Franklin County Public Schools hit by ransomware attack

Jason Dunovant May 16, 2023 0

Franklin County Public Schools were closed Monday following a ransomware attack that is still impacting the school division.

According to a statement from schools Superintendent Bernice Cobbs, the decision

Basic Cyber Hygiene and how to protect yourself if the worst occurs

Presented by

Jeff Nosenzo

Vice President, Brown Insurance

- Specializes in both Business and Personal insurance
- Certified Authority on Workers Compensation
- Passionate about Risk Management practices and tactics
- Serves on multiple Boards such as: Blacksburg Partnership, NRV Home Builders Association, Main Street Connect, etc.
- 2004 Virginia Tech Pamplin College of Business graduate
- Resides in Blacksburg with wife Joy and 7-year-old son Braden
- Loves long walks on the beach as the wind blows through his hair

Presented by

Jeff Wynn

President, New River Computing Inc.

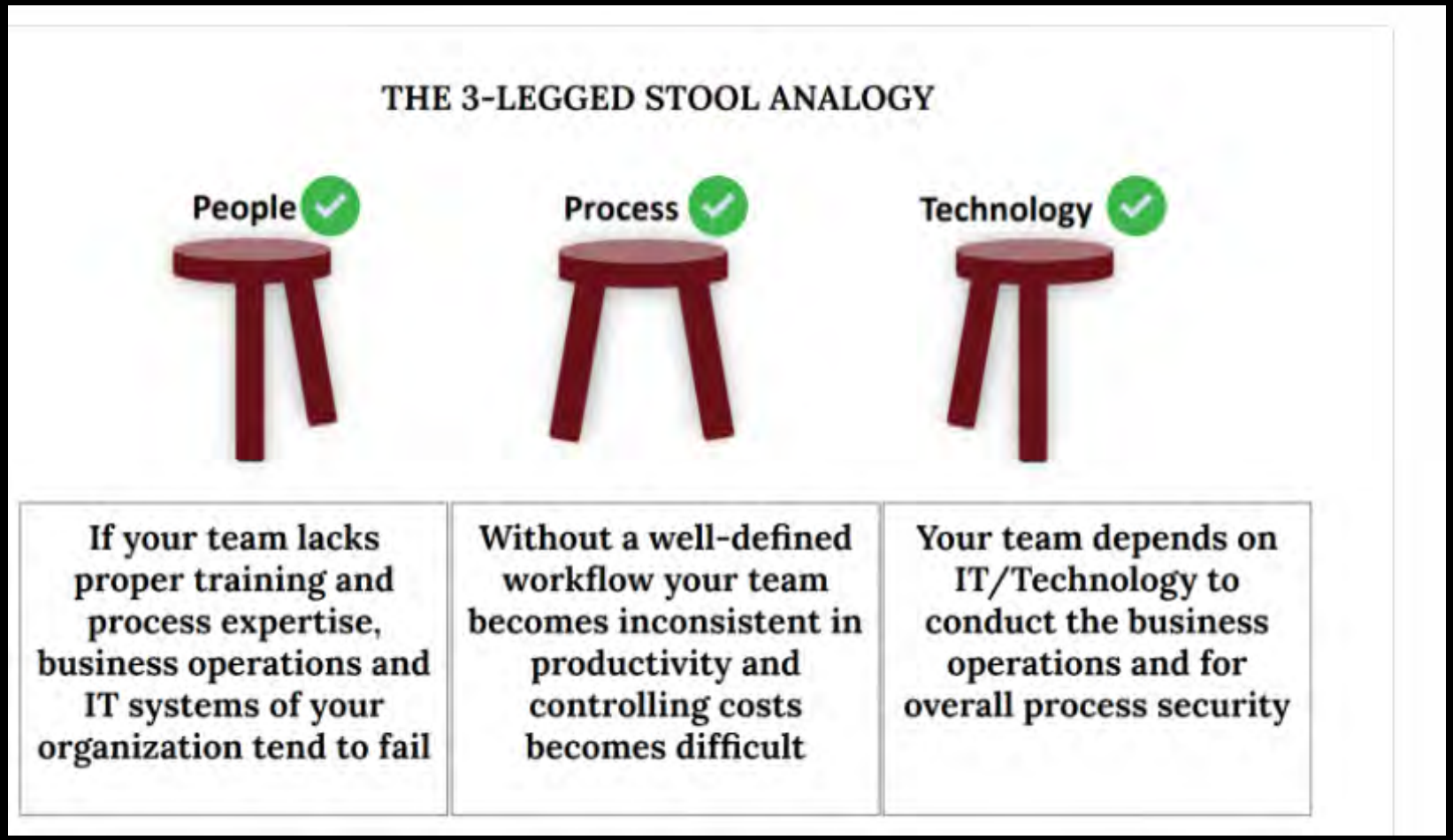
- Cybersecurity Evangelist
- Microsoft 365 Immersion Experience Qualified Facilitator
- Serves on Blacksburg Partnership and Onward NRV Boards
- Previously was an analyst at Virginia Tech along time ago
- Before that, Sysadmin at Appalachian Trail Conservancy
- BS, Engineering Science and Mechanics, Virginia Tech
- MS, Environmental Engineering, Virginia Tech
- Enjoys traveling & camping with wife Lesa and our dogs
- Has no work-life boundaries

The 5-question test

- Do you have **MFA** for email and sensitive information?
- Do you have **backups** and are you sure they are working?
- Do you have **up-to-date, active antivirus** installed on all computers?
- Do you have a written documented **breach response plan**?
- Do you have **up-to-date, active firewall** technology?

How you can check each of these yourself:

- Do you have **MFA** for email and sensitive information?
  - *Do you get prompted?*
- Do you have **backups** and are you sure they are working?
  - *Do you do test restores?*
- Do you have **up-to-date, active antivirus** installed on all computers?
  - *Open AV on each machine and look.*
- Do you have a written documented **breach response plan**?
  - *Templates exist—Adapt to your needs*
- Do you have **up-to-date, active firewall** technology?
  - *Do you pay a subscription like antivirus?*



- Security as a three-legged stool

Spotting Phishing attacks

THE SLAM METHOD

S **SENDER**
ANALYZE THE SENDER'S EMAIL ADDRESS CAREFULLY

L **LINKS**
HOVER YOUR MOUSE OVER LINKS, WITHOUT CLICKING, TO SEE THEIR TRUE PATH

A **ATTACHMENTS**
USE CAUTION WHEN OPENING UNSOLICITED OR UNEXPECTED ATTACHMENTS

M **MESSAGING**
WATCH FOR MISSPELLINGS, AND "OUT OF CHARACTER" PHRASING, WITHIN THE BODY OF AN EMAIL


Multi-Factor Authentication
Password
Verification
Access

What do I do if my organization is compromised?

What do I do if my organization is compromised?

Step 1: Contact your lawyer

What do I do if my organization is compromised?

Step 1: Contact your lawyer

Step 2: Implement your incident response plan

Self assessment questionnaire

NETWORK SECURITY CONTROLS

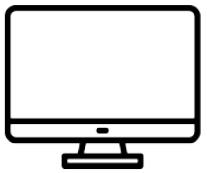
7. Indicate whether the Applicant currently has the following in place:

a.	A Chief Information Security Officer or other individual assigned responsibility for privacy and security practices	☐ Yes	☐ No	
b.	Up-to-date, active firewall technology	☐ Yes	☐ No	
c.	Up-to-date, active anti-virus software on all computers, networks, and mobile devices	☐ Yes	☐ No	
d.	A process in place to regularly download, test, and install patches	☐ Yes	☐ No	
	If Yes, is this process automated?	☐ Yes	☐ No	
	If Yes, are critical patches installed within 30 days of release?	☐ Yes	☐ No	
e.	Intrusion Detection System (IDS)	☐ Yes	☐ No	
f.	Intrusion Prevention System (IPS)	☐ Yes	☐ No	
g.	Data Loss Prevention System (DLP)	☐ Yes	☐ No	
h.	Multi-factor authentication for administrative or privileged access	☐ Yes	☐ No	☐ N/A
i.	Multi-factor authentication for remote access to the Applicant's network and other systems and programs that contain private or sensitive data in bulk	☐ Yes	☐ No	☐ N/A
j.	Multi-factor authentication for remote access to email	☐ Yes	☐ No	☐ N/A
k.	Remote access to the Applicant's network limited to VPN	☐ Yes	☐ No	☐ N/A
l.	Backup and recovery procedures in place for all important business and customer data	☐ Yes	☐ No	
	If Yes, are such procedures automated?	☐ Yes	☐ No	
	If Yes, are such procedures tested on an annual basis?	☐ Yes	☐ No	
m.	Annual penetration testing	☐ Yes	☐ No	
	If Yes, is such testing conducted by a third party service provider?	☐ Yes	☐ No	
n.	Annual network security assessments	☐ Yes	☐ No	
	If Yes, are such assessments conducted by a third party service provider?	☐ Yes	☐ No	
o.	Systematic storage and monitoring of network and security logs	☐ Yes	☐ No	
p.	Enforced password complexity requirements	☐ Yes	☐ No	
q.	Procedures in place to terminate user access rights as part of the employee exit process	☐ Yes	☐ No	

Compliance v. Security

EvilProxy Attacks

User



Office.com

Target Website

Offffice.com