MPSC
Michigan Public Service Commission

# Issue Brief

# Cybersecurity

## 1. What is cybersecurity?

Cybersecurity is a **combination of strategy, policy, and standards that safeguard the security and operations** of interconnected technology. Cybersecurity encompasses the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities. It includes computer network operation protection, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure.[1]

## 2. What is utility critical infrastructure?

Utility critical infrastructure includes **electricity, natural gas, water and telecommunications systems** that deliver crucial services to society. It is especially important to prevent disruptions to critical infrastructure with early detection of intrusion in on-going efforts to assure safe and reliable power, water, and communications services.

## 3. Why do cybersecurity threats concern the utility industry?

Cybersecurity threats are increasing in frequency and severity. From the largest international corporation, to the individual on their smartphone and every type and size of entity in between, these threats are becoming an increasingly **unpredictable and dangerous hazard** to the interconnected world. Networks are under attack daily across the state and country from a variety of sources, using a variety of methods, all of which are **growing in sophistication**. In 2017, malware affected a Ukrainian electric transmission station resulting in a blackout of a portion of the Ukrainian capital.[2] In Michigan, utilities are regularly targeted with cyberattacks. In most cases, governments, industry, and operators of critical infrastructure are containing threats. State agencies, national organizations, and critical infrastructure providers have increased collaboration to combat the growing threat environment.

## 4. What is cybersecurity planning?

Cybersecurity planning aims to **prevent damage to, unauthorized use of, or exploitation** of electronic information and communications systems and the information it contains to ensure confidentiality, integrity, and availability of the systems. Planning many times involves confidential sharing of highly sensitive information.

## 5. What is the Michigan Public Service Commission (MPSC) doing to address cybersecurity?

The MPSC fully **recognizes and prioritizes** the importance of effective cybersecurity with Michigan's critical infrastructure providers and has technical staff experts dedicated to monitoring utility cybersecurity defense programs. In Case No. U-17000, the MPSC specifically recognized cybersecurity as a high priority strategic issue warranting ongoing MPSC attention and involvement. The MPSC Staff report in the case stated that as Michigan transitions to a more technologically advanced power grid, it is important that proper actions are taken by utilities to address cybersecurity threats.

---

[1] CNSSI 4009, NIST SP 800-53 Rev 4, NIPP, DHS National Preparedness Goal; White House Cyberspace Policy Review, May 2009

[2] https://www.wired.com/story/crash-override-malware/

The MPSC Staff regularly conducts cybersecurity information **sharing sessions** with Michigan utilities when cybersecurity threats and industry best practices are explored and discussed. **Statewide partners** participating in these discussions include the Michigan State Police and the Department of Management and Budget.

The MPSC Staff, Michigan Agency for Energy Staff, state utility representatives, and cybersecurity professionals have an ongoing commitment to **continuing education and training events** addressing cybersecurity policy, industry best practices, and the changing environment of cyber threats.

MPSC orders in Case Nos. U-17735 and U-17767 established directives in utility rate cases for Consumers Energy (Consumers) and DTE Electric (DTE), respectively, that instructed both utilities to provide MPSC Staff with annual **reports** addressing the utilities' cybersecurity programs.

## 6. How have utilities responded to the MPSC's directives?

Consumers and DTE **meet with MPSC Staff annually** to discuss a full range of cybersecurity issues including staff training, cyber attack prevention, and internal cybersecurity programs.

## 7. How has the MPSC instructed other Michigan regulated utilities to address cybersecurity?

In MPSC Case Nos. U-18043 and U-18203, the Commission amended the rules governing the technical standards for electric service and are requiring regulated utilities to address cybersecurity reporting. The revised technical standards primarily require investor-owned and cooperative utilities to **provide the MPSC with an annual report on cybersecurity programs and planning, a description of cybersecurity training for employees, and notifications as soon as a cybersecurity incident is detected** that results in a loss of service, financial harm, or breach of sensitive business or customer data. The MPSC adopted final rules on December 20, 2018.

## 8. Have any laws been passed regarding cybersecurity?

It is important that utilities disclose and report cyber incidents to the public in a **transparent and informative manner**, while protecting sensitive confidential information that could be detrimental to individuals and/or businesses. In 2018, Public Act 68 of 2018 was enacted to address exemptions from disclosure when entities report cyber incidents and practices. MCL 15.243

## 9. What are the next steps?

The MPSC is **working to amend the rules governing the technical standards for natural gas service for regulated utilities to address cybersecurity reporting.** This public process will include seeking input from natural gas service providers and soliciting stakeholder public comments.

Cybersecurity threats and cybersecurity protection are **evolutionary processes**. The MPSC continues to collaborate with critical infrastructure providers, the Michigan State Police, and other agencies and stakeholders assuring best practices are being implemented to protect the state's critical energy infrastructure from cybersecurity threats.

**For more information, visit:**
**www.michigan.gov/mpsc**

***December 20, 2018***