ABOUT MHCC

- Independent regulatory agency with a mission to plan for health system needs, promote informed decision-making, increase accountability, and improve access to health care

- Facilitate collaboration among health care consumers, payers, and providers to achieve widespread adoption and optimized use of health IT

- Increase timely access to accurate health information

- Advance health IT statewide by promoting optimal adoption and use, identifying challenges, and raising awareness through outreach activities

- Balance the need for information sharing with consumers’ desire for strong privacy and security protections
AGENDA

- Trends in health care data breaches
- Cybersecurity Self-Assessment Readiness Tool
- Buy Maryland Cybersecurity (BMC) Tax Credit
- Practical Steps to Improve Cybersecurity
- Q&A
Exponential growth in hacking/IT related breaches in Maryland and the nation; accounting for the majority of records compromised

- Ransomware, the most common type of malware, represents a quarter of hacking/ IT breaches nationally

Health care providers in all states increasingly being targeted

- In 2016, Maryland was one of fifteen states where providers accounted for all reported breaches

High profile incidents like the Equifax breach and WannaCry virus highlight the importance of cybersecurity basics

Evolving cyber threats require more focus on changing end-user behavior to reduce risk of a breach

Note: MHCC analyzed data on health care data breaches affecting >500 individual. Data was obtain from the Department of Health and Human Services, Office for Civil Rights Online Portal.
Available to health care providers to help assess cybersecurity readiness and identify potential gaps that may create risk

Questions align with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), a set of standards, best practices, and recommendations for improving cybersecurity

Includes a series of self-evaluation statements grouped by people, processes, policies, and technology

Results can help inform your practice about the adequacy of existing cyber protections

PRACTICAL STEPS TO IMPROVE CYBERSECURITY

KRISH BHATNAGAR, CISSP, PMP
HEAD, SECURITY SERVICES, MOKXA TECHNOLOGIES
Back to Basics: Practical Ways to Improve Cybersecurity at Your Practice

Collaborate | Innovate | Solutions
AGENDA

- State of Cybersecurity for SMBs
- Cybersecurity challenges for small practices
- Cost of breaches
- Top 5 security steps for small business
- Understanding and managing security risk
STATE OF CYBERSECURITY FOR SMBs

60% of small businesses say attacks are becoming more severe and more sophisticated.

Ponemon 2017 State of Cybersecurity in SMBs

58% of malware attack victims are categorized as small businesses.

Verizon 2018 DBIR

92.4% of malware is delivered via email.

Verizon 2018 DBIR

In 2017, cyber attacks cost small and medium-sized businesses an average of $2,235,000.

Ponemon 2017 State of Cybersecurity in SMBs
CHALLENGES FOR SMALL PRACTICES

- Lack of resources & funding
- Lack of technical expertise
- Strict regulatory requirements
- Attack could shut down business

NUMBER OF RECORDS BREACHED BY INDUSTRY

- Healthcare: 34%
- Government: 15%
- Technology: 8%
- Retail: 6%
- Education: 5%
- Other: 8%
- Financial: 1%

Image: Gemalto
# COST OF BREACHES

## Penalties

*HIPAA Violations*

1. Max Penalty - $50K per violation
2. Annual Max - $1.5M

*Criminal penalties*

1. Knowingly buy/sell - $50K & 1Y
2. False pretenses - $100K & 5Y
3. Intent to sell - $250K & 5Y

## Cost Components of Data Breach

1. Investigation
2. Remediation
3. Notification
4. Identity theft repair & credit monitoring
5. Regulatory fines
6. Interrupted business operations
7. Loss of business
8. Class-action law suited
TOP 5 SECURITY STEPS FOR SMALL PRACTICES

1. Secure your employees
2. Control access
3. Secure enterprise data
4. Manage network & devices
5. Secure your applications
1. SECURE YOUR EMPLOYEES

- Train employees on cybersecurity
- Avoid email ‘phishing’
- Do not forget physical security
2. CONTROL ACCESS

- Ensure individual access
- Ensure role based access
- Add strong authentication
3. SECURE ENTERPRISE DATA

- Ensure data security in motion & at rest
- Apply encryption
- Maintain data backups
4. MANAGE NETWORK & DEVICES

- Deploy Firewalls & malware protection
- Patch systems regularly
- Control wireless access
5. SECURE YOUR APPLICATIONS

- Control input parameters
- Secure websites
- Use Public Key Infrastructure
MANAGING SECURITY RISK

- Understanding and managing security risk
  - Assess security risks first and then build plan
  - Determine likelihood and impact
  - Determine ‘crown jewels’
  - Understand liabilities if outsourcing

- Security Model for small business
  - Tailor plan to identified risks
  - Plan for ongoing set of activities
  - Implement formal security policies
  - Utilize cash and tax incentives
  - Consider cyber insurance
THANK YOU

Contact Information:

Krish Bhatnagar, CISSP, PMP
Head, Security Solutions
301-343-6727
kbhatnagar@mokxa.com
BUY MARYLAND CYBERSECURITY (BMC) TAX CREDIT

LAUREN SATYSHUR
HEALTH IT PROGRAM MANAGER, OFFICE OF CYBERSECURITY & AEROSPACE, MARYLAND DEPARTMENT OF COMMERCE
Cyber OPEN FOR BUSINESS
Maryland’s Cybersecurity Innovation

**Unique Assets**
- 115,500 tech industry jobs
- 60 federal agencies
- NSA/SCYBERCOM
- 20 military facilities

**Workforce**
- 3rd more cyber engineers than rest of nation
- 4% concentration of STEM professionals
- 26 NSA certified CABS
- 9% professional and technical workforce

**Incentives**
- SBP Tax Credit
- Cyber Investment Tax Credit
- R&D Tax Credit
- Seed and venture funding

**Innovation**
- 92 innovation ranking
- #2 best state for opportunity
- 83% growth in startup revenue
- 35+ incubators, accelerator, research parks
Buy Maryland Cybersecurity (BMC) Tax Credit

June 1, 2018

In a big win for everyone in Maryland, the state legislature passed a landmark cybersecurity tax credit for small businesses.
Buy Maryland Cybersecurity (BMC) Tax Credit

- Too many small businesses have not had the necessary financial and human resources to improve their cybersecurity.

- BMC is aimed at reducing the alarming statistics of data breaches affecting hundreds of thousands of Maryland residents by stimulating investment in cyber products & services.
Tax Benefit to Buyer
+ Use Case

- Your business can claim a credit on your state income tax equal to **50% of the cost** to purchase qualified cybersecurity products and services, **up to a maximum of $50,000 in credits** ($100,000 total purchase.)

- **Use case for a small medical practice:**
  Purchase made directly from a Qualified Maryland Cybersecurity Seller

  Purchase price of cybersecurity technology or service: $2,000
  Calculate the 50% of purchase price tax credit ($2,000 x .5 = $1,000)

  **Tax Credit Amount = $1,000**
Program Definitions & Eligibility

Your business is eligible for the state income tax credit if you are a Maryland entity with fewer than 50 full-time employees.

**Cybersecurity** technology means products or goods intended to detect or prevent activity intended to result in unauthorized access to, exfiltration of, manipulation of, or impairment to the integrity, confidentiality, or availability of an information system or information stored on or transiting an information system.

A **Qualified Maryland Cybersecurity Company** (QMCC) is a company that has been certified by the Department of Commerce.
A Qualified Maryland Cybersecurity Company (QMCC) is a company that meets the following requirements and has been certified by the Department of Commerce (Commerce):

- Has its headquarters and base of operations in Maryland;
- Has fewer than 50 employees;
- OR is designated as a minority-owned, woman-owned, veteran-owned or service-disabled-veteran-owned-business.
BMC Tax Credit Form

Qualified BUYER Application

To qualify for the credit, please complete and submit the Qualified Maryland Company BUYER application to the Department of Commerce. [DOWNLOAD HERE.]
Find Maryland Cyber Companies
https://www.mdcyber.com/listings/
CONTACTS
For information about Buy Maryland Cybersecurity Tax Credit:

Abigail McKnight, Tax Specialist
Office of Finance Programs
410-767-7234

Lauren Satyshur, Program Manager, Healthcare Technology
Division of Cyber and Aerospace
410-767-4278

Kenneth McCreedy, Senior Director
Division of Cyber and Aerospace
410-767 6438
Buy Maryland Cybersecurity (BMC) Tax Credit

View the current list of Qualified Maryland Cybersecurity Sellers
[ COMING SOON ]

http://commerce.maryland.gov/fund/programs-for-businesses/buy-maryland-cybersecurity-tax-credit
This seminar will explore questions like:
• Cloud Security vs Local Security?
• Who are the cloud providers serving small and medium size businesses?
• Does going to cloud automatically increase the security?
• Options for engaging cloud services securely?
THANK YOU

Any Questions?

Anene Onyeabo
Program Manager
Maryland Health Care Commission
(410) 764-3285
anene.onyeabo@maryland.gov

Lauren Satyshur
Health IT Program Manager
Maryland Department of Commerce
(410) 767-4278
lauren.satyshur@maryland.gov

Krish Bhatnagar
Head, Security Services
Mokxa Technologies
(301) 343-6727
kbhatnagar@mokxa.com