Protecting your Practice from Cyber Attackers and AI

Pacific Dental Conference

CANADIAN DENTAL ASSOCIATION

Steve McEvoy

March 8th, 2024

Hey Steve – where are all the graphics?

I can't be 100% certain that all the graphics used in my presentation are royalty free. The only way to stave them off for certain is to remove all the graphics.

My apologies that this will be less visually interesting, but if you were at my presentation, it will still make sense and you can use it for reference. Thanks for coming!

Fun!

Entertaining!

The Internet is _____

Unruly

Scary

Dangerous

Annoying

Confusing

(Cyber) Security is _____

Complicated

Difficult

Expensive

How can you be 100% safe from Cyber crime with little effort?

The Internet has some scary s**t going on

This is a self defense course

What Cyber Incident in the last week is affecting your Practice?

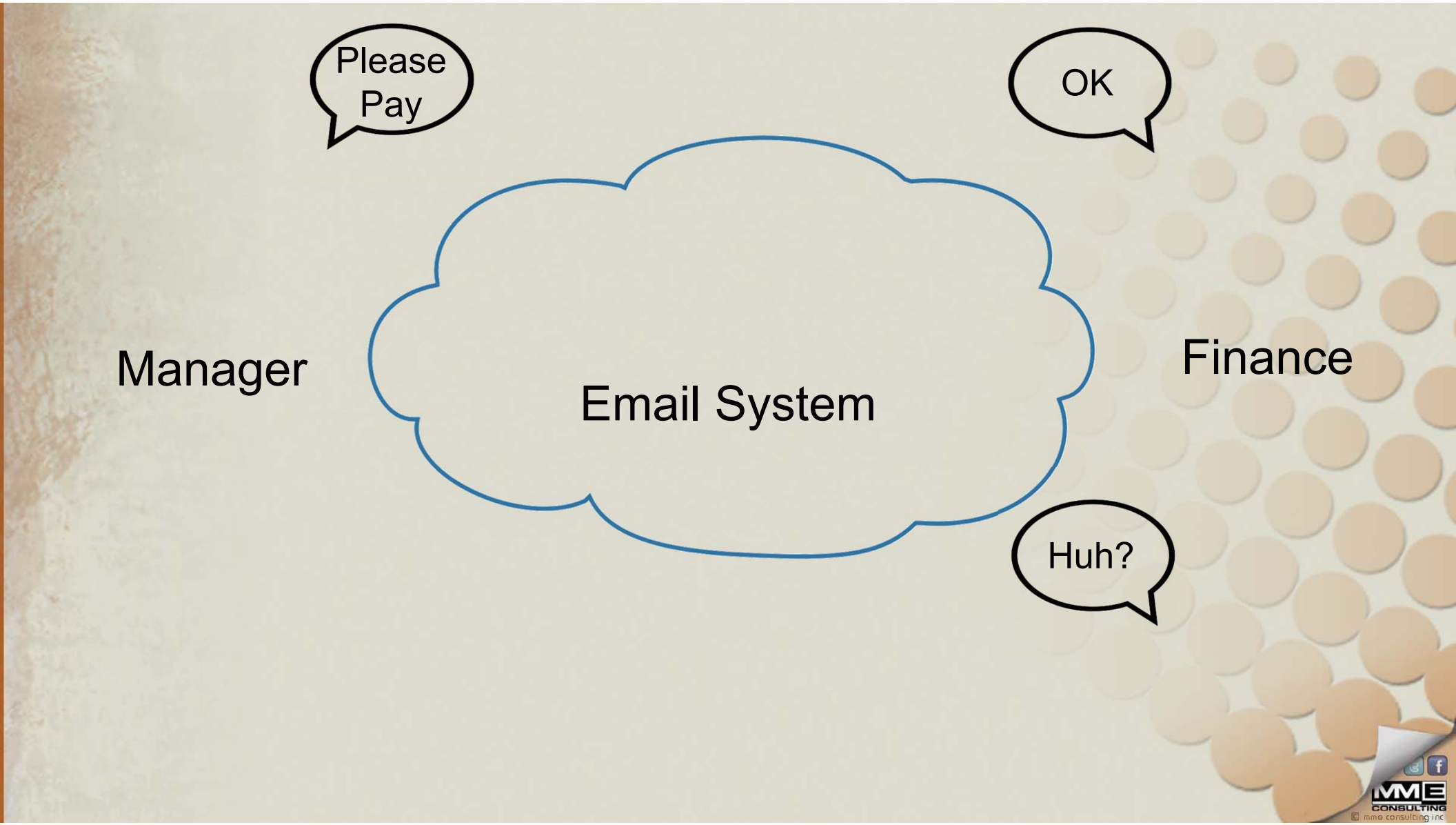
Subscribe Sign in

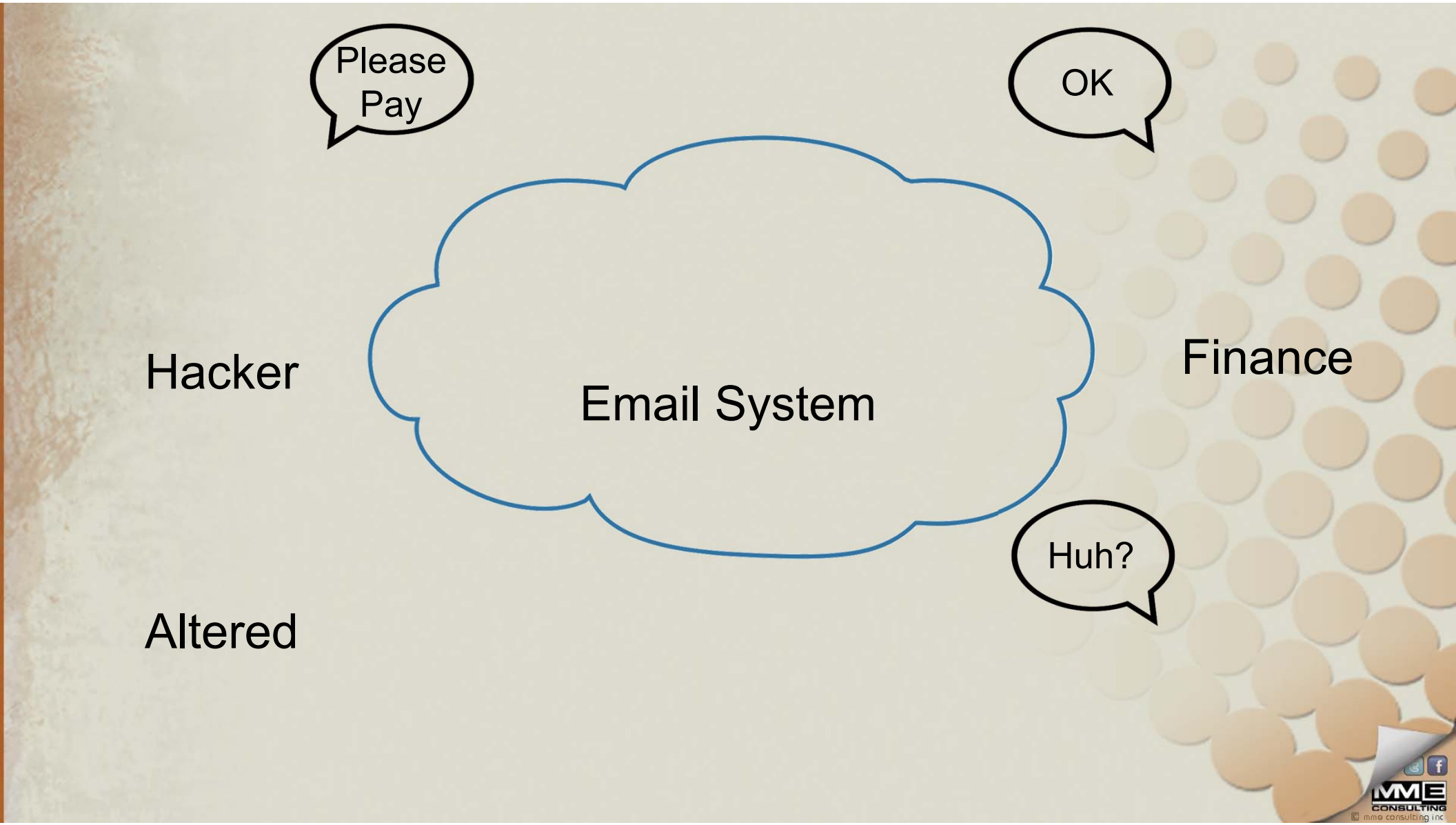
Change Healthcare is a juggernaut in the health-care world, processing 15 billion claims totaling more than $1.5 trillion a year, the company says. It operates the largest electronic "clearinghouse" in the business, acting as a pipeline that connects health-care providers with insurance companies who pay for their services and determine what patients owe. It supported tens of thousands of physicians, dentists, pharmacies and hospitals, handling 50 percent of

KEY POINTS

- Change Healthcare's systems are down for the fourth day in a row after parent company UnitedHealth Group disclosed a suspected cyberattack on Wednesday.
- UnitedHealth said it identified a "suspected nation-state-associated" actor behind the attack, according to a filing with the U.S. Securities and Exchange Commission on Thursday.
- In an update at around 2 p.m. ET Saturday, Change Healthcare said the disruption is expected to continue "at least" through the day.

Let me tell you a story …


Please Pay
OK
Manager
Email System
Finance
Huh?

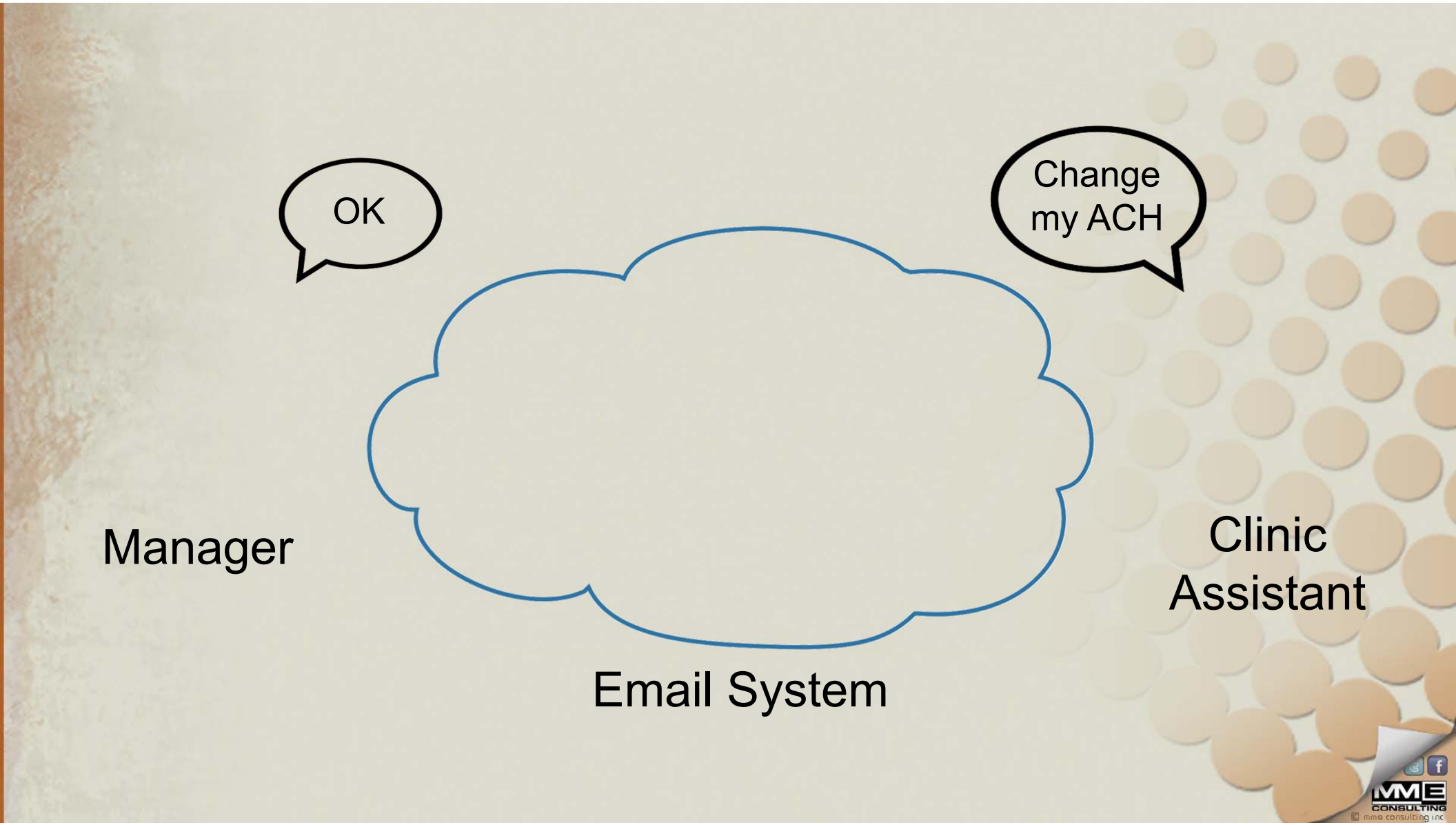

Please Pay
OK
Hacker
Email System
Finance
Huh?
Altered

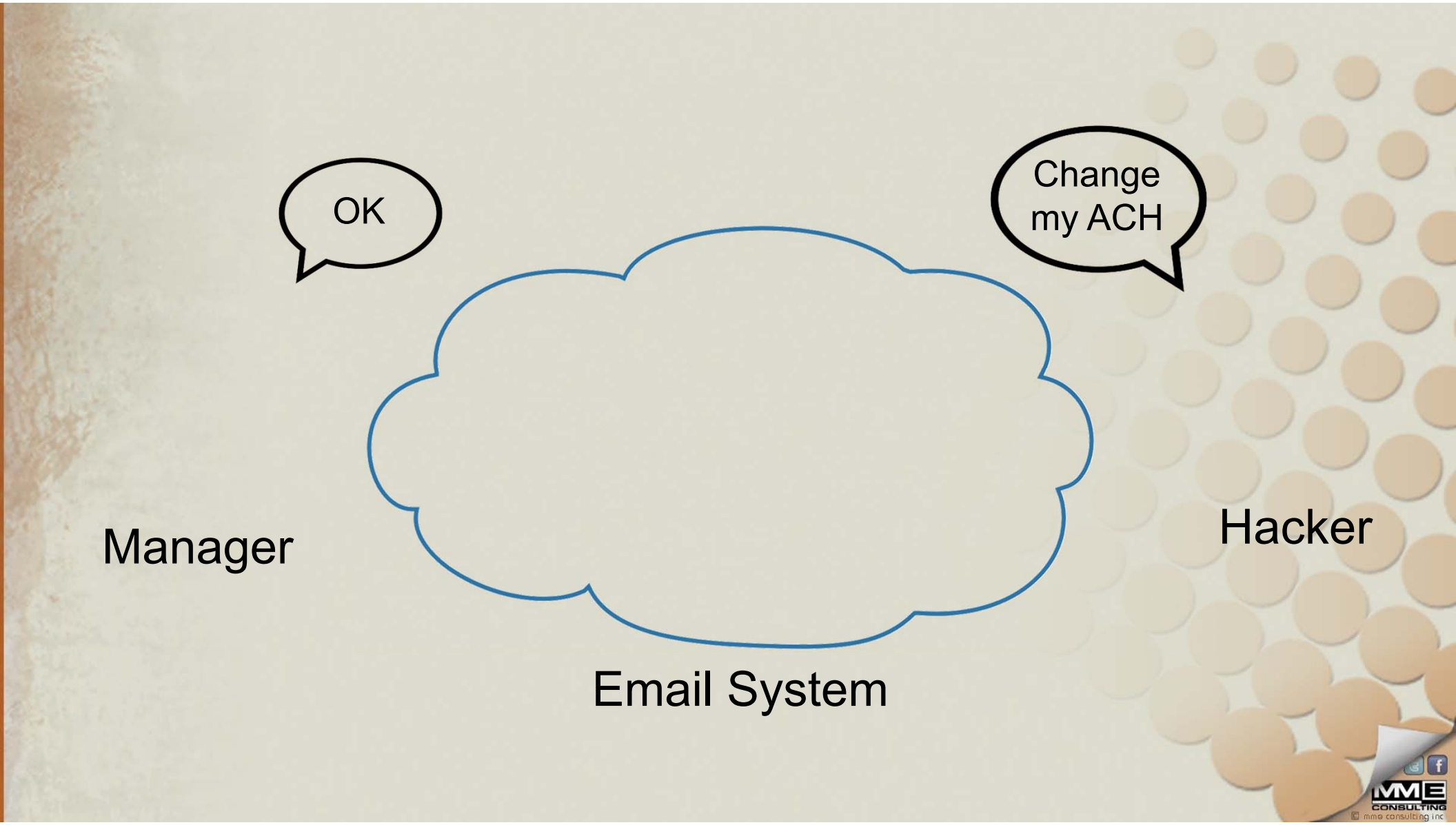
Technology Fails

- Manager Reused Password
- MFA Not Enabled for email accounts
- Geo-Blocking not enabled
  - (Hacker was in Sweden)

Size of the Haul?

About $1,000


OK
Change my ACH
Manager
Clinic Assistant
Email System


OK
Change my ACH
Manager
Hacker
Email System

Technology Fails

- Clinic User Reused Password
- MFA Not Enabled for email accounts

Size of the Haul?

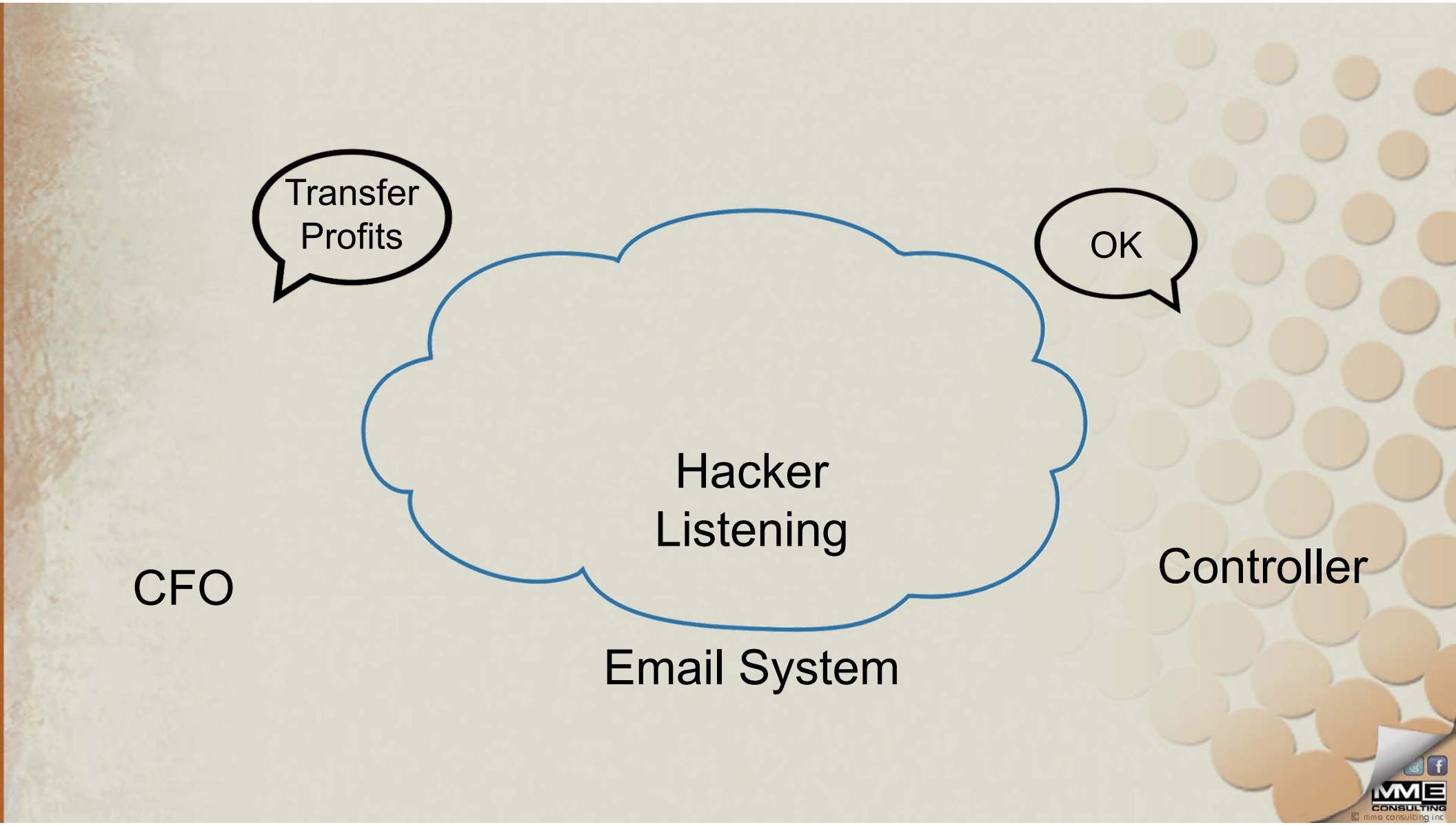
About $5,000

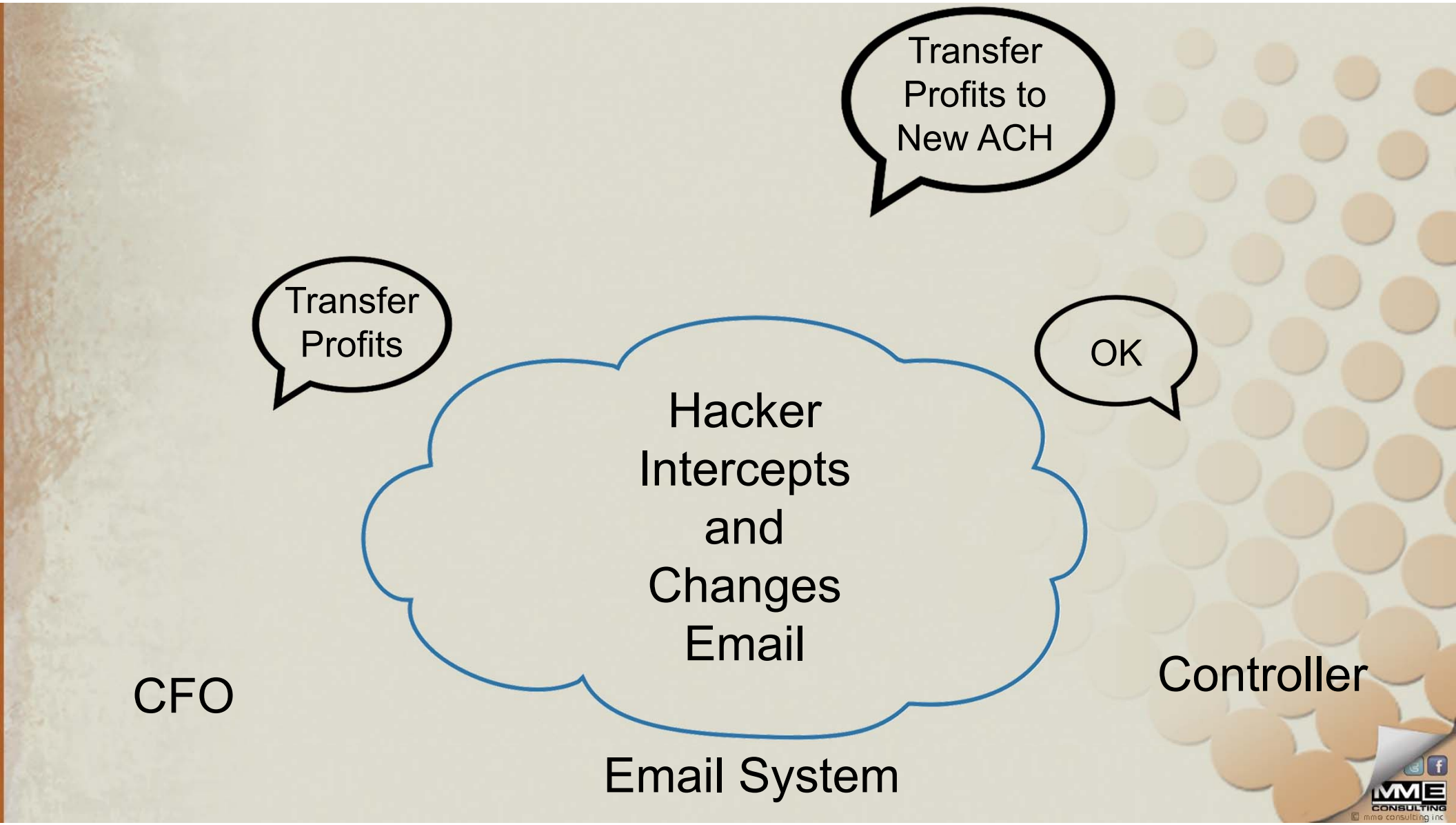
Just one more …

Secret Service

Size of the Haul?

About $800,000!


Transfer Profits
OK
Hacker Listening
CFO
Controller
Email System


Transfer Profits to New ACH
Transfer Profits
OK
Hacker Intercepts and Changes Email
CFO
Controller
Email System

Solution for All Three Events?

- No New Technology Required!
- Free!
- Almost no Training Required
- Can be implemented TODAY!

Solution for All Three Events

Telephone

Financial Change Policy

- Any change in a payment process needs verbal confirmation with the requestor
  - New vendor
  - New account
  - Change of money flow of any kind
- Independent confirmation by the person processing the change
  - You call them to verify

Artificial Intelligence (AI)

- Google CEO quoted as saying that "AI is the most profound technology humanity is working on. More profound than fire, electricity, or anything that we have done in the past"

- So big that even Googles CEO is coming out and saying government regulation is needed, and fast.

How can AI help an Orthodontic Practice?

Augmenting an Orthodontic Practice with AI

- Orthodontics requires extensive knowledge and expertise, which can be time-consuming and overwhelming for Orthodontists.
- **ChatGPT**, an AI language model, can help augment some of the work in an Orthodontics Practice.
- In this presentation, we will explore how an orthodontist might use **ChatGPT** to enhance their Practice.

Understanding ChatGPT

- ChatGPT is a large language model trained using natural language processing techniques that can understand and generate human-like responses to a wide range of questions and tasks

Leveraging ChatGPT in an Orthodontics Practice

- Orthodontists can use ChatGPT to assist with:
  - Patient communication
  - Marketing materials and communications
  - Staff training and much more
- The use of ChatGPT can help orthodontists save time and improve the quality of care they provide to their patients.

Who Wrote That?

How can we use this at the Practice?

Web Content

Team Training Tools

Security's Weakest Link?

Phishing

Old Nigerian Prince phishing attacks are still out there, but most of us have gotten wise

Spear Phishing

Social Engineering

- Best Feature of a Smart Phone?
- What do we do with them?
- What can a hacker learn from a photo?

Meta Data

What do you know about me?

- White
- Male
- 50’s ish
- Probably Married
- Not Broke
- Exactly where I live
- Who my neighbors are
- … and I might be an ideal target for a hack

What could I do with that Info?

- As a Stalker?
- Contact customer service pretending to be you to reset a password
  - Memes - Security questions
  - Photo – Address
- Make a super convincing Phishing email
  - Since they know so much about you

Send

From GuyNaughty@gmail.com

To... Steven McEvoy;

Cc...

Subject I need your Approval to Paint My House the Same color as yours

Hi Steve,

I hope you don't mind. I live at 21 Bixby Court, just on the other side of your street. I tried stopping by to touch base in person, but no one was home.

I was talking to Chris Holmes our common neighbor and he gave me your email (I hope you don't mind)

I am looking to repaint my house and my wife and I are going to use the same colors of your house (love the sand and terracotta colors)!

The HOA needs us to get an approval from our surrounding neighbors in order to give us the green light.

If you have a quick minute could you please have a look at my application to the HOA and sign it online for me? Hopefully this isn't to big a hassle.

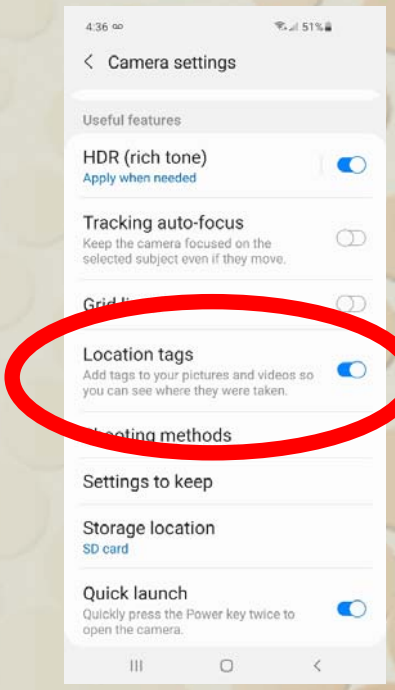
Here is a link to the PDF. Bad link to install Ransomware

BTW – say Hi to Karen for me.

Guy
Dr. Guy Naughty
21 Bixby Court

Protecting Yourself

- Consider if the place you are posting to removes the meta data (Exif data) from photos that are uploaded
- Don’t use Social Media (gasp!)
- Turn off Geo Tagging in your Camera App



What can we learn?

By just reviewing your website …

- Practice Name
- Doctors Name
- Where its located (and time zone)
- Orthodontic Practice
- Windows Computers (?)
- X-ray machine (?)

And with a bit more research …

- Who sells that brand of X-ray Machine (?)
- Where that Company is located
- What's the Average Fee for Orthodontic Services

How would you Phish them?

- Email?
  - Unsolicited Resume with infected PDF attached?
    - ChatGPT to the rescue here!
  - Some sort of scam for the X-ray machine?

- How about a Phone Call?

Meet Dr. Thomas & Team

VS.

What do we know so far?

- ThomasOrthodontics.com
- Thomas Orthodontic
- Dr. Larry Thomas
- California Office
- Orthodontic Practice
- Windows Computers
- CBCT X-ray machine
  - But I don't know what model (yet)

To Learn what Brand of X-ray

- Initial Call Video
- See my link to the video on YouTube

And with a bit more research …

- Dexis Imaging makes the iCAT
- Dexis support of ICAT is in Philadelphia

DEXIS™

And now for the win …

A couple of weeks later I place another call

See my link to the 2nd video on YouTube

With about 15 minutes of time invested …

- Got a staff member to click on a link
- Accessed Patient Information
- Copied software to a computer in the office and ran an application
- Gathered information about their network
- Copied information out of their office
- Gathered more social engineering info for a future hack if needed

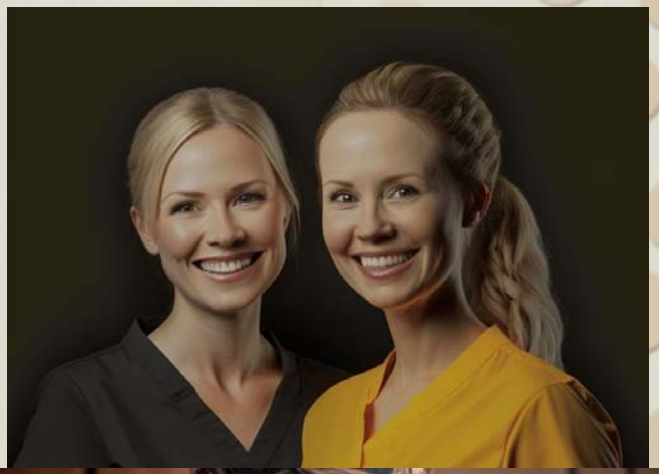
What could they have done?

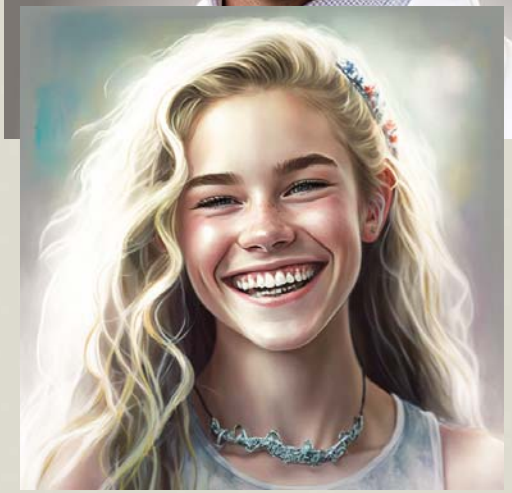
- Question the validity
- Ask Dr. Thomas if he asked for this
- Call them back
- Never let a stranger onto you computer or device (ever!)
- Make it David's the IT guys problem

Camille and Hilari

MidJourney Graphic AI

AI Generated Images





A very real and unfortunately very near future is upon us where we will be fighting off motivated individuals using AI to attempt to exploit us.

Good guys have AI tools with Morals, Bad guys don’t.

Takeaways…..

- Financial Change Policy
- Consider turning of Geo Tagging in Camera App
- Be skeptical of any inbound initiated call that requests information or access to a computer
  - Default to NO unless you confirm
- Explore using ChatGPT for positives within the Practice

Takeaways…..

- Be wary
- Get Cyber awareness training for your entire Team
  - Cyber Insurance Carriers are starting to require
- You are going to need help (Human and/or AI)

Cyber Warfare

There is open warfare raging on the Internet. Organized groups, some are even state sponsored. There are Billions of dollars to be had for the winners.

They are particularity interested in attacking health care providers – JUST LIKE YOU – since they are aware that you have external pressures w.r.t. data security – ePHI and HIPAA. (or is it PIPPA in Canada?)

LATEST HEALTH DATA BREACHES NEWS

Ransomware Attack on Digital Dental Records Impacts Many Providers

On Monday, a ransomware attack on the Digital Dental Record and PerCSoft's cloud remote management software infected "many" dentist offices before the threat was contained.

By Jessica Davis

August 29, 2019 - The computers systems of a large number of US dental offices were **infected** with ransomware on Monday, after a malware attack on the Digital Dental Record and PerCSoft's cloud remote management software. The impacted providers are still attempting to recover access to their patient data and systems.

Wisconsin-based Digital Dental Record and PerCSoft partnered on DDS Safe a medical records retention and backup solution. Digital Dental Record also provides dentists with a quality record keeping system.

WDA
WISCONSIN DENTAL ASSOCIATION

August 29, 2019

To all Wisconsin Dental Association members:

As we head into the holiday weekend, I want to take a moment to update you on an ongoing situation involving DDS Safe, a WDA endorsed product that is part of the WDA Insurance & Services Corp. At 8:44 a.m. on Monday, Aug. 26, WDAISC learned that ransomware had been deployed on the remote management software DDS Safe uses to back up client data. PerCSoft, the IT vendor for DDS Safe, took immediate action to contain the threat; however, roughly 400 practices around the country lost access to electronic files as a result of the virus.

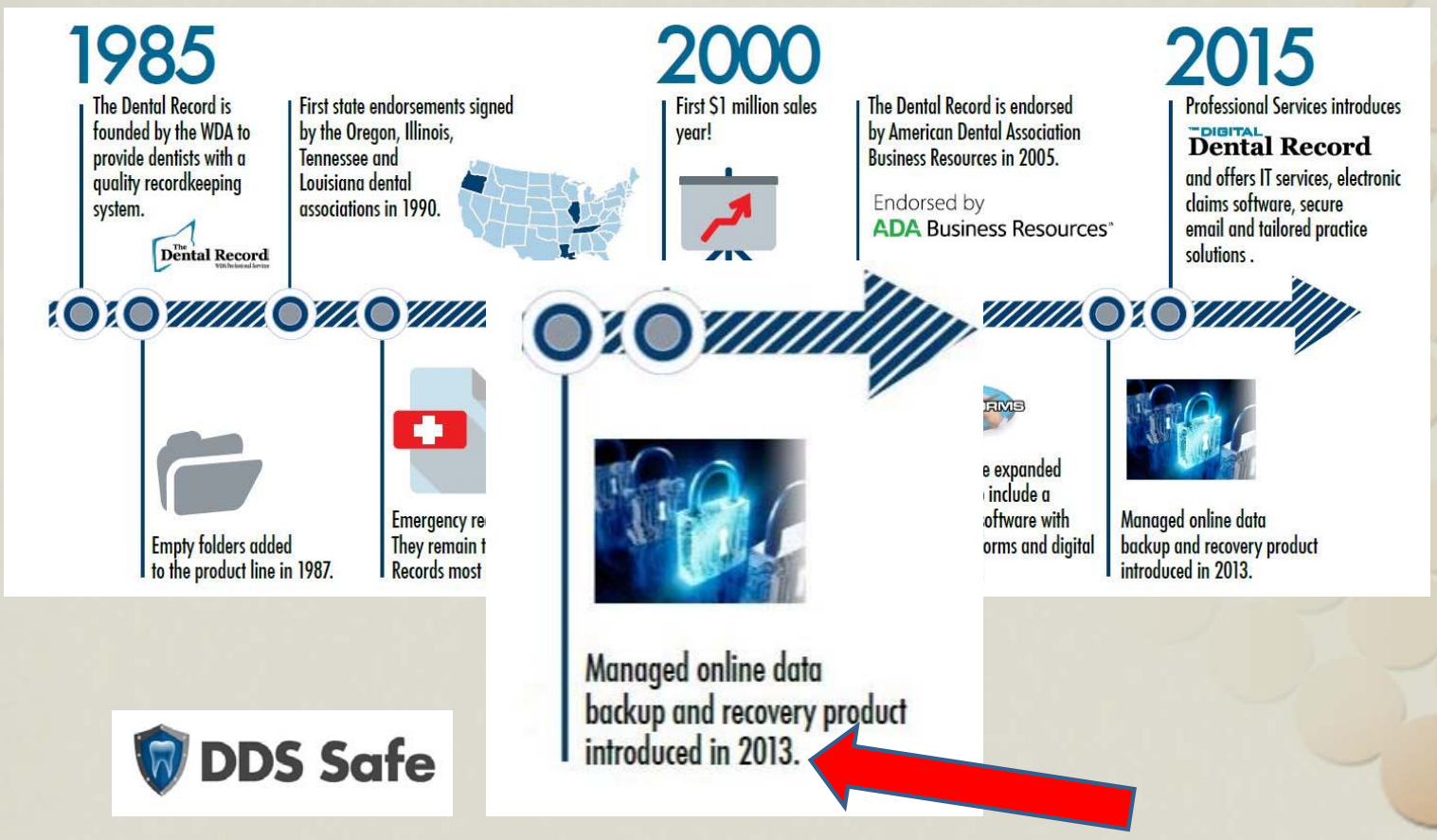
As we head into the holiday weekend, I want to take a moment to update you on an ongoing situation involving DDS Safe, a WDA endorsed product that is part of the WDA Insurance & Services Corp. At 8:44 a.m. on Monday, Aug. 26, WDAISC learned that ransomware had been deployed on the remote management software DDS Safe uses to back up client data. PerCSoft, the IT vendor for DDS Safe, took immediate action to contain the threat; however, roughly 400 practices around the country lost access to electronic files as a result of the virus.

situation, offering our assistance and fielding calls from members and the media. We are working closely with legal counsel, our insurers, the ADA and WDAISC leadership to ask questions, get answers and determine our next steps moving forward. At all times, what is good and right for our members, our members' livelihoods and the strength of the WDA is top of mind.

Our understanding is that only a small percentage of the affected practices are in Wisconsin, and that WDAISC and PerCSoft have been in touch with most of them. If you continue to have questions or would like to discuss this matter further, please feel free to reach out to WDAISC President Mara Roberts (mroberts@profinsprog.com – add "DDS Safe" to your subject line – or 414.755.4170). We will also provide updates on WDA.org as they are available.

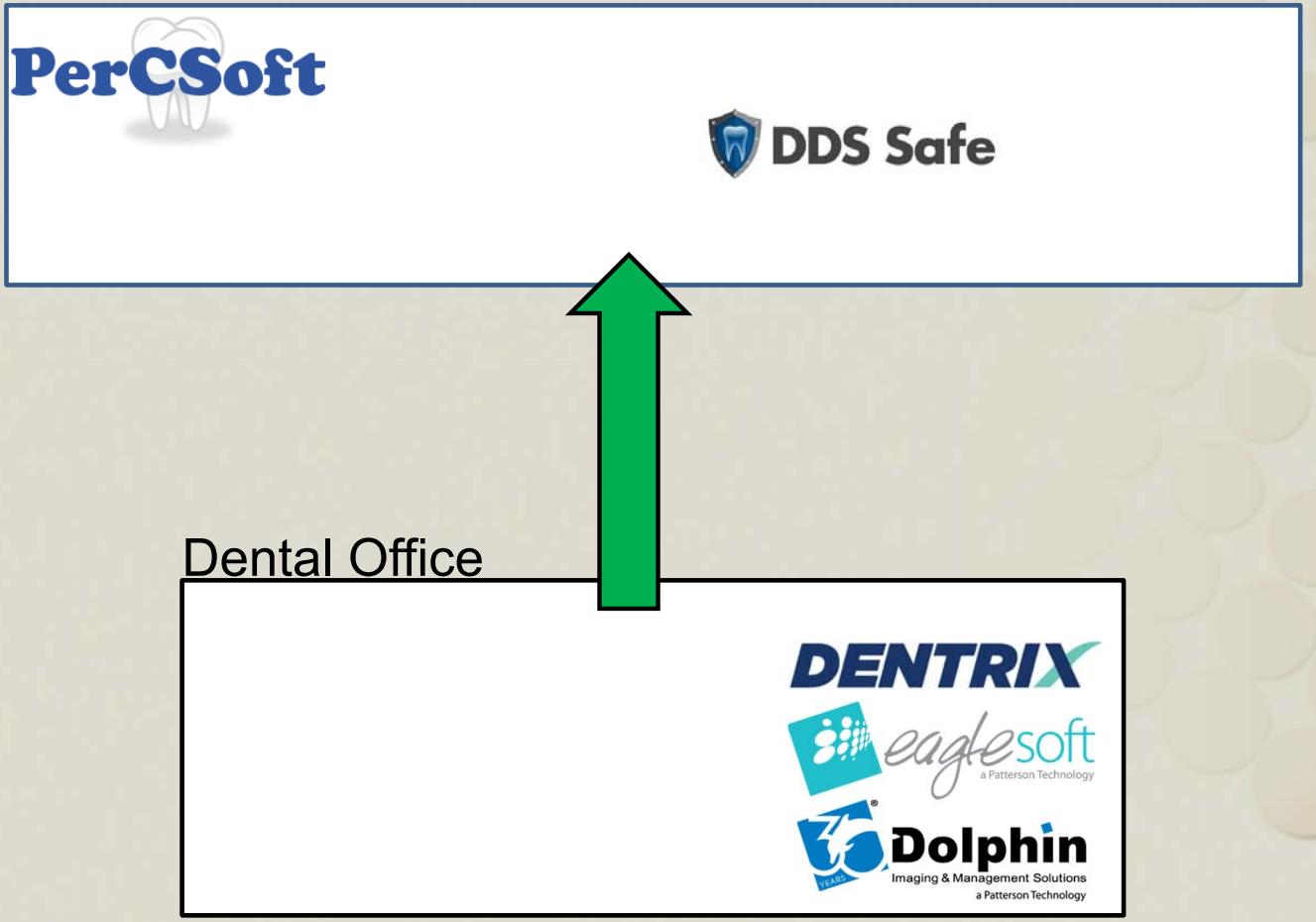
Anyone Here?

The Dental Record



DDS Safe

How did it Happen?



How did it Happen?

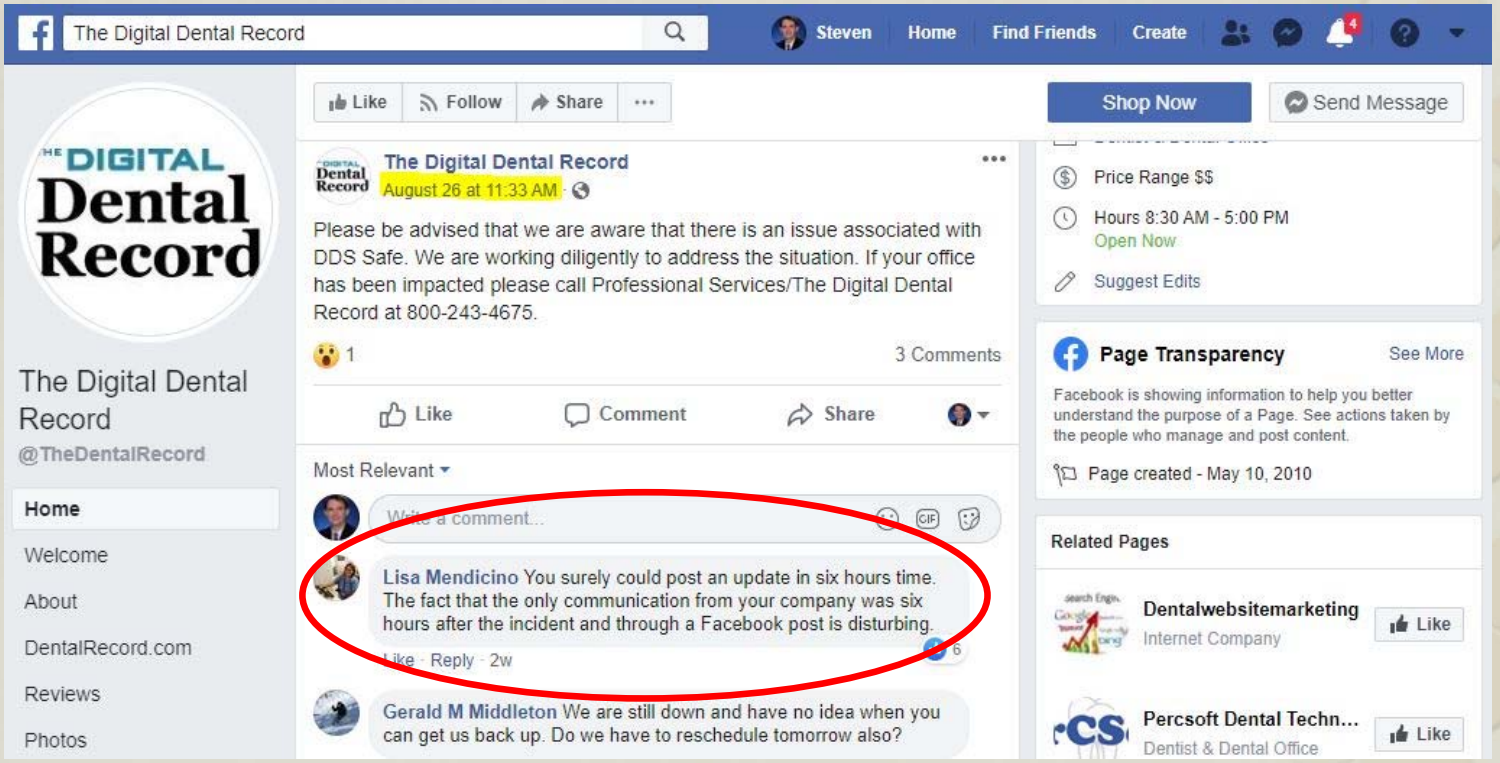
PerCSoft

Un-
DDS Safe

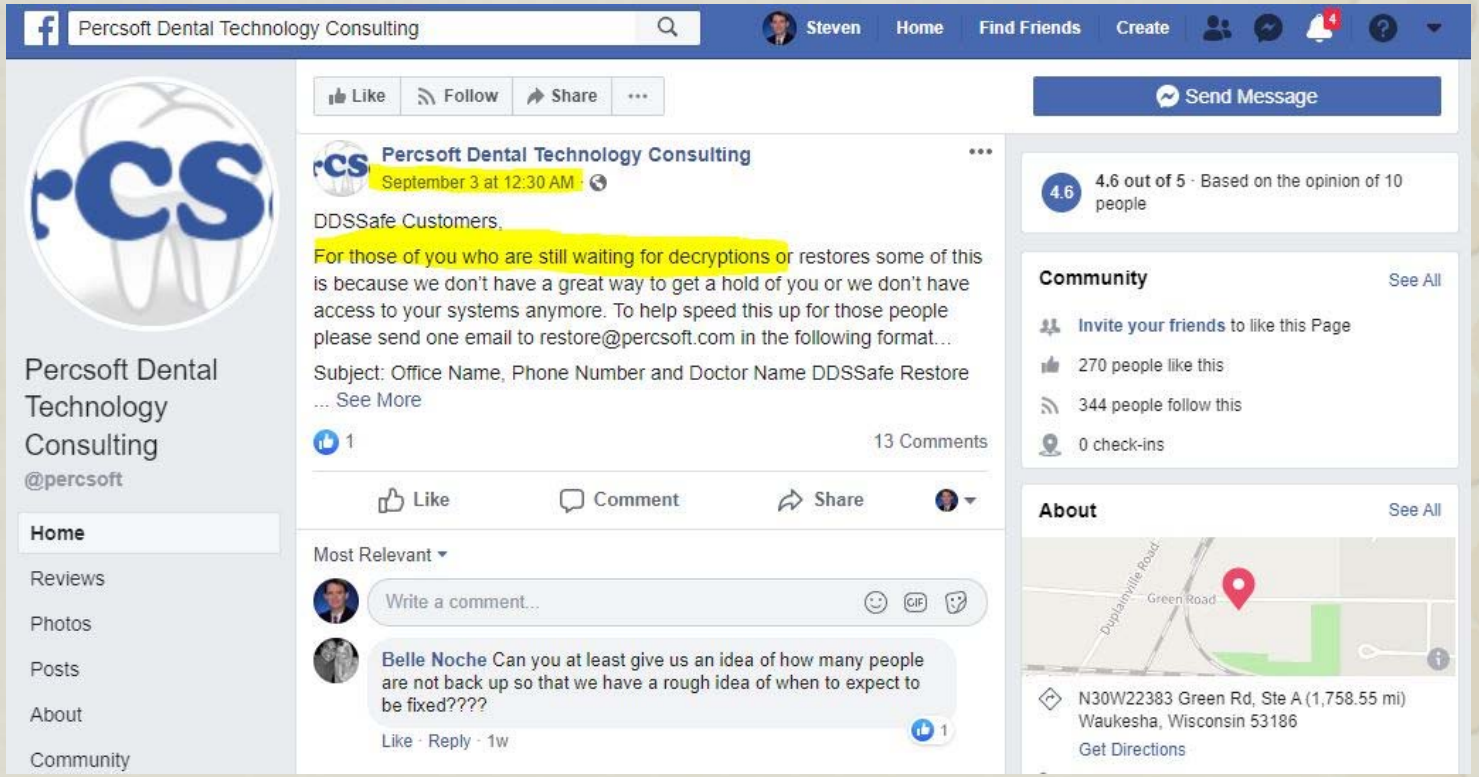
Over 400 !!
Dental Office

DENTRIX
eaglesoft
a Patterson Technology
Dolphin
Imaging & Management Solutions
a Patterson Technology

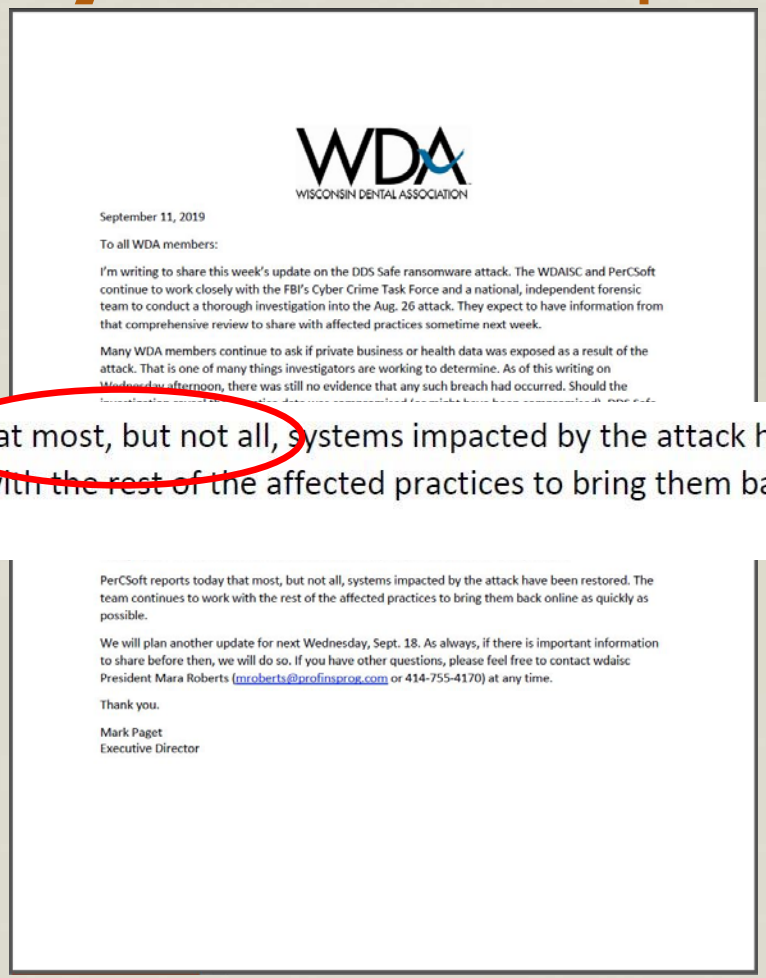
Discovered Monday Aug 26th



9 Days Later – Sept 3rd



17 Days Later – Sept 11th



WDA
WISCONSIN DENTAL ASSOCIATION

September 11, 2019

To all WDA members:

I'm writing to share this week's update on the DDS Safe ransomware attack. The WDAISC and PerCSoft continue to work closely with the FBI's Cyber Crime Task Force and a national, independent forensic team to conduct a thorough investigation into the Aug. 26 attack. They expect to have information from that comprehensive review to share with affected practices sometime next week.

Many WDA members continue to ask if private business or health data was exposed as a result of the attack. That is one of many things investigators are working to determine. As of this writing on Wednesday afternoon, there was still no evidence that any such breach had occurred. Should the

PerCSoft reports today that most, but not all, systems impacted by the attack have been restored. The team continues to work with the rest of the affected practices to bring them back online as quickly as possible.

PerCSoft reports today that most, but not all, systems impacted by the attack have been restored. The team continues to work with the rest of the affected practices to bring them back online as quickly as possible.

We will plan another update for next Wednesday, Sept. 18. As always, if there is important information to share before then, we will do so. If you have other questions, please feel free to contact wdaisc President Mara Roberts (mroberts@profinsprog.com or 414-755-4170) at any time.

Thank you.

Mark Paget
Executive Director

Head in the Sand is not a strategy

There may be some of you in the audience vaguely aware that this risk exists for your business (your Practice is a business after all) but unclear where to start.

“I haven’t been hacked yet doing what we’ve been doing – so it must be good enough”

I would argue that **most of my clients can do better**, and I know the risk they are under. The challenge is **evolving day to day** (not by month or year).

As the IT team, **we are the underdog trying to catch up with defenses to counter a highly motivated offense**.

Top 5 'Gotta Do's'

- What would Steve do if he owned a Practice?

Security Building Blocks

Brick Wall Picture – build your defense from the hacker one brick at a time.

Cybersecurity is a VERY large topic. Trying to make your Practice 'secure' all at once is overwhelming

Bite sized chunks – start with one or two, add more as you are ready to adopt them.

Make it easy for yourself. Don't start with all unless you can really tackle them all.

Set a goal to add them at some pace that makes sense.

It Starts With You!

Cybersecurity Mantra

Cybersecurity Mantra

- As the leader you must **Commit to it**
- Security is a **CEO decision**
  - you cannot delegate this
- It's EASY – just **decide right now!**
- You have to **live the mantra** along with your team

Move the Mantra Forward

- **Communicate** with your Team
- **Explain the risks** and your **commitment**
- **Motivate and Enable** others to act

Educate your Team

What is the most likely Source of a Breach?

- Most breaches are started by a staff member being successfully 'Phished'
  - Clicked a link
  - Opened an attachment
  - Fooled by a faked email

The Defense is to Educate your Team

- They don’t have this knowledge when hired
- Use a structured setting
- Share the risks and your concerns
- Make it clear this is now Practice culture

Educate your Team

- Build it into HR
  - Cybersecurity Policy
  - Part of employment manual
  - Onboarding training
  - Peer mentoring

Educate your Team

- Have **knowledgeable people** train them about Cybersecurity risks
  - Phishing attacks
  - ePHI
- Online Cyber Awareness Training is Available
  - Self Paced
  - Inexpensive
  - Annual
  - Every person!

Educate your Team

- Build good habits from the start with new hires
- 'Old dawgs' don't like to learn new tricks
- Make it clear that **non-compliance and/or circumvention** puts the Practice at **great risk**

Security Focused IT Team

Use a Security Focused IT Company

- Unless you DIY – you need to find your own nerds that believe in this Mantra
- Sadly they may only pay lip service to it just to tick the box, and nobody really notices until its too late.
- Talk to your IT company's manager about your own commitment, and judge their response
- Get an external **third party audit** done to see the current state of your network.

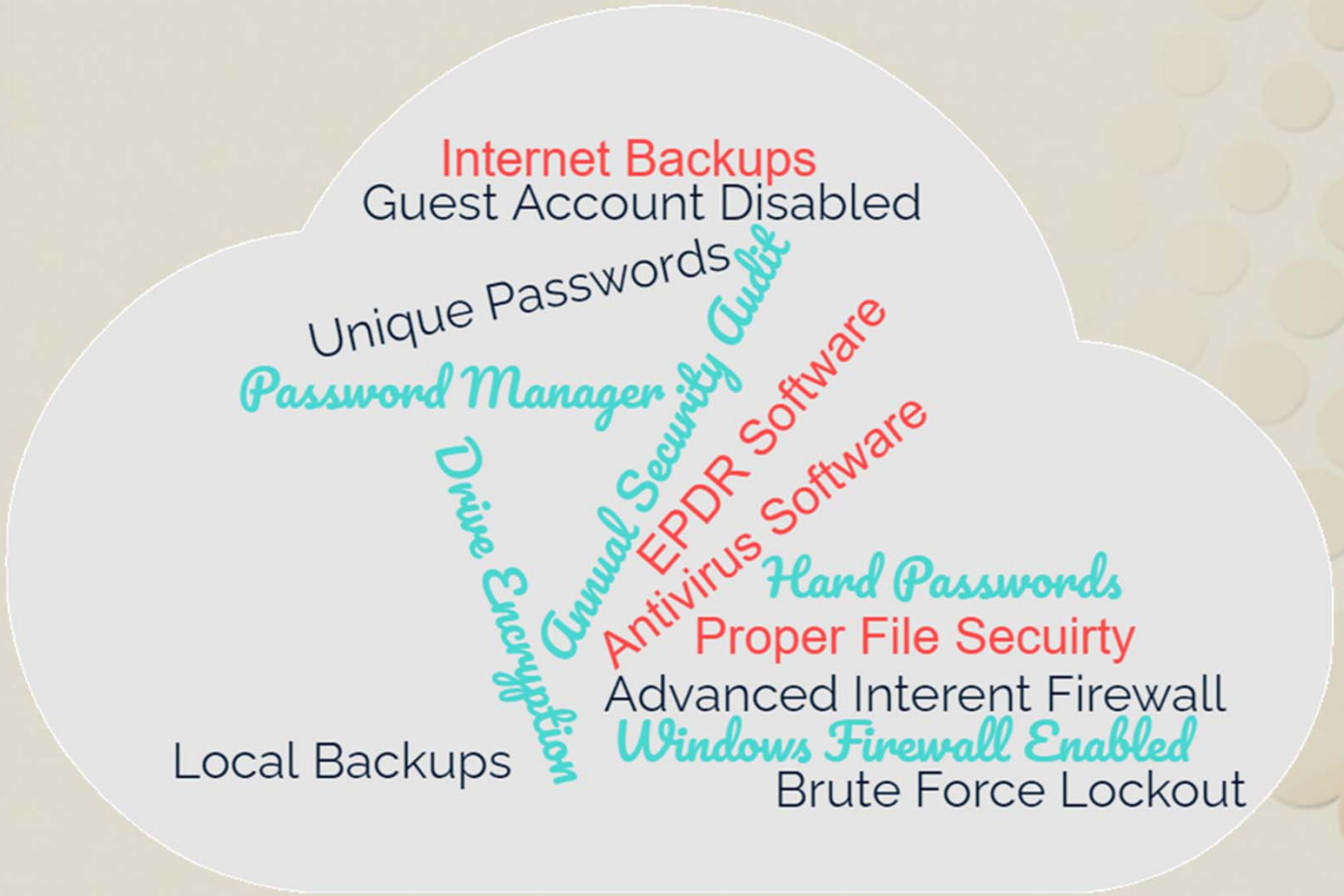
Have they given up?

- They may be beat down about this
  - by their clients relentless **demand to minimize costs**
  - By their clients relentless **complaints about the hassles**
  - By the **software companies poor designs** that just prefer that security it defeated
- They throw in the towel and have a lax standard that functionally works for most Practices at a minimal cost, but is less than ideal.

Enable Them!

- Give them the approval for the extra effort to **raise the bar for you**
  - Expect there will be some (modest) costs to this
- You don't have to build the entire brick wall all at once
  - Spread the costs
  - Easier on the staff training
  - Start with the most important bits

Are they at least Doing the Basics?



Do they drink the Kool-Aid?

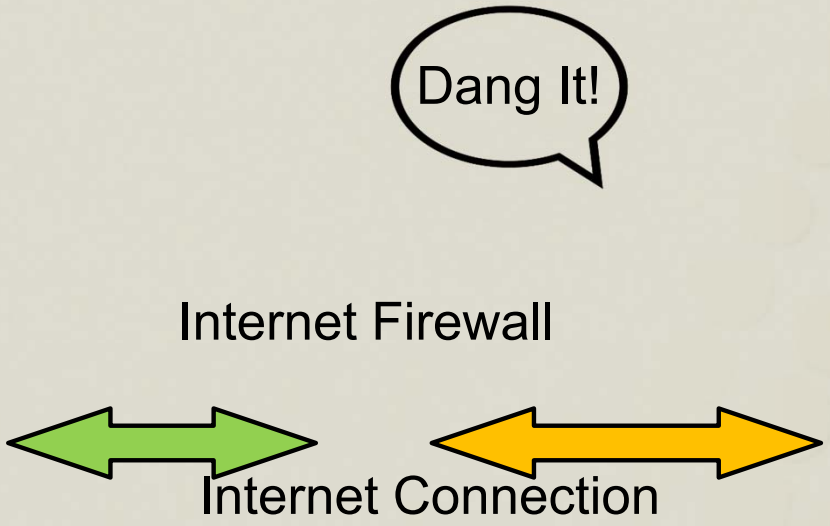
- Do they run their own business as safe and secure as you want yours to be?
- **They have the Keys to YOUR kingdom!**
- Hackers are deliberately attacking IT companies in order to attack 100's of their clients at a time

Stop & Think

- Have you shared your Mantra specifically and clearly?
- Do you see them evolving the security?
  - Security challenges change constantly
  - If you don't see any activity from them, don't assume its happening behind the scenes. Ask.
- Do they take Security seriously at their own business?

Security Keen
IT Team

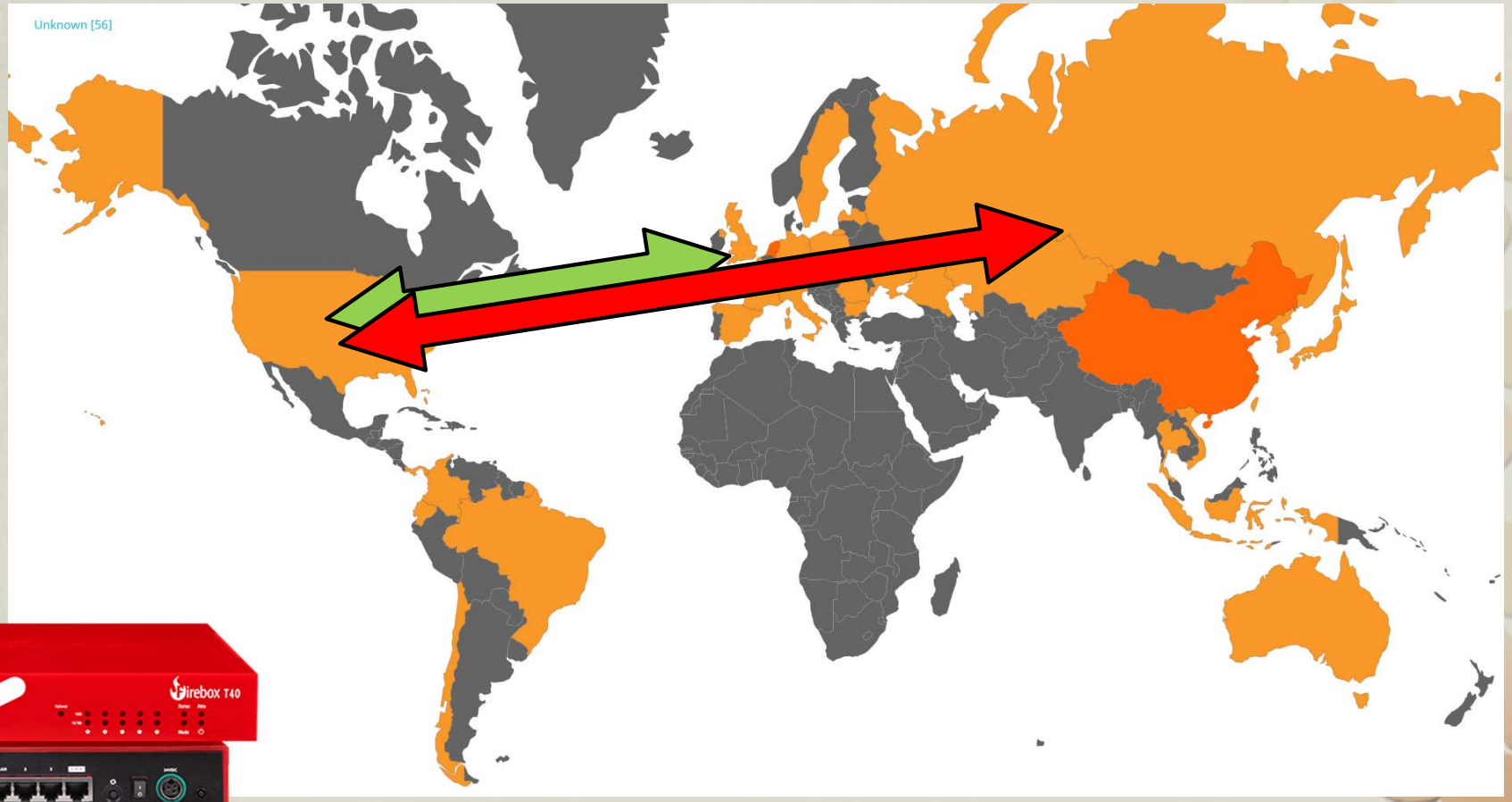
Advanced Internet Firewall



Advanced Security Internet Firewall

- Not just a regular Internet Firewall
- Does all sorts of new tricks (too many to cover all)

GeoBlocking



Reputation Enabled Defense (RED)

- Keeping you from **known bad sites**
- If you click on a link that it knows is going to a website that has bad stuff, it won't let you do it.

Advanced Security Internet Firewall

- Many Practices own these, but the **features are Turned Off!**
- It is **NOT a Set & Forget device**

Stop & Think

- Do you know that you have an advanced security Internet firewall?
  - Is it less than 5 years old?

- Do you know that all the security features are actively enabled?

Advanced
Firewall

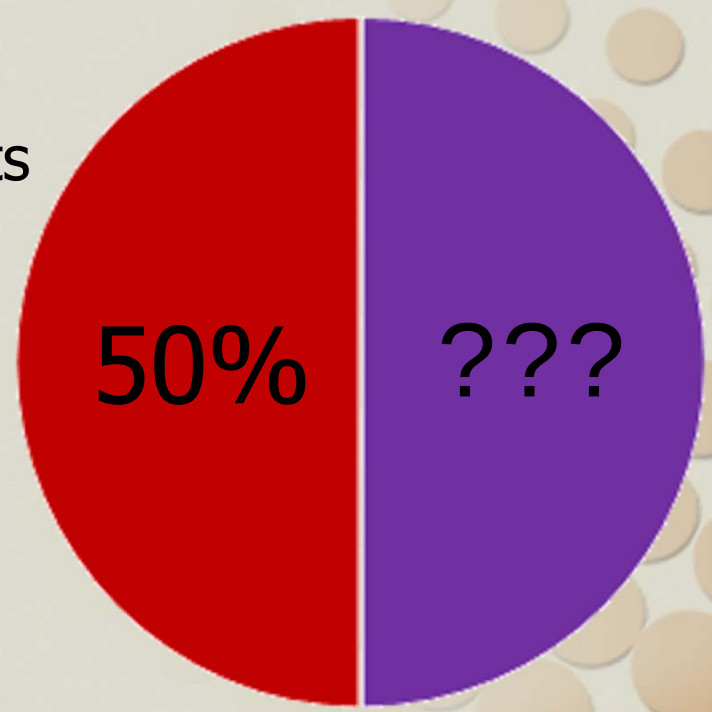
Antivirus Software

Internet Firewall

Last Line of Defense!

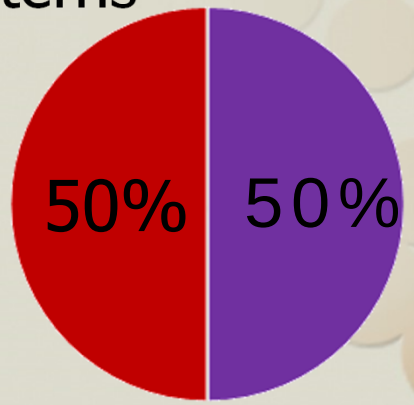
Traditional Antivirus Software

- Stops the well **Known Risks**
  - Only defending about 50% of the threats
- Installed on EVERY PC and Server
- Needs to be Managed



Endpoint **P**rotection **D**etection & **R**esponse

- New thing – **EPDR**
  - a.k.a. 'Next Gen Antivirus'
- Trying to detect the **Unknown** 50%
  - Looks for peculiar behavior patterns
- Must be Managed
  - Not 'Run and Done'



Stop & Think

- Do you have Antivirus on every device?
- Is it actively Managed?

- Do you have EPDR software?
- On every device?
- Is it actively Managed?

AV & EPDR

Cyber Insurance

- Do you have specific Cyber Insurance coverage?
- A single 'Event' can easily exceed $100K
  - IT Expenses
  - Cybersecurity specialists
  - Legal Team
  - Practice Impact
  - Ransom Paid (?)
- Carry at least $1 million

Cyber Insurance

Takeaways…..

- Set your Practices Mantra
- Communicate with your Team and Train
- Enable your Security Focused IT Team
- Fully Utilize an Advanced Internet Firewall
- Utilize Antivirus and EPDR Software

Advanced Firewall

AV & EPDR

Mantra

Team Training

Security Nerds

Takeaways…..

- Sit down with your IT provider and discuss this presentation
  - Download this presentation PDF
  - Ask "Should we be doing these things?"
  - If they dismiss it, maybe its time to look for a more security conscious IT provider.

Thank You!

Presentation online at
www.mmeconsulting.com/Presentations

steve@mmeconsulting.com

MME CONSULTING
MMEconsulting.com

Technology Planning and Integration for Dental Specialists