THOMPSON COBURN LLP Lincoln Churchill ADVISORS BLACKCLOAK

The Potential Cyber Security Crisis Hiding in Plain Sight (At Home)

Although high-profile cyber breaches are increasing in both frequency and severity, a question remains – what level of attention is this important topic receiving from corporate C-suites and their respective Boards, given the outsized implications of potential data breaches? As the global workplace continues to be reshaped by more people working from remote locations (particularly from home), how has this changed the cyber breach risk profile of corporations, and what can be done to combat the increasing risks?

Though many corporations have begun implementing policies governing employees' use of non-corporate *public* WiFi hotspots (e.g., hotels, airports, coffee shops, etc.), less consideration has been given to employees' *home* WiFi networks. It is a given that that employees will access sensitive corporate information from home WiFi networks on both work-issued and personal electronic devices. Beyond the obvious inherent risks of data theft that could include sensitive corporate information, as well as vendor, employee or customer personal data, hackers could also capitalize on personal Internet usage, memberships or leaked passwords. Hackers will invariably look for the easiest route to access information, so why would they try to penetrate a sophisticated, state-of-the art corporate cybersecurity program when they can achieve the same cyber breach by targeting a home network with minimal, standard security?

Think how many people have access to the average home WiFi network in any given month. In addition to immediate family members with their work and personal electronic devices, extended family, friends, neighbors and service providers (e.g., babysitters) often log on. It is logical to assume that any experienced hacker wanting to gain access to a corporate network could likely bypass the best-laid security plans of the corporation and try to gain access at the weakest point in the chain – via the home network of an employee.

Consider for a moment the FBI's "urgent bulletin" issued in early 2018 stating that up to 500,000 home and small office Internet routers were identified as having been compromised with what is believed to be Russian-sponsored malware. These inherent weaknesses in consumer-controlled interfaces present too high of a risk for the information they contain, particularly given that many consumers do little to nothing to enhance the security of their home network – virtual private networks (VPNs) that serve to mask Internet surfing do little to decrease the security risk exposure.

In recognition of the growing corporate risks from cyber breaches / attacks, the U.S. Securities and Exchange Commission (SEC) has recently issued revised and expanded guidance on public

company disclosures of cybersecurity risks and incidents, including the involvement of the company Board in cyber risk oversight. All U.S. states now have enacted legal requirements for the disclosure of security breaches. Notably, the New York Department of Financial Services has expanded the notice requirement to include not just nonpublic personal information that is breached, but also certain proprietary business information. This expansion is especially noteworthy as the New York requirement is being touted as a model for other states, both within and outside the financial sector. In addition to penalties under legal or regulatory requirements for cybersecurity and breach notice, companies and their Boards and senior management also face increasing risk of liability from private lawsuits – from affected consumers, shareholders and partners.

Interestingly, cyber security risk disclaimers have been increasingly added to select publicly-traded company "Safe Harbor" statements acknowledging the risk of a data breach – and the fact that companies cannot fully ensure it will not happen – representing uncertainties that could materially affect the company. Recognizing potential cyber breach threats is an important first step. However, protecting against a cyber breach *while* simultaneously preparing for the worst-case crisis scenarios (operational, legal, stock price and reputational) requires urgent attention by corporations worldwide.

The adverse implications to an untimely or inadequate corporate response to a breach cannot be overstated. In addition to the likely immediate impact on corporate reputation, market position and equity valuation, there are long-term risks and significant legal liabilities from potential shareholder and regulator lawsuits, along with those from customers directly impacted.

Possible Actions to Consider:

- Corporations should ensure that the proper internal controls are put in place and formally communicated to employees at all global locations, including:
    - True multifactor authentication, encryption, endpoint (malware protection);
    - VPNs, firewalls, Intrusion Detection / Intrusion Prevention Systems (IDS/IPS);
    - Behavioral and artificial intelligence anti-malware software;
    - Data retention and destruction schedules and protocols; and
    - Privileged Access Management.

- Employees should be instructed to upgrade their home cyber security controls to ensure they are effective against today's threats, which should include:
    - Reset home routers and keep all router software updated;
    - Utilize a VPN to connect to WiFi;
    - Change default passwords on hardware;
    - Update all passwords regularly and securely store them in an encrypted password safe;
    - Regularly update and patch computers / devices and the programs that run on them; and
    - Use various anti-malware software technologies.

- With the aid of corporate and crisis communications experts as well as internal and external legal counsel, create a Crisis Communications Plan incorporating the most probable cyber breach scenarios and response protocols.
    - The plan must specifically identify which employees (the "rapid response team") are responsible for handling each component of the crisis acknowledgement and remedial steps.
        - After a cyber crisis has occurred is not the time to designate such roles.
        - The crisis communications plan should assign responsibility to individuals tasked with contacting legal authorities, media outlets, employees, shareholders and impacted communities.
        - This is extremely important to avoid confusion and delay in the event of a breach, where every minute counts.
    - Once the initial plan is developed, the rapid response team should practice "war gaming" scenarios through tabletop exercises, at least annually.
        - Participants should include the C-suite along with corporate communications and legal experts, ensuring proper responses and information dissemination strategies are in place were an actual breach occur.
        - Internal Investor Relations, Corporate Communications and Public Affairs professionals should lead this process under the direction of counsel to cover by privilege.
    - Ultimately, the optimal corporate response represents a balancing act between legal and communications skill sets to ensure the proper amount of transparency is provided to all relevant audiences.

Summary

In the current environment, the corporate response time to acknowledge a cyber breach and take appropriate remedial action is now measured in minutes, with a company's reputation, stock price and legal exposure all hanging in the balance. Different stakeholders require varying levels of transparency should a breach occur, which speaks to the importance of a balanced response that covers both legal and corporate communications transparency. Furthermore, a bifurcated Crisis Communications Plan should be constructed, providing a roadmap for the initial response to a given crisis, while a secondary plan is ready to address the long tail after the initial breach is publicly acknowledged.

Internal communication is also key so that management teams understand the nature and scope of risks to the organization, and the ways in which crucial information is accessed and disseminated. Consider utilizing individuals such as legal counsel or consultants who can translate between the management team and company security professionals in conveying and understanding security risks and controls to address them.

Lastly, companies should focus on the cybersecurity practices of its management team and Board and consider providing concierge cybersecurity assistance so the threats from their personal lives, devices and networks do not impact the company.

Lincoln Churchill Advisors
Lincoln Churchill Advisors (LCA) is a leading boutique communications firm providing strategic advice, trusted counsel and proven program execution with a focus on Investor Relations, Corporate & Crisis Communications, Event-driven Communications and Internal Communications.

Understanding that one size does not fit all, LCA avoids "off-the-shelf" solutions in favor of thoughtful, insightful and fully actionable counsel precisely aligned to the situation at hand.

LCA creates customized, highly relevant and impactful Crisis Communications Preparedness Plans that can be rapidly adapted and deployed when needed. Simply put, LCA helps companies stand head and shoulders above their competition in dynamic, ever-changing markets. www.lincolnchurchilladvisors.com

Jim Shreve – Thompson Coburn LLP
[The information provided herein is intended for general purposes only and is not intended to be legal advice]

Jim serves as a trusted advisor to clients facing complex cybersecurity and privacy issues — particularly those in the country's most highly regulated industries. He is the chair of Thompson Coburn's Cybersecurity practice, was named a Fellow of Information Privacy, and holds CIPP/US and CIPT certifications from the International Association of Privacy Professionals.

Jim advises all types of companies on the myriad legal concerns surrounding confidential information and how such information is stored and transmitted. Applying the law to rapidly changing technology and software capabilities, Jim provides clients with a profile of their potential risk, then works closely with their management team, legal, IT, and compliance information security teams to develop a comprehensive and practical plan for risk avoidance and responding to cyber and data-related issues.

Should a company face a security breach, Jim draws on his years of experience handling thousands of incidents to counsel clients through every step of cyber and information security incidents, including notification, reporting, and all associated state, federal, and global regulatory requirements.

Jim helps clients develop robust and responsive security and privacy policies and governance documents, meet applicable data safeguarding requirements, and implement compliance programs.

A recognized thought leader in the fields of cybersecurity and privacy, Jim has presented on a variety of in-the-news cybersecurity topics for industry organizations and associations, including the RSA Conference, the International Association of Privacy Professionals, the ABA and the Mortgage Bankers Association. www.thompsoncoburn.com

Dr. Chris Pierson – BLACKCLOAK

Chris is the Founder & CEO of BLACKCLOAK - a concierge cybersecurity protection suite for high-net-worth individuals and top C-Suite executives. Dr. Pierson is a globally recognized cybersecurity & privacy expert, entrepreneur, thought leader, and Board Advisor. He also serves on the Department of Homeland Security's Data Privacy & Integrity Advisory Committee, Cybersecurity Subcommittee, and is a Distinguished Fellow of the Ponemon Institute.

Previously, Chris was a founding executive of Viewpost, a FinTech payments company, serving as their CSO and General Counsel and was also the first Chief Privacy Officer, SVP for the Royal Bank of Scotland's (RBS) U.S. operations leading its privacy and data protection program. Chris was also a corporate attorney for Lewis and Roca where he established its CyberSecurity Practice representing companies who were hacked and fell victim to data breaches.

Chris is a graduate of Boston College (B.A., M.A.) and The University of Iowa (Ph.D., J.D.), is a globally recognized keynote speaker & cybersecurity thought leader, Board advisor for startups, and is frequently quoted by the media on cybersecurity & privacy. www.blackcloak.io