



CANASA Monitoring Symposium

TORONTO OCTOBER 2017

CANASA Monitoring Symposium

Areas we will cover today:

- 1) The Disruptors
- 2) 3rd Party Stations
- 3) Threats and new entrants
- 4) Cyber risk (LITE)

CANASA Monitoring Symposium

▶ CONSIDER

- ▶ The largest room booking company does not own a Hotel
- ▶ The largest ride for hire company does not own a Taxi cab
- ▶ The largest retail sales company does not own any retail stores
- ▶ 1 of the most watched Networks has no studios, towers or Live News

CANASA Monitoring Symposium

“ REPETITION doesn't create memories.
New experiences do”

Brian Chesky CEO and Co-Founder of Airbnb

CANASA Monitoring Symposium

OUR CHALLENGES

- ▶ Application of TECHNOLOGY to an outdated Industry
- ▶ Focus on the User Experience (UX)
- ▶ User –friendly and ease of purchase

CANASA Monitoring Symposium

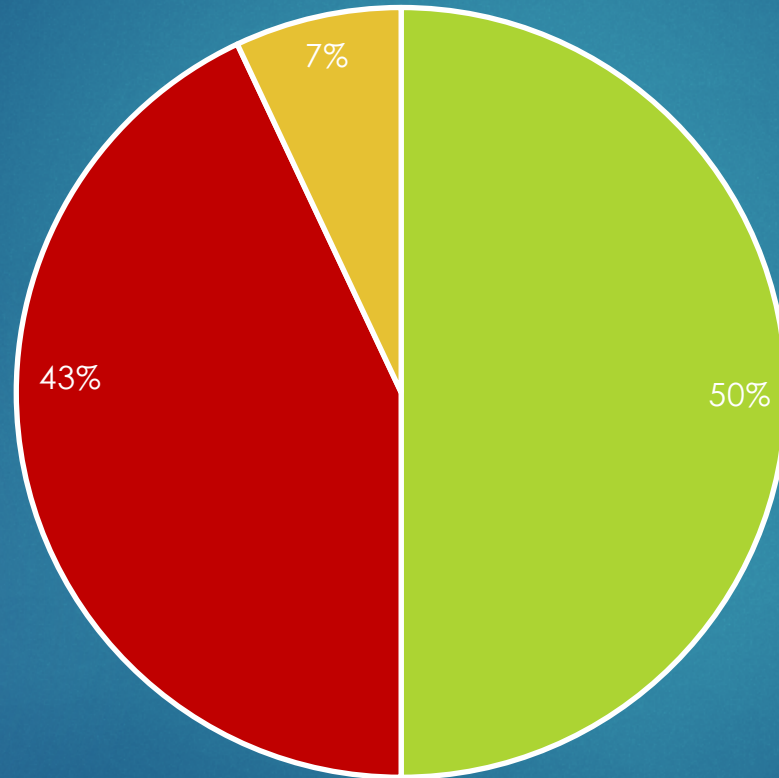
TREND 2016

- ▶ RFI Communications switched to Rapid Response
- ▶ Red Hawk Fire and Security partnered with Affiliated Monitoring
- ▶ Comtronics switched to National Monitoring Center

CANASA Monitoring Symposium

Source – SSN 2017/01

Respondent's Company Profile

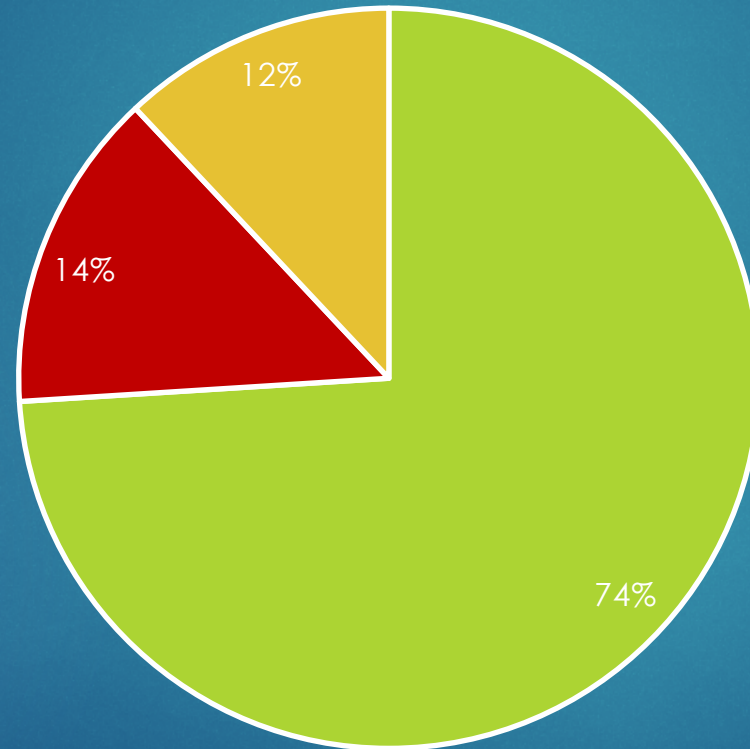


■ YES ■ NO ■ DO NOT MONITOR

CANASA Monitoring Symposium

Source SSN 2017/01

Will More Companies switch to 3rd party Stations

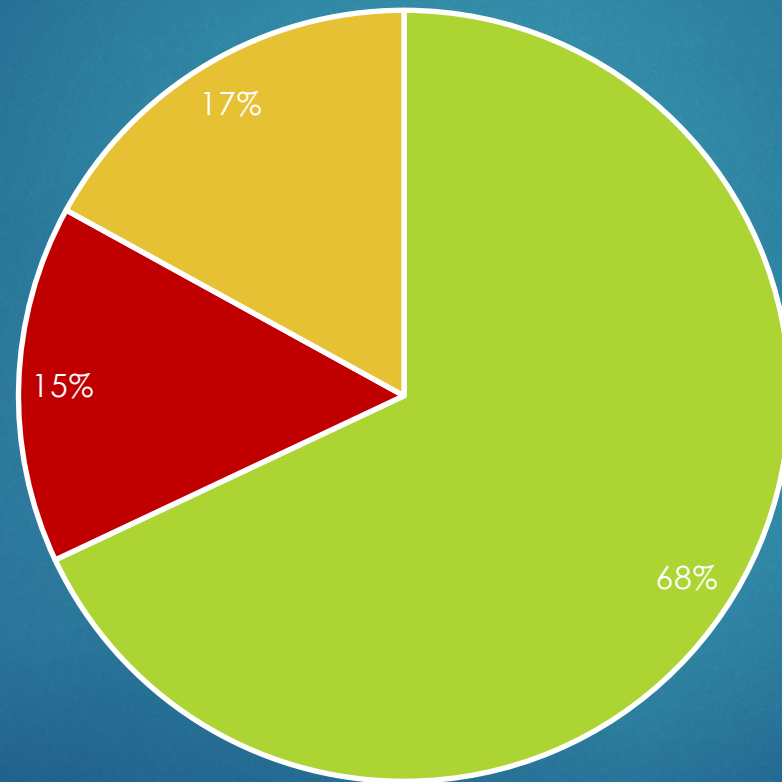


■ YES ■ NO ■ NOT SURE

CANASA Monitoring Symposium

Source SSN 2017/01

Benefits



■ YES-Faster w/technology 68

■ NO-More control

■ Other

CANASA Monitoring Symposium

PROS

- ▶ 3rd Party Stations can afford bleeding edge technologies
- ▶ Allows Alarm Companies to focus on new revenue producing services and opportunities
- ▶ Per account monitoring is less at a 3rd Party Station – better cost efficiencies
- ▶ 3rd Party stations have greater resources, can offer Dealer Programs and Technical Assistance

CANASA Monitoring Symposium

CONS

- ▶ Fear of:
 - ▶ Losing control
 - ▶ Quality dilution
 - ▶ The unknown – You don't know what you don't know
 - ▶ Client's perception
 - ▶ Accounts being poached or stolen

CANASA Monitoring Symposium

THREATS

- ▶ HOME Depot – IDEAL Security with Telephone dialer
- ▶ ABODE – Works with Alexis, self monitored or can use Professional Monitoring services
- ▶ Canary – Motion detector activated cameras – MIY
- ▶ SimpliSafe – Wireless, APP based, MIY or Professional Monitoring available

CANASA Monitoring Symposium

THREATS

▶ BEST BUY

Partners with Vivint (May 4 2017)

IN STORE DISPLAYS



SHARE

COMPANY NEWS

MAY 4, 2017

Best Buy Partners With Vivint Smart Home To Launch Leading-Edge Smart Home Service

BEST BUY STAFF WRITER

RICHFIELD, Minn. and PROVO, Utah (May 4, 2017) – Best Buy and Vivint Smart Home today announced a strategic partnership to give customers an easy way to automate and manage their homes, called Best Buy Smart Home powered by Vivint. With a nationwide rollout beginning this summer, Best Buy customers will be able to visit one of more than 400 of the chain’s large-format stores to consult with a smart home expert, design a comprehensive system, and receive professional installation and monitoring, often within 24 hours.

Guided by in-store experts, customers can select from a suite of leading smart home products from Vivint and other partners – including smart locks, lights, cameras, thermostats and more – and purchase their products upfront or take advantage of special financing. Accompanying service plans include 24/7 professional monitoring with emergency response, always-on cellular connection, 30-day video storage, online and phone support, in-home service and equipment protection. Customers also have the option to select a no-contract service plan. Vivint’s smart home platform works with voice assistants, such as Amazon Echo and Google Home, enabling consumers to control their smart home devices with their voice.

“Best Buy is all about helping customers pursue their passions and enrich their lives with the help of technology,” said Asheesh Saksena, Chief Strategic Growth Officer at Best Buy. “To deliver on that

CANASA Monitoring Symposium

THREATS

- ▶ Nest Security System (September 20 2017)

Direct to Consumer, MIY

“What if it is so easy to use you actually use it”

• Company | September 20, 2017

From now on, this is security.



You're getting home from a family vacation. It's been a long trip, it's late, and you just want to go to sleep in your own bed. With a passed-out child in one arm and a suitcase in the other, you fumble with the keys and open the front door. And right away, it hits you – the dreaded alarm countdown. In the ensuing mad scramble to enter your code, the ear-piercing alarm goes off and your kids wake up – along with the rest of the neighborhood. Welcome home.

If you have a security system, you know the scenario all too well. A false alarm is a harrowing experience that leaves even the most steadfast person shaken to the core. It just takes a couple of them before you stop using your security

CANASA Monitoring Symposium

THREATS


- ▶ ADT & SAMSUNG announce a partnership (October 2 2017)
DIY with SAMSUNG SmartThings and Professional Monitoring Services with ADT

Home > Smart Home > Samsung SmartThings and ADT partner on new home...

SAMSUNG SMARTTHINGS AND ADT PARTNER ON NEW HOME SECURITY HUB

By Kim Wetzel — Posted on October 2, 2017 6:00 am

f 9 t + Subscribe > Share



The best part of this minimalist Pacific Northwest cabin is outside the window.

There aren't too many things to see but enjoying outdoor views.

The whole setup is an ADT-compatible DIY home security solution.

It's not just an smart-home device that automates, controls, and protects your home.

Images captured by smart home cameras like the one below.

Threats like this can be avoided.

Founded in 1874, ADT home security is one of America's oldest companies — older than even Ford and Coca-Cola. Meanwhile, technology company SmartThings was founded in 2012 and bought by Samsung in 2014, making it a kindergartner in the business world.

Samsung SmartThings and ADT — more than 100 years apart in age — are unlikely partners. But that's why executives for both companies think their new DIY home security partnership works so well: it combines the old-school hard-wired home protection of ADT with the invisible but powerful smart home capabilities of Samsung SmartThings.

CANASA Monitoring Symposium

DIY

PROS

- ▶ Peel & Stick wireless installation
- ▶ No Monitoring fees
- ▶ No Annual Contracts
- ▶ No phone lines required for the more sophisticated unit

CONS

- ▶ Peel & Stick wireless installation
- ▶ Perceived value
- ▶ No Professional Consulting

CANASA Monitoring Symposium

New Entrants - THE DISRUPTORS

The BIG 4:

- ▶ MICROSOFT
- ▶ GOOGLE (NEST, Dropcam)
- ▶ APPLE
- ▶ AMAZON

CANASA Monitoring Symposium

What do we have to offer?

- ▶ A Welcome mat into into homes and businesses
- ▶ Sticky Clients
- ▶ Low acquisition costs
- ▶ Ability to leverage additional services
- ▶ Bundling
- ▶ DATA, DATA, DATA

CANASA Monitoring Symposium

Where we are today:

5 years ago were you installing:

- ▶ Wireless locks controlled by an Alarm APP?
- ▶ Programmable thermostats controlled by an Alarm APP?
- ▶ Video doorbells on your Smartphone controlled by an Alarm APP?
- ▶ Offering SHaaS (Smart Home as a Service)?
- ▶ Have the ability to integrate with Siri (Apple), Google Home, Alexa (Amazon)?

CANASA Monitoring Symposium

CYBER THREATS

- ▶ News - [EQUIFAX breach exposes 143 MILLION in US to identity theft](#)



The image is a screenshot of a Forbes article. On the left, there is a navigation bar with the Forbes logo and a 'LOG IN' button. Below the navigation bar is a 'YOUR READING LIST' section with three items: 'Equifax Data Breach Impacts 143 Million Americans', 'Goals of Life: More Than What's On Paper: The Journey To a Parking Spot', and 'PODCAST: Can You See the Future? And How to Prepare for It'. The main article content is on the right. It features a date and time stamp 'SEP 7, 2017 @ 10:42 PM' and a view count '37,981'. The title is 'Equifax Data Breach Impacts 143 Million Americans'. Below the title are social media sharing icons for email, Facebook, Twitter, LinkedIn, and Google+. The author is 'Lee Mathews, CONTRIBUTOR' with a bio: 'Observing, pondering, and writing about tech. Generally in that order. FULL BIO'. A disclaimer states 'Opinions expressed by Forbes Contributors are their own.' The article text begins with 'Equifax is one of the largest credit reporting agencies in America, which makes an announcement the company just issued particularly disconcerting. An authorized third party gained access to Equifax data on as many as 143 million Americans. That's nearly half the population of the United States as of the last census.' On the right side of the article, there is an advertisement placeholder that says 'Ad created by Google' and 'Repeat this ad'.

CANASA Monitoring Symposium

CYBER THREATS

Why steal it if you can immobilize it?

► News – August 17 2017

[Unpatchable Flaw
in Modern Cars Allows Hackers to Disable
Safety Features](#)

Hacker News

Unpatchable Flaw in Modern Cars Allows Hackers to Disable Safety Features

Thursday, August 17, 2017 Mohit Kumar

Tweet Share 48 Share 747 Share 1.33K Share

Unpatchable Car Hack



Today, many automobiles companies are offering vehicles that run on the mostly drive-by-wire system, which means a majority of car's functions—from instrument cluster to steering, brakes, and accelerator—are electronically controlled.

No doubt these auto-control systems make your driving experience much better, but at the same time, they also increase the risk of getting hacked.

Car Hacking is a hot topic, though it is not new for security researchers who hack cars. A few of them have already demonstrated how to hijack a car remotely, how to disable car's crucial functions like airbags, and even how to remotely steal cars.

Now, security researchers have discovered a new hacking trick that can allow attackers to disable airbags and other safety systems of the connected cars, affecting a large number of vendors and

CANASA Monitoring Symposium

CYBER THREATS

► [News – August 15 2017](#)

[Smart locks lobotomized After Failed Automatic Update](#)

Security Sales and Integration

SECURITY SALES
& INTEGRATION

View Inventory Access Control Business Automation Fire & Intrusion

News

Smart Locks Lobotomized After Failed Automatic Update

Hundreds of LockSafe customers were left with nonfunctional smart locks after receiving the wrong over-the-air firmware update.

🕒 August 15, 2017 👤 Steve Karantzoulidis 💬 [Jump to Comments](#)

LockState customers were in for a surprise after an automatic update failed and bricked their smart locks last week, rendering them useless.

The company told Threatpost that more than 500 customers using model 6000i RemoteLocks were impacted. The issue stems from an over-the-air firmware update to its 6000i systems meant for its 7000i model locks.

The update caused first-generation models of the 6000i locks to malfunction, rendering them unable to be locked and no longer able to receive over-the-air updates.

“We realize the impact that this issue may have on you and your business and we are deeply sorry. Every employee and resource at LockState is focused on resolving this for you as quickly as possible,” CEO of LockState Nolan Mondrow told customers in an email. “After a software update was sent to your lock, it failed to reconnect to our web service making a remote fix impossible.”

In total, about 11 of the company’s keyless lock systems in use today are affected. The smart lock allows users to manage doors remotely, monitor usage of the door and receive alerts when the assigned codes are used.



Locksafe's 6000i RemoteLocks were impacted by an incorrect firmware update.

CANASA Monitoring Symposium

CYBER THREATS

► News – June 7 2016

University of Calgary paid \$20K in ransomware attack “No evidence cyber attackers released personal or university data to public”



The screenshot shows a news article from CBC News. The main headline is "University of Calgary paid \$20K in ransomware attack". Below the headline, it states "No evidence cyberattackers released personal or university data to public". The article is dated June 07, 2016, 2:27 PM MT. A video player is embedded in the article, showing a sign for the University of Calgary at 2500 University Drive NW. The video player has a play button and a progress bar showing 00:00 / 01:47. Below the video, there are social media sharing options and a list of related stories. The related stories include "The University of Calgary paid a demanded \$20,000 after a 'ransomware' cyberattack on its computer systems.", "The university announced the ransom payment Tuesday, a week after the initial attack.", and "As part of efforts to maintain all options to address these systems issues, the university has paid a ransom totalling about \$20,000 Cdn that was demanded as part of this ransomware attack." Linda Dalgetty, vice-president of finances and services, said in a release. There are also two bullet points: "University of Calgary cyber attack part of increasing problem, experts say" and "Ransomware: What you need to know".

University of Calgary paid \$20K in ransomware attack

No evidence cyberattackers released personal or university data to public

CBC News | Posted: Jun 07, 2016 2:27 PM MT | Last Updated: Jun 08, 2016 8:26 AM MT

University of Calgary pays \$20K in ransomware attack

UNIVERSITY OF CALGARY
2500 University Drive NW

00:00 / 01:47

University of Calgary pays \$20K in ransomware attack 1:47

Most related

- The University of Calgary paid a demanded \$20,000 after a "ransomware" cyberattack on its computer systems.
- The university announced the ransom payment Tuesday, a week after the initial attack.
- "As part of efforts to maintain all options to address these systems issues, the university has paid a ransom totalling about \$20,000 Cdn that was demanded as part of this ransomware attack," Linda Dalgetty, vice-president of finances and services, said in a release.

- University of Calgary cyber attack part of increasing problem, experts say
- Ransomware: What you need to know

CANASA Monitoring Symposium

FBI Internet Crime Complaint Center (IC3) 2016 Statistics:

Most prevalent and damaging:

- Business email compromise (BEC)
- Ransomware
- Tech Support Fraud
- Extortion

CANASA Monitoring Symposium

FBI Internet Crime Complaint Center (IC3) 2016 Statistics:

- ▶ 2016 losses exceeded 1.3B an increase of 24% over the previous year.
- ▶ Important to note that the best guess on this figure is that it represents only 15% of fraud victims.
- ▶ Estimated losses are therefore thought to be closer to 9B.

CANASA Monitoring Symposium

ASK YOURSELF

- ▶ Are you connecting Security systems via IP?
- ▶ Are you downloading information via IP?
- ▶ Are you gaining remote access via open ports?
- ▶ Are you sending your Clients emails?
- ▶ And the BIG question – do you have Cyber Insurance?

CANASA Monitoring symposium 2017

Thank you for your time.

Questions and comments?