You’ve Been Hacked, Now What?

Jake Blacksten
Jacobb@udel.edu

Scott Taber
Tabers@gvsu.edu
The North Star

CMMC

Utilizes the collection of existing frameworks and standards

Core programming built from CMMC 2.0 and NIST while also mapping to other frameworks

Consists of 6 domains

- Access Control
- ID & Authentication
- Media Protection
- Systems & Information Integrity
- System & Communication
- Physical Protection
The content contained within this presentation and any supporting documentation is meant for the purposes of learning basic cybersecurity awareness. It is not meant to provide or imply any form of certification within the CMMC, NIST or other regulatory model or framework. We hope you find this information useful in gaining a general understanding of basic cyber hygiene.

Should you require a more formal path to certification, the America’s SBDC Cybersecurity Task Force is able to provide several sources of professional training, consulting and assessment from within our group of sponsors and resource providers.
What To Do During A Data Breach

1. Determine the scope of the breach
2. Respond quickly
3. Patch the holes
4. Inform the right people/agencies
5. Learn from mistakes
Determining Scope
Stay Calm and Gather Information

- What do you know about the breach?
- What data was taken?
- How was it accessed?
- Who does the attack affect?
- Are the attackers still in the system?
Responding Quickly!
Mobilize your breach response team right away to prevent additional data loss.
Stop The Leak

1. Take all affected equipment offline immediately.
2. Do not power off any machines until forensic team allows.
3. Closely monitor all entry and exit points (Physical & Virtual).
4. Update credentials of all users affected.
Additional Response Measures

- Remove improperly posted information from your website and others.
- Interview people who discovered the breach.
- Do not destroy any forensic evidence, stop using infected machines.
## Common Causes of Data Breach

<table>
<thead>
<tr>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Weak/Stolen Passwords</strong></td>
</tr>
<tr>
<td><strong>Out-of-date Software</strong></td>
</tr>
<tr>
<td><strong>Use of Unsecure networks</strong></td>
</tr>
<tr>
<td><strong>Device Loss/Stolen</strong></td>
</tr>
<tr>
<td><strong>Virus or Malware</strong></td>
</tr>
<tr>
<td><strong>Installing bad software/ Plugging in unknow devices</strong></td>
</tr>
</tbody>
</table>
# Time It Takes A Hacker To Brute Force Your Passwords In 2022

<table>
<thead>
<tr>
<th>Number of Characters</th>
<th>Numbers Only</th>
<th>Lowercase Letters</th>
<th>Upper and Lowercase Letters</th>
<th>Numbers, Upper and Lowercase Letters</th>
<th>Numbers, Upper and Lowercase Letters, Symbols</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Instantly</td>
<td>Instantly</td>
<td>Instantly</td>
<td>Instantly</td>
<td>Instantly</td>
</tr>
<tr>
<td>5</td>
<td>Instantly</td>
<td>Instantly</td>
<td>Instantly</td>
<td>Instantly</td>
<td>Instantly</td>
</tr>
<tr>
<td>6</td>
<td>Instantly</td>
<td>Instantly</td>
<td>Instantly</td>
<td>Instantly</td>
<td>Instantly</td>
</tr>
<tr>
<td>7</td>
<td>Instantly</td>
<td>Instantly</td>
<td>2 secs</td>
<td>7 secs</td>
<td>31 secs</td>
</tr>
<tr>
<td>8</td>
<td>Instantly</td>
<td>Instantly</td>
<td>2 mins</td>
<td>7 mins</td>
<td>39 mins</td>
</tr>
<tr>
<td>9</td>
<td>Instantly</td>
<td>10 secs</td>
<td>1 hour</td>
<td>7 hours</td>
<td>2 days</td>
</tr>
<tr>
<td>10</td>
<td>Instantly</td>
<td>4 mins</td>
<td>3 days</td>
<td>3 weeks</td>
<td>5 months</td>
</tr>
<tr>
<td>11</td>
<td>Instantly</td>
<td>2 hours</td>
<td>5 months</td>
<td>3 years</td>
<td>34 years</td>
</tr>
<tr>
<td>12</td>
<td>2 secs</td>
<td>2 days</td>
<td>24 years</td>
<td>200 years</td>
<td>3k years</td>
</tr>
<tr>
<td>13</td>
<td>19 secs</td>
<td>2 months</td>
<td>1k years</td>
<td>12k years</td>
<td>202k years</td>
</tr>
<tr>
<td>14</td>
<td>3 mins</td>
<td>4 years</td>
<td>64k years</td>
<td>750k years</td>
<td>16m years</td>
</tr>
<tr>
<td>15</td>
<td>32 mins</td>
<td>100 years</td>
<td>3m years</td>
<td>46m years</td>
<td>1bn years</td>
</tr>
<tr>
<td>16</td>
<td>5 hours</td>
<td>3k years</td>
<td>173m years</td>
<td>3bn years</td>
<td>92bn years</td>
</tr>
<tr>
<td>17</td>
<td>2 days</td>
<td>69k years</td>
<td>9bn years</td>
<td>179bn years</td>
<td>7tn years</td>
</tr>
<tr>
<td>18</td>
<td>3 weeks</td>
<td>2m years</td>
<td>467bn years</td>
<td>11tn years</td>
<td>438tn years</td>
</tr>
</tbody>
</table>

Learn about our methodology at [hivesystems.io/password](http://hivesystems.io/password)
Fixing Vulnerabilities

Verify With Forensics Team
- Verify Cause
- Check no data was encrypted
- Analyze all backups
- Review logs for affected machines

Communication Plan
Create a plan that reaches all affected parties and do not be misleading or withhold information

Network Segmentation
Make sure you quarantined all infected machines, and they did not leak over

Patch/Update
- Change all passwords for all users
- Update and patch all systems in accordance with the forensics report
- Implement 2-factor

Anticipate Customer Questions
Notify Appropriate Parties
Who Should I Contact?

Determine Legal Requirements
All states have legislation about security breaches. Check your state and local laws.

Law Enforcement
Determine what local law enforcement you report breaches to. This could be police, local FBI field offices, etc.

Health Records Involved?
HIPAA has its own rules and regulations and making sure you follow them is important.

Notify Affected Businesses
If your breach affects other businesses say with credit cards or bank information you will want to contact them.
Notifying Individuals

Consult with your law enforcement contact

Designate a point person within your organization for releasing information

Consider using letters, websites, and toll-free numbers

Consider offering at least a year of free credit monitoring or other support

Clearly describe the incident to your customers using the following information:

- Date of breach
- What information was taken
- Where they can find more information
- Details on credit monitoring
- What you are doing to fix it

FTC has a full template dedicated to this online [here](http://www.AmericasSBDC.org/Cybersecurity)
Preventing Future Breaches
Lessons Learned

As the business responds to an event, make sure they incorporate the lessons they learned into their security program going forward. You want to prevent the same type of attack from happening again.

If the business was subject to a ransomware attack, they need to take the time to train their employees and themselves on identifying malicious links.

Questions To Ask Yourself

• Why was I a target?
• What did I do well and what did I do poorly when responding?
• What changes can I make to prevent this again?
• Did my response plan work or does it need to be updated?
All devices need to have antivirus/antimalware installed on them.

Antivirus works by storing known signatures (fingerprints of files) of malicious code and files and compares them to the files stored on your machine.

Make sure that whatever software you choose offers total protection, not all are created equally.

More advanced company protection might require endpoint protection or Network Intrusion Detection software.
Did My Backups Work?

What Types of Backups Do You Run?

- **Full System Backup**: Creates exact copy of computer hard drive.
- **File Level Backup**: Creates a backup of only user generated files.
- **Incremental Backup**: Combination of both.
Additional Thing To Consider

- Cyber insurance
- Cyber Attorney
- Cybersecurity Consultant
- Cybersecurity Tools
- Cybersecurity Policies
- Cybersecurity Training
Thank You!

Jake Blacksten
Jacobb@udel.edu

Scott Taber
Tabers@gvsu.edu