Cyber Attack: How to Protect Your Center

Jeremy D. Rucker

Attorney

Spencer Fane LLP

O: 214.459.5880
M: 817.821.5002
jrucker@spencerfane.com
www.spencerfane.com
www.jeremydrucker.com

Iowa Oncology Society

KANSAS SOCIETY OF CLINICAL ONCOLOGY

MISSOURI ONCOLOGY SOCIETY

Disclosure of Conflicts of Interest

Jeremy Rucker has no relevant financial relationships to disclose.

Disclaimer

The information and opinions in this presentation and the supplemental materials are provided “AS IS” and should not be used or referred to as primary legal sources, nor construed as establishing medical standards of care for the purposes of litigation, including expert testimony. The standard of care is dependent upon the particular facts and circumstances of each individual case and no generalization can be made that would apply to all cases. The presenter does not warrant the accuracy or completeness of the information presented herein and disclaims all liability that may arise from the reliance on statements and information presented. The information presented should be used as a resource, selected and adapted only with the advice of your attorney.

What is a Cyber Attack

Attack initiated from a computer against a computer system that compromises the confidentiality, integrity, or availability of the target computer or information stored on it.

- Data theft
- Gaining (or attempting to gain) unauthorized access to computer system
- Denial-of-service
- Installation of viruses
- Unauthorized or inappropriate use of computer system
- Unauthorized changes to computer system

What is a Cyber Attack

General Categories of Attack:

- Insiders
- Social Engineering
- Exploitation Malware
- Extortion and Blackmail (ransomware)

Ransomware

- Ransomware is malicious software, or malware, that threat actors use to encrypt your data and deny you access to it until a ransom is paid.
- Nobody cares how intrinsically valuable your data is.
- You need it. The hackers know it. You will pay to get it if you have not prepared.
- Also – exfiltration + publication is the recent trend (+ calling, ++ reporting crimes, anticipate calling HHS).

Ransomware

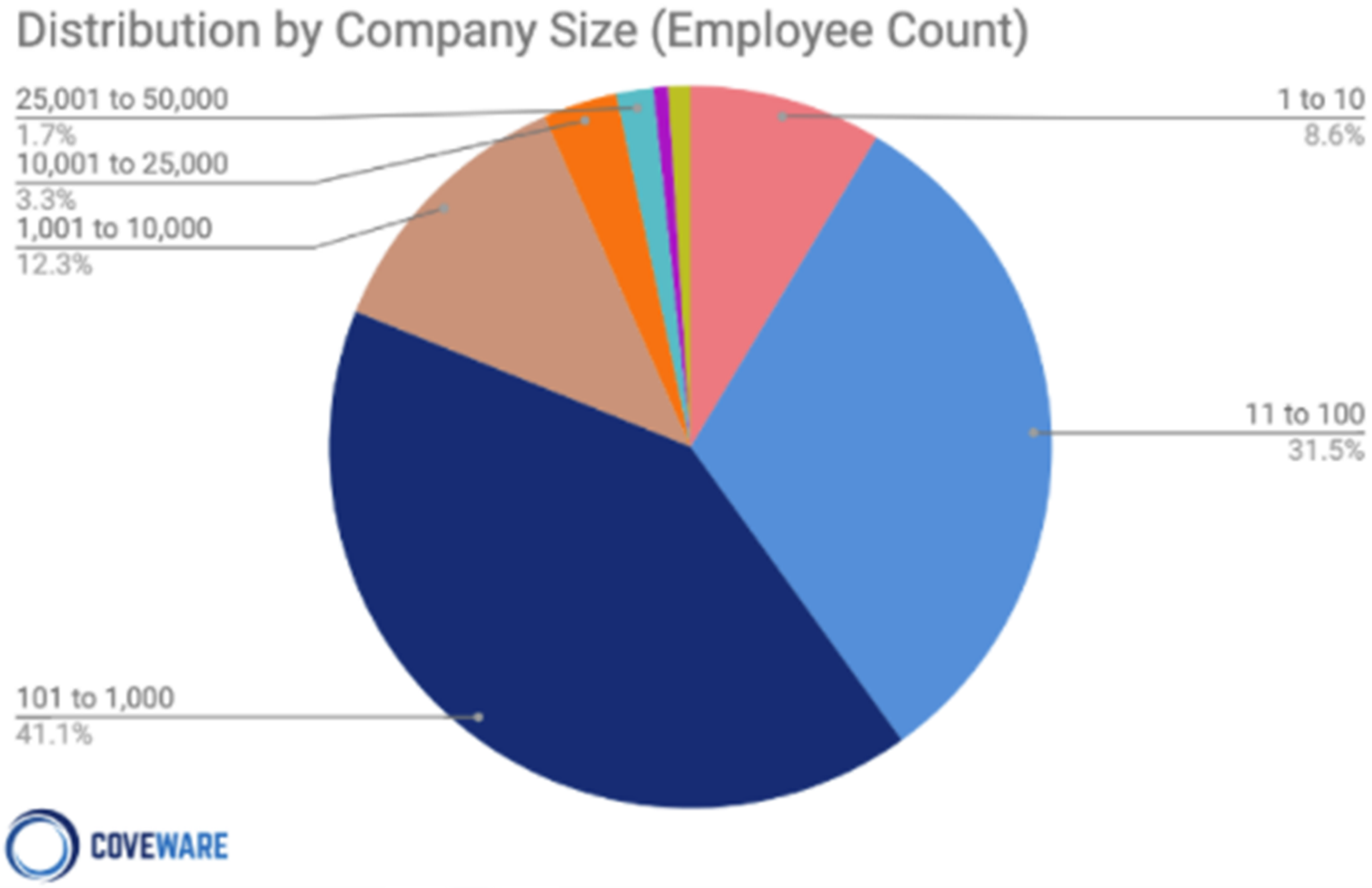
U.S. Health & Human Services – FACT SHEET: Ransomware and HIPAA*

- When electronic protected health information (ePHI) is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the information), and thus is a "disclosure" not permitted under the HIPAA Privacy Rule.
- Unless the covered entity or business associate can demonstrate that there is a "…low probability that the PHI has been compromised," based on the factors set forth in the Breach Notification Rule, a breach of PHI is presumed to have occurred. The entity must then comply with the applicable breach notification provisions, including notification to affected individuals without unreasonable delay, to the Secretary of HHS, and to the media (for breaches affecting over 500 individuals) in accordance with HIPAA breach notification requirements. See 45 C.F.R. 164.400-414.
- To demonstrate that there is a low probability that the protected health information (PHI) has been compromised because of a breach, a risk assessment considering at least the following four factors (see 45 C.F.R. 164.402(2)) must be conducted:
  - the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
  - the unauthorized person who used the PHI or to whom the disclosure was made;
  - whether the PHI was actually acquired or viewed; and
  - the extent to which the risk to the PHI has been mitigated.
- If the electronic PHI (ePHI) is encrypted by the entity in a manner consistent with the Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals such that it is no longer "unsecured PHI," then the entity is not required to conduct a risk assessment to determine if there is a low probability of compromise, and breach notification is not required.

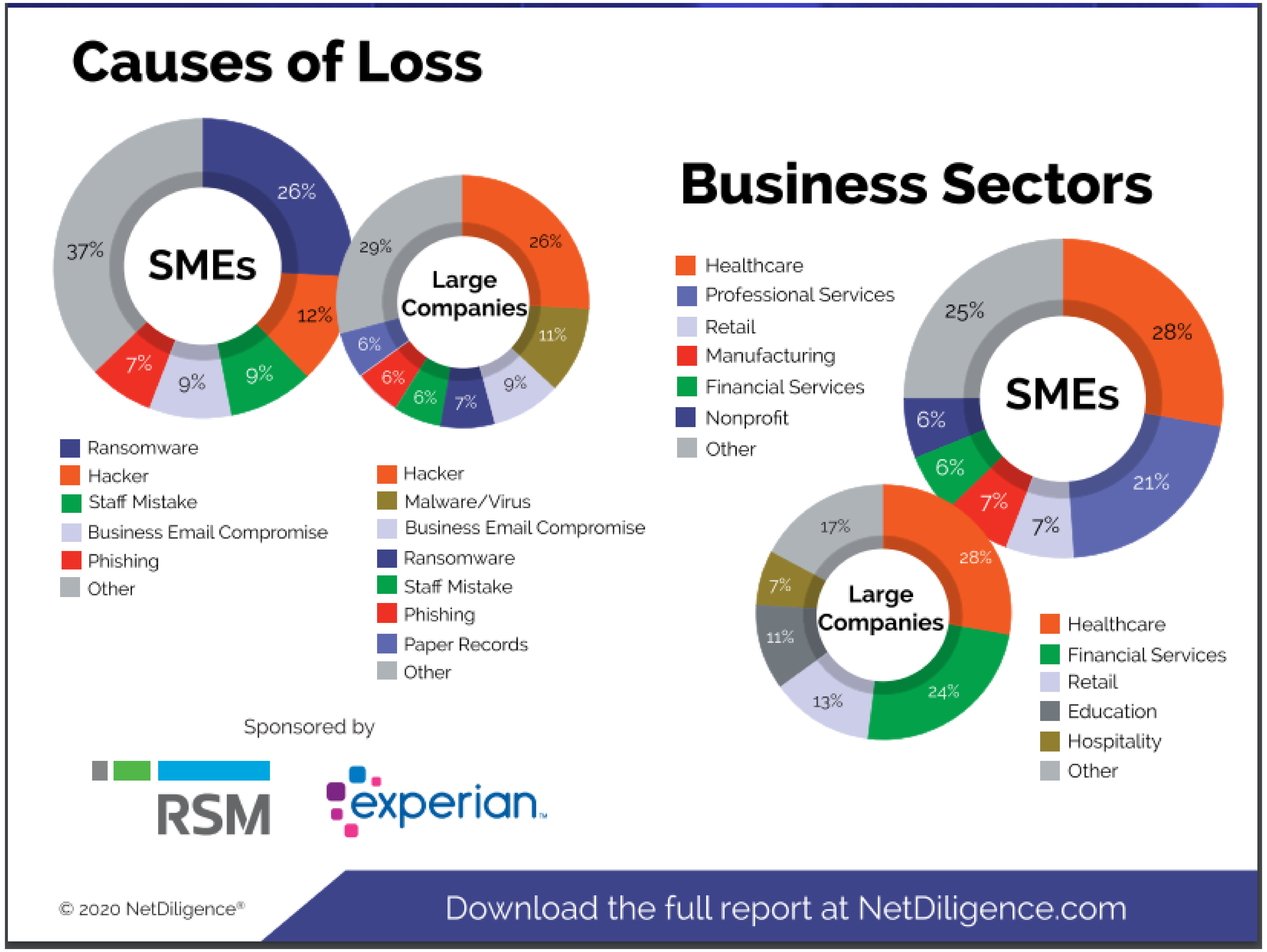
* U.S. Dept. of Health & Human Services, *FACT SHEET: Ransomware and HIPAA*, https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

Who is at risk from an attack?

- Every organization with a computer connected to the internet is at risk.
- Every single one.
- Yes, yours also!



How much is healthcare under attack?



Causes of Loss

- Ransomware
- Hacker
- Staff Mistake
- Business Email Compromise
- Phishing
- Other

- Hacker
- Malware/Virus
- Business Email Compromise
- Ransomware
- Staff Mistake
- Phishing
- Paper Records
- Other

Business Sectors

- Healthcare
- Professional Services
- Retail
- Manufacturing
- Financial Services
- Nonprofit
- Other

- Healthcare
- Financial Services
- Retail
- Education
- Hospitality
- Other

Sponsored by

RSM experian.

Download the full report at NetDiligence.com

Ransomware - what is the impact?

- Your computer systems are shut down.
- You have no access to your data.
- Any operations requiring either computers or data are now shut down.
- Your sensitive information – PHI – is stolen and published on the threat actor’s shame site.

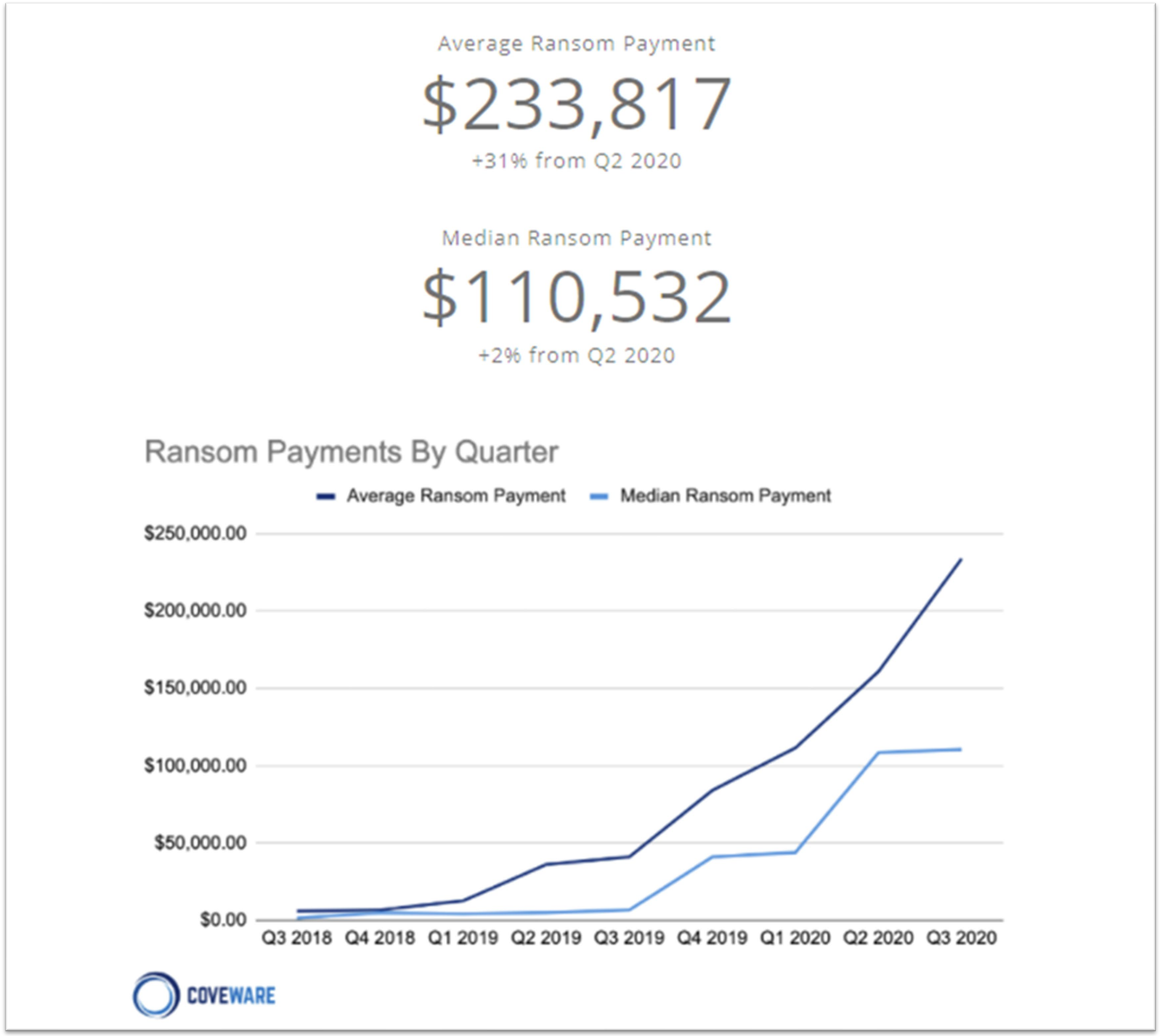
Downtime from a Ransomware Attack is still the most Dangerous Complication

Average Days of Downtime

19

+19% from Q2 2020

Ransomware - what is the impact?



Average Ransom Payment

$233,817

+31% from Q2 2020

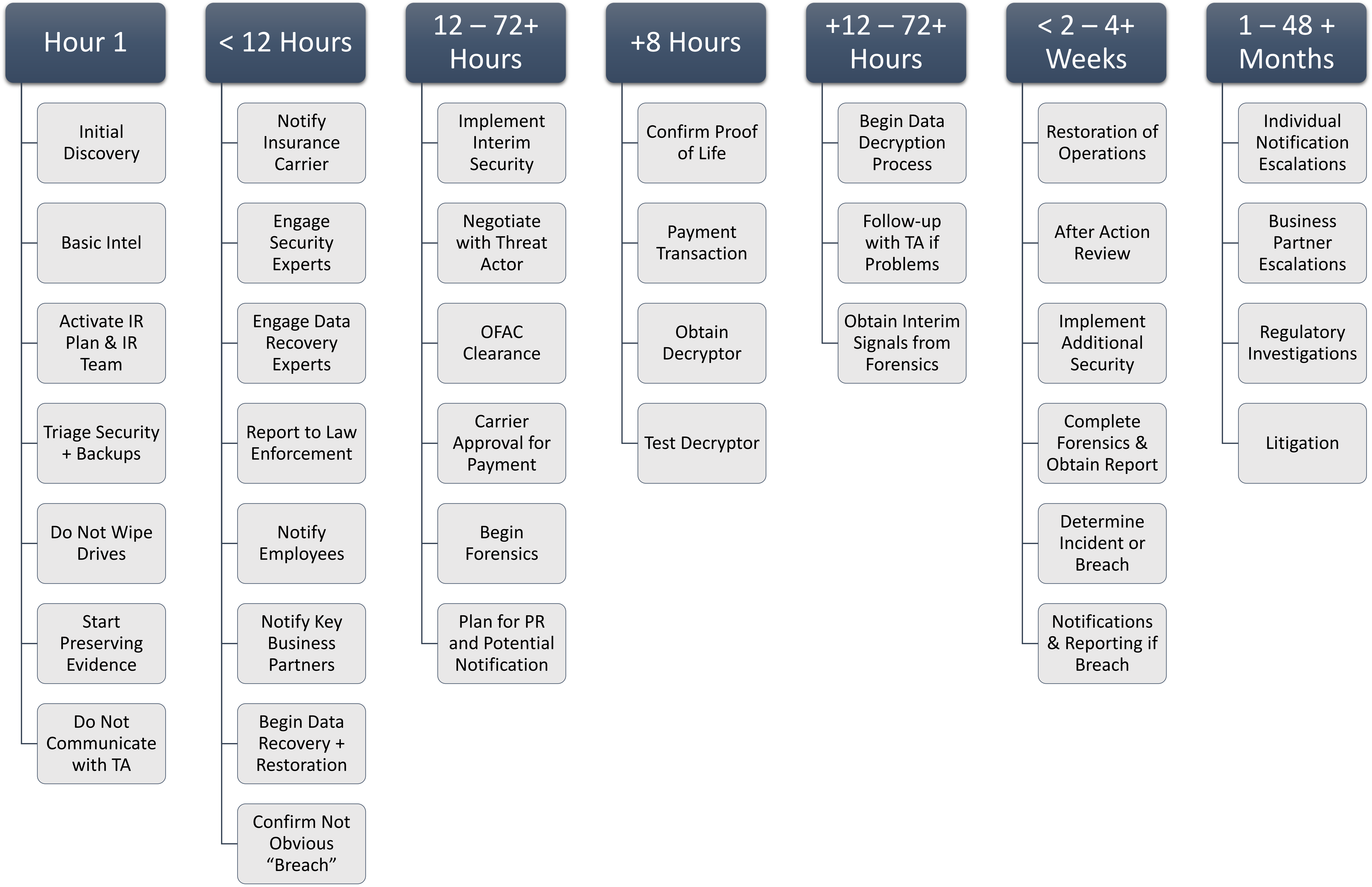
Median Ransom Payment

$110,532

+2% from Q2 2020

Ransom Payments By Quarter

Ransomware Timeline



Hour 1
- Initial Discovery
- Basic Intel
- Activate IR Plan & IR Team
- Triage Security + Backups
- Do Not Wipe Drives
- Start Preserving Evidence
- Do Not Communicate with TA

< 12 Hours
- Notify Insurance Carrier
- Engage Security Experts
- Engage Data Recovery Experts
- Report to Law Enforcement
- Notify Employees
- Notify Key Business Partners
- Begin Data Recovery + Restoration
- Confirm Not Obvious “Breach”

12 – 72+ Hours
- Implement Interim Security
- Negotiate with Threat Actor
- OFAC Clearance
- Carrier Approval for Payment
- Begin Forensics
- Plan for PR and Potential Notification

+8 Hours
- Confirm Proof of Life
- Payment Transaction
- Obtain Decryptor
- Test Decryptor

+12 – 72+ Hours
- Begin Data Decryption Process
- Follow-up with TA if Problems
- Obtain Interim Signals from Forensics

< 2 – 4+ Weeks
- Restoration of Operations
- After Action Review
- Implement Additional Security
- Complete Forensics & Obtain Report
- Determine Incident or Breach
- Notifications & Reporting if Breach

1 – 48 + Months
- Individual Notification Escalations
- Business Partner Escalations
- Regulatory Investigations
- Litigation

Ransomware - common causes

RDP Access	• This is random – scanning web for Internet facing RDP access • Virtual Private Network (VPN) with Multifactor Authentication (MFA)
Phishing	• Email phishing tool • Workforce training and simulated phishing
Unpatched / Outdated Software	• Install patches timely • No unsupported software
Passwords	• Multifactor Authentication (MFA) • Longer passphrases
Backups, Backups, Backups!	• 3-2-1 Backup Process • Something comparable – you may end up with only your offline backup

How to better protect your practice

1. Perform a risk analysis to better understand your organization’s greatest risks – you cannot mitigate what you do not know exists.
2. Backup your data, system images, and configurations, regularly test them, and keep at least one copy of the backups offline. Consider the “3-2-1 backup rule.”
3. Encrypt all sensitive data to ensure that if it is stolen its confidentiality is not compromised.
4. Update and patch your systems promptly, especially external-facing systems. Configure automatic updates on workstations and laptops where feasible.
5. Require multifactor authentication (MFA) for every login when reasonable, especially external-facing systems and services. MFA is using two steps to login instead of just one.

How to better protect your practice

6. Require cybersecurity and phishing training and exercises for all members of your organization, especially senior leadership.

7. De-escalate privilege to the minimum necessary on user accounts, especially for high value target users such as executives, accounting, human resources, and for vendor access.

8. Use a reputable firewall that is configured to block access to known malicious IP addresses.

9. Use a reputable endpoint detection and response (EDR) solution.

10. Identify external-facing systems by looking up IP addresses and DNS subdomains for your organization.

11. Block public access to the services Remote Desktop Protocol (RDP), Secure Shell (SSH), Telnet, and File Transfer Protocol (FTP).

How to better protect your practice

12. Perform vulnerability scans against external-facing systems.

13. Have a security team and check their work.

14. Have an incident response plan and business continuity plan and regularly exercise both.

15. Segment your networks.

16. Choose third-party service providers that are dependable and secure.

17. Implement a cybersecurity framework (e.g., NIST)

18. Review/implement employee policies (e.g., PHI access/use policy)

19. Monitor vulnerability reports

20. Implement anti-virus and other measures to protect against malware

How to better protect your practice

21. Actively monitor and manage log files to detect security incidents
22. Use read-only versions of documents and materials when possible
23. Grant access to PHI only to those with a business need to know

Cyber Incident Response Plan

- Every organization should develop an incident response plan
- Identify cyber attack scenarios and planned responses
- Components:
  - Incident response team
  - Reporting and notification obligations
  - Response steps
  - Investigation
  - Recovery

Incident Response Team

- Develop incident response plan
- Develop checklist for handling initial investigation
- Promote cybersecurity throughout the organization
- Secure organization’s computer network prior to cyber attacks
- Address potential data breach issues
- Direct post-incident reviews and effectiveness of organization’s response

Prepare for resilience: questions your breach coach wants you to ask now

1. Have you collectively brainstormed to think about your greatest cyber risks?
2. Do you have an Incident Response Plan (IRP)?
3. Do you know when to activate the IRP?
4. Does each member of the Security Incident Response Team (SIRT) understand his or her role and responsibility under the IRP?
5. Do you have redundancies for those roles and responsibilities?
6. Do you know who is the "head coach" and, what if that person is unavailable?
7. Do you know what external parties are needed under the IRP?

Prepare for resilience: questions your breach coach wants you to ask now

8. Do you have easy access to all internal and external parties' contact information, with redundancies, including personal cell numbers?
9. Do you have relationships already established with those third parties?
10. Do you have those third parties pre-approved under your cyber insurance policy?
11. Do you have your insurance policy, policy number, and claims contact information handy?
12. How will you access all of this information if your network is down?
13. Have you practiced a mock scenario to test your preparedness? What about if your "head coach" is unavailable?
14. Have you performed After Action Reviews (AAR) and revised your IRP for lessons learned?

Jeremy D. Rucker

Attorney

Spencer Fane LLP

O: 214.459.5880

M: 817.821.5002

jrucker@spencerfane.com

www.spencerfane.com

www.jeremydrucker.com

Iowa Oncology Society

KANSAS SOCIETY OF CLINICAL ONCOLOGY

MISSOURI ONCOLOGY SOCIETY