

Lessons Learned from a Ransomware Incident

We hear about destructive ransomware in the news almost daily, with major organizations suffering from debilitating ransomware attacks. This program goes into an actual ransomware incident from 2023 and steps that were taken to recover from the incident, both organizationally and technologically. We will discuss what we learned that can help you protect against attacks in the future, and what to do to recover when the worst happens.

Join Camden County Assignment Judge Deborah Silverman Katz and Judiciary Chief Information Security Officer Sajed Naseem on this timely presentation.

Speakers:

Hon. Deborah Silverman Katz, A.J.S.C., Camden
Sajed Naseem, Chief Information Security Officer
Administrative Office of the Courts, Trenton



Lessons Learned from a Ransomware Incident

Judge Silverman Katz and Sajed Naseem, CISO
New Jersey Judiciary

Information Security Triad
Confidentiality, Integrity, Availability

August 2023

Imagination is more important than knowledge. For knowledge is limited to all we know and understand, while imagination embraces the entire world, and all there ever will be to know and understand.

A vivid imagination frees you from the bounds of deductive reasoning, he liked to say. The truly creative and innovative are not stymied by an unclear path or lack of knowledge, they imagine the goal, what they want to achieve, and then build the path to it.

- Albert Einstein

Roles and Responsibilities

- How did we get to this role?
- Judge Silverman Katz: point person from the vicinage during the ransomware attacks:
- **R. 1:33-4 (a)** “The Assignment Judge shall be the chief judicial officer within the vicinage, and shall have the plenary responsibility for the administration of all courts therein, subject to the direction of the Chief Justice and the rules of the Supreme Court.”
- **R. 1:33-4 (b)** “The Assignment Judge shall be the authorized representative of the Chief Justice for the efficient and economic management of all courts within the vicinage. The responsibilities of the Assignment Judge shall also include all such matters affecting county and municipal governments, including but not limited to budgets, personnel, and facilities.”
- Outreach from the County- told of potential attack
- Outreach to stakeholders- brought them into the information group, to determine what was at risk, who needed to be informed, what needed to be done
- Outreach to the AOC- Director Grant and SN, copy to the CJ

Roles and Responsibilities

- Chief Information Security Officer (CISO)
- Saturday morning text message
- Outreach from the AJ
- CISO discussed situation with internal teams
- AOC, AJ and Internal teams met to discuss situation
- AOC was responsible for protecting the network
- AJ was responsible to ensure that County staff have a temporary place to work (paper and 5th floor of Camden vicinage)

Incident Response (Partial Timeline)

April 1: Received a text message that Camden Metro PD had a ransomware and another ransomware variant hit the Prosecutors Office

April 1: Received a message that an IP was trying hundreds of userID on Judiciary VPN

April 6: Call with Camden Metro PD at 6:30pm to discuss the situation. Ransomware is called “***X ransomware***.” This was also a former “zero day” vulnerability which was exploited

April 7: Judiciary call at 9am with Judge Grant

April 8-9: Enabled few users for Camden Metro PD

April 10: Call with Camden County Prosecutor’s Office to discuss the situation. ***No name of ransomware.***

April 11: Judiciary determined that name of the ransomware to assist forensics.

April 12: Camden vicinage setup Camden County Prosecutor’s Office staff in Judiciary space in the courthouse with eCourts access.

April 6-April 13: Significant collaboration within Judiciary

New Jersey Judiciary

Confidential \ Judiciary Employees Only

How to respond to crisis with varying opinions?

- **Vicinage Initial Roles**
 - Meetings with AJ and County Stakeholders (County Administration, Metro Administration, CCPO, Vicinage Personnel, AOC)
 - Education about what exactly was going on (what is ransomware, what was at risk, what systems were potentially involved, how to best protect judiciary)
 - Vicinage Meetings (TCA, Division Managers)
 - All Stakeholder Meetings
- **Information Gathering at the Vicinage Level**
- **Information Gathering at the AOC Level**
- **Vicinage and AOC collaboration**
- **Stakeholder Collaboration**
 - Control of the meetings
 - Control of the direction
 - Differing opinions

Technology Questions

- Network connections (Judiciary, Third Party, Inter-governmental)
- Work and home devices were in scope
- Forensic report
- Infrastructure upgrades
- Unknown issues
- Running the organization

Leadership and Management Questions

- Who will set the strategy (business and technology)?
- Who will make the unpopular decision?
- Who will say “I don’t know” and will find out the answers?
- Who will focus on the goal during differences of opinion?
- Leaders (direction) and managers (process driven) may be different

Lessons Learned (taking responsibility for errors we create)

1. **Judiciary leadership:** we will shutdown all connection to a compromise account and/or locations (partner offices, third party vendors)
2. **Cyberattacks related to New Jersey Judiciary partners (police departments, law firms, prosecutor, intergovernmental partners):** cyberattacks at partners could cause serious harm to the Judiciary. They may have several technological connections to the Judiciary.
3. **Technology:** Judiciary may stop all or partial connections to and from the compromised partner including third party vendors (*this could include blocking IPs, emails, eCourts, file transfer, cloud*)
4. **Help Desk:** notified to not enable any users from the partners during a cyberattack
5. **Alternative work location (physical or virtual):** we may choose to provide an alternative work location (like at Camden Vicinage for Camden Prosecutor)
6. **Judiciary electronic communication:** encrypted and confidential
7. **Confidentiality:** users are required to be in a confidential work area (*please note that 16 minutes after the April 6th call, news outlets reported the ransomware*).
8. **Certification:** from leadership and/or attorney is required before opening connections. This will include a legal and technological assessment.

News Report

- Few minutes after our meeting on April 6, news report came out (we are in real life)

4 NEW YORK
CYBERATTACK

LOCAL WEATHER INVESTIGATIONS BAQUERO VIDEO TV LISTINGS OUR VOICES NEWSLETTERS

77° LW

Ransomware Attack at NJ County Police Department Locks Up Criminal Investigative Files

Sources familiar with the matter said the hackers were demanding hundreds of thousands of dollars to unlock the files as a result of the malware.

By Jonathan Dienst • Published April 6, 2023 • Updated on April 7, 2023 at 7:11 pm



Trending Stories

NASSAU COUNTY

Alleged drunk driver smashes into Ferrari on Long Island, killing couple: Police

NASSAU COUNTY

Driver was high, going 120 mph before Long Island crash that killed dad, 2 kids: Cops

TRAVEL

Need a passport in a hurry? Here's how to speed up the renewal process

NYPD

Cyclist run down by driver fleeing NYC police chase

New Jersey Judiciary

Confidential \ Judiciary Employees Only

Ransomware - Aftermath



Author: Joseph Cheng, CISA, CISSP, CPM, MACIS
Date Published: 7 October 2022

The Social and Psychological Consequences of Ransomware Attacks

The Register

New York county still dealing with ransomware eight months after attack

Also: Covid-19 no issue, Edinboro fined more than it can pay, UK to A1 (in CC:Jeff), and the world's CRITICAL infra.

[View Article](#) [Print Article](#) [Share Article](#)

SECURITY IS KEY The fallout from an eight-month-old cyber attack in a county in Long Island, New York, has been described as "fruit-rotting" as leaders try to make sure it isn't spreading.

Suffolk County will tell with a memorandum dated in early September 2022, which led county executive Steven Bellone to issue [this press release](#) on Sept. 14, 2022. It's the latest public-facing document about the ransomware attack.

Belmont officials said Belmont has the state of emergency in Suffolk County, and county legislators have introduced a resolution to increase the county's disaster fund. In Suffolk County, a state of emergency gives executives the ability to use state resources and the state without legislative approval.

Belmont said the plan is to continue to support Suffolk County chief of Police Police Captain William J. Bellone and his team working on the 11th floor of the county seat on Hempstead St. 11th floor was closed down by the state office building.

New Jersey Judiciary

Confidential \ Judiciary Employees Only

Social and Psychological Impacts

The social impacts of ransomware attacks can cause lasting damage to an enterprise, its customers and its employees. Social impacts can occur when service is disrupted. For example, because affected enterprises have to shut down operations, their employees may be temporarily laid off, which increases unemployment and can lead to financial stress.

There are strong associations between higher levels of financial stress and increased alcohol consumption, which can lead to other negative effects. Victimization can also cause individuals to be unwilling to adopt new technologies in the future, leading to people losing confidence in businesses and governments.

There is also a wide range of psychological responses to ransomware attacks. In many cases, victims respond more negatively to the effects of the attack than the attack itself, and each individual handles the threat of a cyberattack differently. Some may proactively face the problem while others may exhibit protective or avoidance behaviors to prevent attacks.

Following ransomware attacks, people may feel fear, worry, disappointment, frustration, distrust and helplessness. This can lead to long-term psychological consequences such as depression, panic attacks and post-traumatic stress disorder. Guilt and shame are also compounded when victims are blamed by their organization, family members or society for falling victim to the attack.

Although there is some acknowledgment of these impacts in the literature, few reports evaluate all damages—whether they be financial, reputational, social or psychological. In the current enterprise reporting regime, the social and psychological impacts on victims have been largely overlooked and unreported. This can be attributed to lack of awareness and lack of a reliable and standardized method to evaluate and monetize the impacts.

Conclusions

- During a crisis, you may have varying opinions
- The human factor is important as people want to work together but also want to get back up and running
- Leadership will need to make unpopular decisions
- You may start to identify leaders who otherwise may not have the title of “leader”
- Knowing each member of your team and engaging with your team
- The work is data-driven, and risk-based (*should we open connections or should we leave them closed?*)
- Assign different people to lead the varies teams (AOC, Vicinage, technology)
- Meet often and keep communication confidential but transparent

Q & A

New Jersey Judiciary

Confidential \ Judiciary Employees Only

Independence Integrity Fairness Quality Service

Acknowledge and enhance the potential of every person in our organization to contribute to the administration of justice through participation, training, and technology.

New Jersey Judiciary

Sajed Naseem

Confidential \ Judiciary Employees Only

About the Panelists...

Sajed (“Saj”) Naseem is Chief Information Security Officer (CISO) of the New Jersey Judiciary in Trenton, New Jersey, and has more than 20 years of experience with information technology and information security across many industries.

As the CISO of the New Jersey Judiciary, Mr. Naseem has focused on cybersecurity readiness and performance, information governance and network security. He is also an Adjunct Professor at St. John’s University.

Mr. Naseem received his undergraduate degree from Stony Brook University and his Masters degrees from St. John’s University and Columbia University.

Honorable Deborah Silverman Katz, AJSC is Assignment Judge, Camden Vicinage, Superior Court of New Jersey, and sits in Camden, New Jersey. She was appointed to the court in 2008 and reappointed in 2015.

Prior to her appointment to the bench, Judge Katz served as Assistant Camden County Counsel from 1997-2008. Prior to that she was Assistant Counsel to the Pennsylvania Supreme Court’s Office of Disciplinary Counsel.

Judge Katz received her undergraduate degree from Adelphi University and her J.D. from Hofstra University School of Law.