SAINT PAUL
MINNESOTA

CITY OF SAINT PAUL
OFFICE OF MAYOR MELVIN CARTER

15 W. Kellogg Blvd,
Saint Paul, MN 55102
Tel: 651-266-8510

DOCUMENT TRANSMITTAL SHEET

To: Legislative Commission on Cybersecurity
Rep. Kristin Bahner, Rep. Steve Elkins, Rep. Jim Nash, Rep. Bjorn Olson
Sen. Mark Koran, Sen. Eric Lucero, Sen. Melissa Wiklund, Sen. Tou Xiong

From: Mayor Melvin Carter's Office, City of Saint Paul
Date: August 26, 2025
Re: Submission of Materials – Operation Secure Saint Paul

Enclosures:

1. Public Presentation
2. Digital Security Timeline
3. Letter to Major General Shawn Manke

STPAUL.GOV

SAINT PAUL'S RESPONSE TO DIGITAL SECURITY INCIDENT

LEGISLATIVE COMMISSION ON CYBERSECURITY | AUG 27, 2025

In today's presentation

- Opening Remarks and Grounding
- Information Security Program Overview
- Digital Security Incident Response
- Key Partnerships
- Appendix: Detailed Timeline

What we cannot discuss today in public session:

- Ongoing Criminal Investigation
- Attribution
- Specific Forensic Evidence
- Operational Security

Ongoing Criminal Investigation

The City of Saint Paul is part of an active, multi-agency investigation with state and federal partners, including the FBI, DHS, BCA, Minnesota Department of IT, and Minnesota National Guard.

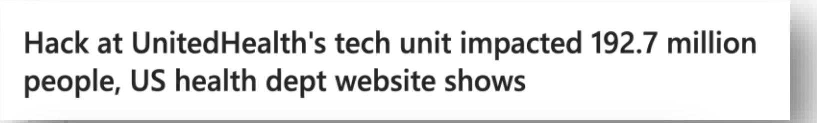
Opening Remarks

The State of Cybersecurity

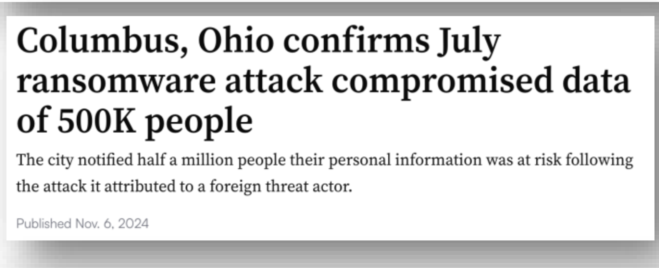
SAINT PAUL
MINNESOTA

Cyberattacks are a global issue — cities, corporations, and institutions everywhere are targeted daily

- Saint Paul is not unique in experiencing a criminal cyber threat by actors using ransomware tactics.
- What is unique is our decisive response and swift recovery with the support of partners. We did not pay the ransom demand.
- Conducting regular backups of our information system is standard operating procedure. This blocked the threat actors from holding hostage access to our system and limited the amount of information they exfiltrated.
- What is unique is our decisive response and swift recovery with the support of partners.



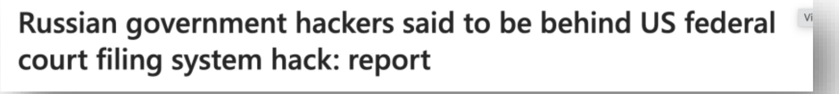
Hack at UnitedHealth's tech unit impacted 192.7 million people, US health dept website shows



Columbus, Ohio confirms July ransomware attack compromised data of 500K people

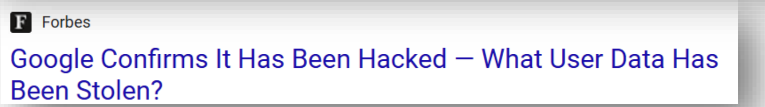
The city notified half a million people their personal information was at risk following the attack it attributed to a foreign threat actor.

Published Nov. 6, 2024



Russian government hackers said to be behind US federal court filing system hack: report

Vi



Forbes

Google Confirms It Has Been Hacked — What User Data Has Been Stolen?

Two Lines of Effort Defined Our Response: Investigating the Threat and Sustaining City Services

1. Immediate Investigation & Response

- Forensic analysis, containment, and threat isolation
- Activated national and state cyber partners

2. Continuity of Government Services

- 911 answered without interruption
- Payroll processed on time
- City business and resident services continued

Our Emergency Management department supported the activation of the Emergency Operations Center

- Unified local, state, and federal coordination
- Minnesota National Guard Cyber Protection Team deployed
- Structured support for both technical response and continuity

The City has a strong security foundation pre-incident that enabled our swift recovery.

- In 2022, the City created the Chief Information Security Officer (CISO) role to drive cyber strategy.

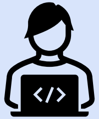
- Proactive safeguards already in place included:
    - Multi-Factor Authentication (MFA) required for remote and VPN access to City services
    - Advanced endpoint detection monitoring tools to detect suspicious activity
    - Air-gapped backups protecting critical data
    - Employee cybersecurity training and phishing awareness campaigns

- We were able to detect, contain, and recover quickly when the threat actor entered our systems.

What is endpoint detection?

- Security software that runs on every computer and device to spot unusual or suspicious activity in real time.

- Helps IT teams quickly isolate, investigate, and stop threats.



Key Milestone:
Operation Secure Saint Paul

- Coordinated effort spanning every City department, with more than 3,000 employees supported through new security protocols.
- Deployed advanced endpoint detection across thousands of devices, verified clean backups, and reestablished secure network access.
- Implemented structured check-in/check-out for employees and devices to ensure system integrity.
- Leveraged Guard support to expand capacity, sustain operations, and accelerate recovery timelines.

Overview of Key Partnerships

- **State of Minnesota:** Provided intelligence, technical expertise, and operational support that restored emergency systems, kept state leadership connected, and ensured accountability during Operation Secure Saint Paul.

- **Minnesota National Guard:** Deployed for 17 days, bringing surge capacity and credibility that safeguarded public safety operations, accelerated recovery, and strengthened planning.

- **Federal Partners:** FBI and CISA delivered investigative leadership, forensic insight, and national intelligence that connected Saint Paul's response to best practices and broader protection.

- **Incident Response Partner:** Supplied independent expertise to guide forensics, containment, and secure recovery, ensuring the City's response followed industry standards.

Preparation and Partnerships Make the Difference in Cyber Defense

1. Our proactive steps — MFA, endpoint detection, backups, and training — gave us the foundation to respond quickly.

2. National Guard, state, federal, and private-sector expertise accelerated recovery and strengthened our defenses.

3. Efforts that were already underway such as modernizing infrastructure, upgrading identity systems, and expanding cloud-based services are being accelerated.

4. Continuous employee awareness, phishing training, and strong credential practices are as vital as technology.

5. **A message for others: No city is immune. The best defense is to prepare, invest, and continuously build resilience to evolving threats.**

Technology and Security Investments

Training

SAINT PAUL
MINNESOTA

The City of Saint Paul has a robust information security program

Even before the incident, Saint Paul had been strengthening its cybersecurity foundation — investing in modern tools, clear policies, and employee awareness to reduce risk and build resilience including:

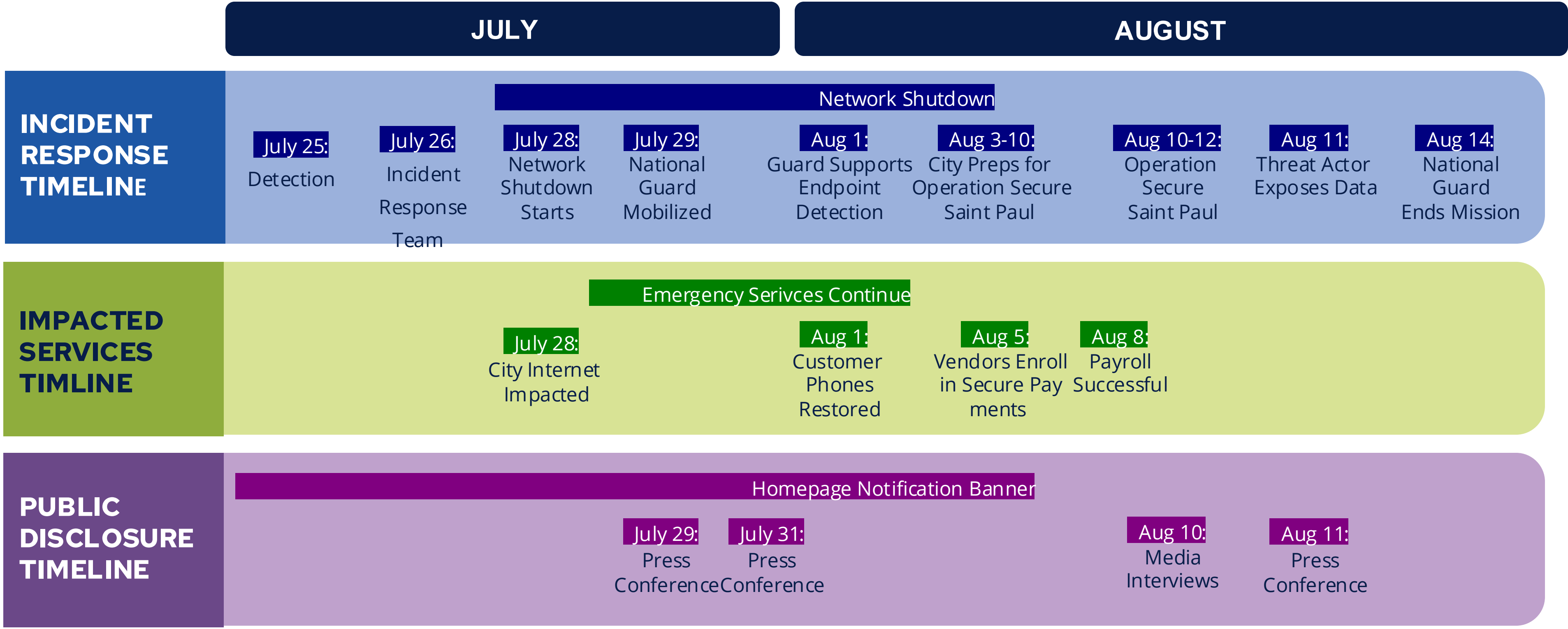
- **Modernized defenses** with advanced endpoint detection, operating system upgrades, and secure-by-design methodology.
- **Built a stronger security program** through clear policies, governance, and risk/exposure management.
- **Third-Party/Vendor** accountable through independent cloud and third-party security reviews.
- **Protected digital credentials and email** with multi-factor authentication, Email system-level protections, and tighter credential controls.
- **Building a secure culture** with phishing awareness training and the *Firewall* cybersecurity newsletter.

Our Response

Our Whole-of-Government Response

Timeline Overview: Emergency Phase

City of Saint Paul



JULY | AUGUST

INCIDENT RESPONSE TIMELINE

Network Shutdown

July 25: Detection

July 26: Incident Response Team

July 28: Network Shutdown Starts

July 29: National Guard Mobilized

Aug 1: Guard Supports Endpoint Detection

Aug 3-10: City Preps for Operation Secure Saint Paul

Aug 10-12: Operation Secure Saint Paul

Aug 11: Threat Actor Exposes Data

Aug 14: National Guard Ends Mission

IMPACTED SERVICES TIMLINE

Emergency Serivces Continue

July 28: City Internet Impacted

Aug 1: Customer Phones Restored

Aug 5: Vendors Enroll in Secure Payments

Aug 8: Payroll Successful

PUBLIC DISCLOSURE TIMELINE

Homepage Notification Banner

July 29: Press Conference

July 31: Press Conference

Aug 10: Media Interviews

Aug 11: Press Conference

ONGOING COMMUNICATION & COLLABORATION WITH PARTNERS: FBI, BCA, MNIT, MNNG, CISA, & HSEM

On July 25, 2025, the City detected threat actors inside our digital systems

- A sophisticated cyber threat actor motivated by financial gain established initial access to City systems.
- City security tools spotted the threat early enough to give us time to activate Incident Command and response team, check defenses, and confirm backups.
- Within days, the City shut down the network to contain the threat.
- This action allowed us to protect our systems, data, and services.

Federal Joint Advisory on Interlock Ransomware (July 22, 2025)

- CISA alerted the public just three days before the City's digital security incident
- Alert warned that Interlock ransomware uses compromised websites and fake updates to steal and encrypt data, and urged organizations to patch, train staff, and require MFA.

Incident Response Partner

Engaging a specialized **Incident Response (IR) team** is the national standard when responding to a cyberattack. The City retained a private incident response partner on July 26 to provide independent expertise, accelerate containment, and ensure our recovery followed industry best practices. Their team has worked side-by-side with OTC, the Minnesota National Guard, and federal partners throughout this process.

Key Contributions:

- Leading forensic investigations to track and understand attacker activity.
- Supporting containment strategies and secure recovery planning.
- Guiding deployment of endpoint detection tools
- Advising on system hardening, Active Directory security, and network segmentation.
- Coordinating closely with City, the Minnesota National Guard, and federal agencies to ensure a unified response.

Data Exposure Addressed with Transparency and Employee Protections

- On August 11, a set of data was exposed on the threat actor's leak site after the City refused to pay a ransom.
- The exposed material came from a Parks and Recreation network drive, not core city service-related data. We immediately began a careful review of the data to determine what was accessed and who may be affected. This is ongoing.
- The City is following all legal notification requirements and will continue directly contacting any impacted employees.
- **Proactively offered every City employee 12 months of free identity theft protection and credit monitoring.**

In accordance with Minnesota Statutes §13.055, the City will:

- ✓ Notify affected individuals in writing.
- ✓ Prepare and share investigation reports on any breach.
- ✓ Follow required security assessments and coordination protocols.

Restoring Services Safely and Securely

- Clean backups from July 25 provided a provided a robust and reliable foundation for rebuilding systems.

- Services are being restored carefully and in phases — ensuring they are tested and secure before returning online.

- Public safety prioritized:
  - Police/Fire/EMS response remained uninterrupted throughout
  - Criminal legal access and essential operations were restored first

- This rigorous process enabled the City to confidently issue the August 20 attestation affirming the security of our Microsoft 365 environment and email systems.

- Work was done in close partnership with our independent incident response vendor to validate every step.

Key Partnerships

Incident Response Support with Local, State, and Federal Cybersecurity Experts and Law Enforcement

SAINT PAUL
MINNESOTA

City of Saint Paul Emergency Management

- **Activated the Emergency Operations Center (EOC):** Unified City, county, state, federal, and Guard partners under one coordinated structure.
- **Operationalized the Incident Support Model:** Ensured clear roles, responsibilities, and communication across departments.
- **Maintained Citywide Continuity:** Set expectations that core services continue.
- **Coordinated Information Flow:** Provided regular situational updates to leadership, employees, and partners.
- **Enabled Surge Capacity:** Integrated state and federal resources to accelerate recovery and support City staff.

State of Minnesota Partnerships

State partners were force multipliers in Saint Paul's response, providing intelligence, technical expertise, and operational capacity that directly accelerated recovery.

Key Contributions

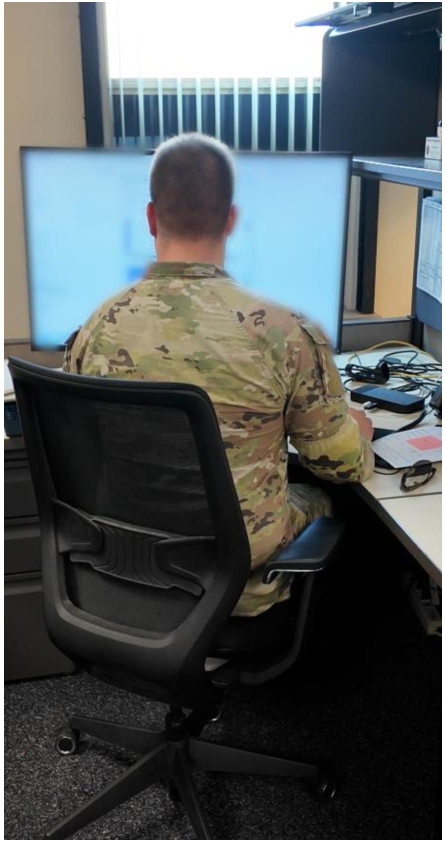
- BCA, MNIT, and Ramsey County ECC partnered with the Minnesota National Guard to install secure hard drives and enabled backup CAD access for Police and Fire vehicles — restoring a lifeline for emergency response.
- Delivered real-time threat intelligence, forensic support, and statewide visibility into attacker tactics.
- Maintained continuous information flow between Saint Paul's Emergency Operations Center and state leadership.
- Augmented City planning for Operation Secure Saint Paul, supporting check-in/out and accountability for thousands of employees.

Takeaway: State partners were indispensable — ensuring emergency response continuity while strengthening Saint Paul's security and recovery.

Minnesota National Guard's Cyber Protection Team

The City of Saint Paul is deeply grateful for the Guard's support and partnership in helping protect our community and accelerate recovery.

- Deployed for 17 days to support the City's response and recovery.
- Brought expertise, professionalism, and credibility, working seamlessly with City staff and federal/state partners.
- Focused on continuity of critical services, including public safety operations.
- Supported the deployment of endpoint detection software across thousands of City devices.
- Instrumental in successful planning and execution of Operation Secure Saint Paul.
- Accelerated recovery timelines by providing surge capacity and technical skillsets.



Federal Partnerships

Federal partners provided critical investigative leadership, intelligence sharing, and cyber defense resources that strengthened Saint Paul's response and informed statewide protection.

Key Contributions

- **FBI:** Led the criminal investigation and digital forensic analysis, producing intelligence reports that guided MNIT, HSEM, and local partners. Provided direct situational awareness to protect other Minnesota jurisdictions.
- **CISA (DHS):** Delivered information-sharing and cyber hygiene services, supporting both immediate defense and long-term prevention. Shared national intelligence on ransomware tactics, helping benchmark Saint Paul's response.

Key Takeaway: Federal partners ensured Saint Paul's response was connected to national intelligence, aligned to best practices, and informed by forensic insight — turning a local incident into shared awareness for the state and beyond.

In Closing

Closing Reflections

- Cyber threats are borderless and growing, affecting governments, hospitals, schools, and businesses worldwide. Saint Paul's experience underscores that no community is immune.

- From the first hours, we acted decisively to protect critical services, safeguard emergency response, and limit the attacker's impact.

- By mobilizing local, state, and federal partners, we brought together intelligence, expertise, and resources that accelerated our recovery and expanded our capacity.

- We executed a dual strategy: immediate investigation and containment, while ensuring continuity of government operations so 911 calls were answered and city business continued.

- Today, Saint Paul emerges stronger, with modernized defenses, tested coordination structures, and renewed partnerships. We are more resilient, more prepared, and more committed than ever to protecting our community.

Thank You

Appendix: Response Timeline

Day-by-Day Overview of City Response

SAINT PAUL
MINNESOTA

Our Response Timeline

City of Saint Paul

Day 1 | July 25

DETECTION

Suspicious activity was identified involving compromised privileged accounts on a backup server.

- **Immediately deactivated the accounts, isolated affected servers, and increased monitoring to contain the threat.**

Day 2 | July 26

ESCALATION

The severity of the threat became clear and attacker persistence was confirmed.

- **Engaged private sector incident response firm and expanded forensic monitoring across City systems.**

Day 3 | July 27

CONTAINMENT

The City took protective action to limit attacker movement across the network.

- **VPN access disabled for most staff, while maintaining secure access for public safety. Microsoft 365 remained available.**

Day 1-3: Outcomes

✓ Threat detected, contained quickly.

✓ External incident response team engaged within 24 hours of detection.

✓ Early protective measures implemented to limit attacker movement.

Our Response Timeline

City of Saint Paul

Day 4 | July 28

NETWORK SHUTDOWN

Threat actors attempted to encrypt virtual servers within City systems.

- **Executed a full network shutdown while activating the Emergency Operations Center to coordinate the response, with intelligence and investigation support from federal partners.**

Day 5 | July 29
NATIONAL GUARD STARTS MISSION

Once the scope of the threat was understood, the City informed employees, residents, and partners openly and responsibly City prepared to inform employees, residents, and partners.

- **Mayor Carter declared a local emergency, the City publicly disclosed the incident, and Governor Walz activated the Minnesota National Guard to support recovery and security.**

Day 6 | July 30

CONTINUITY & PREPARATION

City maintains continuity of services under emergency protocols.

- **Emergency services remained fully operational; Implemented contingency operations to ensure on-time payroll the following week.**

Our Response Timeline

Day 7 | July 31

CONTINUITY & RESTORATION

Departments relied on manual processes to keep critical work moving, with payroll the top priority.

- **Payroll was processed securely and on time, ensuring every employee received pay without interruption.**
- **Mayor Carter updated the public at a pressconference.**
- **Threat actor "indicators of attack" provided to MNIT, which were distributed statewide through the MN Fusion Center to elevate monitoring.**

Day 8 | Aug 1

CONTINUITY & RESTORATION

Customer service phone lines were brought back online, and planning advanced for priority system recovery.

- **A backup Public Safety Mobile Data Terminal (MDT) solution was tested, providing direct CAD access through a multi-agency effort that included the National Guard.**

Day 9 | Aug 2

CONTINUITY & RESTORATION

Core services and enterprise projects continued despite disruption.

- **The Minnesota National Guard deployed into City facilities to begin installing endpoint detection across devices.**

Our Response Timeline

City of Saint Paul

Day 10 | Aug 3
BUILDING OPERATION SECURE SAINT PAUL

Departments sustained critical services while planners convened at the Emergency Operations Center.

- **Launched enterprise-wide coordination to drive password resets and endpoint protection installs.**

Day 11 | Aug 4
BUILDING OPERATION SECURE SAINT PAUL

System validation and recovery efforts expanded.

- **Nine additional National Guard personnel arrived to support Operation Secure Saint Paul and continue system validation.**

Day 12 | Aug 5
BUILDING OPERATION SECURE SAINT PAUL

Critical incident response workstreams advanced in tandem.

- **Forensic analysis, system restoration, and heightened security posture activities moved in sync and executed at an accelerated pace.**

Our Response Timeline

Day 13 | Aug 6
BUILDING OPERATION SECURE SAINT PAUL

Departments sustained critical services while planners convened at the Western District Headquarters.

- **Departments finalized the structure of Operation Secure Saint Paul, aligning on logistics, staffing, and service continuity while resets and device protections could be carried out.**
- **Critical incident response workstreams—digital forensics, system restoration, and elevating security posture—continued.**

Day 14 | Aug 7
BUILDING OPERATION SECURE SAINT PAUL

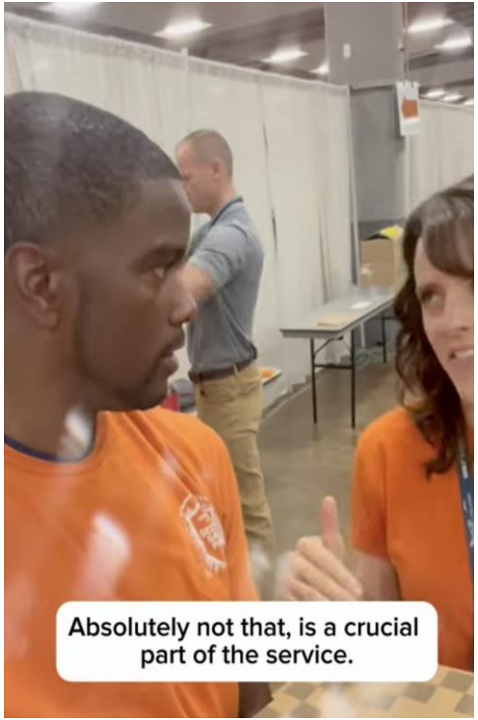
Detailed Operation Secure Saint Paul information provided to staff.

Day 15 | Aug 8

SUCCESSFUL PAYROLL POST-INCIDENT

Planners met onsite at Roy Wilkins Auditorium to confirm logistics, layout, and support needs for Operation Secure Saint Paul.

- **Finalized readiness of venue and staffing model.**
- **Employees were paid on schedule despite ongoing system disruptions.**



Our Response Timeline

Day 16 | Aug 9
READY FOR OPERATION SECURE SAINT PAUL

Final preparations began at Roy Wilkins Auditorium to stage equipment, stations, and logistics for Operation Secure Saint Paul.

- **Venue fully outfitted with IT and operational support infrastructure; Guard and City teams confirmed readiness for employee resets.**

Day 17 | Aug 10
OPERATION SECURE SAINT PAUL STARTS

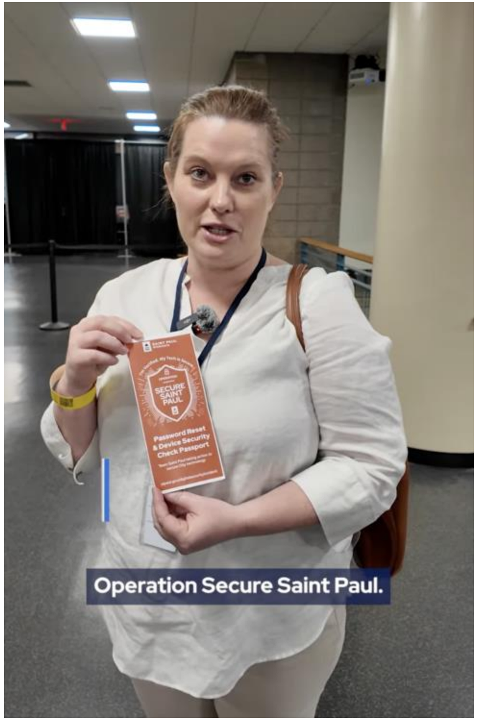
First day of in-person employee password resets and device security scans. Large volumes of staff successfully processed.

- **Nearly 1,000 employees verified, reset, and scanned; processes validated as efficient and secure**

Day 18 | Aug 11
THREAT ACTOR EXPOSES DATA; OPERATION CONTINES

Threat actor released data after the City refused to pay ransom.

- **Mayor Carter updated the public at a press conference.**
- **Public disclosure made; review/notification process initiated in line with legal and regulatory requirements.**



Operation Secure Saint Paul.

Our Response Timeline

City of Saint Paul

Day 19 | Aug 12
OPERATION SECURE SAINT PAUL COMPLETED

Large-scale employee resets and device scans continued at Roy Wilkins Auditorium, wrapping up the planned multi-day event.

- **By the close of OSSP, more than 3,000 employees had completed password resets and endpoint detection installs, significantly increasing network security coverage.**

Day 20 | Aug 13

OPERATION SECURE SAINT PAUL DEMOBILIZED

Modified OSSP remained open for employees who missed their scheduled reset and vendors who are on City network

- **Relocated ongoing OSSP support to City Hall to accommodate new and returning staff.**

Day 21 | Aug 14
NATIONAL GUARD COMPLETES MISSION

After 17 days of continuous support, the Minnesota National Guard's Cyber Protection Team formally completed its mission in Saint Paul.

- **Guard demobilized following successful deployment of endpoint detection across City devices and critical support for OSSP.**

I just wanted to stop by and say how much I appreciate you guys.

Our Response Timeline

Day 22 | Aug 15

SYSTEMS RESTORATION

With the Minnesota National Guard mission complete, City IT and partner teams assumed full responsibility for continuing recovery and security operations.

- **City-led teams sustained endpoint monitoring, device compliance checks, and service restoration under the Incident Command structure.**

Day 23 | Aug 16

SYSTEMS RESTORATION

Departments reported progress reconnecting to applications and network services. City reached a steady operational rhythm with password resets, device protections, and service testing integrated into normal support workflows.

- **City IT and vendors validated systems for phased reactivation while maintaining strict security protocols.**

Day 24 | Aug 17

SYSTEMS RESTORATION

Our Response Timeline

City of Saint Paul

Day 25 | Aug 18

SYSTEMS RESTORATION

With staff secured and network protections in place, the City focused on stabilizing core services and supporting employees through ongoing recovery.

- **Incident Command transitioned all-employee updates to a twice-weekly cadence, underscoring that recovery had entered a structured, sustained phase.**

Day 26 | Aug 19

SYSTEMS RESTORATION

Departments continued phased service restoration, working closely with City IT to validate and bring applications back online.

- **City IT coordinated testing and documentation to ensure systems met heightened security standards before reactivation.**

Day 27 | Aug 20

SYSTEMS RESTORATION

The City re-established email connectivity with key partners after providing independent attestation of the security of its Microsoft 365 environment.

- **Attestation, signed by a nationally recognized incident response firm, reassured partners that the City's systems were secure—marking a milestone of recovery.**
- **Saint Paul Emergency Management sent attestation through MN Fusion Center to elevate urgency.**

SAINT PAUL
MINNESOTA

CITY OF SAINT PAUL
OFFICE OF MAYOR MELVIN CARTER

15 W. Kellogg Blvd,
Saint Paul, MN 55102
Tel: 651-266-8510

Digital Security Incident Timeline

Key Dates

- July 25 – Initial detection of suspicious activity on SPRWS backup server flagged by endpoint detection
- July 26 – Engaged Moxfive as incident response vendor
- July 27 – Disabled VPN access for most staff (exception: public safety/CJIS)
- July 28 – Attempted encryption activity triggers defensive shutdown of City network; Emergency Operations Center activated
- July 29 – Mayor declares local state of emergency; Governor Walz issues Executive Order deploying Minnesota National Guard
- July 31 – Microsoft 365 environment confirmed clean internally; customer service hotlines reestablished via Zendesk
- August 1 – National Guard deployed into City facilities to assist with endpoint detection installations; City Council extends local emergency
- August 3–6 – Operation Secure Saint Paul (OSSP) planning sessions with departmental leaders
- August 7 – OSSP formally announced to all staff; held at Roy Wilkins Auditorium
- August 8 – Payroll successfully deployed on schedule; final OSSP planning walkthrough at venue
- August 10–13 – Operation Secure Saint Paul: more than 3,000 employees reset and scanned; Aug. 13 final vendor/staff day
- August 14 – Minnesota National Guard completes 17-day mission, demobilizes
- August 18 – Credential resets and device scans move to City Hall Room 68 for new hires and remaining staff
- August 20 – City issues attestation confirming Microsoft 365/email environment secure for partner reconnection

Detailed Timeline

July 25, 2025: Suspicious activity first detected

Suspicious activity was first detected at Saint Paul Regional Water Services (SPRWS). Endpoint detection flagged unusual behavior on a backup server tied to privileged service accounts with elevated access.

- Immediately secured compromised accounts and isolated affected servers.
- Proactively restricted access to targeted internal systems.

July 26: Engaged cybersecurity incident response vendor support.

We engaged an external cybersecurity vendor to support ongoing containment and forensic investigation efforts.

- Continued to take significant and proactive steps to defend digital infrastructure and limit the impact of this incident over the weekend.

July 27: VPN Disabled

As part of our defensive strategy, we temporarily disabled VPN access for most users to reduce risk while we continued our investigation.

- Exception for public safety and CJIS users

July 28: Attempted Encryption and Network Shutdown

The threat actor attempted encryption of virtual servers. City leadership took decisive action.

Defensive shutdown of City network. More aggressive action (the current digital security incident) was taken by threat actors, prompting a swift and decisive decision to successfully shut down their access. We initiated a full network shutdown to contain the threat.

EOC activated. City teams worked with cybersecurity response partners to assess, contain, and begin recovery and coordinate communications.

July 29: State of Emergency Declared

Mayor Carter issued emergency declaration. We asked for the support of our local, state, and federal partners—including the Minnesota National Guard, FBI, and national cybersecurity experts—who began working alongside us to investigate, contain, and recover from this incident.

Gov. Walz issues Executive Order 25-08 authorizing the Minnesota National Guard to assist Saint Paul in responding to the July 25 cyberattack by deploying personnel, equipment, and resources to maintain essential city services.

Emergency response and payroll. We worked from the beginning to ensure our emergency services remained fully operational, and that we were able to continue with payroll for our employees.

July 31

Completed full scan of Microsoft 365. Received critical assurance that our Microsoft environment was clean, as we moved into the next stage of restoration.

Transferred critical customer service operations to ZenDesk. We were able to begin setting up temporary customer service phone numbers through ZenDesk. This is allowing residents to reach us by phone while we work to bring our City phone system back online. We are still encouraging residents to use email for quicker response times.

August 1: National Guard Deployed to City Facilities

Began deployment of new security software. OTC and the National Guard began installing enhanced security controls across all City devices. As of August 6, we currently at 81% completion of this effort.

City Council unanimously voted to extend Mayor Carter's local state of emergency for 90 days in response to the ongoing digital security incident. This action ensures the City can continue mobilizing local, state, and federal resources to protect essential services and support the coordinated investigation and recovery.

August 3: Planning Begins for Operation Secure Saint Paul

Conducted initial planning session for Operation Secure Saint Paul. Brought together leaders from every City department to begin coordinating a citywide password reset for all employee credentials and a device security checkup.

August 4

Deployed additional employees for customer service. We began onboarding additional employees to serve in customer support roles as we bring critical customer-facing phone lines online through ZenDesk.

August 5

Groundwork Completed for Full SPPD CAD Access. All squad Mobile Data Terminals – the in-squad computers that allow officers to securely access dispatch information, run license plates, and communicate with dispatch – now meet the security requirements to reconnect to the Computer-Aided Dispatch (CAD) system.

500 Vendors Enrolled for Secure ACH Payments. The Office of Financial Services sent PaymentWorks registration links to 2,000 vendors. As of August 6, more than 500 vendors have completed registration and are now able to receive payments via ACH.

Successful Payroll Test. We successfully transferred a test file to US Bank. This is an incredibly important milestone. We continue to be on track for payroll on Friday.

The Ramsey County Board of Commissioners voted today to issue a Local State of Emergency as the City continues our incident response. This declaration will allow the County to request additional state and federal assistance and provide increased support to constituents.

August 6

Anticipated Full Completion for SPFD CAD Access. By EOD, all SPFD Mobile Data Terminals will have full CAD access.

Reconvened Full Planning Team for Operation Secure Saint Paul (OSSP). We met again with representatives from each department to finalize logistics for our citywide password reset and device security checkup.

Anticipated Communications for OSSP. We plan to share details with City staff later today, following our second planning session with the full Operation Secure Saint Paul team.

August 8: Payroll Delivered On Time Despite Incident

The City successfully processed and delivered payroll on time for all employees, demonstrating resilience even while core systems remained offline.

- Completed payroll transmission through a secure, clean environment.
- Distributed printed pay statements as digital access remained limited.
- Final planning walkthrough held at Roy Wilkins Auditorium for OSSP.

August 9: Full Setup for Operation Secure Saint Paul

Roy Wilkins Auditorium was converted into a secure reset and device upgrade center—the largest coordinated cybersecurity event in City history.

- Completed technical setup of reset stations, wired connections, and security scanning equipment.
- Trained staff and Minnesota National Guard teams on intake, credential verification, and device scanning protocols.
- Communicated final instructions to staff citywide, including Everbridge enrollment and out-of-office guidance.

August 10-13: Operation Secure Saint Paul Executed

Thousands of City employees reset their credentials and secured their devices in-person, closing a critical security gap.

- Nearly 1,000 employees completed resets and device scans on day 1.
- Installed advanced endpoint protection across nearly all City devices.
- Coordinated logistics across departments to ensure shift coverage while employees attended OSSP.
- Provided Everbridge emergency notifications to all subscribers while Microsoft Outlook/Teams were temporarily offline.

August 11: Threat Actor Data Exposure Disclosed

Because the City refused to pay ransom, the threat actor released a limited amount of employee-related data.

- Publicly disclosed the exposure during an IC update and press briefing.
- Launched forensic review of exposed files to identify impacted individuals.
- Directed HR to provide 12 months of free credit monitoring and identity theft protection to all employees.
- Reaffirmed commitment to transparency and ongoing notifications.

August 13: Operation Secure Saint Paul Concludes

The City concluded its mass credential reset and device security event.

- Extended access for employees and vendors who missed earlier sessions.
- Transitioned reset operations to City Hall for late-returning staff.

August 14: National Guard Completes Mission

The Minnesota National Guard Cyber Protection Team completed their 17-day mission and demobilized.

- Guard provided endpoint security installation, Microsoft system hardening, and technical surge capacity.
- Mayor Carter and City leadership issued public thanks for their expertise and partnership.
- Transitioned Guard responsibilities back to OTC and contractors as recovery continued.

August 15-17: Shift from Emergency to Recovery Operations

With OSSP completed and Guard support winding down, the City moved from emergency response into the recovery phase.

- Incident Commander Jaime Wascalus announced a shift to critical restoration and recovery operations.
- Reduced IC update cadence from daily to twice-weekly (Monday/Friday).
- Began methodical system clearance and staged restoration process.

August 18: Recovery Operations Continue at City Hall

OSSP reset operations transitioned from Roy Wilkins Auditorium to City Hall for ongoing staff and new hires.

- Opened City Hall Room 68 (Studio) for walk-in resets and device scans.
- Established sustained recovery process with identity verification, MFA enrollment, and software checks.
- Reiterated that full service restoration requires 95% device completion

August 20: Attestation Confirms M365 Security

The City formally confirmed its Microsoft 365 and email environment as secure, allowing partners to reconnect with confidence.

- Issued a formal security attestation signed by the City's independent incident response vendor.
- Shared attestation with key partners including Ramsey County.
- Partners reconnected email and communications systems following confirmation.

###

OFFICE OF MAYOR MELVIN CARTER

CITY OF SAINT PAUL

390 City Hall
15 Kellogg Boulevard West
Saint Paul, Minnesota 55102

August 26, 2025

Major General Shawn Manke
The Adjutant General
Minnesota National Guard
20 12th Street West
Saint Paul, MN 55155

Major General Manke,

On behalf of the City of Saint Paul, I want to express our deepest gratitude to you and the Minnesota National Guard's Cyber Protection Team for the invaluable contributions during the recent ransomware attack against our city's information infrastructure. This partnership was essential to our investigation, response, and restoration efforts.

It is clear the Minnesota National Guard stands ready to serve not only in times of natural disaster or national security threats, but also in defending the digital frontlines of our local communities.

Throughout their 17-day deployment, all 34 Guard members assigned to this mission stood in lockstep with our administration and displayed extraordinary commitment to supporting our Office of Technology and Communications and Emergency Management teams. They strengthened the efforts of our technical teams, and their expertise was instrumental in helping us reach this pivotal point in our recovery. Most importantly, their support ensured our emergency response services, and city payroll continued uninterrupted.

Operation Secure Saint Paul was the foundation of our response, a three-day event that guided nearly 3,000 employees through the critical process of resetting their credentials and securing their devices. Guard members arrived early, stayed late, and calmly assisted employees. They understood that the success of this event was mission critical, and they helped us make that happen.

There were numerous examples when Guard members went above and beyond to support our teammates, but one instance in particular truly demonstrates this commitment. After leaving the first day of Operation Secure Saint Paul event, Major Luke Voeller was flagged down by a Saint Paul Police officer. Instead of going home following his 16-hour day, Major Voeller assisted the officer in his squad car to ensure he could access the critical emergency software on his squad computer.

Beyond the technical accomplishments, the Guard's presence brought something equally important: a unifying sense of safety and support the kept our teams engaged, focused, and confident that we were moving in the right direction.

Saint Paul is stronger, safer, and better prepared today because of your team's dedication. Not only have we strengthened our ability to defend against future threats, but it also provides a foundation for how we can move forward together as a more resilient Minnesota.

With sincere appreciation,

Mayor Melvin Carter

CC: Governor Tim Walz
Lt. Governor Peggy Flanagan
Brigadier General Simon Schaefer
Chief Master Sgt. Lisa Erikson
LTC Brian Morgan