ARE YOUR PEOPLE READY TO BE HACKED?

Healthcare organizations are a juicy target for hackers who want to steal sensitive data. Often, the way they get in is through employees who are tricked into providing access.

$5.40
the value of a stolen credit card on the dark web

$250
the value of a single patient's stolen healthcare data

HEALTHCARE RECORDS ARE VALUABLE

because they can be exploited in many ways, from submitting false claims to purchasing prescriptions and even receiving treatments.

	2018	2021
PATIENTS AFFECTED BY BREACHES	14.4M	44.91M
# OF BREACHES	369	679

HACKERS HAVE A LARGE AND GROWING ARSENAL OF WEAPONS

they use to attack healthcare systems. Once inside, they can lock you out and demand ransom, as well as embed themselves into operations and continually extract sensitive data — putting providers and the patients they care for at an ongoing and escalating risk.

SINGLE EXTORTION	Ransomware
DOUBLE EXTORTION	The above + data exfiltration
TRIPLE EXTORTION	All the above + Distributed Denial of Service
QUADRUPLE EXTORTION	All the above + your customers become the next targets

These **DATA BREACHES** are **COSTING HEALTHCARE PROVIDERS A LOT OF MONEY.**

AVERAGE COST OF BREACH

NON-HEALTHCARE COMPANIES
$4.2M
(PER INCIDENT)

HEALTHCARE ORGANIZATIONS
$9.23M
(PER INCIDENT)

HACKERS ARE PATIENT AND METHODICAL.

Once they get in, they will use that access to work their way into other areas. Hackers can be inside a system for two weeks or longer before they are ever detected — plenty of time to become embedded across many layers and very hard to expel.

HOW CAN A PROVIDER SHORE UP ITS DEFENSES?

IT MUST EDUCATE THE WEAKEST LINK IN THE SYSTEM — EMPLOYEES.

Every individual provides hackers multiple opportunities to gain access. The surfaces they leave vulnerable include unsecure or exposed passwords, outdated software, unprotected documents just to name a few. They also fall prey to increasingly sophisticated phishing and spear phishing campaigns through well-designed emails.

CYBERCRIMINALS HAVE MANY SOPHISTICATED METHODS OF ATTACK

AND ARE CONSTANTLY CREATING NEW ONES.

They are hard to recognize, which is why they are so successful.

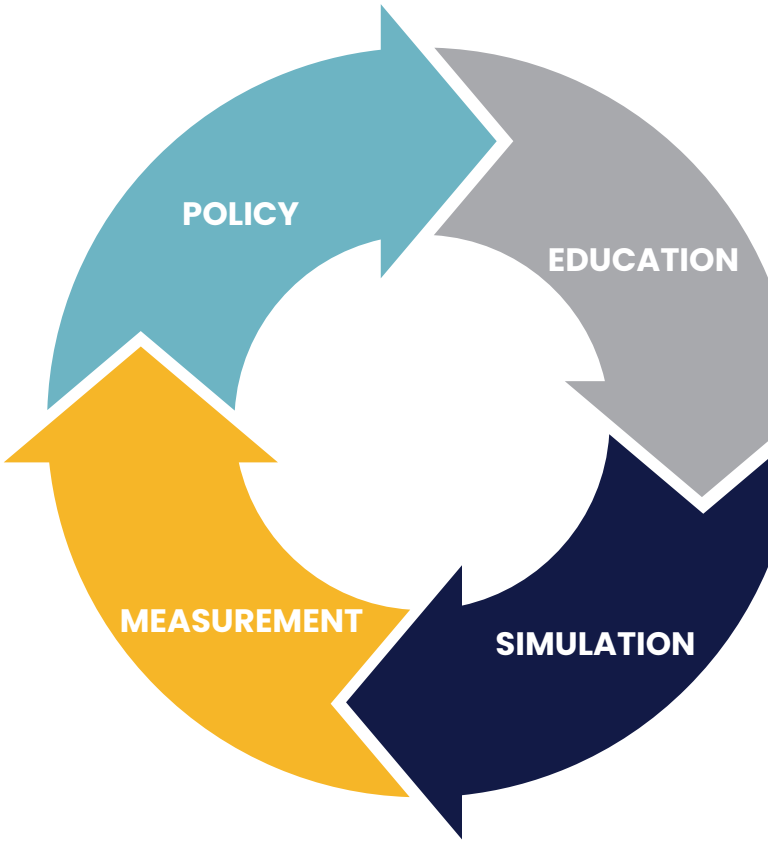
Constantly helping everyone get better is the way to increase everyone's vigilance against cyberattacks. People are the No. 1 target entry point for a cyberattack. Invest with this risk in mind, because giving people the tools and training to successfully ward off cyberattacks is time and money well spent.

USE THESE FIVE STEPS TO UP YOUR DEFENSES:

1. Define clear security policies and make them accessible
2. Establish procedures for managing attacks (including supporting the employee)
3. Develop an evolving infosec education program (hackers innovate rapidly)
4. Check for OSINT vulnerabilities (both company and exec team)
5. Pay attention to breach patterns, particularly those affecting your cohorts

AT CONCORD, WE RELY ON A REPEATING CYCLE OF EDUCATION AND TESTING TO MAKE SURE OUR EMPLOYEES DO NOT FALL PREY TO HACKERS.

Simulation is the single most effective way to measure how effective your training program is. Concord regularly simulates phishing and spear-phishing attacks, and measure how well we do in avoiding falling for the trap. Over time, people learn to scrutinize emails more closely, resulting in fewer successful simulated attacks.



CONCORD TECHNOLOGIES HELPS HEALTHCARE COMPANIES EXCHANGE DOCUMENTS AND OPTIMIZE CRITICAL WORKFLOWS MILLIONS OF TIMES A DAY.

Data privacy and security are critically important to us. There's no single solution to prevent attacks, so we apply security at all levels, and across all attack surfaces, a process known as Security In Depth. This means blocking attacks on each surface while also preventing an attack on one surface being used to then attack others.

Ready to learn more? Request a Demo.

CONCORD TECHNOLOGIES

2025 First Avenue Suite 800 • Seattle, WA 98121
+1 206-441-3346 • sales@concord.net • concord.net