STOUGHTON UTILITIES

Incident Response Plan

Last Revised: March 14, 2017

CONFIDENTIAL INFORMATION

This document is the property of Stoughton Utilities, containing information that is considered public policy, and is subject to release pursuant to public records statutes, Wis. Stat. §§ 19.31-19.39. Copying or use of this document in whole or in part is strictly prohibited without prior written permission of Stoughton Utilities.

Introduction

This document describes a plan for how Stoughton Utilities employees should respond in the event of a security incident. It is important to know this in advance, because in the middle of a crisis, it can be difficult to put together a careful plan, especially when key staff members may be unavailable, and computers, phones, etc., may not be working.

This plan uses the term 'security incident' to mean any deliberate attack(s) on Stoughton Utilities' physical security, communications, or information processing systems. The attacker could be a vandal, terrorist, malicious stranger, disgruntled employee, amateur or professional hacker, or a state-sponsored entity, and their intention might be to steal information or money, interrupt utility operations, damage utility infrastructure, or damage the utility's reputation.

Having a plan in place will allow you to react more quickly and intelligently, and help the utility control the consequences to operations and security.

In broad terms, you should react to a security incident by:

- Immediately investigate the incident to determine what has happened, what harm has been done, and if the incident is still in progress.
- Take action as soon as possible to limit the scope of the damage. This typically includes preventing further unauthorized access to customer or utility information and systems.
    - However, keep in mind that in many cases it is impossible to undo the damage already done.
- Notify those who need to be notified of what has happened, and what you are doing about it.
- Complete your investigation as to what happened and why. Use this opportunity to identify how your security processes and systems could be improved
- Notify all those necessary of your investigation findings.
- Start to make any appropriate changes identified in your findings for improving your security processes and systems.

The rest of this document is spent expanding on the above points, giving useful specific details, and laying out a specific set of actions and responsibilities.

Immediate Investigation

It is part of Stoughton Utilities' and the City of Stoughton's network security policies that all staff are required to report any suspicious behavior or signs of a security problem. For the purposes of this plan, all references are made to Stoughton Utilities.

Stoughton Utilities has designated a primary employee in the organization responsible for dealing with any security problems or questions. If the primary employee is not available, secondary employees are available who are expected to seek out computer expertise from the primary designee, or other competent technology staff.

Investigation Contacts:

Role:	Name:	Email:	Office Phone:	Cell Phone:
Primary	Brian Hoops	BHoops@stoughtonutilities.com	(608) 877-7412	(608) 770-7050
Secondary	Sean Grady	SOGrady@stoughtonutilities.com	(608) 877-7416	(608) 575-3732
External	Rodney Scheel	RJScheel@ci.stoughton.wi.us	(608) 873-6619	(608) 577-1891
External	Pat Conlin	PConlin@ci.stoughton.wi.us	(608) 873-6859	(608) 209-7530

When a security incident occurs, or is suspected, this person (or people) should investigate to see if there really is a problem. If there is, then:

- If there is any threat whatsoever of physical harm to staff or others (for example, from a physical intruder or suspicious package or device) withdraw immediately and call 911.
- If there is no immediate threat, start a written event log by noting date and time of all actions.
- Your first priority is to limit the damage to your customers and your company (as described in the next section), but your next highest priority should be to try to preserve information about the attack.
- If the attack involved physical evidence (such as from a break-in), preserve any evidence, do not disturb the area, notify the police, and take photos of the scene.
- If the attack affected computers, make every effort to NOT use the computers:
    - **DO NOT** log on to any computer or system,
    - **DO NOT** turn off or remove power to any computer or system. Doing so may destroy forensic evidence of what the attackers did and how they did it.
    - **DO** disconnect affected devices from all networks and external connections, and remove Stoughton Utilities' network's ability to access the internet.
- If it is absolutely critical that the computers be used, make copies of any relevant files on a thumbdrive, DVD, or similar, before using them again.
- Try to identify at a high level what damage has been done. Has sensitive information about the utility or its customers possibly been stolen, changed without permission, or destroyed/deleted? Have the utility's SCADA systems been accessed or controlled remotely?
- Make an estimate of how sensitive this information is, and how many customers and/or which facilities have possibly been affected.

Limit the Damage

If there is any chance that damage is still being done (for example, if attackers are still accessing/downloading computer files, controlling critical infrastructure, or a cyber-attack is in-progress), your first priority must be to limit the damage. Where possible, DO NOT turn computers off, but instead disconnect them from all network connections so that hackers cannot get in (or stay in) and viruses, etc., cannot spread to other devices.

If there is any physical damage (for example, broken locks on doors) try to secure the area to prevent anyone else from getting in after the fact.

Notify Those Who Need To Be Notified

There are some people you should notify because they can help you, and others you need to notify because you are legally obliged to. Contact the first set of people as soon as you know there is a real problem, and contact the second set of people as soon as is reasonable or required.

When you contact the police, inform them of any immediately noticeable impact to critical utility infrastructure, including electric substations, water pumping and storage facilities, wastewater treatment pumps and controls, SCADA, etc.

Any cyber attack or intrusion to Stoughton Utilities' network or physical systems should be reported to the Department of Homeland Security Wisconsin Fusion Center. *This report will be made by the local police department if deemed appropriate.*

People to contact as soon as possible:

Role:	Name:	Title:	Phone:
Management	Robert Kardasz	Utilities Director	(608) 209-7807
Management / IT	Brian Hoops	Assistant Director	(608) 770-7050
Law Enforcement	Emergency		911
Insurer	CVMIC	Cyber Liability Insurance – Data Breach Coach	(800) 817-2665
Insurer	CVMIC	Cyber Liability Insurance – Network Extortion	(800) 523-9254

People to contact as soon as reasonable:

Role:	Name:	Title:	Phone:
Law Enforcement	Greg Leck	Police Chief	(608) 873-3374
Risk Manager	Amy Jo Gillingham	Director of HR and Risk Management	(608) 646-0274
Legal	Matthew Dregne	City Attorney	(608) 259-2618
Finance	Jamin Friedl	Finance Manager	(608) 877-7415

Stoughton Utilities may be required by law to notify any potentially affected customers directly. You will need to consult the City Attorney and our credit card merchant bank to clarify this point.

No employee should communicate with anyone outside of the Utilities Director or Assistant Utilities Director about any details or generalities surrounding any suspected or actual incident. All communications with law enforcement or the public will be coordinated by the Assistant Utilities Director.

Customer Credit Card Data Breach

Alert all necessary parties.

Be sure to notify:

a. Stoughton Utilities' merchant bank
b. Local FBI Office (contact to be made through local law enforcement)
c. U.S. Secret Service (if Visa payment data is compromised) (contact to be made through local law enforcement)

Notify applicable card associations:

Visa

Provide the compromised Visa accounts to Visa Fraud Control Group within ten (10) business days. For assistance, contact (650) 432-2978. Account numbers must be securely sent to Visa as instructed by the Visa Fraud Control Group. It is critical that all potentially compromised accounts are provided. Visa will distribute the compromised Visa account numbers to issuers and ensure the confidentiality of entity and non-public information.

See Visa's "What to do if compromised" documentation for additional activities that must be performed. That documentation can be found at

http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_what_to_do_if_compromised.pdf

MasterCard

Contact our merchant bank for specific details on what to do following a compromise. Details on the merchant bank (aka. the acquirer) can be found in the Merchant Manual at http://www.mastercard.com/us/wce/PDF/12999_MERC-Entire_Manual.pdf.

Our merchant bank will assist when you call MasterCard at (636) 722-4100.

Discover Card

Contact your relationship manager or call the support line at (800) 347-3083 for further guidance.

Perform an analysis of legal requirements for reporting compromises in every state where clients were affected. The following source of information must be used:
http://www.ncsl.org/programs/lis/cip/priv/breach.htm

Complete The Investigation (as soon as possible)

Investigating the problem may be expensive if over-done, so Stoughton Utilities needs to review how serious the problem might be (using the worst-case scenario to estimate) and decide how much time and effort it should put into the investigation.

At a minimum, the utility should try to figure out:

- When the attack happened,
- Over what time period,
- What the damage was (for example, what data was affected, what happened to it, which people were affected),
- How the attack succeeded (if it did).

Try to figure out what could have been done to prevent the attack from causing damage.

The Assistant Utilities Director and all affected parties will meet to review the results of any investigation to determine the root cause of the compromise and evaluate the effectiveness of the *Incident Response Plan*. Review other security controls to determine their appropriateness for the current risks. Any identified areas in which the plan, policy or security control can be made more effective or efficient, must be updated accordingly.

Report Your Findings

As a result of notifying people above, you probably have been asked for reports on what happened and why. Decide who needs this information, and/or has a legal right to it, and give them a copy of your investigation report. Remember that some of this information might be very sensitive, and where appropriate, you can give people a partial version with some information removed. Discuss any questions with the Assistant Utilities Director to determine what information should be redacted and for whom.