BUS 248 - Final Presentation
Cyber Risk Management Team

TEAM- Pr3dator

An Information Security Risk program proposal to Health Please Leadership
18 Oct 2018

PR3DATOR TEAM

- Threat Landscape
- Security Risks
- Tools/Techniques
- Legal Regulations
- Stakeholder Analysis
- Project Timeline

About Us

Our firm started as a group of security experts who crossed paths in a research project at San Jose State University. Our founders include security experts with varying backgrounds in hardware & software development, with security expertise in across network and application security.

SECURITY GOAL

THREAT LANDSCAPE

Current Threat Landscape (2018)

- **Growing Cyber Attack surface**
  - By 2020, the installed base of IoT devices is forecasted to grow to almost 31 billion worldwide.
- **PHI**
  - A person's PHI (Protected Health Information) is worth up to ten times more than credit cards on the black market. [names, birth dates, policy numbers, diagnosis codes and billing information]
- **Electronic Health Record**
  - EHR Systems remains the most lucrative target.
  - Not just subjective to financial loss or data loss

WHAT WE UNDERSTAND ?

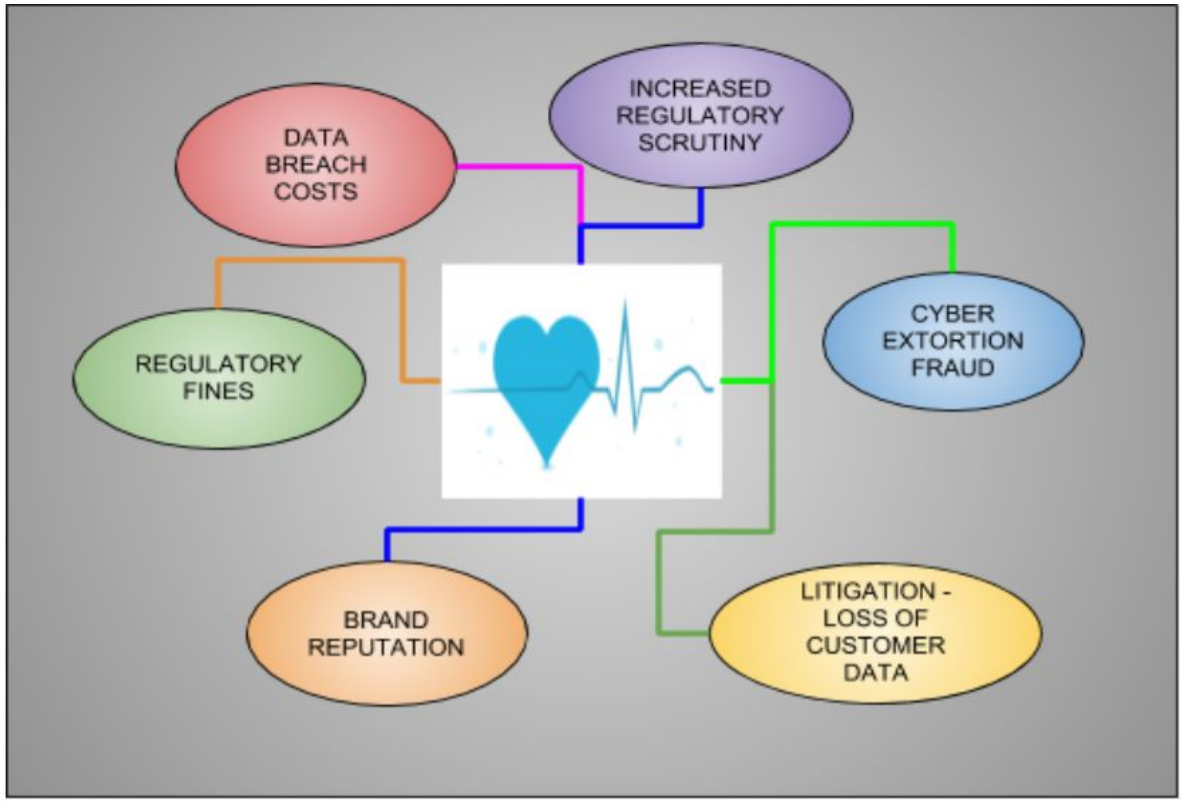
- **Threat Actors**
  - Hackers, Hacktivists, Corporations, Script Kiddies , Insiders, Users
- **People | Process | Technology**
- **Security Momentum**
  - Mass * Velocity (No of assets, Data Load, Product Market - Supply & Demand)
- **Importance of Security KPI**
- **Compliance, IT Support, What’s Next ?**
- **Attack Surfaces**
  - Devices, Communication channel, Cloud Interface, Application Interface

What we offer (Cyber Risk Services)

- Cyber Assurance
- Cyber Threat Modelling
- Risk Assessment
- Application Security
- Vulnerability Management
- Policy and Procedure Review & Development
- Network Monitoring
- Log Review & Analysis
- Incident Response
- Staff Augmentation

Information Security Risks

CYBER RISK INVOLVED



Common IOT Cyber Security Vulnerabilities

- Hardcoded credentials. Ex: hostname, port , credentials to access the server.
- Lack of encryption between the client's IOT device (in this case smart wearable sensor) and the central server. Sometimes the AES encryption key to protect the data in transit between the IOT device and the server was hardcoded in the IOT device.
- Lacking encryption of sensitive data at rest.
- Sensitive data disclosure. Ex: wireless configuration to access the client users local network.

Business Impact To Health Please Customers And Users

- Hacker's can steal the PHI (Protected Health Information) and EHR (Electronic Health Record) corresponding to their user base collected from their "half-million" smart wearable trackers. Not only could Health Please's Confidential Data get stolen , this will also have a profound impact to the privacy of Health Please's half-million users.
- Hacked IOT devices can be used to perform malicious activity such as launch large scale DDOS (Denial Of Service) attacks against internet services and bring them down. This is a reality and in fact 2017 was the most active year ever for IOT Cyber Attacks.

Product Prototype

IoT Health Necklace Tracker - Prototype

- Measure thoracic fluids
- Records
  - Heart rate
  - Respiration rate
  - Heart rate variability
- Monitors
  - Stroke volume
  - Cardiac output
  - Single-lead ECG
  - Posture

IoT - Necklace

IoT Health Necklace Tracker - Implementation

- IoT Necklace with sensors, storing user's data in the Cloud and processing data through a Mobile application

IoT - Necklace

Security Assessment

Tools & Techniques

IoT Security Standards & Projects

OWASP IoT Security Assessment

- Internet of Things Project
- Security Testing Guides
- Framework Assessment

Coverage Testing & Checklist

- Security Guidance

NIST IoT Projects

- Security and Privacy Risk Considerations

The European Union Agency for Network and Information Security (ENISA)

- Baseline Security Recommendations for IoT

OWASP Ecosystem Approach

- Exposure Identification
- Product Threat Modeling
- Impact Determination
- Security Testing Execution
- Remediation Plan & Execution

OWASP TOP 10 + SANS 25 CROSS-REFERENCE THREAT ASSESSMENT

ATTACK	COMPONENT	IMPACT	LIKELIHOOD OF EXPLOITATION	OVERALL IMPACT
BLUESNARFING	BLUETOOTH	LOW	MEDIUM	LOW RISK
BLUEJACKING	BLUETOOTH	LOW	MEDIUM	LOW RISK
BLUEBUGGING	BLUETOOTH	LOW	MEDIUM	MEDIUM RISK
BLUETOOTH PACKET SNIFFING	BLUETOOTH	MEDIUM	MEDIUM	HIGH RISK
WIRELESS DISASSOCIATION	WIRELESS	MEDIUM	LOW	MEDIUM RISK
WIRELESS ENCRYPTION ATTACKS (WEP, WPA, WPA2/KRACK)	WIRELESS	HIGH	HIGH	HIGH RISK

IoT Security Testing Methodology

- Functional Evaluation
- Device Reconnaissance
- Cloud & Web APIs
- Mobile & Control Applications
- Network
- Physical Embedded hardware Inspection
- Physical Device Attacks
- Radio (RF)

IoT Device Hacking Prevention - Value Manipulation

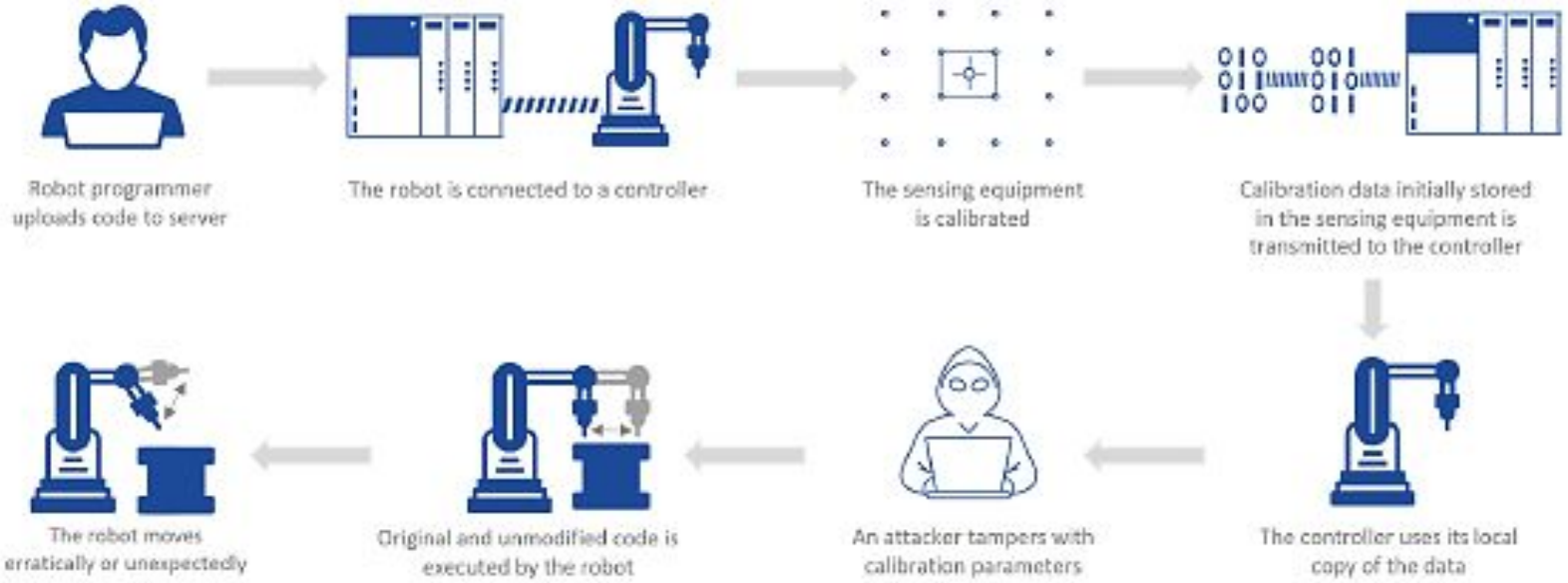


Image credit: ENISA

IoT Device Hacking Prevention - Sample Report

IOT SYSTEM COMPROMISE

IMPACT

High – Crucial: By allowing the sensors to report and accept incorrect values, the IoT environment is put at risk – a malfunctioning industrial robot can cause severe physical damage to whatever it is working with, and in the worst case scenario, to the people working with it.

EASE OF DETECTION	CASCADE EFFECT RISK
Easy – Medium: its detection is between easy and medium since an operator can see whether the outcome and the robot's behaviour are correct or not.	**Medium:** The cascade effect risk is medium, but it can vary depending on the number of sensors compromised in the robot, and on the number of robots involved.

ASSETS AFFECTED	STAKEHOLDERS INVOLVED
Sensors Actuators Decision making Software Sensitive information	IoT experts, software developers and manufacturers IT/Security solutions architects

ATTACK STEPS (SAMPLE BASED ON A REAL-CASE ATTACK SCENARIO)

1. The robot programmer uploads code to aserver
2. The robot is connected to a controller or its configuration has changed
3. The sensing equipment is calibrated
4. The calibration data initially stored in the sensing equipment is transmitted to the controller during the system boot
5. The controller uses its local copy of the data
6. An attacker remotely or locally tampers with calibration parameters
7. Original and unmodified code is executed by the robot
8. The robot moves erratically or unexpectedly because the true error is different from the error that the controller knows

RECOVERY TIME / EFFORT	GAPS AND CHALLENGES
Medium – High: depending on the number of sensors, and the robots involved, the recovery time can range from a few days to weeks.	Insecure design or development Lack of awareness and knowledge

COUNTERMEASURES

- ✓ **GP-PS-10**: Establish and maintain asset management procedures and configuration controls for key network and information systems
- ✓ **GP-PS-11**: Identify significant risks using a defence-in-depth approach
- ✓ **GP-TM-15**: Design with system and operational disruption in mind, preventing the system from causing unacceptable risk of injury or physical damage
- ✓ **GP-TM-31**: Measures for tamper protection and detection. Detection and reaction to hardware tampering should not rely on network connectivity
- ✓ **GP-TM-54**: Data input validation (ensuring that data is safe prior to use) and output filtering
- ✓ **GP-TM-56**: Implement regular monitoring to verify the device behaviour, to detect malware and to discover integrity errors
- ✓ **GP-OP-09**: Ensure the personnel practices promote privacy and security – train employees in good privacy and security practices

Image credit: ENISA

Regulatory Standards In Healthcare Industry

WHAT IS HIPAA?

- HIPAA is legislation that provides for data privacy and security provisions for safeguarding medical information.
- Under the HIPAA Privacy Rule, health-care providers are required to protect and keep confidential all personal health information for patients, and are strictly regulated in the use or disclosure of such information without proper authorization from the patient.
- This information is referred to as PHI includes all individually identifiable health information, including demographic data, medical histories, test results, insurance information, and other information used to identify a patient or provide health-care services or health-care coverage.

WHY DO YOU HAVE TO CARE?

- HIPAA is now extending its reach to cover the Internet Of Medical Things as these devices store sensitive patient information. .
- With the growing threats to the unsecured IoMT (Network Connected Medical Devices) and PHI (Protected HealthCare Information) the penalties are going to grow as well.
- More HIPAA audits are expected to focus on organization's adherence to the HIPAA Privacy, Security and Breach Notification Rules.
- HIPAA violations can carry fines as high as $50,000 per occurrence, and a maximum annual penalty of $1.5 million per violation
- Fines and charges are categorized into "Reasonable Cause," which range from $100 to $50,000 per incident, with no jail time involved; and "Willful Neglect," ranging from $10,000 to $50,000 for each incident and carrying the possibility of criminal charges.
- HIPAA fines for non-compliance reach $20 million in 2016.

EU GDPR -

The European Union General Data Protection Regulation

IMAGE CREDIT: GTB Technologies

WHAT IS GDPR?

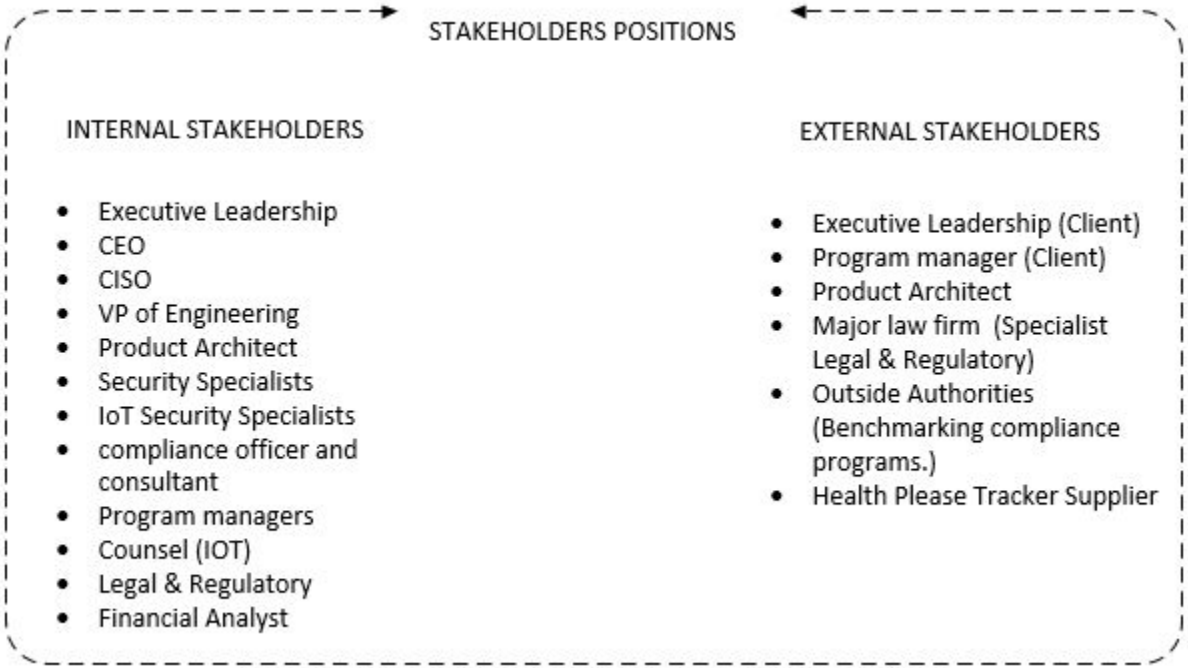
- EU's General Data Protection Regulation (GDPR) effective date: May 25, 2018
- Europe's omnibus new framework for data protection law applies to (almost) all entities that collect and process EU personal data regardless of where the data are processed.

WHAT WE SHOULD BE AWARE OF?

- Entities found to be in breach of GDPR could be fined up to 4 percent of annual global turnover or €20 Million (whichever is greater).
- Smaller infringements, such as an organization's failure to have their records in order, could result in fines of up to 2 percent of annual global turnover or €10 million (whichever is greater).

Stakeholder Analysis

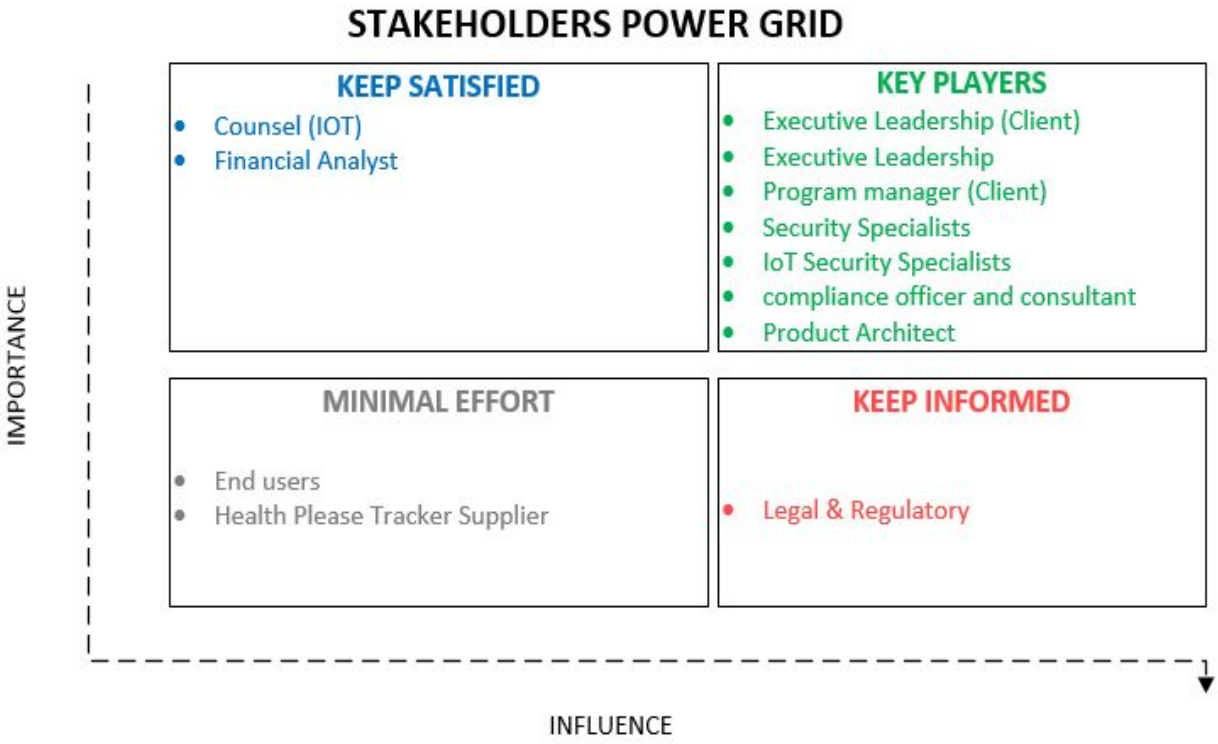
STAKEHOLDER POSITIONS



Health Please Security Stakeholders Positions

STAKEHOLDER MANAGEMENT APPROACH

This step enables the team to easily see which stakeholders are expected to be blockers or critics, and which stakeholders are likely to be advocates and supporters of the initiative.



Stakeholders stand to benefit here....

- Meet Wearable Product’s expectation in terms of Security and Compliance.
- Increasing Market share, Sales continue like they are doing.
- Enhance customer loyalty and Safety.
- Could be easy to expand in to foreign countries because of good security and regulations.
- Could establish more partnerships with healthcare companies and medical professionals.
- Health please can built a trusted brand platform based on the security and Compliance achievements.
- Suggestions and Improvements for the next release.

Project Plan Proposal

Project Timeline

Phase 1 - Status Assessment
(6-8 weeks)

- Cyber Threat Modelling
- Risk Assessment

Phase 2 - Training & Implementation
(12-16 weeks)

- Staff Augmentation
- Source code review
- STRIDE model training

Phase 3 - Long term Security upkeep
(6 months)

- Tool Selection & Deployment
- Policy and Procedure Review
- Network Monitoring and Log Review
- Incident Response

QUESTIONS ?

REFERENCES

1. Hacked IOT devices powered a massive internet outage by bringing down the Internet Infrastructure Company DynDNS
2. A New Cyber Concern: Hack Attacks on Medical Devices
3. HIPAA fines at record levels
4. Top 10 HIPAA violations
5. Privacy and Cybersecurity Top 10 for 2018