Cybersecurity And Cooling Technology: What You Need To Know

Aldo Leiva, Cybersecurity And Advocacy Counsel
Baker, Donelson, Bearman, Caldwell & Berkowitz, PC
Adam Green Chairman, Water Technology & Water Treatment Group, Baker, Donelson, Bearman, Caldwell & Berkowitz, PC

Abstract

Cybersecurity risks and data protection vulnerabilities present significant legal, operational and business threats to the cooling technology industry. The relevance of these challenges was highlighted in 2013, when national retailer, Target, was subject to a $202 million data breach through its HVAC contractor, who had access to the client's server infrastructure. Because of the evolving nature of the threats, cybersecurity remains a high priority issue in cooling technology across all industries including hospitality, healthcare, education and others. In 2018, the American Water Works Association identified cybersecurity as a critically important issue facing the water industry. The failure to adapt to this ongoing threat places the vendor at a competitive disadvantage and their client at risk. Cooling technology providers are challenged to develop sound cybersecurity plans to ensure that both their own internal systems and their clients' systems are protected. This publication addresses general information and considerations that may be explored by cooling technology companies in developing such plans and mitigating against related risks.

Introduction

Cooling technology companies service a wide variety of commercial, residential, industrial, healthcare and government industries. Regardless of the industry setting, cooling technology providers are often engaged in ongoing "partnerships" with their owner and operator clientele to provide the desired environmental control services and to ensure that building water systems achieve the desired level of efficiency and useful life through the avoidance of corrosion, scale and microbiological fouling.

These partnerships have become increasingly technological in a number of aspects ranging from continuous real-time monitoring and equipment control, and to online field service reports to periodic billing and payment. While such continuous connectivity and data exchanges enable rapid responses and seamless payment transactions, such communications and services must be rendered securely and safely, for the benefit of both the customer and the cooling technology company. Connected networks demand close partnering and authentication of access credentials between the cooling technology provider and the customer.

In 2013, retailer Target was the subject of a well-publicized cybersecurity breach. In this instance, an HVAC contractor's computer system which had access to the Target system infrastructure was compromised with malware for the purpose of infiltrating the Target network. The net result was devastating to the customer as Target reportedly incurred expenses exceeding $290 million as a result of the incident.

The 2013 Target data breach provides a critical lesson in how networked services between cooling technology providers and clients are being targeted by cyber criminals. Since that event, customers are expecting all vendors with whom they interact, including cooling technology providers, to properly secure their computer systems. Deferral of the issue until a crisis arises is no longer an option as wary owners are including cybersecurity policies as part of their due diligence procedures when vetting vendors. Those who are unprepared or unwilling to address cybersecurity and data breach preparedness efforts not only are subject to potential lawsuits and regulatory enforcement actions, but are also at a competitive disadvantage in the cooling technology market. Failure to adequately assess risk and train staff also subjects cooling technology companies to being targeted in email phishing scams whereby fraudulent payments are solicited and often paid.

Adam Green

Aldo Leiva

This paper will provide an overview of cybersecurity matters that should be considered by cooling technology companies in starting to assess both their and their customers' potential cybersecurity vulnerabilities and opportunities.

Terminology 101: ICS, Scada and IOT

Cooling technology providers render services and related products in a wide variety of settings in both the public and private sectors, ranging from residential and commercial buildings to oil refineries, chemical plants, and thermal power stations. Due to this broad applicability across key strategic, industrial, and commercial sectors, cooling technology professionals provide integral support for essential assets that contribute to the orderly functioning of the American society and economy. Because of this integral support, if the risks associated with the growing technological threats are not managed properly and the proper precautions taken, both the cooling technology provider and their clients can be exposed to serious, legal, operational, and business risks. In recognition of these ongoing risks, the American Water Works Association indicated that "Cyber risk is the top threat facing business and critical infrastructure in the United States." Therefore, any vulnerabilities that exist in the systems and technologies implemented by cooling technology providers similarly create potential risk for their clients, and most importantly, critical infrastructure.

Such technologies may include Industrial Control Systems (ICS), which help facilitate operations via a network of modular controllers, field connections, and sensors. Larger HVAC systems may incorporate a Supervisory Control and Data Acquisition System (SCADA), which relies on computers (hardware), networked data communications, software applications, and graphical user interfaces to provide remote access and control large-scale processes over large distances. When such systems were initially implemented, the control systems and devices communicated with each other within an isolated or local network, and had no connection to larger networks. As the Internet grew and large corporate networks were created to share data, once-isolated control networks were connected to larger networks, thereby exposing such networks to a higher risk of cyber-attacks by malicious hackers, cybercriminals, and nation states.

In the meantime, rapidly-evolving and emergent technologies have

resulted in a technological landscape that further enhances connectivity, communications, data collection and transmittal, by converting physical environments into sensor-imbedded interactive devices that are connected to the Internet. The term "Internet of Things" or "IOT," has been coined to describe this growing technological shift, which will affect engineering and network computing services by creating wireless connectivity with billions of devices, ranging from wearable fitness devices to large scale wireless thermostatic systems.

Many such devices will be deployed within "smart" buildings, vehicles, critical infrastructure, and public works. However, each such device provides a potential access point to systems, such as SCADA systems, which were designed with connectivity, and not security, in mind, due to the perceived low risk of access for malicious purposes at the time such systems were implemented. These devices have become more common in the cooling technology industry over time, and because of this the risks associated with them for cooling technology providers, has grown with their increasing prevalence.

However, as of 2010, cybersecurity researchers were alarmed to observe the emergence of the Stuxnet virus, which specifically targeted industrial computer systems and caused significant damage to an Iranian nuclear power plant, by seizing control of nuclear centrifuges and forcing them offline. Specifically, this virus was designed to target Programmable Logic Controllers (PLCs), which control machinery on assembly lines and in HVAC systems. The virus targeted systems using the Microsoft Windows operating system, and sought out Siemens STEP 7 software, which operated such physical devices as the centrifuges in question. While the attack targeted a rogue nation state, it also demonstrated the reality of an industrial-scale cyber warfare attack, which can be adopted by cyber-criminal networks, cyber-terrorists, foreign cyber-military forces, and foreign intelligence organizations. Cooling technology providers and their clients are not immune to such an attack as shown by the attack on Target and its customers in 2013 as discussed more fully below. As an example, the recent Marriott/Starwood data breach has been linked to Chinese intelligence authorities, which are believed to have conducted the attack to collect valuable personal information on individuals and officials.

In light of this heightened risk environment, both government and non-profit entities have sought to develop resources, assessment tools, and educational information to promote and enhance cybersecurity in virtually all industries and settings in the U.S. Because of the technical expertise required to identify and protect against threats in an ever-evolving environment, cybersecurity consulting firms have rapidly grown to meet the growing demand for such services in every critical infrastructure sector.

Unfortunately, cyber threats are projected to increase due to several factors, which are also fueling the expansion of IOT. First, a new internet protocol, known as IPv6, is being implemented worldwide, which will allow essentially any object/device on the planet to have unique internet ID, which, coupled with the continued expansion of broadband internet and dropping prices of "smart" devices, will lead to more devices (and users) being connected to the internet than ever before.

As applied to the cooling industry, the use of sensors has been established in HVAC systems for years, and the enhancement of such sensors by wirelessly connecting them to internet networks will allow for increased data collection, storage, trouble shooting, maintenance, and real-time monitoring. New online management platforms will expand monitoring to ducts to measure such variables as airflow, temperature, and static airflow. The benefits of such technology will not only extend to preventive maintenance, rapid response, and increased energy efficiency, but will provide useful data to improve upon business practices and provide enhanced feedback from customers and clients. However, such enhanced connectivity will also subject HVAC systems and cooling technology providers to cybersecurity risks, which have been crystallized in the well-known case study of the massive Target data breach of 2013.

The Target Data Breach

In 2013, news outlets widely reported Target's unprecedented data breach of over 110 million customers, which included personal information and payment card account information. As a consequence, Target faced an onslaught of lawsuits and regulatory investigations, which ultimately cost the company $290 million. In the course of such lawsuits and investigations, the details of how the hackers were able to access Target's computer network were revealed, and the cause of the breach was ultimately traced to an unfortunate refrigeration/HVAC company that provided services to several Target locations.

The criminal hackers had deployed a phishing email to Target suppliers and an HVAC employee was deceived into opening one such email, which resulted in a malicious code ("malware") to be downloaded onto the HVAC vendor's computer network, without the employee's knowledge. Unfortunately, the HVAC vendor's computer system did not have adequate security and system protections and did not detect the malware or the intrusion onto the network. The malware ultimately revealed log-on credentials that had allowed the HVAC vendor to communicate with Target's billing system. By using such credentials, the hackers gained access to the Target computer network and were ultimately able to infiltrate a Target customer service database, which contained personal information and payment card account data.

Following the Target data breach, the fact that many companies use Internet-connected HVAC systems, often without adequate cybersecurity controls or policies, became an area of concern, as a potential gateway for hackers to access large corporate systems. Cloud security service provider Qualys reported that its researchers had identified approximately 55,000 HVAC systems that were connected to the Internet, and which were subject to exploitation by hackers. Most significantly, Qualys also reported that it had conducted additional network scanning on Target and had still been able to virtually view Target's HVAC system online, even after disclosure of how the hackers had gained access to the Target system. Thereafter, a remotely-accessible HVAC system at the Sochi Olympic Arena, was determined to have inadequate security, as it lacked authentication requirements to access the HVAC control system, which necessitated a reconfiguration of the system prior to the Olympics and opening ceremonies.

Practical Consequences Of The Target Data Breach

Contracts

In the wake of the Target data breach, businesses have identified vendors and service providers as potential sources of risk, liability, and compliance exposure. As such, contracts with third party service providers and vendors have incorporated cybersecurity provisions, especially where third parties have access to or use of a company's system and data. In light of this, cooling technology vendors may be contractually required to represent and warrant that their access, use, storage, and disposal of client/customer data shall be done in compliance with all applicable federal, state, and foreign data protection laws, and corresponding regulations. Contracts may also require cooling technology vendors to adopt industry-appropriate standards and practices, such as those issued by such organizations as the International Organization for Standardization (ISO) or by U.S. authorities, such as the National Institute of Standards and Technology (NIST), which are also discussed in this paper.

Owner clientele may also impose cybersecurity standards on cool-

ing technology vendors that support such owner's effort to demonstrate due diligence efforts to their own customers or regulators. For example, vendors may be required to submit detailed network infrastructure diagrams as part of this process. Vendors may also be required to consent to cybersecurity audits and may also have to disclose instances of actual or threatened data breaches or similar cybersecurity vulnerabilities. In addition, vendors may be subject to risk assessments, based on their access to critical assets, and, depending on the degree or nature of such access, may be contractually required to maintain acceptable cybersecurity risk programs to address such risks.

Data breach notification requirements may be required pursuant to any applicable state-specific or industry-specific laws or regulations. The vendor may also be contractually required to cooperate in any data breach investigations, including any private investigations that do not involve law enforcement authorities. In addition, the cost of any such breach may be borne exclusively by the vendor, if so required under the contract, and may also be required to indemnify the customer/client for any losses arising out of the data breach.

Contracts may also require that vendors affirm that they themselves have cybersecurity policies in place to address cybersecurity matters and safeguarding of customer/client data and systems. To the extent that vendors outsource or contract management of the entirety or a portion of their own computer infrastructure, vendors may similarly be required to impose downstream cybersecurity requirements on their own vendors and subcontractors.

In the event that the cooling technology vendor will have access to or will be entrusted with highly-sensitive personal information, encryption might be contractually imposed, with potential reference to encryption standards established by NIST's Federal Information Processing Standards (FIPS). Similarly, if the client/customer is sharing credit card payment data with the vendor, the vendor may be required to comply with Payment Card Industry (PCI) data security standards.

Vendors that serve public sector entities must also review their government contracts for similar requirements, and must also assess their compliance requirements with NIST 800-171, which, as of December 31, 2017, imposed specific security standards on vendors that process, store, or transmit information that is deemed "sensitive" but not "classified" for such federal agencies as the Department of Defense, the General Services Administration, and the National Aeronautics and Space Administration. Vendors subject to such requirements must assess and document their level of compliance in handling such information, including configuration of computer networks, access control, incident response policies, and means/methods by which portable computer media are managed.

In summary, contracts executed by cooling technology companies may impose legal requirements that are enforceable under contract law, including the imposition of cybersecurity standards that may otherwise be voluntary (i.e. such as the NIST Framework, discussed below), but which by reference in a contract, convert them into legally enforceable requirements.

Supply Chain Security

Due to complexity of supply chains, which often involve foreign/international participants, cooling technology vendors should better understand their overall supply chain risk management, particularly within their computer and cybersecurity supply chain relationship networks. A key example of the heightened scrutiny on foreign vendors is a new procurement ban against Russian-based cybersecurity firm Kaspersky Labs, which is now barred from contracting with the Pentagon, the General Services Administration, and NASA, out of concerns of reported ties between Kaspersky and the Kremlin. In light of these developments, cooling technology vendors should consider assessing their supply chain risk management programs to ensure that they:

1. Determine cybersecurity requirements for suppliers;
2. Impose contractual cybersecurity requirements on their own vendors and suppliers;
3. Communicate to suppliers that such requirements will be verified and validated;
4. Verify that all cybersecurity requirements are met via the appropriate methodologies, and
5. Manage all the above activities.

Such an assessment should be applied to all applicable technologies that are used by the cooling technology vendor, such as information technology, industrial control systems (discussed above), and any IOT devices (also discussed above.)

Legal And Regulatory Requirements

In addition to contractual obligations, cooling technology companies may be subject to both federal and state cybersecurity laws and regulations, which will be determined by such factors as their individual business practices (i.e. types of data collected, stored, or transmitted), technology adopted/implemented (i.e. hardware, software, network configuration, etc.), types of clients/customers served (i.e. businesses, consumers, government entities), and jurisdictions in which they are doing business or intend to do business. While a comprehensive summary of all potentially applicable cybersecurity-related laws and regulations is beyond the scope of this paper, provided below are selected laws/regulations that may be reviewed by cooling technology companies and their counsel.

Federal Laws and Enforcement Actions

At present, there is no single federal data protection or cybersecurity law (or any single enforcement authority) that governs cybersecurity matters/practices by U.S. businesses. Rather, several such laws and regulations are industry-specific. For example, the 1996 Health Insurance Portability and Accountability Act (HIPAA), requires that regulated healthcare organizations take measures to protect their computer systems, networks, and information, while the Gramm-Leach-Bliley Act (GLBA) requires financial institutions to "establish appropriate safeguards" to protect customer personal information "(1) to insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer." The Federal Information Security Management Act (FISMA) applies to all federal government agencies and requires the development and implementation of mandatory policies to address information security. As noted above, such laws, while not necessarily directly applicable to cooling technology companies that do not participate in such industries, may lead private or public customers subject to such laws to contractually impose cybersecurity requirements on cooling technology vendors. For example, a cooling technology vendor servicing a hospital may be contractually obligated to comply with HIPAA, if such vendor potentially has access to protected health information of hospital patients (even if such data is not actually viewed by the vendor).

The Federal Trade Commission (FTC) Act allows the FTC to enforce consumer protections provided in Section 5 of the Act, by bringing enforcement actions against business entities that participate in "unfair or deceptive acts or practices." Under this broad authority, the FTC has brought dozens of cases against companies that have allegedly failed to provide appropriate protections for customer data. The FTC recently approved a final settlement with

Uber Technologies, over allegations that the company had deceived customers about its privacy and data security practices. Specifically, the FTC alleged that, despite Uber's claim that consumer data was "securely stored within our databases," Uber's security practices failed to provide reasonable security to prevent unauthorized access to consumers' personal information in databases Uber stored with a third-party cloud provider. The FTC also alleged that the company similarly failed to protect Uber driver information. Under the terms of the final settlement, Uber is subject to imposition of civil penalties if it fails to notify the FTC of future data breaches involving customers or drivers, and is also prohibited from making misrepresentations regarding its data security practices. Uber is also required to implement a comprehensive privacy program and has agreed to submit to independent third party assessments of its program for 20 years. Cooling technology vendors should therefore ensure that their public representations regarding the status of their cybersecurity protections (perhaps via advertising materials or on websites) are accurate and do not run afoul of FTC cybersecurity guidance and recommendations.

Publicly traded companies must also consider their compliance posture as to Securities and Exchange Commission (SEC) guidance on cybersecurity risks and incident disclosures. On September 26, 2018, the SEC announced the imposition of a $ 1,000,000.00 fine with a financial services entity to settle charges arising out of a 2016 cybersecurity incident wherein customer information was compromised. This enforcement action, the first-ever enforcement of the SEC's Identity Theft Red Flags Rule, demonstrates the heightened federal enforcement environment at this time, in regard to cybersecurity practices by regulated companies. Therefore it is necessary for those cooling technology providers that are publicly traded to be aware of these additional requirements.

State Laws

In addition to federal laws and enforcement actions, companies should consider the applicability of state laws that relate to cybersecurity and data breach notification requirements. As of the present time, all fifty U.S. states have imposed data breach notification laws, governing any such incidents that affect residents of the respective states. The legal requirements vary among the states, and several states have now required that regulated companies must take "reasonable measures" to protect and secure data that contains personal information. Although several attempts have been made to implement a single national data protection law, such efforts have thus far been fruitless, and companies are cautioned to determine whether they collect, store, or transmit personal information in specific states or relating to residents of specific states.

Critical Infrastructure Protection Considerations

As referenced above, cooling technology companies interface with many critical infrastructure sectors, in both the private and public sectors, and such companies should therefore be familiar with critical cybersecurity threats that place such sectors (their customers) and themselves at risk. Although multiple cybersecurity standards have been developed over the years by several organizations, groups, and think tanks, a recent study has reported that 70% of surveyed organizations identified the NIST Cybersecurity Framework ("Framework") as the most popular standard. The Framework was developed pursuant to Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," which was issued by President Obama in February 2013, and authorized creation of a voluntary critical infrastructure Cybersecurity Framework to address and manage cybersecurity risk. In 2014, the Cybersecurity Enhancement Act of 2014 (CEA) further updated the role of NIST in identifying and developing cybersecurity risk frameworks for voluntary use by critical infrastructure owners and operators, such as cooling tower technologies, to help identify, assess, and manage cyber risks.

The latest version of the Framework, issued in April 2018, provides a potential tool for cooling technology companies to:

1. Describe their current cybersecurity posture;
2. Describe their target state for cybersecurity;
3. Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;
4. Assess progress toward the target state; and
5. Communicate among internal and external stakeholders about cybersecurity risk.

While these five primary functions serve as a useful general framework for analyzing an organization's cybersecurity status, the Framework itself is intended only to complement, rather than replace an organization's risk management, cybersecurity, or compliance programs.

Among the specific measures that may be considered in any such programs, whether based on the Framework or not, are:

1. Developing a formal cybersecurity governance and risk management program, including preparation of formal policies and planning ongoing measures to assess cybersecurity vulnerabilities and maintain inventories of the business technological infrastructure.
2. Creating a Business Continuity and Disaster Recovery Plan to prepare for data breaches, cyber incidents, and similar emergencies/events, and periodically test such plans via drills and staff exercises.
3. Adopt measures to harden critical servers and related hardware, while ensuring that critical software updates are applied on a timely basis.
4. Secure system access by ensuring that physical, administrative, and technical safeguards are in place, such as effective passwords and multi-factor authentication measures.
5. Implement appropriate controls on applications and third party accounts, including separate accounts for administrators and users.
6. Consider encryption of devices where theft or loss is a possibility, such as a laptop, smartphone, or tablet, as well as encryption of communications.
7. Identify and review all customer agreements, vendor agreements, supplier agreements, third party service agreements for compliance with any applicable cybersecurity terms and conditions, and establish procedures for emergency response with such parties in the event of a data breach or similar incident.
8. Initiate a cybersecurity awareness and training program for staff, including on-going training in new risks and potential vulnerabilities
9. Implement a personnel security program to further control access, including periodic background checks and review of the applicable cybersecurity policies.

Additional Cost Considerations

Costs of Data Breach

In further assessing the appropriate level of investment to address potential vulnerabilities, cooling technology companies should further familiarize themselves with potential costs of action or inaction. According to the 2018 Ponemon Data Breach Cost Report, the average cost of a data breach per compromised record was $ 148.00, reflecting a continuing trend of annual increases in total cost, per-capita cost, and average size of data breach (by number of records lost or stolen). The reason for such increasing cost be-

comes apparent when analyzing the multiple and complex measures that must be undertaken by any company seeking to remediate a data breach.

First, affected companies assume breach detection and escalation costs, for such services as forensic and investigative activities, assessment and audit services, crisis management teams, and communications to and with executives and managing boards of directors. Second, notification costs are assumed for creating contact databases, assessing regulatory compliance requirements, engagement of outside experts (including legal counsel), mail expenses, and email and website buildouts for notification. Third, post data breach costs are incurred for help desk set up, follow up investigations, remediation measures (such as credit monitoring and identity theft protection services for affected customers), legal expenses, and regulatory response/defense. Lastly, independent of any lawsuits that may be filed by affected businesses or customers, a data breach may result in loss of business and negative impact on reputation.

Cyber Insurance

Because of the above-described costs, a common component of many cybersecurity programs is securing cybersecurity or data breach insurance, which started being offered by insurance companies in the early 2000s. Such early policies included coverage for business interruption, data asset loss, extortion, crisis management costs, and liability arising out of data breaches. Since that time, as data breach incidents have continued to occur and increase in cost and scope of affected individuals, cyber insurance policies have also been expanded to cover such costs as forensic analysis, privacy or security breach notification and response, and data loss or destruction. Other insurable costs include investigation costs, litigation costs, data restoration, litigation damages, regulatory defense, and penalties.

Among the various types of insurance coverage, first-party coverage addresses costs related to activities that the insured has to undertake in response to a data breach, such as hiring of attorneys, public relations firms, crisis management firms, or computer forensics firms. Other immediate costs include notification costs (i.e. printing and mailing costs), credit monitoring services for affected customers, and establishment of call centers to address customer questions and issues.

In addition, coverages may extend to training employees, establishing data breach information portals/websites, creation of cybersecurity incident response templates, compensation for loss of income (i.e. business interruption), and restoring lost data.

Third-party coverage policies protect the insured from liability to affected third parties, and may include coverage of litigation damages, costs of litigation defense, and costs of regulatory fines and defenses of same.

Conclusion

The current state of the legal, regulatory, and threat environment within which cooling technology companies operate mandates thorough, competent, and on-going assessments of their individual cybersecurity vulnerabilities, preparedness, and resiliency. As participants across multiple critical infrastructure sectors, cooling tower companies stand much to lose if appropriate measures are not taken to address the important issue of cybersecurity, but also have much to gain if they avail themselves of the various resources, both public and private, which are available to strengthen their cybersecurity posture.

The information in this article is provided for general informational purposes only, and may not reflect the current law in your jurisdiction. No information contained in this article should be construed as legal advice from Baker, Donelson, Bearman, Caldwell & Berkowitz, PC or the individual authors, nor is it intended to be a substitute for legal counsel on any subject matter. No reader of this article should act or refrain from acting on the basis of any information included in, or accessible through, this article without seeking the appropriate legal or other professional advice on the particular facts and circumstances at issue from a lawyer licensed in the recipient's state, country or other appropriate licensing jurisdiction.