CompTIA

Business of Technology Use Case: **Cybersecurity**

To help accelerate the adoption of emerging technologies, CompTIA has created a series of use cases that highlight examples of solving real-world business problems and how you can do the same.

How to Succeed in IoT Security

Hard-luck opportunity opened the door for an MSP to save the day and gain a loyal customer

In this edition, learn how a traditional MSP added IoT security expertise into its business, solved a client's challenges and scaled its business to generate additional revenue.

OVERVIEW

Syber Networks, a Las Vegas-based managed solutions provider, has long preached the need to protect data on any device, including personal devices that access company information. But one construction customer didn't want to listen and learned a hard lesson after an employee's mobile phone was stolen out of a gym locker. The mistake may end up costing the company millions of dollars in business, but it helped Syber Networks effectively demonstrate the value that Internet of Things (IoT) technology and cybersecurity can mean to a business—a lesson learned that's paved the way for a better relationship.

CHALLENGE

Syber Networks was founded as a traditional managed services provider and developed a strong security practice as hacking and cyberattack risks increased over time. Like many MSPs, Syber Networks is challenged getting customers to truly understand and appreciate the importance of investing in security—and the risk of not doing so. The MSP's experience is not unique. In its "Cybersecurity for Digital Operations" research report, CompTIA found that 55% of executives were completely satisfied with their current cybersecurity solution. By contrast, only 35% of the IT staff were completely satisfied, indicating that those in charge may not comprehend security risks as much as their own IT staffs.

To that end, one Syber Networks prospect sat on a cybersecurity proposal for months—until the MSP got a call that one of the company's employees had a mobile phone stolen. The unsecure phone gave the thief direct access to the construction company customer's Exchange Server and OneDrive—and information on upcoming construction projects the company was bidding on. The MSP previously recommended implement PIN codes for employees' phones, but the client the client didn't want to force employees to do so. Syber Networks quickly

disabled the credentials remotely once the phone was reported stolen to management, but the damage was done. Over time, the construction firm learned that it had been underbid on millions of dollars in projects, losing many of them to the same rival firm."We're pretty sure someone stole the phone for the information on it and the competitor downloaded our information," said Rory Jackson, president of Syber Networks. "The good news is the company is now ready to focus on security gaps on any and all devices that touched its network."

SOLUTION

Syber Networks had previously identified security and IoT technologies as priorities to help transform the company and keep it relevant long term with customers. The MSP invested in new software tools to analyze IoT devices and their vulnerabilities, as well as research and training for staff to learn IoT tech and how devices and sensors communicate.

After the theft of the mobile phone, Syber Networks reviewed their previous proposal with the customer. The company agreed to implement two separate Wi-Fi/LAN networks for all wired and wireless IoT devices, networks that had no access to internal resources. One network covered all thermostats, HVAC and a solar power controller. The second network covered all BYOD devices and company-issued mobile devices, including Office365 for email.

Separate firewall policies were created for each network. The first network's policies were based on the needs of the device and what the IoT device needed to access, including IP address, domain names and specific ports. They also added geolocation blocking as it was discovered the HVAC system was curiously sending packets to China. Devices under the second network would allow access using a new management portal with specific policies in place to minimize risk from user behavior. All devices now must be approved by IT and are required to adhere to new security enhancements and policies—including a pin code for mobile devices. Syber Networks monitors the health of all connected devices through Microsoft Intune, further supporting the client.

OUTCOME

Unfortunately, the construction customer learned the hard way that IoT security is important, but Syber Networks' response helped and even solidified the relationship. The customer is ready to invest in additional software for project management and construction management that require two-factor authentication as a much-needed additional security layer, Jackson said. It also gave Syber Networks an example to use with other clients reluctant to invest in security.

"It can be hard to get clients to understand the importance of IT security. Too many businesses think they're 'OK' and don't need security, but it's critical to continue to communicate the potential risks to build trust," Jackson said. "Predicting these trends and getting ahead of them instills a sense of high confidence with clients. We built a relationship upon the notion that we were keeping them secure by being proactive when it came to IoT." Investing in IoT security solutions has helped Syber Networks

> "You have to look at IoT security and IT security as cheap insurance. You're paying a small monthly fee vs. paying out to ransomware or losing millions in business to a competitor."
>
> ~Rory Jackson

differentiate itself from other MSPs that haven't developed that skill. "We've added a few customers because of their high use of IoT devices in their business, but **mostly** we were able to add it to our current offerings and sell it as a new solution to our customers," Jackson said. "We're also now doing two-factor authentication where applicable, such as company VPNs or Office 365."

> "Too many businesses think they're 'OK' and don't need security, but it's critical to continue to communicate the potential risks to build trust."
>
> ~Rory Jackson

SUMMARY

The example of a stolen phone demonstrates the importance of talking to customers about cybersecurity, but more specifically about IoT and mobile security. Cellphones may not fit the popular notion of a typical IoT device, but they very much are just that, Jackson said. Solution providers that don't market themselves as cybersecurity, mobile or IoT experts are missing out on opportunity. If you don't have the skills now, find a partner while you develop them and take advantage of resources like CompTIA's resource hubs around IoT, cybersecurity, and more.

"It's one thing to tell someone that they need stronger security, and show them how someone can get in, but if you can show them a real-world example, they tend to listen more closely," Jackson said. "Too often, it isn't until something happens that someone will act. You have to look at IoT security and IT security as cheap insurance. You're paying a small monthly fee vs. paying out to ransomware or losing millions in business to a competitor."

ADDITIONAL RESOURCES

How to Become a Trusted Business Partner: An IoT Use Case
https://www.comptia.org/content/use-cases/turning-new-regulations-into-iot-opportunity/

2019 Trends in Internet of Things
https://www.comptia.org/content/research/iot-industry-trends-analysis

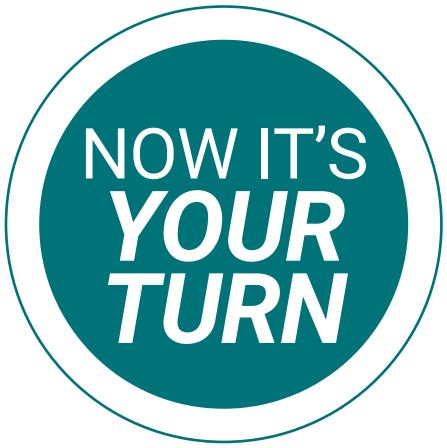
Business Opportunities in Emerging Technologies: Internet of Things
https://www.comptia.org/content/business-opportunities-in-emerging-technologies-internet-of-things

2020 Emerging Technology Top 10 List
https://www.comptia.org/content/infographic/2020-emerging-technology-top-10-list

10 Emerging Technologies Making an Impact in 2020
https://www.comptia.org/blog/emerging-technologies-impact-2020

4 Things to Know About Emerging Technology
https://www.comptia.org/blog/4-things-to-know-about-emerging-technology

CompTIA



It's a constant challenge to convince customers that innovative technologies can help them be more efficient, effective, and secure. But developing solutions incorporating emerging tech such as IoT into your current portfolio can build closer relationships with customers and solve real-world business problems. Here are some next steps to take within your own organization.

Embrace the idea of introducing new technologies and solutions to customers. Research, educate, and train your teams on how the tech can help you grow the business and increase customer loyalty.

Identify gaps or missing elements in your customer's existing infrastructure, including opportunities to make them more productive and secure.

Talk with your customer about how the technologies fit into larger solutions to solve specific business problems.

Once the solution has been successfully implemented, continue the conversation, and talk about additional opportunities to work together. Develop a strategy for long-term support.