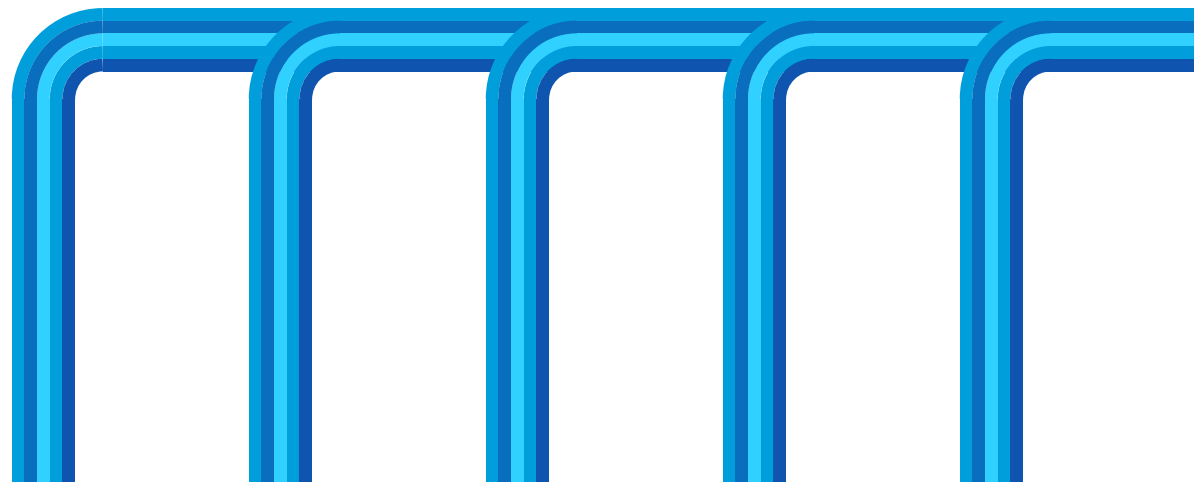


Healthcare and Cybersecurity

Helping protect the digital transformation



Digital technology is helping transform how healthcare is delivered. But it's also opening the industry to greater risk of cyberattacks.



Providers



Payers



Pharma



**Medical
Equipment
Manufacturers**



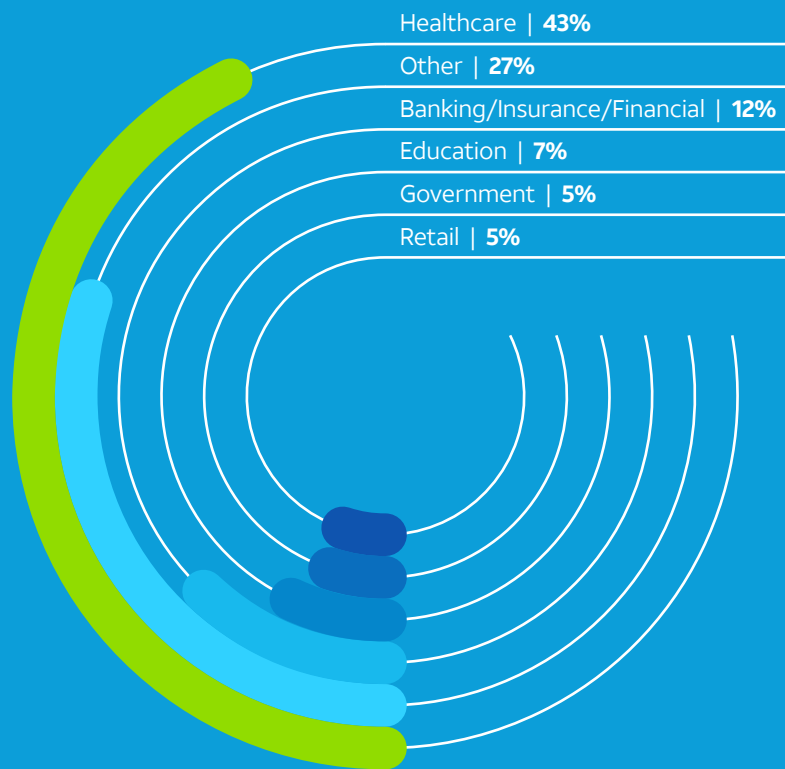
**Long-term
Care**

The healthcare industry is turning to digital innovation to improve the patient and member experience, enhance communication and collaboration, protect private and proprietary data, and deliver care to remotely located patients.

Yet, without a modern cybersecurity and compliance regimen aligned to digital transformation initiatives, healthcare organizations may be exposed to new and increased threats and vulnerabilities that can put organizational and patient data at risk.

Healthcare experienced more cyberattacks in 2019 than any other industry.*

Total cyberattack breaches by industry*



510

The number of healthcare data breaches of 500 or more records – a new record for a single year**

\$17.6B

Estimated cost of data breaches to the healthcare industry in 2019*

The impact of breaches extends far beyond the immediate cost, according to a survey of cross-industry C-suite executives.***

The top three business impacts from a security threat were:



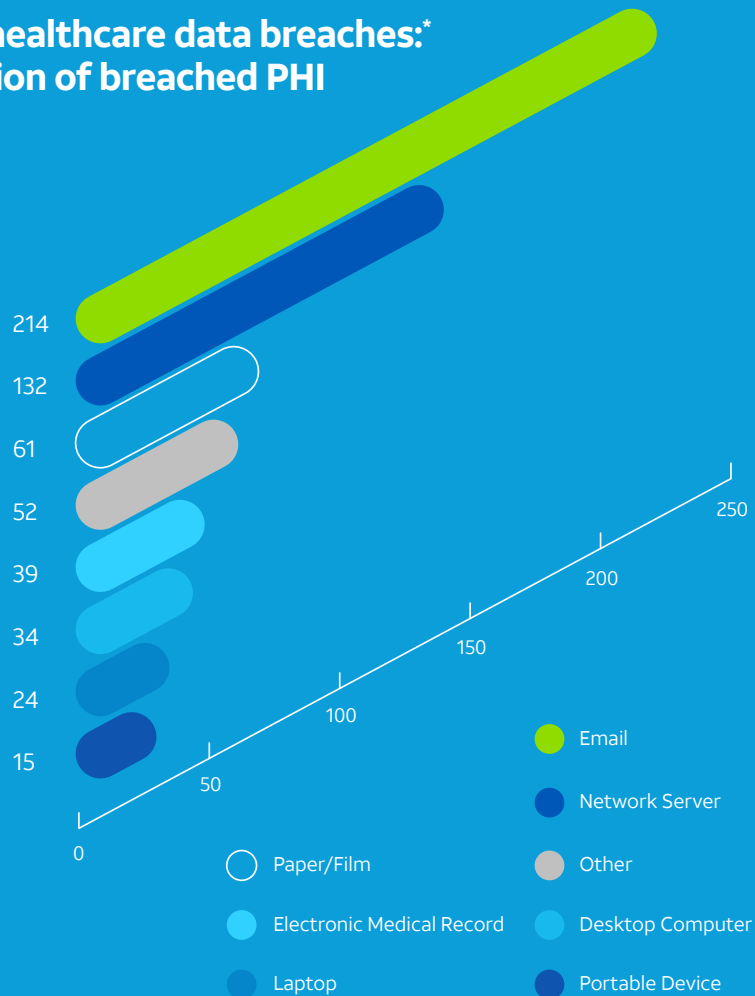
* <https://www.forgerock.com/resources/view/107130151/analyst-report/forgerock-consumer-identity-breach-report.pdf>

** <https://www.hipaajournal.com/2019-healthcare-data-breach-report>

*** C-SUITE PERSPECTIVES: From Defense to Offense – Executives Turn Information Security Into a Competitive Advantage, Radware

Email is the primary cyber threat healthcare organizations face.*

2019 healthcare data breaches: Location of breached PHI



214

The number of healthcare data breaches in 2019 from email*

300%

Increase in the number of impostor emails in the first quarter of 2019, compared to 1Q 2018**

55%

Portion of impostor emails with subject lines that included "payment", "request", "urgent", and related terms.**

77%

Portion of email attacks on healthcare companies that used malicious URLs.**

* <https://www.hipaajournal.com/2019-healthcare-data-breach-report/>

** <https://www.proofpoint.com/us/corporate-blog/post/new-healthcare-report-reveals-top-trends-people-centric-cyber-attacks>

COVID-19 is worsening the problem in 2020 by creating fear and uncertainty, and by disrupting work patterns.

“Scammers have specifically targeted physicians and other health professionals during the pandemic, and with the threat not going away any time soon, physicians must be extra vigilant...”*



American Medical Association advice for physicians:**



Practice/Office

Beware of phishing attacks



Medical devices

Ensure proper access controls, password protection and encryption



Phone and Tablet

Keep apps up to date and use encryption if possible



Home Network

Make sure your home network has the same protections as your practice



Home PC

Consider using VPN and/or a cloud-based service

* <https://www.ama-assn.org/practice-management/digital/online-scammers-target-doctors-amid-covid-19-how-stay-safe>

** <https://www.ama-assn.org/system/files/2020-04/cybersecurity-work-from-home-covid-19.pdf>

AT&T can help

As a leader in networking, connectivity, and cybersecurity, AT&T Business takes a holistic approach, with helpful advice to guide your digital and business transformation.

We can help make it faster and safer to improve the patient and member experience, enhance communication and collaboration, protect private and proprietary data, and deliver care to remotely located patients.

6

Six ways AT&T Cybersecurity can help your organization engage in a safe digital transformation:

1. Cyber risk strategy and planning
2. Mobile device security
3. Data security and compliance
4. Email and internet security
5. Cloud security
6. FirstNet[®], Built with AT&T

1. Cyber risk strategy and planning

How healthcare is transforming

Today's connected healthcare organizations are taking advantage of digital and network transformation to create modern patient experiences, drive cost efficiencies, and deliver innovation faster.

How cybersecurity fits in

Healthcare organizations must address cyber risk as part of the strategy, design, and delivery of any digital or network transformation initiative.

How AT&T Cybersecurity can help

AT&T Cybersecurity can provide [cybersecurity consulting](#) services tailored to help healthcare providers develop a strategy and plan managing for cyber risk and compliance.



How mature is your cybersecurity posture?
Compare it against your peers.

2. Mobile device security

How healthcare is transforming

In-home care providers and first responders use AT&T mobile data networks to access internal applications to send critical patient information in near real time from mobile devices.

How cybersecurity fits in

Healthcare organizations must provide mobile and remote employees with highly secure and encrypted access to internal systems and devices that are protected against emergent mobile-based attacks.

How AT&T Cybersecurity can help

AT&T Cybersecurity provides [endpoint security](#) for mobile devices and network security services like [AT&T Global Security Gateway](#) that helps to protect remote access to the web as well as internal applications and data.



3. Data security and compliance

How healthcare is transforming

Healthcare providers and payers transmit sensitive electronic personal health information (ePHI) across internal MPLS networks and share data with third-party suppliers, such as medical labs over the internet.

How cybersecurity fits in

Healthcare organizations must work to provide that ePHI is handled in accordance with regulatory requirements like HIPAA, HITRUST and the GDPR.

How AT&T Cybersecurity can help

AT&T Cybersecurity consulting helps healthcare organizations to accelerate and simplify compliance efforts with [regulatory and industry standards-based assessments](#).



4. Email and internet security

How healthcare is transforming

Clinicians, researchers, and other staff members require fast and reliable broadband internet connectivity and e-mail for daily work.

How cybersecurity fits in

Healthcare organizations should train staff to recognize web and email-based attacks like phishing and ransomware. By segmenting and monitoring the network and email, organizations can work to protect devices and sensitive data from web and email-based attacks.

How AT&T Cybersecurity can help

AT&T Cybersecurity can help on multiple fronts with [cybersecurity awareness training](#) for employees, [secure web and email gateways](#) and [managed firewall services](#).



5. Cloud security

How healthcare is transforming

Virtualized care solutions allow healthcare providers to connect with patients through public cloud infrastructure and applications to schedule appointments, provide medical advice, and share other personal health info.

How cybersecurity fits in

Healthcare organizations must protect web applications and patient data against cyber threats and fraud by establishing cloud security policies and continuously monitoring for threats against public cloud environments.

How AT&T Cybersecurity can help

AT&T Cybersecurity provides comprehensive cloud security solutions, including [cloud security assessment](#) services, [application layer security](#), and [threat detection and response](#) for multi-cloud and SaaS environments.



6. FirstNet: Highly secure connectivity healthcare providers can count on

Healthcare providers, including doctors, nurses and other staff members on the front line, are eligible for FirstNet. Built with AT&T. FirstNet is the only communications network [built with and for first responders](#).

FirstNet offers an available comprehensive suite of solutions that customers may deploy to address their applicable security requirements. The highly available, redundant, physically separate, dedicated core was designed to comply with many standard security regulations and needs, and it will continue to evolve to take advantage of new technologies and address emerging requirements.

FirstNet Security Operations Center

- Closely collaborates with AT&T security experts
- Monitors and manages FirstNet traffic 24x7x365
- Focuses solely on the security needs of FirstNet



Why AT&T Cybersecurity

AT&T Cybersecurity has a rich heritage in helping make it safer for organizations to innovate.

140+

years of managing and protecting a global network that carries more than

446

petabytes per day



8 global SOCs monitored

24/7/365

20M+

threat indicators submitted daily by

145k

security professionals as part of our OpenThreat Exchange™ community



25+

years of cybersecurity consulting practice with an average of

12

years experience



More than

2,000

cybersecurity specialists



Named a leader among managed security services providers (MSSPs) by Forrester and IDC*

Take action now



Discover

Review AT&T Cybersecurity solutions online.

[Explore](#)



Consider

Take our online cybersecurity risk self-assessment to see where your organization stands. Get immediate, customized results.

[Start](#)



Engage

Contact AT&T Cybersecurity today to get started.

[Contact us online](#)

Call AT&T: 888.613.6023

