COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 22, Number 2. February 10, 2022 Privacy Briefs: February 2022

By Jane Anderson

◆ **Tensions between the U.S. and Russia could lead to a heightened risk of Russian state-sponsored cyberattacks on U.S. interests, including health care organizations, federal agencies warned.** Russia would consider conducting a cyberattack on the U.S. homeland if Moscow perceived that a U.S. or NATO response to a potential Russian invasion of Ukraine threatened Russia's long-term national security, according to a Department of Homeland Security intelligence bulletin obtained by CNN.[1] 1 The Cybersecurity & Infrastructure Security Agency (CISA), FBI and the National Security Agency have urged organizations to be prepared with cyber incident response, resilience, and continuity of operations plans so that critical functions and operations can be kept running if technology systems are disrupted or need to be taken offline. The three agencies also urged organizations to enhance their cyber posture by following best practices, and to increase organizational vigilance by staying current on threat reporting.[2] John Riggi, national advisor for cybersecurity and risk at the American Hospital Association, warned that hospitals and health systems could be targeted directly, or could become "incidental victims or collateral damage of Russian-deployed malware or destructive ransomware that inadvertently penetrates U.S. health care." Riggi noted that "a cyberattack could disrupt a mission-critical service provider to hospitals," and added that "this is a good reminder for all to have robust downtime procedures, redundancy and business continuity plans to sustain a loss of on-premises or cloud-based mission-critical services or technology for up to four to six weeks."[3]

◆ **CISA also advised U.S. critical infrastructure organizations to review a Microsoft blog on malware identified in Ukraine and take action to strengthen their networks against potential cyberattacks.**[4] The Microsoft Threat Intelligence Center reported evidence of destructive malware in systems belonging to several Ukrainian government agencies and organizations that work closely with the Ukrainian government.[5] The malware is disguised as ransomware, but if activated by the attacker, it would render the infected computer system inoperable. "As we have seen in the past, destructive malware targeting Ukraine can spread rapidly across the globe," said Riggi. "It is again strongly recommended to assess any direct, 3rd party business associate connections and email contacts in Ukraine and that region of the world. Consider blocking such connections. Although geo-fencing for all inbound and outbound traffic related to Ukraine and that region may help mitigate direct cyber risk presented by this threat, it will have limited impact in reducing indirect risk, in which the malware transits through other nations, proxies and third parties. Thus, increased monitoring of networks and incident response preparedness is also strongly recommended."[6]

◆ **Ciox Health has notified more than 80 provider organizations, including facilities from multiple large health systems, that an incident involving unauthorized access to a Ciox employee's email account may have compromised protected health information.**[7] According to Ciox, an unauthorized person accessed a Ciox employee's email account between June 24 and July 2 of last year and, during that time, may have downloaded emails and attachments in the account. Ciox determined that some emails and attachments in the account contained "limited patient information related to Ciox billing inquiries and/or other customer service requests." According to Ciox, the information included patient names, provider names, dates of birth, dates of service, and "in very limited instances," Social Security numbers, driver's license numbers, health insurance information,

and clinical or treatment information. "Ciox believes that the account access occurred for purposes of sending phishing emails to individuals unrelated to Ciox, not to access patient information," the company said.

◆ **Vision benefit company EyeMed will pay $600,000 to New York to resolve a data breach that compromised the personal information of approximately 2.1 million consumers nationwide, including 98,632 in New York, state Attorney General Letitia James announced.**[8] EyeMed experienced a data breach in June 2020 where attackers gained access to an EyeMed email account with sensitive customer information, including names, addresses, Social Security numbers, identification numbers for health and vision insurance accounts, medical diagnoses and conditions, and medical treatment information, James said in a press release. In July 2020, the attacker sent approximately 2,000 phishing emails from the compromised email account to EyeMed clients, seeking login credentials for their accounts. EyeMed's IT department noticed the phishing emails and also received inquiries from clients about the emails. EyeMed then blocked the attacker's access to its system. The New York attorney general's office determined that, at the time of the attack, EyeMed had failed to implement multifactor authentication for the affected email account, despite the fact that the account was accessible via a web browser and contained a large volume of consumers' sensitive personal information. Additionally, EyeMed failed to implement sufficient password management requirements for the enrollment email account, and failed to maintain adequate logging of its email accounts, the attorney general's office found. As part of the settlement, EyeMed also is required to enact a series of measures to protect consumers' personal information.

◆ **A former South Georgia Medical Center employee has been arrested in the case of a November data breach at the medical facility, according to hospital officials.**[9] Ronald Dean, the hospital's president and chief executive officer, said that a worker "left employment" with the medical center on Nov. 11. On Nov. 12, security software put out an alert that there had been an unauthorized download of data by an employee, Dean explained. The information left the facility on a USB stick, he said. Data on the USB stick included names, dates of birth and test results, but not financial data, Social Security numbers or medical records, Dean said. The employee pinpointed by the investigation had legitimate access to the files, which ultimately were recovered, Dean said, adding that the organization does not believe the downloaded information was used in any way. The former medical center employee is "charged with felony computer theft and felony computer invasion of privacy," a sheriff's office statement said. The hospital is mailing letters to affected patients, offering free credit monitoring and identity restoration services, and limiting the use of USB drives by employees.

◆ **Hackers breached the computer records of southeast Florida's Broward Health in October and may have accessed personal and financial information on more than 1.3 million people, the health system said.**[10] Social Security numbers, patient medical histories and bank account information are among the data that potentially were exposed in the breach, according to a notice Broward Health filed with the Office of the Maine Attorney General, which requires breach reporting when state residents are affected by a breach. A Broward Health spokesperson said that the incident did not appear to involve ransomware, and that patient care was not disrupted. The intruders accessed Broward Health's computer networks via a "third-party medical provider," according to the breach notice, which stated, "this personal information was exfiltrated, or removed, from Broward Health's systems, however, there is no evidence the information was actually misused by the intruder."

◆ **The HHS Health Sector Cybersecurity Coordination Center (HC3) said the threat posed by BlackMatter ransomware-as-a-service has been reduced to "guarded," given that the group hasn't claimed a victim since Oct. 31, 2021, and appears to have shut down operations.**[11] In September, HC3 had said that BlackMatter was a "highly sophisticated, financially-motivated cybercriminal operation that posed an elevated risk to the healthcare and public health (HPH) sector despite the group's claims to not target healthcare entities." The group's suspected predecessors—DarkSide and REvil—had claimed health sector victims, along with high-profile victims such as the Colonial Pipeline, and HC3 is aware of at least four health care or health care-related

organizations that have been affected by BlackMatter ransomware incidents. BlackMatter, which emerged in July 2021, is a Russian-speaking threat group likely originating from Eastern Europe. The group claimed it was shutting down operations on Nov. 1. HC3 can confirm that the BlackMatter leak site no longer is operational, and said that no known ransomware variants are believed to be successors at this time. However, "while the group appears to have shut down operations, other actors seeking lucrative payouts from ransomware attacks are likely to fill this void," HC3 said.

1 Sean Lyngaas, "DHS warns of potential Russia cyberattacks amid tensions," CNN, January 24, 2022, https://cnn.it/30tJla9.
2 Cybersecurity & Infrastructure Security Agency, "Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure," alert AA22-011A, January 11, 2022, https://bit.ly/3J4d9BX.
3 American Hospital Association, "Agencies recommend action to protect critical infrastructure from cyber threats," news release, January 12, 2022, https://bit.ly/34vGS0x.
4 Cybersecurity & Infrastructure Security Agency, "Microsoft Warns of Destructive Malware Targeting Ukrainian Organizations," news release, January 16, 2022, https://bit.ly/3GyUkFs.
5 Tom Burt, "Malware attacks targeting Ukraine government," *Microsoft On the Issues* (blog), January 15, 2022, https://bit.ly/3snQ4nn.
6 American Hospital Association, "CISA: Organizations should review Microsoft malware warning," news release, January 18, 2022, https://bit.ly/3utomYN.
7 Ciox Health, "Notice of Email Security Incident," news release, January 2022, https://bit.ly/3B20ddl.
8 New York State Office of the Attorney General, "Attorney General James Announces $600,000 Agreement with EyeMed After 2020 Data Breach," news release, January 24, 2022, https://on.ny.gov/3sg3v8N.
9 Terry Richards, "Ex-hospital worker arrested in SGMC data breach," *Valdosta Daily Times*, January 14, 2022, https://bit.ly/3J95x10.
10 Sean Lyngaas, "Hackers breached Florida health care system, potentially exposing data on 1.3 million people," CNN, January 4, 2022, https://cnn.it/3gs5ph6.
11 HHS Office of Information Security, "Cyber Threat Posed by BlackMatter RaaS Reduced to Guarded (Blue)," Report: 202201281300, January 28, 2022, https://bit.ly/34liyWL.