Top 10 Cybersecurity Trends Impacting Public Sector Entities

Shannon Tufts, PhD
NCLGISA Strike Team, NC JCTF
Professor of Public Law & Government
919.369.3179 cell
tufts@unc.edu

UNC SCHOOL OF GOVERNMENT

NC Public Sector Significant Cyber Incident Statistics

UNC SCHOOL OF GOVERNMENT

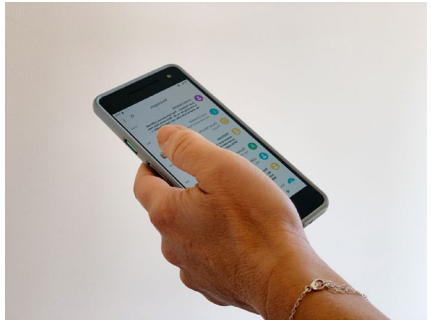
- Significant cyber attacks happen every 14 seconds worldwide
- Increase of 350% since 2018

NC Public Sector Statistics

- 2019: 10 (reported) significant cyber incidents
- 2020,: 24 significant cyber incidents
- 2021: 20+ significant cyber incidents; 160+ orgs remediated*
- 2022: 13 significant cyber incidents as of June 2, 2022 (+6 smaller cases)
- Downtime from significant cyber incidents increased 200 percent
- NC public sector incident costs average ~$700k-$1.5 million

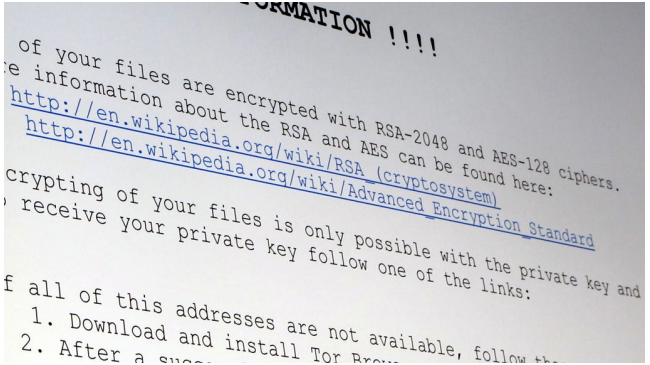
It is 11:39 pm on a Friday night…

UNC SCHOOL OF GOVERNMENT



Hey Shannon, it is Chris. We have a problem….ummm, all of our servers are locked up, our doors are not operational, we have year-end close out starting Monday, and we have no phone service. There is a note about paying a ransom on all of our machines.

What should we do?
Can you help us?



I Hit The Bat Signal!

UNC SCHOOL OF GOVERNMENT

- Immediately contact to State JCTF, including NCLGISA Strike Team Members, to start triaging situation with impacted entity's IT staff
  - --NCEM Cyber Lead to establish scoping call with impacted entity & JCTF
    --National Guard Cyber Security Response Unit
    --NCDIT ESRMO
    --Federal Partners
    --Other key agencies based on event
  - NCLGISA stands up:
    - Zoom channel is established for comms
    - Zoom room link published to the impacted entity to provide them with live support throughout the event 24/7 (team works shifts to ensure someone comes online whenever the client logs on)

NC Joint Cyber Task Force

Formalized by EO 254

UNC SCHOOL OF GOVERNMENT

State & Local Partners

--NCLGISA Cyber Strike Team (deployed onsite within 12-18 hours)
--NC National Guard G6 (deployed onsite within 12-18 hours)
--NC DIT
--NC DPS (NCEM Cyber Unit & NC ISAAC)
--NC Community College System Office (for all CC engagements)

Federal Partners

--FBI
--US Secret Service
--Department of Homeland Security (Cybersecurity and Infrastructure Security Agency)

Other Partners Based on Impacted Entity

--911
--NC SBI
--SBoE
--DHHS
--DPI
--MCNC

Boots on the Ground for Incident Response

UNC SCHOOL OF GOVERNMENT

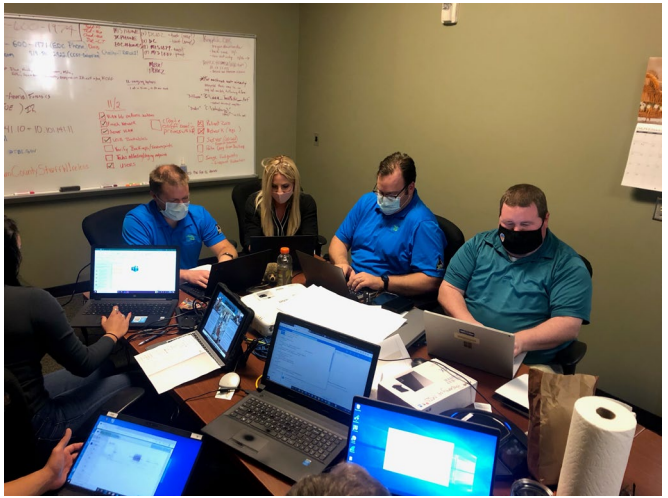
Onsite @ impacted entity within 4-12 hours of the initial scoping call

Work ~200 hours per significant incident (weekends, holidays, and after-hours are all within scope to get the job done)

Typical Strike Team and NCCCS Incident Staffing:

- 2 people on-site for days 1-2
- 1-2 folks on-site for days 3-6
- 12-16 hour operational periods when onsite
- Strike team syncs every evening for 2-3 hours to review logs, discuss game plans for rebuild during incident response
- Team members not on-site are typically reviewing CyberTriage images, logs, etc to perform what we call “sys admin forensic review/threat hunting”
- Some events take weeks or months, so those obviously consume more hours (usually after traditional day job hours and on the weekends)

Welcome to the War Room



Meet the NCLGISA Cybersecurity Strike Team

UNC SCHOOL OF GOVERNMENT

- Scott Clark, CIO, Town of Fuquay-Varina
- Randy Cress, Assistant County Manager/CIO, Rowan County
- Mark Seelenbacher, CIO, Henderson County
- Chad Coble, CIO, Stanly County
- Ted Norris, Deputy CIO, Onslow County
- Logan Steese, CIO, Currituck County
- Amy Walker, CTO, Ashe County Schools
- Shannon Tufts, UNC SOG Faculty Member

Strike Team IR Services

UNC SCHOOL OF GOVERNMENT

1. **Immediate and Sustained Structural Services During and Post-Breach:**
   a. Incident command/ITSL expertise
   b. Project management*
   c. Cyber liability insurance expertise and guidance*
   d. Guidance related to public records/breach notification*
   e. Documentation support
   f. Communication and coordination guidance*
   g. Resource identification and leverage from NCLGISA community and state of NC

2. **Identification:**
   a. Research variant and offer insight from previous events
   b. Analyze entry point and spread of breach
   c. Review log files to determine data exfiltration

3. **Containment:**
   a. Recommendations to isolate attack
   b. Recommendations to preserve evidence for forensic investigations

4. **Eradication:**
   1. Recommendations of approach and tools to assist and mitigate future attacks
   2. Assist with tool deployment as needed
   3. Provide recommendations on network protocols, network design/security, applications/services, backup strategies, etc
   4. Onsite rebuild assistance (time-permitting)

5. **Recovery:**
   1. Prioritization of recovery steps, down to department level (if not already established)
   2. Assistance with hardening infrastructure by applying CIS Level One Controls
   3. Expertise in firewalls, networking, and other infrastructure components (onsite or remote assistance depending on availability)
   4. Scripting services for imaging, etc
   5. Expertise with governmental systems and their critical interdependences
   6. General troubleshooting of infrastructure and application issues

Additional Strike Team Services Available to All Public Entities

UNC SCHOOL OF GOVERNMENT

- Website with Resources: https://www.nclgisa.org/page/strike-team
- Cybersecurity pre-plan checklists and training materials
- Ongoing Shodan reviews for all government IPs (please email your public IP range(s) to itstriketeam@nclgisa.org)
- Weekly Nessus scanning for vulnerabilities (please email your public IP range(s) to itstriketeam@nclgisa.org)
- Consultation on cyber-related questions including backup strategies, centralized logging, EDR, IDS/IPS, MFA, and specific technologies
- Regular “Strike Team” office hours
    - Successfully remediated 164 public entities impacted by Microsoft ProxyLogon vulnerability by holding all-day/evening virtual sessions for 10 days, including weekends

Key Cybersecurity Legislation

G.S. 143-800, amended by SL2021-180

G.S. 143B-1320, amended by SL2021-180

G.S. 143B-1379(c), amended by SL2021-180

Article 84, Various Technology Regulations.

GS143-800: State entities and ransomware payments.

UNC SCHOOL OF GOVERNMENT

(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

UNC SCHOOL OF GOVERNMENT

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.

.

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

Methods of Contact to Report Cybersecurity Incident

UNC SCHOOL OF GOVERNMENT

- **NCLGISA Strike Team:** itstriketeam@nclgisa.org or (919) 726-6508 (monitored 24/7)
- **NC EM 24 Hr Watch:** 800-858-0368 (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

Top Cyber Trends

UNC SCHOOL OF GOVERNMENT

Trend #1

UNC SCHOOL OF GOVERNMENT

Recognize These?

UNC SCHOOL OF GOVERNMENT

- 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?

Trend #2 & #3

UNC SCHOOL OF GOVERNMENT

Trend #2

UNC SCHOOL OF GOVERNMENT

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

UNC SCHOOL OF GOVERNMENT

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

Trend #3: Ransomware

- 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 24 months.

Ransomware Attack Timeline

UNC SCHOOL OF GOVERNMENT

M1
- An employee opens a phishing email and clicks on a link containing ransomware.

M2
- The ransomware downloads onto the employee's computer and starts executing malicious code.

M3
- The ransomware creates a connection via the Internet with the threat actor's command and control (C2) server.

M4
- The ransomware steals/harvests credentials to gain access to more accounts.

M5
- 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.

M6
- 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

UNC SCHOOL OF GOVERNMENT

- 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**

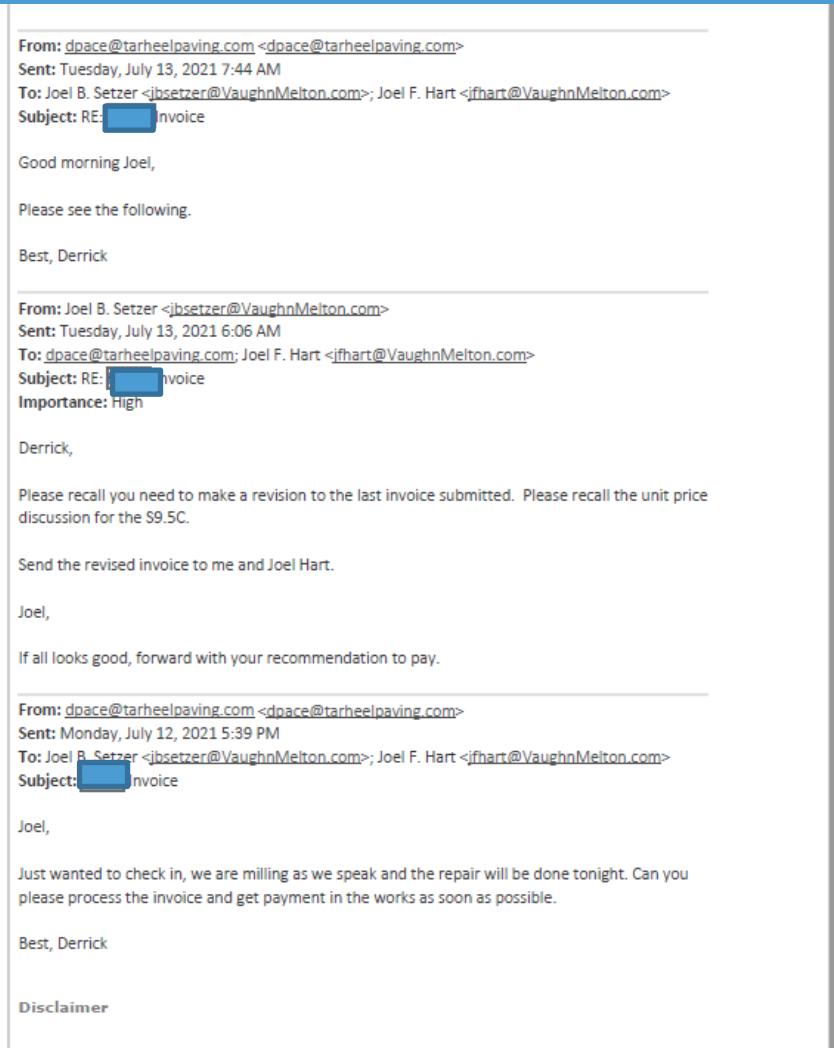
Trend #4

UNC SCHOOL OF GOVERNMENT


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

SCHOOL OF GOVERNMENT

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 Bank 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

UNC SCHOOL OF GOVERNMENT

Did You Catch It?

UNC SCHOOL OF GOVERNMENT

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: R[redacted]nvoice

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: R[redacted]nvoice
Importance: High

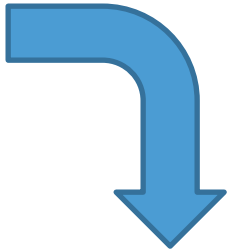
Derrick,

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]nvoice

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

New Cyber Liability Insurance Requirements

Insurance = Risky Business

UNC SCHOOL OF GOVERNMENT

- 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 Insurance Requirements

UNC SCHOOL OF GOVERNMENT

- 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?

UNC SCHOOL OF GOVERNMENT

NCLGISA IT Strike Team Recommendations for Non-IT Staff

UNC SCHOOL OF GOVERNMENT

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.

- 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.

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)

UNC SCHOOL OF GOVERNMENT

- Have I Been Pwned (look for data breaches associated with your email accounts)
- 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)


UNC
SCHOOL OF
GOVERNMENT