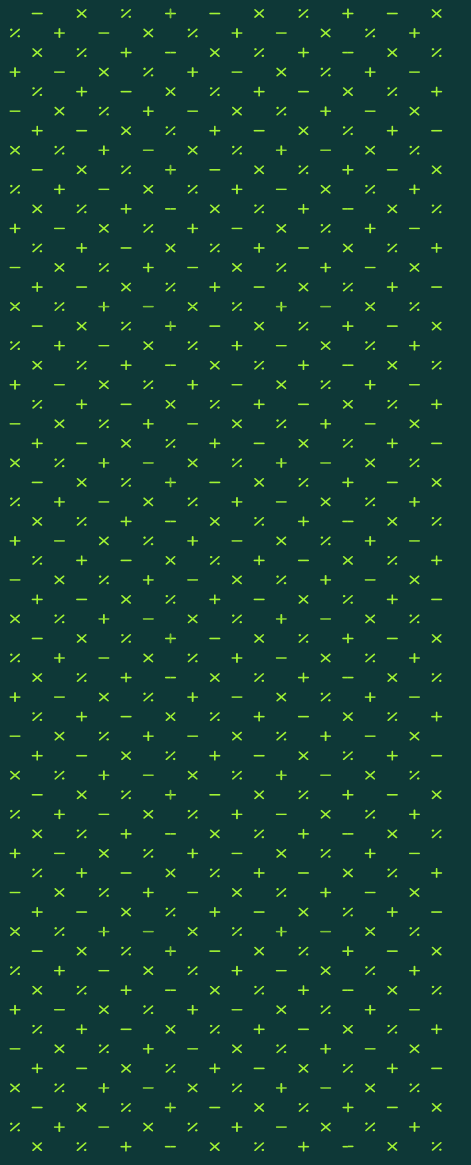
MOSSADAMS

Revenue Resiliency vs Cyber Threats



Agenda

01 THE CURRENT STATE OF CYBERSECURITY

02 CYBERTHREATS AND RISKS

03 CYBERSECURITY AND REVENUE RESILIENCE BEST PRACTICES

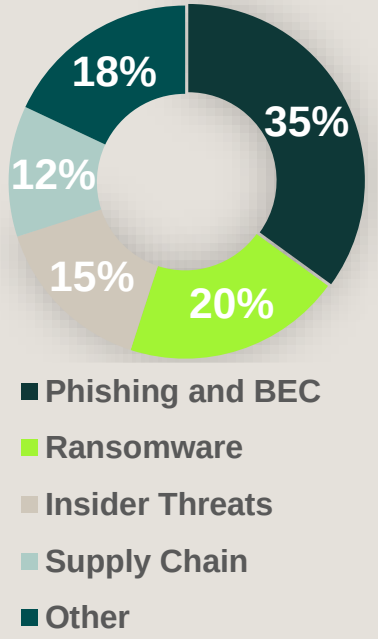
04 KEY TAKEAWAYS

05 Q&A

The Current State of Cybersecurity

The State of Cybersecurity

Attack types in healthcare breaches in 2023



$3M
Average cost of a breach with under 500 employees

$10M
Average cost of a healthcare breach

Data breach costs continue to rise

SMB companies are more likely to experience a breach

Healthcare data breach costs have increased 53% since 2020

$5.13M
Average total cost of a ransomware attack

207
Average number of days to identify a breach

70
Average number of days to contain a breach

Cybersecurity events have outsized impacts on SMBs

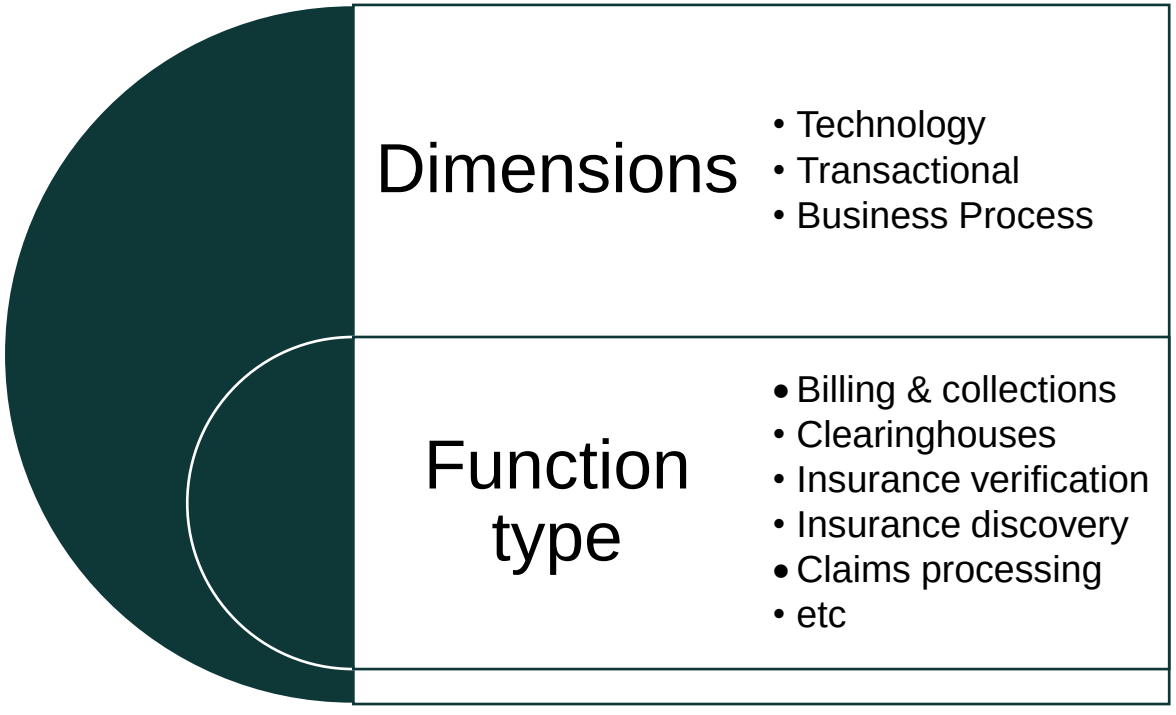
70%

Of CEOs are concerned about their organizations' ability to avert or minimize damage to the business from a cyberattack

Impacts of Cybersecurity Incidents on Healthcare

- Disruption of patient care
- Financial losses
- Patient harm
- Regulatory scrutiny
- Loss of trust

Identifying vendors and other third parties whose security impacts revenue can be a challenge



Assessment tool to identify vendors and third parties

	Technology	Transactional	Business Process
Billing & collections	Vendor A	Vendor B Vendor C	(none)
Clearinghouse	(none)	Vendor D	(none)
Insurance verification	Vendor E	(none)	Vendor F

Vendor risk assessment tracking

Vendor	Risk Rating (1-10)	Risk Management
Vendor A	3	Baseline monitoring
Vendor B	5	Enhanced monitoring
Vendor C	9	Backup “fail over” vendor

Cyberthreats and Risks

Social Engineering (Phishing)

An email or phone call that requests sensitive information (e.g., IT system access data or bank details) in the hope that an employee will inadvertently provide it

- A social engineering attack preys on the psychological willingness of employees to divulge an organization's confidential information.
- These attacks involve an email or phone call from a malicious actor who appears to be an individual or well-known business.
- The target tends to be an unaware or untrained employee who may be willing to share desirable information, such as their system password or sensitive information.
- 90% of all cyberattacks begin with phishing.

Business Email Compromise (BEC)

Specific types of BEC

False Invoice Scheme: Attackers pretend to be a supplier requesting funds transfers for payments to an account owned by fraudsters.

Account Compromise: An executive or employee email account is hacked and used to request invoice payments to vendors listed in their email contacts. Payments are then sent to fraudulent bank accounts.

Attorney Impersonation: An attacker impersonates a lawyer or other representative from a company's law firm who is responsible for sensitive matters.

Data Theft: HR and bookkeeping employees are targeted in order to obtain personal or otherwise sensitive information about employees or executives. This data can be very helpful for future attacks.

Whaling/CEO Fraud: BEC and spear phishing-focused attacks that appear to come from a company's executive management or Board of Directors.

Ransomware

A type of malware that attempts to extort money from a user by infecting and taking control of their systems, files, and documents

- Attackers encrypt data and hold it until a ransom is paid.
- Some attackers also exfiltrate the data and threaten to publish sensitive data online.
- Ransomware can spread quickly through a network, infecting multiple systems.
- It is relatively easy to deploy and has a high success rate.
- It is delivered by using phishing emails or exploiting known software vulnerabilities.
- Dealing with an attack is complicated and costly.
- Organizations have experienced significant business impact from ransomware, including loss of revenue, damage to their brand, unplanned workforce reductions, and even closure of the business altogether.

Other Threats and Risks

Cybersecurity threats are acts performed by individuals who have harmful intent.

The goal is to steal data and cause damage to/disrupt computing systems.

Compromised Credentials: When lost, stolen, or exposed credentials give attackers unfettered access.

Malicious insiders: Disgruntled employees can expose private information or provide information about company-specific vulnerabilities.

Malware: Malicious programs that disrupt systems or encrypt files and demand payment to decrypt.

Password Attacks: Similar to compromised credentials, attackers use various methods to identify weak/reused passwords.

Cloud Vulnerabilities/Misconfigurations: Misconfiguring cloud file repository access settings, or the prevalence of “shadow IT”.

Cybersecurity and Revenue Resilience Best Practices

Healthcare organizations should mobilize all functions to become more resilient

HHS Path Forward on Cyber Improvements

- HHS released sector-specific cybersecurity performance goals (CPGs) to help prioritize key security actions and reduce risk.
- Provides resources to incentivize and implement cybersecurity practices.
- Implements an HHS-wide strategy to support greater enforcement and accountability.
- Expands and matures the “one-stop shop” within HHS for healthcare sector cybersecurity.

Essential CPGs

- **Mitigate Known Vulnerabilities**
- **Email Security**
- **Multifactor Authentication**
- **Basic Cybersecurity Training**
- **Strong Encryption**
- **Revoke Credentials for Departing Workforce Members**
- **Basic Incident Planning and Preparedness**
- **Unique Credentials**
- **Separate User and Privileged Accounts**
- **Vendor/Supplier Cybersecurity Requirements**

Enhanced CPGs

- **Asset Inventory**
- **Third-Party Vulnerability Disclosure**
- **Third-Party Incident Reporting**
- **Cybersecurity Testing**
- **Cybersecurity Mitigation**
- **Detect and Respond to Relevant Threats and Tactics, Techniques, and Procedures (TTP)**
- **Network Segmentation**
- **Centralized Log Collection**
- **Centralized Incident Planning and Preparedness**
- **Configuration Management**

Backup for critical functions

Revenue cycle vendors are beginning to focus on providing standby capabilities for critical revenue-related functions. This approach can allow providers to resume revenue cycle functions within hours or days.

Functions where this is becoming common:

- Eligibility verification
- Patient liability estimation
- Bill scrubber
- Clearinghouse
- Billing & collections

In order for providers to receive the benefits of this approach, they should plan to have the “fail over” solution implemented and have at least a core set of employees trained on its use.

Finance / Rev Cycle Concerns

Cost: how much will this all cost?

- Cyber team
- Backup vendors
- Cyber insurance
- Other internal costs

Oversight: how should I be collaborating with IT security?

- Setting priorities
- Shared understanding of risks
- Drills
- Response to incidents

Board: what updates should I give my Board?

- Level of investment in cyber risk management
- Communicate potential financial and operational impact of a cyber event
- Risks in the environment

What you can do now

- Evaluate your vendor management strategy
- Identify critical functions and develop risk management approach for each, with consideration of “fail over” vendors
- Proactively collaborate with Board on risk management approach
- Work with IT security team on periodic drills and business continuity planning
- At least annually, stress test your liquidity based on impact scenarios

Potential Changes to Healthcare Cybersecurity Regulations

- Regulatory bodies may increase fines and penalties for non-compliance with cybersecurity regulations
- Regulations may expand to cover new technologies like AI, IoT, and cloud computing, increasing compliance burdens
- Organizations may be required to notify patients and regulators of breaches more quickly
- Regulations may emphasize a risk-based approach to cybersecurity, requiring organizations to prioritize and manage risks effectively
- Increased focus on governance and oversight of cybersecurity programs

Key Takeaways

- Cybersecurity is an investment in patient safety.
- Securing information is a financial risk function.
- Data breaches are expensive, and recovery costs can exceed estimates very quickly, so ensure there is a viable plan to respond, recover, and reduce these expenditures.
- Hold business partners and vendors to the same standard of cybersecurity in your enterprise.
- Educate your workforce on the threats and risks regularly.
- Attacks will continue to evolve in sophistication, so defensive measures must keep up.

Best Practice Guidelines

- https://405d.hhs.gov/Documents/tech-vol1-508.pdf
- https://405d.hhs.gov/Documents/tech-vol2-508.pdf
- https://405d.hhs.gov/information#hicp
- https://www.nist.gov/cyberframework/updating-nist-cybersecurity-framework-journey-csf-20
- https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/healthcare-and-public-health-sector
- https://www.cisecurity.org/cis-benchmarks

Questions

Troy Hawes, Managing Director
Cybersecurity Consulting
troy.hawes@mossadams.com
206-302-6529

Richard Riter, Health Care Consulting Director – Revenue Cycle
richard.riter@mossadams.com
206-748-4915

The material appearing in this presentation is for informational purposes only and should not be construed as advice of any kind, including, without limitation, legal, accounting, or investment advice. This information is not intended to create, and receipt does not constitute, a legal relationship, including, but not limited to, an accountant-client relationship. Although this information may have been prepared by professionals, it should not be used as a substitute for professional services. If legal, accounting, investment, or other professional advice is required, the services of a professional should be sought.

Praxity does not practice the profession of public accountancy or provide audit, tax, consulting or other professional services. Services are delivered by member firms, which are independent separate legal entities. The Alliance does not constitute a joint venture, partnership or network between participating firms and Praxity does not guarantee the services or the quality of services provided by participating firms. Praxity is not a 'network' within the meaning of the IESBA Code of Ethics. Praxity is organised as an international not-for-profit entity under Belgian law with its registered office in Belgium. Praxity has its registered administrative office at Suite 2, Beechwood, 57 Church Street, Epsom, Surrey KT17 4PX, UK. which is operated under Praxity - Global Alliance Limited (company number: 07873027), a limited by guarantee company registered in England and Wales.

Assurance, tax, and consulting offered through Moss Adams LLP. ISO/IEC 27001 services offered through Moss Adams Certifications LLC. Investment advisory offered through Moss Adams Wealth Advisors LLC.

©2024 Moss Adams LLP

THANK YOU

The material appearing in this presentation is for informational purposes only and should not be construed as advice of any kind, including, without limitation, legal, accounting, or investment advice. This information is not intended to create, and receipt does not constitute, a legal relationship, including, but not limited to, an accountant-client relationship. Although this information may have been prepared by professionals, it should not be used as a substitute for professional services. If legal, accounting, investment, or other professional advice is required, the services of a professional should be sought.

Praxity does not practice the profession of public accountancy or provide audit, tax, consulting or other professional services. Services are delivered by member firms, which are independent separate legal entities. The Alliance does not constitute a joint venture, partnership or network between participating firms and Praxity does not guarantee the services or the quality of services provided by participating firms. Praxity is not a 'network' within the meaning of the IESBA Code of Ethics. Praxity is organised as an international not-for-profit entity under Belgian law with its registered office in Belgium. Praxity has its registered administrative office at Suite 2, Beechwood, 57 Church Street, Epsom, Surrey KT17 4PX, UK. which is operated under Praxity - Global Alliance Limited (company number: 07873027), a limited by guarantee company registered in England and Wales.

Assurance, tax, and consulting offered through Moss Adams LLP. ISO/IEC 27001 services offered through Moss Adams Certifications LLC. Investment advisory offered through Moss Adams Wealth Advisors LLC.

©2024 Moss Adams LLP

THANK YOU