

STATE OF NEW YORK
PUBLIC SERVICE COMMISSION

At a session of the Public Service
Commission held in the City of
Albany on August 15, 2013

COMMISSIONERS PRESENT:

Garry A. Brown, Chairman
Patricia L. Acampora
Gregg C. Sayre
Diane X. Burman

CASE 13-M-0178 - In the Matter of a Comprehensive Review of
Security for the Protection of Personally
Identifiable Customer Information.

ORDER DIRECTING THE CREATION OF AN
IMPLEMENTATION PLAN

(Issued and Effective August 19, 2013)

BY THE COMMISSION:

BACKGROUND

The past two years have seen a dramatic increase in national attention on cyber security. Within the utility community there has been for a decade an increasing focus given to cyber security for the protection of operational control systems. There has been less attention, in most instances, given to the need for upgraded cyber security for the protection of non-operational business systems and detailed personal information of the many customers maintained in those utility data systems. Any compromise of such personal information can expose many thousands of customers to identity theft and fraud.

Following a report presented to the Commission by Department of Public Service Staff (Staff) in July 2012 regarding a breach of customer privacy security at New York State Electric & Gas Corporation (NYSEG) and the then ongoing follow-up customer privacy security reviews at the other large energy utilities, the Commission directed all Class A and B

utilities to respond to Staff questions regarding the measures taken by each company to protect customer information from malicious cyber intrusion.

The list of Class A and Class B utilities included the large energy utilities, four major telecommunications companies, two large water companies, and several smaller electric and gas companies.

After discussions and on-site reviews with the smaller electric and gas companies, Staff determined they have little or no vulnerability to malicious cyber intrusion for purposes of customer identity theft. Some of those smaller companies have no interactive websites that could be used to gain access to company networks or databases. Some have only paper based billing procedures. Some of those same companies do maintain digital customer records, but only on standalone computers that are not connected to the Internet or to other company computers that are connected to the Internet. Having determined that the threat of electronic data theft from these companies is remote or nonexistent; such companies were excluded from further review.

Following on-site audits of customer privacy protections at the major telecommunications utilities, Staff concluded that the customer data protection measures in place at those companies were comprehensive and strong. Accordingly, Staff determined that little additional benefit could be gained from further review, however, Staff did provide the telecommunications companies with some recommendations for ongoing sharing of emerging threat information and regarding some technical countermeasures that were already under development.

The risk of the compromise of large quantities of personally identifiable customer information is most present at

the large energy utilities in New York. Further, recent threat intelligence indicates energy utilities are a target of sophisticated cyber attacks for apparent purposes of customer identity theft, as well as for the purpose of possible malicious operations system compromise.

Water companies have also recently been the subject of malicious cyber probing and scanning. Staff found that cyber defenses at the water companies were advancing but in need of further development to address emerging threats. Given the large number of New York customers served by American Water and United Water, follow-up review of customer privacy protections from cyber threats is warranted.

DISCUSSION

In presenting the results of its review to the Commission, Staff identified several areas where companies could both improve their practices and procedures or upgrade their technical network upgrades. Specifically, Staff made nine recommendations. We have reviewed the recommendations presented to us by Staff and have determined that the utilities should consider implementation of such and either develop plans to ensure timely and proper implementation or explain why action on such recommendations is unnecessary. Staff's findings and the nine recommendations related thereto are detailed hereafter.

Staff's Findings and Recommendations

Companies should address proactively known and potential future threats. Recognizing that a compromise of customer data resulting from a cyber-intrusion will remain a possibility in spite of robust defenses, it is essential to carefully prepare for such contingency. Preparations should include:

- 1) Planning for a possible network breach and compromise of personally identifiable customer information should include specific post-incidents response and recovery drills.
- 2) Establishment of a contractual relationship with a well qualified third-party forensics expert to ensure rapid response to any breach incident.
- 3) Establishment of a contractual relationship with a credit monitoring service for prompt response in the event of a possible compromise of customer information.

Companies should make efforts to address the human element that is a constant factor in the effectiveness of cyber security. Company employees can make mistakes, errors and misjudgments in the handling of customer account information. Company personnel can inadvertently introduce malicious software into company networks by falling victim to increasingly inventive hacking techniques. In recognition of these vulnerabilities, companies should:

- 4) Conduct additional and more frequent customer privacy related security training for both employees and contractors, particularly as to sophisticated social engineering hacker techniques.

Companies should eliminate or isolate customer data to the greatest extent practicable consistent with day-to-day business demands to protect their customers from the possibility of identity theft. Accordingly, companies should:

- 5) Improve inventory control of customer information so as to better know what is necessary for continued business functions, as opposed to what is no longer necessary and therefore properly subject to disposal.
- 6) Improve segregation of personally identifiable customer information from less sensitive business data, as well as electronic masking of personally identifiable information.

Companies should consider how physical security improvements may be made to enhance their cyber security. At some companies there is a need to:

- 7) Upgrade physical security measures for the protection of critical cyber equipment and to limit unauthorized physical access to that equipment.

Companies should increase their internal awareness that all organizations with large sets of personally identifiable customer data, including utilities, are attractive targets for cyber identity theft and take steps to address vulnerabilities to data systems. Energy sector companies, including utilities, have been shown to be the frequent subject of malicious scanning and probing for vulnerabilities in cyber defenses looking for ways to gain access to company systems.

The attention given to identifying and acquiring next generation cyber security defensive technology varied among companies. Most companies need to devote more resources to researching and identifying the best current and next generation network monitoring and detection tools, and to establish a process for doing that on a continuous basis.

Therefore, the large energy utilities particularly, should:

- 8) Upgrade technical security controls by procuring and deploying next-generation intrusion detection systems and security information event management solutions.

Finally, all the companies need to be committed to acquisition of the good defensive technology for the protection of their business networks. External examination through qualified third party assessors is necessary in order to make sure that utility companies are keeping up with the rapidly developing electronic intrusion capabilities that are directed at stealing customer data, and to better ensure that utility companies are identifying the most reasonably deployable and effective preventative measures available. Objective external scrutiny of an organization's security posture by qualified

experts who have knowledge of the latest threat and technical solutions information is now more important than ever in the constantly evolving cyber environment. Therefore, companies should:

- 9) Conduct regular third-party vulnerability assessments of the protection of sensitive customer information

We recognize that these overall findings and nine recommendations apply broadly to our regulated utilities in varying degrees. We note that improved protection of customer privacy information from compromise can be achieved in many respects by more diligent enforcement of existing company policies and procedures, or through only the minor modification or extension of those existing policies and procedures. We are also encouraged by Staff's finding that many of the things that can be done for the better protection of customer information are simply a matter of "running a tighter ship" and do not entail significant workplace disruption or significant cost.

Finally, while all of Staff's recommendations are essential to a consideration of best practices, we consider Staff's ninth item to be the most important recommendation above. Although most companies conduct some third-party evaluation and testing of their data system security, the frequency and regularity of such testing was not well established. We note that the quality and effectiveness of a cyber security program cannot be sufficiently ensured without the benefit of reasonably frequent external analysis. Given the threat environment that exists for utility operations, we believe that third party evaluations, including penetration testing of utility business systems, should be a regular practice.

In considering how to implement the recommendation for third-party vulnerability assessments, companies should consider the following guidelines:

The scope of annual third party audits should include, at minimum, an examination of executive level leadership and support for customer privacy related cyber security, company policies and procedures regarding customer privacy protection, the quality of data network security (including intrusion detection and intrusion protection, network access controls, and data loss prevention tools), the sufficiency of segregation of customer data from other business systems data, training and employee threat awareness education regarding cyber threats to the security of customer data, the adequacy of limitations on access to customer data by vendors and consultants, physical security for the protection of data systems, and post incident response protocols and drills for a suspected or known breach of customer data security.

While we leave it up to individual companies to determine when and how such recommendations should be implemented to best fit their individual needs, we are of the opinion that given the extent and increasing sophistication of cyber threats a first third-party audit should be completed no later than July 1, 2014, with subsequent annual audits to be commenced no later than the one year completion date anniversary of the previous audit. We also believe that any third-party

consultants retained for this purpose have a high level of experience and expertise.¹

CONCLUSION

We believe that the Staff recommendations discussed herein should be considered by utilities when creating or updating their cyber security policies and procedures. Accordingly, we direct the large electric, gas and water utilities to prepare Implementation Plans within 60 days of the issuance of this Order detailing steps that have been taken or are being taken in response to the recommendations herein. If a utility believes a recommendation should not be implemented, an explanation for its determination should be provided.

These Implementation Plans should address specifically the actions the companies have taken to institute post incident response and recovery procedures, contractual arrangements for third-party forensics and customer credit

¹ Staff informs us that certification by the Payment Card Industry Security Standards Council appears to offer the best available assurance of competence for this type of audit work. The PCI SSC (the Council), is an open global forum, launched in 2006, that develops, maintains and manages the PCI Security Standards. Council standards cover everything from the point of entry of card data into a system, to how the data is processed, through secure payment applications. The Council seeks to protect and educate industry players such as merchants, processors, financial institutions, and any other organizations that store, process, and transmit customer data. These standards include an assessment methodology for taking inventory of an organization's IT assets and business processes for electronic customer transactions payment and analyze them for vulnerabilities that could expose customer data. Additionally, as we understand it, estimates regarding the cost of annual cyber security audits limited to the protection of customer data provided by several companies certified by the PCI Security Standards Council were far less than the cost to a utility for responding to and mitigating the consequences of a breach of customer data security.

monitoring in the event of an incident, additional and more frequent employee training on cyber intrusion awareness, improvements in inventory control and segregation of customer data, improvements to strengthen the physical security that limits employee access to customer data, the procurement and deployment of next-generation security technologies and tools, as well as for steps being taken to secure the services of consultants to conduct the annual third party audits.

The utilities should maintain these plans and produce them upon request of Staff for inspection. Staff will develop a schedule to review the company implementation plans and begin those reviews following the 60 day period.

The Commission orders:

1. The utilities are directed to create implementation plans within 60 days of the issuance of this Order consistent with the procedures and requirements detailed in the body of this Order.
2. This proceeding is continued.

By the Commission,

Kathleen H. Burgess

Digitally Signed by Secretary
New York Public Service Commission

KATHLEEN H. BURGESS
Secretary