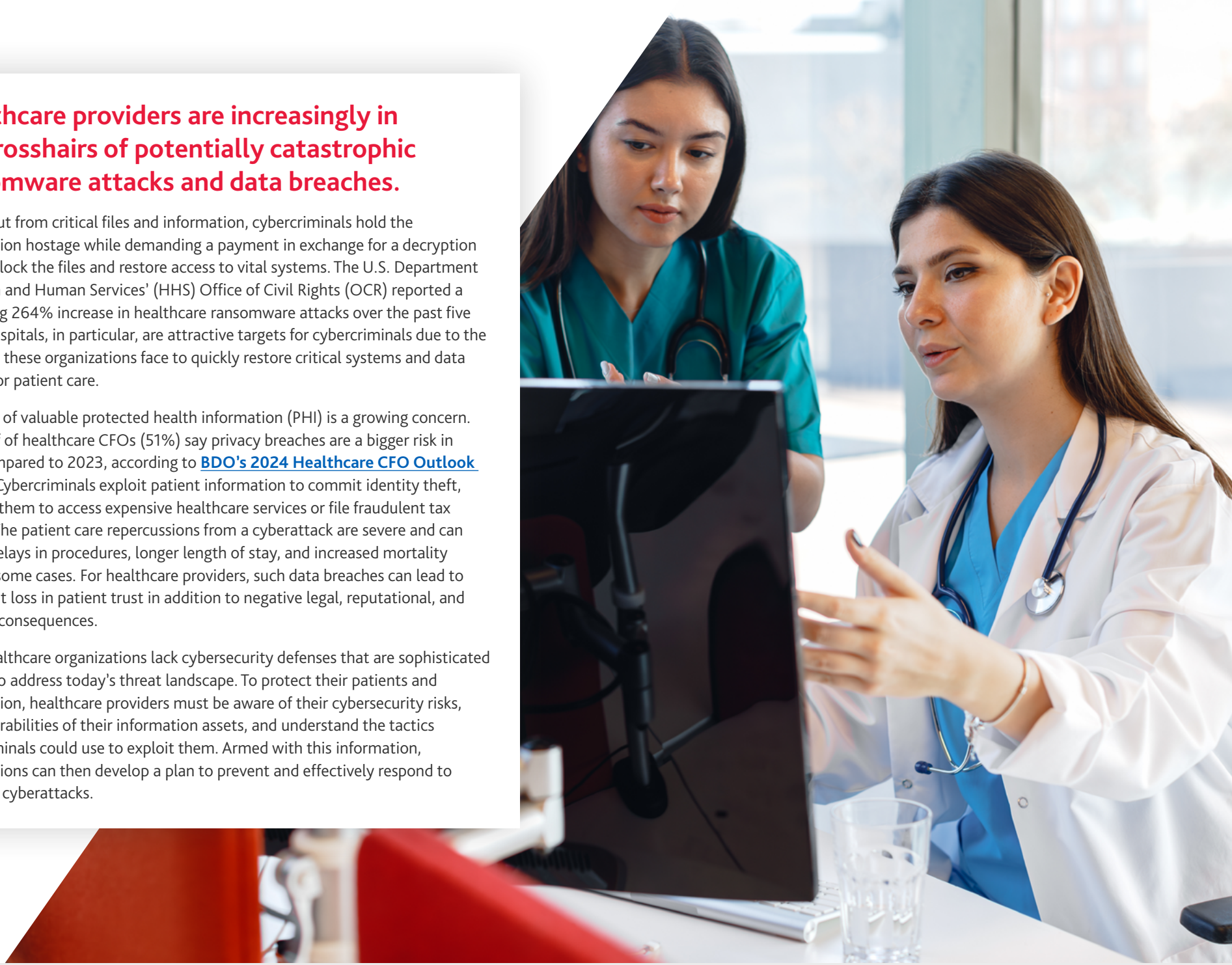
Healthcare Security in 2024: **The Cyberthreat Landscape**

Healthcare providers are increasingly in the crosshairs of potentially catastrophic ransomware attacks and data breaches.

Locked out from critical files and information, cybercriminals hold the organization hostage while demanding a payment in exchange for a decryption key to unlock the files and restore access to vital systems. The U.S. Department of Health and Human Services' (HHS) Office of Civil Rights (OCR) reported a staggering 264% increase in healthcare ransomware attacks over the past five years. Hospitals, in particular, are attractive targets for cybercriminals due to the pressures these organizations face to quickly restore critical systems and data needed for patient care.

The theft of valuable protected health information (PHI) is a growing concern. Over half of healthcare CFOs (51%) say privacy breaches are a bigger risk in 2024 compared to 2023, according to **BDO's 2024 Healthcare CFO Outlook Survey**. Cybercriminals exploit patient information to commit identity theft, enabling them to access expensive healthcare services or file fraudulent tax returns. The patient care repercussions from a cyberattack are severe and can lead to delays in procedures, longer length of stay, and increased mortality rates, in some cases. For healthcare providers, such data breaches can lead to significant loss in patient trust in addition to negative legal, reputational, and financial consequences.

Many healthcare organizations lack cybersecurity defenses that are sophisticated enough to address today's threat landscape. To protect their patients and organization, healthcare providers must be aware of their cybersecurity risks, the vulnerabilities of their information assets, and understand the tactics cybercriminals could use to exploit them. Armed with this information, organizations can then develop a plan to prevent and effectively respond to potential cyberattacks.



The Evolution of Cybersecurity in Healthcare

Healthcare providers are increasingly interested in improving the maturity of their cybersecurity posture. In the past decade, growing enforcement of the Health Insurance Portability and Accountability Act (HIPAA) prompted providers to enhance their security measures to safeguard patient data.

Unfortunately, healthcare providers' cybersecurity resources and budgets are often limited and inadequate to address their critical vulnerabilities. This leaves gaps in their cybersecurity posture. Often, lack of up-to-date hardware and software asset inventory coupled with weak vulnerability and patch management processes can lead to the exploitation of security flaws in outdated IT systems — wreaking havoc. Additionally, not all healthcare providers are able to prioritize and invest enough resources in third-party risk management programs. Cybercriminals can also exploit vulnerabilities in commonly used third-party tools for backdoor access to operations-critical systems within the healthcare provider's environment.

Cybercriminals know that third-party suppliers may be even further behind on cybersecurity maturity than healthcare providers and may have fewer resources to patch security flaws in their digital infrastructure. In the event healthcare providers, third-party vendors, or business associates suffer a cyberattack, the downstream exposure can be devastating.

Primary Methods of Attack

Phishing is one of the most common ways cybercriminals breach healthcare organizations' systems and infrastructure. By clicking one phishing link, it's possible for end-users to essentially give hackers the credentials and access they need to hijack IT systems and disrupt a healthcare provider's operations. Hackers can also trick users into exporting PHI or money through malicious links.

Generative artificial intelligence has allowed cybercriminals to impersonate trusted individuals in increasingly sophisticated social engineering attacks. Using a short clip of an executive's voice, hackers can generate convincing voice messages directing employees to send PHI, wire money, or provide credentials to cybercriminals. Generative AI can also help cybercriminals create more persuasive emails by capturing the writing style of a trusted individual. Besides social engineering attacks, threat actors with limited programming capabilities can use generative AI to aid in developing malware that can exploit electronic health records (EHR) and other critical systems.

While social engineering attacks remain popular, hackers are still focused on discovering and exploiting outdated and unpatched technology.

Developing a Mitigation Plan

Once a healthcare provider understands their cyber risks and the potential impact to their organization, they must develop a security mitigation plan using defense-in-depth, and other industry-leading principles.

To create additional layers of defense, healthcare providers must segment information networks to reduce impact. User credentials that can be used to access multiple organizational systems are an ideal target for cybercriminals. When developing an information security framework, organizations should follow the principle of least privilege — limiting user access to only the systems they need to perform their job duties. Administrator-level credentials should be role-based and only be provided to a limited number of well-trained users. These accounts should be reviewed periodically.

Hackers are increasingly targeting the weakest links and other vulnerable points across healthcare providers' supply chains. These targets are often business associates or third parties that offer services to healthcare organizations — especially if those suppliers have access to sensitive information, such as PHI. HIPAA requires healthcare providers to perform due diligence and evaluate the effectiveness of business associates' cybersecurity controls. Healthcare providers and their third parties must develop and implement appropriate remediation based on the results of their due diligence to reduce their risk profile.

While it is imperative for healthcare organizations to have a robust cybersecurity strategy to reduce the impact and likelihood of cyberattacks, they should also develop and periodically test their incident response plans. These plans should address the following responsibilities:

1. **Who will prioritize which clinical and business systems must be restored first during an outage**
2. **Who will be assigned to work with law enforcement**
3. **How employees will be notified of the incident**
4. **When and how patients will be notified that their health information may have been accessed in a cyber-breach**
5. **Which key roles and responsibilities lie with different parts of the organization, including clinical, business, technical, and legal teams**

Developing incident response plans and testing them periodically helps healthcare providers better prepare to restore critical systems and operational processes during a breach or ransomware crisis.

Defense-in-Depth:

A strategy where multiple layers of defense measures are established in case a security control is breached in one of the layers. When one layer falls, the next layer remains intact to defend the system from being compromised.

Legal Consequences After a Cyberattack

Beyond the financial and reputational consequences of a cyberattack, some healthcare providers may find their cyberattacks lead to a HIPAA violation. In 2023, the HHS' OCR settled its first ever **phishing cyberattack investigation**.

To avoid a HIPAA violation lawsuit, healthcare providers need to follow the HIPAA Security Rule, which establishes the standards providers must follow to protect PHI. According to **HHS guidance**, to comply with the HIPAA Security Rule, healthcare providers must take steps to "evaluate risks and vulnerabilities in their environments and to implement reasonable and appropriate security measures to protect against reasonably anticipated threats or hazards to the security or integrity of e-PHI."

The HHS has designed a **four-tier structure** to penalize healthcare providers that violate the HIPAA Security Rule. Lower-tier penalties are issued when healthcare providers violate a part of the HIPAA Security Rule but took a reasonable amount of care to follow the law. Higher-tier penalties are issued when healthcare providers are deemed to be willfully negligent of the HIPAA Security Rule and/or fail to correct the violation. For Tier Four violations, the most serious level, there is a minimum penalty of $50,000 per violation.

It is challenging to develop a cybersecurity framework that is aligned with today's evolving regulatory landscape. Healthcare organizations should consider pursuing a **SOC for Cybersecurity report**, which provides organizations with third-party attestation that their cybersecurity risk management program is effective and aligned with the latest regulatory requirements.

Healthcare organizations should also review the **latest cybersecurity disclosure rules** from the Securities and Exchange Commission (SEC), including updated reporting requirements for SEC Forms 8-K and 10-K filings.

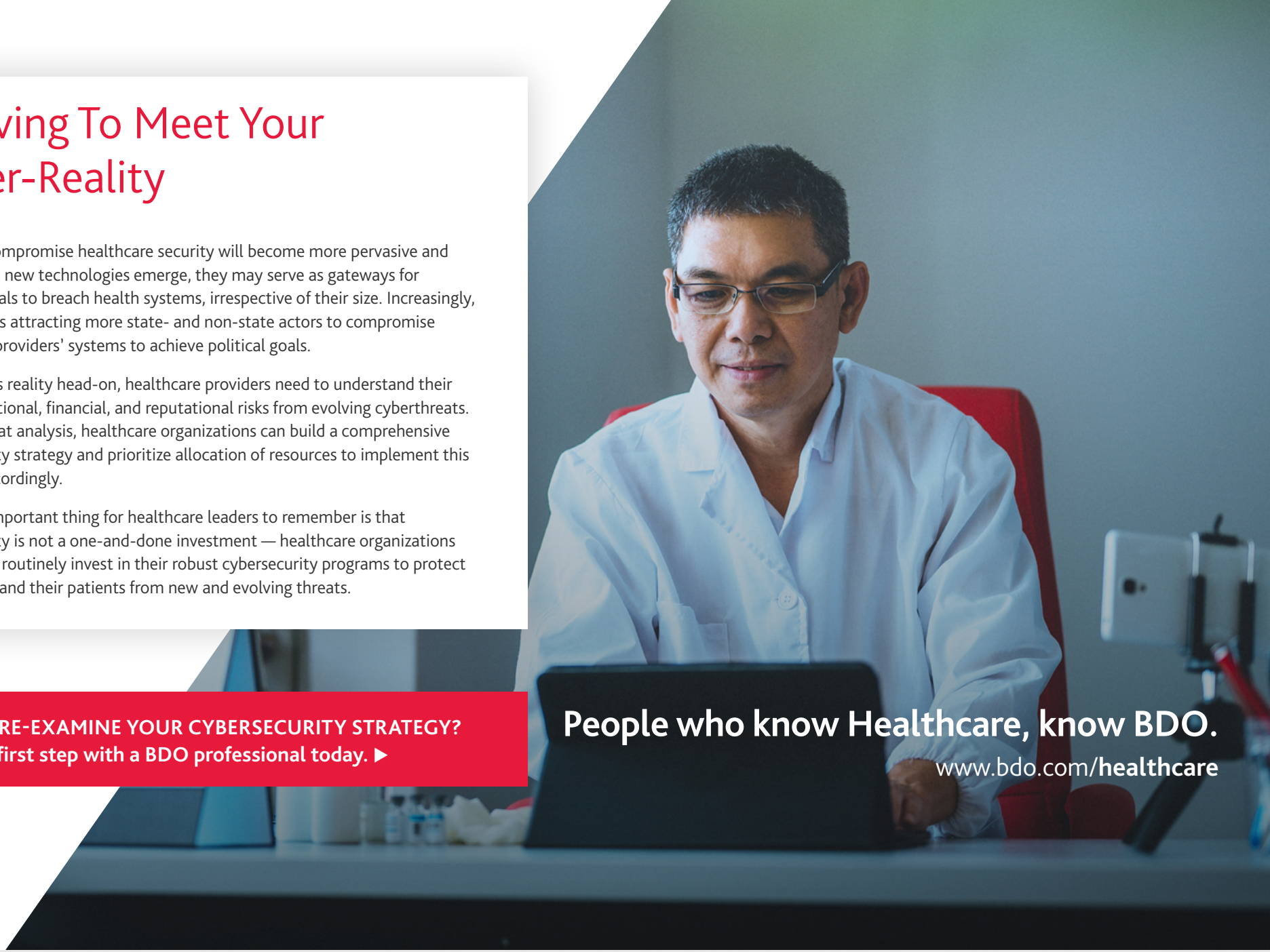
READY TO TAKE ACTION TO MEET YOUR CYBERSECURITY COMPLIANCE NEEDS?
Reach out to BDO's third-party attestation professionals today. ▶

Evolving To Meet Your Cyber-Reality

Efforts to compromise healthcare security will become more pervasive and complex. As new technologies emerge, they may serve as gateways for cybercriminals to breach health systems, irrespective of their size. Increasingly, hacktivism is attracting more state- and non-state actors to compromise healthcare providers' systems to achieve political goals.

To meet this reality head-on, healthcare providers need to understand their legal, operational, financial, and reputational risks from evolving cyberthreats. Based on that analysis, healthcare organizations can build a comprehensive cybersecurity strategy and prioritize allocation of resources to implement this strategy accordingly.

The most important thing for healthcare leaders to remember is that cybersecurity is not a one-and-done investment — healthcare organizations will need to routinely invest in their robust cybersecurity programs to protect themselves and their patients from new and evolving threats.



TIME TO RE-EXAMINE YOUR CYBERSECURITY STRATEGY?
Take the first step with a BDO professional today. ▶

People who know Healthcare, know BDO.

www.bdo.com/**healthcare**