Technology Security

Presenter(s)
Heather Helm, NMDP Product Owner, Donor Services
Rob Hanson, NMDP Cyber Security and Privacy Director
Disclosures

The following faculty and planning committee staff have no financial disclosures:

<table>
<thead>
<tr>
<th>Name</th>
<th>Institution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Heather Helm</td>
<td>NMDP/Be The Match</td>
</tr>
<tr>
<td>Rob Hanson</td>
<td>NMDP/Be The Match</td>
</tr>
<tr>
<td>Brandon Knez</td>
<td>NMDP/Be The Match</td>
</tr>
<tr>
<td>Lara Rauchwarter</td>
<td>NMDP/Be The Match</td>
</tr>
</tbody>
</table>
Disclosures

The following faculty and planning committee staff have the following financial disclosures:

<table>
<thead>
<tr>
<th>Name</th>
<th>Institution</th>
<th>Disclosure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jackie Foster, MPH, RN, OCN</td>
<td>NMDP/Be The Match</td>
<td>Pfizer, stock ownership (spouse)</td>
</tr>
</tbody>
</table>
Learning objectives

At the conclusion of this session, attendees will be able to:

• Examine the different types of cyber-criminals that are targeting healthcare and their motives for stealing and monetizing healthcare data.
• Explore why healthcare staff, not the technology, are the primary target of these cyber-attacks.
• Apply basic techniques to foil cyber-attacks in your daily workplace.
Cyber Risk Climate Change

- Monetization of medical records
- Attack methods (ransomware), sophistication
- Disruptive technologies (social, mobile, analytics, cloud)
- Accountability and regulatory changes (General Data Protection Regulation)
- Health sector breaches
- Business impact and consequences (breach costs, sanctions)

The success of our shared mission depends on managing cyber risks across a connected healthcare ecosystem and interconnected networks.
Hacking Economics: Medical Records

Because of the unique information in medical records, hackers can offer more valuable products to clients.

1. Higher black market sales prices (compared to financial or retail records)
2. Procurement of pharmaceutical drugs
3. Medical insurance fraud
4. Tax fraud
5. “Fullz” to replace a complete identity, credentials (e.g., Passports)
6. Medical applications are critical for patient care - ripe for extortion (ransomware)
7. Healthcare is a soft target
Hacking Economics: Medical Records
Hacking Economics: Medical Records
Hacking Economics: Medical Records
# Threat Actors and Motives

**Activist Arthur**  
**Motive:** Social, political, or religious justice  
**Skill:** Varied  
**Tactic:** Website defacement, social media hijacking, visible damage

**Script Kiddie Sal**  
**Motive:** Curiosity, thrill, or ego  
**Skills:** Basic security / computer skills  
**Tactic:** Pursues targets of opportunity, not targets of choice

**Big Money Mabel**  
**Motive:** Financial gain  
**Skills:** Moderate – Advanced, organized  
**Tactic:** Extortion, fraud via opportunistic, broad phishing, ransomware, malware

**Malicious Molly**  
**Motive:** Personal gain, career advancement  
**Skills:** Limited  
**Tactic:** Data exfiltration

**Nation State Cyber Crime**  
**Motive:** Military intelligence, nationalism  
**Skills:** Advanced, highly funded  
**Tactic:** Targeted advanced threats

**Negligent Ned**  
**Motive:** Get it done!  
**Skills:** Varied  
**Tactic:** Improper data handling
Threat Actors and Motives

Activist Arthur
- Motive: Social, political, or religious justice
- Skill: Varied
- Tactic: Website defacement, social media hijacking, visible damage

Script Kiddie Sal
- Motive: Curiosity, thrill, or ego
- Skills: Basic security / computer skills
- Tactic: Pursues targets of opportunity, not targets of choice

Big Money Mabel
- Motive: Financial gain
- Skills: Moderate – Advanced, organized
- Tactic: Extortion, fraud via opportunistic, broad phishing, ransomware, malware

Nation State Cyber Crime
- Motive: Military intelligence, nationalism
- Skills: Advanced, highly funded
- Tactic: Targeted advanced threats

Negligent Ned
- Motive: Get it done!
- Skills: Varied
- Tactic: Improper data handling

Malicious Molly
- Motive: Person gain, career advancement
- Skills: Limited
- Tactic: Data exfiltration
### Healthcare and Non Profit Data Breach Events

**Jan 2016 - Oct 2017**

<table>
<thead>
<tr>
<th>Category</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hacking / Ransomware</td>
<td>317</td>
</tr>
<tr>
<td>Insider Negligence / Disclosure</td>
<td>271</td>
</tr>
<tr>
<td>Hard Copy Loss</td>
<td>155</td>
</tr>
<tr>
<td>Portable Media</td>
<td>37</td>
</tr>
<tr>
<td>Malicious Insider</td>
<td>11</td>
</tr>
<tr>
<td>Stationary Media</td>
<td>1</td>
</tr>
<tr>
<td>Payment Card Fraud</td>
<td>0</td>
</tr>
</tbody>
</table>

Big Money Mabel

**Motive:** Financial gain

**Skills:** Moderate – Advanced, organized

**Tactic:** Extortion, fraud via opportunistic, broad phishing, ransomware, malware
Hi team,

In preparation for election day, we have outlined our company policies in the portal. Please be advised of our non-solicitation policies that require employees to refrain from activities including passing out political literature during work hours, excluding breaks. We have established a neutral dress code that prohibits the wearing of buttons, badges, or other political dress. Those who are not in compliance with our policies will be disciplined if the conduct creates a disruption in the workplace.

To record your acknowledgment, visit the portal. All employees are required to sign this document by COB.

We appreciate your cooperation. Your efforts help us foster our inclusive culture of diversity and mutual respect.

17.28% Industry Susceptibility
You have been hacked by a computer virus called WannaCry. The following sections contain information about what happened to your computer, how you can recover your files, and how you should pay to decrypt them.

**What Happened to My Computer?**
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

**Can I Recover My Files?**
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don’t pay in 7 days, you won’t be able to recover your files forever.
We will have free events for users who are so poor that they couldn’t pay in 6 months.

**How Do I Pay?**
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00 am - 11:00 am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address: 12tYDPgwueZ9Nymgw519p7AA8isjr6SMw

Copy
Negligent Ned

**Motive:** Get it done!

**Skills:** Varied

**Tactic:** Improper data handling
Top Causes for Negligent Data Disclosure

1. IT Systems Administrator improperly configures systems
2. Credential Sharing to Medical Records Systems
3. Misdirected email of health information
Protect Your Credentials

- *Health Informatics Research* survey of medical staff
- Willingness to share credentials to PHI
- Results indicated:
  - 74% of health professionals admit to using the credential of another medical staff member; 4.75 times on average.
  - 100% of medical residents obtained a credential from another medical staff member, while only 58% of nurses claimed to use a borrowed credential.
  - Job duties exceed access rights - #1 reason for borrowing credentials.
Reminder: Network Partners are responsible for protecting credentials and notifying Be The Match of personnel changes and terminations.
Thank You for Attending

Heather Helm
Product Owner, Donor Services
NMDP / Be The Match
Email: hhelm@nmdp.org

Rob Hanson
Information Security and Data Privacy Director
NMDP / Be The Match
Email: rhanson@nmdp.org
References

• Healthcare Informatics Research: Prevalence of Sharing Access Credentials in Electronic Medical Records
• Cybercrime and Other Threats Faced by the Healthcare Industry
• Health Warning Cyberattacks are targeting the health care industry
Evaluation Reminder

Please complete the Council Meeting 2017 evaluation in order to receive continuing education credits and to provide suggestions for future topics.

We appreciate your feedback!