TOP 10 CYBERSECURITY TRENDS: BASED ON RECENT NC PUBLIC SECTOR CYBER INCIDENTS

SHANNON TUFTS, PHD
UNC SCHOOL OF GOVERNMENT
NCLGISA CYBERSECURITY STRIKE TEAM , NC JCTF

IT Strike Team

Significant Cyber Incident Statistics

- Significant cyber attacks happen every 14 seconds
- Increase of 350% since 2018

NC Public Sector Statistics

- 2019: 10 (reported) significant cyber incidents
- 2020,: 24 significant cyber incidents
- 2021: 20+ significant cyber incidents
- 2022: 9 significant cyber incidents as of March 30, 2022
- Downtime from significant cyber incidents increased 200 percent

AVERAGE BREACH STATISTICS

- Less than 50% of breaches get detected internally
- ~191-197 days to ID a breach
- ~ 66-69 days to contain it
- Average recovery takes 6-9 months
- Most entities only recover 80% of data/functionality due to encryption
- Typically takes 16.7 days to bring network back up in most limited way

TOP 10 TRENDS

NEW NC LEGISLATION RELATED TO CYBER SECURITY INCIDENTS & RANSOM PAYMENTS

G.S. 143B-1320, AMENDED BY SL2021-180

G.S. 143B-1379(C), AMENDED BY SL2021-180

G.S. 143-800, AMENDED BY SL2021-180

ARTICLE 84, VARIOUS TECHNOLOGY REGULATIONS.

GS143-800: STATE ENTITIES AND RANSOMWARE PAYMENTS.

(a) No State agency or local government entity shall submit payment or otherwise communicate with an entity that has engaged in a cybersecurity incident on an information technology system by encrypting data and then subsequently offering to decrypt that data in exchange for a ransom payment.

(b) Any State agency or local government entity experiencing a ransom request in connection with a cybersecurity incident shall consult with the Department of Information Technology in accordance with G.S. 143B-1379.

(c) The following definitions apply in this section:

(1) Local government entity. – A local political subdivision of the State, including, but not limited to, a city, a county, a local school administrative unit as defined in G.S. 115C-5, or a community college.

CYBERSECURITY INCIDENT REPORTING REQUIREMENT

G.S. 143B-1379(C), AMENDED BY SL2021-180

(c) Local government entities, as defined in **G.S. 143-800(c)(1)**, shall report cybersecurity incidents to the Department. Information shared as part of this process will be protected from public disclosure under G.S. 132-6.1(c). Private sector entities are encouraged to report cybersecurity incidents to the Department.

GS143-800(c)(1): Local government entity. – A local political subdivision of the State, including, but not limited to, a city, a county, a local school administrative unit as defined in G.S. 115C-5, or a community college.

A SIGNIFICANT CYBERSECURITY INCIDENT…

- **G.S. 143B-1320(a)(14a)** Ransomware attack. – A cybersecurity incident where a malicious actor introduces software into an information system that encrypts data and renders the systems that rely on that data unusable, followed by a demand for a ransom payment in exchange for decryption of the affected data.

- **G.S. 143B-1320(a)(16a)** Significant cybersecurity incident. – A cybersecurity incident that is likely to result in demonstrable harm to the State's security interests, economy, critical infrastructure, or to the public confidence, civil liberties, or public health and safety of the residents of North Carolina. A significant cybersecurity incident is determined by the following factors:

  a. Incidents that meet thresholds identified by the Department jointly with the Department of Public Safety that involve information: 1. That is not releasable to the public and that is restricted or highly restricted according to Statewide Data Classification and Handling Policy; or 2. That involves the exfiltration, modification, deletion, or unauthorized access, or lack of availability to information or systems within certain parameters to include (i) a specific threshold of number of records or users affected as defined in G.S. 75-65 or (ii) any additional data types with required security controls.

  b. Incidents that involve information that is not recoverable or cannot be recovered within defined timelines required to meet operational commitments defined jointly by the State agency and the Department or can be recovered only through additional measures and has a high or medium functional impact to the mission of an agency

WHO YOU GONNA CALL?

NC Joint Cyber Task Force (JCTF)

State & Local Partners

NC National Guard G6
NC DIT
NC DPS
NCEM Cyber Unit
NC ISAAC
NCLGISA Cyber Strike Team

Federal Partners

FBI
USSS
DHS-CISA

Other Partners Based on Event

911
NC SBI
SBoE
DHHS
DPI
MCNC
NC Community College System

METHODS OF CONTACT TO REPORT CYBERSECURITY INCIDENT

- **NC EM 24 Hr Watch: 800-858-0368 (monitored 24/7)**
- **NCLGISA Strike Team: itstriketeam@nclgisa.org or (919) 726-6508 (monitored 24/7)**
- **FBI IC3: https://www.ic3.gov/**
  - If you have a situation involving financial fraud,please contact the FBI first because there is a ~72 hour window for fund recovery before it is moved off-shore.
- **NCDIT:** https://it.nc.gov/resources/cybersecurity-risk-management/statewide-cybersecurity-incident-report-form

2


SOCIAL
ENGINEERING
The clever manipulation
of the natural human
tendency to trust.

CYBER SECURITY KNOWLEDGE

What does the https:// at the beginning of a URL mean?

1. The site has special high definition
2. The information entered into the site is encrypted
3. The site is the newest version available
4. The site is not accessible to certain computers
5. I have no clue!

All Financial, PII, PHI (and more) Collections Must Use HTTPS://

RECOGNIZE THESE?

- What was your favorite teacher's name?
- What was the name of your childhood pet?
- What was your childhood best friend's name?
- What was the first car you had?
- Where were you born?
- What was the name of your high school?

SPREADING HOLIDAY CHEER!

Voice Phishing Example

CYBER SECURITY KNOWLEDGE

Does Amazon, Apple, Facebook, or the IRS ever call you on the phone unannounced?

NEW (& OLD) METHODS OF ATTACK

DATA EXFILTRATION W/O ENCRYPTION

- Conducted via various tactics, like SQL injections or TA access to data within systems
- Ransom note may be posted but not a normal practice
- Data is either sold on dark web and/or posted publicly for free
- Recent cases indicate the impacted entity was unaware of the data exfiltration until it was found posted on the internet by a 3rd party
- Breach notification may be required depending on the type of data exfiltrated

LEGAL ISSUES WITH DATA EXFIL

- Most agencies don’t have sufficient logging to determine what data was removed
- Hard to validate extent of breach notice requirements

CYBER SECURITY KNOWLEDGE

Criminals access someone's computer and encrypt the files/data. The user is unable to access the data unless they pay the criminals to decrypt the files. This is called:

1. Botnet
2. Ransomware
3. Driving
4. Spam
5. I have no clue!

Pro Tip

Never Pay!

RANSOMWARE: WHAT IS IT?

- Ransomware is a type of malware that attempts to extort money from user or organization by infecting or taking control of the victim's computer, files, servers, etc.
- Ransomware usually encrypts files, folders, machines, servers to prevent access and use unless the ransom is paid to receive the decryption key.
- Data exfiltration has become more widespread as part of ransomware events in the past 16-19 months.

TIMELINE OF A RANSOMWARE ATTACK

Month 1	• An employee opens a phishing email and clicks on a link containing ransomware.
Month 2	• The ransomware downloads onto the employee's computer and starts executing malicious code.
Month 3	• The ransomware creates a connection via the Internet with the threat actor's command and control (C2) server.
Month 4	• The ransomware steals/harvests credentials to gain access to more accounts.
Month 5	• The ransomware looks for files to encrypt on local computers and on servers via the network, moving laterally across the network to compromise multiple accounts. Data exfiltration might also be occurring during this timeframe.
Month 6	• The ransomware starts the encryption process, typically attacking domain controllers and backups first. The government is now aware they have been compromised. The threat actor leaves a ransom note demanding payment in exchange for the decrpytion key.

COMMON ATTACK VECTORS

- Phishing emails loaded w/ malware
- Password brute forcing
- Remote Desktop Protocol
- VPN exploits
- Other unpatched CVEs
  - Microsoft applications
- Outdated infrastructure
- **Open ports per vendor instructions**

CYBER SECURITY KNOWLEDGE

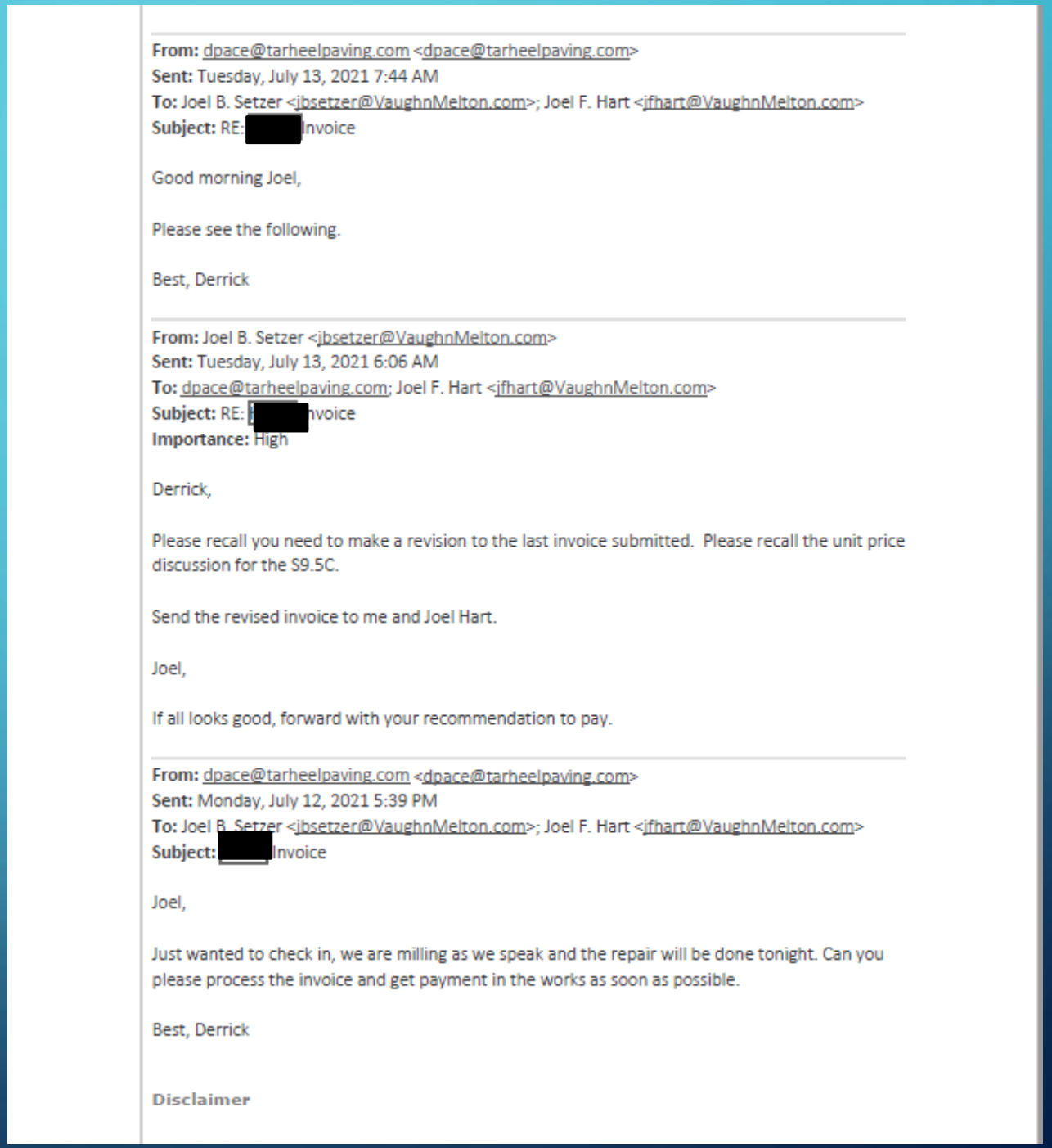
True or False:

A “phishing” email can be used to initiate a ransomware attack.


Business Email
Compromise:
The $9 Billion Security
Threat You Can't Ignore

JUST A NORMAL DAY…

MAKING MOVES, PROCESSING PAYMENTS



From: dpace@tarheelpaving.com <dpace@tarheelpaving.com>
Sent: Tuesday, July 13, 2021 7:44 AM
To: Joel B. Setzer <jbsetzer@VaughnMelton.com>; Joel F. Hart <jfhart@VaughnMelton.com>
Subject: RE: [redacted] Invoice

Good morning Joel,

Please see the following.

Best, Derrick

From: Joel B. Setzer <jbsetzer@VaughnMelton.com>
Sent: Tuesday, July 13, 2021 6:06 AM
To: dpace@tarheelpaving.com; Joel F. Hart <jfhart@VaughnMelton.com>
Subject: RE: [redacted] Invoice
Importance: High

Derrick,

Please recall you need to make a revision to the last invoice submitted. Please recall the unit price discussion for the S9.5C.

Send the revised invoice to me and Joel Hart.

Joel,

If all looks good, forward with your recommendation to pay.

From: dpace@tarheelpaving.com <dpace@tarheelpaving.com>
Sent: Monday, July 12, 2021 5:39 PM
To: Joel B. Setzer <jbsetzer@VaughnMelton.com>; Joel F. Hart <jfhart@VaughnMelton.com>
Subject: [redacted] Invoice

Joel,

Just wanted to check in, we are milling as we speak and the repair will be done tonight. Can you please process the invoice and get payment in the works as soon as possible.

Best, Derrick

Disclaimer

WHAT CAN POSSIBLY GO WRONG?

Joel

JOEL SETZER, PE | OFFICE LEADER | SYLVA NC OFFICE
C: 828.226.9158 | O: 828.477.4993 | www.vaughnmelton.com

DEPENDABLE | PROACTIVE | CREATIVE | EMPATHETIC | CONSCIENTIOUS

P.E. Registration States: NC; KY; TN; GA; SC

From: Derrick pace <dpace@tarhealpaving.com>
Sent: Tuesday, July 13, 2021 9:30 AM
To: Joel B. Setzer <jbsetzer@VaughnMelton.com>
Cc: Joel F. Hart <jfhart@VaughnMelton.com>
Subject: Re: FW[redacted] Invoice

Hi Joel/Hart,

Find the attachment for our new bank details and make sure the payment is sent by ACH or Wire Transfer.

Let me know if you need anything else.

Best, Derrick

On Tue, Jul 13, 2021 at 3:58 PM Joel B. Setzer <jbsetzer@vaughnmelton.com> wrote:

> Joel,
>
> The quantities match the prior invoice. Per your prior email, I am assuming the quantities match your record. Please advise asap if there are any differences.
>
> Seth,
>
> We are hoping to close out the fiscal part of the project to assist with County accounting processes. The last discussions were mid-June. At the time, the concrete had passed testing and we were awaiting the asphalt testing results. Can this be expedited as it is needed to get closure?

SEEMS GOOD TO ME SO LET'S CUT THAT CHECK!

From: Marcus [redacted]
To: Samantha [redacted]
Cc: Randall [redacted]
Subject: FW: Tarheel Invoice - Recommendation to Pay
Date: Friday, July 16, 2021 4:40:25 PM
Attachments: image001.png
Paving & Asphalt Rank Details.pdf

Sam,

Next week we should get the approved invoice from Tarheel for the paving project at Solid Waste. The contractor's payment information is attached and note the highlighted information below from the engineer regarding timing for the work completed; I agree.

Thanks and please let me know if you have any questions,
Marcus

From: Joel B. Setzer <jbsetzer@VaughnMelton.com>
Sent: Wednesday, July 14, 2021 1:34 PM
To: Marcus [redacted].gov>
Cc: Joel F. Hart <jfhart@VaughnMelton.com>
Subject: Tarheel Invoice - Recommendation to Pay

Good Afternoon,

We have evaluated the testing reports on the asphalt pavement. All aspects of the reports indicate full compliance with NCDOT specifications, except the density achieved on the surface (S9.5C) mix. The density requirements for this mix is 92% and they achieved an average of 90.9% on the four areas. Area 1, which carries the highest volume and weight of trucks did get a 92.0% density.

NCDOT does have waivers for "small quantities" which would also apply.

Given that the asphalt is in specifications in all other categories and given the highest volume area is meeting density, it is my recommendation to accept the work and pay Tarheel the invoice.

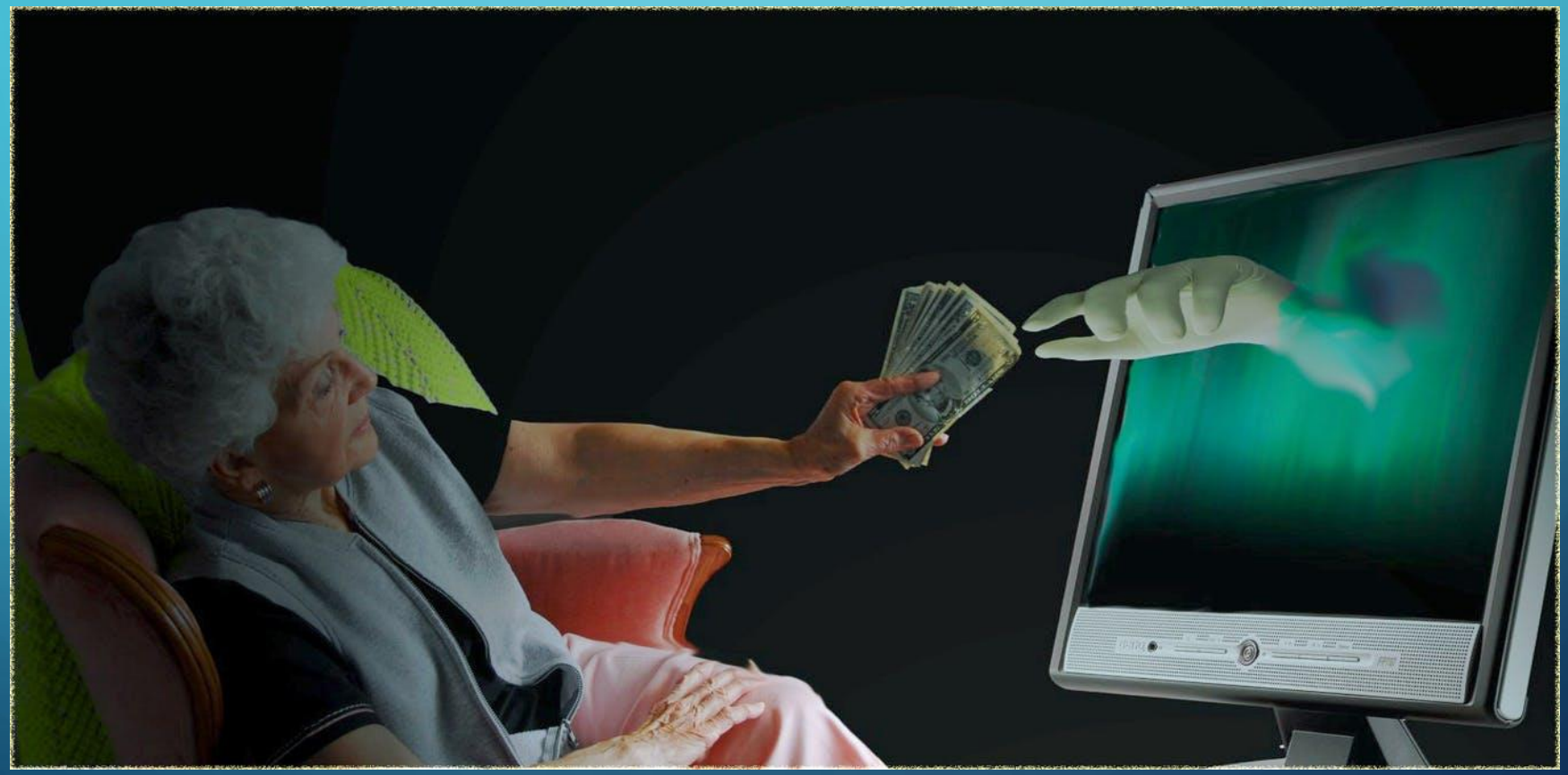
In regards to what was done before June 30 and after, all of this work was done prior to June 30. The slipped area repaired did not create any new pay quantities because it was basically warranty work.

My recommendation is based upon an assumption that the repaired slipped area is still performing well. If it is not, please let me know.

Let me know if we need to discuss any of this information or the recommendation.

Thanks,

BUT THINGS WEREN'T AS THEY APPEARED



DID YOU CATCH IT?

From: dpace@tarheelpaving.com <dpace@tarheelpaving.com>
Sent: Tuesday, July 13, 2021 7:44 AM
To: Joel B. Setzer <jbsetzer@VaughnMelton.com>; Joel F. Hart <jfhart@VaughnMelton.com>
Subject: RE: [redacted] Invoice

Good morning Joel,

Please see the following.

Best, Derrick

From: Joel B. Setzer <jbsetzer@VaughnMelton.com>
Sent: Tuesday, July 13, 2021 6:06 AM
To: dpace@tarheelpaving.com; Joel F. Hart <jfhart@VaughnMelton.com>
Subject: RE: [redacted] Invoice
Importance: High

Derrick,

Please recall you need to make a revision to the last invoice submitted. Please recall the unit price discussion for the S9.5C.

Send the revised invoice to me and Joel Hart.

Joel,

If all looks good, forward with your recommendation to pay.

From: Derrick pace <dpace@tarhealpaving.com>
Sent: Tuesday, July 13, 2021 9:30 AM
To: Joel B. Setzer <jbsetzer@VaughnMelton.com>
Cc: Joel F. Hart <jfhart@VaughnMelton.com>
Subject: Re: FW: [redacted] Invoice

Hi Joel/Hart,

Find the attachment for our new bank details and make sure the payment is sent by ACH or Wire Transfer.

Let me know if you need anything else.

Best, Derrick

BUSINESS EMAIL COMPROMISE SCAMS & DIRECT DEPOSIT SCAMS ARE PREVENTABLE.

- Question everything
- Require a formal process for changes, including physical confirmation
- Ask IT to review before changes are made

5 6 7 8

NEW ATTACK VECTORS

COMPROMISED VENDOR CREDENTIALS & NON-IT MANAGED EQUIPMENT

- Vendors aren’t changing their service account passwords
- Breach within the past 6 months occurred due to this issue
- Who is liable?

- What about those Linux/SQL servers that someone in admin is running?

EXPOSED PORTS/DATABASES

A free service (Shodan) shows open ports/publicly exposed:

- 3389
- 2701
- 389/636
- 445
- ICS (HVAC)
- Printers

- Who is managing your firewalls?

PAY ATTENTION TO CVES

- Unpatched systems are the TA's best friend
- 80+% of all events related to unpatched systems

- Strike Team offers Nessus scans & Shodan reports for local governments
- NC DIT ESRMO offers these for state agencies

HYPER-V, RDP, PLEASE SAVE ME!

- Hyper-V usually domain joined….
  - Takes down phones, printers, etc

- Just Say No to RDP!
  - If you have to say yes, then MFA is a MUST for all users

9

NEW CYBER LIABILITY INSURANCE REQUIREMENTS

INSURANCE = RISKY BUSINESS

- Pay out has been too high for the industry to maintain profit margin
- Ave cost of cyber incident is $8.83 million
- Ransomware and data exfiltration leading causes of higher payouts
- Expect 15-30% increase in premiums moving forward
- Expect substantial new requirements to mitigate risk of large payouts
  - AIG has stated that it will trim 30% of customers due to failures to meet requirements
- Also expect decreases/sublimits on business interruption coverage
- Previous cyber incidents will also eliminate coverage or substantially raise rates

NEW CYBER INSURANCE REQUIREMENTS

- MFA on all email accounts, VPNs, and privileged user accounts
- Endpoint protection: Some carriers are requiring NextGen AV
  - Windows Defender is considered bare minimum (side note: many recent events only had Defender)
- Employee education/training: Phishing training specifically noted
- Air gapped backups for all critical on-prem systems
  - Less than 30 days old
- Patching cadence documentation
- Backup testing
- Data governance/management
  - Privacy
- IDS/IPS
- EDR
- DLP
- Specific requirements re: vendors

WHAT CAN YOU DO TO PROTECT YOURSELF AND YOUR ORGANIZATION?

NCLGISA IT STRIKE TEAM RECOMMENDATIONS FOR NON-IT STAFF

1. If you suspect ransomware, contact your IT department immediately! They should start severing all Internet-based connections asap.

2. Don't turn off your computer/server, just disconnect it from the Internet (ethernet and wireless)

3. Do not try to stay up and "functional", as it will allow for rapid, catastrophic proliferation across your networks and into any interconnections you might have with neighboring entities. ** No, you cannot just turn on your computer really quickly and insert a flash drive for those files you really need.

4. Use strong passwords (and unique ones) plus MFA (multifactor authentication) in your organization and personally.

CYBER SECURITY KNOWLEDGE

Which of these options is a form of multi-factor authentication?

1. User name and password
2. Security image to verify you are not a robot and password
3. One time code sent to phone and password
4. Two questions: 1) Name of childhood best friend and 2) City where your parents met
5. I have no clue!

- If you leave your phone laying around with the screen unlocked or text previews available on the locked screen, you are a security problem.
- It might seem like a pain, but if you use your organization's network for anything involving personal data (like checking your bank account, logging into your doctor's portal, etc), it is worth the headache to have MFA.

5. Do not allow vendors to have open tunnels into your environment for remote support. Use a documented process for external access.

6. Do not use the same credentials for domain, system or software administration and your local accounts. Many of the recent breaches have involved compromised domain administrator credentials, which often are found to be the same as cached local administrator credentials.

7. Ask for immutable backups that are stored physically and virtually apart from the network for critical systems. After attacking the domain controller(s), most current variants go straight to encrypting your backups.

8. Determine what servers contain sensitive data (PHI, PII, financial data, CJIS data, etc) and keep this on file outside of the network.

CYBER SECURITY KNOWLEDGE

Yes or No:

Do any of your vendors have persistent tunnels to “support” your software?

9. Know your cyber-liability insurance policy well and have conversations with them prior to an event to determine their standard course of action (preferred vendors, etc).

10. Require user education for phishing messages and aggressive response to mitigate anyone who falls for phishing. Exposed credentials and malware downloads are part of the problem and can be limited with proper education.

11. Create a Continuity of Operations plan for your entity including defining who will serve as Incident Commander and drill it to make sure it works for your team!

12. Work with senior leadership to create a prioritization document for bringing departments/applications back online.

GREAT FREE RESOURCES

(LINKS ARE EMBEDDED)

- Purple Knight (Active Directory Risk Assessment Tool)
- PingCastle (AD Security Assessment Tool)
- SCAP Tool (Security Assessment for STIG & CIS Controls)
- KnowBe4 Weak Password Checker & Other Free Tools
- CISA Cyber Hygiene Offerings
- Nessus Scanning Offering (from NCLGISA Cybersecurity Strike Team)