ATA BUSINESS AMPLIFIED + ATA SECURE

Understand why you need IT security

By Jon Joyner, COO of ATA Secure

I am a regular attendee of the UTA conference for Tennessee's Utilities. When you run a booth at a conference, you tend to have minutes (if not seconds) to give someone you just met a piece of advice. My job is IT security. When I have only seconds to give someone advice regarding IT security, I tend to echo the phrase "Understand why you need IT security". There's a lot of truth in that statement.

When I say "understand…", I'm not telling utility managers and staff to get the technical details of IT security. I have watched plenty of utility managers nearly go cross-eyed when an IT security professional rattles off terms like UTM, packet inspection, cloud computing, encryption, and DDoS attacks. You could spend a lifetime learning those concepts. Instead, I am trying to get those individuals to think about what needs to be secured and how vulnerable those systems can be.

I see it quite a bit when I perform security assessments for utilities. Enhancements like AMI, wireless, and fiber networks can provide a lot of improvements for utility operations. Often, these improvements are sold with the promises of more efficient and accurate billing systems, faster response times, and even the ability to cut-off non-paying customers without going to their homes. Sounds fantastic. However, these improvements almost always result in security deficiencies as well.

AMI is a game-changer for utilities. The ability to bill, cut-off, and provision customers without leaving your building is incredibly useful. However, implementing AMI can result in remote access needs for vendors, additional VPNs, more endpoints within your network to be compromised (read 'hacked'), and an overall increase in an attack surface. This rule is a nearly universal rule for IT.

Adding components to your computer systems can very easily create large security issues. AMI also seems to couple with the deployment of fiber of utility poles.

Fiber networks are good investments for utilities and can provide an excellent pathway for AMI gateways back to billing systems. However, fiber build-out in your plant means you might have extended your corporate (production) network out to your customers. I see fiber networks following the model that wireless networks have provided.

Wireless networks are not even optional at this point; if you want to be a competitive organization these days, you must provide wireless networking. However, a poorly deployed wireless network means the inquisitive 12-year old that lives a block away from the utility has a new network to explore

Imagine a situation in which a new utility has deployed an AMI solution. In the process, a firewall had to be reconfigured to allow the AMI vendor into the network. This firewall change was implemented quickly (and hastily), and as the utility began to reach the end of the AMI deployment, an associated computer system was suddenly breached, data on said systems was encrypted and ransomed, and the utility had to stop AMI deployment immediately to address a true business disaster.

The actual cost of the AMI deployment was not simply the invoice from the AMI vendor. The true cost of the AMI deployment would be the cost of the AMI and cost of the network breach (not considering the loss of goodwill and public opinion).

Am I blaming AMI vendors, wireless networks, and fiber deployments? Absolutely not. These technologies are relatively young, and it can be difficult to conceptualize what the risks can be when improving a network. Utility managers cannot be asked to analyze the IT security of a system and understand the nuanced risks that come with technological changes. That's where IT security professionals can help.

When I mention "understand why you need security", I really mean that utility managers should look at IT security as an investment just as they would AMI, wireless networks, and fiber deployments. IT security can take the shape of security audits/risk assessments, penetration testing, policy and procedure review, PCI DSS requirements, and even some managed services solutions.

Utility managers should strongly consider having a periodic risk assessment performed simply to understand how at-risk their network has become. When you are reviewing the deployment of any technological improvements, consider having a simple risk assessment performed before and after the deployment.

These assessments will help you and your IT department/consultants understand exactly what solutions should be implemented. A risk assessment can be performed in as little as a few days by a good security auditor. As part of the audit process, you should receive a written report of findings that you can review over time.This risk assessment can be a requirement for your insurance application.

If you are not working with a trusted IT partner, contact ATA Secure. We have worked with numerous utilities, local governments, and private organizations to harden their IT security controls, perform risk assessments, PCI DSS mandates, and even in establishing an appropriate cybersecurity insurance policy. We are passionate about security and more than eager to help.

Take the next step.


info@atacpa.net

www.atacpa.net


731.664.0102

ATA is a long-term business advisor to its clients and provides other services that are not traditionally associated with accounting through its Family of Firms. For example, Revolution Partners, ATA's wealth management partner gives financial planning expertise; ATA Technologies provides trustworthy IT solutions; ATA Secure equips businesses with cybersecurity; Sodium Halogen focuses on growth through the design and development of marketing and digital products; Adelsberger Marketing offers video, social media, and digital content for small businesses; and Center Point Business Solutions is a comprehensive human resource management agency.