WISCONSIN UNDER ATTACK | RESPONDING TO CYBER CRIMINALS

CRT & groupsense

SARAH FRATER

LTC, MI, WIARNG
Director, Cybersecurity Operation

LTC Sarah Frater is the Director of Cybersecurity Operations for the Wisconsin Department of Military Affairs, Wisconsin National Guard. Sarah has been in the military for over 20 years, with multiple overseas deployments. Her career has involved intelligence, security, and cybersecurity, with positions in both public and private sector.

Today LTC Frater is on the front lines of Cyber Response, providing guidance and response services to Wisconsin critical infrastructure, municipalities, and schools.

KURTIS MINDER

CEO at GroupSense

Kurtis Minder is the CEO and co-founder of GroupSense, a leading provider in Digital Risk solutions. Kurtis built a robust cyber reconnaissance operation protecting some of the largest enterprises and government organizations.

Kurtis has been the lead negotiator at GroupSense for ransomware response cases. He has successfully navigated and negotiated some of the largest ransomware, breach, and data extortion cases world-wide.

With over 20 years in the information security industry, Kurtis brings a unique blend of technical, sales and executive acumen.

THE DIGITAL PANDEMIC

IT ISN'T JUST WISCONSIN

The value of ransom demands has gone up, with some demands exceedingly well over **$1 million**.

Cybersecurity & Infrastructure Security Agency, 2021

The total ransomware costs are projected to exceed **$20 billion** in 2021.

Cybercrime Magazine, 2019

Experts estimate that a ransomware attack will occur every **11 seconds** in 2021.

Cybercrime Magazine, 2019

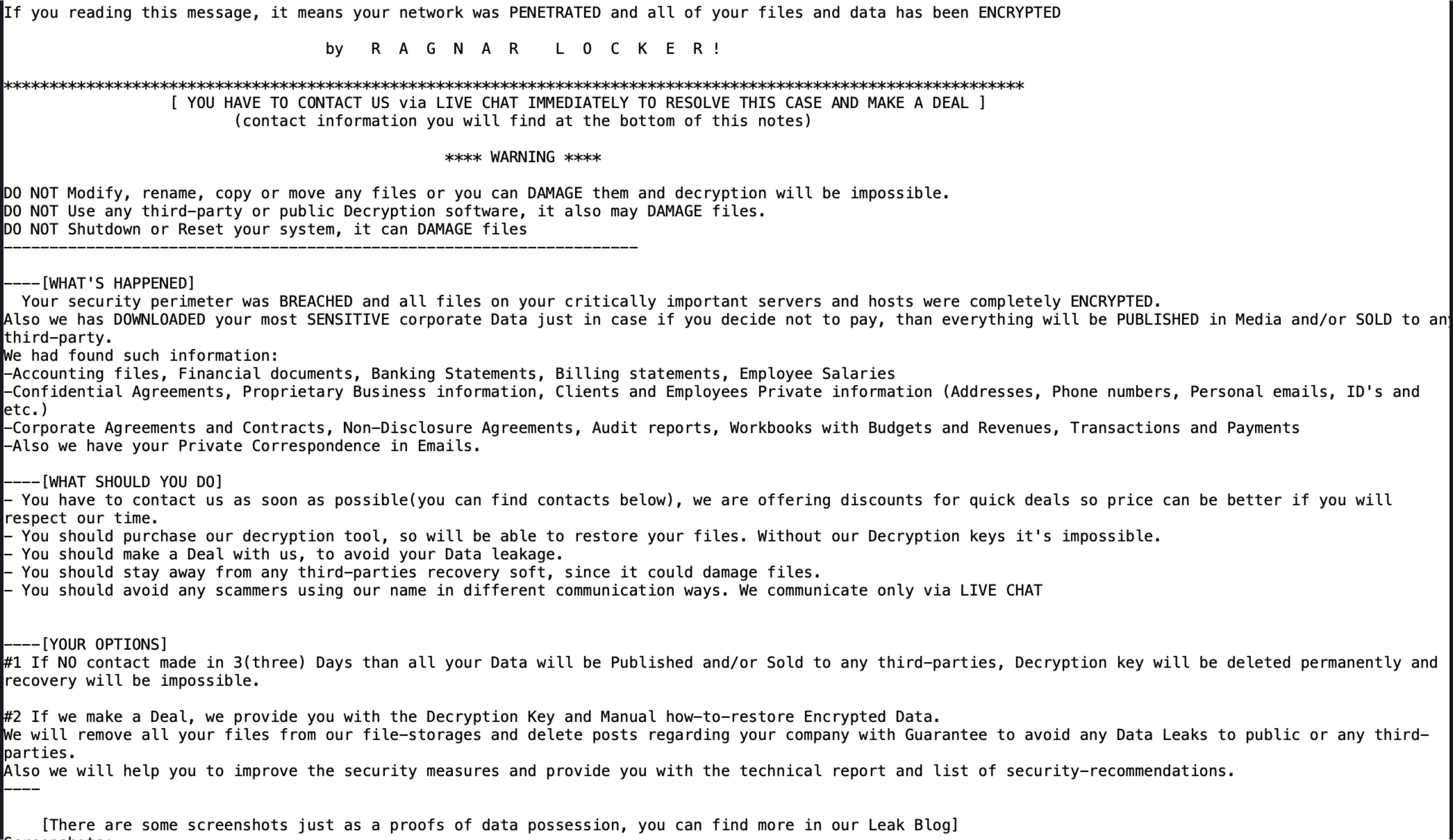
On average, ransomware attacks cause **15 business days of downtime**. Due to this inactivity, businesses lost around **$8,500 an hour**.

Health IT Security, 2020

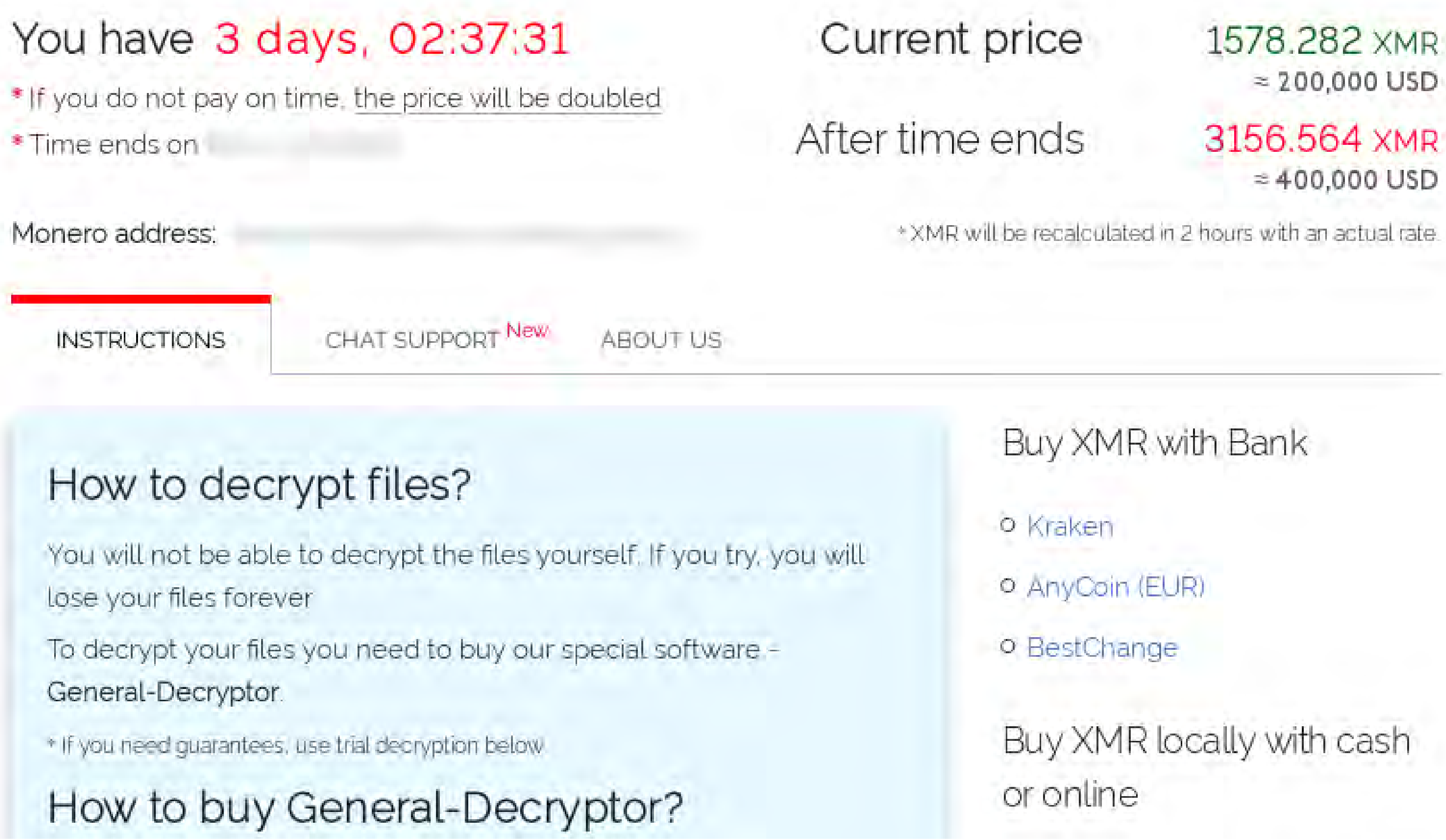
In 2019, nearly **56% of organizations** across multiple industries reported a ransomware attack.

CISO Magazine

What happens in a ransomware attack?



```
If you reading this message, it means your network was PENETRATED and all of your files and data has been ENCRYPTED

                                   by   R  A  G  N  A  R    L  O  C  K  E  R !

***************************************************************************************************************
                  [ YOU HAVE TO CONTACT US via LIVE CHAT IMMEDIATELY TO RESOLVE THIS CASE AND MAKE A DEAL ]
                         (contact information you will find at the bottom of this notes)

                                                **** WARNING ****

DO NOT Modify, rename, copy or move any files or you can DAMAGE them and decryption will be impossible.
DO NOT Use any third-party or public Decryption software, it also may DAMAGE files.
DO NOT Shutdown or Reset your system, it can DAMAGE files
---------------------------------------------------------------------


----[WHAT'S HAPPENED]
  Your security perimeter was BREACHED and all files on your critically important servers and hosts were completely ENCRYPTED.
Also we has DOWNLOADED your most SENSITIVE corporate Data just in case if you decide not to pay, than everything will be PUBLISHED in Media and/or SOLD to any
third-party.
We had found such information:
-Accounting files, Financial documents, Banking Statements, Billing statements, Employee Salaries
-Confidential Agreements, Proprietary Business information, Clients and Employees Private information (Addresses, Phone numbers, Personal emails, ID's and
etc.)
-Corporate Agreements and Contracts, Non-Disclosure Agreements, Audit reports, Workbooks with Budgets and Revenues, Transactions and Payments
-Also we have your Private Correspondence in Emails.

----[WHAT SHOULD YOU DO]
- You have to contact us as soon as possible(you can find contacts below), we are offering discounts for quick deals so price can be better if you will
respect our time.
- You should purchase our decryption tool, so will be able to restore your files. Without our Decryption keys it's impossible.
- You should make a Deal with us, to avoid your Data leakage.
- You should stay away from any third-parties recovery soft, since it could damage files.
- You should avoid any scammers using our name in different communication ways. We communicate only via LIVE CHAT



----[YOUR OPTIONS]
#1 If NO contact made in 3(three) Days than all your Data will be Published and/or Sold to any third-parties, Decryption key will be deleted permanently and
recovery will be impossible.

#2 If we make a Deal, we provide you with the Decryption Key and Manual how-to-restore Encrypted Data.
We will remove all your files from our file-storages and delete posts regarding your company with Guarantee to avoid any Data Leaks to public or any third-
parties.
Also we will help you to improve the security measures and provide you with the technical report and list of security-recommendations.
----

    [There are some screenshots just as a proofs of data possession, you can find more in our Leak Blog]
Screenshots:
```



You have 3 days, 02:37:31

* If you do not pay on time, the price will be doubled

* Time ends on [redacted]

Current price 1578.282 XMR ≈ 200,000 USD

After time ends 3156.564 XMR ≈ 400,000 USD

Monero address: [redacted]

* XMR will be recalculated in 2 hours with an actual rate

How to decrypt files?

You will not be able to decrypt the files yourself. If you try, you will lose your files forever

To decrypt your files you need to buy our special software - General-Decryptor.

* If you need guarantees, use trial decryption below

How to buy General-Decryptor?

Buy XMR with Bank

- Kraken
- AnyCoin (EUR)
- BestChange

Buy XMR locally with cash or online

CYBER RESPONSE TEAM (CRT)

- Nested in DHS Strategic Plan, WI Homeland Security Strategy
- Initiated in 2015
- DMA led in collaboration with DET, WEM, and WSIC
- US Department of Homeland Security Grant Funding
- 136 members (117 public / 19 private)
- 23 facilitators (WSIC, National Guard, Coast Guard, WEM, DET, DPI, CISA, DHS)
- All volunteer

CYBER RESPONSE TEAM (CRT)

SUPPORT COVERS ALL 16 CRITICAL INFRASTRUCTURE SECTORS

- Agriculture and Food
- Financial Services
- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Government Facilities (including elections, education)
- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials and Waste
- Transportation Systems
- Water and Wastewater Systems

CYBER RESPONSE TEAM (CRT)

Mission: To provide support for critical infrastructure in the state of Wisconsin in order to prevent, mitigate and respond to cyber incidents, through training, assessment, and incident response.

Vision: Coordinated response effort from the state volunteer Cyber Response Team (CRT) and National Guard, assisting in both preventing and responding effectively in the event of an emergency.

TRAINING

CRT/WING Quarterly Training Program

- Foundations: required for incident responders
- Skills: incident response tools and processes

Annual Exercise

- 2021: based on GridEx
- Advanced Skills

Cyber Shield

- Nationwide exercise hosted by NGB
- Participated in 2017, 2019, 2021
- 9 state partners, 17 military
- 3 registered for 2022

Training Courses

- SANS SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling
- SANS FOR500: Windows Forensic Analysis
- SANS FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics
- SANS FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response

ASSESSMENT

CISA Assessment Evaluation and Standardization (AES)

- Cyber Resilience Review (CRR)
- External Dependencies Management (EDM)
- Risk and Vulnerability Assessment (RVA)
- High Value Assets (HVA)

Process

- Request an assessment
- 2 CISA Cybersecurity Advisors + 1 CRT member

INCIDENT RESPONSE

- Call to WEM Duty Officer: (800) 943-0003, Option 2
- Initiate Cyber Response Management Group (CRMG)
    - Facilitated by DMA Cybersecurity Operations
    - Contact Incident Response Team Leads / WSIC
    - May include State CISO, HSC/CY, WCSPWG, DET, WSIC, WEM, WING, federal agencies, other state, local, and tribal personnel
    - Coordination call with requesting organization
    - Deploy volunteers if requested
- Complete final report
- Sanitize systems

NATIONAL GUARD CAPABILITIES

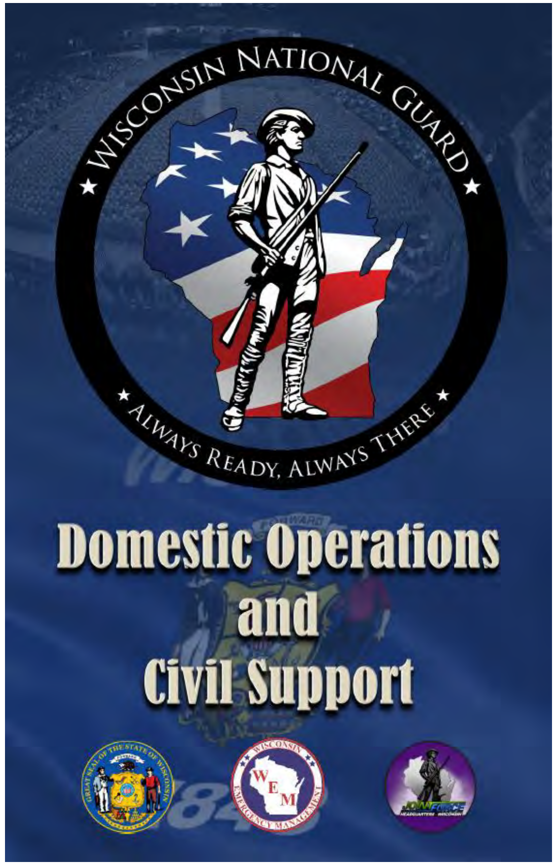
Defensive Cyberspace Operations Element (DCOE)

- Most states have a DCOE at their state headquarters
- Approximately 10 personnel
- Trained in both incident management and cyber operations
- Capable of sustained operations

Cyber Protection Team (CPT)

- Approximately 35 personnel split between Wisconsin and Illinois
- 22 are in Wisconsin
- Ready to augment the DCOE as needed for domestic operations

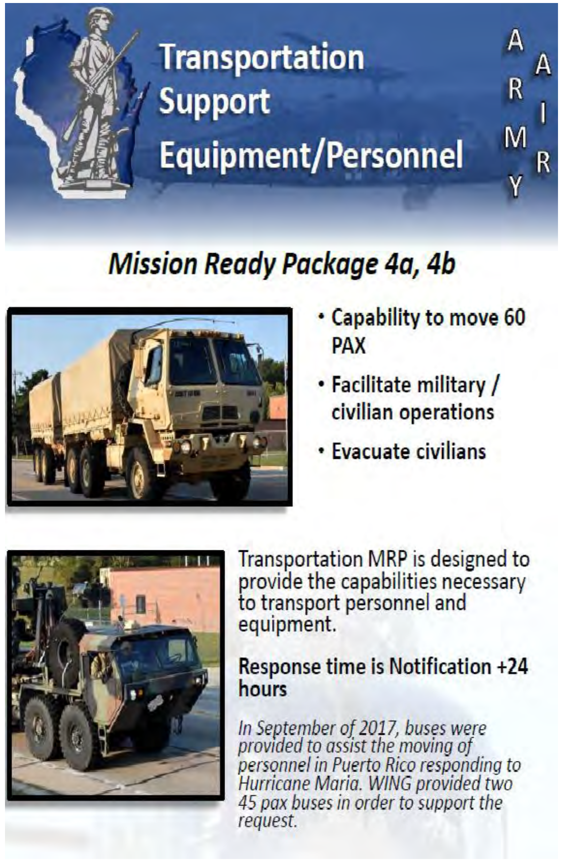
MISSION READY PACKAGE (MRP)



Wisconsin National Guard

Always Ready, Always There

Domestic Operations and Civil Support



Transportation Support Equipment/Personnel

ARMY AIR

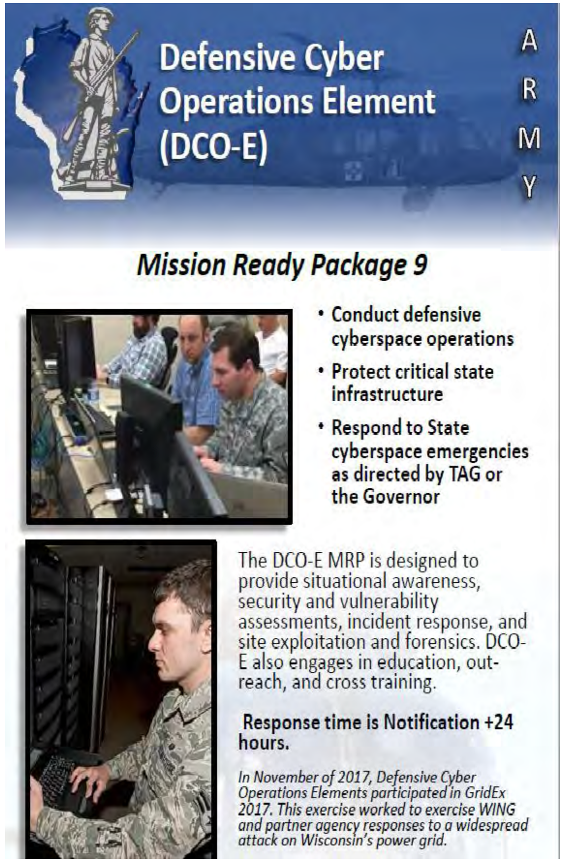
Mission Ready Package 4a, 4b

- Capability to move 60 PAX
- Facilitate military / civilian operations
- Evacuate civilians

Transportation MRP is designed to provide the capabilities necessary to transport personnel and equipment.

Response time is Notification +24 hours

In September of 2017, buses were provided to assist the moving of personnel in Puerto Rico responding to Hurricane Maria. WING provided two 45 pax buses in order to support the request.



Defensive Cyber Operations Element (DCO-E)

ARMY

Mission Ready Package 9

- Conduct defensive cyberspace operations
- Protect critical state infrastructure
- Respond to State cyberspace emergencies as directed by TAG or the Governor

The DCO-E MRP is designed to provide situational awareness, security and vulnerability assessments, incident response, and site exploitation and forensics. DCO-E also engages in education, out-reach, and cross training.

Response time is Notification +24 hours.

In November of 2017, Defensive Cyber Operations Elements participated in GridEx 2017. This exercise worked to exercise WING and partner agency responses to a widespread attack on Wisconsin's power grid.

EMERGENCY MANAGEMENT ASSISTANCE COMPACT (EMAC)

- Successfully utilized EMAC for 2020 civil disturbance response.
- The National Guard is heavily relied upon by states through EMAC thanks to the speed and efficiency of the National Guard as a force multiplier.
- On average, National Guard represents approximately 42% of the resources deployed through EMAC.
- The National Guard & EMAC: emacweb.org

HOW CAN YOU HELP?

- Request an assessment: CISA, CRT, National Guard, Coast Guard
- Implement multi-factor authentication
- Write/Review/Update your Continuity of Operations Plan
  - Have a printed copy
  - Cyber Insurance / Infrastructure Support / CRT
- Encourage your staff to join the CRT
- Start a cyber club
  - Cyber Patriot / Go CyberStart / National Cyber Cup

LEADERSHIP CYBERSECURITY CHALLENGES

Two-thirds of organizations consider cybersecurity merely as an afterthought instead of including it in the planning stage of new business initiatives.

- Cybersecurity STILL is not a priority for many organizations
- Leadership lacks familiarity with cybersecurity issues, nuances
- Difficult to assess risk, measure asset value
- “It won’t happen to me” syndrome
- “We have an incident response plan….”

COMMON MISCONCEPTIONS

- Cyber breaches are covered by general liability insurance or misunderstanding of Cyber Insurance Policy fine print
- Compliance with industry standards is enough for a security program
- Overconfidence that organizations won’t be breached
- You can’t prevent a breach (Why try so hard?)

HOW RANSOMWARE BREAKS THINGS

- Most organizations feel prepared for a ransomware attack, e.g., ”We have backups”, “We have an incident response plan.” “We have EDR/MDR”
- Brand / PR / Customer fallout is not considered
- Who is in the room? Who is in charge? Who owns the financial component?
- Is the door really locked?
- OFAC?
- Law Enforcement?
- Outcomes…

MY DISTILLED LIST

Password Policy
Maintain and publish a password policy for your organization. The policy should illustrate the importance of password security and credential use in the organization.

Use a password manager
Use an enterprise-friendly password manager and require employees to use this as part of the security program.

Enable Multi-Factor Authentication Everywhere Possible
Enable the 2FA or MFA capability on everything used in the business. This includes email, network access, remote access, and any web-based applications.

Email Security and Email Policy
Have a strong policy about using corporate email for personal use. Restrict access to personal mail on company assets.

Patch

Backups
Keep at least one manual backup of your data offsite in a secure location.

Secure Remote Access
If remote access is required, use a zero-trust access method or a VPN. Use two-factor authentication.

Digital Risk Protection Services
The indicators of compromise (IOCs) related to malware strains associated with ransomware are quickly and easily available on the internet.

Security Awareness Training
In order to combat threats, the team needs to be made aware of them.

LESSONS LEARNED IN THE TRENCHES

Do Not Panic

You have options. This is recoverable. Revert to your plan and execute.

Do Not Engage

Don’t let anyone go to the site / respond. It can start a timer. Tone, language, style, and content can significantly impact odds and costs negatively.

Don’t Shut Down

Don’t shut down machines, this can cause file corruption, and hinders the incident response process.

Do Not Bury Your Head

Having backups and restoring doesn’t mean this is over. There are many other things to consider.

Engage Legal Counsel

It is likely you are subject to breach disclosure laws - bring legal help to determine your obligations.

Engage PR Support

You will have to notify impacted constituents. Do this carefully and with professional guidance.

Engage IR

Bring in incident response assistance to understand the scope of the attack and to ensure the threat actors no longer have access.

Contact Insurance

Your insurer may have requirements dictating how the response is carried out. Engage them early.

Bring in a Professional Responder

Bring in a professional that has firsthand experience with the entire ransomware process.

Consider Sanctions

Your country may have rules about which entities you can transact with. Responders can help you avoid penalties.

Notify Law Enforcement

It is best practice to make local law enforcement aware of the situation.

Monitor

It is likely the threat actor took a significant amount of data. Monitor just in case it surfaces elsewhere.

Action Items:

Update your Continuity of Operations Plan

Exercise your Continuity of Operations Plan

Refer IT/Cybersecurity professionals to join the CRT

Request an assessment

HOW TO REACH THE CRT

WEM Duty Officer: (800) 943-0003, Option 2

Let them know you have a cyber incident.

Add this as a step in your Continuity of Operations Plan.

Identify-Protect-Detect
Respond-Recover

CRT

groupsense

THANK YOU | Q&A

LTC SARAH FRATER

DIRECTOR, CYBERSECURITY OPERATIONS

SARAH.R.FRATER.MIL@ARMY.MIL

KURTIS MINDER

CEO, GROUPSENSE

KURTIS@GROUPSENSE.IO