**Altman Vilandrie & Company**
One Montgomery Street #2100
San Francisco, CA 94104
415-489-3250

# Are your company's IoT devices secure?

## Internet of Things Breaches are Common, Costly for U.S Firms

Altman Vilandrie & Company White Paper
June 2017

***From connected cars to supply chains, nearly half of companies have experienced data and devices breaches over the past two years.***

A survey conducted by Altman Vilandrie & Company of approximately 400 IT executives across 19 industries shows that nearly half of IOT security buyers have experienced a breach in the last two years. The financial impact of these breaches are significant, representing 13.4% of the total revenues for smaller companies and hundreds of millions of dollars for the biggest firms. IoT breaches can also render connected consumer and commercial products unsafe, endangering customers and employees and exposing companies to significant lawsuits.

Despite the very real financial, legal and public safety vulnerabilities, IoT security is not uniformly receiving the attention it deserves from IT buyers – particularly compared to the global focus on traditional cybersecurity threats. To combat future breaches companies are investing in products that "defend" against attacks and selecting providers based on brand/reputation – not necessarily pricing or other factors.

**Altman Vilandrie & Company**

Founded
2002

Offices
Boston, MA
New York, NY
San Francisco, CA

Specialization
Telecom
Media
Technology

Size
100+ employees

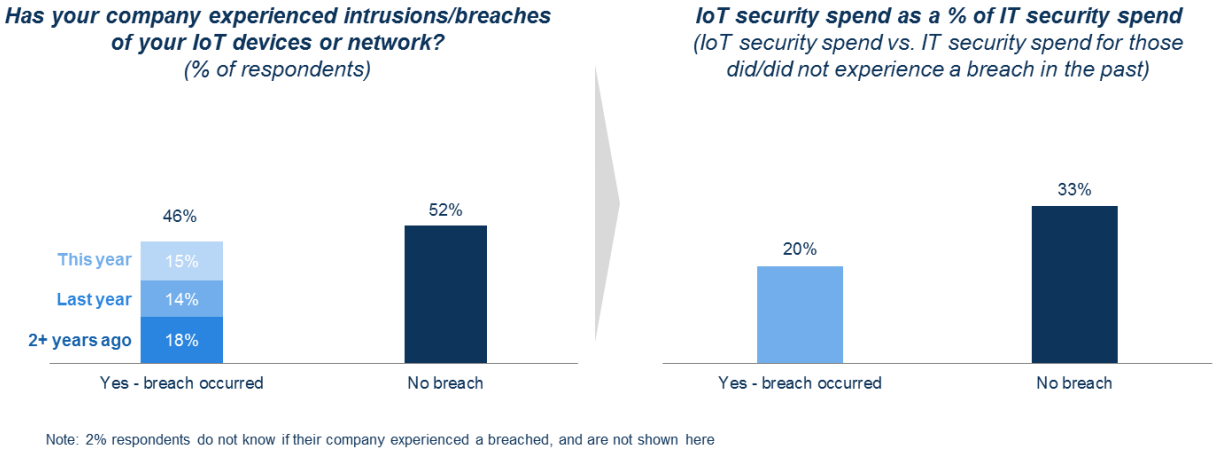
### The Internet of Things Is becoming an everyday reality for IT decision makers

Ranging from connected cars to "smart" street lights to asset tracking devices for industrial supply chains, the number of devices connected to the Internet or a corporate network is growing at an exponential pace. These connected devices, collectively called the "Internet of Things" (IoT), are projected to reach nearly 18 billion devices by 2022[1] – easily eclipsing mobile phones and tablets. As so often comes with exponential growth, there have also been growing pains. One of the greatest challenges has been security, both for the device owner and others. As we saw with the 2016 DDoS attack on DYN, security breaches in IoT connected devices can allow cybercriminals to shut down marquee Internet names such as Twitter, Spotify, and Reddit. This highlights the risk that even the largest companies face and the impact security breaches can have on the broader market.

### Investing in security yields results

As IT decision makers and senior business executives become increasingly aware of IoT security breaches and their ramifications, some have gone to great lengths to secure the devices and the data traffic on their IoT networks; others have not. The findings clearly show that companies spending more money to secure their networks are being breached at a lower rate. According to Altman Vilandrie & Co.'s 2017 IoT Security Survey, 46% of IoT security buyers have experienced an IoT related security intrusion / breach in the last two years, while 52% have not and 2% "don't know". Companies that have not experienced a security breach are dedicating 65% proportionally more budget to IoT security (33% of IT security budget vs. 20%). We expect continued investment across both leading and lagging companies. This aligns with market research by IDC showing IoT security spending will outpace more general Cybersecurity spending by 2.3x over the next 3 years (15.2% CAGR vs. 6.4% CAGR)[2].

[1] Ericsson mobility report, 2016; https://www.ericsson.com/assets/local/mobility-report/documents/2016/ericsson-mobility-report-november-2016.pdf
[2] Worldwide Internet of Things Security Products Forecast, 2016–2020; Worldwide IT Security Products Forecast, 2015–2019




## Top priorities: maintaining device control and protecting company data

There are several reasons why businesses look to secure IoT devices and networks. Most commonly, the survey respondents noted "*preventing loss of control over IoT devices"* as the top reason for buying IoT security. It makes sense that loss of control is the highest priority given the public safety issues involved. Take, for example, the IoT device exposure that left 1.4 million Jeep vehicles susceptible to hacking in 2015[3]. Breaches at first seemed to be only capable of controlling low-impact systems such as air conditioning. Later the vulnerabilities were shown to be much greater, allowing hackers to potentially control core driving safety systems, such as disabling brakes at low speeds and turning the steering wheel. A mass recall was issued in the form of a software update sent via USB stick to car owners. Jeep experienced not only the tangible financial losses of the recall, but also likely suffered in public image due to concerns that its vehicles were unsafe.


*Respondents noted "preventing loss of control over IoT devices" as the top reason why businesses purchase IoT security.*

After *"preventing loss of control over IoT devices"*, traditional cybersecurity concerns such as *"preventing breaches of customer information"* and *"preventing breaches of company data"* are ranked as the next most important

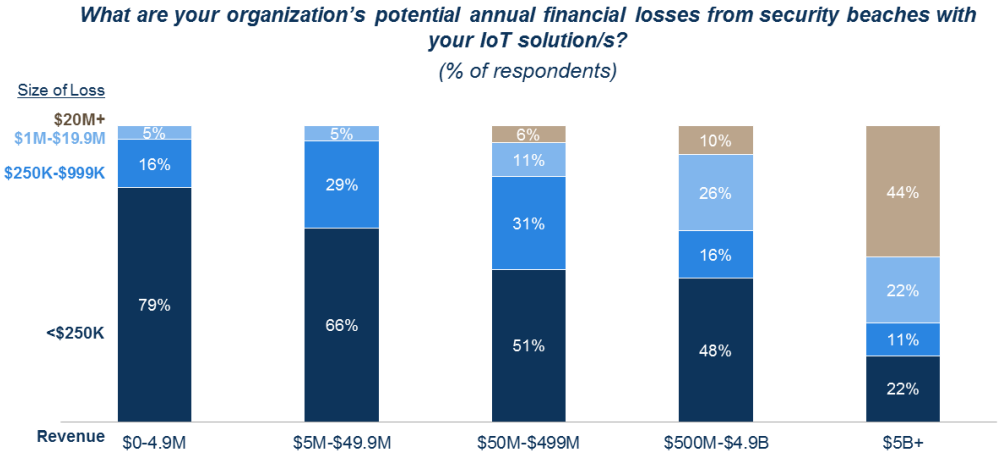
[3] Wired Magazine

reasons to adopt IoT security. We find that direct *"compliance"* and *"customer requirements"* are less likely reasons for adopting IoT specific security. Regulation could one day become more important, but to date is not the leading driver across all industries. There are, of course, several industries that indicate higher compliance-driven adoption, such as telecommunications and public utilities.

### Security incidents impact bottom line substantially

The impact of the attacks on IoT systems is substantial and the likelihood of those attacks is meaningful. Companies with less than $5M in company revenue report potential losses of $255K on average, were they to experience a breach. While this may appear small to some businesses, it represents approximately 13.4% of company revenues. Meanwhile, losses experienced by $5B+ companies can cost well above $20M. Regardless of company size, are at risk for substantial losses when their systems are breached.

> *Companies with **less than $5M** in company revenue report potential **losses of $255K** on average, were they to experience a breach.*

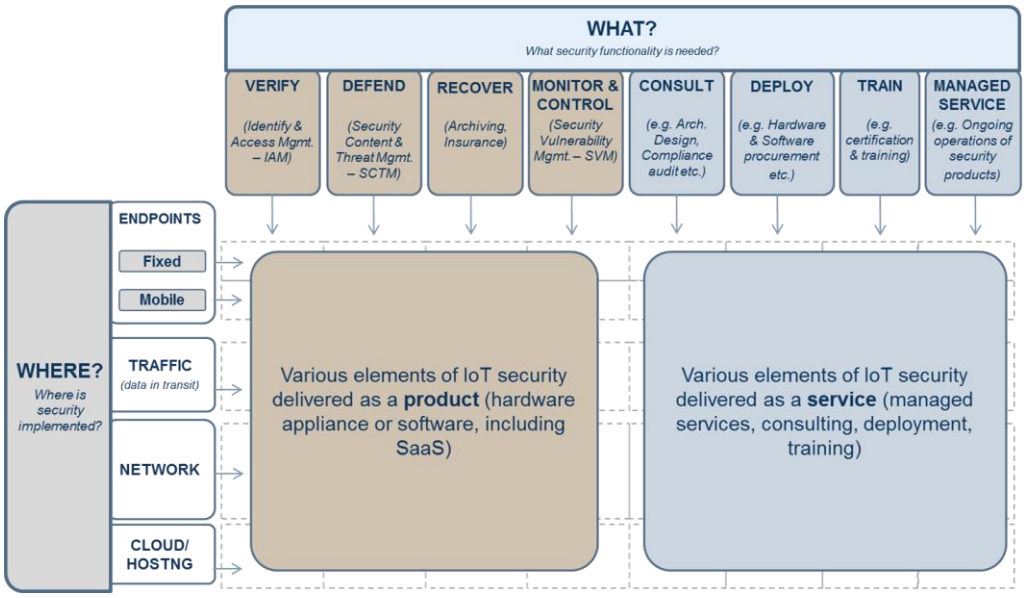



### Different products for different security needs

To protect against the attacks, businesses employ various kinds of security solutions. Our clients find it helpful when we categorize the complex set of security solutions into a framework based on *what* functionality is being provided and *where* in the IoT network topology the security solution being applied.

Certain products are designed to "Verify" the identities of users and manage access to IoT devices. Other products "Defend" secured content in ways like traditional firewalls, but including network intrusion detection and data loss prevention; this includes defense from attacks such as DDoS. Yet another set of products are classified as "Recover" to archive and backup data as well as provide insurance for security breaches. Finally, a set of products will "Monitor & Control" vulnerabilities to the network, alerting necessary parties to potential threats and providing visibility into the data flowing through IoT solutions.

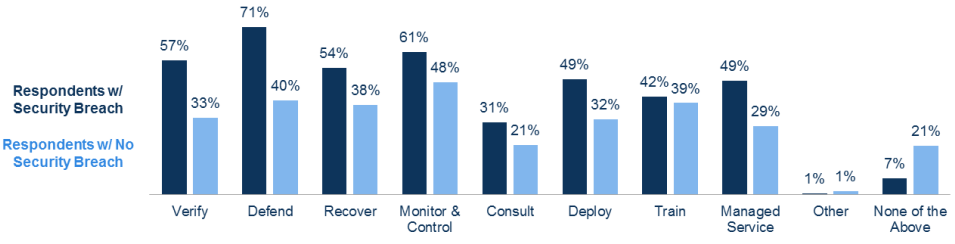
In addition to these product classes, there is a set of Professional Services solutions that are used to secure IoT solutions. These include "Consult" services to improve architectural layout and select vendors, "Deploy" services to install and setup devices with security, "Train" services to ensure employees are well-equipped to use IoT with best security practices, and "Managed Services" which deliver security end-to-end as a service.




### IoT security needs vary based on past experience with IoT security breaches

The types of IoT security products companies are looking to add varies based on past security breach experience. We see that companies without a past security breach tend to want to add *Monitor & Control* products to their IoT security suites in the next 1-2 years. Conversely, those that have experienced a breach look to *Defend* products to better secure their IoT networks.

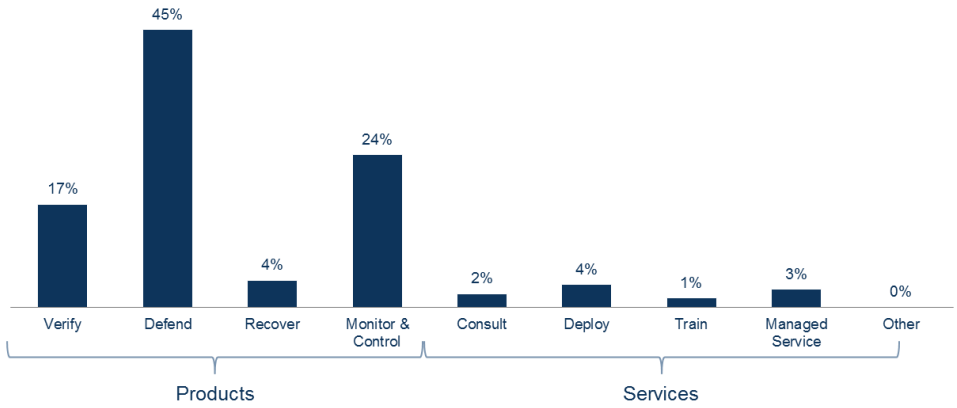
***Which of the following IoT security areas, if any, does your organization wish to add in the next 1-2 years?***
*(% of respondents who do not already have a solution in the given security area)*




In practice, products and services are often bundled together to achieve optimal security. Our survey finds that 70% of buyers prefer to purchase bundles of IoT security solutions rather than standalone. *Verify, Defend, Recover*, and *Monitor & Control* products are the most commonly bundled product categories. Of survey respondents that bundle, 45% of respondents indicate that they prefer *Defend* products to be the anchor of their bundle.

***What solutions do you consider the anchor solution for a bundled offering?***

*(% selecting each solution)*

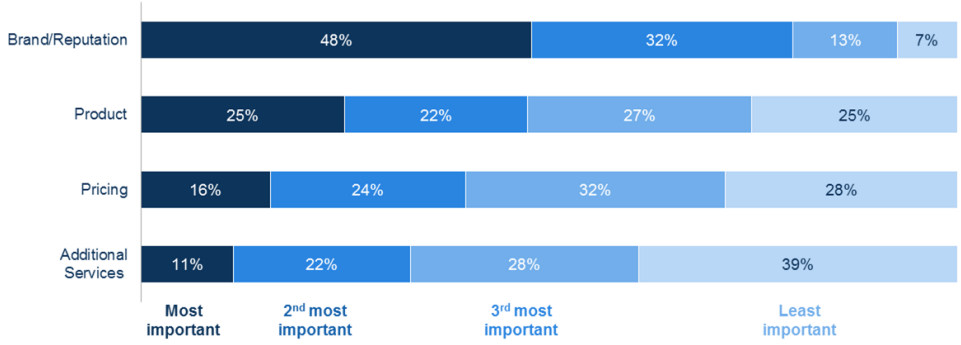



## Brand and reputation are the most important vendor selection criteria

Aside from identifying drivers of adoption and purchasing behavior patterns, we also examined how IoT security vendors are selected, and the criteria that are most important. A key finding is that participants in the survey look at *Brand & Reputation* of a vendor before considering product, pricing, or other factors. Building a brand in Defend and other important IoT security solution categories will be key to ensuring success for IoT security vendors.

***What are the most important selection criteria when determining the vendor for a given IoT security solution?***

*(% of respondents)*



### "Winners" are still being determined

Increased spending on IoT security will be driven by the sheer growth in number of connected devices and the importance of securing them. Successful vendors will need a broad solutions portfolio to provide and integrate the multi-faceted security bundles that companies want. "Defend" products are in the most demand, but will not work without a well thought-out set of verification, and monitoring solutions. Vendors will need to educate IT buyers on the importance of a complete solution that works together for maximum effect.

When working with our clients, we often find the most successful companies are those with a well-defined target customer and good alignment to that customer's needs across sales, marketing and product organizations. This can be a challenge for businesses in a rapidly changing environment, but is important for all of us since, as we saw with the DYN attack, we all have an interest in the Internet of Things.

*The most successful companies are those with a well-defined target customer and good alignment to that customer's needs across sales, marketing and product organizations.*

### Sources

The survey materials referenced throughout this whitepaper are from an April 2017 survey conducted by Altman Vilandrie & Co. The survey data includes responses from 397 IT decision-makers that have purchased some form of IoT security solutions. Respondents represented 19 industries. 63% of respondents are Director or Manager levels, with 27% representing C-suite or VP/SVP level. A diversity of company sizes were represented, with 25% of organizations less than $5M revenue, 33% between $5M-$49.9M of revenue, 20% $5M-$499M, 18% $500M-$5B, and 5% 5B+. Topics covered in the survey included IoT use cases, IoT security adoption, challenges solved by IoT security, exposure to IoT security incidents, demand for specific functionality, spend and budgeting for IoT security, vendor selection criteria, and bundled purchasing behaviors.

### About Altman Vilandrie & Company

Altman Vilandrie & Company is a strategy consulting group that focuses on the telecom, media, technology and investor sectors. The company's consultants are experienced in strategy, marketing, finance, M&A, technology, regulatory and operations disciplines. Based in Boston, with offices in New York City and San Francisco, Altman Vilandrie & Company enables clients to seize new opportunities, navigate mounting challenges, improve business performance, and increase investor value within complex and converging industries.

Ninety percent of the boutique firm's operator clients are large- to mid-cap companies including service providers, technology and software developers, and media companies. Altman Vilandrie & Company's financial clients include many of the largest and most prominent investors in the telecom, media and technology markets.

*Stefan Bewley, Ryan Dean, Adrien Fedida and Kevin Maxwell contributed to the development of this paper.*