Telemedicine and Technical Risk Management

Peter House
2019 NRTRC Conference
2019-08-29
Table of Contents

• About
• The Current State of Affairs
• Virtual care considerations
• Cost optimization
  - Budget considerations
  - Training
  - Technology
  - Cyberinsurance
• Strategic Threat Modeling
• Roadmap
About Me

• Working in technology for 20 years
• Working in risk management for 11 years
• Holds numerous industry certifications:
  - CompTIA Advanced Security Practitioner
  - CompTIA Cybersecurity Analyst
  - Information Technology Infrastructure Library (ITIL) v3
  - TOGAF 9.0 Enterprise Architecture
  - And so on, and so forth...
Current State of Cyber

• Phishing attacks increased by 4% to 52%
• Advanced malware attacks increased by 8% to 24%
• Employee/contractor negligence increased as a root cause by 3% to 61%

*Source: 2018 State of Cybersecurity in Small & Medium Sized Businesses – Ponemon Institute, November 2018
70% of organizations are considered to be cyber novices

*Source: 2018 Hiscox Cyber Readiness Report - Hiscox Ltd*
The Ground Floor
The Internet is a Public Place

<table>
<thead>
<tr>
<th>TOP COUNTRIES</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>5,076</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TOP CITIES</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>San Jose</td>
<td>52</td>
</tr>
<tr>
<td>Seattle</td>
<td>28</td>
</tr>
<tr>
<td>Houston</td>
<td>20</td>
</tr>
<tr>
<td>Minneapolis</td>
<td>19</td>
</tr>
<tr>
<td>Portland</td>
<td>17</td>
</tr>
</tbody>
</table>

```
HTTP/1.1 200 OK
Server: Netwave IP Camera
Date: Mon, 26 Aug 2019 18:19:20 GMT
Content-Type: text/html
Content-Length: 2574
Cache-Control: private
Connection: close
```

```
HTTP/1.1 200 OK
Server: Netwave IP Camera
Date: Mon, 26 Aug 2019 18:22:06 GMT
Content-Type: text/html
Content-Length: 2574
Cache-Control: private
Connection: close
```
“Nobody is trying.”

“Nobody is trying,” said Sarah Zatko, the Chief Scientist at the Cyber Independent Testing Lab (CITL), a non-profit organization that conducts independent tests of software security. “We found no consistency in a vendor or product line doing better or showing improvement. There was no evidence that anybody is making a concerted effort to address the safety hygiene of their products,” she said.

Zatko presented the findings of CITL’s extensive study in Las Vegas on Friday on the sidelines of the Black Hat and DEF CON conferences at an event hosted by The Hewlett Foundation. CITL was started by Sarah and her husband Pelter (aka “Mudge”) Zatko. It bills itself as a kind of “Consumer Reports” for cyber security, partnering with that organization as well as The Ford Foundation, The Digital Standard and online payments firm Stripe.

The CITL study surveyed firmware from 18 vendors including ASUS, D-Link, Linksys, NETGEAR, Ubiquiti and others. In all, more than 6,000 firmware versions were analyzed, totaling close to 3 million binaries created from 2003 to 2018. It is the first longitudinal study of IoT software safety, according to Zatko.

CITL researchers studied publicly available firmware images and evaluated them for the presence of standard security features such as the use of non-executable stacks, Address Space Layout Randomization (ASLR) and stack guards, which prevent buffer overflow attacks.

Sarah Zatko is the Chief Scientist at CITL
Virtual Care Risk

• Site to site connections
  - Home
  - Organizational
  - Mobile

• No visibility on « cyber hygiene »

• Potential entry point into a larger network
Cost Optimization

Effectiveness of Technologies in Protecting Data
Please rate the effectiveness of the following technologies in protecting enterprise data.

- Encryption
- Multifactor authentication tools
- Firewalls
- SIEM
- Endpoint security tools
- Threat intelligence
- Security data analysis tools
- Application security tools
- Cloud security tools
- Endpoint detection and response (EDR) tools
- Cloud services providers
- Orchestration tools
- Managed security service providers
- Antivirus
- Deception/honeypots
- Mobile security tools
- Data leak protection
- Passwords

Base: 315 respondents in 2018; not asked in 2017
Data: UBM survey of security professionals, May 2018

*Source: BlackHat 2018 – Where Cybersecurity Stands 2018
Protecting Virtual Care Devices

- Invest in encryption
- Think beyond the standards
  - Network security monitoring and logging
  - Multi-factor authentication
- Segregate as much as possible
- Train and hold accountable staff and contractors
Humans: Complex Yet Simple

*Source: 2018 Hiscox Cyber Readiness Report - Hiscox Ltd*
Strongly Consider

• General training and ongoing awareness programs:
  - Phishing
  - Social Engineering

• Specialized training IT staff or specialized IT vendors

• Developing a culture of respect (not fear) for cyber
Budget Considerations

- A healthy organization has an IT budget of approximately 5.5% of total operating*.
- Mature IT programs spend around 12.5% on cyber, in contrast to immature organizations at 10%**.
- Quick math:
  - 0.006875 % of total operating
  - 10 million operating budget means
  - $550,000 on IT
  - $68,750 on cyber

*Gartner Press Release - Gartner Says Many Organizations Falsely Equate IT Security Spending With Maturity
**2018 Hiscox Cyber Readiness Report – Hiscox Ltd
Regarding Insurance

- Complete applications accurately
- Gather backing for answers to application questions
- Exhibit due care over the life of the premium
Take Care, Take Care, Take Care

- Establish responsibility
- Require regular reporting
- Develop or enhance the culture of due care
  - Start with leadership
  - Start simply
  - Leverage gamification
We Don’t Drive Tanks to Work

- Am I a target of opportunity or of intent?
- What are the consequences of a breach?
- What is the cost of downtime and recovery?
- What risk can I ... ?
  - Transfer
  - Mitigate
  - Accept
The Road Ahead

• 30 Days:
  - Request and review reports on cyber-readiness
  - Interview key staff/stakeholders on what keeps them up at night
  - Review current cyberinsurance premium/options
  - Initiate culture shift

• 6 months:
  - Implement key missing risk mitigating technologies
  - Establish reporting and responsibility structure and cadence
  - Initiate training program
  - Develop cyber protection strategy with key staff/stakeholders

• 1 year:
  - Review program success
  - Revise budget to meet best practices/your specific needs
THANK YOU