Computer Threats

James M.T. Morrison
FBI Houston (Retired)
Introduction

James M.T. Morrison (Uglymother)
• Cybersecurity Technologist with HPE
• 22 Years of Experience with the FBI
• 30+ Years in the IT field
• BS in Computer Engineering, MBA Technical Management
• GCED, GREM, GCIA, GCIH, GCFA, GCFE, GPEN, GWAPT, GMOB, A+, Net+
“Today’s cyber threat is bigger than any one government agency—frankly, bigger than government itself, but I think no agency brings the same combination of scope and scale, experience, tools, and relationships that the FBI has.”

“The key is having the private sector start to form relationships with their local field office beforehand,”
FBI: Businesses beware, ransomware is hitting harder

By: Andrew Eversden

The Rise of Municipal Ransomware

America’s smallest cities and towns stand on the frontlines of cyber warfare.

Kara Frederick
September 3, 2019  Politics and law; Cities
The rise of cyber crime

- **2 Trillion**: The global cost of cyber crime will be over $2 trillion by 2019.
- **29 Million**: Records Exposed - ITRC Data Breach Reports more than 29 million records were exposed in 858 publicised breaches.
- **4 Million**: Average Cost - Ponemon's Institute analysis puts the average cost of a breach at $4 million, rising to $7 million in the US.
- **48%**: Malicious Intent - 48% of data security breaches are caused by malicious intent.
- **52%**: Human Error & System Failure - 52% of data security breaches are caused by human error and system failures.
- **80 Billion**: Global Spending - Over 80 billion was spent in 2016 to combat cyber crime.
• Less than half of companies globally are sufficiently prepared for a cybersecurity attack, according to a PricewaterhouseCoopers report.

• Over 40 percent of companies have sensitive files that are unprotected and open to every employee, according to TechRepublic.
Executive Opinion

• 80% of executives think they are “good” on cyber security while only 20% of IT personnel rate their cyber security better than “fair.”
Privacy/Breach Notification
Laws

Data
Privacy
Cost Over Time

- Companies with less than 500 employees suffered losses of more than $2.5 million
  - 67% of data breach costs were realized within the first year after a breach
  - 22% accrued in the second year
  - 11% accumulated more than two years after a breach.
Social Attacks

• Phishing
• Pretexting

• More than 90% of attacks start with an e-mail or social media attack
Ransomware

• A new organization will fall victim to ransomware every 14 seconds in 2019, and every 11 seconds by 2021. (Source: Cyber Security Ventures)
• Ransomware attacks have increased over 97 percent in the past two years. (Source: Phishme)
• 34% of businesses hit with malware took a week or more to regain access to their data. (Source: Kaspersky)
How Much Downtime Does a Ransomware Attack Cause?

Q3 2019: 12.1 Days
Q4 2019: 16.2 Days

Average number of days a ransomware incident lasts.

Coveware Q4 2019 Ransomware Marketplace report: [Link](https://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate)
Combating Social Attacks

- Don’t be Curious/Greedy
- ~80% of Employees Do not Click EVER
- ~5% will click on everything (Find Them)
- Practice Phishing
Exploit the Telecommuter

F.B.I.’s Urgent Request: Reboot Your Router to Stop Russia-Linked Malware

NordVPN confirms it was hacked

Zack Whittaker  @zackwhittaker  /  9:15 am CDT  •  October 21, 2019
Weakness of 3rd Party Relationships

- What access does the 3rd Party need?
- Data flows to 3rd parties need to be monitored
- When writing a contract with a 3rd party, data breach incident handling should be included.
- If you carry cyber insurance, how is the 3rd party handled?
- Only 15% of firms report being notified by a third-party vendor notifying them of a breach the vendor caused
### Why Care About Supply Chain

#### What Does Supply Chain Have to Do with Cyber Risks?

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>80%</td>
<td>80% of all info breaches originate in the supply chain.</td>
</tr>
<tr>
<td>45%</td>
<td>45% of all cyber breaches were attributed to past partners.</td>
</tr>
<tr>
<td>72%</td>
<td>72% of companies do NOT have full visibility into their supply chains.</td>
</tr>
<tr>
<td>59%</td>
<td>59% of companies do NOT have a process for assessing cybersecurity of third party providers with which they share data or networks.</td>
</tr>
<tr>
<td>40%</td>
<td>40% of attack campaigns targeted manufacturing and service sectors (20% each).</td>
</tr>
</tbody>
</table>
Internet of Things (IoT)

- The number of connected devices on the Internet will exceed 50 billion by 2020, according to Cisco. To put it another way, the number of IoT devices will be three times as high as the global population by 2021. And by 2022, 1 trillion networked sensors will be embedded in the world around us, with up to 45 trillion in 20 years.

Time to Get Serious about Hardware Cybersecurity
Public Enemy #1 & #2
1. About 40% of organizations store privileged and administrative passwords in a Word document or spreadsheet.
2. When people are asked to include a number in a password, the majority simply add a “1” or a “2” at the end.
3. Two-thirds of people use no more than two passwords for all their online accounts.
Passwords – Best Practices

- Do not use the same password for all websites
- Use Password Managers
  - Cloud-Based or Apps are Most Common
- Longer is Better (Add 4 to the min password)
- Alter your Password Patterns
  - Don’t Capitalize First Letter
  - Don’t End with Numbers
## Passwords – Who Cares

### How long will it take to crack your password?

<table>
<thead>
<tr>
<th>Length of Password (Chars)</th>
<th>Only Numbers</th>
<th>Mixed Lower and Upper case alphabets</th>
<th>Mixed numbers, Lower and Upper case alphabets</th>
<th>Mixed numbers, Lower and Upper case alphabets, symbols</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Instantly</td>
<td>Instantly</td>
<td>Instantly</td>
<td>Instantly</td>
</tr>
<tr>
<td>4</td>
<td>Instantly</td>
<td>Instantly</td>
<td>Instantly</td>
<td>Instantly</td>
</tr>
<tr>
<td>5</td>
<td>Instantly</td>
<td>8 secs</td>
<td>3 mins</td>
<td>13 mins</td>
</tr>
<tr>
<td>6</td>
<td>Instantly</td>
<td>5 mins</td>
<td>3 hours</td>
<td>17 hours</td>
</tr>
<tr>
<td>7</td>
<td>Instantly</td>
<td>3 hours</td>
<td>10 days</td>
<td>57 days</td>
</tr>
<tr>
<td>8</td>
<td>4 secs</td>
<td>4 days</td>
<td>153 days</td>
<td>12 years</td>
</tr>
<tr>
<td>9</td>
<td>40 secs</td>
<td>169 days</td>
<td>1 year</td>
<td>928 years</td>
</tr>
<tr>
<td>10</td>
<td>6 mins</td>
<td>16 years</td>
<td>106 years</td>
<td>71k years</td>
</tr>
<tr>
<td>11</td>
<td>1 hour</td>
<td>600 years</td>
<td>6k years</td>
<td>5m years</td>
</tr>
<tr>
<td>12</td>
<td>11 hours</td>
<td>21k years</td>
<td>108k years</td>
<td>423m years</td>
</tr>
<tr>
<td>13</td>
<td>4 days</td>
<td>778k years</td>
<td>25m years</td>
<td>5bn years</td>
</tr>
<tr>
<td>14</td>
<td>46 days</td>
<td>28m years</td>
<td>1bn years</td>
<td>2tn years</td>
</tr>
<tr>
<td>15</td>
<td>1 year</td>
<td>1bn years</td>
<td>97bn years</td>
<td>193tn years</td>
</tr>
<tr>
<td>16</td>
<td>12 years</td>
<td>36bn years</td>
<td>6tn years</td>
<td>14qn years</td>
</tr>
<tr>
<td>17</td>
<td>126 years</td>
<td>1tn years</td>
<td>374tn years</td>
<td>1qt years</td>
</tr>
</tbody>
</table>
Your Internet browser, operating system, anti-virus, and other programs should be updated regularly. Use an external or cloud-based backup system to save photos and documents.
1. Have an Incident Response Plan and Test it
2. Backup critical information and test your backups
3. Get an External Security Evaluation
4. Implement Two-factor Authentication
5. Encrypt Data at Rest
6. Train and Test your Employees
7. Evaluate Who Has Access and Who Needs It
8. Evaluate Processes that Rely on E-Mail
Breach Response is Key

- Average lifecycle of a breach was 279 days with companies taking 206 days to first identify a breach after it occurs and an additional 73 days to contain the breach.
Time is Money

• Companies in the study who were able to detect and contain a breach in less than 200 days spent $1.2 million less on the total cost of a breach.
Planning is Crucial

• Having an incident response team in place and extensive testing of incident response plans had $1.23 million less total costs for a data breach on average.
InfraGard is a partnership between the FBI and the private sector. It is an association of persons who represent businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the U.S.

Designed to help protect the 16 Critical Infrastructures

One of which is Healthcare and Public Health Sector

Membership is Free
James Morrison
FBI (Retired)
GCED, GFCE, GCFA, GPEN, GCIA, GCIH, GREM, GMOB
CEH, MBA, MA
281-889-0565
mail@txcyberguy.com