tracesecurity

Practical, worry-free cybersecurity.

Cyberattacks on the Louisiana Government and How To Avoid Them!

Vikash “Vik” Ramnanan

What are we going to cover?

- What is Ransomware and why is it a problem?
- Louisiana Government Hacks Overview
- Ransomware Prevention and Responses

About TraceSecurity

Who we are and what we do.

- We are a cybersecurity company founded in 2004.

- We deliver services to cater to each client’s size and complexity.

- Headquartered in Baton Rouge, Louisiana with approximately 80 employees.

Ooops, your files have been encrypted!

Ransomware

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Copy

Check Payment

Decrypt

Close to Home

Governor declares state of emergency after ransomware attack on Louisiana

- Issue drivers' licenses
- Renew vehicle registrations
- Apply for food stamps
- Report child abuse
- Check election results

State of Louisiana

EXECUTIVE DEPARTMENT

PROCLAMATION NUMBER 115 JBE 2019

STATE OF EMERGENCY – CYBERSECURITY INCIDENT

WHEREAS, the Louisiana Homeland Security and Emergency Assistance and Disaster Act, La. R.S. 29:721, *et seq.*, confers upon the Governor of the State of Louisiana emergency powers to deal with emergencies, including those caused by breach of cybersecurity, in order to ensure that preparations of this State will be adequate to deal with such emergencies or disasters and to preserve the lives and property of the people of the State of Louisiana;

WHEREAS, when the Governor determines that an emergency has occurred, or the threat thereof is imminent, La. R.S. 29:724(B)(1) empowers the Governor to declare a state of emergency by executive order or proclamation, or both;

WHEREAS, there have been severe, intentional cybersecurity breaches in the Sabine, Morehouse, and City of Monroe school systems that may potentially compromise other public and private entities throughout the State of Louisiana;

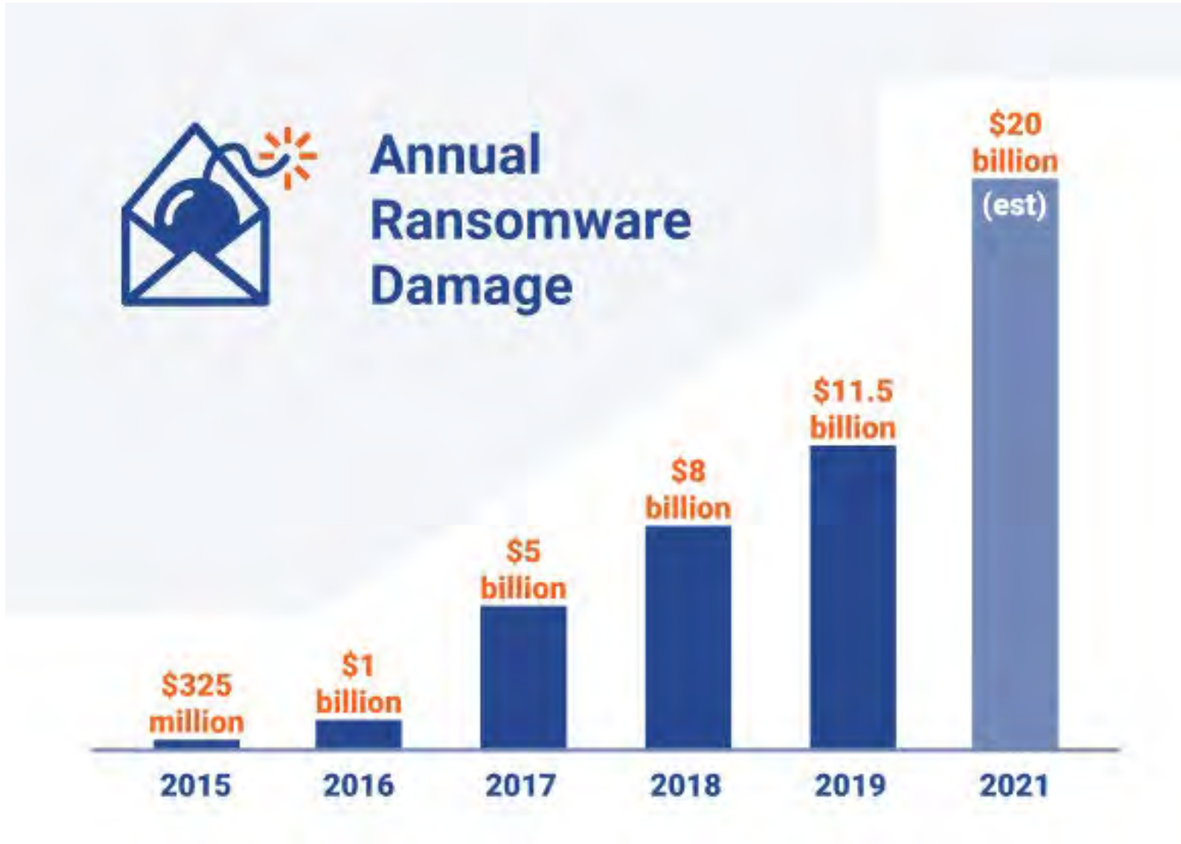
WHEREAS, there is significant risk that this emergency is ongoing; and

WHEREAS, the State anticipates various state agencies and political subdivisions will need to work cooperatively to mitigate any damage, current or future, as a result of these cybersecurity breaches.

Ransomware

Scope of the Problem

- FBI estimated that $140m has been paid to ransomware operators over the past six years[1].
- Ransomware attackers collected an average of around $84,000
- Estimates put the cost of 2019's ransomware incidents in excess of $11.5 billion.
  - Data loss
  - Operation Downtime
  - Resetting and replacing infrastructure
  - Productivity
  - Forensics
  - Reputation
  - Life



Security Awareness Training

- User Training
  - 95% of cybersecurity breaches due to human error
  - Common methods of introducing ransomware is via a link in an email, text message, or social media post.
  - Ransomware is then downloaded to the target's device and spreads through the network and files.
  - Its more important than ever for your employees to be aware of the latest cybersecurity threats.

Least Privilege & Separation of Duties

- Separation of Duties
  - Identify what is needed for each role and only allow access for those services
  - Use security groups or rules bases system

- Least Privilege
  - Restrict users' permissions to install and run unwanted software applications
  - Configure access controls-File, Directory and Network Share permissions
  - This is an ongoing process that should be evaluated regularly.

Network Hardening

- Network Hardening
  - Your network should be segmented logically and physically.
  - Disable unnecessary ports and close off RDP access from the Internet, RDP compromise is the primary attack vector in 59% of attacks
  - Software Whitelisting/Blacklisting
  - Use and maintain preventative software programs.
    - Antivirus software
    - Firewalls
    - Email Filters, Spam Filters , DMARC Policy

Patch Management

- Patch Management
  - Develop a patch management program, "Patch Early and Patch Often" to close known vulnerabilities.
  - Patches can be managed and applied manually or handled with a solution (ex. Windows Server Update Services (WSUS)).
  - Build redundancy into the infrastructure
  - Include all devices connected to the network

Security Testing

- Social Engineering Testing
  - Phishing, Vishing and Smishing
  - Physically test proper visitation procedures
- Penetration Testing
  - The goal for these engagements is to find vulnerabilities and attempt to exploit them to see what data or systems can be compromised or manipulated.
- Regularly Assess the Network
  - Conduct periodic Risk Assessments and have a defined vulnerability management plan

Backing Up Data

- Backup Data
  - Develop a backup plan
  - Backup frequently to meet your Recovery Point Objective
  - Utilize an offsite backup
  - Ensure that backups are safeguarded and only available to authorized personnel

Incident Response & Lessons Learned

- Incident Response Plan
  - Have a plan in place and test that plan regularly
  - Define an Incident Response Team and specific response procedures for ransomware
  - Outline Containment, Eradication, and Recovery for the affected system and notify law enforcement
  - Lessons Learned

Most Companies Overestimate Their Cybersecurity Posture, but Resilience Is Possible

- Get in front of the problem
- Assess your current vulnerabilities
- Determine future steps

Do you know what you would do if affected by a ransomware attack?

tracesecurity

Practical, worry-free cybersecurity.

Questions?

Contact us for more information about this webinar!

vikashr@tracesecurity.com | 225-612-2121 | www.tracesecurity.com