Preparing Your Organization For A Cyber Incident

UNC SCHOOL OF GOVERNMENT

www.sog.unc.edu

Shannon Tufts, PhD
Professor of Public Law and Government
Member, NC Joint Cybersecurity Task Force

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: 15+ significant cyber incidents
- Downtime from significant cyber incidents increased 200 percent
- Incident costs average ~$700k-$1.5 million

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 Threats

This Photo by Unknown Author is licensed under CC BY-NC

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.

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


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

Disclaimer
The information contained in this communication from the sender is confidential. It is intended solely for use by the recipient and others authorized to receive it. If you are not the recipient, you are hereby notified that any disclosure, copying, distribution or taking action in relation of the contents of this information is strictly prohibited and may be unlawful.

This email has been scanned for viruses and malware, and may have been automatically archived by **Mimecast Ltd**, an Innovator in Software as a Service (SaaS) for business. Providing a **safer**and **more useful** place for your human generated data. Specializing in; Security, archiving and compliance. To find out more Click Here.

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.

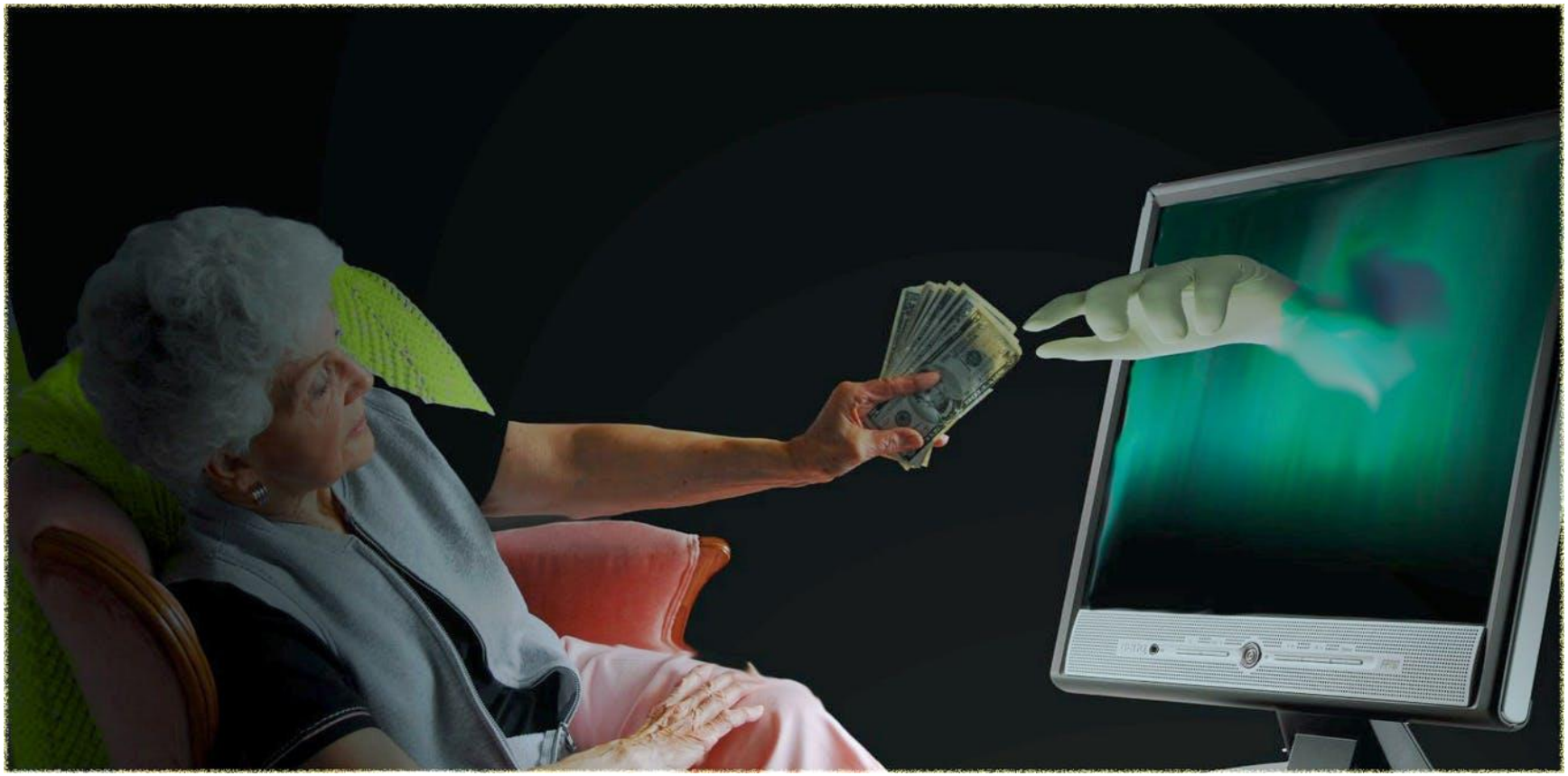
In regards to what was done before June 30 and after, all of this work was done prior to June 30. The slipped area repaired did not create any new pay quantities because it was basically warranty work.

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



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

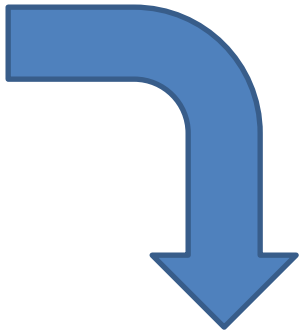
Derrick,

Please recall you need to make a revision to the last invoice submitted. Please recall the unit price discussion for the $9.5C.

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

Disclaimer
The information contained in this communication from the sender is confidential. It is intended solely for use by the recipient and others authorized to receive it. If you are not the recipient, you are hereby notified that any disclosure, copying, distribution or taking action in relation of the contents of this information is strictly prohibited and may be unlawful.

This email has been scanned for viruses and malware, and may have been automatically archived by **Mimecast Ltd**, an innovator in Software as a Service (SaaS) for business. Providing a **safer**and **more useful** place for your human generated data. Specializing in; Security, archiving and compliance. To find out more Click Here.

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 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

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

- NCLGISA Strike Team: itstriketeam@nclgisa.org or (919) 726-6508
- NC ISAAC: ncisaac@ncsbi.gov or 919-716-1111
- NCDIT: https://it.nc.gov/resources/cybersecurity-risk-management/statewide-cybersecurity-incident-report-form
- FBI IC3: https://www.ic3.gov/
  - If you have a situation involving financial fraud, like business email compromise or direct deposit fraud, please contact the FBI first because there is a ~72 hour window for fund recovery before it is moved off-shore.

Ways

Attorneys Can Prepare Their Orgs for Cyber Incidents

Cyber Liability Insurance

- Get to know your policy
  - Sublimits
  - Exclusions
  - Third party coverage
- Ask questions of your insurance carrier before you have an incident
  - Are you required to use their IR vendors?
- Ensure your staff are answering insurance questionnaires honestly and accurately

New Cyber Insurance Requirements

- Multifactor Authentication on all email accounts, VPNs, and privileged user accounts
- Endpoint protection: Some carriers are requiring NextGen AV
  - Windows Defender is considered bare minimum
- 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
- Requirements/exclusions re: specific vendors

2 Certificates of Insurance: 3rd Party Cyber Coverage

- RFP Requirement for All Software-Based Services, Vendors Supporting Systems, etc.

- Cyber Insurance: The contractor shall maintain cyber liability in the minimum amount of $1,000,000 per occurrence, including third-party coverage for incidents or associated impacts caused directly or indirectly by said vendor.

Breach Notification Requirements

Application of NCGS 75-65 to Governmental Entities
§ 132-1.10. Social security numbers and other personal identifying information. … (c1) If an agency of the State or its political subdivisions, or any agent or employee of a government agency, experiences a security breach, as defined in Article 2A of Chapter 75 of the General Statutes, the agency shall comply with the requirements of G.S. 75-65. …

§ 75-65. Protection from security breaches. (a) Any business that owns or licenses personal information of residents of North Carolina or any business that conducts business in North Carolina that owns or licenses personal information in any form (whether computerized, paper, or otherwise) shall provide notice to the affected person that there has been a security breach following discovery or notification of the breach. The disclosure notification shall be made without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (c) of this section, and consistent with any measures necessary to determine sufficient contact information, determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system. For the purposes of this section, personal information shall not include electronic identification numbers, electronic mail names or addresses, Internet account numbers, Internet identification names, parent's legal surname prior to marriage, or a password unless this information would permit access to a person's financial account or resources.

(b) Any business that maintains or possesses records or data containing personal information of residents of North Carolina that the business does not own or license, or any business that conducts business in North Carolina that maintains or possesses records or data containing personal information that the business does not own or license shall notify the owner or licensee of the information of any security breach immediately following discovery of the breach, consistent with the legitimate needs of law enforcement as provided in subsection (c) of this section….

Burden of Notice

Data Identification & Classification

- Prioritize a clear map of what data resides on which systems/servers in the event of notification requirements

- If possible, invest in segregation of PII, PHI, and other protected information from standard file servers

4 Tabletop Exercises & Breach Attack Simulations

- Ensure your organization has an Incident Response plan
- Test the plan with real-world scenarios (aka TTX)
- Leverage breach attack simulation tools if possible

5 Facilitate IT & EM Connection

- Assist with bridging the gap between IT and EM
- Bring both to the table to understand the conversations that will be had during an event
- EM has strong Incident Management training to be leveraged, which is invaluable during a cyber incident


QUESTIONS