McWane's Commitment to Cybersecurity for its iHydrant Products

Introduction

Cybersecurity is a vital aspect of our business, as we provide services and solutions that collect, store, and process personal and confidential data from our customers. We are committed to protecting our customers' data from unauthorized access, exposure, or damage, and to ensuring the availability and performance of our system and services. Our system consists of cloud-based iHydrant utility software, including its associated data collection, data storage and event notification services ("System").

To achieve this, we follow the National Institutes of Standards and Technology (NIST) Cybersecurity Framework, which is a widely recognized and evolving set of best practices and standards for cybersecurity.

Benefits of the NIST Cybersecurity Framework

The NIST Cybersecurity Framework provides a comprehensive and flexible approach to managing cybersecurity risks and improving resilience. It consists of six core functions:

- Identify
- Protect
- Detect
- Respond
- Recover
- Govern

These functions are further divided into categories and subcategories that cover various aspects of cybersecurity, such as asset management, access control, data security, incident response, and recovery planning.

By following the NIST Cybersecurity Framework, we benefit from:

- Clear and consistent understanding of cybersecurity objectives, roles, and responsibilities.
- Systematic and proactive identification and assessment of System's cybersecurity risks and vulnerabilities.
- Robust and layered protection of our System, services, and data from various types of Cybersecurity Incidents (breaches or attempted breaches of our System's security policy that affect the System's integrity or availability or results in unauthorized access to the System).
- Timely and effective detection and response to any Cybersecurity Incidents that may occur.
- Rapid and smooth recovery of our System, services, and data in the event of a Cybersecurity Incident.
- Continuous and adaptive improvement of our cybersecurity posture and performance.

Our Approach

Cybersecurity Incident Response and Recovery

- We maintain a regularly updated Security Breach Incident Response Plan.
- Once a Cybersecurity Incident is confirmed, we will expeditiously marshal the appropriate internal technical resources to:
  - cease any continuation of the identified Cybersecurity Incident activity; and,

    - assess what has happened and any consequences of the Cybersecurity Incident.
- We also maintain a regularly updated data recovery plan.
- We will apply reasonable efforts to reconfigure and rebuild the System and its database such that:
    - normal customer access and operations may resume.
    - the System database will be rebuilt to no less accurate data than its contents as of 72 hours prior to the start of the Cybersecurity Incident; and,
    - the System will return to maintaining its 96% minimum monthly uptime commitment.

Web Services Environment

- We manage the System and associated services within a virtualized and relocatable Microsoft Azure secured datacenter environment, wherein both external and internal access to data is tightly controlled and all software changes must follow authorized engineering update procedures.
- Microsoft Azure has specific protections implemented to identify and impede denial-of-service attacks, ransomware attacks, and unauthorized security breaches.
- Microsoft Azure provides antivirus and anti-malware protection, and we supplement this with CrowdStrike, GlobalProtect, secured engineering practices, and both internal and third party access controls.
- Microsoft Azure offers tools to identify Cybersecurity Incidents and we proactively monitor our information technology environment for suspicious activity.

Data Communications Security

- All iHydrant devices use private cellular addressing to isolate them from external contacts and we implement fully encrypted and authenticated device communications. Each customer's System access is controlled via rigorous log-in procedures, and we meticulously enforce access credential terminations for departing employees. The System uses a multi-tenant architecture such that each customer's data is isolated from other customers' data with individual access credentials which prevent any cross-customer data access. Third party access is limited to Microsoft Azure approved partners and allowed only for System monitoring and support purposes.
- Cellular usage is reviewed monthly, and both firewall and Microsoft Azure logs are monitored automatically for suspicious activity such as multiple failed log-in attempts.

Database and Data Security

- We continue to implement industry-recommended techniques to further shield the System database and its isolated backup database from exposure to Cybersecurity Incidents.
- Following NIST-standard processes, and as Cybersecurity Incidents evolve, we will identify and implement additional tools and techniques to further secure the System's database and its isolated backup database from Cybersecurity Incidents, ensuring that the System's main database can be rebuilt or repaired from its isolated backup database when required.
- The backup database is stored using multiple and compounded isolation techniques, such that a Cybersecurity Incident on the System will have no access to the isolated backup database.
- Database consistency checks are run on a periodic basis to identify any data corruption or anomalies, which could indicate a System flaw or an otherwise undetected Cybersecurity Incident.

Preventative Actions

- We maintain an ongoing NIST-compliant and proactive approach to cybersecurity.
- We apply tools and techniques which both:
    - Improve the System's shielding against both known and unknown or unidentified cybersecurity threats; and,
    - Minimize the risk of adverse outcomes, should a Cybersecurity Incident occur.
- We arrange for periodic execution of cybersecurity industry-standard penetration testing to identify any newly determined cybersecurity risks.

- We implement System fixes to address all high and medium cybersecurity risks identified during periodic penetration testing and will verify those remediations with re-testing.

Data Exposure

- We understand that both contractual responsibilities for securing customers' confidential data and jurisdictional legal obligations for securing personal data vary and may change over time, such that we must maintain awareness of our obligations and all such data must be secured.
- We proactively monitor System access logs for any unusual activity which might indicate an attempt to cyber-attack the System.
- Our cybersecurity activities, as described herein, are designed to:
  - Reduce the likelihood of a Cybersecurity Incident occurring, including the additional risk of unauthorized access to, and/or release of personal or confidential data.
  - Shorten the System's recovery time to re-establishing normal System operations; and,
  - Harden the System via cybersecurity improvements to further reduce the possibility of future Cybersecurity Incidents.
- Microsoft Azure's logs record all accesses made to the System and any abnormal accesses will be reviewed and could trigger incidence response and data recovery plans.

Conclusion

Cybersecurity is a key priority for our business, as we value our customers' trust and satisfaction. Although Cybersecurity Incidents may still occur in spite of our efforts, the NIST Cybersecurity Framework helps us to manage and improve our cybersecurity capabilities and resilience, and to deliver high-quality and secure web-based services and solutions to our customers.