What's at stake
• Mirai took out large parts of the Internet
- Mirai took out large parts of the Internet
- Ukrainian grid black out by hacking
• Mirai took out large parts of the Internet
• Ukrainian grid black out by hacking
• WannaCry shuts 30% of UK NHS
• Mirai took out large parts of the Internet
• Ukrainian grid black out by hacking
• WannaCry shuts 30% of UK NHS
• NotPetya disrupts global logistics & manufacturing, including vaccines
Are you vulnerable?
Vulnerabilities reported to NIST per year

17,736
Software Complexity

- Modern Car
- Facebook
- Windows Vista
- Hadron Collider
- Boeing 787
- Android
- Google Chrome
- Linux Kernel 2.6.0
- Mars Curiosity
- Hubble Telescope
- F-22 Raptor
- Space Shuttle

Millions of Lines of Software Code
Supply Chain Vulnerabilities
Is this how hacks work?

Highly Skilled Hacker

1337 0-Days

Best Defenses Known/Available
OPM
DNC
Mirai
WannaCry
NotPetya
Equifax

“Known but Unmitigated Vulnerabilities”

“Known but Unmitigated Vulnerabilities”

“Known but Unmitigated Vulnerabilities”

“Known but Unmitigated Vulnerabilities”

“Known but Unmitigated Vulnerabilities”

“Known but Unmitigated Vulnerabilities”
Forecasted Global Cybersecurity Spending, 2015-2019:

$1 Trillion
ONE HUNDRED PERCENT of companies will be hacked over the same time period.
In 2018, Apple became the world’s first $1 Trillion company.
In 2019, Apple will spend around $1 Billion on security.
Last week, a 14-year old reported a major security flaw in Apple’s products.
Are you vulnerable?
Know your hackers
Nation State
- IR • FR • CN
- RU • IL • AU
- US • NK
- UK • SK

Increasingly Willing

Professional
- Exploit Dev
- Coders
- Criminals
- DDoS
- Blackhat SEO

Increasingly capable

Accident
- Hacktivists
- Terrorists
- Ideological
- Increasingly Hard to Distinguish

Increasingly
Hard to
Distinguish

Willingness

Capabilities

5kr1p7 K1dd13

Increasingly
capable

Professional
- Operators
- Social Bots
- Hosting
- Ransomware
- Botnets

Professional
- Operators
- Social Bots
- Hosting
- Ransomware
- Botnets

Ideological
- Hacktivists
- Terrorists
- Ideological
I Am The Cavalry

Five Motivations of Security Researchers

- Protect
- Puzzle
- Pride/Prestige
- Profit/Payment
- Protest/Patriot

https://iamthecavalry.org/motivations
Jay Radcliffe
Security researcher
Diabetic patient
Father of diabetic patient
Vulnerability Research, Disclosure, and Law
DoD’s Vulnerability Disclosure Policy Results

- Total valid reports resolved: 2,837
- Participating hackers: 645+
- High or critical severity vulnerabilities: 100+

Hackers from 50 countries including: India, Great Britain, Pakistan, Philippines, Egypt, Russia, France, Australia and Canada
DMCA Rules

- Intended to fight counterfeiting of DVDs
- Makes illegal circumvention of a technical protection mechanism (TPM) to access copyrighted works
- CFAA is the primary tool to prosecute cybercrimes
DMCA Exemptions

- “Solely for good-faith security research”
- “On a lawfully acquired device”
- “With the authorization of the owner”
- Conducted in an environment “designed to avoid any harm to individuals or the public”

- US DOJ in favor of exemptions: “the DMCA was not created to protect [voting machines], and is ill-suited to do so.”
Supply Chain Risk
Supply Chain Risk Vectors

Supplier facilitated risk – Implementation, operation, and maintenance
Counterfeit – Unverified components
Malicious Taint – Subverted components or systems
Unintended Taint – Known software vulnerabilities
<table>
<thead>
<tr>
<th>PARTS</th>
<th>COMPOUND PARTS</th>
<th>FINAL GOODS ASSEMBLED</th>
<th>OPERATOR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Procurement Guidance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4. **System information:**
   - List of 3rd Party Software
   - List of Accounts
   - List of Network Ports
   - List of firewall rules (if applicable)
   - Documentation of Security Capabilities/Configurations for System Hardening
   - Scanning Requirements

Provides more granular information as to how the system is setup and managed within the Mayo Clinic environment.

Provide vendor documentation (i.e. Bill of Materials) for the bulleted items. Template provided.

5. **Vulnerability Assessment, including:**
   - Testing Results
   - Remediation Tracking

Provides an in-depth vulnerability assessment, outstanding vulnerabilities and appropriate remediation plans and timelines to resolve the issues. This provides Mayo Clinic with appropriate information on risks that may be introduced into the patient care environment and allows for collaborative mitigation strategies to be detailed.

Complete a vulnerability assessment as detailed in the Vendor Assessment Book (pdf). Once testing is completed, complete the VA Statement of Methodology and document findings and remediation plans in a report. Example VA Statement of Methodology (pdf) and Vulnerability Assessment Template report provided.

6. **Mayo Clinic Information Security Schedule**

Provides advanced copy of Mayo Clinic’s Information Security Schedule that Supply Chain Management will negotiate as part of the purchase contract or vendor agreements.

- Ensure appropriate vendor internal staff receives Mayo’s Information Security Schedule for review.
- Perform review and prepare any proposed redline items.
- Provide a vendor contact to the Mayo proponent for the redlined ISS negotiation.

---

https://www.mayoclinic.org/documents/medical-device-vendor-instructions/doc-20389647
Perspectives on Cybersecurity

Beau Woods
Cyber Safety Innovation Fellow, Atlantic Council Leader, I Am The Cavalry (.org)
Appendix
Coordinated Vulnerability Disclosure
US Department of Commerce, NTIA Template

ISO/IEC 29147 Standard for Vulnerability Disclosure
https://www.iso.org/standard/45170.html

ISO/IEC 30111 Standard for Vulnerability Handling Processes
https://www.iso.org/standard/53231.html

National Governor’s Association

US Department of Justice
https://www.justice.gov/criminal-ccips/page/file/983996/download

It Takes a Village Comic (Atlantic Council and HackerOne)
http://publications.atlanticcouncil.org/hacktivity/
BSides Events Tracker
http://www.securitybsides.com/w/page/12194156/FrontPage

Hackers: the Internet’s immune system (TED Talk, Keren Elazari)
https://www.ted.com/talks/keren_elazari_hackers_the_internet_s_immune_system

Can hackers break my heart (TEDx Talk, Marie Moe)
https://www.youtube.com/watch?v=W1YWpVMpPi8
ZOMBIE Food Pyramid

- Bones, Gristle: Gnaw sparingly
- Stomach Group: 2-3 Servings
- Intestines Group: 2-3 Servings
- Heart & Lungs Group: 3-5 Servings
- Liver Group: 2-4 Servings
- Brain Group: 6-11 Servings
Defensible Infrastructure

Operational Excellence

Situational Awareness

Countermeasures

- Secure by Design
- Secure Baseline Configurations
- Secure Deployment Guidance
- Operating System and Software Support Lifetimes
- Coordinated Vulnerability Disclosure
- DevSecOps
- Visible Ops
- Endpoint Security
- Active Defense
- Intrusion Prevention
- Anti-Everything
- Penetration Testing
- Threat Intelligence
- Security Monitoring
- Threat Hunting
- Network Admission Control

- Vulnerability Management
- Change Management
- Egress Filtering
- Software Updateable
- Software Ingredients or Components List
- Evidence Capture and Logging

- Countermeasures
- Secure by Design
- Secure Baseline Configurations
- Secure Deployment Guidance
- Operating System and Software Support Lifetimes
- Coordinated Vulnerability Disclosure
- DevSecOps
- Visible Ops
- Endpoint Security
- Active Defense
- Intrusion Prevention
- Anti-Everything
- Penetration Testing
- Threat Intelligence
- Security Monitoring
- Threat Hunting
- Network Admission Control

- Vulnerability Management
- Change Management
- Egress Filtering
- Software Updateable
- Software Ingredients or Components List
- Evidence Capture and Logging
1. No default passwords
2. Coordinated vulnerability disclosure policy
3. Keep devices updated

Code of Practice for IoT Security

https://www.gov.uk/government/publications/secure-by-design