AGENCY WORKFORCE MANAGEMENT

Ransomware: 6 Tips to Protect Your Agency

Today's Presenter

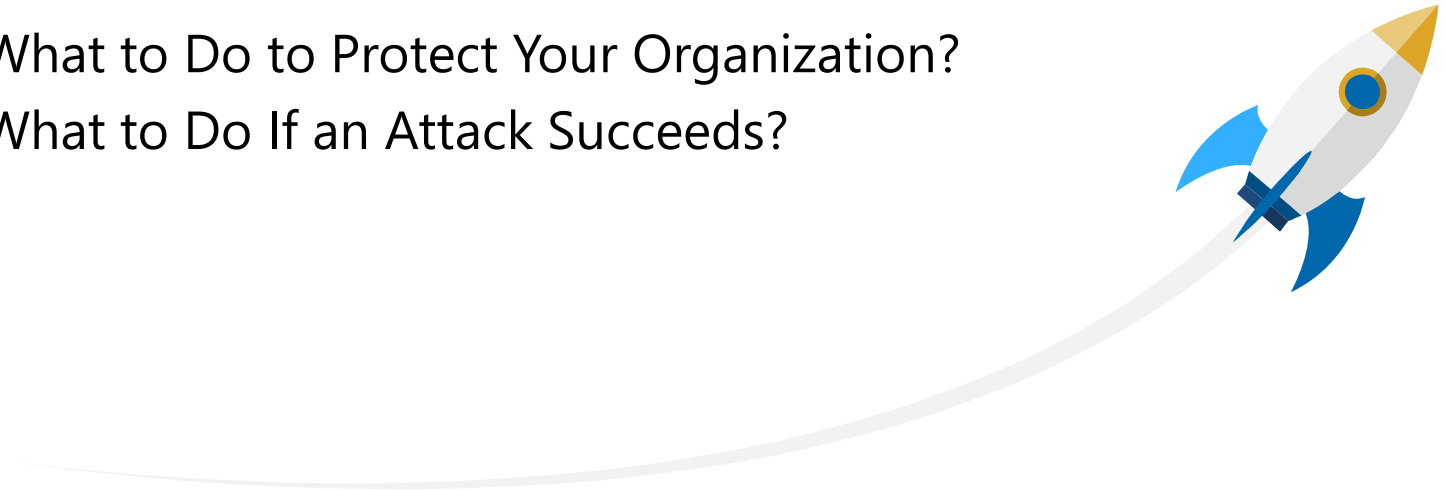
Joe Cornaglia

Director of Agency Solutions

Joe is the Director of Agency Solutions and works among the Business Development, Agency Consultants, and Marketing teams to help agencies learn more about the benefits of Agency Workforce Management. Joe holds a Bachelor's degree in Business Administration/Marketing from Drexel University in Philadelphia, Pennsylvania.

Agenda

- What Are Ransomware Attacks?
- What to Do to Protect Your Organization?
- What to Do If an Attack Succeeds?



AGENCY WORKFORCE MANAGEMENT

Agency Workforce Management

About MITC, What We Do, Who We Serve

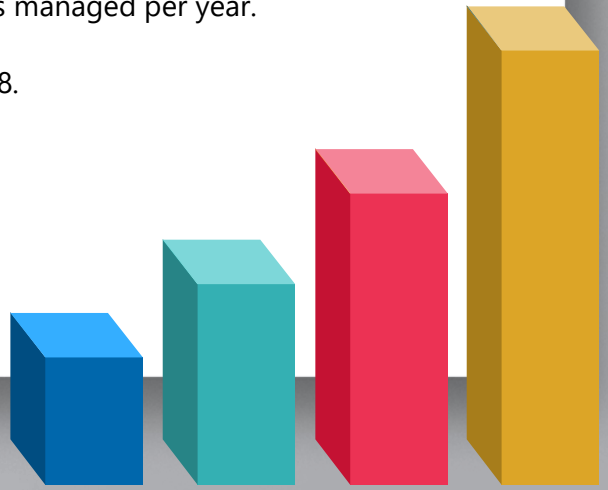
Hundreds of Agencies Use Agency Workforce Management

- MITC has provided 28 years of continuous service to customers in every state in the USA, Canada, the United Kingdom, New Zealand, & Australia.
- Agency Workforce Management is used by I/DD and Behavioral Health agencies.
- Thousands of employees and managers use Agency Workforce Management every day.

AGENCY WORKFORCE MANAGEMENT

2018 Facts & Figures

- **145,680:** Number of employees & clients managed by customers using MITC.
- **26,763,600:** Number of telephone timekeeping calls managed per year.
- **73,955,516:** Number of time and attendance transactions managed per year.
- **53,922,480:** Number of timecard pre-payroll & billing records managed per year.
- **145:** Number of new implementations in progress at the end of 2018.
- **15,684:** Number of service requests received in 2018.



AGENCY WORKFORCE MANAGEMENT

Providers Throughout the USA and Canada Use Agency Workforce Management

Available as an Integrated Solution or to Solve Discrete Problems

myCLIENTS

mySCHEDULES

myATTENDANCE

myTRAINING

myCHECKIN

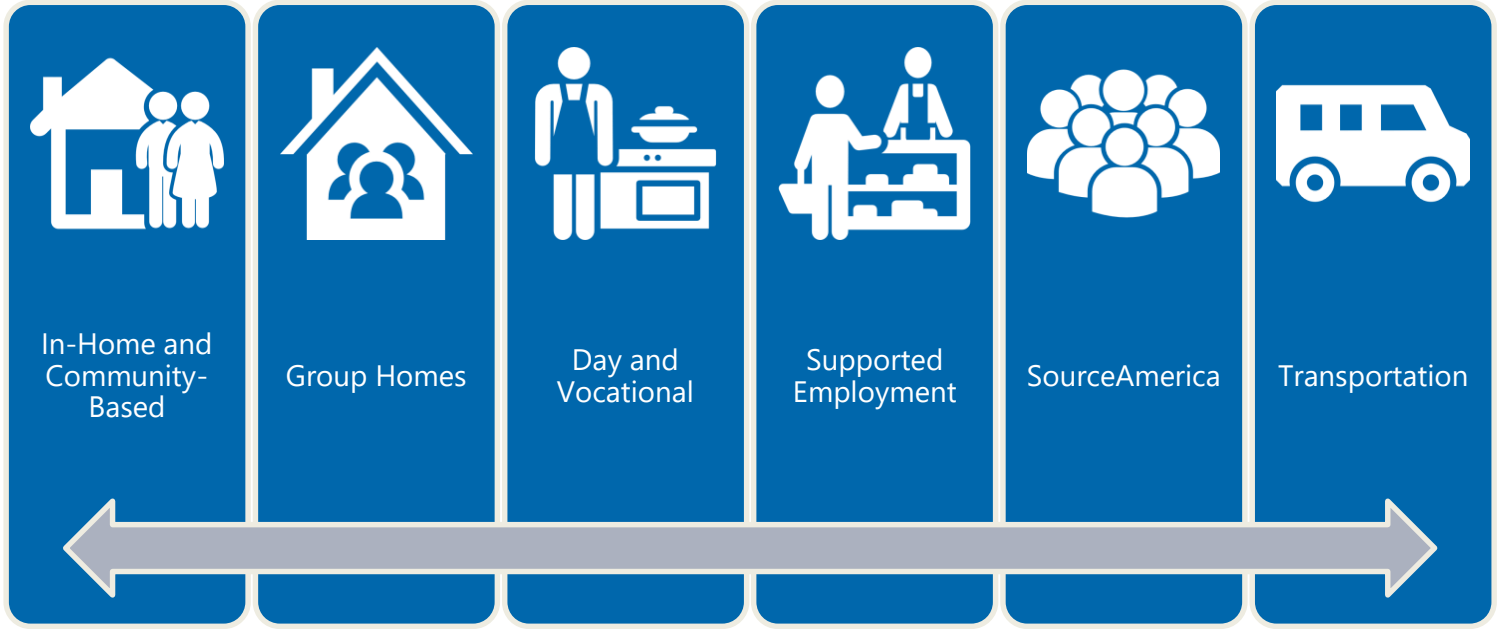
myCOMMUNICATIONS

mySAFETYMANAGER

myAPPLICANTS

AGENCY WORKFORCE MANAGEMENT

Agency Workforce Management Is Used in All Programs



AGENCY WORKFORCE MANAGEMENT

Unlike general purpose systems, MITC provides a complete solution and services to support all the needs of an agency.

Agency Workforce Management Solutions for Staff & Clients

Staff Solutions

- Time & Attendance
- Scheduling
- HR Manager
- Payroll Integration
- Applicant Tracking
- Mileage & Expenses

Client Solutions

- Door Clock
- Client Timesheets
- Piece & Production
- Scheduling
- Billing
- Documentation

AGENCY WORKFORCE MANAGEMENT

Flexible and Modular Solutions Make Up Agency Workforce Management

- Solutions are modular and scalable
- Different hardware and software
- Choose a customer-hosted or a cloud solution

What Makes Agency Workforce Management Different?

- Continuous stream of software updates and services designed for agencies.
- Specially trained personnel to help agencies successfully implement solutions.
- Structured implementation plans have been proven at hundreds of agencies.
- Choose from customer-hosted or cloud solutions.
- Software, services, and implementation plans are all designed for agencies.
- Agency Workforce Management includes 24x365 service.

AGENCY WORKFORCE MANAGEMENT

AGENCY WORKFORCE MANAGEMENT

What Are Ransomware Attacks?

What Are Ransomware Attacks?

- Ransomware is conducted by criminals who have little chance currently of being apprehended. Usually they operate out of states without a regulatory environment

Ransomware attack danger

- Ransomware is the fastest growing malware threat, targeting users of all types—from the home user to the corporate network
- Ransomware targets home users, businesses, and government networks and can lead to temporary or permanent loss of sensitive or proprietary information, disruption to regular operations, financial losses incurred to restore systems and files, and potential harm to an organization's reputation such as HIPAA violations

SMO focus

- Small-to-medium sized organizations (SMOs) with their own in-house computer networks are targeted by ransomware criminals as SMO's typically have weaker IT defenses

Encryption

- Ransomware is a form of malware that targets your critical data and systems for the purpose of extortion by using encryption
- After the user has been locked out of the data or system, the cyber actor demands a ransom payment
- After receiving payment, the cyber actor will purportedly provide an avenue to the victim to regain access to the system or data

How ransomware works

- Attacker gains access to your server
- Cracks the administrator password
- Locks or encrypts key data on server
- Reaches out to any PC's switched on
- Locks or encrypts key data on PC, laptops etc
- Messages to send money

Cloud

- Ransomware attacks are one of the main reasons so many organizations are moving their key applications to the Cloud

City government attacked

- Wednesday, May 22nd 2019: The Wall Street Journal reported 10,000 government computers have been frozen for two weeks

- Baltimore, MD - May 2019: Ransomeware attack on systems

Providers attacked

- 2018: An agency in Ohio reported a major ransomware attack that had a major impact on operations and caused significant unbudgeted IT costs. Over 50 computers were effected
- August 2019: two agencies in Louisiana suffered an attack
- August 2018: Large agency in Maryland attacked

Local government attacked

- A Florida city is paying $600,000 in Bitcoins to a hacker who took over local government computers after an employee clicked on a malicious email link three weeks ago.
- Riviera Beach officials voted to pay 65 Bitcoins to the hacker who seized the city's computer systems, forcing the local police and fire departments to write down the hundreds of daily 911 calls on paper. The 65 Bitcoins, equals $600,000. Once the payment is made, they hope to get access to data encrypted by the hacker!

ISP attacked

- May 2019: A small internet service provider used by many organizations in Hagerstown, Maryland was attacked
- No internet service was available for a week

Ransomware attacks can expose HIPAA protected data

- If the databases on your server(s) contain Protected Health Information, HIPAA violations could occur

Microsoft RDP used

- Recent ransomware attacks have high-lighted the vulnerability to organizations from using Remote Desktop Protocol. RDP is commonly used by IT companies working remotely on your IT or employees working from home
- Security researchers at Check Point identified a sweeping array of vulnerabilities in Remote Desktop Protocol (RDP) clients for Windows, Linux and Mac.
- RDP is designed for remote access on a local area network (LAN). Establishing remote desktop connections to computers on remote networks may require VPN tunneling, port-forwarding, and firewall configurations that compromise security - such as opening the default listening port, TCP 3389.

What to Do to Protect Your Organization?

Proactive Prevention is the Best Defense

- Prevention is the most effective defense against ransomware
- It is critical to take precautions for protection
- Infections can be devastating to an individual or organization, and recovery may be a difficult process requiring the services of a reputable data recovery specialist.

Consider the Cloud

- Professional data centers or software providers offering Cloud solutions, can afford much more stringent controls than individual organizations
- Share the cost!

Business Continuity Considerations

- Back up data regularly (daily). Verify the integrity of those backups and test the restoration process to ensure it is working
- Conduct penetration tests and vulnerability assessment.
- Secure your backups. **Ensure backups are not connected permanently to the computers and networks they are backing up.** Examples are securing backups in the cloud or physically storing backups offline.
- Some instances of ransomware have the capability to lock cloud-based backups when systems continuously back up in real time, also known as persistent synchronization.
- Backups are critical in ransomware recovery and response; if you are infected, a backup may be the best way to recover your critical data.

Backup “Do Not”s

- Do not backup to another internal drive
- Do not back up to a connected computer
- Do not use Cloud backup without disconnecting when complete
- Use external drives. Remove from the server after the back up is complete
- Locate backups offsite
- Maintain a daily backup (5 or 7) rotation
- Maintain a weekly offsite backup rotation (3)
- Never use the same backup device sequentially

RDP

- Consider disabling Remote Desktop protocol (RDP)

Staff training

- Implement an awareness and training program.
- Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Mandate staff to turn off computers when not in use, particularly at night and over weekends

Email

- Consider using an internal communication system like myCommunications for internal use
- “Closed” messaging systems cannot receive messages from outside
- Avoid “free” email services like Gmail, AOL etc. with weak protection

IT

- Configure firewalls to block access to known malicious IP addresses
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system
- Set anti-virus and anti-malware programs to conduct regular scans automatically

Administrator Rights

- Manage the use of privileged accounts based on the principle of least privilege
- No users should be assigned administrative access unless absolutely needed
- Those with a need for administrator accounts should only use them when necessary

Insurance

- Consider cyber insurance
- These policies are getting more expensive with the growing number of attacks
- $1,000,000 coverage is needed for an organization with 100 devices

What to Do If an Attack Succeeds?

Isolation

- Isolate the infected computer(s) immediately
- Infected systems should be removed from the network as soon as possible to prevent ransomware from attacking networked or share drives.

Power Off

- Power-off affected devices that have not yet been completely corrupted. This may afford more time to clean and recover data, contain damage, and prevent worsening conditions.

Secure backups

- Hopefully backups will have been removed daily from physical contact with the server
- Immediately secure the backup data or systems by taking them offline
- Ensure backups are free of malware.

Passwords

- **Change all online account passwords and network passwords after removing the system from the network.** Furthermore, change all system passwords once the malware is removed from the system

Forensic specialist

- It may be necessary to call in forensic IT specialists to “clean” infected computers, re-install operating systems and application software
- This process can take several days, assuming the right resources are immediately available

HIPAA

- Verify if Protected Health Information was exposed
- Follow HIPAA notification rules if PHI was exposed

Implement your security incident response and business continuity plan

- Ideally, organizations will have ensured they have appropriate backups
- Their response to an attack will be to restore the data from a known clean backup. Having a data backup can eliminate the need to pay a ransom to recover data.

Law enforcement

- Any entity infected with ransomware should contact law enforcement. Law enforcement may be able to use legal authorities and tools that are unavailable to most organizations. Law enforcement can enlist the assistance of international law enforcement partners to locate the stolen or encrypted data or identify the perpetrator. These tools and relationships can greatly increase the odds of successfully apprehending the criminal, thereby preventing future losses.

AGENCY WORKFORCE MANAGEMENT

Contact Us Today!
301-228-2105
info@mitcsoftware.com

Thank You!

With over 28 years of experience, MITC is here to help. Use our expertise, developed from working with hundreds of agencies to help you select the system you need!