

How to Excel at Cybersecurity: A Self-Defense Course

Steven McEvoy

Sunday, April 12, 2026



American Association of Oral and Maxillofacial Surgeons

Oral and maxillofacial surgeons:
The experts in face, mouth and jaw surgery®

Thanks for attending my presentation!

As I mentioned at the end of the in person presentation I always strip the graphics out of my posted online talks in case of any licensing issues.

Please email me if you would like a little help with a review of the Cybersecurity at your Practice.

Hackers are Logging in Not Breaking in

Attention!

Do not rename encrypted files.

Do not try to decrypt your data using third party software, it

We are always ready to cooperate and find the best way to solve

The faster you write - the more favorable conditions will be

Our company values its reputation. We give all guarantees of

Private financial information including: clients data, bills

- Manufacturing documents including: datagrams, schemas, draw

- And more...

What are the dangers of leaking your company's data.

First of all, you will receive fines from the government such

confidential. Your leaked data will be used by all the hacker

Bank details

Disaster Recovery Plan Activated

- Restored 3TB of data to server from local hardened backup device
- All systems were rescanned with EDR
- All passwords were changed
- Replaced hard drives on infected PCs
- Recovery took 8+ hour
- Practice was ready for patients by Sunday evening

Monday – “What Happened?”

- Hackers had phished the Doctors windows login
- They used his login to connect remotely
- Doctor’s login was an ‘Admin’ to the network
- They looked around days before the attack to get the lay or the land
- They launched their attack in the early hours Sunday
- The EDR software automatically shut them down after several minutes and began notifying everyone

Happy Ending?

- The IT recovery was a success, but fact that it had started in the first place muted that
- The hacker announced on the internet they had breached the network and unfounded claims of data exported
- There is an ambulance chaser class of attorney that skims the dark web for these announcements and immediately began to pursue a class action.
- The PR damage is done regardless of the IT recovery

What could have saved the day?

Two things stand out as possibilities:

- Cyber awareness training may have enabled the doctor to spot the phish and steer clear, preventing it from beginning.
- Multi-Factor Authentication was not setup for the Doctors remote access method. If it had, even if they had his username and password, they wouldn't have been able to login to the office network.

Any Remote Access to
the network needs to be
MFA protected

ePHI is Gold



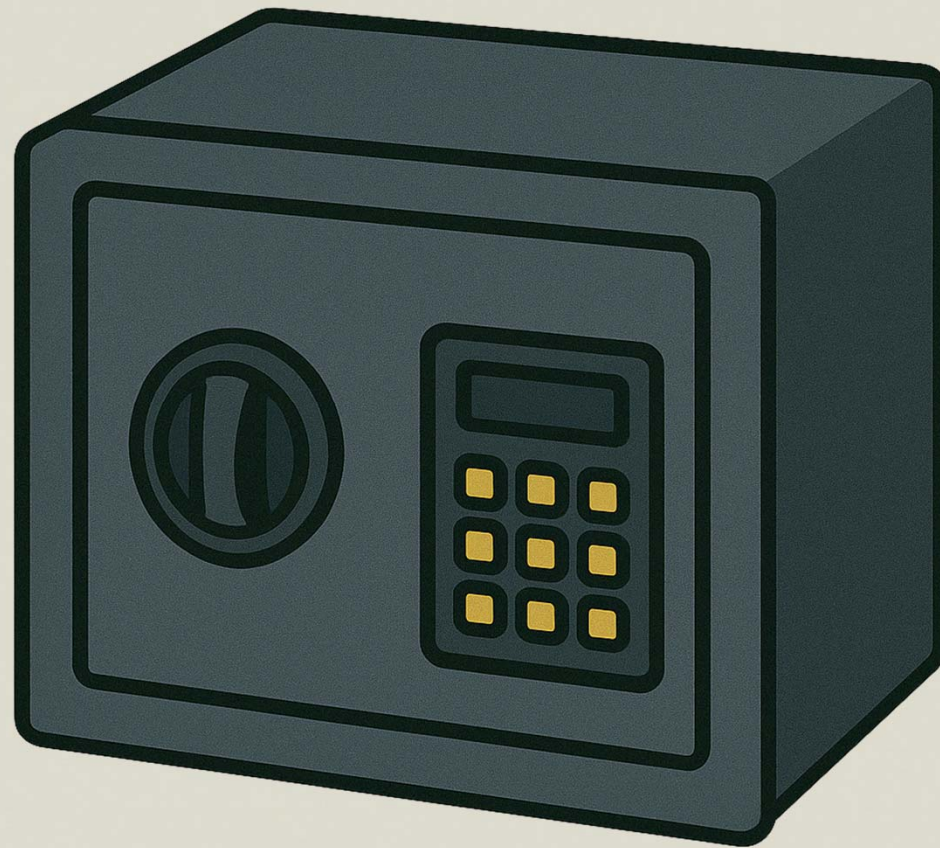
What would you do to Protect this at Home?



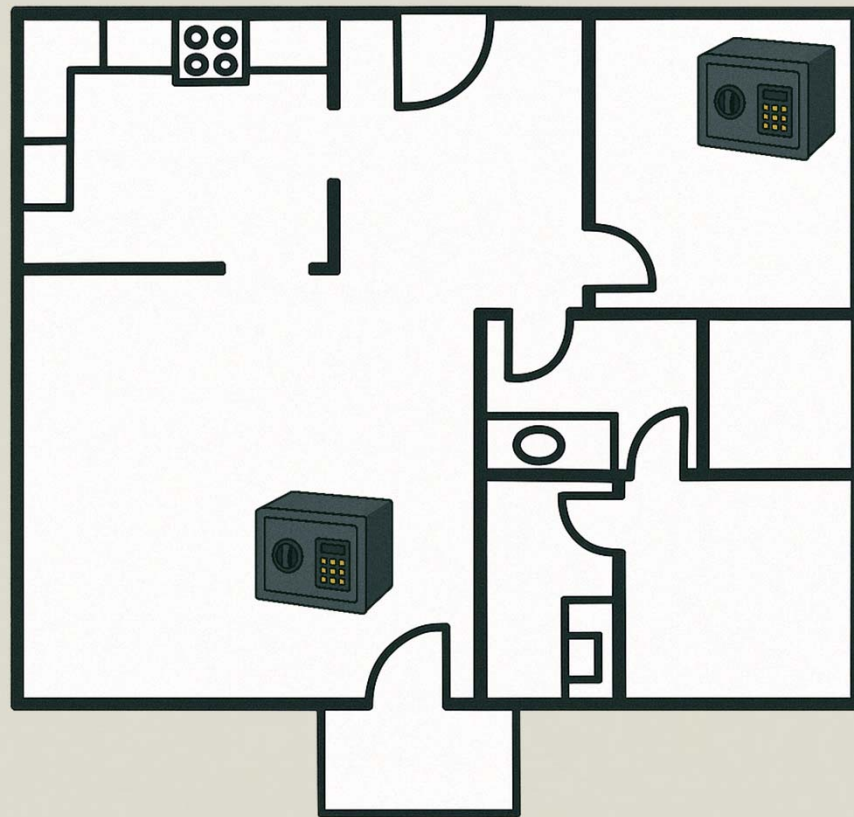
Put it in a Safe



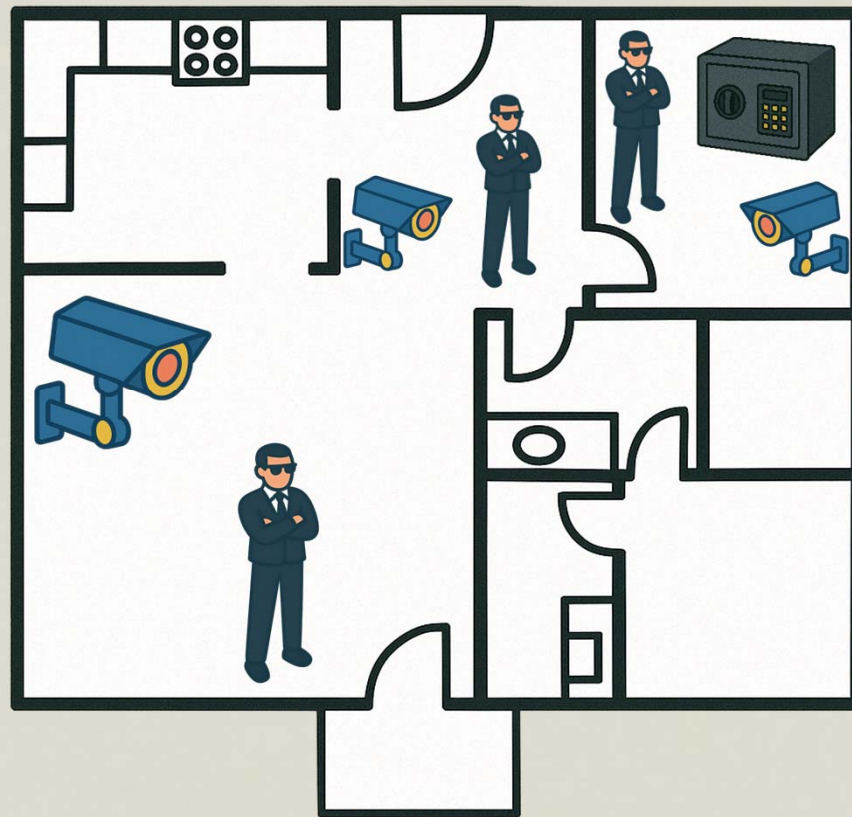
Lock the Safe!



Where in the House?



Monitoring



Insure It!



Leaving the House



Leaving the House



Leaving the House



What about Outside?



Security Measures



Security Measures



Security Measures



Security Measures



Security Measures



Security Measures



Security Measures



All the Thief needs to do then is...

- Breach the wall to get to the yard, or...
- Fool the guards and get through the gate
- Avoid the dogs, guards and cameras in the yard
- Pick the lock to the front door and disable alarm
- Avoid the guards and cameras inside the house
- Crack the safe
- Steal the gold
- Get back out through all the security



Which would you choose?



Why don't we put the same effort into Protecting ePHI?



'House' vs. 'Office Network' Analogy

- **Gold** = ePHI
- **Safe** = Your Practice Management Application
- **House** (rooms and contents) = Server and your Data
- Security **Cameras** = Monitoring and Recording
- Inside **Guards** = Your Staff and EDR Tools
- **Front Door Lock** = Your Windows Login to Server
- Alarm **codes, combinations, keys** = Passwords & MFA
- **Insurance** = Backups and Cyber Insurance

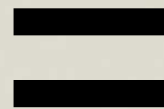
House vs. Office Network Analogy

- **Yard** = Your property, your own Internal Network of PCs, Printers, etc. beyond the Server.
- Outside **Cameras, Dogs** = EDR Software
- **Fence, Gate and Guards** = Internet Firewall
- **Street, sidewalk and neighbors** = Internet

5 Essential Steps in Securing your Practice

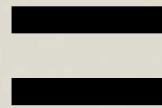
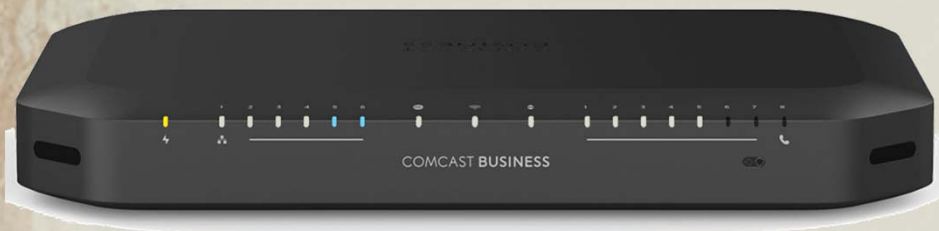


Advanced Security Internet Firewall



- WatchGuard
- SonicWall
- Fortinet
- Sophos
- Others ...

Old or Basic Internet Firewalls



Advanced Security Internet Firewall with Advanced Features OFF



=



Advanced Security Internet Firewall

- The Advanced Features are NOT on by default
- Your IT people must put in the work to deal with the consequences of enabling the advanced features
- They need 'tuning'
- NOT 'Set and Forget'
- Usually a Subscription



Advanced Security EDR Software



=

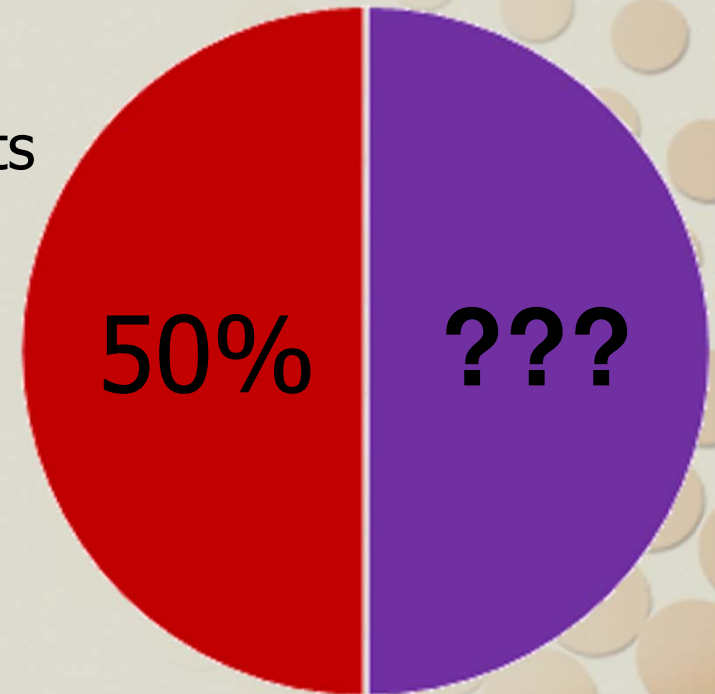
- Sentinel One
- CrowdStrike
- Others ...





Traditional Antivirus Software

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



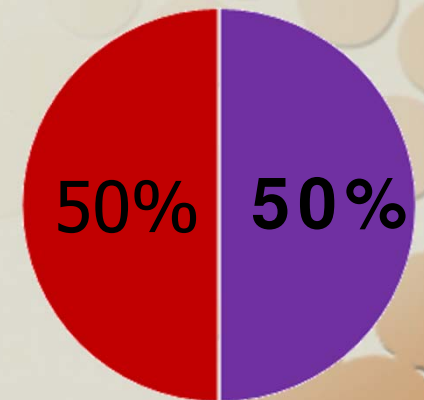
Endpoint Detection & Response

- New thing – **EDR**
 - a.k.a. 'Next Gen Antivirus'



- Trying to detect the **Unknown** 50%
 - Looks for peculiar behavior patterns

- Must be Managed
 - Not 'Run and Done'



Advanced Security EDR Software without Advanced Features Enabled



=



Advanced Security EDR Software without Monitoring



=



Advanced Security EDR Software

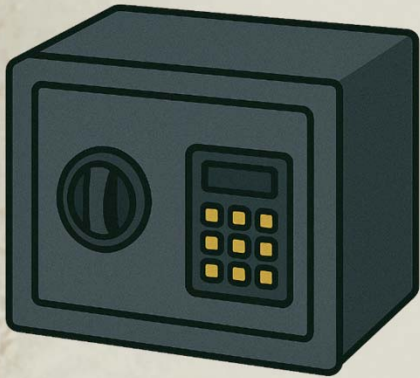
- The Advanced Features are NOT on by default
- Your IT people must put in the work to deal with the consequences of enabling the advanced features
- They need 'tuning'
- NOT 'Set and Forget'
- Usually a Subscription



Questions?



Use Great Passwords and a Password Manager App



=

DogHatBeerHead26

+

1Password.com

Recommendation for Great Passwords (Simple Complexity)

Starting TODAY! (2026 and on)

- Three or Four unassociated dictionary words
- At LEAST 12 characters in length
- Capitalize First Letters
- Add a 2-digit year to the end (reminder)

DogHatBeerHead26

Password Manager Apps

Put passwords in their place.

Works with Touch ID

9:15 AM

Favorites

Search

- Amazon
wendy.c.appleseed@gmail.com
- Evernote
wendy.c.appleseed@gmail.com
- WestJet Mastercard
5555 **** 4444
- TD Chequing
TD Canada Trust
- Personal
Wendy Appleseed
- AgileBits Forum
WendyAppleseed
- Trello
wendy_appleseed@agilebits.com

Keep your information safe and secure.

Secured by your Master Password that only you know.

Master Password

Features for a Password Manager

- Available Everywhere we are:
 - Phones (iOS and Android)
 - Computer (Windows, Mac, Web)
- Sync'd across all my devices
 - Means linked to Cloud
- Secure Web Browser Plugin
 - Fills the passwords in for you (securely)

Features for a Password Manager

- Secure!
 - Especially if Cloud!
 - Encrypted
 - Smart Company
 - Reliable Company
- Free! ?
 - Free is bad
 - Affordable is good

1Password.com

... and others ...

Enterprise eMail with Advanced Security

 Microsoft
Office 365
Advanced Threat Protection

=

 **Suite**
for Business



Enterprise eMail with Advanced Security

- NOT free Gmail!
 - Free = Bad (they are reading your email)
- Advanced Security Not Enabled by Default
- Require MFA on every account
- Setup Geo-Blocking
- Setup DMARC/DKIM/SPF records
- Enable 30+ days of detailed logging
- Monitored by your IT Team

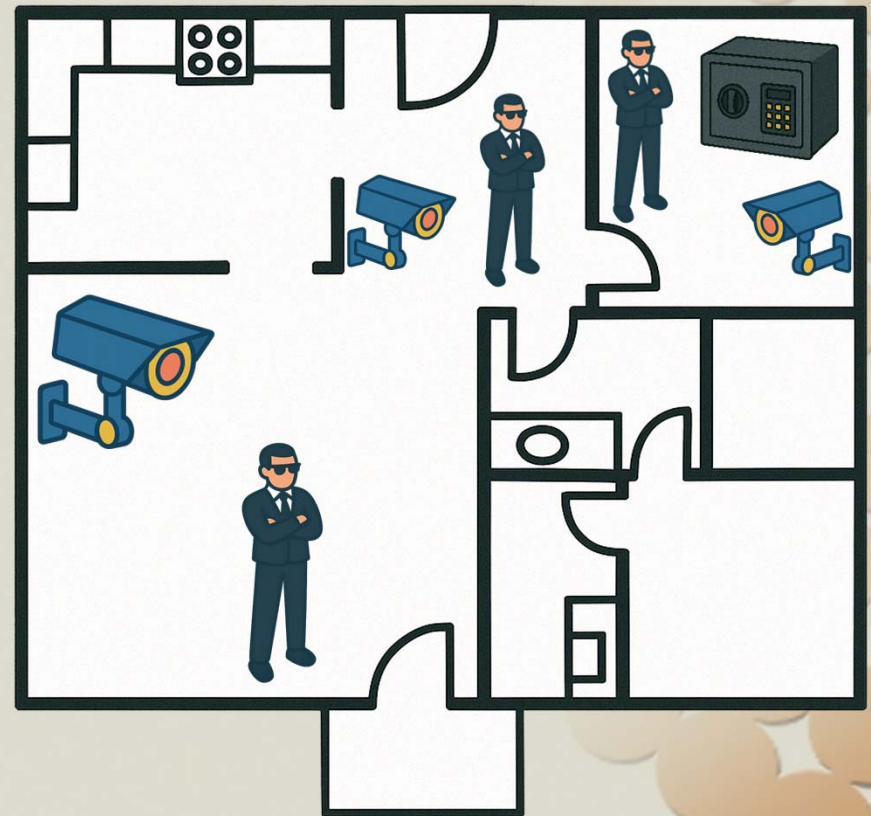
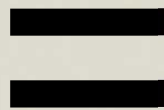


Security's Weakest Link?



Cyber Awareness Training for Staff

Cyber Awareness
Training for your
Team



Cyber Awareness Training for ALL your Staff

- Educate them on how to spot Phishing, Smishing, Sextortion, Spam and Scams
- Everyone especially includes the Doctors
- Online Course – takes <90 minutes
- Annual Refresher
- Reasonable Cost – about \$30 /yr per person
- Cyber Insurance policies are starting to require this



Cyber Awareness Training for ALL your Staff

- You can search for vendors offering this training
- MME Consulting offers online Cyber Awareness training for \$30/yr per person



Insurance (because bad things can happen)

Backups
+
Cyber Insurance =



Backups

- Setup Multiple Backups
- Local Onsite Backup to a Hardened Device
 - Hacker Resistant
 - NOT a traditional USB device
- Cloud Backup
 - 30+ days of daily recovery options
 - Immutable
- Backup ALL your data, including the PM Database



Cyber Insurance

- 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

Let me tell you a story ...

Just one more ...



Size of the Haul?

About \$800,000!



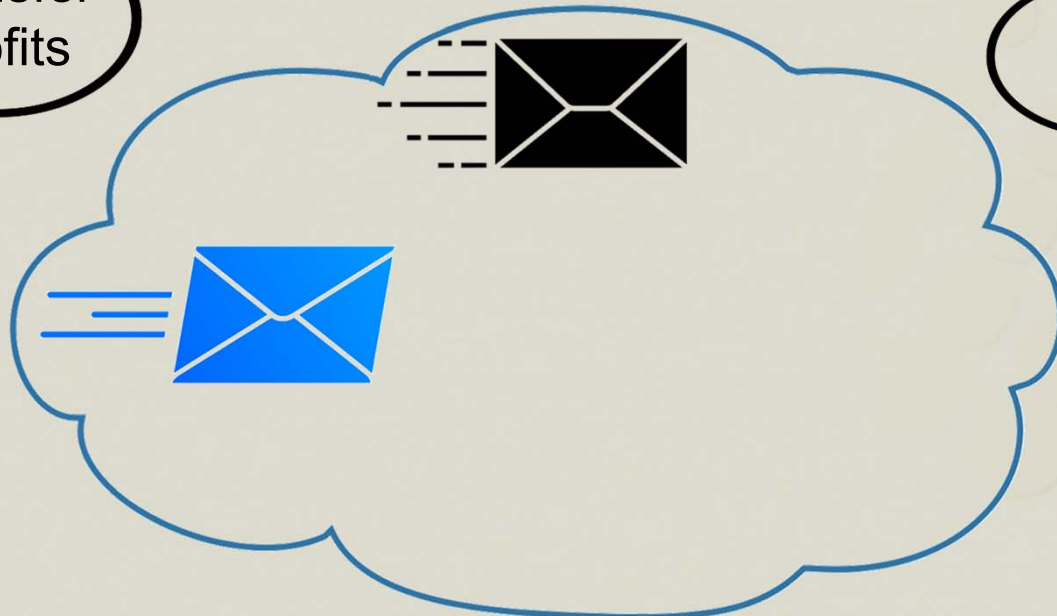


CFO

Transfer Profits



Transfer Profits to New ACH



Email System

OK



Controller

Solution for All Three Events?

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

Solution for All Three Events

Use the Phone!

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

What Should You Do?

Don't panic

Implement one step at a time

Get help from a good IT company

Takeaways.....

1. Use an Advanced Security Internet Firewall with all the features enabled and Monitored
2. Use an Advanced EDR solution with all the features enabled and Monitored
3. Use great passwords wherever the 'Gold' is
4. Use a proper Password Manager app
5. Give ALL your staff annual Cyber Awareness training

A few more takeaways.....

6. Have a robust, hacker resistant Backup strategy that has 30+ days of immutable backups
7. Have dedicated Cyber Insurance for >\$1 million
8. Use an enterprise class email system that is setup properly with advanced security settings
9. Have a Financial Change Policy that **REQUIRES** person to person confirmation

A few more takeaways.....

10. Only use a remote access process that is protected by MFA



Ask for help if you need it!

AI



MME

STEVE

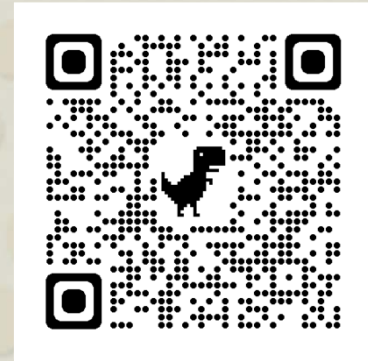
Solves Puzzles



Thank You!

Presentation online at
www.mmeconsulting.com/Presentations

steve@mmeconsulting.com



MME
CONSULTING
MMEconsulting.com

Technology
Planning
and Integration
for
Dental Specialists



mme consulting inc