DynamicQuest.com

IT solutions *for* healthcare.

No other industry faces greater IT challenges. Compliance and security require the highest level of expertise.

INSIDE ›

How to ensure protection and high performance for your IT.

DYNAMIC QUEST®

Healthcare is entrusted with more data—and more important data—than other industries. Healthcare organizations face greater IT challenges than any other category. The industry presents hackers with many more vulnerabilities—and the consequences are the highest.

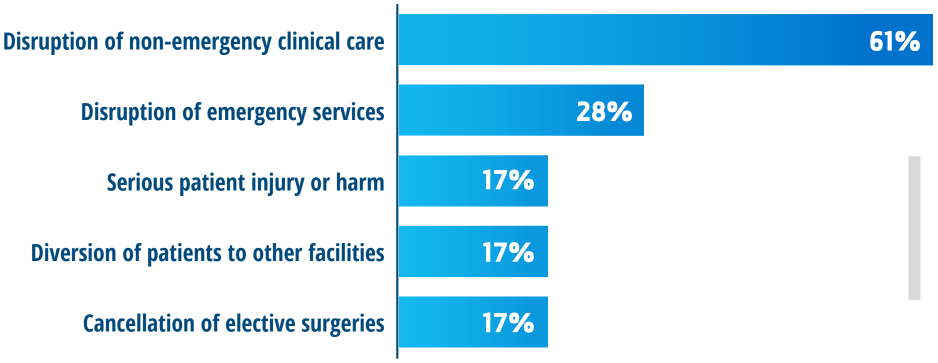
The volume of data—and the associated risk—is staggering. Among many reasons that healthcare is especially vulnerable is that it deals with so much data. Every byte is a valuable asset; it must be diligently safeguarded and tracked.

There is no room for "okay" solutions with the stakes so high. Security breaches in the healthcare space are devastating, with lives and livelihoods at risk. Cyberattacks can interfere with life-sustaining medical devices, affecting patient health directly.

IT management in healthcare requires close collaboration between providers and their IT counterparts. Communication and mutual understanding are critical. Only IT professionals who work day to day in healthcare can provide dependable technical support healthcare organizations need to ensure compliance.

COMPLIANCE + SECURITY
Distinct but Intertwined

The regulations surrounding healthcare enforce the highest possible standards of security, due to the consequential nature of the data and processes involved. Complying with HIPAA regulations, however, is not just about repelling hackers. Training, auditing and reporting are among many requirements that go beyond the usual definition of security.



SIGNIFICANT SECURITY INCIDENTS

Types of patient safety issues

COMPLIANCE

Everybody knows what HIPAA is, right? It's been around for decades, yet its complexity—and the changing conditions of healthcare and technology—make it difficult for even the most diligent organizations to ensure they are compliant.

It's not just HIPAA. There's also HITECH, PHI/ePHI, SRA and more. An IT firm that specializes in healthcare has the broad expertise to help your organization stay compliant.

HIPAA compliance is impossible without the strongest possible security. As we show in the next section, the threats to healthcare IT are proliferating. An active program to implement, monitor, improve and adapt a thorough security regimen can meet the challenge.

COMPLIANCE *is* COMPLICATED

Requirements include (but are not limited to) the following:

6 Annual Audits

- Security Risk Assessment
- Privacy Assessment
- HITECH Subtitle D Audit
- Security Standards Audit
- Asset and Device Audit
- Physical Site Audit

Annual HIPAA and Security Awareness Training

Emergency Contingency Plan

ePHI Access Logs

Identity Access Controls

Notice of Privacy Practices (NPP)

Defined Process for Breach Response

SECURITY

Risks continue to rise. Digital technology generates new benefits at breakneck speed. Most advances, however, introduce new threats. As we all learned to love our smartphones, hackers learned to exploit new vulnerabilities.

Many healthcare organizations are overconfident. This is understandable: If an entity has been fortunate enough to have avoided a serious breach, it is human nature to put the risk out of mind and expect a trouble-free existence. Experts note this overconfidence as contributing to the problem.

> *Michael Ebert, a KPMG partner and healthcare leader at the firm's Cyber Practice, has vividly observed the increased cyber security threat to confidential patient information. He sees overconfidence among healthcare providers and payers, citing the quarter of Forbes respondents who say they don't know their organization's capabilities to detect risk to their systems.*

HOW BAD CAN IT BE?

Ransomware attacks are more common than most realize (possibly due to underreporting by victims). A study by Comparitech reported attacks on 600 organizations, **costing nearly $21 billion.**

$6 Trillion

Estimated cost of security breaches to healthcare organizations by end of 2020.

*https://techjury.net/blog/healthcare-data-breaches-statistics/#gref.

90%

of healthcare organizations reported at least one security breach in the past 3 years.

*Beckers Health IT

TOP THREATS

Experts know how healthcare hackers think. They know where to look for security gaps the healthcare industry is particularly vulnerable to. They can identify vulnerabilities and implement protective solutions quickly.

RANSOMWARE

The healthcare industry suffers more ransomware attacks than any other. It's an attractive target for hackers because they know how disruptive an IT breakdown can be. Victims can lose not just money, but lives. Data leaks can prompt lawsuits with devastating effects.

CLOUD SECURITY

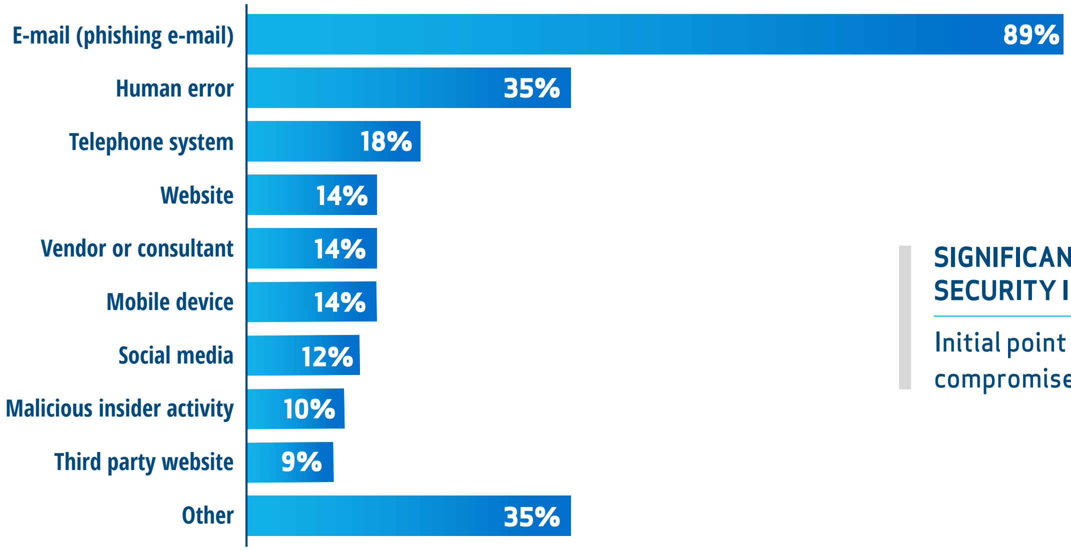
Insufficiently protected data on the cloud is an invitation to hackers. Most healthcare providers take advantage of the undeniable benefits of cloud-based IT. But anything less than top-level protection is a ticking time bomb.

IOT DEVICES

They present tempting targets. Patients wearing insulin pumps, heart monitors and pacemakers benefit from physicians' continual monitoring of their vital signs. But these devices are also access points for hackers.

SMARTPHONES

Everybody's got one, and they're a gateway to hackers. Healthcare programs have made a miracle out of the ubiquity of smartphones, with patients accessing advice and feedback at any time. Unfortunately these same devices present vast new opportunities for those intent on breaking into the IT system.

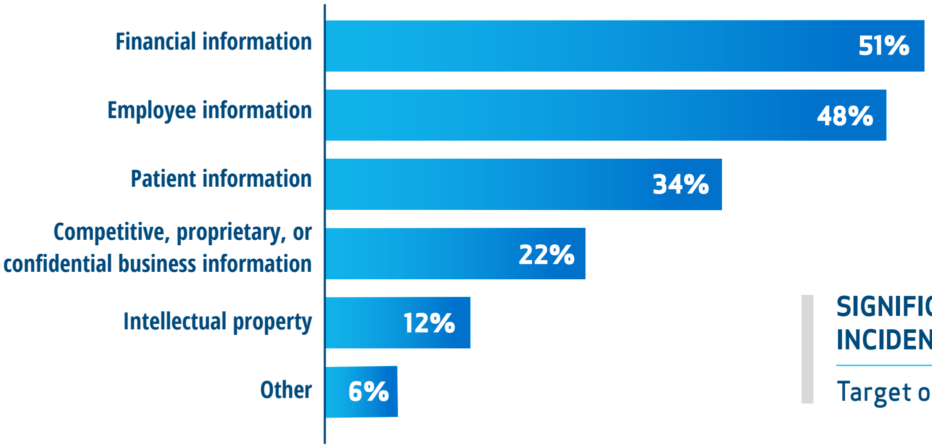


SIGNIFICANT SECURITY INCIDENTS

Initial point of compromise

WHAT DO HACKERS WANT?

Financial information is their primary target. They also seek employee and patient information. All three categories can provide leverage for ransomware demands or other damage.

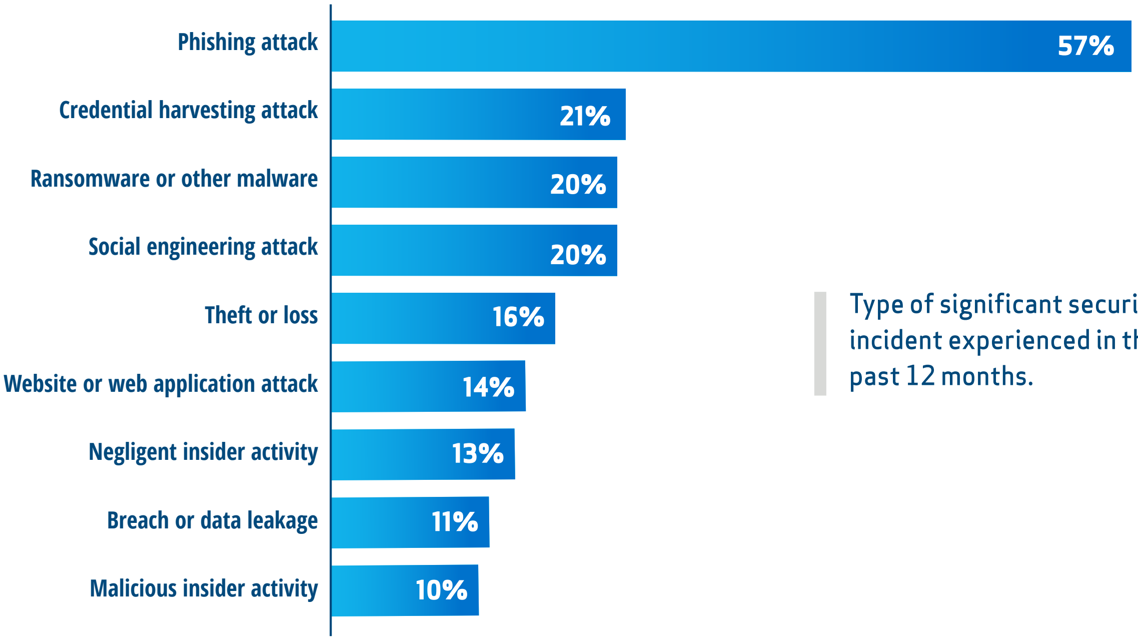


SIGNIFICANT SECURITY INCIDENTS

Target of threat actors

HOW DO THEY GET IN?

Phishing attacks are the most common method. Many other techniques are out there, but exploiting email mistakes by under-trained personnel leads the pack.



Type of significant security incident experienced in the past 12 months.

TAKE ACTION

The strongest protection comes from experts in healthcare IT.

Any decent IT firm knows about technology. The healthcare space requires more. Only technical people with deep knowledge of the unique threats to healthcare organizations can provide the necessary guidance.

A Managed Service Provide (MSP) maintains and strengthens all aspects of an IT system. Some MSPs have special expertise in healthcare's unique regulatory environment, and its challenging security risks. An MSP with this expertise knows the most advanced measures to ensure protection.

A multi-layered approach is the strongest defense. No solution can guarantee 100% security for healthcare IT. The goal is to put as many layers in place as possible, to minimize the potential for a security breach. Because no solution can promise 100% protection, a data recovery plan is crucial. A solid plan preserves your data and helps protect you from the ravages of a serious breach or ransomware demand.

COMPLIANCE & REGULATORY SUPPORT.

Our team of engineers will assist your organization with compliance and regulatory requirements related to your patients' privacy and digital health information.

SERVICE DESK.

Gain access to our IT infrastructure 24x7x365. Our team of professionals will always be available to answer, resolve and route end-user support needs. Our Service Desk solution is also customizable to include a combination of Tier 1, 2 or 3 tickets.

HOW A KNOWLEDGEABLE MSP CAN HELP.

When you bring a Managed Service Provider on board they will need to carry out a security risk analysis (SRA). Its purpose is to ascertain where your business is in comparison to the HIPAA requirements. This analysis will examine:

- Who has access to information and how this is managed
- Training assessment for managers and IT administrators
- How security controls are put in place
- How patient data is stored
- How incident response plans are created and implemented

CLOUD MIGRATION & SUPPORT SERVICES.

Healthcare providers can access a more secure, compliant environment through our data center and hybrid cloud solutions. Protect your patients' critical health care data and meet regulatory compliance standards. Our data center is HIPAA compliant and is SOC 2 Type 2 certified.

IMPROVE MULTI-LOCATION SUPPORT.

Healthcare practices with multiple locations require a network solution that ensures interoperability between different offices. Our team will help consolidate systems to ensure your technology stack is secure and all information is accessible through a centralized data system.

HIPAA SECURITY RISK ASSESSMENT (SRA).

The HIPAA Security Rule requires healthcare organizations to perform an annual Security Risk Assessment (SRA) to assess potential risk to ePHI. Our team continually seeks to incorporate current cybersecurity best practices so your organization can feel content that ePHI is secure and properly documented.

NETWORK ACCESS CONTROL (NAC) SOLUTIONS.

This solution identifies and documents each type of user and device. It continually scans for threats or out-of-date spyware protection. NAC solutions help keep interconnected devices and equipment secure.

DISASTER RECOVERY/BUSINESS CONTINUITY.

Important for any organization, but (once again) critical for healthcare companies. Research reveals widespread vulnerability, with many companies implementing necessary processes only after suffering devastating incidents. A solid system and data recovery plan will ensure that you are not left at the mercy of a ransomware demand for payment in order to recover your critical business data.

50%

of healthcare organizations report having conducted end-to-end security risk assessments.

*HIMSS Cybersecurity Survey

Dynamic Quest's HIPAA/HITECH Auditing & Compliance Support.

HIPAA/HITECH outlines specific auditing requirements healthcare organizations must comply with, as well as penalties for organizations whose information security systems are not in compliance with its standards.

Working with a managed IT service provider that understands these audit requirements is critical. Dynamic Quest's information systems provide protocols and controls to help keep Electronic Protected Health Information (ePHI) secure.

Dynamic Quest will perform an assessment of potential risks to the integrity, accessibility, and confidentiality of ePHI that your company collects against the standards set by HIPAA/HITECH. Our team will work alongside you to ensure you have a secure technology environment.

> *We care for your data.*
> *You care for your patients.*

Dynamic Quest serves a broad range of industries. We have special expertise in healthcare, but also offer Managed IT Services to businesses of all kinds.

DYNAMIC QUEST MANAGED IT SERVICES INCLUDE:

OVERALL CARE

- Periodic review of strategic plans
- Monthly ticket and open action item reports
- 24x7x365 Help Desk support
- Unlimited phone support
- Hardware acquisition through preferred partners
- Security scan

SERVER CARE

- Backup monitoring
- Service availability monitoring
- Anti-virus and anti-spyware management
- Patch management
- Operating system support
- Server troubleshooting

SECURITY ESSENTIALS

- **Advanced Malware Detection and Prevention**
- **Email Defense Spam Filtering**
- **Cloud Based DNS Filtering**
- **Security Awareness Training Foundation Edition**
- **Dark Web Monitoring**
- **Anti-Virus and Anti-Spyware Management**

NETWORK CARE

- Network monitoring and management
- Firewall management
- SAN management
- DNS and web hosting liaison
- Network performance tuning

WORKSTATION CARE

- Desktop optimization
- Anti-virus and anti-spyware management
- VPN client management
- Workstation troubleshooting
- Microsoft Office support

Call us today to find out more:
833-437-9378