# Cybersecurity Resources to Protect Your Practice

**By Loretta Verbeck, MS, FACMPE, CHC**

It is difficult to make it through an entire week without a new cyberattack making the news. The FBI reported in their 2020 Internet Crime Report 791,790 complaints regarding cybercrime last year, representing an increase of more than 300,000 over 2019. The reported losses from these crimes exceeded $4.1 billion. By some estimates, only 15% of cybercrimes are reported, meaning the actual number of victims may be 1.5 to 2.5 million. Phishing scams, ransomware, and server attacks continue to impact individuals and businesses, with the business of medicine maintaining a high spot on the list.

Healthcare organizations must be diligent in their efforts to protect the systems that contain protected health information (PHI) and other sensitive information, such as employee personally identifiable information (PII), from cybercrime attacks. However, understanding the necessary steps and implementing the appropriate safeguards to

manage cybersecurity can be overwhelming for many practices.

To assist policyholders with the daunting task of cybersecurity, SVMIC is committed to providing members with resources, including a series of articles that will guide policyholders through the steps necessary to develop an effective cybersecurity program. Topics will include:

- Security Risk Analysis
- The Importance of Proper System Backups
- Understanding Cyber Liability Coverage
- Ransomware
- Using Technology to Secure Systems
- Responding to Security Incidents

SVMIC has partnered with Tokio Marine HCC to provide all policyholders with cyber liability coverage and cybersecurity resources through CyberNET. To access these resources, visit this link which will require you to log in to your Vantage® account. Here you will find sample security policies, resources for responding to security incidents, cybersecurity training videos, and more.

Because ransomware and email fraud are two of the most common cyberattacks, CyberNET provides critical information on both topics.

Top 8 Ways to Beat Ransomware is an eight-step checklist including:

1. Training videos for employees
2. Detailed information to assist with remote desktop protocol (RDP) and access control
3. Instructions for installing software patches
4. Information on creating effective backups
5. Implementing two-factor authentication
6. Installing and updating anti-virus programs
7. Instructions for email security settings
8. Installing an endpoint security program

Top 5 Ways to Protect Against Business Email Compromise (BEC) is a five-step checklist including:

1. Implementing two-factor authentication
2. Detailed information to prevent fraudulent wire transfers
3. Training videos for employees
4. Configuring email systems to filter out phishing emails automatically
5. Installing an endpoint security program

The Department of Health and Human Services, Office for Civil Rights (OCR), is responsible for enforcing HIPAA Security Rule violations, which are frequently associated

with cybersecurity incidents. As a part of Security Rule compliance, all workforce members must receive ongoing security awareness training. By utilizing these resources, you can train your workforce, protect your organization from a cybersecurity incident, **and** meet existing Security Rule requirements.

Even with these resources, it can be a challenge to implement safeguards if you are not a technology expert. The good news that by utilizing the CyberNET resources, you have access to pre-paid cybersecurity experts who can provide guidance. Should you need more advice than your policy covers, the cybersecurity expert can refer you to other sources of information or consultants who can work with you on your cybersecurity program.

These resources are provided as a value-added benefit by SVMIC as a part of your cyber liability policy, and policyholders are strongly encouraged to take advantage of them. Doing so can help reduce the risk of a cyberattack and the financial and reputational damage that typically follows a successful attack.

Our mission at SVMIC is to protect, support, and advocate for physicians and other healthcare providers. Providing members with these and other resources to address cybersecurity is one way we accomplish this mission.

If you have questions about cybersecurity or access to these resources, call 800-342-2239 or email contactsvmic@svmic.com.

**If you experience a cybersecurity incident**, contact the SVMIC Claims Department as soon as possible by calling 800-342-2239.

Other individuals in your organization may benefit from these articles and resources, such as your administrator, privacy or security officer, or information technology professional. They can sign up for a Vantage account here.

---