SMART GRID FORUMS: COMBATTING RANSOMWARE ATTACKS

Emil Gurevitch

Background

Vulnerability Research & Penetration Testing

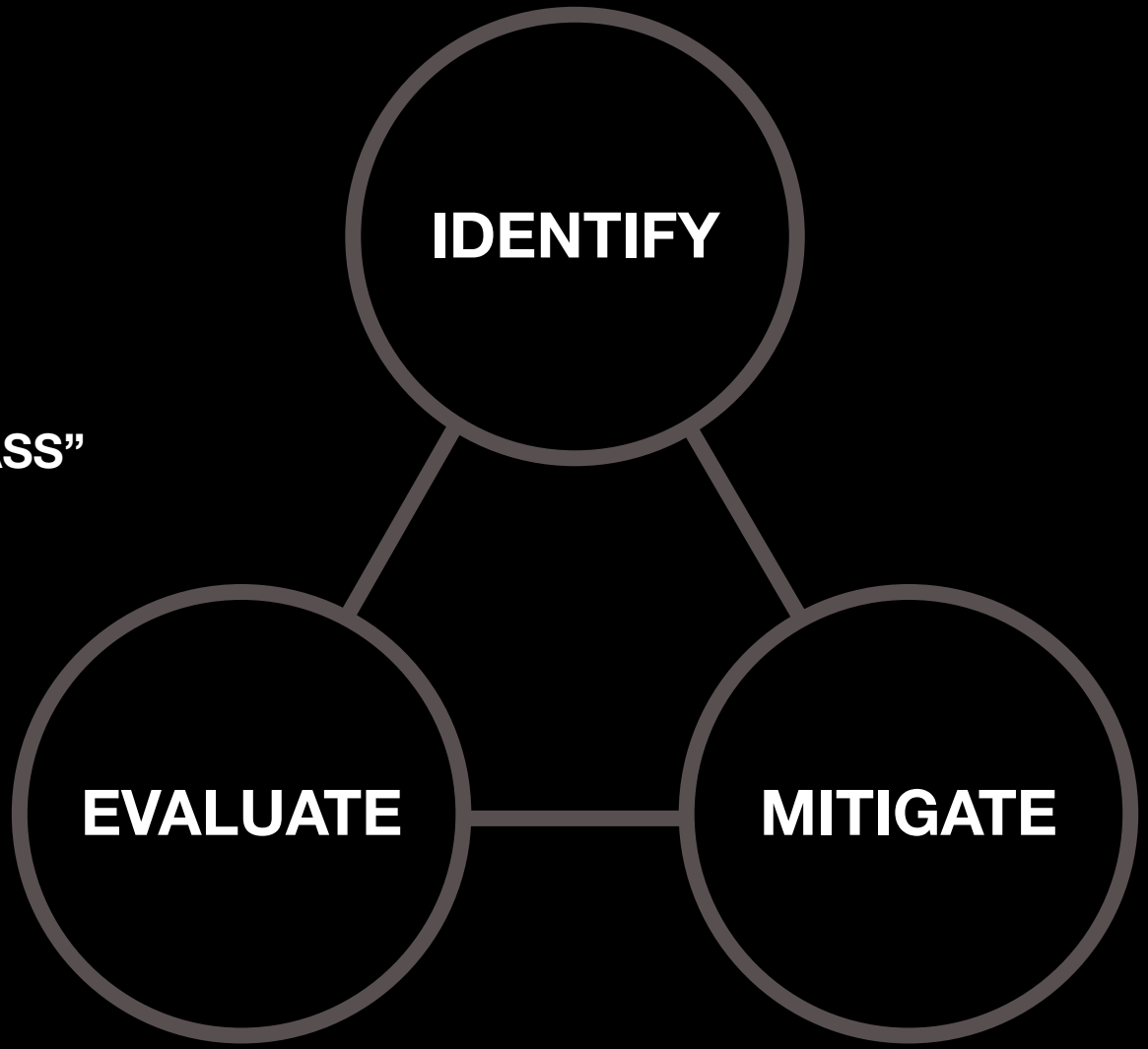
SMART GRIDS

Product Security & Threat Detection Solutions

Fundamentals

Cybersecurity is all about effective risk management

"THE SECURITY COMPASS"



There is already a lot of good actionable guidance on how to mitigate ransomware attacks, use it!

cisa.gov/ransomware

1. **Secure, full-system, off-line backups** that work
2. **Build a culture of security** within your company to mitigate social engineering attacks
3. **Patch systems and software**
4. **Invest in effective monitoring and threat detection** so you know when you have been breached
5. Develop and Test **Incident Response Plans and Business Continuity Plans**
6. **Perform penetration testing** to find your vulnerabilities

…

Real-world example of what good cyber risk management looks like

Utility X picked up on new threat intel: criminals are hacking smart meters for financial gains

KrebsonSecurity
In-depth security news and investigation

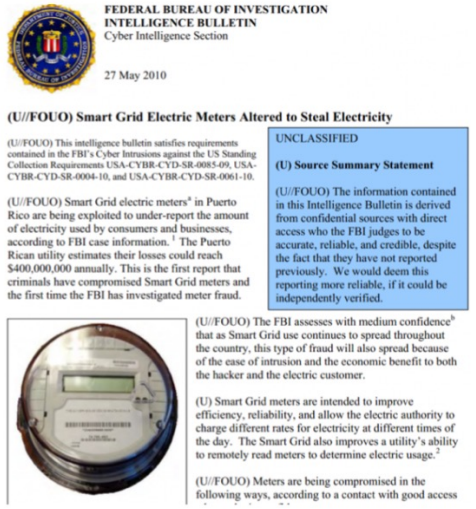
09 FBI: Smart Meter Hacks Likely to Spread

APR 12

A series of hacks perpetrated against so-called "smart meter" installations over the past several years may have cost a single U.S. electric utility hundreds of millions of dollars annually, the **FBI** said in a cyber intelligence bulletin obtained by KrebsOnSecurity. The law enforcement agency said this is the first known report of criminals compromising the hi-tech meters, and that it expects this type of fraud to spread across the country as more utilities deploy smart grid technology.

Smart meters are intended to improve efficiency, reliability, and allow the electric utility to charge different rates for electricity at different times of day. Smart grid technology also holds the promise of improving a utility's ability to remotely read meters to determine electric usage.

But it appears that some of these meters are smarter than others in their ability to deter hackers and block unauthorized modifications. The FBI warns that insiders and individuals with only a moderate level of computer knowledge are likely able to compromise meters with low-cost tools and software readily available on the Internet.



FEDERAL BUREAU OF INVESTIGATION
INTELLIGENCE BULLETIN
Cyber Intelligence Section

27 May 2010

(U//FOUO) Smart Grid Electric Meters Altered to Steal Electricity

(U//FOUO) This intelligence bulletin satisfies requirements contained in the FBI's Cyber Intrusions against the US Standing Collection Requirements USA-CYBR-CYD-SR-0085-09, USA-CYBR-CYD-SR-0004-10, and USA-CYBR-CYD-SR-0061-10.

(U//FOUO) Smart Grid electric meters[a] in Puerto Rico are being exploited to under-report the amount of electricity used by consumers and businesses, according to FBI case information.[1] The Puerto Rican utility estimates their losses could reach $400,000,000 annually. This is the first report that criminals have compromised Smart Grid meters and the first time the FBI has investigated meter fraud.

UNCLASSIFIED

(U) Source Summary Statement

(U//FOUO) The information contained in this Intelligence Bulletin is derived from confidential sources with direct access who the FBI judges to be accurate, reliable, and credible, despite the fact that they have not reported previously. We would deem this reporting more reliable, if it could be independently verified.

(U//FOUO) The FBI assesses with medium confidence[b] that as Smart Grid use continues to spread throughout the country, this type of fraud will also spread because of the ease of intrusion and the economic benefit to both the hacker and the electric customer.

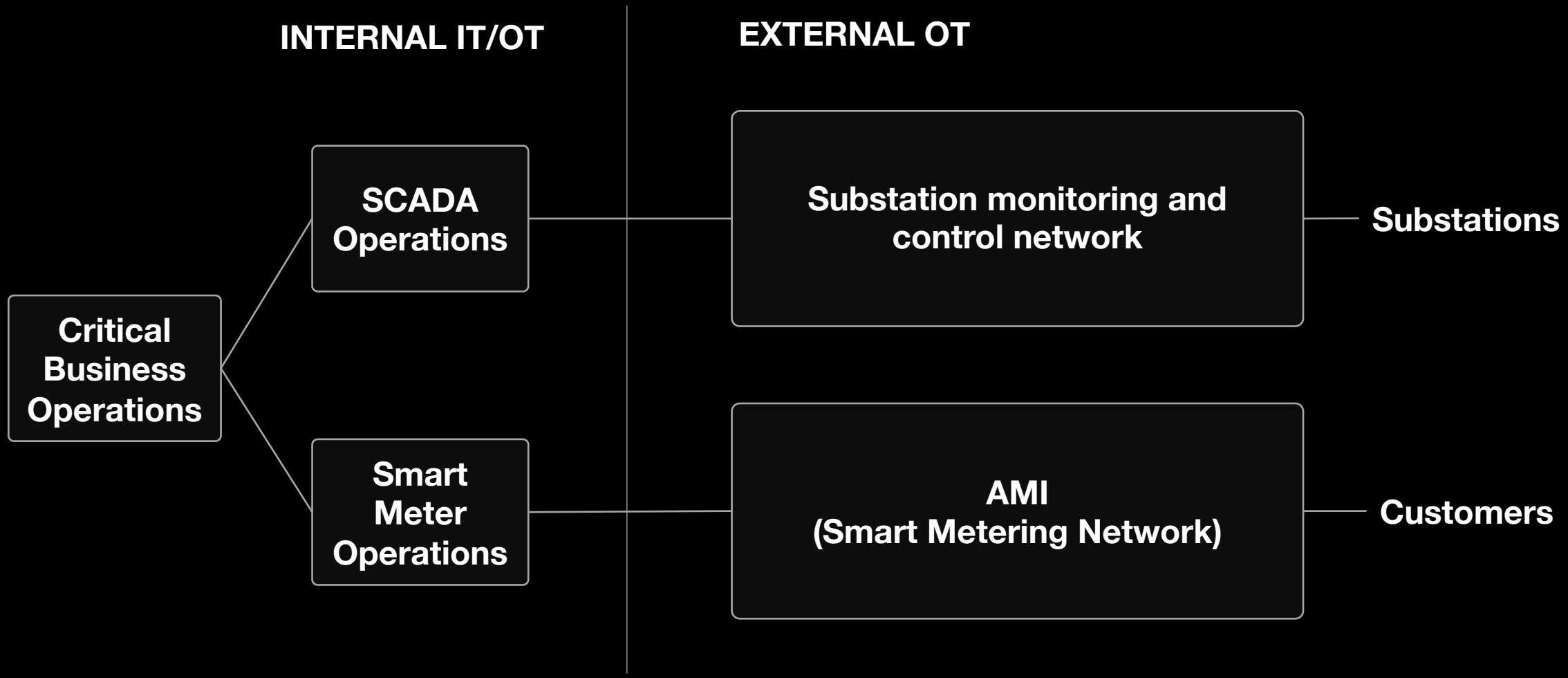
(U) Smart Grid meters are intended to improve efficiency, reliability, and allow the electric authority to charge different rates for electricity at different times of the day. The Smart Grid also improves a utility's ability to remotely read meters to determine electric usage.[2]

(U//FOUO) Meters are being compromised in the following ways, according to a contact with good access

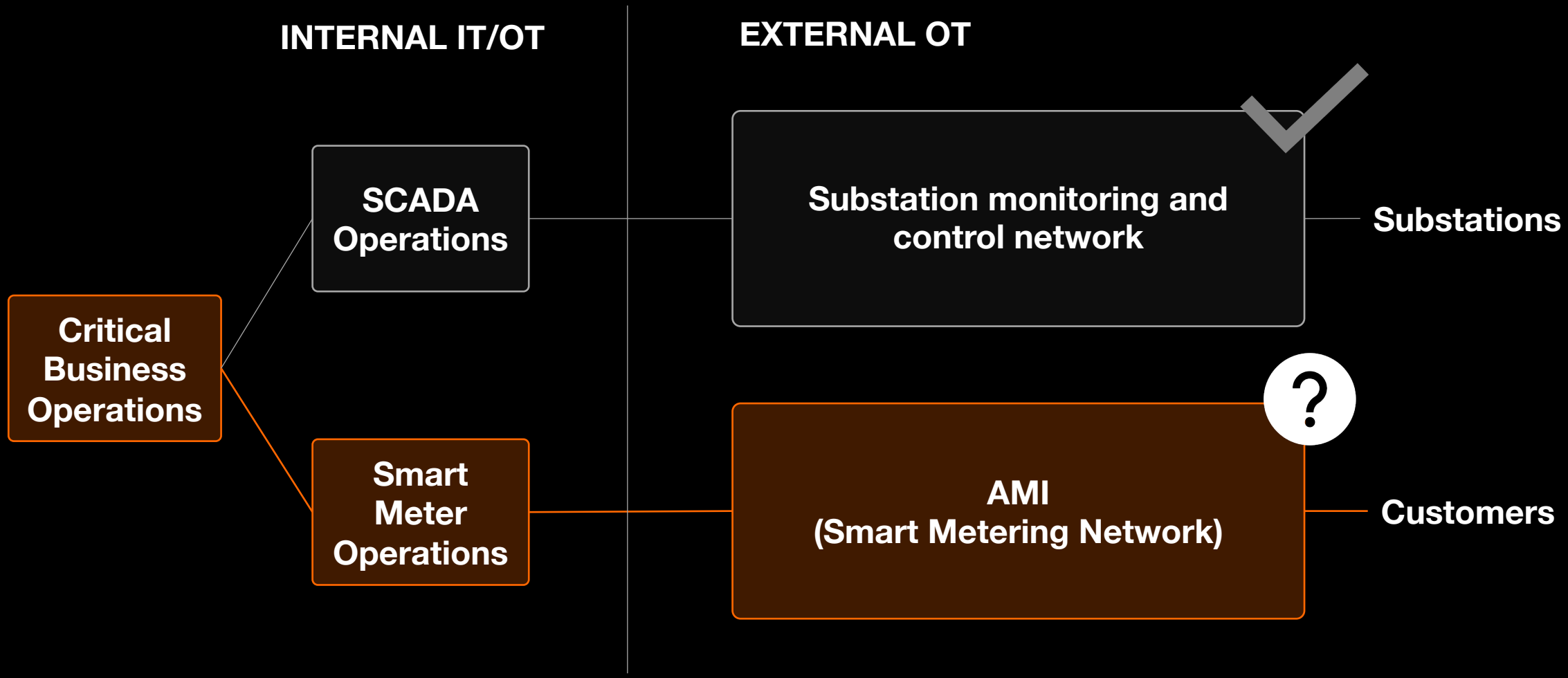
Part of an FBI alert about smart meter hacks.

OSGP ALLIANCE
Networked Energy Services

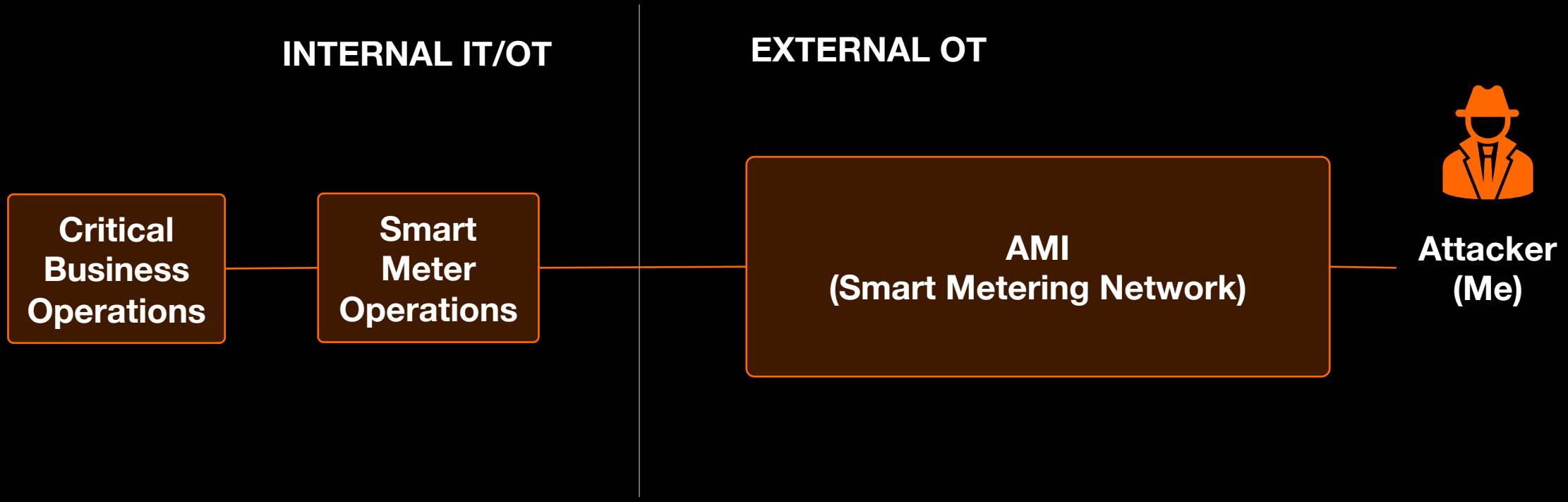
Utility X re-assessed their systems to better understand the risk of these new “smart meter hacks”



Utility X wanted to understand the cyber risks associated with their external smart metering system



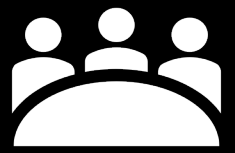
Utility X invested in a comprehensive pentest-driven risk assessment of their external smart meter network



Outcomes

Fixes and improvements

Better prepared for attacks



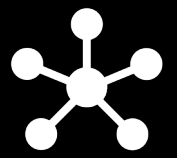
Better awareness of smart meter cyber risk

The smart meter system checks all the boxes for future ransomware-style attacks

Essential for business-critical processes

Remote on/off switch

Energy consumption is personal data (GDPR)



External network is exposed and is slow to patch

Key Takeaways

- To mitigate today's ransomware attacks, focus on the fundamentals—take a risk-based approach and follow available guidance
- For tomorrow's ransomware attacks, pay attention to the smart meter network as it may not be receiving the attention it deserves
- I hope you will share your concrete examples of successes or failures so we can all improve — the bad guys share their work, so should we!

See you at the Q&A!

Emil Gurevitch
Emil.Gurevitch@networkedenergy.com

networkedenergy.com osgp.org