

“Defending the Canoe Through Cyber Services”



27th Best Practices Forum
Friday March 10th 2017



Cybersecurity Updates Trends, and Precautions

Friday March 10th 2017

Edgardo Nieves – Morris Heights Health Center



A decorative vertical bar on the left side of the slide, featuring a dark blue background with glowing green and yellow binary code (0s and 1s) and numbers (0-9) arranged in a vertical column.

Introduction

WHO WE ARE

Since 1981, Morris Heights Health Center (MHHC) has had a record of distinction as the major provider of health care to Morris Heights and the surrounding Bronx areas. Born out of the local need for quality care in the area, MHHC is a non-profit organization funded by federal, state and foundation grants and private and corporate donations.

For over a quarter of a century, we've provided quality primary healthcare services to all members of the community, including the medically, socially and economically disadvantaged — from medical and dental services to counseling. Proudly, we've always been at the forefront in both the local and medical communities.

ABOUT MHHC

- **Morris Heights Health Center is recognized as a Level III Patient Centered Medical Home, a member of the Bronx Accountable Health Network and a pioneer ACO, as well as the Bronx Partners in Community Health PPS (NY State Delivery System Reform Incentive Payment - DSRIP).**
- **MHHC was the first federally funded community health center in New York City to be accredited by the Joint Commission.**
- **Morris Heights serves over 50,000 distinct patients annually**
- **MHHC has 10 main locations and is in 20 School Based Health Facilities**

SERVICES OFFERED

- Primary Care
- Pediatrics
- School Based Health
- Behavioral Health
- Dental
- Social Services
- Podiatry
- Pediatric Endocrinology
- Extended Care
- WIC Program
- HIV Care Services
- Hepatitis C
- Ophthalmology
- Cardiology
- OB/GYN
- X-Ray and Lab
- Gastroenterology
- Ear, Nose and Throat
- Physical Therapy
- Pulmonary
- AmbSurg (essure, colpo, LEEP)
- Telephone Triage



Current State of Healthcare as an FQHC specific to technology:

- Changing communication patterns (email, chat, texting, social media, video) Emergence of Social Media as a dominant web application.
- Software as a Service replacing institutionally owned infrastructure.
- Virtualization replacing one-computer-one-application model.
- Notion of mobile computing over desktop computing in many industries, including healthcare
- Intensified IT related regulatory environment (Audit, Credit Cards, Records Retention, Incident Notification, Grant funding requirements, etc.)
- Sophistication of IT security threats has led to increased number of more complex and focused exploits.
- Need and demand for interfaces/Interoperability growing exponentially...



Some common misconceptions about Cybersecurity

- Smaller organizations like FQHC's are not going to get attacked
- Compliance means security
- 'X' never gets attacked/infected (Apple hardware and software, devices like DVR's or Cameras)
- Software is the only way to address Cybersecurity
- It's all about keeping the criminals out
- Cybersecurity is an issue only for IT

Recent Settlements/Fines from HHS/OCR

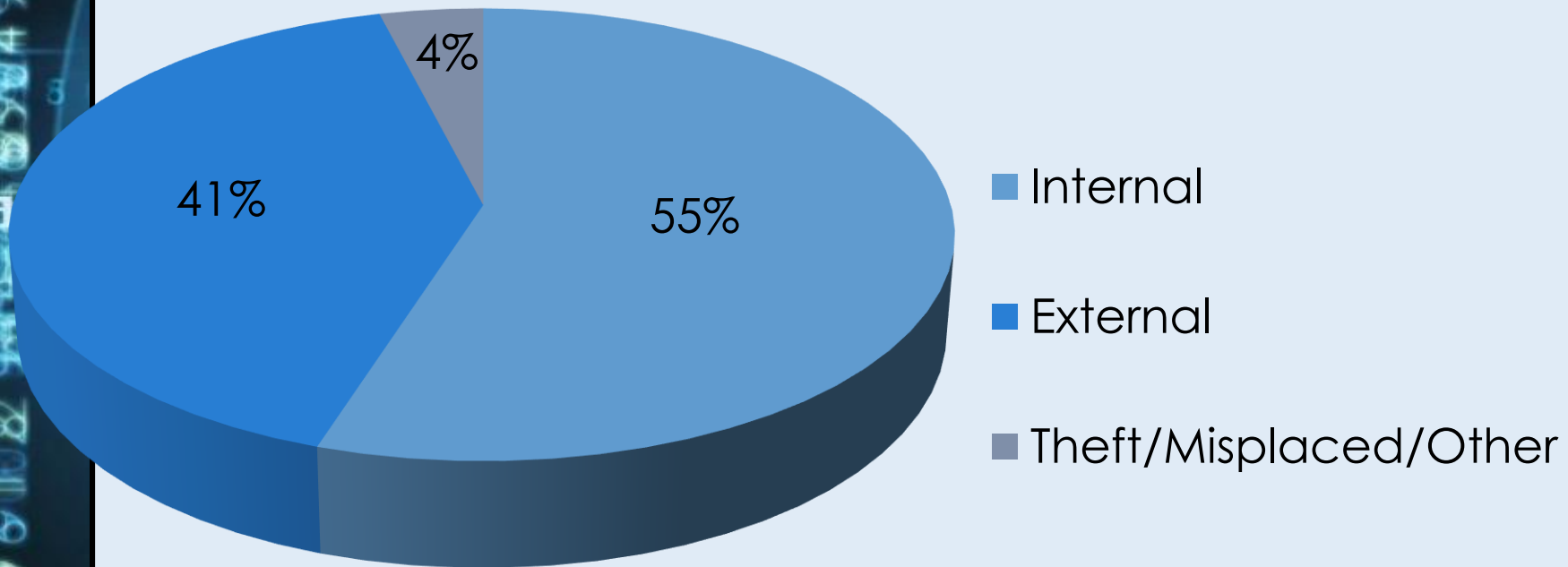
- **An Illinois based Health Network:** First ever HIPAA enforcement action for lack of timely breach notification - **\$475,000** in January 2017
- **Another Illinois based Network in Downers Grove:** The largest HIPAA payment involving one organization to-date **\$5,550,000**
- **A New York Based Medical Research Institute:** At the end of 2016, this entity agreed to pay **\$3,900,000** to settle claims it violated HIPAA
- **A New York City Based Hospital:** In this instance, the entity allowed film crews to film patients without their consent. The cost: **\$2,200,000**
- **A California Based Healthcare Provider:** The entity agreed to pay **\$2,140,000** after it was discovered they did not change the default settings on one of their servers, exposing over 30,000 patient records to the Internet

A decorative vertical bar on the left side of the slide, featuring a dark blue background with glowing green and yellow binary code (0s and 1s) and numbers (0-9) arranged in a vertical, slightly blurred pattern.

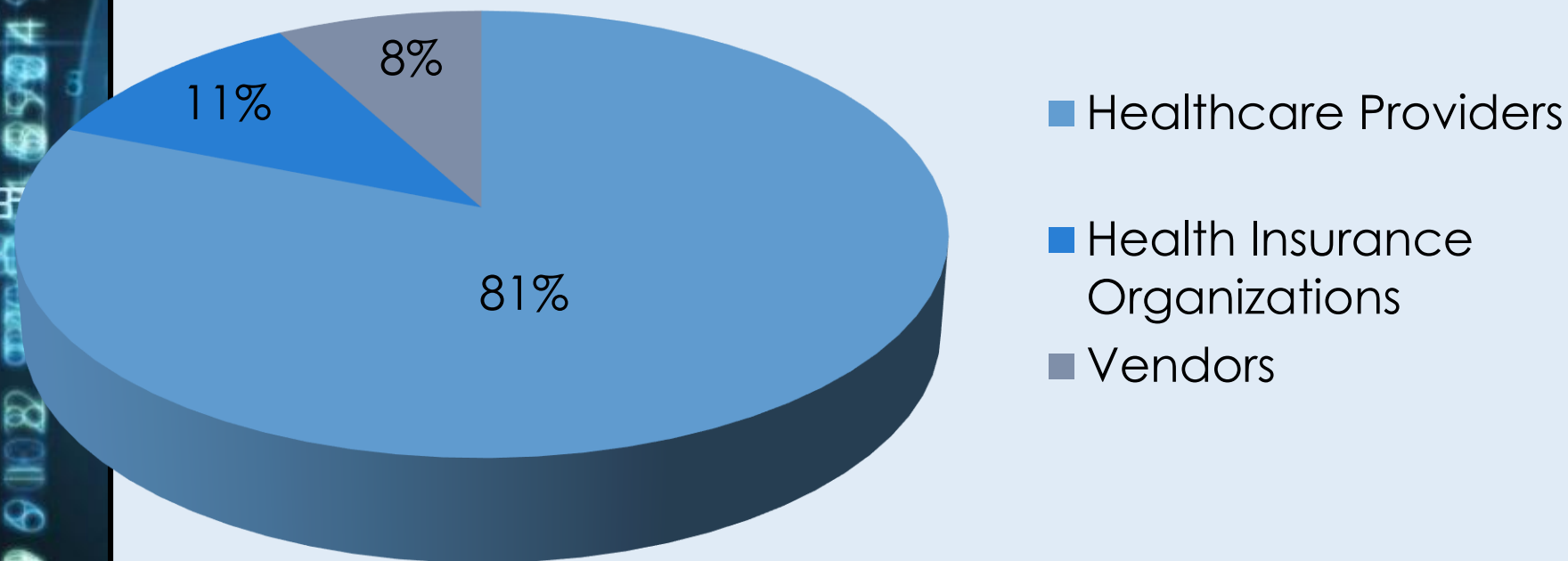
2017 Security Breach Data So Far

With 2016 seeing an average of a major breach per day reported in Healthcare, 2017 has continued this trend. Here is a breakdown of recent 2017 activity...

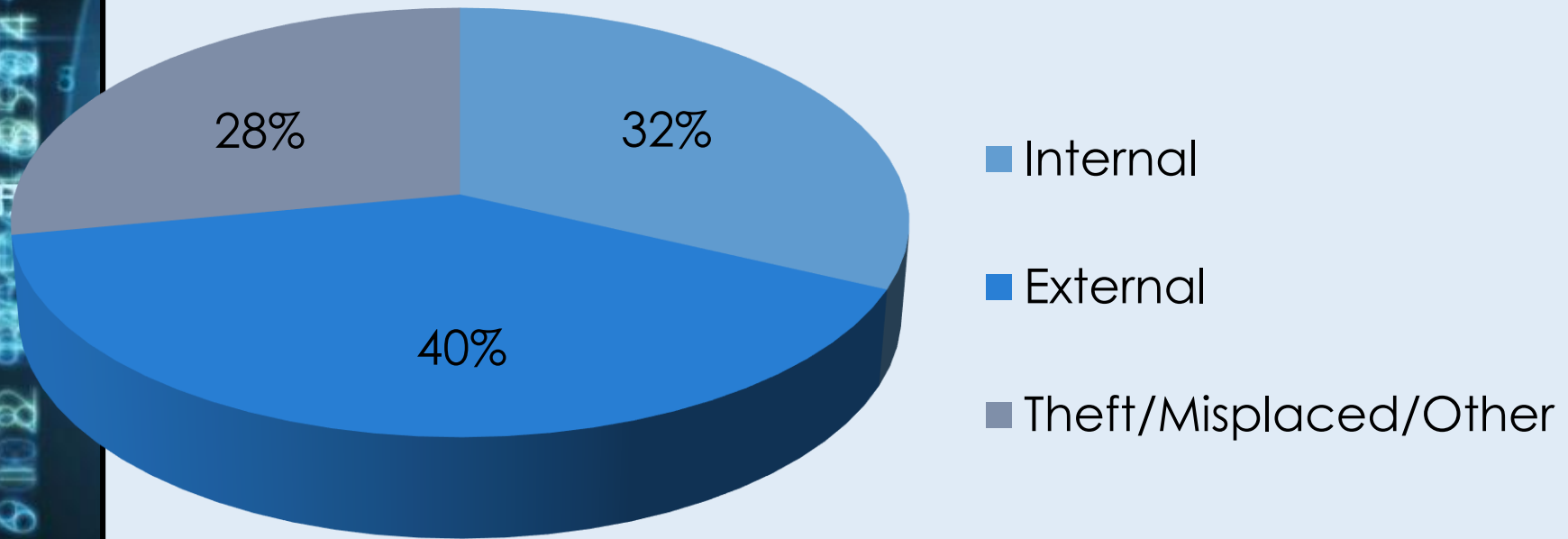
Percentage of Records by Incident for the beginning of 2017



Types of Organizations Reporting Breaches in 2017



Percentage of Types of Breach Incidents





Three realities for FQHC's and similar entities in 2017 regarding Cybersecurity

- There is not one current security approach or architecture that can “fix it all”
- Cybersecurity risks and attacks will come from an ever-growing list of sources (BYOD, Internet of Things, Cloud, etc)
- Your entity has been, and will continue to be, targeted...

Why target FQHC's?

Sold on major "Dark Web" sites like Python Market, Silk Road and AlphaBay, FQHC's EHR data, which has names, Social Security Numbers, Addresses etc. has clear value.

In 2017, this data is being used to do things such as:

- Obtain driver's licenses, passports, and other official government IDs
- Get prescription drugs
- Submit false insurance claims
- Open Credit Card accounts
- File tax returns to intercept refund checks



Internet of Things

The Internet of Things, an umbrella label for the growing number of mechanical and digital devices (and even living creatures) that are given unique identifiers and are able to send and/or receive data over a network, creates new opportunities for Cybersecurity Threats.

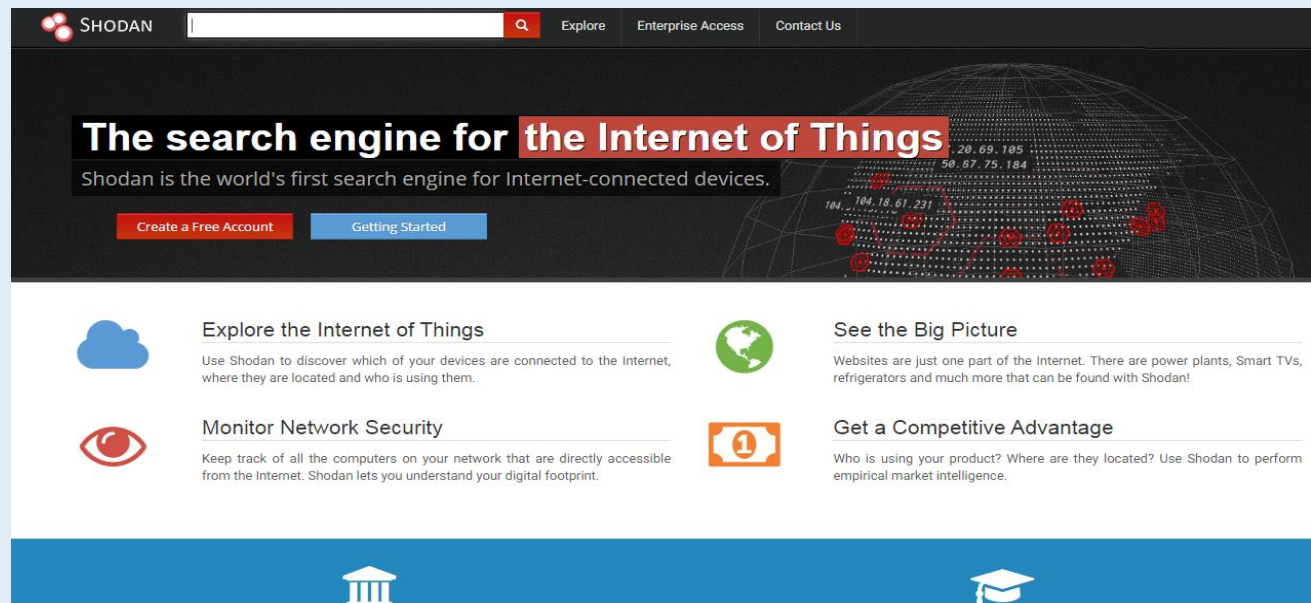
Many **Medical Devices** are considered a part of the IoT today, and that number is forecasted to only increase. Many of these devices are being rolled out faster than we are able to properly secure them.

In October of 2016, the world saw the largest DDoS attack on record to date. The attack was aimed at DynDNS services, and leveraged a BotNet built largely on Mirai Malware. This Malware targets devices such as Nest Thermostats, DVR's and other IoT devices that are poorly (or not at all) secured.

These IoT “zombified” devices were used to successfully bring down connectivity to crucial Internet connected services by creating a flood of junk traffic. Connectivity to crucial SaaS applications (such as hosted EHRs) was effected. Attacks of this nature demonstrate that disruption to business associates can easily cause disruption to Healthcare.

Shodan.io

- Shodan is a search engine that indexes Internet connected devices.
- The site lists devices hardware, IP and software information.
- Unsecured devices can be vulnerable to attack
- Cybercriminals can leverage BotNets to gather the same information
- Recent studies leveraging Shodan showed thousands of Healthcare devices (including some in FQHCs) were vulnerable to attack do to not being updated, being on unsupported software etc.



The screenshot shows the Shodan.io homepage. At the top is a navigation bar with the Shodan logo, a search bar, and links for 'Explore', 'Enterprise Access', and 'Contact Us'. The main header features the text 'The search engine for the Internet of Things' in a large, bold font, with 'the Internet of Things' highlighted in a red box. Below this is the tagline 'Shodan is the world's first search engine for Internet-connected devices.' and two buttons: 'Create a Free Account' and 'Getting Started'. The background of the header is a dark, wireframe globe with red dots representing connected devices. Below the header is a grid of four feature sections, each with an icon and a title. The first section has a cloud icon and is titled 'Explore the Internet of Things'. The second has a globe icon and is titled 'See the Big Picture'. The third has an eye icon and is titled 'Monitor Network Security'. The fourth has a coin icon and is titled 'Get a Competitive Advantage'. The footer is a solid blue bar with a white icon of a classical building on the left and a white icon of a graduation cap on the right.

SHODAN

Explore Enterprise Access Contact Us

The search engine for the Internet of Things

Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account Getting Started

Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

How can they exploit this?

www.defaultpassword.com/?action=dpl&char=a

default password list

Browse by character: **A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 0-9**

Displaying 152 passwords of total 1812 entrys.

Manufacturer	Product	Revision	Protocol	User	Password	Access	Validated
a	a	a	HTTP	9000	iloveyou	microsoft	No
a	pussy	1.0	Other	I Love	You!	difficult	No
aaa	aa	aaa	Multi	aaa	aaa	aaa	No
aaa	aaa	aaa	Multi	aaa	aaa	aaa	No
aaaawara	pagal	dewana	Multi	pappu	singh	hola	No
Accelerated Networks	DSL CPE and DSLAM		Telnet	sysadm	anicust		No
acer	acer	acer	Multi	acer	acer		No
actiontec	gt701-gw		Multi	admin	admin		No
Actiontec	GT701-WG		HTTP	admin	password	192.168.1.1	No
admin	admin	admin	Multi	admin	admin	admin	No
ADP	ADP Payroll HR database All		Multi	sysadmin	master	Admin	
Adtran	MX2800		Telnet	n/a	adtran		No
ADTRAN	NetVanta 7100		Multi	admin	password		No
Advanced Integration	PC BIOS		Console	n/a	Advance	Admin	No
ajEFTmqE	wMzNxfOvZggyGmLwppXlBCMjbUknucIZzaPru		Console	IOEJyIQU	UIELGbkHb	gBrqAKOokyLONbbp	No
Alcatel	4400		Multi	superusers	superuser	Superuser	No
Alcatel	Office 4200		Multi	n/a	1064	Admin	No
Alcatel	OmniPCX Office	4.1	Other	ftp_inst	pbxk1064	Installer	No
Alcatel	OmniPCX Office	4.1	Multi	ftp_admi	kilo1987	Admin	No
Alcatel	OmniPCX Office	4.1	Other	ftp_oper	help1954	Operator	No
Alcatel	OmniPCX Office	4.1	Other	ftp_admi	kilo1987	Admin	No
Alcatel	OmniPCX Office	4.1	Other	ftp_nmc	tuxalize	NMC	No
Alcatel	OmniStack 6024		Telnet	admin	switch	Admin	No
Alcatel	PBX	4400	Port 2533	dhs3pms	dhs3pms	unknown	Yes
Alcatel	PBX	4400	Port 2533	halt	tlah	unknown	Yes
Alcatel	PBX	4400	Port 2533	dhs3mt	dhs3mt	unknown	Yes
Alcatel	PBX	4400	Port 2533	client	client	unknown	Yes
Alcatel	PBX	4400	Port 2533	install	llatsni	unknown	Yes
Alcatel	PBX	4400	Port 2533	kermi	kermi	unknown	Yes
Alcatel	PBX	4400	Port 2533	at4400	at4400	unknown	Yes
Alcatel	PBX	4400	Port 2533	root	letacla	unknown	Yes
Alcatel	PBX	4400	Port 2533	mtch	mtch	unknown	Yes
Alcatel	PBX	4400	Port 2533	mtcl	mtcl	unknown	Yes
Alcatel	PBX	4400	Port 2533	adffexc	adffexc	unknown	Yes
Alcatel Thomson	SpeedTouch580	4.3.19	HTTP	admin	admin		No
allan	ass		Multi	tool	face	tool	No
allied	CJ8MO E-U		Telnet	(none)	(none)	Admin	No
Allied	Telesyn		Multi	secoff	secoff	Admin	No
Allied	Telesyn		Multi	manager	friend	Admin	No
Allied Telesyn	All	All	Telnet	manager	friend	Admin	No
Allied Telesyn	Generic Switch/Router		Multi	manager	friend	Admin	No
Allied Telesyn	Switch	AT-8124XL 1.0.3	Multi	admin	(none)	Admin	Yes

Security Staffing

- Most industries are finding it hard to recruit and retain qualified Cybersecurity personnel, and healthcare is no different. With hundreds of thousands of positions unfilled today, this gap is expected to grow to over a million by 2020.
- Some Healthcare Providers have turned to third parties to help address their Cybersecurity staffing needs. As such, we are likely to see an increase in things like the notion of the “virtual” CCO (Chief Cybersecurity Officer), managed security services, SaaS and cloud services to help meet the short term gap in staffing.
- 2016 saw many more Healthcare Providers move to third parties for network, server and application monitoring and event correlation through Security Information and Event Management (SIEM). This trend will continue as we come to grips with the fact that internal, often sample-based auditing is not enough to keep up with today’s ever more sophisticated Cybercriminals and their techniques.

A Framework for Staffing

Late last year, the U.S. Commerce Department's NIST (National Institute of Standards and Technology) released a framework to help organizations "more effectively identify, recruit, develop and maintain cybersecurity talent". The framework, known as the NICE Cybersecurity Workforce Framework or, NCWF for short, gives employer organizations a structure to describe and group cybersecurity tasks and help insure they are building proper staffing into their plans to protect their infrastructure and data.

In many industries, and especially Healthcare, Cybersecurity is really in its infancy stage. In early 2017, job titles and roles vary wildly from Healthcare organization to organization. The NCWF brings a framework to help define what roles and titles are needed in a consistent way.

One good example of the value of this framework is helping organizations understand that many Cybersecurity tasks are actually performed by non-IT staff members. Often, Healthcare providers' legal team, internal auditors and even purchasing agents are best suited for certain aspects of Cybersecurity. Indeed, an effective security-focused person may have a different psychological profile than what is often expected to be found in your "typical" IT worker.



Framework Categories

Analyze - Specialty areas responsible for highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.

Collect and Operate - Specialty areas responsible for specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.

Investigate - Specialty areas responsible for the investigation of cyber events and/or crimes of IT systems, networks, and digital evidence.

Operate and Maintain - Specialty areas responsible for providing the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security.

Framework Categories (cont.)

Oversight and Development - Specialty areas providing leadership, management, direction, and/or development and advocacy so that all individuals and the organization may effectively conduct cybersecurity work.

Protect and Defend - Specialty areas responsible for the identification, analysis, and mitigation of threats to internal IT systems or networks.

Securely Provision

Specialty areas concerned with conceptualizing, designing, and building secure IT systems, with responsibility for some aspect of the systems' development.

Cyberseek.org



[About](#) [Interactive map](#) [Career pathway](#) [Who this tool is for](#) [Project partners](#)

About this tool

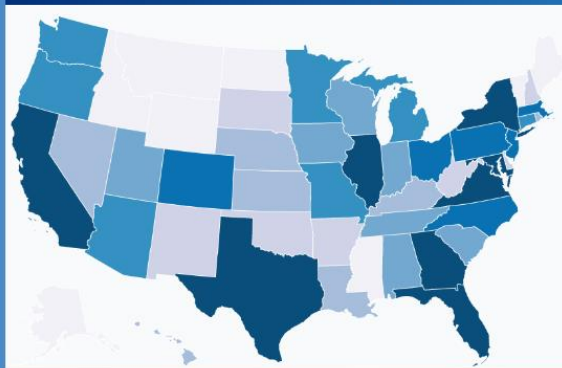
Cybersecurity workers protect our most important and private information, from bank accounts to sensitive military communications. However, there is a dangerous shortage of cybersecurity workers in the United States that puts our digital privacy and infrastructure at risk.

Every year in the U.S. there are 128,000 openings for Information Security Analysts, but only 88,000 workers currently employed in those positions – a talent shortfall of 40,000 workers for cybersecurity's largest job.

There are 220,000 additional openings requesting cybersecurity-related skills, and employers are struggling to find workers who possess them. Jobs requesting cloud security skills, for example, remain open 96 days on average – longer than any other IT skill.

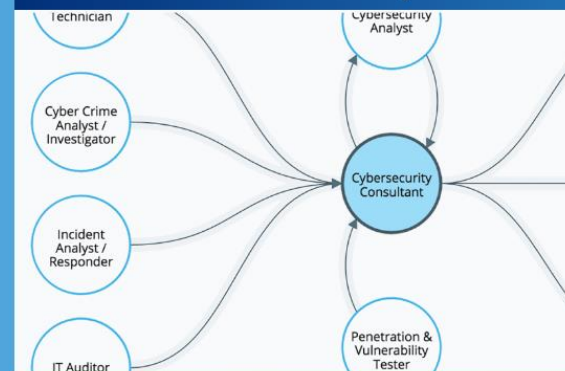
To help close the cybersecurity skills gap, CyberSeek provides detailed, actionable data about supply and demand in the cybersecurity job market.

Interactive Map



A heat map of cybersecurity supply and demand

Career Pathway



An interactive career pathway showing common roles within cybersecurity and transition opportunities between them

Cyberseek.org

Cybersecurity Supply/Demand Heat Map

Cybersecurity talent gaps exist across the country. Closing these gaps requires detailed knowledge of the cybersecurity workforce in your region. This interactive heat map provides a granular snapshot of demand and supply data for cybersecurity jobs at the state and metro area levels, and can be used to grasp the challenges and opportunities facing your local cybersecurity workforce.

Share

States

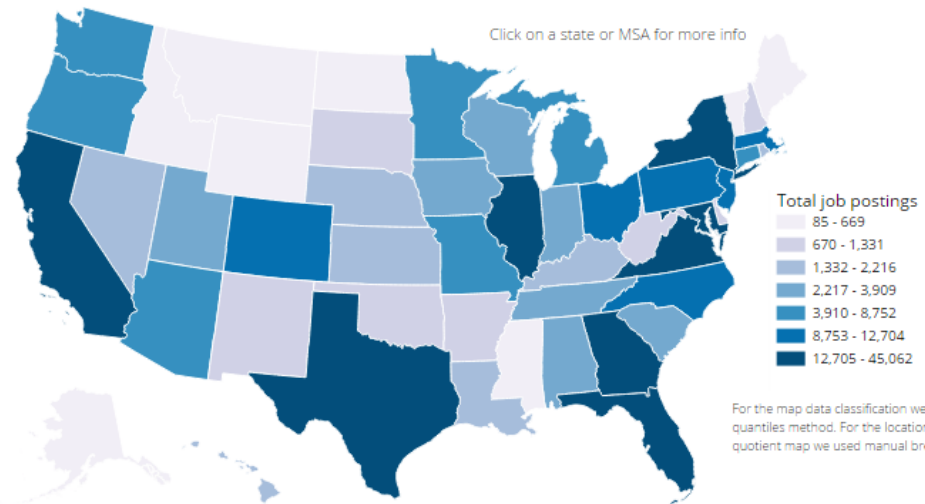
Metro Areas

Total job openings

Search State



Click on a state or MSA for more info



For the map data classification we used quantiles method. For the location quotient map we used manual breaks.

National level

TOTAL CYBERSECURITY JOB OPENINGS ⓘ

348,975

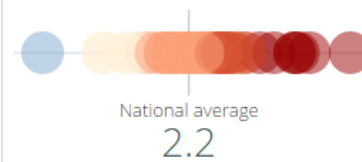
TOTAL EMPLOYED CYBERSECURITY WORKFORCE

778,402

SUPPLY OF CYBERSECURITY WORKERS ⓘ

Very Low

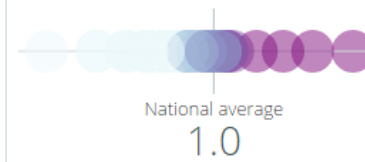
CYBERSECURITY WORKFORCE SUPPLY/DEMAND RATIO



GEOGRAPHIC CONCENTRATION ⓘ

Average

LOCATION QUOTIENT

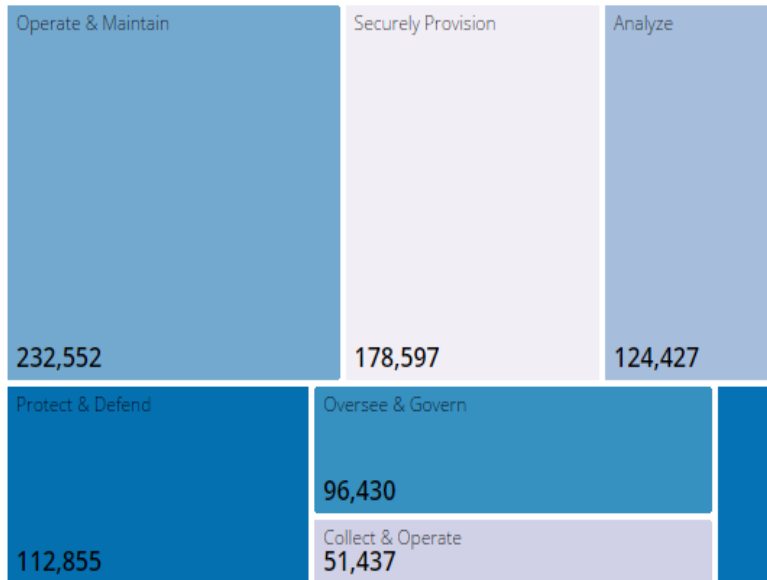


TOP CYBERSECURITY JOB TITLES ⓘ

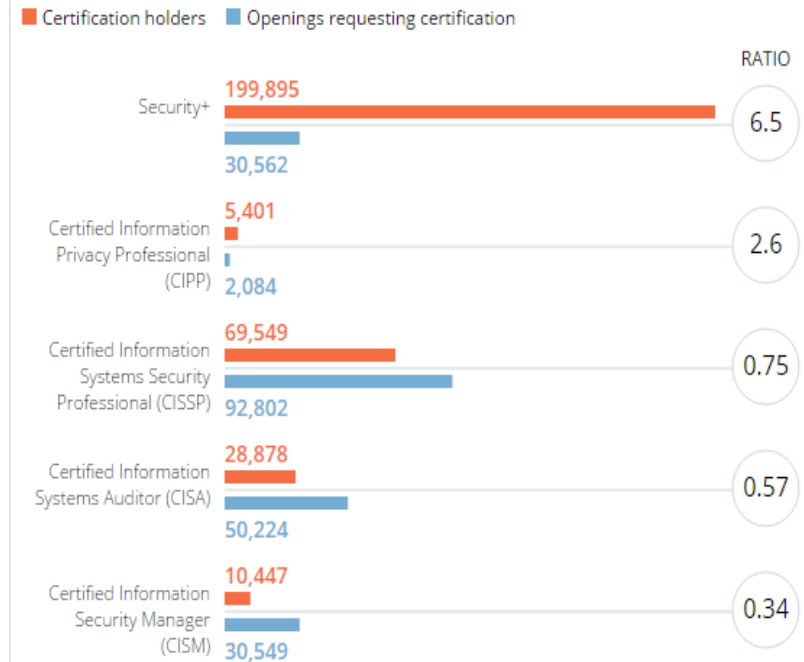
- Cyber Security Analyst / Specialist
- Cyber Security Engineer
- Auditor
- Network Engineer / Architect
- Software Developer / Engineer
- Systems Engineer
- Systems Administrator
- Information Assurance Engineer / Analyst
- Risk Manager / Analyst

Cyberseek.org

POSTINGS BY NICE CYBERSECURITY WORKFORCE FRAMEWORK CATEGORY



CERTIFICATION HOLDERS / OPENINGS REQUESTING CERTIFICATION



A decorative vertical bar on the left side of the slide, featuring a dark blue background with glowing green and yellow binary code (0s and 1s) and numbers (0-9) arranged in a vertical, slightly blurred pattern.

Technology is not the only solution, but it's still **REALLY** important

- While the “people” side of cybersecurity is crucial, technology is still key.
- Vendors (such as Palo Alto, Cisco) work everyday to innovate and redefine the way we secure our networks.
- Crowdstrike, Carbon Black and Symantec are releasing next-generation end-point security.
- Vendors like Rapid7 have been forwarding the notion of cloud security by enhancing auditing, and detecting undefined/unidentified threats.
- What this is all culminating in is actual **machine learning** being used in the battle for Cybersecurity.

Ransomware

Ransomware has come into it's own in 2016. The onslaught of this form of extortion is likely to continue to increase in 2017, especially in Healthcare. A Health Center in California at the end of 2016 is a recent example of the realities of this Cybersecurity threat.

Ransomware has become so pervasive, that the Office of Civil Rights released guidance in the third quarter of 2016 to help Healthcare Providers better address such attacks.

According to the guidance "On average, there have been 4,000 daily ransomware attacks since early 2016 (a 300% increase over the 1,000 daily ransomware attacks reported in 2015)"

nomoreransom.org

<https://www.nomoreransom.org>

NO MORE RANSOM!

★ English ▾

[Crypto Sheriff](#)

[Ransomware: Q&A](#)

[Prevention Advice](#)

[Decryption Tools](#)

[Report a Crime](#)

[Partners](#)

[About the Project](#)

**NEED HELP unlocking your digital life
without paying your attackers*?**

YES

NO

Ransomware is malware that locks your computer and mobile devices or encrypts your electronic files. When this happens, you can't get to the data unless you pay a ransom. However this is not guaranteed and you should never pay!



GOOD NEWS

Prevention is possible. Following simple cyber security advice can help you to avoid becoming a victim of ransomware.



BAD NEWS

Unfortunately, in many cases, once the ransomware has been released into your device there is little you can do unless you have a backup or security software in place.



GOOD NEWS

Nevertheless, it is sometimes possible to help infected users to regain access to their encrypted files or locked systems, without having to pay. We have created a repository of keys and applications that can decrypt data locked by different types of ransomware.

Phishing





Phishing

- In 2017, the route most attackers will take to get to you will not be through your firewall. They are going to use your own staff to gain access to your systems via the social engineering attack commonly known as Phishing
- The attack begins with an email, more and more commonly spoofing someone the victim knows, with a link connected to a malicious payload of code
- In recent Phishing attach trials in healthcare, over a frightening 50% click-through rate was recorded
- Having a process, security infrastructure and education platform around Phishing is **crucial**

Phishing

In late 2016, HHS released a warning that a scam emailing sent to covered entities sent on HHS letterhead was a phishing attack. It tricked people into clicking on a link under the guise of being informed they were about to be included in the HIPAA Privacy, Security, and Breach Notification Rules Audit Program.



Trends for the rest of 2017 and Beyond

- FQHCs (as with most Healthcare organization types) will have increasing pressure to contain cost and shift from making larger, long term investments (CapEx) to relying on external service providers in more pay-as-you-go agreements (OpEx). The impact on planning for Cybersecurity budgeting must reflect this change.
- Cloud adoption amongst FQHCs will continue to expand in 2017 and beyond, and such a trend has direct implications for Cybersecurity. Spending on Cloud services is expected to double to 10 Billion dollars in Healthcare by 2020.
- Related, the notion of BYOD is well documented and discussed, and while still a definite risk, the trend of **Shadow IT**, with its roots often in staff members bringing their “own cloud” to help them share data, be more efficient with external apps, etc, will bring more Cybersecurity risks to the fore for FQHCs, especially as we seek to do *more with less* as FQHCs collectively.
- Overall, IT departments specifically will be charged with supporting and securing existing infrastructure, while at the same time enabling innovation, and responding to an ever-evolving cyber landscape of threats aimed at healthcare.

Some things you can do now

- Check on usage of Dropbox, Google drive, etc.
- Go on a “Phishing trip” of your own!
- **Reset everyone's passwords!** Be sure you enforce complex passwords. Also, do not give any special-case exceptions (Sorry CEOs and other executives)! Two-factor authentication is crucial.
- **Remember, your people are your biggest Cybersecurity threat.** A well maintained and enforced Cybersecurity education and execution program is key.
- **Put your PC's on lockdown.** Block all their USB ports. Make sure only authorized users have access to configure your client machines. **ENCRYPT ALL LAPTOPS.** We've all heard the trope “If it moves – kill it”. The new saying in healthcare is “if it moves, encrypt it”. Also, can you remote-wipe your mobile devices?
- **Make a list of all your partners, interfaces, Business Associates.** Do you know where you patients' data is going? Is it protected? Ask for a copy of their latest risk assessment.

[illegible]

Questions ?