SURGICAL INFORMATION SYSTEMS™

Cybersecurity for ASCs

Ann Geier, MS, RN, CNOR, CASC
Margaret Chappell, MS, BSN

Powering Surgical Performance

Cyberattacks – On the Rise

Powering Surgical Performance

How common are cyberattacks?

- 1 in 3 healthcare organizations have been victims
- 1 in 10 paid ransom/extortion fees
- Facilities are above average in preparation; adequately prepared at best; plan needs an overhaul
- Concerns: ransomware (32%); insider threats (25%); compromised applications (19%)

1 in 3 healthcare organizations have suffered a cyberattack, 1 in 10 paid ransom: 6 things to know; Julie Spitzer; may 23, 2018; Becker's Health IT & CIO Report

Why is Detecting Threats so Difficult?

- Lack of tools to monitor employee and other insiders' activities (27%)
- Lack of staff to analyze permissions data re: employee access (25%)
- More company assets stored on the network or cloud (24%)
- More employees, contractors, business partners have access to network (24%)

- Poll taken at 2018 Healthcare Information and Management Systems Society Conference, March, 2018
- *1 in 3 healthcare organizations have suffered a cyberattack, 1 in 10 paid ransom: 6 things to know*; Julie Spitzer; may 23, 2018; Becker's Health IT & CIO Report

Employees Willing to Sell Data

- Nearly 1 in 5 employees in healthcare would sell confidential data to unauthorized parties
  - » 18% would sell login credentials, installing tracking software, downloading data to a portable drive
    - – Would do it for $500 - $1,000
  - » 24% knew someone in their organization who did this
  - » More likely to occur in provider organizations
  - » 99% said they feel responsible for data security
  - » 97% said they knew the facility’s data security & privacy standards – yet, 21% have their user name and password written down next to computer

» *Losing the Cyber Culture War in Healthcare; Accenture*

» *1 in 5 Health Employees willing to sell confidential data: 7 survey insights;* Julie Spitzer; March 2, 2018; Becker’s Health IT & CIO Report

Attitudes Towards Cybersecurity Training

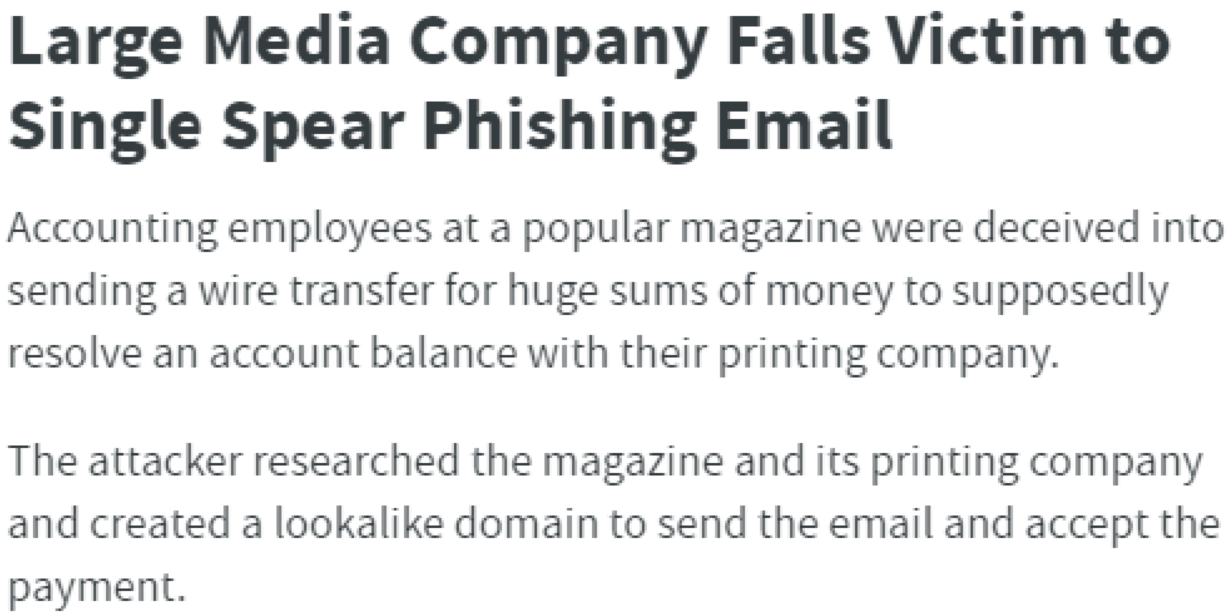
- 16% of respondents said they were unaware of organization's cybersecurity training
- 29% who received training, only received it once
- 17% of those who were trained still write down usernames & passwords
- 19% said they'd be willing to see confidential data
- Frequent training respondents
  - 24% wrote down user names & passwords
  - 28% would sell data

- *Losing the Cyber Culture War in Healthcare; Accenture*
- *1 in 5 Health Employees willing to sell confidential data: 7 survey insights;* Julie Spitzer; March 2, 2018; Becker's Health IT & CIO Report

> “Health organizations are in the throes of a cyber war that is being undermined by their own workforce.”
>
> John Schoew, Managing Director, Accenture

Definitions

- Phishing
  - the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.
- Ransomware is malicious software which locks your screen or encrypts—or scrambles—a user’s computer and/or files.
  - It’s often delivered via harmful email attachments, outdated browser plug-ins, websites, text messages, and more.
  - Some hackers also steal sensitive data (e.g., a investment firm’s financial data) and threaten to make the data public unless a ransom is paid.



Large Media Company Falls Victim to Single Spear Phishing Email

Accounting employees at a popular magazine were deceived into sending a wire transfer for huge sums of money to supposedly resolve an account balance with their printing company.

The attacker researched the magazine and its printing company and created a lookalike domain to send the email and accept the payment.

People are the weakest link

- Microsoft research shows that more than 90 percent of security incidents result from human error, not hacks. This includes falling victim to social engineering attacks such as phishing emails and spoofing that allow criminals to steal credentials.

- Microsoft Cybersecurity E-book

How to protect your center

- 1. Have the right IT support provider in place.
  - Finding the right IT support provider for your center is key
  - A. Interview the provider
  - B. Do they fit your budget?
  - C. The MOST important Question! What do they think you need? Are they on target? Do you agree with their suggestions for your centers needs?
  - D. Check references
  - E. Meet the support staff that will be in your center – do you like them; how do they interact with your staff; how quickly do they respond to calls?

Education

2. Does ***every*** team member in your center know what may happen if they open an email with an attachment that contains malware, a virus or ransomware?

A. Education – ongoing and frequent

B. Utilize your IT support provider

C. Audit the compliance of your team

Set STRICT security controls

3. Check your policies and procedures
    A. Are you practicing what you preach?
    B. Who has access to what? Limit privileges
    C. Password requirements – complexity
    D. Two factor authentication

Disaster Response and Recovery

I have been attacked – NOW WHAT?

4. Policy and Procedure – document what to do and when
   - A. Archive
   - B. Backup
   - C. Test and Audit – frequently, randomly, assess
   - D. Review and correct any issues you identify

Stay Up to Date

5. What are the latest trends in the industry?

   A. The latest attack – what can you learn?

   B. Industry protection – what is new?

   C. Talk to your peers – networking is key

   D. Pretend you have had an attack

Risk Assessment

6. Professional Risk Assessment
    - A. Use a 3rd Party outsider
    - B. Expense
    - C. Look at everything in your center including,
      equipment, software, systems

Actual Occurrence

- 1. Bank Account and ASC

- 2. Accrediting Body and ASC

Questions

Contact

Ann Geier, MS, RN, CNOR, CASC

Chief Nursing Officer

Surgical Information Systems (SIS)

Ann.Geier@sisfirst.com

843-303-0008

www.sisfirst.com

For a copy of my free eBook, “Admin 101: What Every New ASC Administrator Needs to Know”, visit www.sisfirst.com, resources, eBooks

Margaret Chappell, MS, RN, CASC

Chief Executive Officer

Center for Advanced Surgery

Mchappell@chscas.com

781-733-2235

Thank You