IOT: WHY IT WON'T SUCCEED WITHOUT THE CHANNEL

By Michael Davis

APRIL 2016 | US$25

Channel Partners™

TABLE OF CONTENTS

Channel Partners™

ABOUT THE AUTHOR

linkedin.com/in/michaeladavis
@countertack

MICHAEL DAVIS, CTO for CounterTack, is responsible for driving the advancement of CounterTack's endpoint security platform, as well as leveraging his visionary approach to push defenders ahead of attackers. He has earned a reputation as one of the nation's leading authorities on information technology. The list of organizations that rely on his council includes AT&T, Sears, Exelon and the U.S. Department of Defense. Prior to CounterTack, Davis was president of External IT, a national managed IT and cloud services provider; founder of IT security consulting firm Savid Technologies; and senior manager of global threats at McAfee, where he led a team of researchers in cutting-edge security analysis. He was voted one of the "Top 25 Under 25" by BusinessWeek and is a contributing author to the best-selling computer security book, "Hacking Exposed," as well as "Hacking Exposed: Malware and Rootkits." He is a frequent contributor and speaker, including at Black Hat, Interop, SuperStrategies, Cloud Partners and Channel Partners, and InfoSecWorld.

IOT: WHY IT WON'T SUCCEED WITHOUT THE CHANNEL

By Michael A. Davis

CONVERSATIONS WITH ATTENDEES AT THE RECENT CHANNEL PARTNERS CONFERENCE & EXPO REVEALED A GAP

in understanding how the Internet of Things can lead to new and profitable services for customers.

It's time the telecom and IT channel got moving, because the IoT is far from theoretical. I was reminded of that just recently when a Ukrainian power company was attacked, leading to 80,000 customers losing power. In a previous role, I was the CISO of a large energy company that maintained thousands of devices for monitoring valves, the pressure of tanks filled with compressed gas and very remote pump stations. I witnessed the birth of the IoT firsthand and struggled with managing the first wave of devices being rolled out. Since then, the space has exploded in size, scope and complexity, so it's not surprising that partners are confused.

Don't be. Here's a little secret: The channel ecosystem is perfectly suited to own this market. The value of IoT for a business cannot be unlocked without cloud, managed services and telecom — your core competencies. All three must work together for IoT to deliver real-time, actionable, available-anywhere data. Lose one and the service collapses.

We'll talk about how to adapt existing managed services to deliver IoT to customers, but first, let's scope what we mean by "IoT," because the "cloudwashing" phenomenon is at work here.

IoT *is* custom-built devices that run operating systems that are accessible remotely and deliver real-time data. Think a pump running in a manufacturing plant or a heart rate monitor at a hospital, anythingcommonly referred to as the machine-to-machine (M2M) market.

IoT by the Numbers

5.4 Billion – Number of connected devices IoT will result in by 2020.

(Source: Verizon)

By 2019 – Total enterprise spending on security outsourcing services will be 80% of the spending on security software and hardware products, up from 50% in 2015.

(Source: Arbor Networks)

$140 Billion and **$112 Billion** – Amount manufacturers will invest in IoT and logistics firms, respectively, by 2021. Health care and retail are other rich markets.

(Source: BI Intelligence)

Up to 80% – Connected IoT devices currently deployed lack adequate security, with four in five devices on the market vulnerable to malicious or inadvertent attacks and data breaches.

(Source: AdaptiveMobile)

IoT *is not* a tablet or smartphone used by a consumer; you would be surprised how many "IoT vendors" claim these as IoT devices.

Not all IoT services need new strategies. For example, IoT-enabled digital signage or point-of-sale systems can be easily managed by most solutions providers. They really are not that complicated. Beyond these basics, we believe the M2M market is the ripest for entrance because uniqueness and scale make these services difficult for customers to handle internally. We'll explain.

THE IOT MANAGED SERVICE TRIANGLE

A three-legged stool is a wonder of physics. It's more stable than a four-legged stool and can sit stably on an uneven surface because the ends of the legs are always in the same geometric plane. A well-designed three-legged stool also positions each leg equidistant from each of the other two legs, creating a perfect triangle.

Likewise, if your company is missing one of the three elements of an IoT practice — cloud, telecom or managed services — we recommend you tackle that deficiency before moving into the IoT space. Otherwise your offering won't be stable, and you'll end up reliant on third parties that may not be able to deliver. Fly-by-night IoT consulting companies are cropping up like mushrooms, and you don't want your, or your customer's, business relying on them.

While much has been written about cloud, telecom and managed services individually, the unique challenges you must overcome to adapt them to the IoT market have gotten much less ink. Let's look at a few.

CLOUD SPECIALISTS REQUIRED

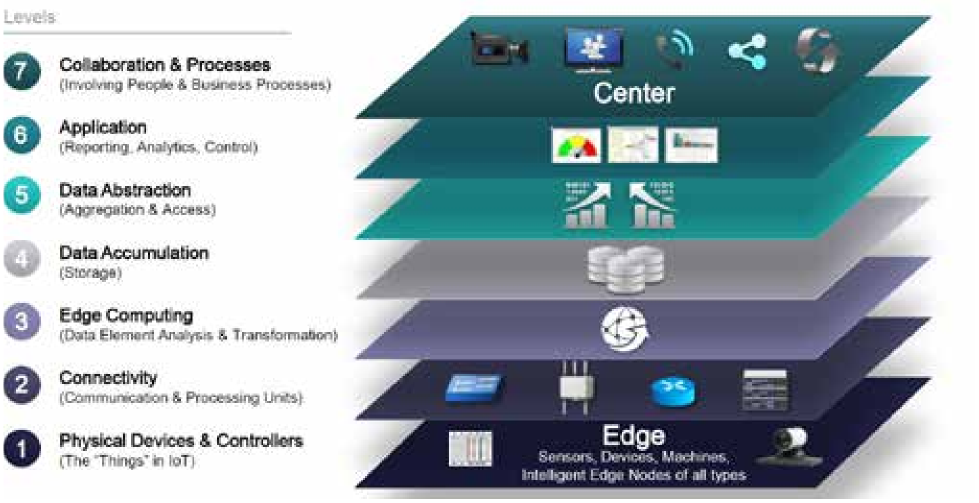
The skills required to put an M2M system into production are second nature for the channel. But unless you have in-house application development expertise, you will need to expand your portfolio to include custom M2M cloud platforms, such as Cisco Jasper, Sierra Wireless, ThingWorx or one of the many other platforms specific to an IoT hardware brand. While vendors such as Amazon, Google and Microsoft like to talk IoT, their cloud platforms are mostly used by developers of IoT software, not implementers.

Don't be put off by the hundreds of M2M cloud offerings; your value to a client is largely in understanding the nuances. It's not necessary to have deep technical expertise with each. These providers get that they need to minimize complexity. If you already have a cloud brokerage business, this is just an extension.

IoT-specific cloud platforms mostly do a common set of tasks, but in slightly different ways. On a macro level, they provide centralized device management; role-based access control; and most importantly, storage of the real-time data IoT devices generate, along with a way to access that data via a website or API.

Data is the reason most customers are in the IoT market in the first place — never forget that.

The New 7-Layer Model


Levels
7 Collaboration & Processes
(Involving People & Business Processes)
6 Application
(Reporting, Analytics, Control)
5 Data Abstraction
(Aggregation & Access)
4 Data Accumulation
(Storage)
3 Edge Computing
(Data Element Analysis & Transformation)
2 Connectivity
(Communication & Processing Units)
1 Physical Devices & Controllers
(The "Things" in IoT)
Center
Edge
Sensors, Devices, Machines,
Intelligent Edge Nodes of all types

Cisco, IBM, Intel and other members of the IoT World Forum Architecture, Management and Analytics Working Group collaborated on a reference model that breaks the IoT concept into seven functional levels: **Devices** send and receive data via **Network Connectivity**; data is normalized, and filtered using **Edge Computing** before landing in **Data Storage** and being **Abstracted** into a format accessible by **Applications**, which process data and provide intelligence to people who will **Act and Collaborate**. Source: Cisco

Depending on the type of IoT project, gathering device data in a central location accessible by the customer may be enough to make your offering a success. Other times, making full use of the device's capabilities will require you to build an analytics layer on top of the data.

Your customers also want visibility and control of IoT devices, but in our experience they'll be busy focusing on the data — and the business insights they can mine from it — and won't want to deal with deploying, configuring, securing and maintaining problem-prone hardware. That's where you come in. By leveraging these focused cloud platforms, you can provide a one-stop managed service that handles configuration of the wired or wireless connection the device is using to transmit data; deployment of devices to the field; inventory and maintenance of these devices, including firmware updates; and assurance that data is being recorded (availability).

Flexibility is key for an IoT offering. You can try to build a one-size-fits-all service that works across multiple industries, but you likely won't succeed. There are too many unique IoT devices and too many cloud platforms to make a cookie-cutter approach feasible. So, you have two options: Focus only on one vertical, or provide a base managed services offering that can be tailored to the needs of the customer.

We recommend the latter. Focus on building an offering in an abstract manner, tying alerting and management tasks together between different platforms using internal human processes and your existing RMM tools. This approach provides the largest revenue opportunity and forces the introduction of repeatable processes early in your managed services growth.

For example, we offered three tiers of managed services for IoT devices, ranging from simple availability monitoring at the basic level to full deployment, connectivity sourcing, technical support and even replacement services at the top end. IoT devices fail, some very frequently, because they tend to be subjected to high temperatures, vibration and even theft. The cost of replacement and provisioning can take a toll. We charged a simple per-device fee that wrapped everything together, but every package, while built from the same tiers, was customized to address the customer's specific IoT device needs.

CONNECTIVITY IS KEY

We cannot stress enough the value of connectivity as part of any IoT offering. For organizations to get the benefits, they need reliable and consistent delivery of data from IoT devices. Yet many sensors are deployed in remote locations, where options such as cable and DSL are not available, so normal routers and traditional PC networking practices may not work. That's where your expertise comes in. Few businesses have the telecom experience to know what type of circuits, MPLS lines or even private cell networks are available, from which carriers, and how to provision and manage them.

Most IoT devices send data to the related cloud platform via 3G/4G, Ethernet or dial-up, with many device manufacturers supporting all the above for failover. Your firm's ability to link these disparate and (in some cases) multicarrier connectivity options via a VPN or private cloud is key.

For example, I had a client for which we provided sensor monitoring for a small remote plant. The location had a local wireless network for the sensors. The system collected data and sent it over an MPLS circuit to the cloud platform. We sourced the circuit, set up a failover 3G connection because these sensors were critical and baked the entire sourcing effort into the monthly recurring revenue that we collected to monitor and manage the sensor devices. The MRR potential is significant, as discussed in-depth in our recent show issue.

We also performed failover testing every six months and provided a report to the customer, so they felt confident that data collection would be uninterrupted. When the blizzard of 2014 hit their area, the MPLS circuit had issues, but that 3G connection worked flawlessly.

One other point: Customers don't want to deal with separate carrier invoices. If you can roll the carrier costs into your monthly management fee (with a data cap) or at minimum have the customer pay you and you pay the carriers, it will simplify your sales process and increase stickiness. We strongly suggest you do this.

MANAGED SERVICES: 3 CONSIDERATIONS

When constructing an IoT managed service, there are a number of potential gotchas, from glitchy firmware upgrades to stringent government regulations on certain industries. Let's look at some areas to address.

Device Management: We mentioned earlier that IoT devices are not like PCs. Sensors are often subject to heat, cold, moisture, vandalism and other environmental challenges not found in a corporate cube farm. And, those challenges extend to the networking equipment supporting sensors. We suggest you partner with hardware vendors that provide hardened versions of their network gear. For example, CradlePoint, Fortinet and others provide ruggedized routers and switches.

Monitoring weather forecasts for areas where you support large concentrations of IoT devices isn't a bad idea, either, because big storms usually cause issues.

Beyond environment, the life cycle of an IoT device brings other challenges. Let's take one of the worst: firmware. If you support fleets of PCs, you've dealt with hundreds of desktop OS versions, applications and browsers, and thousands of related patches. In the IoT world, right now it isn't software so much as firmware that is your PITA. New updates come out regularly, but very rarely do IoT vendors have solid upgrade processes, and forget any consistency between devices. It's common to be unable to perform firmware upgrades remotely, and even if the manufacturer does officially support remote management, updates too often brick the device.

For that reason, many IoT vendors discourage firmware updates unless they're absolutely required. Unsurprisingly, that leads to massive security issues.

When a security flaw is identified within a certain version of firmware, most IoT vendors patch only the latest firmware version. That leaves a company that is a few revisions behind with a hard choice: upgrade older hardware and potentially cause a failure, or don't upgrade and be insecure. Sadly, most opt to remain insecure, leading to all manner of critical infrastructure problems. You may have heard about them in the news.

As a partner, you can help. Maintain a testbed of all versions of sensor hardware and test firmware upgrades in a lab environment before pushing them out. Once you've decided to push new firmware, make like a hawk and stay on top of the process to ensure upgrades go smoothly.

We predict that such a firmware practice alone will be a lead generator for the channel as organizations look to outsource their IoT devices to a MSP — security is top of mind, and new firmware revisions are coming out faster than ever before.

One other thing: Don't take device management lightly. IoT is about process at scale. Some IoT deployments have thousands or even tens of thousands of devices deployed and sending data to a cloud platform. That's great for your per-device revenue model. But as sensor fleets get more diverse, management must become more structured.

And diversity isn't just about hardware. IoT sensors currently tend to use proprietary operating systems written by the manufacturer. This is changing. Many new devices are running Linux, Android and, soon, stripped-down versions of Windows, with the attendant issues. We expect software patching to become a requirement for IoT devices within the next 24 months as more manufacturers opt for commodity hardware and firmware and simply want to be software developers on top of these devices.

Imagine the Windows or iOS/Android mobile app upgrades you do now happening on thousands of IoT devices, some of them finicky and situated miles away from civilization.

Now, most solutions providers have dealt with software patching for years and have a good handle on the process, so don't fret. But do realize this leaves your company with a stack of problems: patching plus the firmware issue multiplied by potentially hundreds of thousands of devices. Be prepared and ensure your processes are documented and followed religiously from the start. Don't think you can build them later.

Then there's pricing the service properly. Because IoT devices fail more frequently compared with traditional computing systems, there is more work to be done, more often. So when developing your managed service, don't leave money on the table. At a minimum, provide availability monitoring of devices as well as reporting on system details such as IP, location and firmware versions. Then, be creative in regards to your fuller feature sets. Perhaps keep a certain amount of inventory on

industrial internet CONSORTIUM

Standards Watchdog

In an effort to encourage IoT standards, AT&T, Cisco, GE, IBM and Intel formed the Industrial Internet Consortium in 2014. The group now includes 230 members, including Dell, Ericsson, HPE, Microsoft, Oracle and Symantec. Notably missing: Apple and Verizon. While the IIC doesn't develop standards itself, it does look to "influence the global standards development process for internet and industrial systems to improve the integration of the digital and physical worlds," from location of sensor devices to data exchange, storage and predictive analytics. GE says that the "Industrial Internet" (its term for IoT) will add $10 to $15 trillion to global GDP by 2035.

hand so you can guarantee replacement within a set number of hours, 24x7. Offering secure decommissioning of devices with written certification that data was removed is another add-on that will be lucrative in many verticals.

Security and Availability: Monitoring for availability is a must, but don't simply provide reactive reporting to your customers. Head off problems by delivering advanced alerting on more than just the device itself. One company worked with a client to be the first-level responder for monitoring critical irrigation sensors. Whenever a certain threshold was met, they would be the triage team — contacting the customer, getting the proper repair team on the phone, pulling the pin on emergency measures if needed. By developing and managing an emergency plan, the provider freed the client to focus on other tasks.

As for security, remember: IoT sensors usually have hooks into the client's — or your — network via VPN or direct connection, so it's critical to keep an attacker from getting control of one of these devices. Properly architecting, designing and assessing the security of IoT devices and connectivity must be part of your offering. We recommend periodic assessments by a neutral third party, but the architecture and configuration of security, such as on network segments, firewalls and even antivirus (yes some IoT devices run AV) adds strategic value.

Be aware of regulations. If a customer is among the 21 critical infrastructure companies as defined in the U.S. Presidential Policy Directive 21 — think financial services, energy, water and wastewater systems, dams — they may be required to implement some of the security controls outlined above following the NIST Cybersecurity Framework. That framework requires a continuous monitoring approach to IoT device security, an effort that an MSP can perform on behalf of the customer.

Providing monthly reporting and attestation that devices adhere to the customer's security controls or the NIST CSF is an excellent way to differentiate your service.

One area of IoT security that is often overlooked is initial configuration. Many IoT devices do not, by default, use secure protocols, such as SSL and TLS, even though they have the option to do so.

Furthermore, securing access to the devices themselves is often overlooked. Enabling SSH instead of telnet and using unique and strong usernames and passwords, seemingly no-brainers in today's PC age, are not always top of mind for IoT systems. Don't let this slip: Many of these devices control access to physical infrastructure, and a breach can cause real physical harm, not to mention damage to the customer's brand.

As an MSP with an IoT practice, understanding what is and is not possible with each and every individual IoT device does take time. Expect to invest in research and meetings with vendors, but it must be done. Adding this expertise as part of your standard provisioning and deployment process upfront can save the client from significant security issues later.

Don't forget to assess your cloud platform and connectivity providers, too. If data is transmitting to a third party or over a provider's network, their security matters. Regular audits of the cloud provider should be a standard part of your IoT service. In each audit, validate that the provider is securely configuring its platform for your customers, especially when it comes to logins and identity and access management. Require two-factor authentication for access to any account or platform that gives the user the rights to update, reset or reconfigure a device. I am constantly amazed at how many organizations give administrative logins to users that need only read access to the data generated by the device. In one case, that changed fast when someone accidentally clicked the "reload" button, which reset a device that was five hours from the nearest local field technician, because they thought it reloaded the data.

Related Reading

News

- Cisco Wraps Jasper Buy, Ready for Next Step in Cloud IoT
- AT&T Highlights IoT Growth, Opportunities for Channel
- Altaworx Debuts Agent Program for IoT, M2M

Reports

- The Internet of Things: Securing the Next Communications Frontier
- DDoS Attacks: Protecting Customers Demands Preparation
- 4G LTE: Capable Network Backup for Remote Locations

PCs, servers and mobile devices generally don't cause physical damage or injury when they don't work properly. Arguably, if any given PC goes south, it's not the end of the world because we have mature management in place using technologies like the cloud, real-time backups and operational process that prevent any single device from being critical to the business.

IoT is not that mature. Every lesson we should have learned from the PC era, and then the mobile and BYOD age, has, apparently, been forgotten. Sloppy management is happening again at a massive scale. You can do better, but it requires diligence, upfront planning and design by your team and then consistent execution to ensure IoT devices are operating 24x7 as they should.

While moving into the IoT market seems confusing, the reality is that the skills your team has developed by being an MSP, a CSP or a telecom agent are the exact building blocks required for a successful IoT practice. Start small, with systems that use a few sensors deployed near your office and simple protocols such as Wi-Fi before launching into remote rugged sensors using 3G cell connections in Alaska. Adapt existing processes to match the IoT life cycle, and ensure your team has mastered all three legs of the IoT managed services triangle — cloud, telecom and managed services — before attempting to build an IoT practice.