2017

COMPASS INTELLIGENCE

DELIVERING METRICS-DRIVEN INTELLIGENCE & INSIGHTS

Understanding Security Risks in an Automated World:

Advancing IoT Brings Risk and Requires Preparation

Date Created: January 2017
Report Created by Compass Intelligence Analyst Team

Table of Contents

List of Figures

About Compass Intelligence

This report was prepared by Compass Intelligence, LLC

About Compass Intelligence

Compass Intelligence is one of the leading market analytics and consulting firms specializing in metrics-driven market intelligence and consulting focused on the entire mobile ecosystem, device recommerce and recycling, IoT, and emerging technology markets. Compass Intelligence provides a number of key services including strategic advisory, market sizing/modeling, competitive benchmarking, executive-level consulting, and turn-key survey services. Providing quality services over 11 years, many of the top technology vendors rely on Compass Intelligence's expertise and insights to make better and more informed planning, strategy, and development decisions. Visit us at http://www.compassintelligence.com to learn more.

Methodology

Compass Intelligence conducts ongoing research by utilizing some of the following research methodologies to complete market forecasting, uncovering the top trends, sharing the latest market drivers and challenges, and performing competitive analysis:

- Ongoing top-down (evaluating market revenues) and bottoms up (evaluating users or units) market sizing of the U.S. and Global IT market expenditures and revenues, as well as user, subscriber, unit, shipments, installed base, and other end-user metrics tracking
    - The Compass Intelligence database of forecasts, metrics tracking, and financial modeling is upwards of 100s of individual and detailed segmentation analysis of the top industries influencing the mobile industry today.
    - Forecasting may be validated using existing market data that falls in a relevant market or has relatable metrics to further refine trending and benchmarking
    - Compass Intelligence may also share informal forecasts and metrics with industry participants to gather feedback and confirmation, which support in validation or refinement of the model or key forecasts.
    - Compass Intelligence often makes assumptions given our market experience around segmentation and modeling to further segment forecasts by key demographic or other industry characteristic

- Continuing vendor analysis through 3rd party sources including earnings report, financial reports, website review, social media, and secondary sites that analyze key vendor or competitive analysis

- Use of existing, internal, and recent survey research collected using the Thought Leaders research and panel owned and managed by Compass Intelligence. These surveys may be conducted with end-users or decision-makers in the consumer or B2B market.

- Conducting briefings, interviews and meetings live, by phone, over chat, via email, web conference, and other tools with managers, owners, and executives of key industry participants, companies, financial investors, and other industry thought leaders.

- Industry trade shows, conferences, events, and organizations. Compass Intelligence is a member, board advisor, and participant in many of the top trade shows and conferences. Leveraging the meetings, sessions, presentations, and relationships at these events, supports in additional market intelligence gathering that is often used in our reporting and final write-ups.

- Additional resources may be used or unique for key reports depending on the topic and experience of our senior staff.

Introduction

Understanding Cyber Risks in an Automated World: Advancing IoT Brings Risk and Requires Preparation

As the entire enterprise and government sectors begin implementation of IoT-based technologies, including automation, monitoring, and tracking of assets, equipment, and systems, the risks levels are expected to advance and introduce threats that could take down companies if not prepared. With cyber-attacks increasing across the globe, companies and entire industries are at risk. Currently, information technology (IT) managers are witnessing an increase in the severity of attacks. The intensity of cyber-attacks on basic back-end applications and equipment, including client-facing services, is becoming a critical and high priority of investment to minimize threat costs and future attacks.

There are several issues that make companies a weak link for cyberattacks. An organization or business with a large footprint can have a plethora of devices that are integrated and interconnected. These devices have multiple functions that can range from automation systems to intrusion detection systems, as well as CRM, sales, and ERP applications. Many of these technologies have been deployed for over a decade and they were not designed to meet the modern challenges of IT security. For example, several technologies in companies have no encryption for data at rest or in motion, which makes information vulnerable. Furthermore, newer devices are not hardened with the latest cybersecurity techniques that makes them a high risk.

Further complicating matters is the acceptance and advancement of mobility and wireless technology. Today's CIOs/CTOs and IT managers are expected to monitor networks, and equipment remotely and have the ability to monitor and access information around the clock. In addition, responsible parties use multiple devices such as tablets and laptop computers. This adds another layer of complexity to a challenging problem because intruders can gain access through into a company's operations when an approved manager accesses a system remotely through a mobile device. Not only do businesses and solution providers have to worry about the products deployed throughout their IT network, but they must also contend with mobile security issues.

A challenge on the horizon for companies across industries is that network infrastructure companies and companies that manage networks are currently collaborating to evaluate the readiness of current network architecture and to develop a roadmap to better protect organizations from cyberattacks because the proliferation of connected devices is expected to increase data traffic and security risks. For technology companies that are not involved on the cutting edge with these entities, they run the risk of developing solutions that may not meet the future needs of their clients. The technology companies have great insight into the actual traffic, anomalies and attacks taking place on the Internet, which makes them an ideal partner because they understand the risks that are facing various industries.

The limited supply of qualified personnel to handle IT security at the growing pace at which attacks are happening, makes this even more challenging. One best practice to solve this challenge is to create partnerships with universities, especially those with expertise in IT security, cybercriminal activity, and

emerging cyber risks. Several companies are partnering with universities to create programs to better train and educate their employees as it relates to cybersecurity and other emerging technology trends. One such partnership is the one between AT&T and Georgia Tech. In collaboration with Georgia Tech, AT&T has developed a master program with the university. Several other such programs are being created throughout the world.

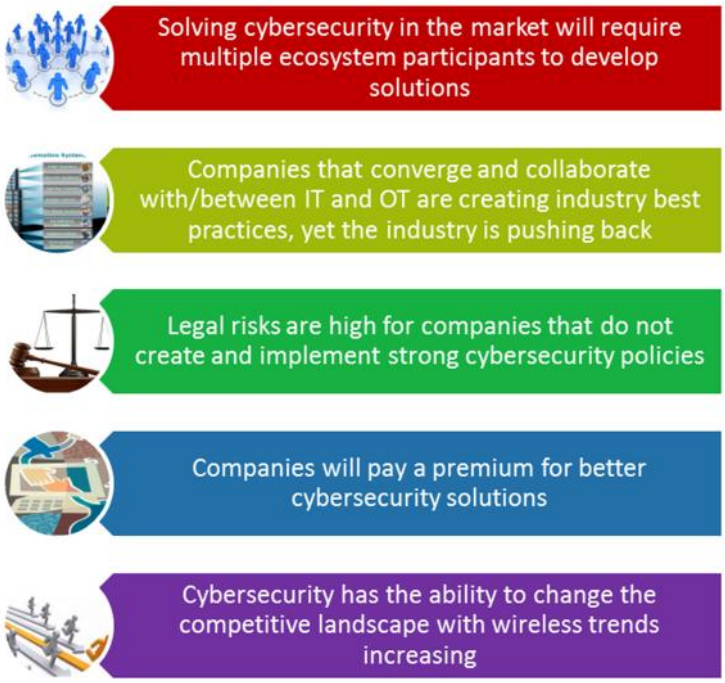
Another hurdle to overcome in the industry is bridging the gap between the facility OT (Operational Technology) and IT (Information Technology) teams. Operational teams may be excellent at understanding operations and processes, but they are not familiar with important IT network protocols and their skill-set is limited in defending against cyberattacks. IT managers are great at managing the network but may not have the entire scope of how the operational systems, applications, and infrastructure is set up. Furthermore, IT may not be that familiar with the protocols that operational mangers are accustomed to working (many of them specific to the industry). If the IT department discovers something on the network they are not familiar with they will revert to “deny by all rule” and shut a device/solution down, which may be impacting operations and even customers. Closing the gap between these two groups is very critical.

One of the driving factors to overcome cyber threats is loss of business and liability concerns. It is estimated that a single breach can cause a decrease of twenty-two percent in net earnings over the following four quarters after it is discovered. What’s even more alarming, there are several legal cases that have the ability to set a precedent that can make the C-level suite and Board of Directors liable for security breaches from end-users and investors. Businesses can no longer be inactive or have weak internal policies. Once a technology solution is deployed, the cyber liability rests with the company.

Top Five Report Key Findings

The below figure displays the top five findings based on Compass Intelligence research. In addition to these findings the study also highlights some of the industry best practices to businesses.

Figure 1: Top Five Key Findings



Source: Compass Intelligence, 2017