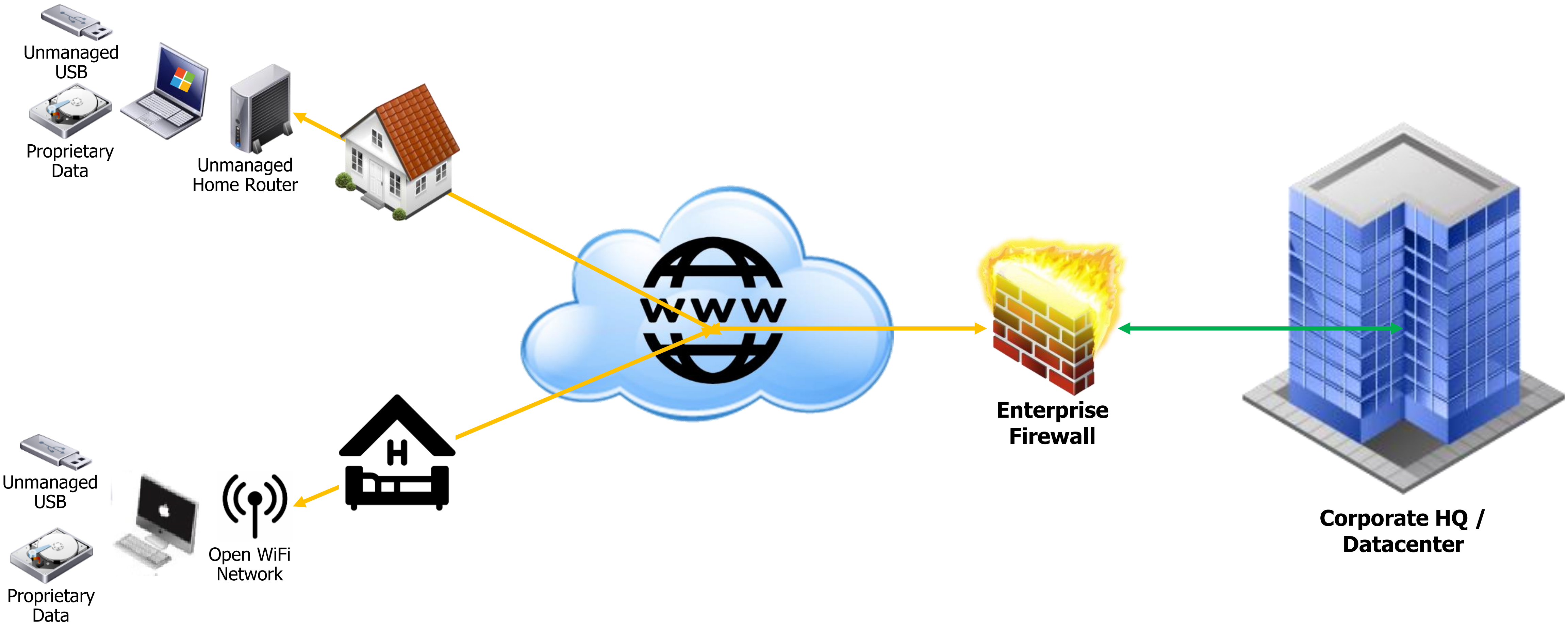
Lack of active filters subject users to sophisticated phishing emails on a daily basis

## Business Continuity

Many Organizations are unprepared to rapidly remediate Ransomware or failover in a disaster

# Where's the beef?

The ***"beef"*** is your organization's proprietary data and work product, and it needs to be protected and secure



# Ransomware

Networking is often the problem

- Ransomware is becoming more sophisticated.
  - Increased use of VPNs for remote users from unsecured networks has opened the door
  - Brute-force password and remote code execution are common vectors
  - Lack of network segmentation allows propagation.
- Recent front-page events like the Pipeline shutdown were the result of an insecure VPN
  - This event could have been prevented by following the recommendations we are going to present here

# Theft

New challenges for your Organization

- ○ Hackers used to disrupt Business Continuity and seek ransom payment
- ○ Now hackers also steal Organizational data and seek ransom payment(s) to not release the data
  - Obviously, there’s no guarantee that they won’t keep coming back

# Digital Identity

A username and a password are not enough anymore!

- Unnecessary password policies cause users to write down passwords
- Brute-force attacks without additional verification allow hackers directly onto proprietary systems
- Users often leave workstations unlocked
- It is common practice to share user accounts and passwords in order “to get it done”

# Phishing

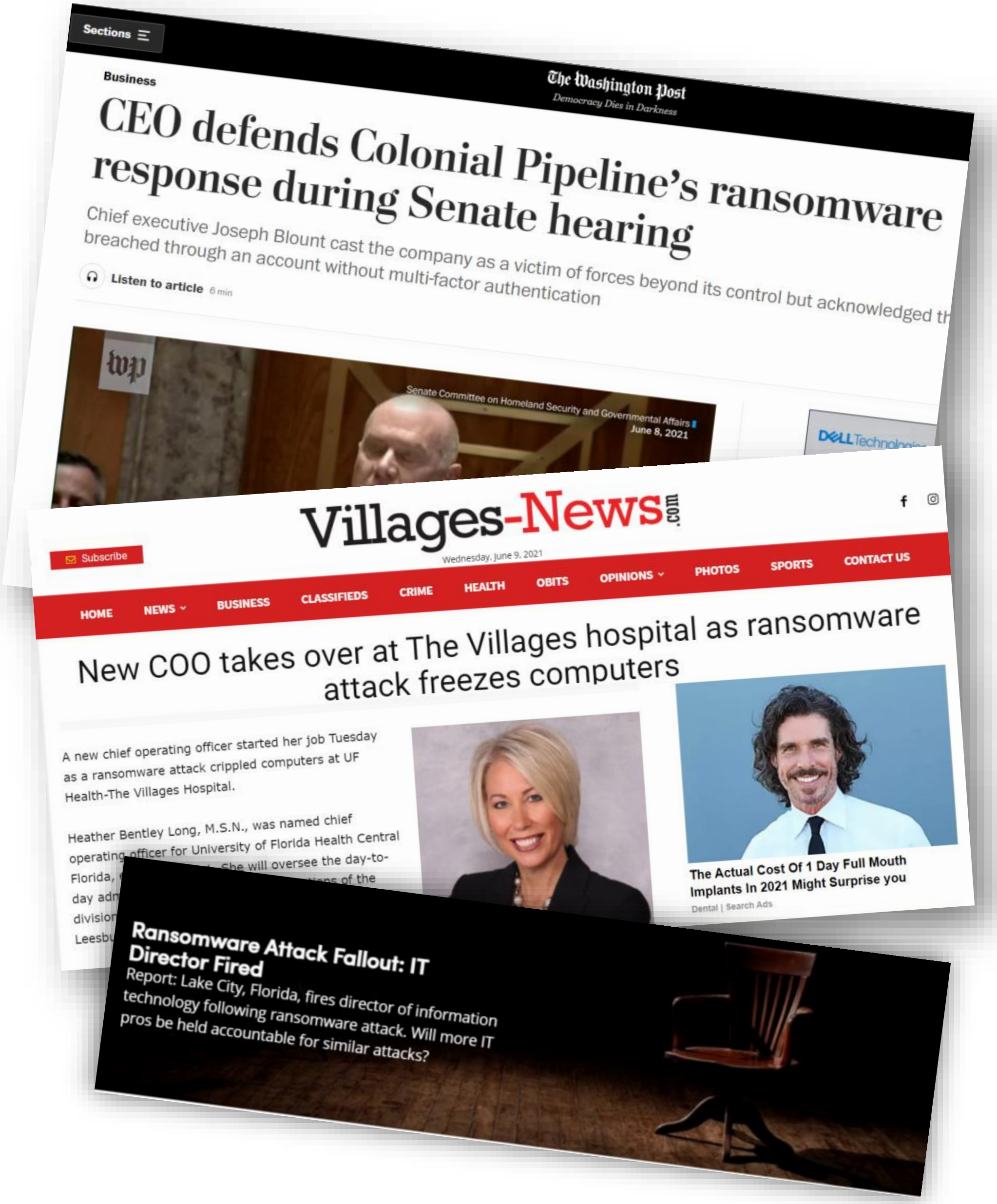
It's not all about deploying payloads anymore

- Hackers are developing more sophisticated Phishing attacks all the time
- It used to be all about delivering a Ransomware payload
- Now, Phishing attacks often identify key players in an organization for specifically target attacks:
  - Phishing from "customer" to AR at your Organization: "Please send future ACH transfers to this new address"
  - Phishing from "employee" to payroll at your Organization: "I changed banks, please send my paycheck…"
  - Phishing from "court" to payroll at your Organization: "John Q. Public is in default, direct 50% of paycheck to…"
- Unfortunately o365 is MUCH MORE vulnerable to Phishing than in-house Mail/Exchange+*
  - It is a larger target, and it is easier to spoof emails

# Business Continuity

Read All About It…

- Ransomware events are likely to occur, even with the best protections in place
- The key is in being able to recover quickly & quietly, without having to pay ransom
- Avoid significant disruptions to Business Continuity
- Don't let you or your Organization become headline news!



Sections

Business

The Washington Post

Democracy Dies in Darkness

CEO defends Colonial Pipeline's ransomware response during Senate hearing

Chief executive Joseph Blount cast the company as a victim of forces beyond its control but acknowledged th breached through an account without multi-factor authentication

Listen to article 6 min

Senate Committee on Homeland Security and Governmental Affairs June 8, 2021

Villages-News.com

Subscribe

Wednesday, June 9, 2021

HOME NEWS BUSINESS CLASSIFIEDS CRIME HEALTH OBITS OPINIONS PHOTOS SPORTS CONTACT US

New COO takes over at The Villages hospital as ransomware attack freezes computers

A new chief operating officer started her job Tuesday as a ransomware attack crippled computers at UF Health-The Villages Hospital.

Heather Bentley Long, M.S.N., was named chief operating officer for University of Florida Health Central Florida, … She will oversee the day-to-day adm… …tions of the division… Leesbu…

The Actual Cost Of 1 Day Full Mouth Implants In 2021 Might Surprise you

Dental | Search Ads

Ransomware Attack Fallout: IT Director Fired

Report: Lake City, Florida, fires director of information technology following ransomware attack. Will more IT pros be held accountable for similar attacks?

"Insanity is doing the same thing over and over and expecting different results."
-Albert Einstein

# Intelligent Information Security -- TPR

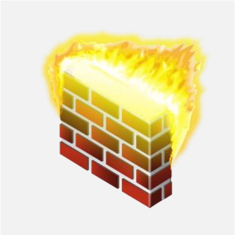
Training, Prevention, Remediation

# TPR – The foundations of Business Continuity

There is an opportunity for success

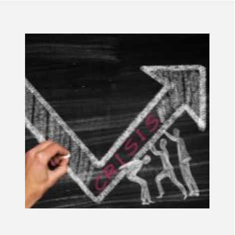
## Training

Educate your users and continually test their awareness to emerging threats using SET



## Prevention

Actively use technology you already own to avoid Ransomware and data exfiltration/theft



## Remediation

Be able to recover quickly and quietly when Ransomware happens and other losses occur

# Be successful - Know who's on first

Understanding all the components is the key to preventing incidents

- Perform Social Engineering Toolkit (SET) tests
- Do Network Penetration Testing
- Use Network Segmentation
- Deploy policies based on current guidelines
- Require 2FA
- Implement a true DMZ
- Stop using VPNs to connect users
- Use a Virtual Desktop to keep data in-house
- Use best-of-breed Endpoint Protection
- Keep firmware up-to-date

# Training

Educate Users to prevent Ransomware attacks

# Training

Knowledge is the key to user success

- Live events with team-building exercises are most effective
  - Mandatory training will help users understand the threats and avoid common mistakes
  - Understanding the challenges will make users sympathetic to new requirements
  - Team building will improve participation in security initiatives
- Webinars can work, but we know they are a drag!
- Recorded sessions are least effective
- Consider the following:
  - In-person group training (with remote participants).
    - The people in the room get the ball rolling and stimulate questions from the remote participants
  - Lunch & Learn
    - A small investment by your Organization will develop a positive attitude about the presentation

# Target Training Audience

Your entire Organization

- The audience for IT Awareness Training is your entire Organization, even the techies and administrators who are already knowledgeable.
  - The Techies will affirm the topics covered to their colleagues, creating confidence.
  - The administrators will share real-world experiences and challenges.
  - The bosses and supervisors presence will confirm the importance of the topic.
  - Team-building will establish enthusiasm and cooperation.

# Training Agenda

- Email security
  - What Phishing looks like today.
  - Testimonial + Q&A.
  - How SET is being deployed to improve security.
- 2FA
  - Why it’s important?
  - How it works for your Organization.
  - What's protected by 2FA and what’s not?
- Filesharing
  - The correct way to share files with colleagues, external recipients, even yourself

- Passwords
  - What is a good password?
  - When can we share a password?
- Sensitive Information
  - What is sensitive information?
  - How to use Microsoft Office to protect sensitive information.
  - How to share sensitive information with authorized people.
- Ransomware avoidance
  - Common ways Ransomware finds its way into systems and across firewalls.

# VMsources user Training and IT Awareness

What VMsources can do for your Organization

- VMsources has built a 60-minute IT Awareness training program for users.
- We learn about the Organization and tailor the program specifically to your needs.
  - Who’s your Email provider?
  - Have you engaged in SET or PEN Testing?
  - Do you use 2FA?
  - How do users connect to the Organization? (RDP, Citrix, Horizon, VPN)
- We engage users with testimonials and encourage Q&A.
- We have team-building exercises to emphasize the topics.
- Optional: Test covering general Information Security topics from a user perspective.
- Each participant gets a certificate of completion.

# Prevention

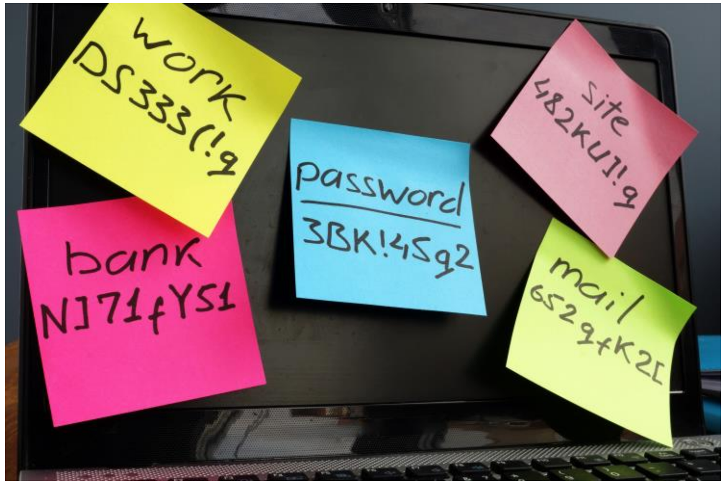
Active measures to improve security

# Identity

Smart and logical policies for your users

# There's more to Password Policy than you think!

- Use intelligent password policy
  - Most password policy is based on dogma, and some is counter-productive
  - How many users have written down their password in plaintext (on a Post-it even!)
  - How many people store sensitive information (passwords) in un-encrypted documents (*.docx, *.xlsx)
  - How often are passwords shared by users on your Organization ("Hey, Bob, login as me with the password 1234Mainstreet#!")



# NIST Digital Identity Guidelines (Publication 800-63B)

## The DO’s

- DO allow use of passphrases
- DO allow the use of cut & paste for passwords
- DO favor users, not administrators
- DO enforce password length
- DO create a banned-list and compare passwords to known-bad passwords
- DO enforce timeout for inactivity
- DO allow users to see their passwords in plain text

## The DO NOT’s

- DO NOT require numbers, special characters or enforce composition rules
- DO NOT use hints or questions
- DO NOT enforce password aging

# Deploy two-factor Authentication (2FA)

- 2FA helps to make sure only authorized users access sensitive data
  - The addition of phone, SMS, or other second-factor drastically reduces the possibility of unauthorized access
- 2FA is the standard in improving security

# File Sharing

Needs to be usable and secure

- Windows file servers should be permissions-based
  - Each user entitles to only certain files based on Active Directory
- Consider deploying true VDI Desktops for users
  - Avoid users leveraging Public Cloud services or email to transfer files from ‘work” to personal computer resources
- Users data MUST be readily available or users will circumvent normal security procedures with USB Drives, email or Public Cloud file sharing

# VMsources MSP and Consulting

What VMsources can do for your Organization

- VMsources can assist in the deployment and adoption of 2FA for your Organization
- VMsources can assist with updating Active Directory Password and Security Policy
  - NIST Recommendations based on Special Publication 800-63B
  - Group Policy and Security Policy to inhibit Ransomware
- VMsources can help to deploy and validate permissions-based file-shares and file sharing
- VMsources can deploy secure Linux-based filesharing services

# Network

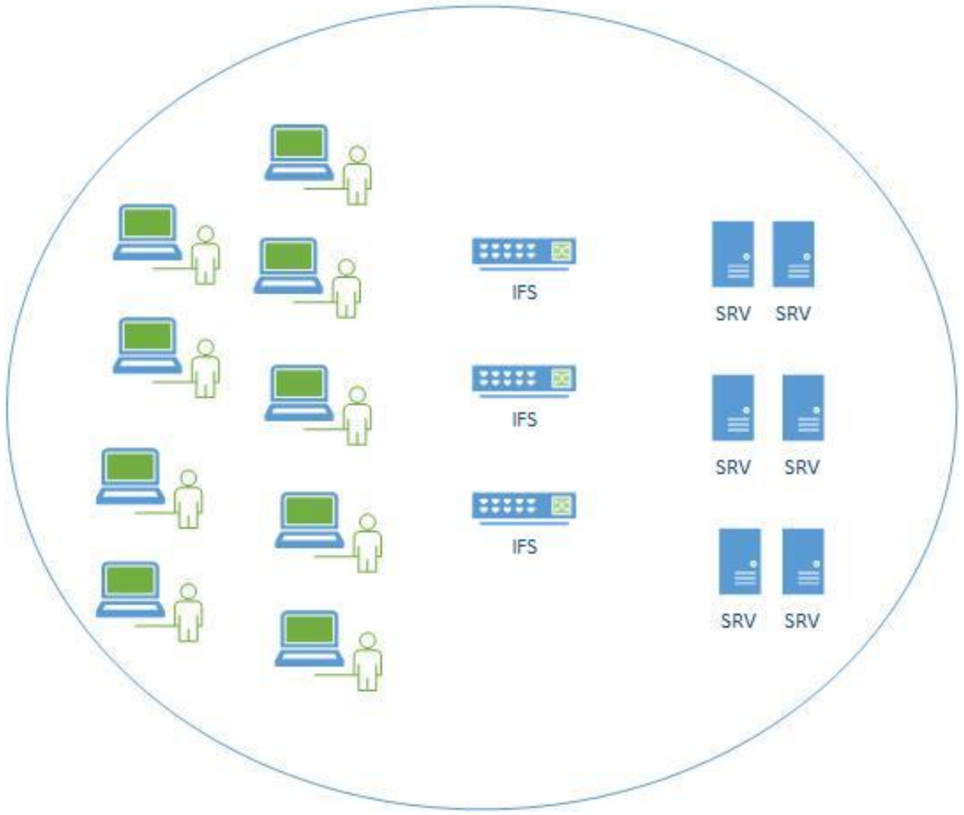
Network segmentation and firewalling means Security

# Understanding a Broadcast Domain

Lack of Network Segmentation often gives Ransomware the foothold it needs

- ○ Broadcast Domains are unrelated to Active Directory
- ○ People often use the terms: “Network,” “Subnet,” “VLAN” interchangeably to refer to the concept of Broadcast Domain
- ○ Refer to a contiguous Network Segment where all hosts can “talk” to each other without restriction
- ○ Within a Broadcast Domain, Malware, Ransomware and Exploits can spread easily
  - Workstations WKS
  - Servers SRV
    - AD, Mail (Exchange), SQL, Terminal Server, Citrix
  - Infrastructure IFS
    - VMware, Backup, Edge (L3)

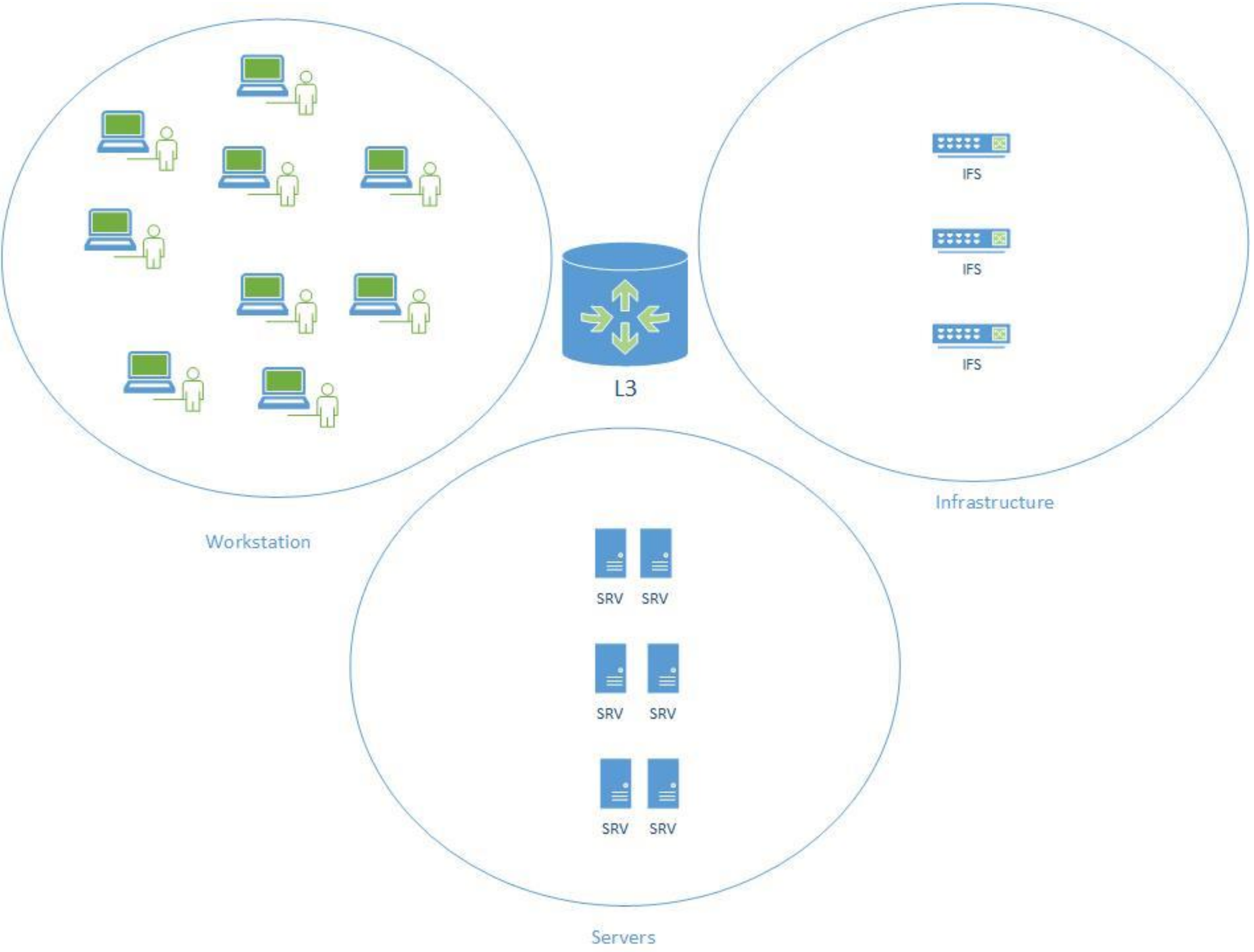
Broadcast Domain



# Network Segmentation

Network Segmentation alone is a huge step forward

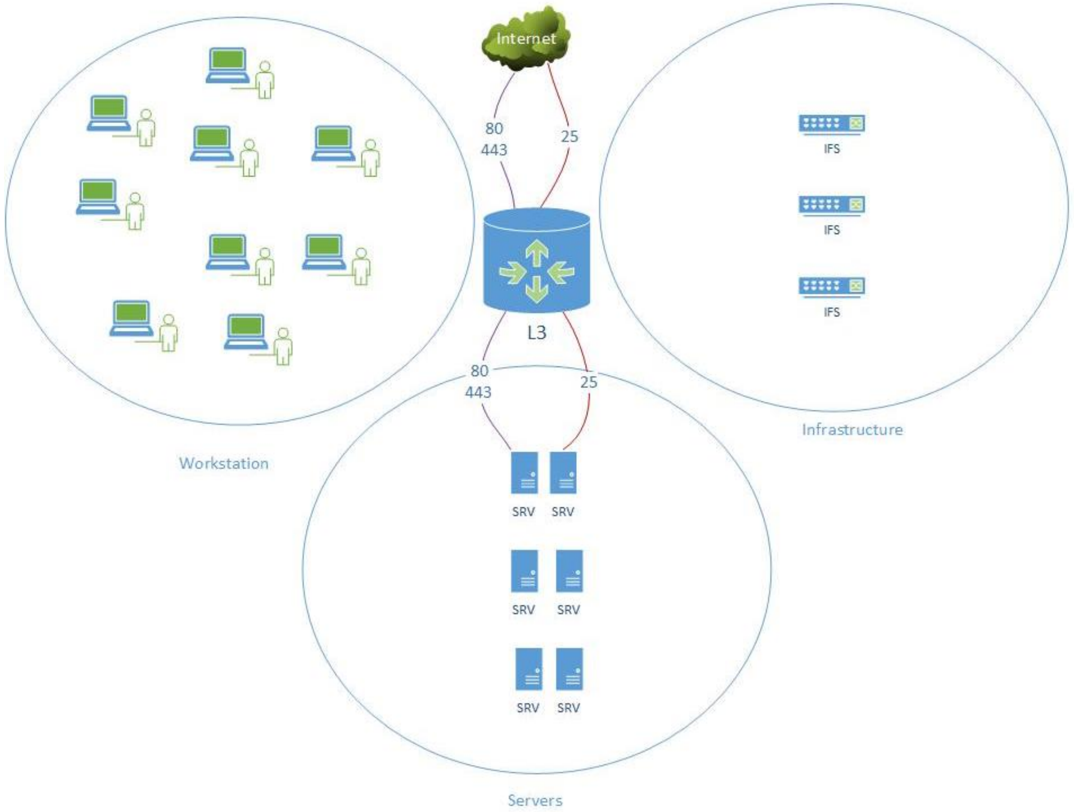
- Network segmentation means moving different categories of system to unique Broadcast Domains
  - Workstation Network
  - Server Network
  - Infrastructure Network
- Communication (AKA: “traffic”) can not pass between different Broadcast Domains unless passing a Firewall
- Routers/Firewalls (L3) inspect traffic and permit or deny based on factors such as:
  - Source/Destination
  - Application (Email, SQL, Web)



# Port Forwarding (NAT) can be dangerous

Firewalls and Routers can only do so much for security without a DMZ

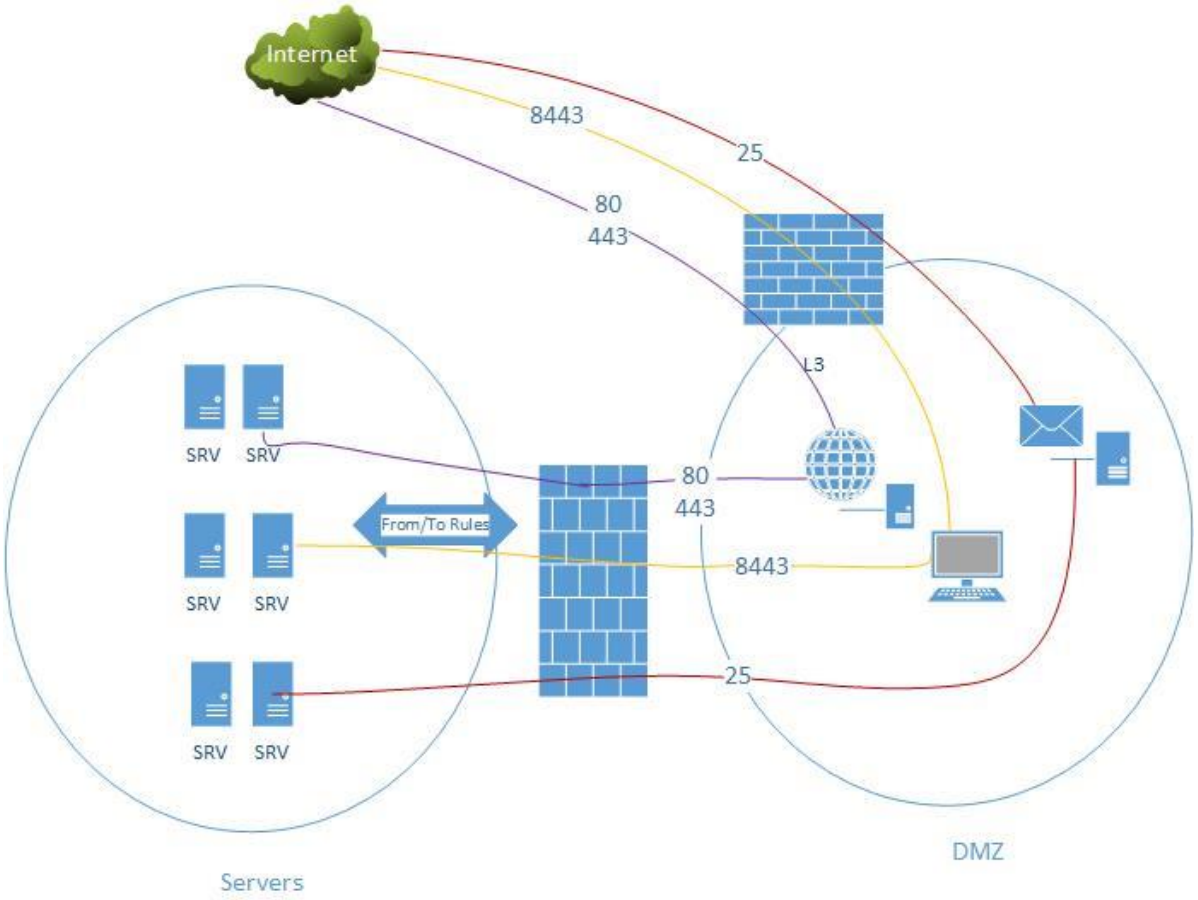
- Applications announce what they are supposed to be using “Ports”
- Port Forwarding is directing certain types of traffic such as Web or Email to the correct Server
- Hackers are able to announce incorrect Ports to introduce exploits
- Port Forwarding from the Internet to any general-purpose Broadcast Domain is a bad idea
  - Remote-code execution vulnerabilities could allow hackers to reach any other system within the Broadcast Domain



# True DMZ

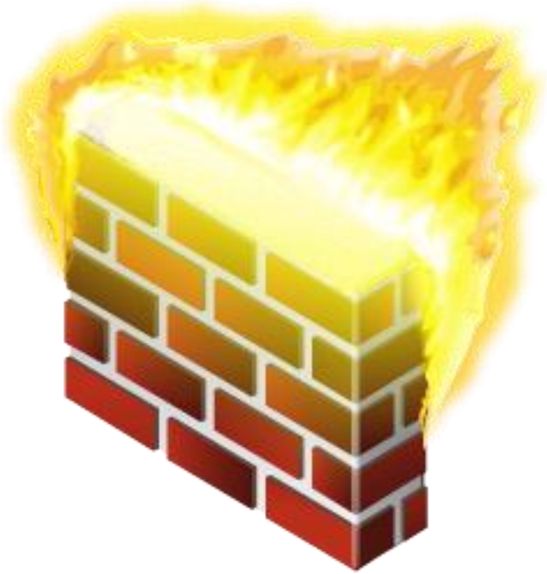
Network Segmentation with a true DMZ is the best network policy to prevent propagation of Ransomware

- A true DMZ (Demilitarized Zone) is a dedicated Broadcast Domain containing Internet-facing servers and/or dedicated proxy-servers
  - Web servers often exist entirely in a DMZ
  - Mail servers (such as Exchange) often place an Internet-facing proxy in the DMZ
  - Virtual Desktop Infrastructure (VDI) should have a Secure Gateway server in the DMZ
- DMZ entities should NOT be a member of Active Directory



# Stateful Firewall with active ruleset

- Geo-IP Blocking
  - Block countries or entire continents which are not relevant to your Organizations
- Domain Name Service (DNS) Blocking
  - Active DNS Blocklists prevent users from going to known bad addresses
- Content Filtering
  - Limit or prevent traffic based on content type as appropriate for your Organizations
- Secure Delivery
  - Prevent access to addresses which do not have HTTPS/SSL secured by a Trusted Certificate Authority (CA)



# VMsources MSP and Consulting

What VMsources can do for your Organization

- VMsources can help create VLANs and then implement Network Segmentation with unique Broadcast Domains for:
    - Desktops
    - Servers
    - Infrastructure
- VMsources can help move Web-facing servers into a true DMZ and/or create secure non-AD proxy Servers
- VMsources can help to remove critical IT Infrastructure (such as: Backup Servers, VMware and Hyper-V) from the main AD domain
- VMsources can help deploy Virtual Firewall technology to implement active protection and Geo-IP blocking

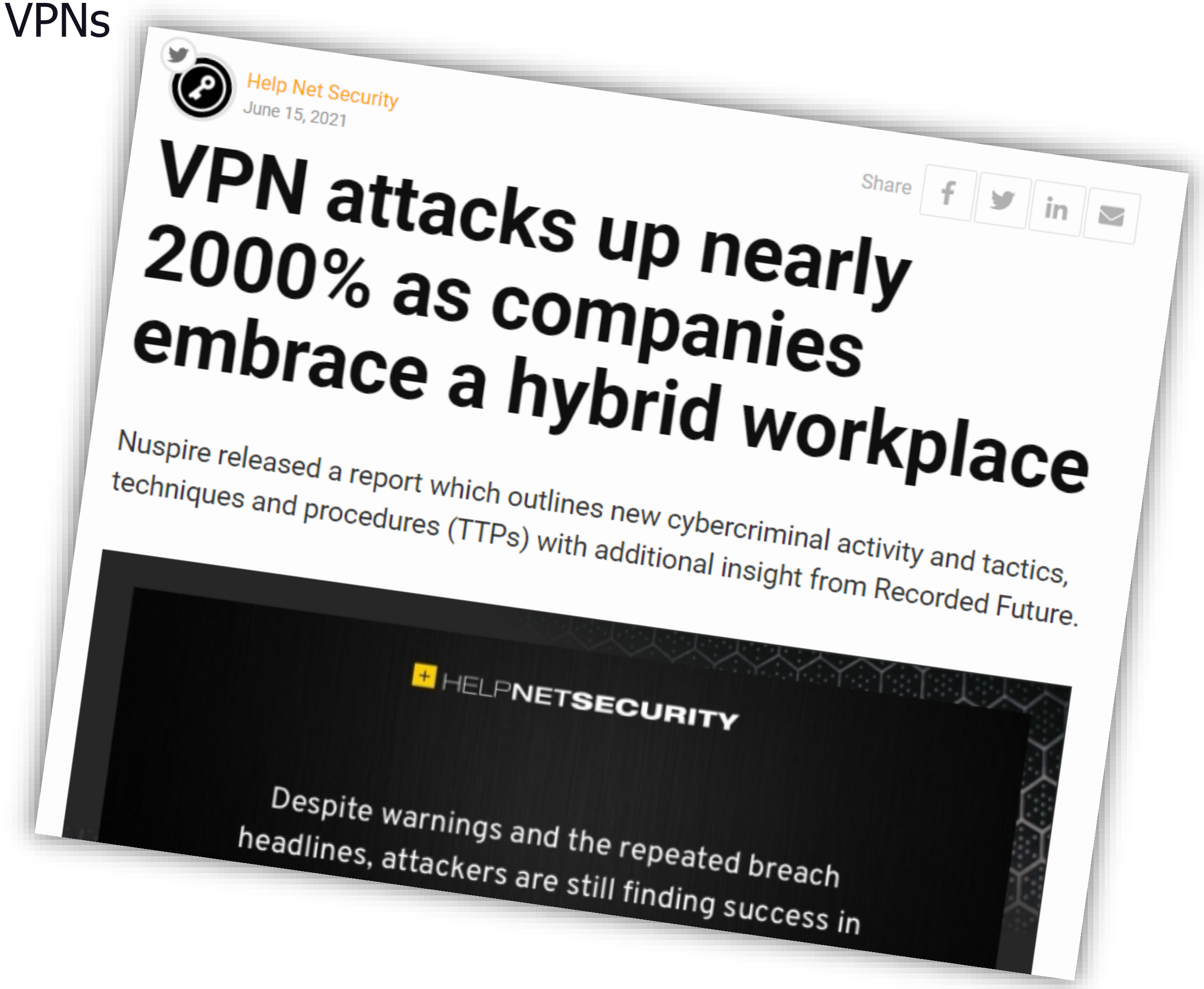
# Desktop

How your users access Organizational data is significant

# VPNs can be a problem

Recent headline news was the result of compromised VPNs

- What you can do:
  - Don’t use VPNs for user connectivity
  - If you must use VPNs for users, use 2FA
  - Increase the strength of the “secrets” or keys used by the VPN
  - Use open VPN technology



Help Net Security
June 15, 2021

Share

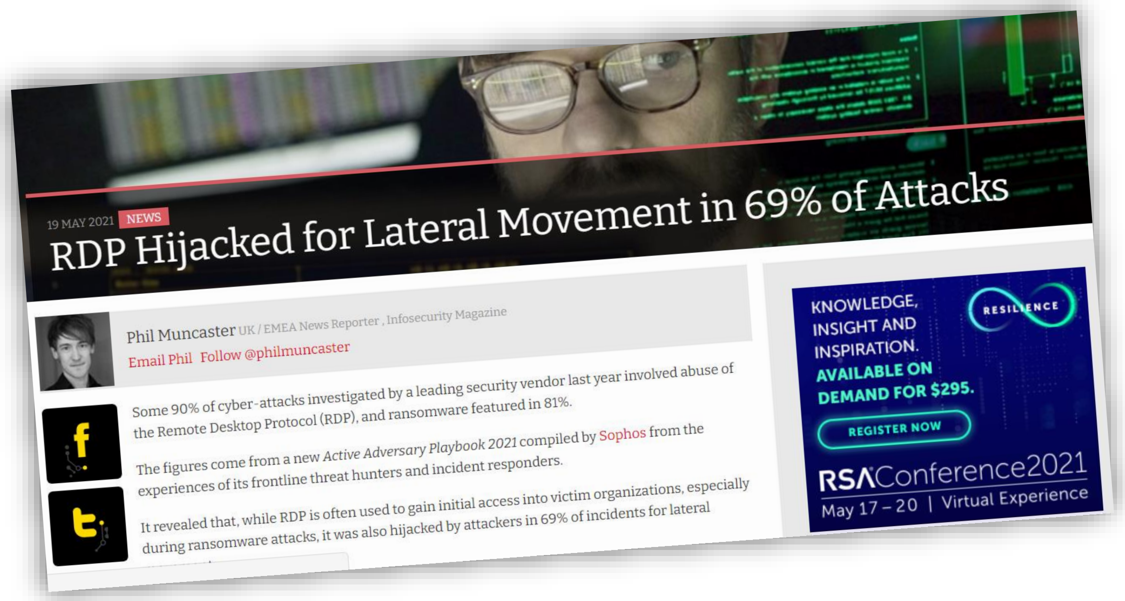
## VPN attacks up nearly 2000% as companies embrace a hybrid workplace

Nuspire released a report which outlines new cybercriminal activity and tactics, techniques and procedures (TTPs) with additional insight from Recorded Future.

Despite warnings and the repeated breach headlines, attackers are still finding success in

# Microsoft Remote Desktop (RDP) is not secure

- Microsoft RDP should never be exposed directly to the internet
- Numerous known vulnerabilities including CVE-2019-0708
- RDP over VPN is not the solution either



19 MAY 2021 NEWS

RDP Hijacked for Lateral Movement in 69% of Attacks

Phil Muncaster UK / EMEA News Reporter , Infosecurity Magazine

Email Phil Follow @philmuncaster

Some 90% of cyber-attacks investigated by a leading security vendor last year involved abuse of the Remote Desktop Protocol (RDP), and ransomware featured in 81%.

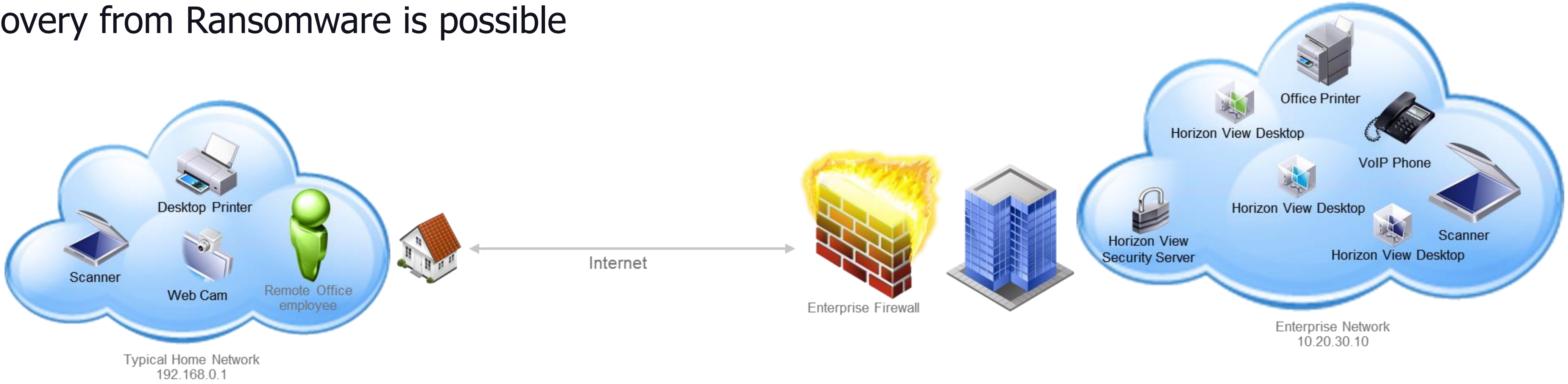
The figures come from a new *Active Adversary Playbook 2021* compiled by Sophos from the experiences of its frontline threat hunters and incident responders.

It revealed that, while RDP is often used to gain initial access into victim organizations, especially during ransomware attacks, it was also hijacked by attackers in 69% of incidents for lateral

# Virtual Desktops (VDI) keeps everything in-house

There’s no VPN required and all desktops are delivered through a Secure Gateway

- Users connect to a Virtual Desktop behind the Organizational Firewall
- No VPN Required
- The Organization controls the data
- Backups are applied by policy
- Recovery from Ransomware is possible



# Endpoint Protection

Look for suspicious behaviors and known payloads

- Best-of-breed Endpoint Protection is part of any security plan
- Are Antivirus and Endpoint Protection the same?
  - NO: Antivirus blocks known payloads whereas Endpoint Protection looks for suspicious behaviors as well
- Effective Endpoint Protection is difficult on physical desktops and almost impossible on remote laptops

# VMsources MSP and Consulting

What VMsources can do for your company

- VMsources can help deploy Virtual Desktop Infrastructure
- We work with several great Endpoint Protection Platforms
- We can help get users off those dangerous VPN Tunnels
- We can secure required VPN tunnels with strong passwords, keys or 2FA

# Remediation

Addressing Business Continuity when bad things happen (and they will happen)

# Things are going to happen

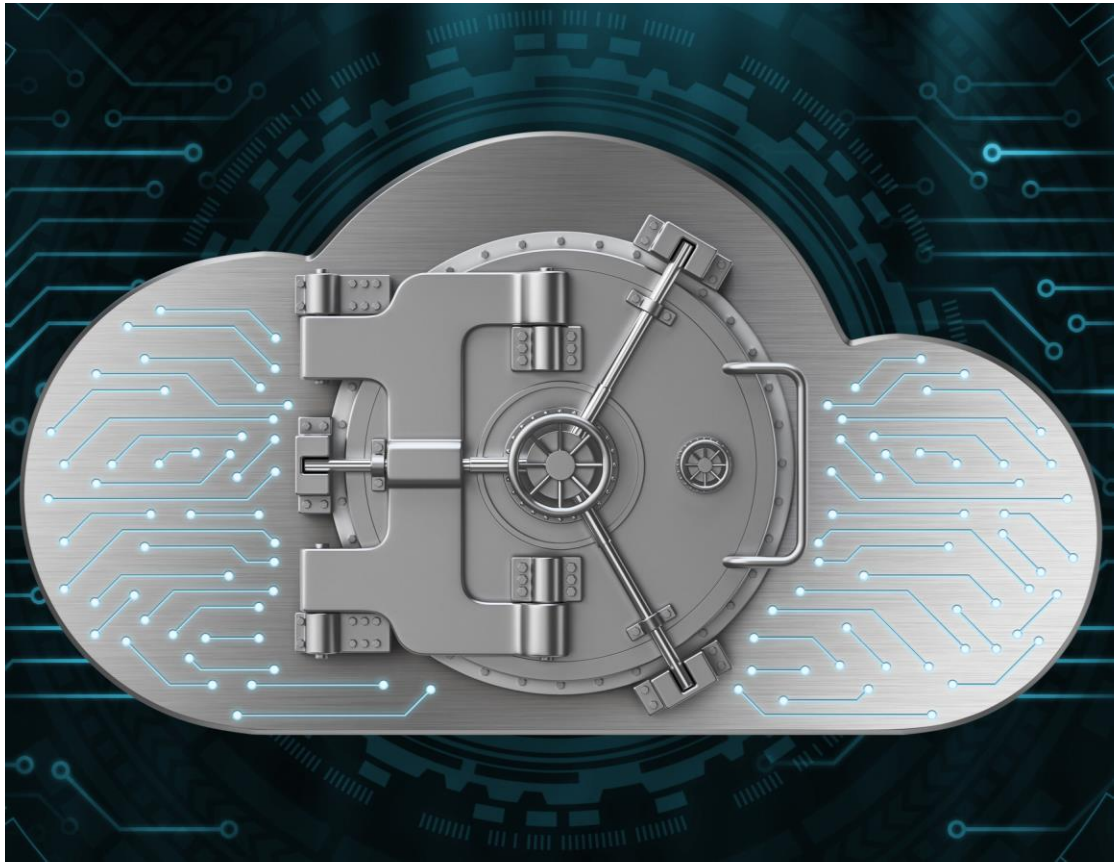
Don’t let your Organization be the next headline news

- No matter what you do, something is likely to slip through the cracks.
- Being able to failover to a DRaaS facility or recover quickly from backups is the threshold by which you will be judged.
- Set the standards in advance, there’s no such thing as a zero-downtime event!
  - The media has taught us that outages of days and huge ransom payments are the NORM!
  - **Be the hero if you can be fully online in 24 hours or less without paying ransom.**
- Common Thresholds:
  - Organizations with DRaaS can expect to failover fully in about 4 hours
  - Organizations protected by Immutable Backups can expect to recover over a period of about 24 hours
- SUCCESS = Rapid failover and/or recovery
- FAILURE = Extended disruption, loss of data, exfiltration, and paying ransom

# Hardened Backups

Existing Backup systems can improve

- ○ A huge problem is Organizations which join Backup Servers and VMware vSphere servers to the AD Domain
  - This effectively allows Ransomware to encrypt the backup files and VMs directly!
- ○ Here are some recommendations:
  - GOOD: Do NOT join your Backup Server or Repository to AD Domain
  - BETTER: Follow 3-2-1 Rule
  - BEST: Combine the two suggestions above with or Immutable Backup technology



# Disaster Recovery as a Service (DRaaS)

DRaaS is the way when rapid recovery is the goal

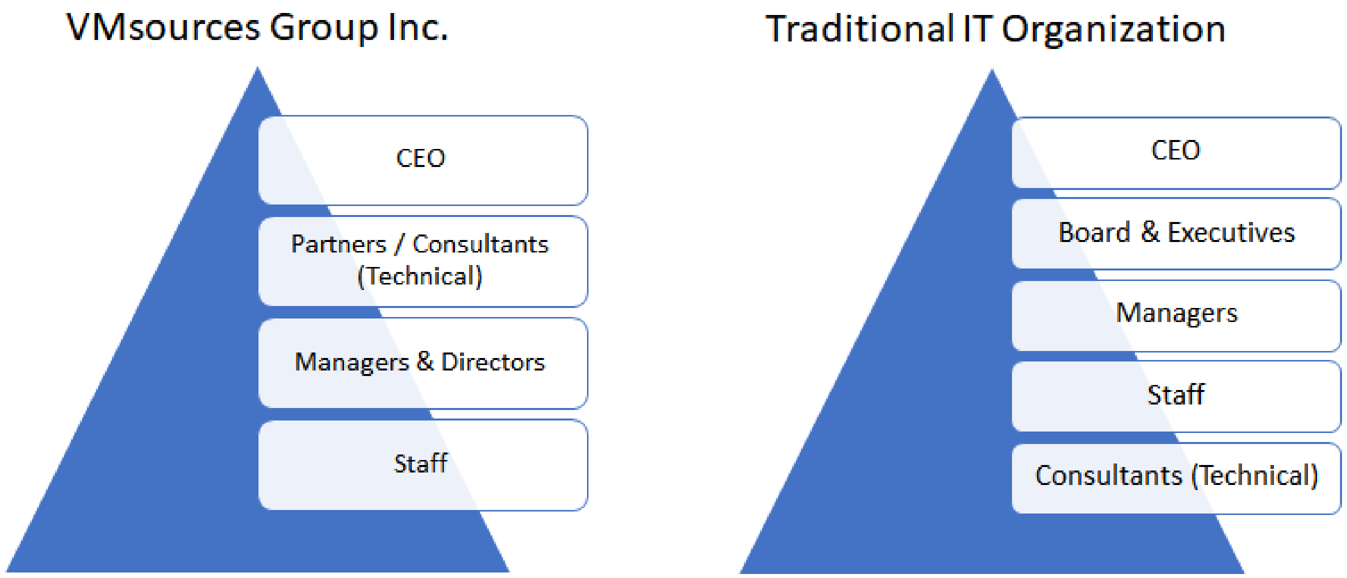
- ○ Deploy an effective Disaster Recovery plan
  - DR or DRaaS should address both physical disasters and logical ones
    - DRaaS maintains a current copy (Replica) of all mission-critical systems at a DR site
    - Understand how far back a replica can be restored (in case of ransomware)
- ○ Test that plan to understand the implications
  - Public IP addresses, DNS, Active Directory and more can all present unanticipated challenges
- ○ Understand the costs of testing and failover
  - Some providers charge exorbitant prices for running any form of failover including testing

# VMsources MSP and Consulting

What VMsources can do for your Organization

- VMsources knows and understands Backups and DRaaS better than anyone else.
- We'll build a white-glove DRaaS plan specifically for your Organization.
  - We're happy to respond to RFPs through normal purchasing channels as well.
- We can assist your Organization with hardening existing technologies.
- We can deploy Veeam Immutable Repositories at your location or in our Cloud to protect against Ransomware.
- We'll help you write an IT Business Continuity Plan that will:
  - Establish realistic expectation for events and recovery
  - Spell out "Who's on first" by diagraming every component of the Backup and/or DRaaS systems and what it does.
  - Provide easy-to-follow flowcharts

VMSOURCES
Cloud & Infrastructure



VMsources Group Inc.

CEO

Partners / Consultants (Technical)

Managers & Directors

Staff

Traditional IT Organization

CEO

Board & Executives

Managers

Staff

Consultants (Technical)

# Simplicity is elegance

VMsources is a customer-facing MSP specializing in Private Cloud, Infrastructure, and Network.

It is VMsources mission to act as the client's advocate at every stage of the project, from concept to completion.

# About Us

We are proud to bring the best technical guidance to the top of a traditional organizational structure.

## VMsources Group Inc.

👤 John Borhek

📱 +1 215 764 6442 X1001

✉ john@vmsources.com

🌐 https://vmsources.com/