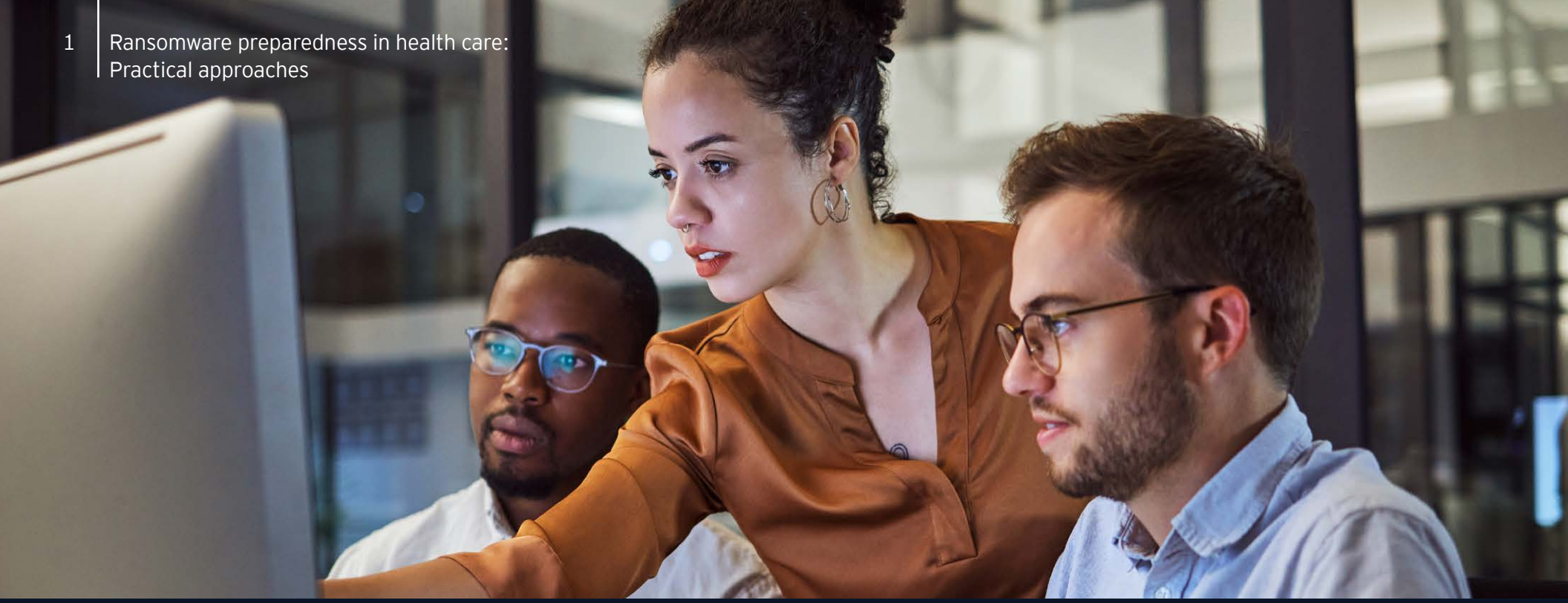
Ransomware preparedness in health care

Practical approaches

EY
Building a better working world



The challenge

Why health care organizations need a proactive approach to ransomware

Ransomware is on the rise across sectors, but its impact is especially significant in health care, where disruptions to operations can be a matter of life and death. From 2021 to 2023, the number of **ransomware attacks on US health care organizations increased by nearly 70%**, according to the FBI's Internet Crime Reports. And during that same three-year span, the health care and public health sector was the primary target for ransomware attacks, topping the list of critical infrastructure sectors each year.[1,2,3] These unsettling trends emphasize how critical it has become for health care organizations to establish robust preparedness, response and recovery plans when it comes to ransomware.

As threat actors' approaches become more sophisticated and as the integration of artificial intelligence (AI) amplifies the effectiveness of ransomware attacks, strong detection and response capabilities are no longer optional in the health care sector. Organizations must prioritize a comprehensive ransomware readiness strategy that includes, but is not limited to, in-depth controls, user training and awareness, specialized readiness playbooks, regular readiness exercises integrated into business continuation plans, the use of advanced technologies for real-time threat analysis and response, and the establishment and practice of response procedures. Anything less, and the organization could jeopardize patient care while exposing itself to substantial reputational, operational, financial and other qualitative risks.

[1]Federal Bureau of Investigation Internet Crime Report 2023, FBI, 2023.
[2]Federal Bureau of Investigation Internet Crime Report 2022, FBI, 2022.
[3]Federal Bureau of Investigation Internet Crime Report 2021, FBI, 2021.

Intensifying urgency

Given the impacts of ransomware on the sector, as well as intensifying scrutiny from governing bodies and regulators, potential regulation and support for health care organizations may be forthcoming. In the meantime, the need for these organizations to prepare for ransomware attacks continues to become increasingly urgent.

However, despite this rapidly growing need, many organizations struggle to develop and execute preparedness, response and recovery plans consistently. The key cybersecurity challenges they face include:

1 Legacy system vulnerabilities

Reliance on outdated medical systems and software and devices that lack built-in security features or vendor support

2 An expanding attack surface area

Growing use of Internet of Things devices and connected medical equipment, which expands the potential attack surface

3 Cyber skill and budget constraints

Limited budgets and resources for cybersecurity initiatives, making it difficult to invest in the necessary technology, personnel and training to build and maintain a robust security posture

4 Multi-vendor integration risk

Having multiple vendors, which poses a growing challenge for security teams in thoroughly evaluating each product; a multi-vendor approach can provide multiple access points for attack through third parties

5 Competing priorities

The prioritization of day-to-day operations combined with a sense of impossibility in getting ahead of cyber threats, as well as the perception of cyber as a sole remit of an IT practitioner — resulting in an adverse impact on the mind and wallet share needed to combat cyber threats at providers and health systems operating under already considerable financial constraints

Phases of an attack

1 Reconnaissance

A threat actor investigates potential targets by collecting and analyzing both publicly available organizational data and results of open port scanning, phishing campaigns and leaked data on dark web forums.

2 Initial access

The threat actor uses phishing emails or exploits kits or software vulnerabilities to access the target organization. The threat actor may also purchase access from an initial access broker, a party that specializes in gaining unauthorized access to an organization and then sells that access.

3 Lateral movement and privilege escalation

The attacker moves undetected throughout the network, seeking higher privileges with access to critical systems and data.

4 Deployment

Once necessary access has been acquired, the attack deploys the ransomware payload, encrypting critical files and data and crippling the victim organization. Organizations will usually receive ransom demands following successful deployment of the ransomware.

Possible consequences

- **Delayed patient care,** caused by factors such as an inability to access patient records
- **Appointment cancellations,** which can create backlogs, reduce patient flows and subject the organization to business losses
- **Disruptions to financial operations,** which can compel owners to cut expenses and can result in stalled insurance payments, meaning patients must pay out of pocket
- **Disruptions to administrative operations,** which can force a facility to revert to manual approaches to billing and prescription processing — leading to increased workloads, time and costs

Take action

Here are four key actions for health care industry leaders who seek to build a strong defense and resilience when it comes to ransomware attacks.

1 Address vulnerabilities and improve disaster recovery and backup capabilities

- Employ the concepts of micro-segmentation and zero trust with a focus on core identity and access management capabilities, particularly privileged access management.
- Use multifactor authentication (MFA) and identify potential gaps in coverage.
- Establish stringent software management and patching protocols based on active tracking of software versions; update schedules and known vulnerabilities.
- Implement thorough data backup procedures that incorporate leading practices, such as regular updates, encryption, use of assorted media and "air gapping" (isolating certain computers or networks and preventing them from establishing external connections).
- Test stored data regularly for restoration and business continuity.

2 Reduce the attack surface and improve detection capabilities

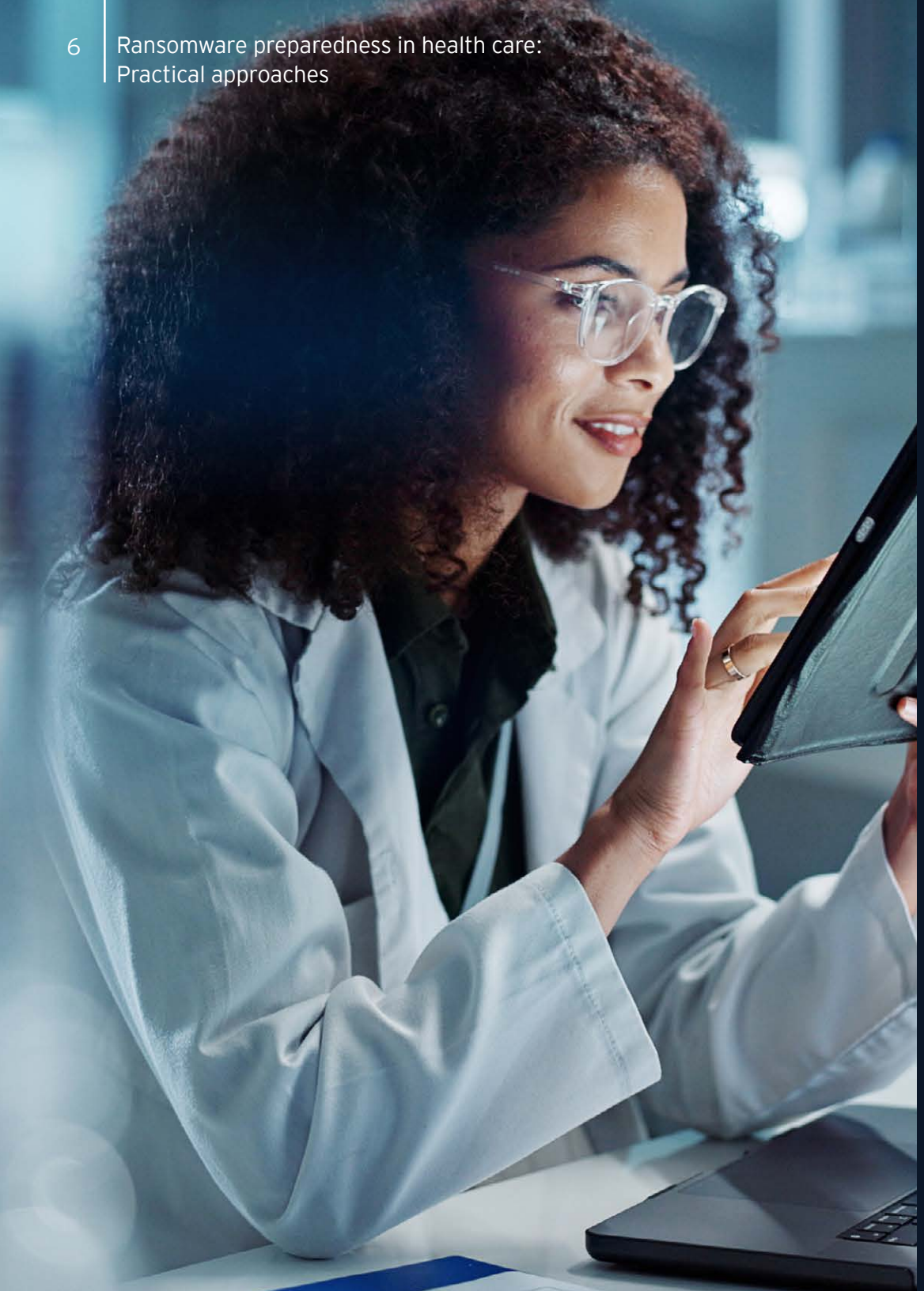
- Merge continuous monitoring with agile detection and response.
- Implement robust endpoint detection and response practices with 24/7 monitoring of all endpoints, including employee computers and medical devices.
- Use antivirus signatures, heuristics scanning, AI and other automated mechanisms for real-time analysis, triaging and anomaly detection.
- Establish protocols to monitor active directory domains throughout the organization and defined processes for system hardening.
- Conduct exercises concerning readiness, response and recovery at least annually; integrate these processes with enterprise business continuation and crisis management plans.

3 Prepare your organization for a breach scenario

- Address coverage and function gaps due to capacity constraints by utilizing emerging technologies, such as AI and automation, and considering available managed services and outsourcing options that can support cyber operations and planning.
- Integrate regular cybersecurity trainings focused on security awareness that support the development of the cyber skills of existing employees.
- Develop ransomware readiness playbooks for key internal groups (e.g., health care technology and security teams; hospital legal teams).
- Consider ways to leverage data minimization and anonymization to protect patient data that exists within your environment and revisit data retention policies to make sure that they are aligned with regulatory requirements and being followed within your organization.

4 Identify, monitor and mitigate cybersecurity risks associated with third parties

- Develop a ransomware readiness playbook for vendors and third parties supporting health care operations.
- Stand up a comprehensive third-party risk management function to track and monitor all third parties that are connected to your organization.
- Collaborate with vendors to evaluate the robustness of their cybersecurity function and establish protocols for prompt remediation of any identified vulnerabilities.



In practice

A Fortune 25 health care organization engaged an EY team to help improve its overall ability to respond to major crisis events. The EY team facilitated a multiphase, simulated cybersecurity incident, an exercise that revealed gaps and inconsistencies that were creating operational, communication and technical challenges during response activities. The organization was able to identify possible improvements to existing crisis management processes and routines, and the exercise provided a safe environment in which the participants could rehearse intergroup coordination and reaffirm their roles and responsibilities during a crisis. The organization used what it learned during a recent ransomware attack on one of its third parties and responded over a week ahead of its competitors, enabling the organization to return more quickly to helping people get the care they needed.

From the field

"

Boards and management teams need to establish organizational policies that place a high priority on patching zero-day vulnerabilities, requires strong passwords and phishing resistant MFA, restricts the use of unauthorized software (e.g., consumer remote access tools), and requires business operations teams to learn how to function with downtime procedures for extended periods of time.

Rather than being surprised by unplanned outages that result from a direct incident or a third-party disruption, organizations should anticipate their inevitability and prepare alternate work procedures. Ultimately, these combined efforts should reduce the impact of incidents and provide a safer workplace while IT systems are unavailable.

– Leading US health system CISO

Contact

Nana Ahwoi
EY Americas Consumer and
Health Cyber Industry Leader
nana.ahwoi@ey.com

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

SCORE no. 24433-241US
BSC no. 2409-64665-CS
ED None.

ey.com