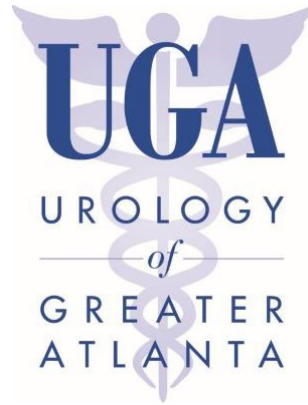


2023 VIZIENT CONNECTIONS SUMMIT

**TOGETHER**  
*we will soar*

SEPT. 18–21, 2023  
WYNN, LAS VEGAS

vizient®



# **We've Been Hacked Now What?**

**Cheris L. Craig, MBA, FACMPE**

Chief Administrative Officer

Urology of Greater Atlanta, LLC

*we will soar*

vizient.

# Disclosure of Financial Relationships

Vizient, Inc., Jointly Accredited for Interprofessional Continuing Education, defines companies to be ineligible as those whose primary business is producing, marketing, selling, re-selling, or distributing healthcare products used by or on patients.

An individual is considered to have a relevant financial relationship if the educational content an individual can control is related to the business lines or products of the ineligible company.

No one in a position to control the content of this educational activity has relevant financial relationships with ineligible companies.

*we will soar*

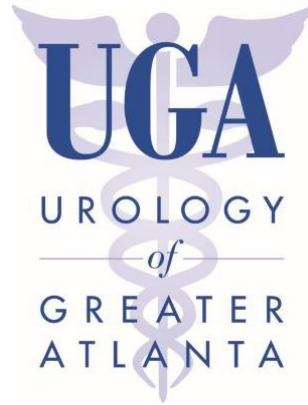
vizient.

# Learning Objectives

- Discuss the importance of preparing for a network intrusion or interruption.
- Identify solutions to enhance network security.
- Describe use of a checklist as an aid when documenting within a system.

*we will soar*

vizient.



# **We've Been Hacked Now What?**

**Cheris L. Craig, MBA, FACMPE**

Chief Administrative Officer

Urology of Greater Atlanta, LLC

*we will soar*

vizient.

# Background

- Practice with 8 physicians, 6 locations, with an ASC, a lab/path department, CT, Ultrasound and X-Ray
- Approximately 80 employees, 120 devices, 1 full-time IT support person
- 21 on-premise servers including some virtual servers
- EPLAN which routes all Internet traffic through the main office with one managed firewall appliance
- Internet access limited to allowed websites only except physicians and 8 staff
- Limited wi-fi with no access for physicians, employees or guests
- Exchange server with email addresses limited to 10 employees
- Hardware appliance for remote access limited to physicians and 4 staff

*we will soar*

vizient.

# What Happened?

- Unauthorized users accessed our network on at least two occasions
- Unauthorized domain users and domain admin accounts were created
- A command line program to manage files on cloud storage, was installed
- An unpacking and encryption software, was installed
- A program to extract and use stored passwords, was installed
- Data encryption steps were taken, but not completed
- Ransomware was the goal of the attackers
- Our file server was compromised
- Data was recovered by the FBI on day 5

*we will soar*

vizient.

```
t: Failed to copy: upload file failed to create session:  
t: Failed to copy: upload file failed to create session:  
t: Failed to copy: upload file failed to create session:  
t: Failed to copy: upload file failed to create session:  
t: Failed to copy: failed to finish upload: Try again  
t: Failed to copy: failed to finish upload: Try again  
t: Failed to copy: failed to finish upload: Try again  
t: Failed to copy: failed to finish upload: Try again  
t: Failed to copy: failed to finish upload: Try again  
t: Failed to copy: failed to finish upload: Try again  
t: Failed to copy: failed to finish upload: Try again  
.h17.txt: Failed to copy: upload file failed to
```

Copying blocked by our stringent Internet restrictions

*we will soar*

vizient.



# Sustaining Operations & Prioritizing Recovery

- Created, documented and distributed information about seeing patients without a computer network
  - How to document visits, order tests, get results, collect payments
- Alerted our cyber liability carrier
- Alerted the answering service and made a plan for urgent calls
- Posted alerts on our website and social media accounts
- IT consultant contracted to be onsite indefinitely
- Created a “Recovery War Room” and a “Data Clean Room”
- Documented and prioritized all systems
- Documented steps for PC rebuild and assigned staff by task
- Contacted vendors to schedule emergency help with software installs

*we will soar*

vizient.

# Top Priorities

## ① Deploy PC's

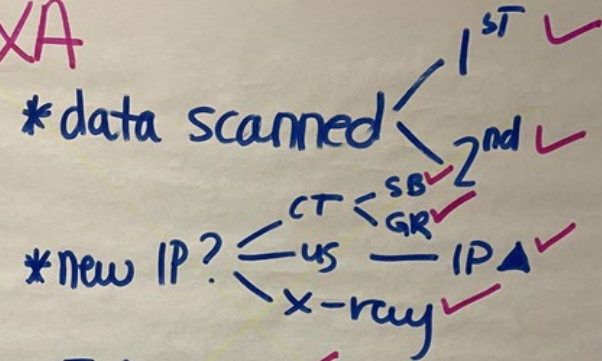
**\*BACK-UP!**

- \* rename ✓
- \* add to domain ✓
- \* install ✓
  - \* red planet - new msi ✓
  - \* office - new license ✓
- \* push PDQ ✓
- \* Modern Standby ✓

## ② Test SRS

- \* Rater ✓
- \* forms all MD's ✓
- \* forms module ✓
- \* Emdeon ✓
- \* path - in house ✓
- \* lab - in house ✓
- \* 4A ✓
- \* EXA ✓
- \* Submit Billing ✓
- \* Mead Lichs ✓
- \* appt/demo ✓
- \* paperport ✓
- \* Templates ✓
- \* port listener ✓
- \* IE Printing ✓

## ③ EXA



- \* Test order ✓
- Test result ✓
- \* virus scan (logmein) ✓

## ④ Psyche

- \* client install ✓
- \* Nice Label

we will soar

vizient

## ⑤ QuickBooks

\* on server ✓

\* load data

UGA-5  
scanned

\* Jennifer ✓

Joshua

Cheris

\* Hybrent

UGA ✓  
Cool Docs  
AMO/Three Docs ✓  
Ocean Blvd  
SCU ✓  
GFIE

NPP ✓

7 Docs

5 Docs

## ⑥ Exchange

\* internal email ✓

\* shared email ✓

\* real email ✓

\* sym messaging ✓

\* Titan ✓

\* old emails & notes

VPP

Overlook

## ⑥ Phone Server

\* move from Windows Home ✓

\* Digital Phones

\* Hold Music

\* Δ IP to digital

\* Sharon

\* Scheduling

\*

## ⑦ Faxability

\* audio codes

\* client

\* ID 460311

\* SCU (DTFM 8050)

\* UGA

\* print to fax

\* email confirmation

\* users

we will soar

vizient

⑧ Red Planet

- \* Install 1@time ✓
- \* w/o config ✓
- \* w/config ✓

⑨ Office

- \* activation
- \* new license ✓
- \* old license ✓
- \* reset count ✓
- \* Macro/Trusted Settings ✓
- \* roll-out

⑩ 230

- \* phones ✓
- \* computers ✓

⑪ 240


⑫ 220

- \* ~~Run~~ Veeam - 30d <sup>back-up</sup>
- \* Log me in ✓
- \* Titan 14 days <sup>open</sup>

we will soar

vizient.

# ⑬ Forensic Eval

- \* punch code drives ✓
- \* paperwork ✓
- \* back-up acc ✓
- \* IFB ✓
- \* Hello Kitty 

Andrew Munn  
(415) 815 8397  
ammunn@fbi.gov

- ## ⑭ Spectrum
- \* allow VLANs on EPLAN

# ⑮ VPN'S

\*GMT.

\*Griffin Imaging

\*OPI ✓

\*\*Blue Ridge

\*Capital Anesthesia ✓

\*Chart Pro

## ⑯ Interpage

- \* emailed key to Ryan ✓
- \* updated Key ✓
- \* client install needed ✓

## ⑰ printers

- \* copiers
- \* scan function

## ⑱ filezilla

These  
outsourced vendors  
(700) 213 1982  
Check  
for VPN

in list  
- Tami@Ransoft  
(951) 824 8813

Thursday

SRS  
des  
print

was remote  
SRS only  
Print & Scan

Preston Smith  
770 434-0942  
psmith@setele.net

we will soar

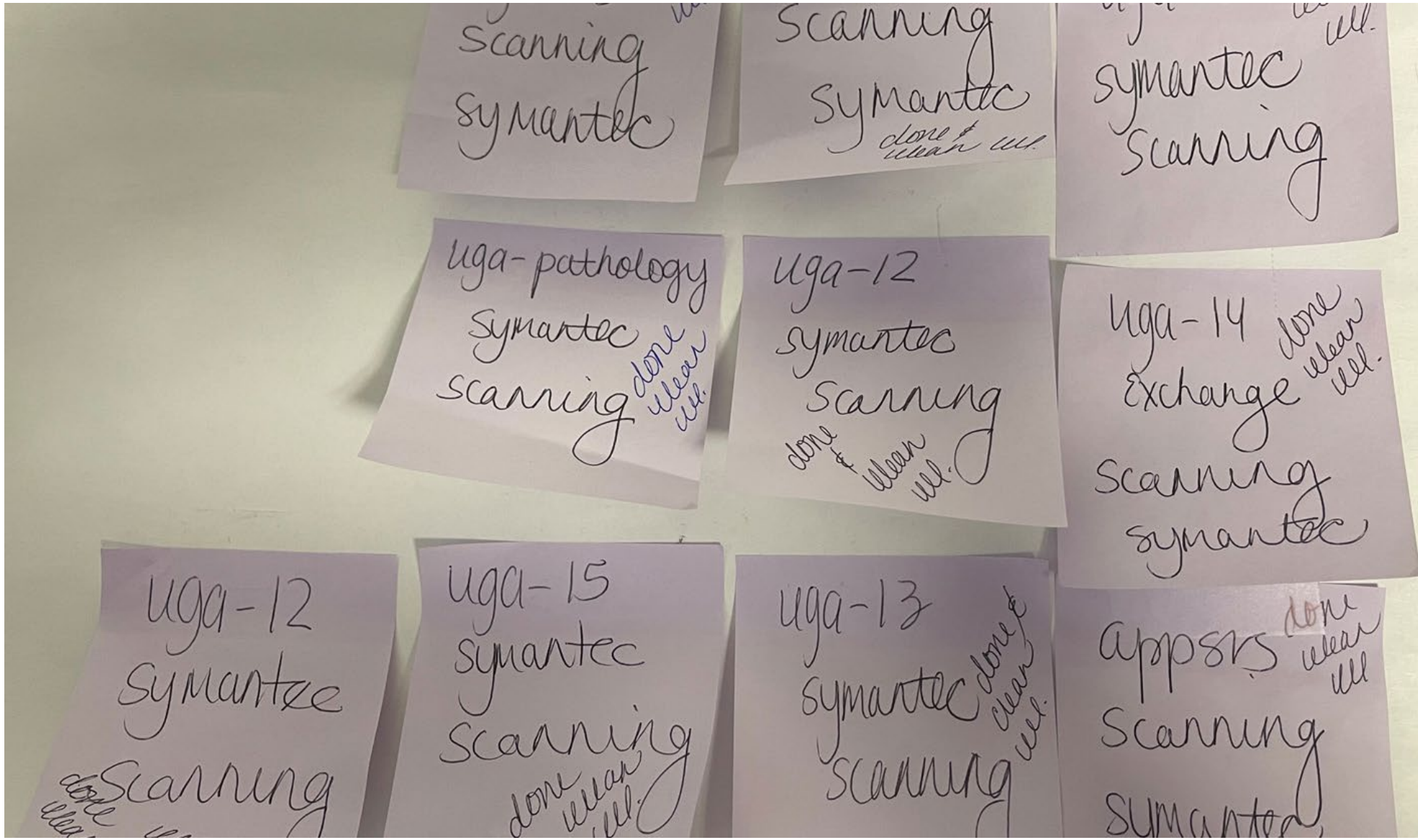
vizient

# Network Rebuild Process

- Due to the potential for dormant and/or time released viruses a decision was made to wipe all systems
- Wiped all servers and PC's, upgraded firmware, reset bios with new installations of operating systems and software
  - Upgraded to current versions
  - License counts had to be reset
- Purchased external hard drives for each server and 3 new PC's for virus scanning
- Used 3 different high-level virus scanning software programs scanned all data multiple times
- Recreated all VPN's and interfaces
- Recreated all group policy, domain users and printers

*we will soar*

vizient.



we will soar

vizient.

# Solutions to Enhance Security

- Firewall and switches should be “smart” not just managed
  - Block network access from unnecessary countries
  - Close unnecessary ports
  - Content filtering
  - Intrusion detection and intrusion prevention
- Endpoint Detection & Response Software solutions analyze security threats to find, isolate and detect ransomware for a quick response
- Remote Monitoring & Management Software can manage vendor access, require MFA and provide virus detection

*we will soar*

vizient.



# Solutions to Enhance Security

- Email filtering vendors solutions receive all email prior to it entering the network
  - Allows for a block senders list
  - Scans and quarantines emails
  - Each email user can allow or block content one email at a time
- Password management tools keep user passwords secure
- PACS system removed from the Internet accessible to specific IP addresses only (includes hospitals)
- VPN implemented for remote access by physicians and managers
- Systems on separate sub-nets or V-Lans
- Wi-fi networks use smart access points and are separated by function

*we will soar*

vizient.

# Recovery Tools Checklist

- Deployment software automates software installation, software updates and reboots
- Inventory software automates software inventory by workstation to identify and avoid outdated versions and anti-virus
- IT documentation service keeps IT data in a single location
  - Accessible by multiple employees
  - Reminder emails about expiration dates
- Data protection services allow for back-up of operating systems and programs in addition to data for faster network recovery.

*we will soar*

vizient.

# Lessons Learned

- No matter how locked down your network is, you are vulnerable
- Document your environment
  - Network Infrastructure
  - Usernames and passwords
  - VPN and other connectivity
    - Care partners such as radiologists
    - Clearinghouse, appointment reminder and transcription services
  - Interfaces
    - EMR to other software such as PM and PACS
    - Equipment, such as lab, UA and path
    - PM to other software such as accounting

*we will soar*

vizient.

# Lessons Learned

- Have hard copies of forms at each office
  - Visit forms
  - Imaging forms such as ultrasound
  - Lab and pathology requisitions for all labs, including in-house
  - Consent forms, patient registration forms and superbills
  - Receipt forms and credit card processing forms
- Keep contacts with vendors up-to-date
- Firewalls and remote access systems don't track activity if you don't have "smart" systems which are enabled
- Block connections on VPN and remote access systems from unnecessary countries
- Keep software up-to-date with patches and versions
- Record software license numbers and keys

*we will soar*

vizient.

# Lessons Learned

- Remove end-of-life equipment
- Data back-ups
  - Do not generally include software back-ups
    - Older software versions may be difficult to obtain
  - Need to be tested regularly
  - Can be infected
- OIG Reporting
  - 60-day requirement is only a guideline
  - Require information on actual data compromised
  - Best efforts to notify affected individuals
- Don't exclusively use domain email addresses for support

*we will soar*

vizient.

# Key Takeaways

- Prepare, it's when not if
- Cyber liability insurance is important but don't count on it to bridge the cashflow gap
- Unlike a professional liability case, the carrier does not provide much assistance with recovery efforts
- Once unauthorized access is gained, access can be shared or sold
- Viruses can be dormant, virus scans won't detect them
- Data can be encrypted and held hostage
- Network security has many facets and changes almost daily

*we will soar*

vizient.

# Impact

**Have there been any new distractions or hardships that have made school more difficult for you? If so, what are they and how do you plan to address those issues?**

Recently my Mom's business has been hacked. It has caused a lot of stress throughout the establishment and our family. We have gotten barely any sleep in the past few weeks. I have just been completely thrown off by this incident and I always forget about assignments now. My Mom and I have to stay up all night just to keep her business afloat. Sometimes we don't get home until 1:45 AM. It's a lot on my Mom to because she has to take me to sports and school and deal with all of her work stuff. Sometimes we have to sleep at her work and come to school the next morning.

**What is your SMART goal for the next two weeks?**

I want to bring up my grades and start to back on track with work.

**What comments would you like to share with your parents about your grades and progress today?**

i just think we need a weekend to just get some sleep and slow down. We have been at work every night of the week and barely getting sleep. I just want to come home one night without going to your work. I think we both need that. We have been non stop working and you have barely gotten 3 hours of sleep every night.

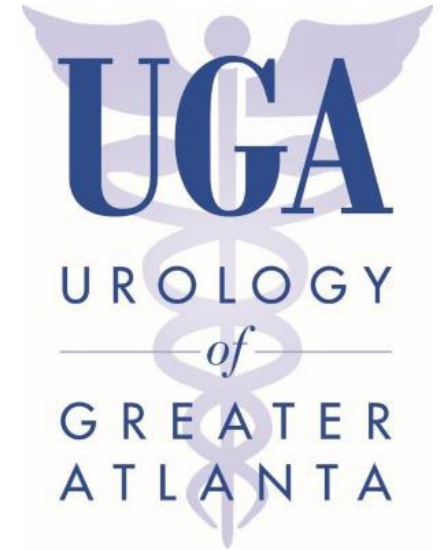
*we will soar*

vizient.

# Questions?

Contact: Cheris L. Craig, MBA FACMPE  
Chief Administrative Officer  
Urology of Greater Atlanta, LLC  
cheriscraig@yahoo.com  
678-575-8888

Cheris L. Craig, [cheriscraig@yahoo.com](mailto:cheriscraig@yahoo.com)



*This educational session is enabled through the generous support of the  
Vizient Member Networks program.*

*we will soar*

vizient.