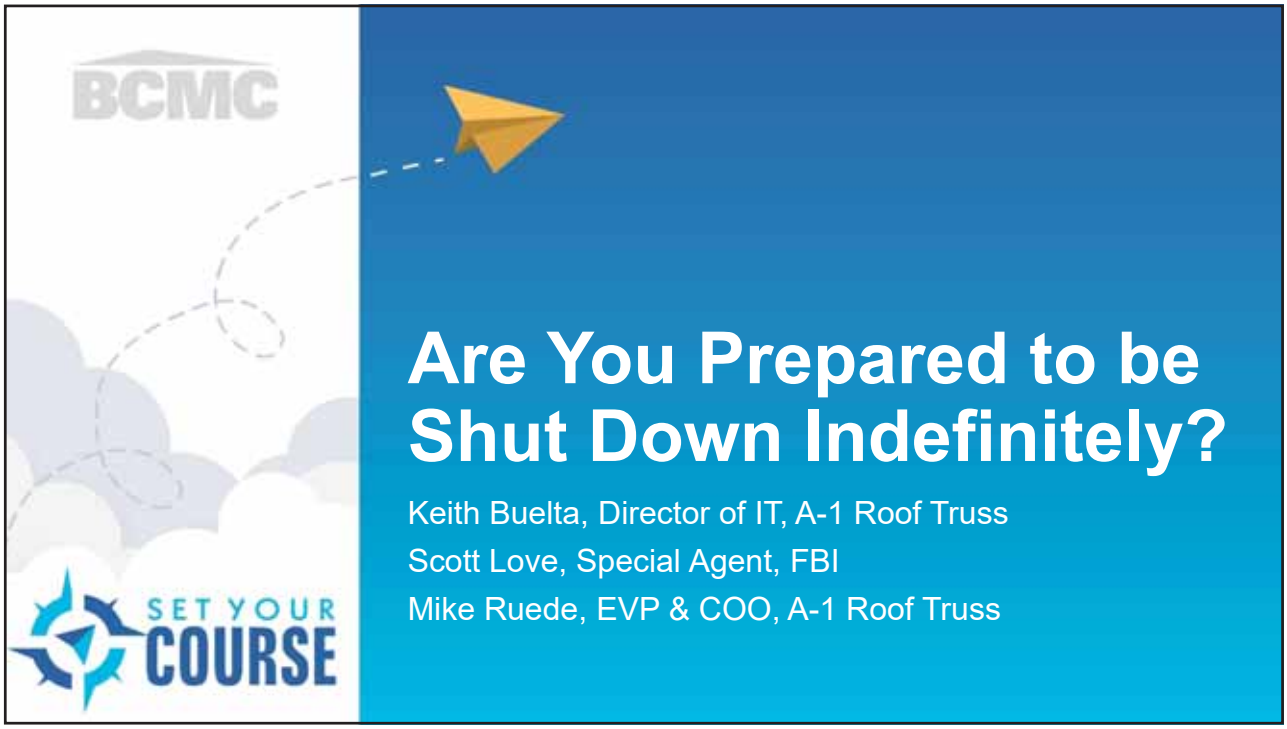
Are You Prepared to Be Shut Down Indefinitely?

Mike Ruede, A-1 Roof Trusses
Keith Buelta, A-1 Roof Trusses
Federal Bureau of Investigation Expert

MiTek®

Handout Sponsor



Summary

- Company infrastructure
- What happened
- Company response
- Company changes
- Costs

BCMC

A-1 Roof Truss

- Opened in 1977 in West Palm Beach, Florida
- Mission
  - Champion an environment of teamwork dedicated to our customers with exceptional workmanship, service and integrity. We are committed to being the premier truss supplier in southeastern United States.
- Vision
  - To be the preferred trade partner for all builders in the southeastern United States.

BCMC

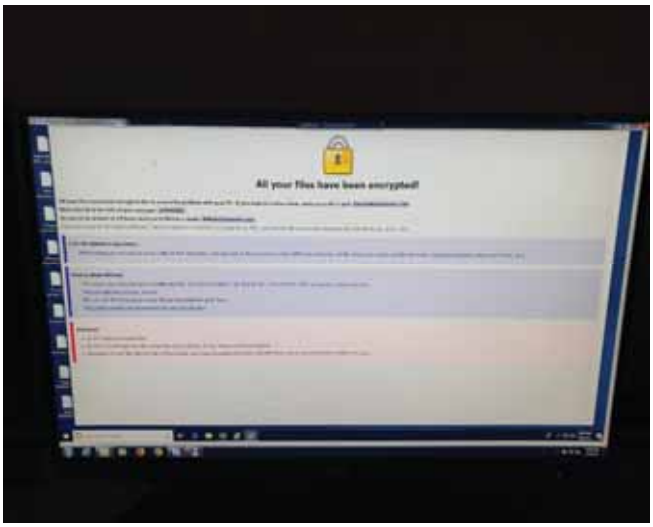
Company Infrastructure

- Firewall with global IP blocking
- Anti-virus on servers and workstations
- Terminal server: port 3389 open
- Local backup: external hard drive swapped out bi-weekly
- Local exchange server

BCMC

What Happened

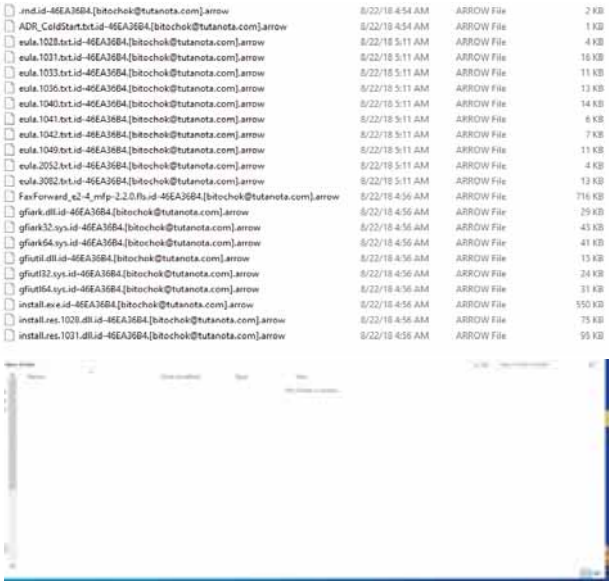
- Owner was out of country needed access to email
- Firewalls global IP blocking disabled to give access to email
- Tuesday 3:00 am attack occurred
- Criminals gained access using open port 3389 and delivered the “payload”



BCMC

What Happened

- Over 5 million files encrypted
- Virus ran for 4 hours uninterrupted
- 5 servers and 19 workstations were destroyed
- All local backups were deleted
- 6:00 am - first contact with virus



BCMC

What We Did

- Identified the “payload” as the virus and shut it down
- Closed all open ports to network from outside
- Unplugged switches to ensure virus was not spreading
- Outsourced a company and began decrypting files after identifying that backups no longer existed
- Manually updated the registry of every device that was on the network to prevent the virus from spreading (over 150)

BCMC

What We Did

- Upgraded and ran virus scans on all network devices before putting them back on the network
- Migrated email to Office 365 and began the restore process from old profiles
- Initiated full company backup after decryption to ensure we had a solid backup before going back online
- Started cutting and building trusses on Monday at 10:00 am

BCMC

What Has Changed - Software

- Anti-virus
- Local admin removal
- Changed backup software
- Changed backup schedule: every 3 hours, local, and offsite
- End user training: KnowB4
- Monthly phishing testing

BCMC

What Has Changed - Software

- Quarterly archiving of old files
- Updated password policies
- Moved website offsite
- Cloud-based ticketing system
- Established encrypted remote access connections for remote users

BCMC

What Has Changed - Hardware

- Firewall
- Segment network
- Virtualize servers: VMware
- Imaged production computers
- Changed backup location: offsite
- Moved cameras offsite

BCMC

Line Item Costs to the Company

Down for 6 days	
Foregone gross profit on lost revenue:	$800,000
Wages lost:	$202,000
Cost of repairing and rebuilding:	$177,000
Cost of new firewall:	$8,000
Firewall and attack monitoring service:	$106,800
New backup software:	$5,000
Costs to update remote access software:	$2,000

BCMC

Total Cost to the Company

$1,300,800

BCMC

Final Thoughts

- You are a target
- User training is key
- Be prepared (have a plan)
- Continually test the plan

BCMC

Questions?

- Keith Buelta
  - Email: keith.buelta@a1truss.com
- Mike Ruede
  - Email: mike.ruede@a1truss.com

BCMC

SBCA Resources

- For more resources on this topic, visit www.sbcindustry.com and search for the below titles:
  - Cybersecurity Topical Library
  - Learning from the Sometimes Painful Experiences of Others
  - Cybersecurity & Disaster Recovery Worksheet
  - A Potential (but Preventable) Risk
  - Who's Handling Your Technology in an Increasingly Information-driven Industry?

BCMC

Learning Labs

Thursday

- 12 pm – Knowing Your People to Keep Your People
- 1:30 pm – Safety
- 3 pm – Cybersecurity

BCMC

Please Fill Out Your Session Evaluation

BCMC

Cybersecurity & Disaster Recovery Planning

Work through these questions with your IT team to ensure you're ready to face anything that threatens your ability to keep your business running.

Business Continuity & Disaster Recovery

Is the Business Continuity/Disaster Recovery plan documented and regularly tested?
Does this plan account for disruptions related to natural disasters (earthquake, hurricane, snowstorm), power outages (both temporary and prolonged), cybersecurity threats, and software/equipment failure?

What is the Recovery Time Objective (RTO)?
RTO is the time goal to restore service after a disruption.

What is the Recovery Point Objective (RPO)?
RPO is the acceptable time threshold of data loss.

Backups

What servers, desktops, and core business data are backed up?
How often are they backed up? Are those backups tested on a regular schedule?

What levels of redundancy are in place?
If a server or other portion of your infrastructure fails, will it be automatically moved to different hardware without disruption?

Are there spare, pre-configured computers available to put into critical infrastructure?
Does this include critical office and shop computers? What is the expected timeframe to replace a machine? If a pre-configured PC isn't available, what is the SLA from the 3rd party hardware supplier?

Digital Safety

What layers are in place to prevent a cybersecurity incident?
Is anti-virus software in place and up to date? Are firewall policies audited regularly to ensure only required ports are open? Is there a monitoring/on-call policy to react to alerts quickly? Are there blocks in place to prevent connections to countries that are not required for business?

Which users have local rights to install software (or viruses)?
Why? What software or process requires this? Do any IT (or other) users operate with domain admin rights on their day-to-day accounts?

Is web traffic monitored and filtered?

Are spam and threat protection enabled on the mail server?

Are all end users regularly trained and tested on cybersecurity?
Can they identify aspects of ransomware, phishing, forged emails or websites?

Is the Wi-Fi secured and monitored with "guest access" policies (if necessary)?

Next Steps

Schedule meeting for follow-up on: _____

6300 Enterprise Lane
Madison, WI 53719
608-274-4849

Notes:

Notes:

How BCMC Contributes to Your Business Success

Best practices are shared by industry experts in every educational session.

Conversations with peers lead to ideas that transform individual businesses.

Meetings with suppliers give insight into opportunities for further innovation.

Coming together for one week every October generates ideas and energy that drive the industry forward throughout the year.

2020 KNOXVILLE

WASTE LESS. BUILD MORE. SELL MORE.

MATCHPOINT® DIRECTDRIVE™ SYSTEM

WASTE LESS LABOR, SPACE, LUMBER AND PRODUCTION TIME.

MiTek's MatchPoint® DirectDrive™ System is a fully integrated software and material handling system boosts roof truss cutting and assembly for greater plant productivity.

The MatchPoint® DirectDrive™ System:

- A cellular approach to truss manufacturing that takes multiple manually managed processes and coordinates them as a whole
- Utilize software and machinery relationship to stabilize the manufacturing schedule – thus allowing for better planning and less variability
- Pick, cut, and deliver material to a build station with no hands touching the material
- Designed to address labor shortages, complex truss designs, material handling issues, and productivity demands

Achieve a new standard of performance for you and your customers with the strongest, most complete commitment to support your success at every step.

Learn more at MiTek-US.com/DirectDrive or call us at 800-325-8075

MiTek®