5 risky security errors healthcare organizations make

Cybersecurity risks affect healthcare organizations everywhere. But did you know that some of the biggest vulnerabilities are hiding in plain sight? Organizations now view print security as one of their top security risks.[1]

1

Undersecuring patient data

By having a network connection to valuable personal health and financial patient data, all medical devices—including printers—are attractive targets for cybercrime.

Healthcare industry:
The most targeted sector by cybercriminals
according to Experian's Data Breach Resolution unit[2]

82%
have faced IoT cyberattacks
Healthcare organizations often face targeted Internet of Things (IoT) cyberattacks[3]

2-3X
more healthcare cyberattacks
took place in 2019 than the average amount for other industries[4]

2

Underestimating the costs of a breach

Healthcare security breaches cost both organizations and patients dearly. Along with financial costs, additional concerns include regulatory fines, civil actions, and loss of business.

Data breaches cost $17 billion
In 2019, breaches cost the healthcare industry more than $17 billion[5]

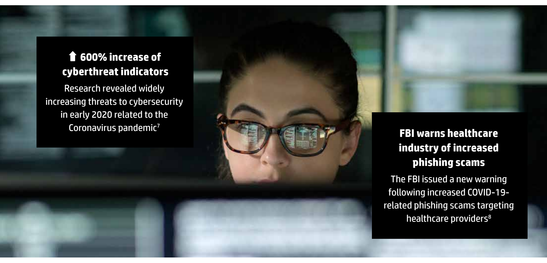
Healthcare is at higher risk
The healthcare industry accounted for 43% of all breaches in 2019[5]

$408 per compromised record
The healthcare industry has the highest per-capita data breach cost—nearly twice that of financial organizations[6]

3

Losing focus on cybersecurity due to the pandemic

Not only do healthcare networks continue to be vulnerable during the COVID-19 outbreak, but cybercriminals are increasingly focused on attacking the healthcare industry.



600% increase of cyberthreat indicators
Research revealed widely increasing threats to cybersecurity in early 2020 related to the Coronavirus pandemic[7]

FBI warns healthcare industry of increased phishing scams
The FBI issued a new warning following increased COVID-19-related phishing scams targeting healthcare providers[8]

4

Mismanaging printer security

Just one unprotected networked printer can result in a security breach. While PC security patches are closely watched, the reality is that most printer fleet security falls behind.

85%
fail to track print logs
Most organizations don't enable print logs to track login attempts and user access[9]

Anti-malware is missing from 69% of printers
Businesses tend not to have anti-malware running on their printers[9]

More than 55% of printers lack updated security
Of the 1.2 million printers tested by HP,[10] more than half were behind in security patches

5

Relying on printer configurations and firewall protection

Maintaining default settings leaves printer fleets at risk. With the sheer volume of data available—even behind a firewall—a single vulnerable device can threaten the entire network.

86%
of printers lack encryptions
Most organizations do not encrypt sensitive print data in motion[9]

Nearly
60%
of printers lack passwords
A significant portion of businesses fail to apply password policies on their printers[9]

50%
of printers lack security management
More than half of organizations use generic admin accounts to manage their printers[10]

It's time to increase your security—HP can help.

With HP, you can develop a security roadmap to mitigate risks, secure data, and better protect patients.

Find out how HP Healthcare solutions can help improve security for your entire organization.

LEARN MORE

1. Quocirca *Global Print Security Study*, Louella Fernandes, January 2019.
2. Experian *Data Breach Resolution*, "*2017 Data Breach Industry Forecast.*"
3. CyberMaxx, "*The future of cybersecurity in healthcare.*"
4. Cybercrime Magazine, "*15 cybersecurity statistics to diagnose the ailing healthcare industry,*" April 10, 2020.
5. ForgeRock *Consumer Identity Breach Report 2020.*
6. Ponemon *2018 Cost of a Data Breach Study* sponsored by IBM.
7. CSOPHIG, "*How Coronavirus is impacting cyberspace,*" March 2020.
8. HIPAA Journal, "*FBI issues flash alert about COVID-19 phishing scams targeting healthcare providers,*" April 22, 2020.
9. Common findings of risk assessments: Stats are calculated by HP using an internal database of results from assessments of 78 organizations. Assessments conducted by the HP Print Security Advisory team from July 2015 to February 2018.
10. 55% of printers behind in security patches: Based on data from 1.2 million printers, using the HP firmware security tool with 8505 Enterprises as of March 2019.

4AA7-9153ENUC, November 2020.