CABLE-TEC EXPO® 2017

SCTE · ISBE

THE NEXT BIG...

DEAL
CONNECTION
INNOVATION
TECHNOLOGY
LEADER
NETWORK

SCTE·ISBE CABLE-TEC EXPO 2017®

DENVER, CO
OCTOBER 17-20

2017 Fall Technical Forum
SCTE·ISBE • NCTA • CABLELABS

I HAD A DATA BREACH? EMERGING PRACTICES ON PREVENTION AND DETECTION

SCTE · ISBE

Implementing a Behavioral Analysis Approach to Thwart IoT Attacks

David Yates
VP Product Line Management
Guavus, A Thales Company

SCTE · ISBE CABLE-TEC EXPO 2017

DENVER, CO
OCTOBER 17-20

Introduction

- The “Internet of Things” (IoT) is here:
  - Experts forecast upwards of 50 billion connected devices by 2020[1]
  - 8.4 billion connected things will be in use worldwide in 2017, up 31% from 2016
  - Total spending on endpoints and services will reach almost $2 trillion in 2017
  - Use of connected things among businesses will drive $964 billion

- Concerns about IoT security are escalating as the number of IoT-enabled products
- IoT product development remains focused on connectivity, not security
  - Any business entering the IoT fray needs to consider security at the outset
  - Prioritize security and by adopt “security by design” practices

Business Trend and Pressures

- There are many business trends and pressures that will impact IoT security
- IoT is a complex system with low-capability users, creating a evolving risk environment
- There will be differing threats, actors, and reasons for targeting IoT
  - Additional considerations: technology’s scale, adoption rates, and regulatory

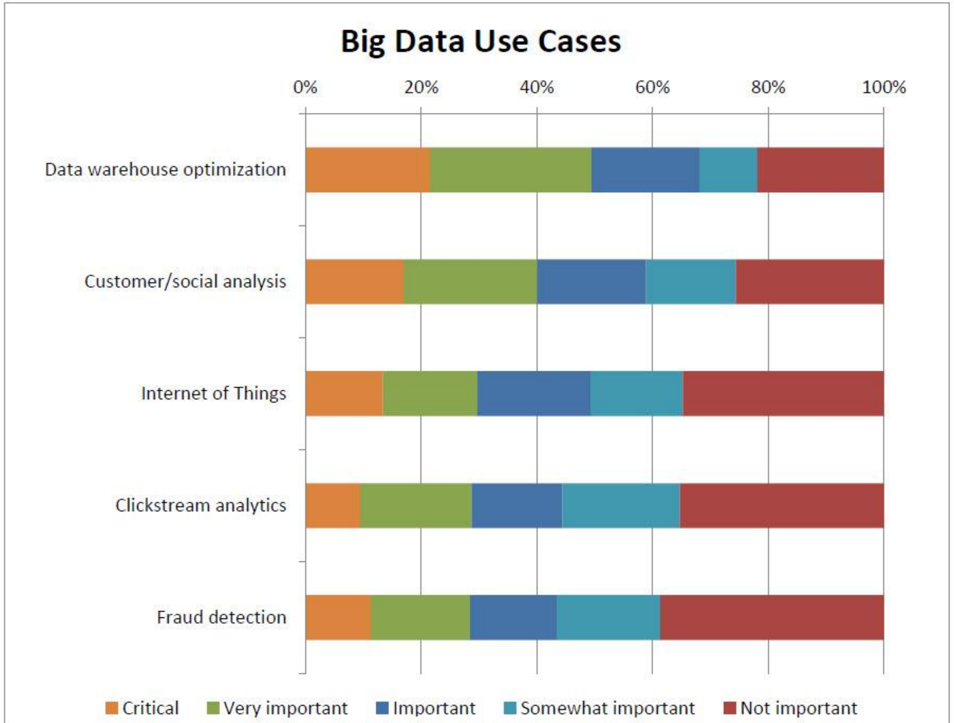
- Consumer products have a faster lifespan—focused on features and quick time to market
  - Rapid obsolescence will occur; large numbers of devices will be unpatched
  - Crowd-sourced development and libraries may increase widespread compromises
- IoT attacks will be based on monetary, ideology, or business disruption

IoT Security Pain Points

- Threats to IoT-enabled devices come in many forms and flavors
- Traditional IT security policies and controls will be untenable
  - New security model need to be data-centric and support all of aspects of OT
  - Security will need to be automated, distributed, context aware, and real time
- Most pressing concern: unauthorized access or control of an IoT device
  - Unauthorized access can alter or maliciously damage the collected data
  - MITM: Unauthorized entity can intercept communication and gain control
  - Spoofing: unknown IoT devices can pose as real user devices and wreak havoc

IoT Security Guiding Principles

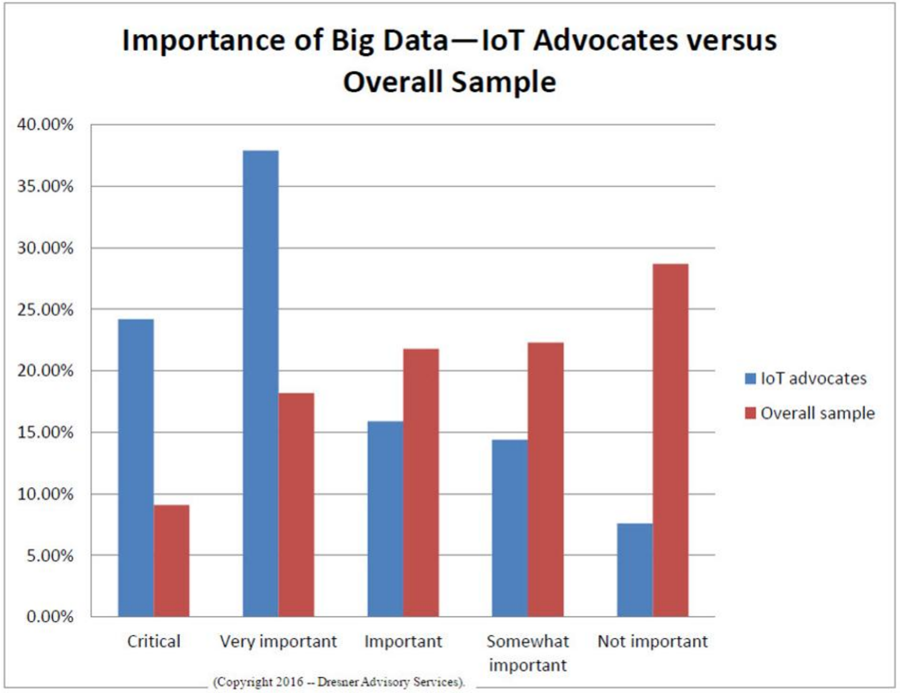
- Strategy: Define quality and security requirements for solutions, systems, and device
    - The level of risk varies according to the product and its functionality
    - Strike a balance between meeting security requirements and customer experience
    - IoT systems need to be safe and reliable with the following underlying attributes:
        - Embedded security
        - Secure access management
        - Self-protection
        - Privacy controls
        - Real-time information processes



(Copyright 2016 -- Dresner Advisory Services).

Big Data Study

- IoT advocates are 3X as likely to consider big data critical to their success
- Data warehouse optimization, customer/social analysis, and IoT are the top three big data uses cases
- Large-scale organizations are adopting big data to better aggregate, analyze and take action on the massive amount of data they generate daily to drive better decisions



(Copyright 2016 -- Dresner Advisory Services).

Big Data Study

- An organization’s ability to manage big data analytics is critically important to their success or failure with IoT
- IoT advocates are 3X as likely to consider big data critical, and 2X as likely to consider big data very important
- IoT advocates see IoT as a core justification for investing in and implementing big data analytics and architectures

Information Analytics in IoT Security

- IoT requires new and complex proficiencies in analytics
  - Ingesting data at speed and volume sets the stage for additional processing.
  - Real-time Analytics processes incoming streams of data from IoT sensors and devices
  - This refined data is then correlated with contextual and historical data to provide a baseline for advanced analytics
- First step is to simplify the process by integrating all the data for an IoT application
  - Silos should be removed and analytics used across a broad spectrum
- Second key step in the streamlining process is to unify the analytics layer
  - Unified into a single engine to ensure scalability and real-time performance

An Example of a Modern Security Analytics Platform

- The focus of the platform: is deliver better business outcomes and value in IoT
- New platform offers a novel conceptual, machine intelligence approach to analytics
  - Provides 360° visibility across data silos (L3 (network), L7 (application
  - Opens up data models for threat hunting through its Security Analytics toolkit and modules built ground up for security
  - Delivers faster analytics in real-time with a unique methodology that ingests data
  - create faster analytics (minutes vs. months) via a set modules and automation
  - Integrated graph-relational view of identity-asset-network-adversary model

Summary

- IoT presents unprecedented opportunities but:
    - IoT challenges are part of the equation; data breaches now a common occurrence
    - Prioritize security and make it a centerpiece of an IoT product strategy of design
- The future for security: security intelligence and insight include three areas of focus:
    - Advanced protection platforms: information-centric protections, endpoint activity monitoring and self-healing, advanced forensic capabilities
    - Predictive intelligence: advanced sharing capabilities, scalable threat intelligence vetting, feed-based to adversary-centric intelligence
    - Security analytics: detect the unknown with Big Data analytics, create advanced visualizations, establish proactive, counter-intelligence capabilities—hunt teams

SCTE · ISBE

THANK YOU!

David Yates
David.Yates@guavus.com
650-823-0674