You Can't Secure It If...

Assessing Cyber Security Risk
You Can't Secure It If...

Assessing Cyber Security Risk
Ensure Privacy & Security

Laws Requiring Protection of Health Information

Safety net provider organizations, not EHR vendors, bear responsibility for protecting the confidentiality, integrity, and availability of electronic health information in an EHR. The following are key concepts to understand as you address protection of health information.

**Privacy.** The HIPAA Privacy Rule protects the privacy of individually identifiable health information. Officially known as the “Standards for Privacy of Individually Identifiable Health Information,” HIPAA is designed to allow for disclosure of health information pertinent to patient care while safeguarding against unauthorized uses.

**Security.** The HIPAA Security Rule focuses specifically on electronic protected health information (ePHI). Its purpose is to set administrative, technical, and physical standards to protect electronic health information.
SECURITY BREACH NOTIFICATION LAWS

2/24/2017

Forty-seven states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or governmental entities to notify individuals of security breaches of information involving personally identifiable information.

Framework for Improving Critical Infrastructure Cybersecurity

Version 1.0

National Institute of Standards and Technology

February 12, 2014
Critical Infrastructure Sectors

There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

- Chemical
- Commercial Facilities
- Critical Manufacturing
- Communications
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Government Facilities
- Healthcare and Public Health
- Nuclear Reactors, Materials, and Waste
- Information Technology
- Transportation Systems
- Water and Wastewater Systems
## Critical Infrastructure Sectors

<table>
<thead>
<tr>
<th>Chemical</th>
<th>Financial Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commercial Facilities</td>
<td>Food &amp; Agriculture</td>
</tr>
<tr>
<td>Communications</td>
<td>Government Facilities</td>
</tr>
<tr>
<td>Critical Manufacturing</td>
<td>Healthcare &amp; Public Health</td>
</tr>
<tr>
<td>Dams</td>
<td>Information Technology</td>
</tr>
<tr>
<td>Defense Industrial Base</td>
<td>Nuclear Reactors/Materials/Waste</td>
</tr>
<tr>
<td>Emergency Services</td>
<td>Transportation</td>
</tr>
<tr>
<td>Energy</td>
<td>Water &amp; Wastewater Systems</td>
</tr>
</tbody>
</table>
Payment Card Industry (PCI) Data Security Standard
Assess Risk

Develop Protocols

Be Vigilant
"We fear that which we do not understand"
"We fear that which we do not understand"

except technology
Abandon previous assumptions
The CIS Critical Security Controls

for

Effective Cyber Defense

Version 6.1
The CIS Critical Security Controls
for
Effective Cyber Defense

Version 6.1

SANS 20
Assess Risk
SANS 20

1: Inventory of Authorized and Unauthorized Devices

2: Inventory of Authorized and Unauthorized Software
You Can't Secure It

if you don't

know it's there
**QR code**

This article is about the type of barcode. For the mathematical coding theory, see Quadratic residue code.

**QR code** (abbreviated from *Quick Response Code*) is the trademark for a type of *matrix barcode* (or two-dimensional *barcode*) first designed for the automotive industry in Japan. A barcode is a machine-readable optical label that contains information about the item to which it is attached. A QR code uses four standardized encoding modes (numeric, alphanumeric, byte/binary, and *kanji*) to efficiently store data; extensions may also be used.[1]

The QR code system became popular outside the automotive industry due to its fast readability and greater storage capacity compared to standard *UPC barcodes*. Applications include product tracking, item identification, time tracking, document management, and general marketing.[2]

https://en.wikipedia.org/wiki/QR_code
SANS 20

3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

4: Continuous Vulnerability Assessment and Remediation
You Can't Secure It

*if you don't*

know how it's configured
Computers are more capable than you think
and Every Thing is now a computer
SANS 20

5: Malware Defenses

6: Application Software Security
You Can't Secure It

if you don't

know how it works
SANS 20

7: Wireless Access Control
SANS 20

10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
SANS 20

8: Data Recovery Capability
Secured

Encrypted

Verified
SANS 20

9: Security Skills Assessment and Appropriate Training to Fill Gaps
You Can't Secure It if you don't know what they are doing with it
You Can't Secure It
if you don't control it
SANS 20

11: Limitation and Control of Network Ports, Protocols, and Services
You Can't Secure It

if you don't

know who has access
SANS 20

9: Security Skills Assessment and Appropriate Training to Fill Gaps
Security Awareness Training
Assessing Cyber Security Risk

presented by
Glenda R. Snodgrass

www.theneteffect.com   (251) 433-0196