Cybersecurity Matters at Utilities

Vigilance is required in protecting your personal information

Roman Gillen is president and CEO of Consumers Power Inc, an electric cooperative based in Philomath, Oregon.

When a major retail outlet suffers a cybersecurity breach, it often becomes the top news story for several days. We all worry about the security of our personal information, particularly when it links to our bank account.

But major retail outlets are not the only places where your personal data is stored. How does the electric utility industry safeguard the personal information collected in the course of providing electric service? Fortunately there are a number of industry best practices in use.

Data encryption is used almost universally to both transmit and store information securely. Powerful algorithms enable sent or stored information to be encoded in such a way that it is unrecognizable and unusable without a corresponding decryption key to reverse the process.

Website developers incorporate data encryption and decryption into the design of utility and other commercial websites so information remains protected even if it is intercepted by a third party.

A variety of organizations monitor and alert utilities to the discovery of data protection vulnerabilities. In the unlikely event a data protection scheme is compromised, utilities immediately shut down the website until the vulnerability is corrected with updated software.

In compliance with state and federal law, credit card utility payments receive special attention. Credit card information is stored in an encrypted format within utility databases.

Utilities employ a variety of technologies to protect their internal and external data networks from unauthorized access. Network appliances called firewalls are used to restrict access to each device on the utility's data network. Firewalls also provide information to help the utility spot attempts to break through the protective electronic barrier. Utilities are also careful to maintain separation among general business networks, their electric transmission and distribution networks, and the Internet in order to make it harder for a vulnerability in one network to affect another.

Employees are required to create complex passwords of a minimum length, use a unique password to access each information system, are forbidden from sharing or reusing passwords, and must change their passwords regularly.

Utility customers can play an important role as well by following the same safe password practices. Customers should apply the latest operating system, antivirus, web browser, and application software updates to their personal computers and smart phones as soon as they become available. Most importantly, customers should always be suspicious of phone and email messages demanding personal information or immediate payment by electronic means. Call the local utility before taking any action to verify who sent the message.

Many utilities now require their customers to provide a personal identification number or PIN before giving out customer information over the phone. Utilities are also reconsidering whether to maintain Social Security numbers, drivers' license numbers, and other personally identifiable information that was routinely requested in years past because the risk of such information falling into the wrong hands outweighs its usefulness.

Utilities must manage many risks in their efforts to keep your lights on. Protecting and safeguarding information has added yet a new dimension to those efforts. Utilities and customers must work together to adequately protect sensitive personal information from falling into the wrong hands. ■