Dealing with a Cyber Attack

Steve Tippmann
Executive Vice President
Tippmann Group
Cybercrime damages are predicted to cost the world $6 trillion annually by 2021, up from $3 trillion in 2015.

- Exponentially more than the damage inflicted from natural disasters in one year
- More profitable than the global trade of all major illegal drugs combined
- By 2021, more than 70 percent of all cryptocurrency transactions annually will be for illegal activity
- Around $76 billion of illegal activity per year involves bitcoin

*according to the Cisco/Cybersecurity Ventures 2019 Cybersecurity Almanac*
Considering the statistics, it's not a question of 'if' a small-to-midsized business will be hacked, but 'when'.

- Even with all of our changes, our IT department is certain we will be hit again
- It is just how we’ve prepared/protected ourselves that can change the outcome

*according to the Cisco/Cybersecurity Ventures 2019 Cybersecurity Almanac*
*according to the Cisco/Cybersecurity Ventures 2019 Cybersecurity Almanac
INTERSTATE WAREHOUSING

Our Systems

- WMS - Warehouse Management System
- E-mail & calendar
- Accounting
- jda.
- RedPrairie
- Exchange
TIPPMANN CONSTRUCTION

Our Systems

Cloud-based File Server – BIM / Customer Files

Accounting

E-mail & calendar

Exchange

sage
ASK YOURSELF
Where Would You Be Without These Applications?

Business Reports and Accounting
All locked and inaccessible.

WMS and EDI Systems
5 Minutes after the attack launched we had zero access.

Phone System
VOIP meant it was impacted as well – we were down to cell phones - contact lists were crucial!

The Ability To Access Email
That’s where we found ourselves and we defaulted to our private accounts.

Servers
EDI, WMS, accounting, reports, history, only our last resort backups were unaffected but those would take days to load.

100% of our 1,300 employees were affected. Everyone had to make adjustments to working without the usual technology.
CYBER ATTACK
Timeline Sunday 20 January (Martin Luther King, Jr. Weekend)

REPORTING
Midnight
Warehouses begin reporting inability to connect to business systems

DETERRMINATION
Early AM
IT investigates and determines issue is ransomware attack after malware found

SECURING THE BUSINESS
Early AM
Verify what systems have been attacked, then secure systems not affected, including facility security and refrigeration operating systems

ENGAGEMENT
Mid - AM
Initial contact with hackers and securing of system and backup data

CRISIS RESPONSE
Mid - AM
Engaged Cyber Security Professionals (Coveware) to handle negotiations. Notified major customers of the situation.

ONSITE SUPPORT
Afternoon
Cyber Security firm (Symplexity) working along IT Staff to secure and bring up network infrastructure

ATTACK IMPACTS
Afternoon
WMS, Accounting & Email servers all down. 600 PC’s impacted, iPhone and iPads down

IARW-WFLO Convention
April 7–10, 2019
Santa Ana Pueblo, New Mexico
NEGOTIATION
Hired firm that specialized in cyber negotiations who took over that aspect.

ENGAGEMENT
Staff at all levels fully engaged at learning the issues and engaging in solutions and communication.

SUPPORT
Operations staff doing whatever IT Needs - From sourcing & getting hardware to monitoring server activity.

THE DECRIPTION KEY
Key is received early AM and is tested in secure environment to ensure its safe.

NEW HARDWARE
New servers are purchased in Atlanta with OS installed and flown or driven to sites by employees.

COMING ONLINE
Data is being reloaded and PC's scanned and cleared by Ops supporting and reporting to IT.
CYBER ATTACK
Timeline Wed – Thurs (23 & 24) January

23rd
CORPORATE
Rebuilding domain & network to bring sites back up online as well corporate systems

23rd
WAREHOUSES
1st Phase
Franklin / Indianapolis begins operations and processing orders in AM

24th
WAREHOUSES
2nd Phase
Murfreesboro, Joliet, Cincinnati begin operations & processing orders in PM

24th
FORENSICS
Hired cyber forensics investigation team (Kroll) to provide further details

24th
WAREHOUSES
3rd Phase
Indianapolis begins operations and processing orders in AM

24th
CUSTOMER INFO
Sent FAQ sheet to customers to help explain the situation and what we have been doing to resolve
CYBER ATTACK
Timeline Fri – Sat (25 & 26) January

WAREHOUSES 4th Phase
Newport News begins operations and processing order in AM

ALL SITES
Finish converting users to Office 365 – This was in process but due to attack deployment is sped up.

WAREHOUSES 5th Phase
Anderson begin operations & processing orders in AM

Recovery
FULL RECOVERY
Approximately 1 week after event all sites are back to normal
Our Team Stories / Lessons Learned
Things Get Done With People...

LEADERS
• Timely decisions
• Clear direction
• Effective communication

IT DEPARTMENT
At every site these folks refused to surrender... at every site there were air mattresses in offices and they took their sleep where they could

TIME MANAGEMENT
Using time wisely during the outage to manually collect inventory information saved us time and set us up for success at start-up.

EXCEPTIONAL INDIVIDUALS
Knowing your employees’ assets and strengths before you get in a crisis allows you to solve issues quicker during an event – example: Heidi – inbound scheduler with strong IT background

TEAMWORK
Be prepared! Have a plan and know your top performing employees in each area:
Increased volume of work when operations resumed:
Day 1 – 58% more than normal
Day 2 – 75% more than normal
Day 3 – 184% more than normal
*Every case pick record was broken during that time

COMMUNICATION
Effective communication of the goal and getting employees to understand the importance of the situation allowed us to drive through the work with positive attitudes

*100+ employees worked more than 70 hours that week
We Couldn’t Have Done It Without Our Customers

CUSTOMERS

We cannot say enough here about the support our customers showed us and offers of help as well as working with us to manage the impact to their operations.