Those ~5~ Things

~~Every Executive~~ Everyone

Should Know When Evaluating Cybersecurity!

DIGITAL SOLUTIONS CONFERENCE
CYBERSECURITY

POWERED BY NMFTA™
National Motor Freight Traffic Association, Inc.

If you are here, then you are interested in:

"Rough roads ahead?

Those **5** Big Issues:

- Awareness of issues that could impact your operations
- Defend / Protect your corporate assets
- Potential Consequences for NOT understanding "Cybersecurity"
- Where you should focus your investment dollars
- Not sure where to start

But first…

Understanding the CyberCircus

Those **5** Common Questions…

- What does "**Cybersecurity**" mean?
- Our operational footprint is **small**. Why bother?
- How **long** is this going to take?
- Isn't Cybersecurity an **expensive** investment?
- What do I need to do right **now** to make a difference?

"Risk" isn't funny…

… but what the tech teams are asking:

- What **Oversights** are we forgetting?
- What’s all the hype about **Phishing**?
- Why are **Passwords** such a pain to change?
- What’s all of this about **Patching** our systems?
- Is **Ransomware** really an issue to worry about?

“Trust me – I’m no threat!”

Those **5** not-so Fun Facts

- 95% of breaches caused by human **mistakes**
- 88% of companies have suffered from **phishing**
- 36 **billion** data records stolen *(1st half of 2021)*
- 300 billion **passwords** used by humans worldwide
- 5% of business owners **believe** they are secure

"Not my idea of hitching a ride"

“Cybersecurity”: *Those **5** Statistics*

• $2.4 **million**	Average cost of a malware attack
• **24,000**	Malicious Mobile Apps launched daily (US)
• **350**%	Rapid growth of Ransomware Attacks ’20 → ‘22
• $4 **Billion**	Losses to Equifax from their breach
• $6 **Trillion**	Projected damage from cybercrime by eo2023

I SEE you!

Those

5 Things …

(no surprises)

DIGITAL SOLUTIONS CONFERENCE
CYBERSECURITY

POWERED BY NMFTA™ National Motor Freight Traffic Association, Inc.

Remember these?

- What **Oversights** are we forgetting?
- What's all the hype about **Phishing**?
- Why are **Passwords** such a pain to change?
- What's all of this about **Patching** our systems?
- Is **Ransomware** really an issue to worry about?

I WANT you!

Those

5 Things …

(no surprises)

#1 Oversights

#1: Oversights … *Those **5** things that lead to big issues*

The rats in the shadows

- Unauthorized **Access** … … *Who's getting in & why?*
- **Old** Code / Apps … … *We'll do it later*
- Open **Networks** … … *Nobody's going to look for me*
- Third-party **Vendors** … … *Let's not make things so difficult*
- **False** Security … … *But we're Compliant!*

Those

5 Things …

(no surprises)

#2 Phishing

DIGITAL SOLUTIONS CONFERENCE
CYBERSECURITY

#2: Phishing … *It's the favorite act in the circus*

- … Online identity theft
- … Uses spoofed emails
- … Lures recipients to fraudulent websites
- … Attempts to reveal sensitive information
- … The single BI66EST email headache!

Let's go Phishing!

#2: Phishing … *It's the fav0rite act in the circus*

- … Online identity theft
- … Uses spo0fed emails
- … Lures recipients to fraudulent websites
- … Attempts to reveal sensitive information
- … The single BI**66**EST email headache!

Let's go ***Phishing!***

#2: Phishing … *Curiosity is a bad idea*

- Asks to **confirm** our personal information
- Web / email **addresses** inaccurate/redirects
- Message is **poorly** written
- **Suspicious** attachment!
- Message makes us panic!

Remember what happened to the cat?

#2: Phishing … *Those **5** reasons to toss it back*

You might have to eat what you catch!

- **Think** before you click
- Avoid apps from **unknown** developers
- Don't respond to **pop-up** windows
- Avoid **sharing** personal / sensitive data online
- **Learn** how & where the phish *swim*

- *(plus, one more):* If it **smells funny** …

Those

5 Things …

(no surprises)

#3 <u>Passwords</u>

#3: Passwords … *Those **5** invitations to trouble*

- … hello
- … 12345
- … qwerty
- … password
- … mynameisdrew

! → *allofthesepasswordsarecrap*

Pa$$wordsMakeMyH3ad-xpL0de!

#3: Passwords … *Those **5** things to remember*

- … Don't **share** them
- … Don't **reuse** them
- … Don't **tell** anyone what's in them *(yuck!)*
- … Replace them as **needed**
- … **Size** DOES Matter!

Use more than you think you should!

#3: Passwords … *Being weird can help!*

- “**Should**” be between 13 & 16 characters
- **26** lower case letters
- **26** UPPER case letters
- **10** numerals
- **33** special characters *(*, $, etc.)*
- **95** total possibilities in each digit

#3: Passwords … *The variables are endless!*

$(95)^1$	95	(Alphanumeric Characters)
$(95)^2$	9,025	
$(95)^3$	857,375	
$(95)^4$	81,450,625	(***"Million"***)
$(95)^5$	7,737,809,375	(***"Billion"***)
$(95)^6$	735,091,890,625	(***"Billion"***)
$(95)^7$	69,833,729,609,375	(***"Trillion"***)
$(95)^8$	6,634,204,312,890,625	(***"Quadrillion"***)
$(95)^9$	63,024,940,972,460,375	(***"Quadrillion"***)
$(95)^{10}$	59,873,693,923,837,890,625	(***"Quintrillion"***)

I hate math problems!

#3: Passwords … *Those **5** $^{(+2)}$ things to remember*

I SHALL USE STRONG P@$$WORDS.
I SHALL USE STRONG P@$$WORDS.
I SHALL USE STRONG P@$$WORDS.
I SHALL USE STRONG P@$$WORDS.
I SHALL USE STRONG P@$$WORDS.
I SHALL USE STRONG P@$$
I SHALL USE STRONG P@$$
I SHALL USE STRONG P@$
I SHALL USE STRONG P@$
I SHALL USE STRONG P@

“Pa$$w0rd!” is a type of Cypher

- **Change** your password on occasion
- **Use** a password vault
- **Choose** a pass-phrase that you will remember
- **Combine** uppercase / lowercase characters
- **Include** special characters *(#, $, %, etc.)*

+ … **Combine** a lyric / poem mixed with numbers;
+ … **Add** a foreign word
+ … **Add** a picture of your puppy *(kidding)*

#3: Passwords … *Those **5** things NOT to do*

- ☠ Include your username, first or last name
- ☠ Use a sport as a password
  ("baseball" & "football" are in the top 100!)
- ☠ Keep a local copy on OneNote or Notepad
- ☠ Store Passwords in Zoom sessions or in *Teams*
- ☠ Include personal data
  (birthdate, spouse name, pet name, car, etc.)

You're making it too easy for me!

Those

5 Things …

(no surprises)

#4 Patching

#4: Patching … *There’s always a hole!*

- The **hole** is in YOUR side of the boat!
- Patches Improve your state of **readiness**
- Operational **effectiveness** can be impacted
- Average lag time: more than 3 **months**!
- Hey—they’re **FREE**!

“Patch Tuesday” is a good place to start

#4: Patching … *No searching required!*

- They include **auto-fix** programs
- They follow a general release **schedule**
- (Most of the time) They **work** as designed
- … buuuut…

… Sometimes, **more** is necessary

Patching: The First Best Step to take!

#4: Patching … *Those **5** things to remember*

- Rely on your system **Automation**
- **Cloud** services include built-in pushes
- Check your **Update Schedule** & Settings
- Use "**Patch Tuesday**" as a routine checkpoint
- Stay **Informed** (bad stuff happens all the time)

Remove the obvious risks first!

Those

5 Things …

(no surprises)

#5 Ransomware

DIGITAL SOLUTIONS CONFERENCE
CYBERSECURITY

POWERED BY NMFTA™
National Motor Freight Traffic Association, Inc.

#5: Ransomware … *Those* ***5*** *Facts*

$20 Billion lost in 2021!

- Malicious Software
- Threatens to Exploit Your Fleet Assets
- Blocks Access to Sensitive Data / Functions
- Locks Files & holds your data hostage
- You may or may not get your data back!

#5: Ransomware … *Those **5** Myths*

- Only targets big companies
- Stopped [just] by backups
- Blocked by antivirus
- Blocked by firewalls
- Unstoppable

Once it's in—it's hard to remove!

#5: Ransomware … *By the numbers*

- **186%** Increase in ransomware attacks against the transportation sector since 2021
- **105%** Increase in weekly ransomware attacks against the trucking industry since 2022
- **71%** Companies worldwide affected by ransomware in 2022
- **65%** Data gets returned when a company pays the ransom
- **57%** Companies successful in recovering anything at all

Insurance isn't always going to cover it!

#5: Ransomware … *One-time problem? Nope!*

- **80%** Companies paid the ransom
  (with <half getting anything back)
- **80%** Ransomware targets were hit again
- **64%** Victim companies still have bad guys in their systems
- **40%** Companies (regardless of size), experienced lay-offs

Phishing→ Malware→ Ransomware→ …?!

#5: Ransomware … *Those **5** Signs of Trouble*

- Privileged User Account Activity
- Suspicious System File Changes
- Unusual Access Requests
- Terminating Critical Sessions
- Mobile Device Profile Changes

Awareness + Process + Policy + Tech = SAFETY

Those

5 Things …

You can do right now!

DIGITAL SOLUTIONS CONFERENCE
CYBERSECURITY

POWERED BY NMFTA™
National Motor Freight Traffic Association, Inc.

Those **5** things *you can do* ***right now***

- Ask the right questions
- Be specific in your focus
- Cover those 5 bases
- Address the fundamentals
- Don’t go it alone

Start with a basic understanding of “Risk”

#1: Ask the Right Questions!

- What is our greatest asset as a business?
- How often do we update our systems?
- How prepared are our fleet operations for a cyber attack?
- What would a hacker want from us?
- How do we think a hacker would exploit us?
- What security tools do/should we deploy right now?
- Who is accountable for addressing vulnerabilities?
- What do we see as the weakest link?

It's okay if the answer forces more questions

#1: Ask the Right Questions!

- What is our greatest asset as a business?
- How often do we update our systems?
- How prepared are our fleet operations for a cyber attack?
- What would a hacker want from us?
- How do we think a hacker would exploit us?
- What security tools do/should we deploy right now?
- Who is accountable for addressing vulnerabilities?
- What do we see as the weakest link?

It's okay if the answer forces more questions

#2: Be Specific in your FOCUS!

- What is the level of risk we are comfortable taking?
- What is the likelihood of exploitation?
- What are the internal & external vulnerabilities?
- What is the impact if those vulnerabilities are exploited?
- Do we [all] understand the relevant threats?
- How / Where would a data breach impact our fleet?

Time (and focus) can make all the difference

#3: Cover those **5** bases …

- **Develop** your Business ***Resilience & Response Plans***
  … to test / validate your processes!
- **Create** Immutable Data ***Back-up Plans***
  … to minimize operational downtime!
- **Establish** your Incident ***Response Plans***
  … to avoid a "Too Late" situation!
- **Mandate** Fleetwide Cybersecurity ***Training / Briefings***
  … to make sure everyone knows at least the basics!
- **Schedule** a Tabletop ***Exercise***
  … to test / validate your processes!

Know the risks, know how to address them!

#4: Address the Fundamentals!

- Ensure you have **Leadership** Support NOW!
- Raise Cybersecurity **Awareness** *(companywide)*
- Establish a workable **Continuity** Plan
- Test / Validate your Emergency **Readiness**
- Check your **Tools** *(are they tuned properly?)*
- Never "Trust" & Always "**Verify**!"
- Passwords / Patches / **Authentication**
- When in **Doubt**—verify before opening

Keep a Clean Machine!

#5: Don't Go it Alone!

- ($) Security Awareness Training
- ($) Governance, Risk & Compliance Preparation
- ($) Data Privacy Policy Review *(GDPR / CCPA)*
- ($$) Business Continuity / Disaster Recovery
- ($$) Security Controls Impact Analysis
- ($$~) Ransomware Defense & Readiness
- ($$) Penetration Testing
- ($$$) Zero Trust Security Architecture

Asking for help may save your fleet operations!

Those

5 Things …

Drew would do

DIGITAL SOLUTIONS CONFERENCE
CYBERSECURITY

What would Drew do? … *Start by recognizing everyone is at risk!*

Small Fleet (1 – 50)	**Mid-size** (51 – 150)	**Large Fleet** (151-300)	**Enterprise** (300+)
1. Train the team	Train the team	NIST / GRC Protocols	NIST / GRC Protocols
2. Update the apps	Evaluate C.I.A.	Train Dept Heads	Deploy / Update Controls
3. Limit access	BC / DR Plans	Gap Analysis	Review SDLC / ZTSA
4. Firewall / VPN	Validate Access	Deploy / Update Controls	Scan the systems
5. System Backups	Gap Analysis	Scan the systems	Tabletop Exercise

Those
5
Things

Thank You!

Drew Blandford-Williams
Guidacent CISO
Threat *Recon* Program Director

drew@guidacent.com
801.668.1877

SCAN ME