TESCO METERING

Understanding Cybersecurity Threats to Utilities

July 23, 2025

9:45 AM – 10:15 AM

Alex Kobrenko

TESCO's Meter School

TESCOOL

TOP 5 GENERAL THREATS

1. Ransomware
2. Phishing
3. Cloud Intrusion
4. Device Attacks
5. DDoS

Source: SentinelOne

TOP GENERAL CYBERSECURITY THREATS

1. RANSOMWARE

- 35% of all attacks were ransomware, which increased 84% over the previous year.
- Ransomware increased by 15% in North America while it declined by 49% in EMEA(Europe, Middle East and Africa)
- 70% of the ransomware targeted SMBs

Source: SentinelOne

2. PHISHING

- Phishing attacks increased by 1,265% driven by growth of Gen AI
- Many targeted cyberattacks start with emails, and 40% of all email threats are phishing attacks
- Business email compromise accounted for 6% of incidents, with spear phishing links used in 50% of the cases

Source: SentinelOne

3. Cloud Intrusion

- Cloud intrusions increased by 75% in 2023
- 23% of cloud security incidents can be attributed to cloud misconfiguration, and 27% of businesses encounter security breaches in their public cloud infrastructure
- Over half of the organizations reported phishing as the most prevalent attack for stealing cloud security credentials

Source: SentinelOne

TOP GENERAL CYBERSECURITY THREATS

4. DEVICE ATTACKS

- In 2023, attackers commonly used edge gateway devices to break into the network without getting noticed
- Only 4% of organizations consider their internet-connected devices and associated technologies secure

Source: SentinelOne

5. DISTRIBUTED DENIAL OF SERVICE (DDOS)

- DDOS attacks increased by 31%, with cybercriminals launching an average of 44,000 attacks daily in 2023
- The Federal Bureau of Investigation (FBI) shut down 13 DDoS-for-hire marketplaces in the first half of 2023. Similarly, in July 2024, United Kingdom(U.K.) authorities disrupted DigitalStress, an illegal service for launching DDOS attacks

Source: SentinelOne

TOP 5 SPECIFIC THREATS

1. Advanced Persistent Threats
2. IoT/Smart Infrastructure Vulnerabilities
3. Supply Chain Attacks
4. Physical Security Breaches
5. Insider Threats

Source: DarkTrace

1. ADVANCED PERSISTENT THREATS (APTS)

Often orchestrated by state-sponsored groups, APTs are prolonged, targeted attacks designed to infiltrate systems and remain undetected for long periods. These threats aim to steal critical information, sabotage systems, or spy on utility operations to gain strategic advantages.

Source: Darktrace

2. IoT/Smart Infrastructure Vulnerabilities

As utilities modernize infrastructure with smart grids and IoT devices, the attack surface expands significantly. These devices often lack robust security features, making them vulnerable to hacking, which can compromise entire networks.

Source: Darktrace

3. SUPPLY CHAIN ATTACKS

Utilities rely on a vast network of suppliers for software and hardware. Attackers can exploit vulnerabilities in the supply chain to introduce compromised components or software, leading to widespread security breaches.

Source: Darktrace

4. PHYSICAL SECURITY BREACHES

While cybersecurity focuses on protecting data, physical security breaches can have cyber-related consequences. Unauthorized physical access to facilities can lead to the installation of malware or direct sabotage of critical systems.

Source: Darktrace

5. INSIDER THREATS

Not all threats come from outside the organization; insider threats involve current or former employees who have access to the network and may misuse their access to steal information or disrupt systems either maliciously or through negligence.

Source: Darktrace

COURSE FEEDBACK

Please Take a Few Minutes To Provide Feeback About The Course & Instructor

Track 5/6 Understanding Cybersecurity Threats to Utilities 72325 8:45AM Alex Kobrenko

tescometering.co
m