HORNETSECURITY
BY proofpoint.

FACTSHEET

CYBERSECURITY IN THE HEALTHCARE SECTOR

Digital disruption in healthcare can affect research, care delivery, trust, and safety

In today's digital healthcare environment, everything from diagnostics and treatment to patient records and billing depends on secure and reliable IT systems. A single breach can have far-reaching consequences, not only compromising sensitive patient data, but also disrupting clinical operations, delaying treatments, and, in severe cases, endangering lives. Unlike in many other industries, downtime in healthcare doesn't just mean lost productivity and financial losses – it can directly impact patients' health, making cybersecurity a critical component of quality care.

Why is healthcare a top target?

» **High-value data:** Healthcare organizations hold rich personal information that is ideal for identity theft, fraud, and extortion

» **Urgency of care:** Time pressure increases the likelihood of paying ransoms to restore operations quickly

» **The human factor:** Busy staff and complex collaboration mean higher exposure to phishing, social engineering, and accidental leaks

» **Outdated infrastructure:** Legacy systems and hard-to-patch environments create exploitable security gaps

PATIENT & OPERATIONAL DATA	RESEARCH DATA
• Patient records & medical histories	• Clinical trial data & protocols
• Diagnoses, lab results, imaging	• Research participant datasets
• Insurance, billing, and payment details	• Genomic & biomarker data
• Staff credentials, emails, and internal documents	• Study results and collaboration documents
Trust, credibility, reputation, stakeholder confidence	**Research Integrity, Employer brand**

HORNETSECURITY
BY proofpoint.

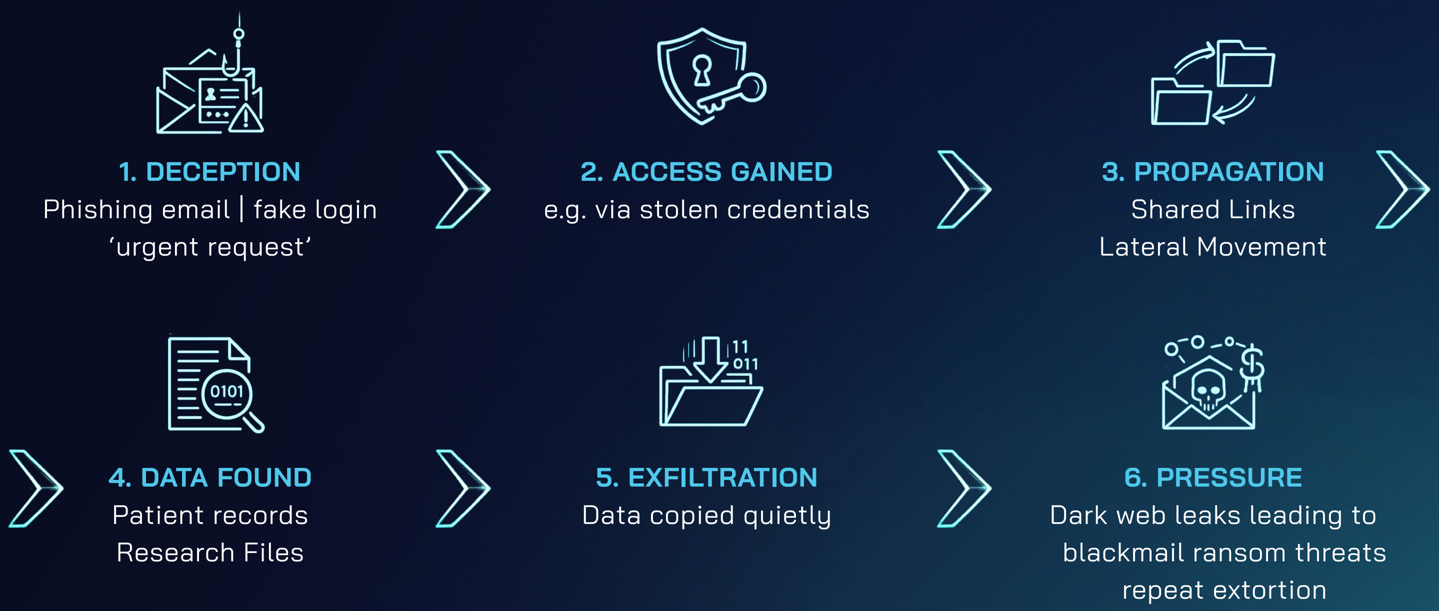
$7.42M
Average cost of a healthcare data breach (costliest industry for 14th year in a row)

279 DAYS
Average time to identify and contain a healthcare breach (longest across industries, >5 weeks longer than the average)

18%
Of healthcare ransomware attacks were caused by compromised credentials

22%
of healthcare attacks were caused by malicious emails

WHAT HAPPENS WHEN DATA IS STOLEN?



1. DECEPTION
Phishing email | fake login
‘urgent request’

2. ACCESS GAINED
e.g. via stolen credentials

3. PROPAGATION
Shared Links
Lateral Movement

4. DATA FOUND
Patient records
Research Files

5. EXFILTRATION
Data copied quietly

6. PRESSURE
Dark web leaks leading to
blackmail ransom threats
repeat extortion

BOOK YOUR DEMO NOW

HORNETSECURITY
BY proofpoint.

10 BEST PRACTICES TO PREVENT DATA BREACHES

✓ Assess & Improve

1. Run regular risk assessments of systems, devices and workflows.

2. Test controls (simulate attacks, validate detection and response plans).

✓ Reduce Human Risk

3. Train staff continuously (e.g., on phishing, social engineering).

4. Build a security-first culture (clear reporting).

✓ Protect Access & Systems

5. Implement strong access controls based on the principle of least privilege.

6. Use multi-factor authentication (MFA) wherever possible.

7. Patch and update IT and medical devices.

✓ Protect & Recover

8. Encrypt sensitive data.

9. Backup critical systems and data using a resilient rule such as 3-2-1-1.

10. Develop an incident response plan that clearly defines roles, contacts, and recovery priorities.

HOW HORNETSECURITY SUPPORTS HEALTHCARE

A comprehensive cloud security suite for Microsoft 365 covering security, compliance, awareness, and backup. It helps healthcare organizations prevent incidents and recover more quickly. Here is an insight into some of the helpful services included:

SECURITY AWARENESS
Strengthen your human firewall with targeted training and realistic phishing simulations to measurably reduce susceptibility to attacks over time.

ADVANCED THREAT PROTECTION
Protects against sophisticated attacks (e.g., spear phishing, ransomware, zero-day exploits) using advanced detection methods.

SPAM & MALWARE PROTECTION
Blocks malicious email content before it reaches your staff’s inboxes, thus protecting clinical communication and reducing inbox-based risks.

365 TOTAL BACKUP
Enables fast recovery of Microsoft 365 data to support the continuity of care and compliance, while reducing the impact of ransomware and accidental deletion.

PERMISSION MANAGEMENT
Enforces least privilege access across Microsoft 365 and highlights risky sharing and misconfigurations.

hornetsecurity.com | info@hornetsecurity.com | +49 511 515 464-0