Sept. 20, 2022
To: CEO and Board of Directors of Berkshire Ontheball
From: Multra guard IDENTIFY Team:Kyle Biery, Melvin Estrada, Mark Hunter, Sam Precie
Subject: Regarding On-Site breach

Summary:

In accordance with this board's Inherent Risk Profile, Cybersecurity Maturity and Statement of Risk Appetite, Multraguard is reporting on the events of July 22nd, 2022.

A nighttime security guard involved with the cyber underground and the leader of a hacking group was hired by the client.

The guard used his security badge to obtain physical access to a computer that controlled the heating, ventilation, and air conditioning (HVAC) for the firm using various methods, including a password-cracking program and a botnet, he rendered the (HVAC) system unstable, eventually leading to a four-hour outage during trading time.

Table 1. Inherent Risk (IR) Profile/Cybersecurity Maturity inputs

Category Inherent Risk	**IR Vulnerabilty**	**Category Cybersecurity Maturity**	**Cybersecurity Maturity Relevant Activities**
Technologies and Connection Types	Significant	**Risk Management & Oversight**	Identified Background Checks as a potential vulnerability
Delivery Channels	Significant	**Threat Intelligence & Collaboration**	
Online/Mobile Products and Technology Services	Significant	**Cybersecurity Controls**	Identified abnormal access & application behavior
Organizational Characteristics	Moderate	**External Dependency Management**	
External Threats	MOST	**Cyber incident Management & Resilience**	Attacker activities were thwarted before network breach or DDOS attack.

Event highlights for ongoing assessment of institutional controls - consistent with (U.S. Federal Financial Institutions Examination Council(FFIEC) “Cybersecurity Assessment Tool”, May 2017)

Lessons Learned:
Failures:

1. Tighter HR requirements / Deeper Background Investigations
2. Better physical security for systems, including limiting electronic access to facilities control areas. Badge access for facilities personnel only. Review contractor's remote access to facilities systems.

Overall Lessons Learned:

3. Systems in place identified unauthorized activity on terminal and/or alarm status on critical (HVAC) equipment and communicated to appropriate personnel.
4. The established systems of backup and restore were available to restore facilities control systems to uncompromised status and normal operation.
5. Facilities vulnerabilities resulted in an overheated server room negatively impacting the direct line of business, trading, by interrupting services for four hours impacting Intrinsic, Business, Performance, Economic and Market value of the organization .

Failures:

First, as seen with the failure to detect the Security Guard's allegiances to the underground hacker group, Human Resources needs to be more thorough with background checks. The need for forensic investigations on personnel should be reviewed and may need to include additional employees.
Secondly, the access to PCs and servers controlling the building facilities equipment need to be secured. Access to these areas were not prohibited to essential personnel. Access control should be reviewed for guards and restricted to essential facility personnel only. Contractor access to systems shall also be reviewed to ensure all systems are consistent with the Board's inherent risk profile and management.

Overall Lessons learned:

In terms of lessons learned, three items stand out. The first is that the implemented Remote Management and Threat Mitigation system on the HVAC systems identified unauthorized/irregular user activity on the terminal and thus should be monitored in similar fashions in the future. Second, established system backups and subsequent implementation were successful in mitigating the issue to a four hour period. The final point is the fact that despite the Facilities computers being on a network isolated from the Line of Business networks, the activities in this incident exploited the vulnerabilities of the server room (power, environmental controls, etc.) which directly impact the company's digital footprint and need a comprehensive review.

For further questions regarding the incident and our examination of the details, please contact Sam Precie or Kyle Biery of Multra-Guard IDENTIFY TEAM via our corporate email (multraguard@cybernet.com) or phone number (403-555-5555).