

mHEALTH SECURITY: STATS AND SOLUTIONS





WHAT IS mHEALTH?

mHealth (also written as m-health) is an abbreviation for mobile health, a term used for the practice of medicine and public health supported by mobile devices.

The term is most commonly used in reference to using mobile communication devices, such as mobile phones and tablets, for health services and information.

HOW DOES mHEALTH POSE SECURITY RISKS?



Vulnerabilities

Design flaws in hardware, software or connectivity; reliance on unreliable or unsecured vendors

Human error and human frailty

Hectic workplace, complex systems, serious temptations to breach privacy

Compliance failure

Improperly secured devices or data can lead to non-compliance, followed by fines or sanctions



PII

(Personally Identifiable Information)

- Name, address, DoB, SSN
- Payment card and bank data
- Medical records
- PHI and ePHI

CRIMINALS ARE LOOKING TO STEAL INFORMATION

Personally Identifiable Information (**PII**) is any valuable information ranging from paper records at admissions desk to full medical records on servers

There are multiple ways to monetize PII from stolen your mHealth projects

THOUSANDS OF PEOPLE HAVE SUFFERED FROM IDENTITY THEFT



Tens of **millions of records** have been exposed, and millions of dollars paid in fines.

Countless hours have been spent to solve problems caused by intruders and intrusive code.

And just imagine the negative **impact on patient care** when access to data is impeded, missing, or wrong.

THE RISK OF mHEALTH BY THE NUMBERS

Nearly

90%



of organizations use
at least one type of
mobile device
to engage patients

HIMSS Mobile Technology
Survey, 2015

THE SECURITY THREATS HEALTHCARE ORGANIZATIONS WORRY MOST ABOUT

1 **76%**

Employee-owned
mobile devices/BYOD

2 **72%**

Unsecure mobile devices

3 **69%**

Unsecure mobile apps

THE STATE OF CYBERSECURITY IN HEALTHCARE ORGANIZATIONS IN 2016

READ THE FULL REPORT NOW



- 1 Healthcare organizations experience at least one cyberattack a month on average.
- 2 47% of healthcare orgs experienced the loss or exposure of patient information over the past 12 months.
- 3 Patient medical records are cited by 81% of healthcare organizations as the most valuable records for hackers to steal.

Source: Ponemon Institute, 2016

THE STATE OF CYBERSECURITY IN HEALTHCARE ORGANIZATIONS IN 2016

(cont.)

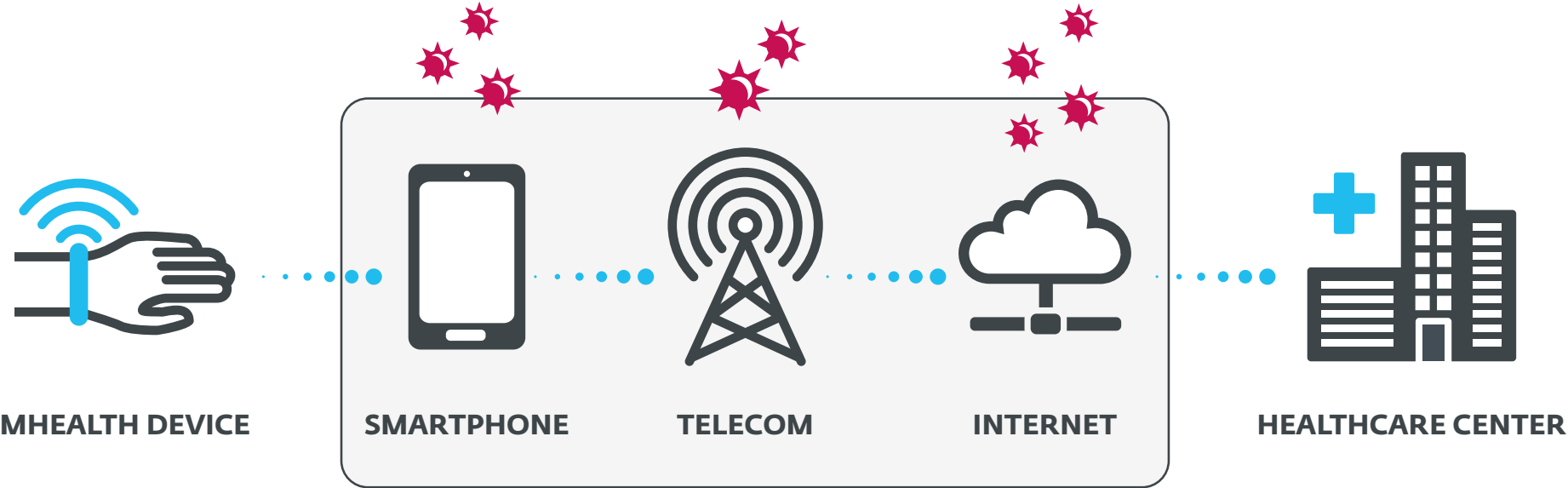



Only one-third of healthcare IT professionals say their organization's cybersecurity posture is "very effective."

Source: Ponemon Institute, 2016

ATTACK SURFACES

Personal health data travels through a long chain of communication devices. Each of them are vulnerable to attack on multiple levels.



 Possible attacks at communication points

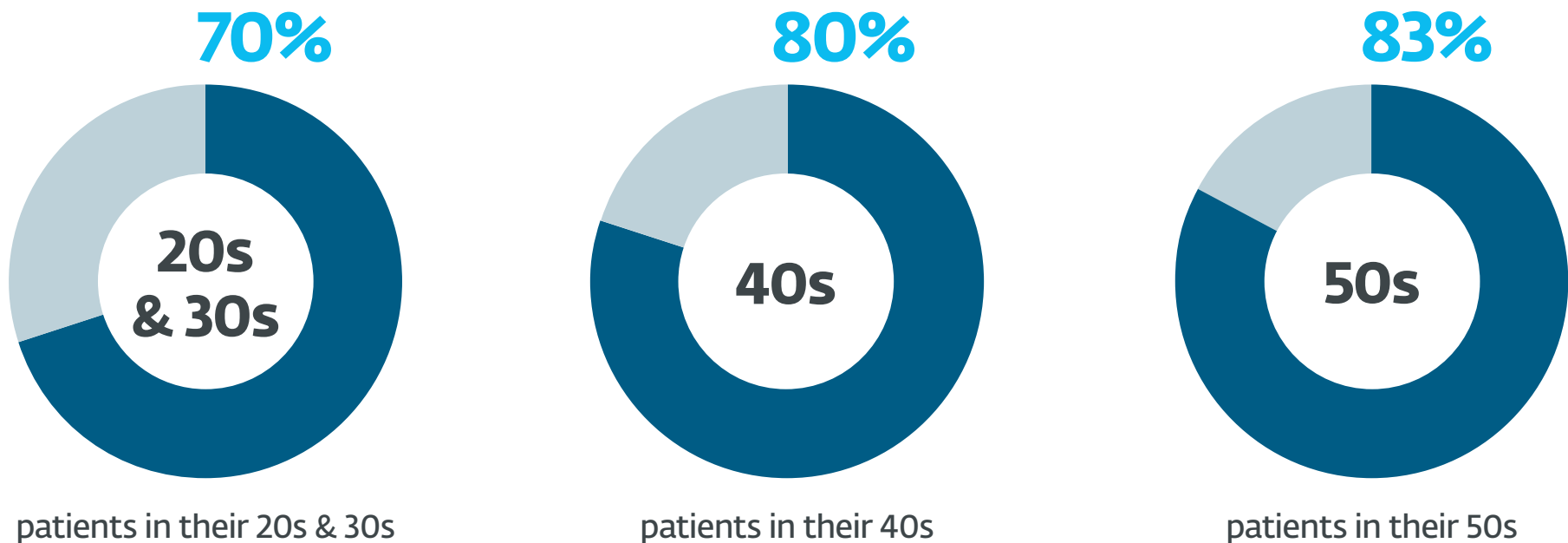
This is just an example. Many communication chains include even more vulnerabilities.

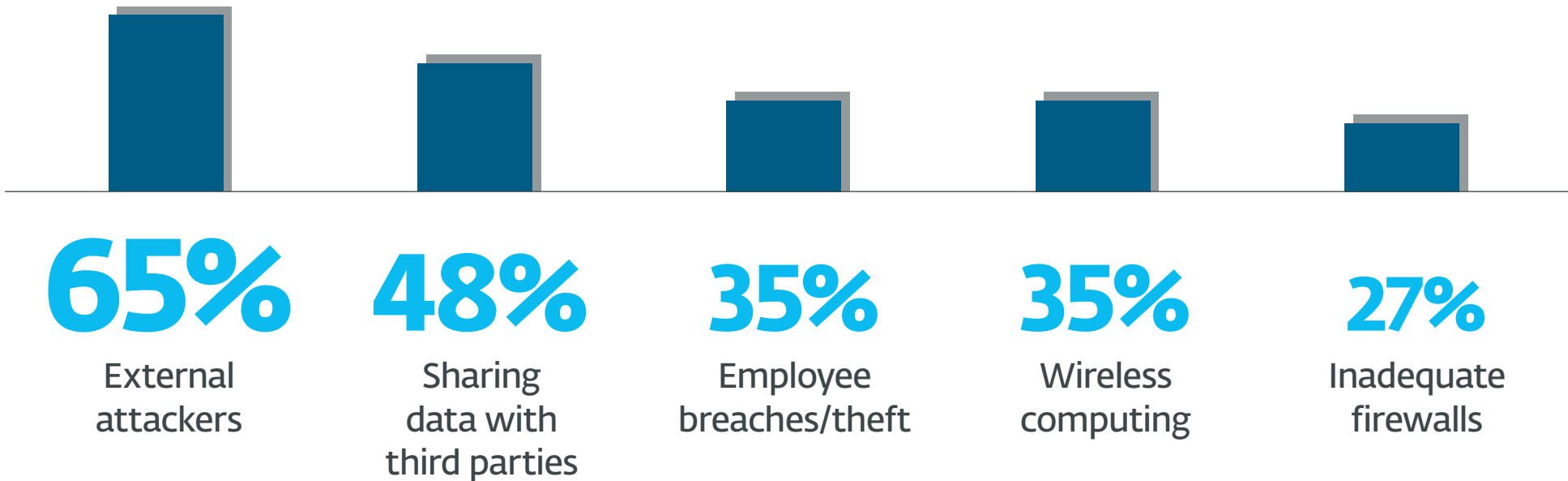


NEGATIVE IMPACT OF SECURITY BREACH

- Reputational damage
- Legal sanctions
- Unbudgeted costs
- Inaccurate data

PATIENTS ARE CONCERNED ABOUT THE SECURITY OF THEIR HEALTH DATA





GREATEST VULNERABILITIES IN DATA SECURITY

by KPMG "Health Care And Cyber Security"

Cyber Security Studies

-  [Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data](#)
-  [Health Care and Cyber Security](#)
-  [2015 Protected Health Information Data Breach Report](#)
-  [2015 HIMSS Cybersecurity Survey](#)

CYBERSECURITY THREAT TRENDS



A review of the many 2016 cybersecurity trend/threat predictors suggests a need to watch for the following:

- Denial of service attacks (as cover for system intrusion, malicious code insertion)
- Very targeted and/or realistic phishing attacks
- Malware attacks on, and/or spread by, servers
- Disgruntled employees and insecure partners

To strengthen your mHealth security posture, see step-by-step tips on the following slides: [Cybersecurity Roadmap](#) and [Four Pillars of Security](#).

mHEALTH CYBERSECURITY ROADMAP



STEP A: ASSESS

- Catalog your digital and physical assets
- Determine risks to your systems

STEP B: BUILD

- Write your security policy statement
- Add policies for specific assets as needed



STEP C: CHOOSE

- Describe the controls that will enforce policies
- List any cybersecurity products you may need

STEP E: EDUCATE

- Share policies with staff, vendors, clients
- Empower employees to report risky practices



STEP D: DEPLOY

- Test and evaluate as you deploy controls
- Identify and correct any problems

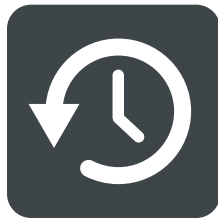


STEP F: FURTHER TEST

- Periodically test and adjust defenses
- Audit systems for changes & threats

FOLLOW THE 4 PILLARS OF PROTECTION

*Keep your devices, data and patients safe by implementing multiple layers of security:
ESET's Four Pillars of Protection. Each pillar is a vital element in mHealth security strategies.*



Backup

[SEE OUR SOLUTION](#)



Encryption

[SEE OUR SOLUTION](#)



Anti-malware

[SEE OUR SOLUTION](#)



**Strong
authentication**

[SEE OUR SOLUTION](#)



Backup



TECHNOLOGY ALLIANCE



STORAGECRAFT®

Backup Fast, Recover Faster

ESET provides the StorageCraft products to meet your backup and recovery needs.

StorageCraft offers a suite of software and services that helps you recover anytime, anywhere, from any situation. It works as an integral part of your overall business continuity plan by protecting your Windows® systems, applications and data from any disruption, large or small.

[READ MORE](#)



Encryption



TECHNOLOGY ALLIANCE

DESlock⁺
protect your data.

DESlock+ is a simple-to-use encryption application for companies large and small. Take advantage of the optimized setup that speeds up the time to adoption for admins. The client side requires minimal user interaction, increasing user compliance and the security of your company data.

[READ MORE](#)



Anti-malware



ENDPOINT SECURITY

Equipped with proactive malware defense and engineered to be light on your systems, endpoint security gives you the protection you need with fewer interruptions and false positives.

Plus, with ESET Remote Administrator, you can easily manage tens or thousands of Windows[®], Mac[®], or Linux[™] endpoints from one spot, eliminating the need for expensive management tools.

[READ MORE](#)



**Strong
authentication**



SECURE AUTHENTICATION

ESET Secure Authentication is a software-based, two-factor authentication system that protects against data breaches due to compromised passwords.

More flexible, cost effective, and comprehensive than hardware OTP tokens or appliances, ESET Secure Authentication is the simple way to strengthen passwords with no extra hardware needed.

[READ MORE](#)



ENJOY SAFER TECHNOLOGY®