

Presented by:

Elisabeth Happel

Centralized Service Technician
PEAKE Technology Partners



CYBER DEFENSE STRATEGIES

for Medical Practices

**Recommended action for any
medical practice to mitigate
the risk of cyber attack.**

CYBER DEFENSE STRATEGIES

for Medical Practices











→ Medical practices, along with many other organizations, are being increasingly targeted for cyber security attacks like ransomware. These attacks can (and will) disrupt patient services, cause data leak breaches, result in financial and data loss, and potentially end in legal or oversight actions.

Rather than being overwhelmed by the threat of a cyber security attack, PEAKE would prefer to offer information that you can use to protect and defend your practice. While there may not be a single action that all practices can take to alleviate the likelihood of an attack, we have found that the following strategies are highly effective for protecting all types and sizes of medical practices.

CYBER DEFENSE STRATEGIES

for Medical Practices

- 1 Hyperlink Hygiene 
- 2 Restoration Resiliency 
- 3 Staff Training 
- 4 Security Risk Assessment 
- 5 Policies 
- 6 Redundancy 
- 7 Communication 
- 8 Defense in Depth 

1 Hyperlink Hygiene

Email

- Phishing emails are still one of the top Cyber Security Attack vectors – links, images, and attachments are gateways to virus downloads.
- Today's technology allows bad actors to create very believable 'spam' emails that carry malicious code within images or links. Even more damaging are spoofing emails that appear to come from within your organization, often from a director or administrator, that direct the recipient to make an emergency payment or take some other action which creates a vulnerability.
- No medical practice should be without a robust email filtering system with proactive and defensive rules to block suspicious emails. Settings in your email security vendor can also block spoofing and require proof of a sender's authenticity.

1 Hyperlink Hygiene

Browser

- Browser redirects, pop-ups, and in-site advertising are subtle or sometimes hidden hyperlinks to unknown and dangerous URLs (websites). These websites serve malware to end-users, which can easily move upstream to the network servers.
- Browser controls should be implemented that block advertisements, extensions, and malicious and suspicious sites. Group policies in Active Directory can also be used to control browser behavior.
- Some organizations may choose to enforce company browser accounts - like Google Business accounts. Then private profiles on browsers are eliminated and browser management can be performed administratively.

2 Restoration Resiliency

Backups

- Regardless of our best efforts, computers can fail and data can be lost.
- Medical Practice Policies should always include Data Backup and Business Continuity & Disaster Recovery plans.
- Backups of data should be automated, frequent, tested, and monitored.
- Recovery and restoration should be tested proactively, and regularly and should align with your Business Continuity Policy.
- Backups (and all other critical functions of your network) should have redundancy and native encryption.

2 Restoration Resiliency

Business
Continuity

- Every organization should create a set of policies and plans for steps to take in case of an event or emergency.
- Leadership and key personnel should know their responsibilities and tasks if there is a break in business continuity.
- Chains of command and communication should be planned and documented on paper, as should Business Continuity and Disaster Recovery plans. In the event that your systems and network are offline, do not find that your carefully made plans are unavailable.

2 Restoration Resiliency ↻

Business
Continuity

- The ability to restore and reconnect to your data is a high priority for your practice to get back to patient service - this should be discussed with your IT support at length, to find the best solutions.
- Recovery and restoration should be tested proactively and regularly and should align with your Business Continuity Policy.

3 Staff Training

- A well-educated staff, at all levels of the organization, is one of your best protections against cyber attacks.
- Providing monthly or quarterly staff training can be cost effective and morale boosting (staff can apply the education in their personal online lives, too). *In 2021 the average cost to an organization to restore systems and data after a ransomware attack was nearly 2 million dollars.*
- There should be organizational awareness that the high level and more public personnel are more likely to be targeted – and are therefore more in need of in-depth training and protective measures. Consider providing both basic staff training and executive level training for more focused learning.

3 Staff Training

- Recognize that cyber security defense training is just as critical and effective as all other forms of training that your staff receives.
- **Staff training should minimally cover:** HIPAA digital education, email attacks, hyperlink and redirection attacks, online hygiene, threat and mitigation communications, and authentication protections like MFA (multi factor authentication). Breaking these modules up quarterly can be more palatable to staff and management alike, and will provide fresh material throughout a year.

4 Security Risk Assessment

- SRAs take an analytical and unbiased look into your current network posture.
- They allow your organization's leadership to set resource priorities to mitigate detected vulnerabilities.
- They remove the emotional approach to fixing network issues (like pet projects).
- SRAs also provide a roadmap for mitigation continuation, so that your practice is constantly increasing its security posture.

5 Policies

- It is not possible to create and maintain a secure network without Policies.
- Policies are the documented standards that the organizational leadership have established (and maintain) as the baselines for how to conduct their business.
- Policies should be reviewed annually, or when network and organizational changes occur to keep them up-to-date and to ensure that your technology aligns with your policy.
- Policies should cover, at a minimum:
 - Passwords and authentication for all users
 - Internet use, access, and privacy
 - Technology and device use
 - Data, system, and network protections
 - Data recovery and Business continuity plans

6 Redundancy

- Every critical function of your Medical Practice should have technical redundancy whenever possible.
- Redundancy will minimize or eradicate single-points of failure.
- Minimal redundancy will include:
 - Access to the Internet - 2 lines
 - Servers that house data and applications - virtualization and image level backups provide redundancy
 - Backups - this is usually implemented with a network appliance and cloud replication

7 Communication

- Talking to your leadership and staff about current threats facing your genre of organization ensures that personnel are aware of the digital landscape.
- Round-table discussions are great ways to role-play or enact Business Continuity and Disaster Recovery plans to ensure that they are comprehensive and relevant.
- Having a live channel of communication for cyber-related questions and concerns will allow for a dialog that helps boost personnel engagement.
- Regular communication amongst staff and stakeholders is a good and constant reminder that security is everyone's responsibility.

8









Defense in Depth



- The best network and data protection is achieved through layers of defense. There should be no point on your network that is accessible directly from public Internet space; everything should be positioned behind multiple protection mechanisms.
- This is implemented with the help of your IT Support company, and should be discussed in detail to ensure that a defensive measure is employed in every area of your domain.
- One critical layer of defense is a robust monitoring system that alerts your IT Support team when there is an event that needs mitigation. Monitoring should exist for network devices, servers, backups, email filtering systems, anti-virus agents, and workstations - and alerts should flow into a central ticketing system so that issues can be addressed.

CYBER DEFENSE STRATEGIES

for Medical Practices

- 1 Hyperlink Hygiene 
- 2 Restoration Resiliency 
- 3 Staff Training 
- 4 Security Risk Assessment 
- 5 Policies 
- 6 Redundancy 
- 7 Communication 
- 8 Defense in Depth 

Any Questions?

Contact a PEAKE Practice Advisor info@peaketechnology.com or (866) 357-3254

Presented by:

Elisabeth Happel

Centralized Service Technician
PEAKE Technology Partners



CYBER DEFENSE STRATEGIES

for Medical Practices

**Recommended action for any
medical practice to mitigate
the risk of cyber attack.**