Feature

Patient Cyber Harm: Strategies and Tips for Prevention, Preparation, Risk Management, and Transparency

Gerard Nussbaum, Zarach Associates LLC; **Elizabeth Hodge**, Akerman LLP; **Sean Sullivan**, Alston & Bird LLP; and **Scott Bennett**, Microchip Technology

In 2020, at the height of the COVID pandemic lockdown, Russian-affiliated cybercriminals planned to attack and bring down more than 400 U.S. hospitals. Thanks to action by U.S. authorities and security researchers, this plot was foiled.[1] While this particular attack failed, health care entities are routinely hit by cyberattacks, bringing down networks, applications, and communication systems. In general, health care delivery organizations (HDOs), which range in size from multi-hospital health systems to single physician practices, are not as well prepared as many other industries to prevent and respond to cyberattacks.[2]

Historically, much of the focus of cybersecurity in health care has been on preventing and responding to data breaches. That is still vitally important. However, as cybercriminals have shifted from stealing patient data to locking down HDOs' systems and data with ransomware, the risk has also shifted. Now, the risk is not just a potential breach of personal information, but patient harm; cyberattacks can and have resulted in physical injury or even the death of patients and staff members.

This article discusses how cyber events can put patients at risk and steps HDO boards and executives should take to minimize the impact of such events.

Cyberattacks Jeopardize HDOs' Ability to Care for Patients

A recent case in Alabama offers insights into the challenges of operating in the midst of a cyberattack outage.[3] In this situation, Springhill Medical Center suffered a cyberattack with a ransomware demand on July 9, 2019 that shut down its network and other systems.

[T]he standard is not perfection; rather, it is whether the board members conducted the appropriate level of due diligence to allow them to make an informed decision.

On July 16, 2019, a pregnant mother was admitted to the hospital, with the infant born the next day. Due to the cyberattack, fetal tracing, which shows when an unborn child may be in distress, was available only at the bedside; normally, fetal trace was displayed on large monitors at the nursing station to support rapid identification and intervention if needed. The electronic health record (EHR) also was not available, so the hospital was using paper charting. Tragically, the infant died. The mother filed a lawsuit against Springhill Medical Center alleging that her child's death was attributable to effects of the ransomware attack on the care provided by the hospital during her labor and delivery.

Also, according to the complaint, the hospital did not apprise the pregnant mother of the cyberattack at time of admission, which would have given her the opportunity to seek care elsewhere. Instead, the hospital stated publicly that it was providing the same high-quality care as normal. These types of stories raise several questions:

- How much do patients need to know about the impact of an ongoing cyberattack on the HDO's operations and its ability to provide care in order to provide informed consent for treatment?
- Does an HDO and its personnel commit malpractice by accepting a patient given their understanding of the impairment of the clinical systems and information flow?
- Can an HDO be held liable for misrepresenting, even unintentionally, its capability to care for patients?
- How much information do HDO staff need to exercise their professional judgement regarding the hospital's ability to provide appropriate levels of care?

Cyberattacks on HDOs Lead to Significant and Sustained Strain on Personnel[4]

Even with robust downtime procedures and a well-trained staff, the unavailability of electronic systems imposes a strain on the delivery of care. It can often take weeks before access to all critical systems is restored,

Cybersecurity has increasingly become a central compliance risk deserving of board level monitoring at companies across sectors.

and months before all systems are back in full operation. During this time, staff use unfamiliar procedures, extra effort must be made to assure clear and timely communications, higher staffing levels may be required to handle the additional workload, and other accommodations must be made. For example, when an HDO is forced to shift to paper charting, patient information is no longer available in real time to multiple personnel (as it would be in the EHR) and illegible handwriting can cause problems. These lingering effects of cyberattacks further burden staff, exacerbate staff burnout, and potentially degrade the ability to provide high quality care. This may lead to longer lengths of stay, poor treatment outcomes and higher complications, and ultimately, greater mortality.

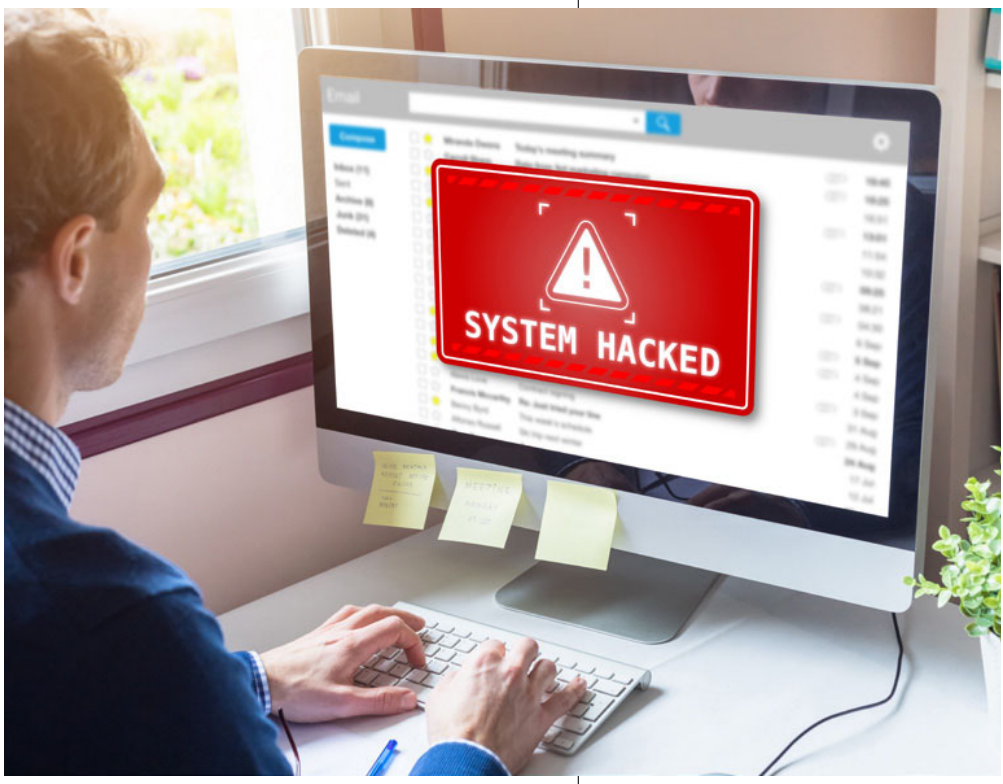
While cyberattacks affect an HDO's data, more importantly, they pose significant risks for harm to patients. Careful preparation and planning are essential to minimizing this danger.

A Culture of Cybersecurity Starts at the Top

According to one study, 23% of all health care data breaches are caused by technology issues, while 77% of breaches are caused by human error.[5] Focusing on the latest and greatest technology, like firewalls, spam filters, VPNs, and the newest encryption standards, will not necessarily prevent an employee from clicking on a malicious link, providing sensitive information to a cyber-criminal, or failing to recognize and report a data breach. For this reason, the most important defense to cyber-risks—more important than spending money on technology solutions—is cultivating a strong culture of cybersecurity within the organization.

An HDO's culture of cybersecurity starts at the top, which means the board of directors. On this point, it is helpful to understand the demarcation of responsibility between the organization's board of directors and its executive or management team. The board monitors and the executive team manages. Specifically, the board is responsible for:

- Approving corporate strategies;
- Selecting a chief executive officer (CEO);
- Overseeing the CEO and senior management, including the Chief Information Security Officer (CISO); and



- Setting the "tone at the top" for ethical conduct.[6]

In contrast, the CEO and executive team are responsible for:

- Developing and implementing corporate strategy; and
- Operating the organization's business under the board's oversight.[7]

The next sections discuss the specific obligations and best practices for HDO boards and executive teams when it comes to cybersecurity.

The Role of the Board

The board's responsibility to ensure the safety of the health care organization and its patients flows from its fiduciary duty to the company. That duty requires that board members act in good faith, exercising the care of an ordinarily prudent person under similar circumstances and in the best interest of the organization.[8] This duty applies to both the board's decision making and oversight functions. And the standard is not perfection;

[W]hen it comes to cyberattacks and technology failures, it is not if, but when.

Gerard M. Nussbaum BS, MS, JD, CPA, CMA, RCDD, CMMT, a Principal with Zarach Associates LLC, provides strategic guidance on the use and deployment of technology. From early-stage startups to large complex health systems and academic medical centers, health care entities turn to Gerard for proactive and concrete assistance. Gerard's guidance integrates multiple perspectives: Bridging Health, Technology and Law™. Gerard is a frequent speaker and author. Gerard may be contacted at: gerard@zarachassociates.com.

rather, it is whether the board members conducted the appropriate level of due diligence to allow them to make an informed decision. What is an appropriate level of diligence varies with the circumstances, though board members should have awareness of what is happening in the organization and the health care sector generally. For example, over the past couple of years, various federal agencies have issued alerts regarding the increasing number of ransomware attacks on health care providers. This publicity might mean that reasonably prudent board members should inquire of the CEO and management team what they are doing to protect the company and patients from this risk.

Increasingly, regulators, shareholders, and individuals affected by cybersecurity incidents are seeking to hold board members and executives responsible for compliance and cybersecurity matters. However, to date, lawsuits against board members for breaching their fiduciary duty with respect to the organization's cybersecurity preparedness have largely been unsuccessful. For example, in a derivative lawsuit brought in the Delaware chancery court against board members and executives of Marriott International, Inc. as a result of a publicized data breach, in ruling on a motion to dismiss, the judge stated, "Cybersecurity has increasingly become a central compliance risk deserving of board level monitoring at companies across sectors."[9] The judge then dismissed the derivative action, finding that the plaintiff did not show "that the directors completely failed to undertake their oversight responsibilities, turned a blind eye to known compliance violations, or consciously failed to remediate cybersecurity failures."[10]

However, when a judge and jury are presented with the right fact pattern, they may find that board members breached their fiduciary duty. In the meantime, regulators may have a more immediate impact on how board members view their responsibility for the organization's cybersecurity posture. Earlier this year the U.S. Securities and Exchange Commission (SEC) issued a proposed rule to "enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and cybersecurity incident reporting by public companies."[11] Among other things, the proposed rule would require public companies to:

- Disclose, on the Form 10-K, management's role in implementing cybersecurity policies and procedures, and the board's oversight of cybersecurity risks; and
- Disclose, in proxy statements and annual reports, whether any board member has cybersecurity expertise.[12]

While most HDOs are not publicly traded, regulatory requirements such as these also affect the standard by which non-publicly traded HDOs may be judged. Even smaller HDOs need to pay attention to these duties, which may be exercised by the owners.

To effectively carry out their oversight role with respect to cybersecurity, the HDO's board members must understand that:

- Cybersecurity is a patient safety issue;
- HDOs are prime targets for malicious cyber actors;
- Cybersecurity should be addressed as an enterprise risk issue and not "just an IT issue"; and
- Cyber-risk cannot be eliminated, only mitigated.

To help board members become (and stay) educated about cybersecurity threats and risks to the organization, the board may want to consider:

- Requesting and receiving regular updates from the CISO or other knowledgeable C-suite executive regarding the organization's cybersecurity;
- Recruiting a board member (or members) with cybersecurity experience. The recent SEC proposed rule discussed above suggests an expectation by regulators and possibly investors that public companies have at least one board member with such expertise;
- Tasking a board committee with oversight of the organization's cybersecurity risk management; and
- Engaging outside resources to assist the board in acquiring cybersecurity knowledge and understanding the information that CISO and other C-suite executives present to the board.

The Role of the Executive Team

The executive team's role is to execute the board's vision for a strong cybersecurity culture within the HDO and to keep the board informed of the cybersecurity threats to the organization's operations, including patient safety, and the risk management strategies being implemented to manage that risk. Executives can do this by:

- Supporting enterprise risk management. It is important to recognize that a significant cyber event could affect not only access to the HDO's data, but also patient safety and the organization's financial health;

- Supporting business impact assessments that focus on impacts to data and patient safety when new technologies or new processes are implemented by the HDO; and
- Implementing the prevention and risk-mitigation strategies discussed below.

The HDO's cybersecurity lead should be someone with gravitas; other employees and leaders throughout the organization should look to that person as someone with authority, status, and independence, who will demand respect, but also be approachable and listen to concerns of others. Spearheaded by this cybersecurity lead, organizations should consider regular communications to employees highlighting technology-based risks to patient care and the importance of good cyber hygiene. Ultimately, every staff member should be empowered as a proactive defender of patients, their data, and the technology needed to provide their care.

Investing in People, Technology, and Preparation

HDOs need to adequately staff and compensate the information security and risk management functions; invest in technology to protect the organization's data, devices, and patients; invest in training staff on cybersecurity best practices; and invest in table-top and other pressure-testing/training exercises.

Contingency and Disaster Recovery Plans

Industry experts have made it clear that when it comes to cyberattacks and technology failures, *it is not if, but when.* Every health care organization that relies on technology should consider how it will, at a minimum, provide care to patients when such technology is not available, inform the public of cyberattacks, and respond to ransomware events.

How will a hospital document patient care when its EHR system is down? What about connecting rural patients with specialists if the telehealth platform is unavailable? Contingency planning should include *ensuring clinical staff can seamlessly shift to paper records,* is trained on how to chart by hand, and can re-integrate paper records into the electronic clinical record once the system is available again (which may require coordination with technology vendors). Every IT system handling patient information should be backed up, and those backups should be stored in secure, off-site locations and tested regularly. Similarly, when a technology used for patient care is unavailable, there should be a backup plan and downtime procedures to follow until technology is restored. This may mean connecting patients and providers using telephone or an alternative secure technology, or if automated alerts are unavailable, then staff should know how to monitor data feeds or devices manually and more frequently. And because cyber issues are unpredictable and even good downtime procedures will put considerable strain on a health care organization, larger providers should be prepared to operate under a contingency mode for several weeks if necessary.

Ransomware is a threat that providers need to be prepared for. Questions to consider before a ransomware event include whether data can be segmented to allow for small scale quarantines, when to contact law enforcement for assistance, what is the public relations plan, and who will be involved in key decisions during such an event. The most difficult question is often whether to pay a ransom, which may not be answerable without specific details, including scope and severity of the attack and the amount of the requested ransom. But if a health system has given these issues some thought—preparing IT systems, training personnel, developing decision trees for leaders, and establishing priorities in advance—then some of these difficult questions may be at least a little easier to address in the midst of a cyberattack.

Finally, providers should not rest after developing contingency plans accounting for downtime procedures, public relations, and ransomware responses. Clinical and administrative staff and leadership should train on these procedures, exercise them, and constantly refine them.

Planning for Diversion

One issue to consider during contingency planning is the need to divert patients to other HDOs because of a cyberattack. A tragic situation from Germany illustrates this. On September 9, 2020, a hospital in Germany was the victim of a cyberattack with ransomware demands. A flaw in the hospital's Citrix systems, which had been generally known since January 2020, was exploited by the hackers. The hospital determined that the cyberattack had impaired its ability to treat patients and went to diversion status. As a result, on September 11, 2020, they diverted a 78-year-old patient with a ruptured aorta to another hospital. Unfortunately, the patient died in transit. German authorities have charged the hackers with involuntary manslaughter/negligent homicide.[13]

Questions that should be considered in planning for diversion situations like this include:

- Who should participate in making the diversion decision?

Elizabeth (Betsy) Hodge is a partner in Akerman LLP's health care practice group and concentrates her practice on compliance and regulatory issues affecting health care providers, payers, and employer-sponsored health plans. Betsy has significant experience with HIPAA and the HITECH Act and assists covered entities and business associates in complying with these laws through the development of policies and procedures, workforce training, analysis of data incidents and notification of breaches, and assisting with government audits and investigations. Betsy also advises clients regarding compliance with a range of other federal and state privacy and data security laws and associated transactional issues. In addition, she counsels clients on state and federal health care regulatory issues.

During a cyberattack is the wrong time to develop a public relations strategy.

Sean Sullivan is a partner with Alston & Bird LLP's Health Care Group. Sean assists health care providers and business associates, including health care technology companies, in avoiding liability by ensuring regulatory compliance in operations; advising on business forms and transaction structures; investigating, disclosing, and resolving potential noncompliance; defending government investigations; and providing regulatory support to litigation and transactions as necessary. He also regularly advises private equity and other investors on the regulatory risks and structuring considerations associated with investing in the health care industry.

- What guidelines should HDOs adopt in advance to guide the diversion decision?
- Is there a need to triage patients before diversion, even when operations are impaired?

Evaluating Risk and Notifying Patients and Health Care Providers

HDOs should develop a framework to evaluate when patients' safety may be at risk due to a cyber incident, including when and how patients and the organization's health care providers will be notified of that risk. The framework should allow the board and the executive team to consider the likelihood and severity of harm to patients from a particular event against the potential reputational harm to the organization, possible unnecessary anxiety for patients, and costs to the health care organization from foregoing procedures, going on diversion, and the inability of downtime procedures to fully capture and bill for all procedures that were performed when information systems and medical devices were down.

In addition, HDOs should develop policies to address when and how patients will be notified of potential risks to their health and safety due to a cyberattack. Related to this, the board and leadership should consider:

- Who will approve the policy regarding providing notice to patients—is this a policy that should be approved by the board;
- Who should be involved in approving notice to patients;
- Who will actually communicate to the patients the potential risks to their health and safety due to the cyberattack; and
- What procedure is in place to document that the physician or other provider notified the patient of the risks created by the cyberattack.

Public Relations

During a cyberattack is the wrong time to develop a public relations strategy. While decision making should be fluid, providers should know what factors need to be considered and who will make decisions. Weighing potential patient safety risks and transparency against reputational risks and financial needs can be difficult, so HDOs should identify the relevant factors and establish decision-making procedures ahead of time.

A key element in handling an outage is clearly communicating with employees and staff, patients, the news media, law enforcement, and government officials. The HDO needs to speak with one voice to communicate in a clear and consistent manner as to the extent of the problem, how the HDO is addressing the situation, and the ability to continue to render quality patient care. This may be difficult in an evolving situation, particularly in this age of social media.

Providing regular updates to the press, even if there is minimal news to share, may be helpful to control the narrative. The HDO should avoid overcommitting as to its ability to render quality patient care. Every reporter seeks to humanize complex topics through patient stories, and patients, families, and the HDO's employees will share their own perspectives through social media. Responding to every story is likely impossible, risks creating patient privacy violations, and distracts from the main narrative. Getting into a war with the press is usually ill-advised.[14] Statements made during the fog of battle may later be used against the HDO in medical malpractice and negligence lawsuits.

Contract Terms

A fulsome cyber-risk mitigation program should include incorporating appropriate protections into agreements with vendors. Providers and their counsel should *never overlook risk-shifting provisions*, insisting on indemnification, limitations of liability, and minimum insurance requirements to ensure proper coverage for cyber events. Any health IT contract

*AHLA would like to thank the leaders of the **Health Information and Technology Practice Group** for contributing this feature article: **Kathleen Kenney**, Polsinelli PC (Chair); **Heather Deixler**, Latham & Watkins LLP (Vice Chair—Education); **M. Leeann Habte**, Best Best & Krieger LLP (Vice Chair—Education); **Elizabeth Hodge**, Akerman LLP (Vice Chair—Education); **Valerie Montague**, Nixon Peabody LLP (Vice Chair—Education); and **Adam Greene**, Davis Wright Tremaine LLP (Vice Chair—Member Engagement).*

should also include clear, understandable, and realistic performance standards, implementation timelines, and periodic reporting requirements.

Agreements should also account for downtime, with representations and warranties around uptime minimums, specifications on response time for technical support, ramifications and levers for minor noncompliance, and clear provisions around when downtime becomes a material breach of the agreement—regardless of force majeure events.

Insurance

All providers should consider *cyber insurance as a complement to existing coverage.* Cyber insurance may help pay for costs associated with a cyberattack such as ransom payments, lost revenue, and breach notification.

HDOs should not overlook other types of insurance, such as professional liability, directors and officers, and commercial general liability. It is critical for HDOs to make sure they have adequate insurance coverage for all potential risks from a cyberattack, including property damage, personal injury, and death.

Outside Consultants

Every HDO needs to recognize the limits of its expertise. Outside experts can help with IT security, dark web monitoring, media relations, incident response (both on the clinical and technology sides), tabletop exercises, technology procurement, ransomware negotiation, and of course, legal obligations. HDOs and their counsel should *develop these relationships before a cyber incident occurs*. HDOs that bring in the right expertise to evaluate weaknesses, understand what can go wrong, develop contingency plans, and exercise and reevaluate those plans, will not only be less likely to experience a significant cyber event, but will have a full roster of experts to help them when they do. Smaller HDOs may need to leverage outside experts to a greater extent as they do not have the same capabilities as larger HDOs: smaller size is not an excuse for failing to anticipate, prepare for, and appropriately respond to a cyberattack.

Providers and their counsel should never overlook risk-shifting provisions . . . .

Conclusion

While the outcome of the *Springhill Medical Center* litigation is unknown at this time, the case is a reminder to HDOs of the need to approach cybersecurity from an enterprise risk management perspective to understand *all* of the ways in which cyberattacks can harm the organization, and their patients and employees, including personal injury and even death. HDOs that are aware of these risks can adopt appropriate prevention and risk-mitigation strategies to protect patients, personnel, and the organization at large.

Scott Bennett is a Senior Corporate Counsel—Data Privacy for Microchip Technology in Phoenix, Arizona.

1 Robert McMillan, Kevin Poulsen, and Dustin Volz, *Leak Reveals Secret World of Pro-Russia Hacking Gang*, Wall St. J., Mar. 29, 2022.

2 Mohammad S Jalali and Jessica P Kaiser, *Cybersecurity in Hospitals: A Systematic, Organizational Perspective*, J. Med. Internet Res. 2018 May; 20(5): e10059, PMID: 29807882, PMCID: PMC5996174, DOI: 10.2196/10059, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5996174/ and https://www.jmir.org/2018/5/e10059/.

3 This matter is currently under litigation. We are using this particular incident as an example. We are not endorsing any specific outcomes to the litigation. Information in this section is drawn from the case filings *Kidd v. Springhill Med. Ctr.*, Civ. Action No. 02-CV-2020-900171 (Circuit Court of Mobile County, Ala.), and news reports, Kevin Poulsen, Robert McMillan, and Melanie Evans, *A Hospital Hit by Hackers, a Baby in Distress: The Case of the First Alleged Ransomware Death,* Wall St. J., Sept. 30, 2021, https://www.wsj.com/articles/ransomware-hackers-hospital-first-alleged-death-11633008116?st=704bxpzzldgdmnx&reflink=desktopwebshare_permalink.

4 Cybersecurity & Infrastructure Security Administration (CISA), CISA Insights: *Provide Medical Care* is in Critical Condition: Analysis and Stakeholder Decision Support to Minimize Further Harm (Sept. 2021).

5 Boston Consulting Group, *Building Cybersecurity Skills,* https://www.bcg.com/capabilities/digital-technology-data/building-cybersecurity-skills.

6 The Business Roundtable, *Principles of Corporate Governance* (Aug. 2016), https://s3.amazonaws.com/brt.org/Principles-of-Corporate-Governance-2016.pdf.

7 *Id.*

8 Corporate Responsibility and Corporate Compliance: A Resource for Health Care Boards of Directors, The Office of Inspector General of the U.S. Department of Health and Human Services and the American Health Lawyers Association, https://oig.hhs.gov/documents/compliance-guidance/816/040203CorpRespRsceGuide.pdf.

9 *Fireman's Retirement Sys. of St. Louis, derivatively on behalf of Marriott Int'l, Inc. v. Sorenson,* C.A. No. 2019-0965-LWW, 2021 WL 4593777, *1 (Del. Ch. Oct. 5, 2021).

10 *Id.*

11 SEC Proposed Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 87 Fed. Reg. 16590, 16590 (Mar. 23, 2022).

12 *Id.* at 16622-16623.

13 *Hacker-Angriff: Ermittlungen wegen fahrlässiger Tötung*, Sueddeutsche Zeitung, Sept. 18, 2020, https://www.sueddeutsche.de/gesundheit/krankenhaeuser-duesseldorf-hacker-angriff-ermittlungen-wegen-fahrlaessiger-toetung-dpa.urn-newsml-dpa-com-20090101-200917-99-598587; *German hospital hacked, patient taken to another city dies,* Assoc. Press, Sept. 17, 2020, https://apnews.com/article/technology-hacking-europe-cf8f8eee1adcec69bcc864f2c4308c94.

14 Mark Casey, *Tenet Health fails to provide update on information systems: Staff reports continued disruption in delivering care,* WPTV, Apr 24, 2022, https://www.wptv.com/news/region-c-palm-beach-county/west-palm-beach/tenet-health-fails-to-provide-update-on-information-systems.