APRIL 2016
www.bdo.com

AN ALERT FROM BDO CONSULTING

BDO KNOWS: CYBERSECURITY

GROWING RANSOMWARE THREAT TO HOSPITALS HIGHLIGHTS INDUSTRY GAPS IN CYBERSECURITY

Following a string of attacks, the U.S. Department of Homeland Security (DHS) and the Canadian Cyber Incident Response Center (CCIRC) issued joint guidance alerting healthcare providers to an increase in ransomware infections, advising individuals and businesses on preventive measures.

The guidance came on the heels of a ransomware attack in March that held the IT system of a Maryland hospital network hostage, demanding payment to unlock access to its networks. The system was offline for a week, forcing employees to turn away patients or treat them without their computer records.

DETAILS

Since February, at least a dozen hospitals have been victim to ransomware, resulting in costly and debilitating damages. One ransomware incident forced a Hollywood hospital to pay $17,000 in bitcoins to regain access to its computer systems.

In March 2016, DHS's United States Computer Emergency Readiness Team and Canada's CCIRC released an alert regarding the increase of ransomware attacks against healthcare organizations. Ransomware is an increasingly prevalent form of cyber extortion in which malicious software blocks access to critical systems or information until a "ransom" is paid. Two of the variants mentioned specifically in the alert — Locky and Samas — infect computers of healthcare facilities and hospitals through spam emails with malicious attachments and through vulnerable Web servers, respectively. A newly discovered ransomware strain, SamSam, is believed to have been developed to target the healthcare industry.

The DHS/CCIRC guidance warns that ransomware, often spread through phishing emails or "drive-by downloading," may lead to temporary or permanent loss of sensitive or proprietary information, a disruption in regular operations, financial losses from restoring the system or potential reputational harm. DHS and CCIRC strongly recommend the following preventive measures to protect against ransomware infection:

- **Employ a data backup and recovery plan for critical information.** Perform and test regular backups to limit the impact of data or system loss, and to speed up the recovery process. Data should be kept on a separate device with backups stored offline.
- **Enlist application whitelisting to help stop malicious software and unapproved programs from running.** Whitelisting is one of the best security strategies; it allows specified programs to run while blocking all others, including those harmful to IT systems.

HOW DO I GET MORE INFORMATION?

For more information about how healthcare providers can safeguard their organizations against cyberattacks, contact:

SHAHRYAR SHAGHAGHI
National Leader, Technology
Advisory Services Head of
International BDO Cybersecurity
sshaghaghi@bdo.com

PATRICK PILCH
BDO Healthcare Advisory
Practice Leader
ppilch@bdo.com

Read more ▶

- **Keep operating systems and software up-to-date with the latest patches.** Making sure vulnerable applications and operating systems are patched with the latest updates largely reduces the number of weak links attackers can exploit.

- **Keep anti-virus software up-to-date.** Scan all software downloaded from the Internet before running it.

- **Restrict users' ability to install and run software applications, applying the principle of least privilege to systems and services.** Doing so may stop malware from running or at least limit its capability to spread.

- **Avoid allowing macros from email attachments.** If an attachment is opened and a user enables macros, embedded code will execute malware on the machine. For businesses like hospitals or healthcare facilities, it may be best to block email messages with attachments from suspicious sources. You can learn how to recognize and avoid email scams here.

- **Avoid unsolicited Web links.** Refer to the DHS' guide on avoiding social engineering and phishing attacks here.

BDO INSIGHTS

Ransomware presents a growing threat to every industry, but as the spate of attacks over the last few months have made clear, healthcare organizations are particularly vulnerable. Because many hospitals rely on out-of-date technology and may prioritize immediate data access over data security, cybercriminals have found their systems relatively easy to penetrate. Moreover, medical records are 10 times more valuable than credit card information on the black market, making healthcare organizations a lucrative target. Most significantly, cyberattacks not only risk compromising personal health Information but can also create disruptions of service that jeopardize patient health and safety.

As the latest ransomware attacks demonstrate, it is important that hospitals implement the DHS guidance to respond to the immediate threat, but it's just as important to build defenses for the long term. BDO recommends the following proactive cybersecurity measures for healthcare facilities:

- **Create a cybersecurity framework.** This helps hospitals prepare so that if and when they do get hacked, they can prevent further infiltration, minimize the damage and quickly redirect staff to practiced protocols so patient care is not compromised.

- **Assess IT workflow and people to identify potential system vulnerabilities.** A breach of data-reliant treatment areas would cause clinical problems, since patients' past and recent medical records would be unavailable. Creating IT perimeters makes it possible to shut down data-reliant treatment areas to protect them from infiltration until the attack is addressed.

- **Assign responsibilities and train staff on cybersecurity.** In the event of a breach, all departments will have to respond effectively, so the response team should reflect that. Response team members should understand reporting laws and agree on backup protocols so hospitals can get back up and running faster — even if in a modified way.

- **Run scenario training events.** Conduct cyberattack simulation events, walking the response team through an incident response plan. This helps uncover planning and response gaps, and leads to preventive remediation work.

- **Implement effective preventive measures.** Hospitals would be wise to introduce new resources to their prevention and response protocols, like those recommended by the DHS and CCIRC. Hospitals can contain system infiltrators by identifying them early and preventing them from gaining access to what they want.

BDO assists healthcare facilities in conducting ongoing security risk assessments and testing controls in line with the DHS and CCIRC's guidelines, in addition to updating cybersecurity risk management programs, strategy and governance.

About The BDO Center for Healthcare Excellence & Innovation
The BDO Center for Healthcare Excellence & Innovation unites recognized industry thought leaders to provide sustainable solutions across the full spectrum of healthcare challenges facing organizations, stakeholders and communities. Leveraging deep healthcare experience in financial, clinical, data analytics and regulatory disciplines, we deliver research-based insights, innovative approaches and value-driven services to help guide efficient healthcare transformation to improve the quality and lower the cost of care. For more information, please visit www.bdo.com/healthcare.

People who know Healthcare, know BDO.

@BDOHealth healthcareblog.bdo.com

Accountants | Consultants | Doctors

www.bdo.com/healthcare

Material discussed is meant to provide general information and should not be acted upon without first obtaining professional advice appropriately tailored to your individual circumstances.