Preventing, Containing, and Managing Cyber Breaches: Where to Begin?

May 22, 2019

Health-care institutions find it difficult to prioritize their competing cybersecurity objectives due to limited information security dollars and busy IT personnel. There seems to be little guidance on where to focus, despite a long list of steps health information custodians should be taking to safeguard their electronic information and to respond appropriately to cybersecurity incidents.

In our experience, regulators tend to focus on certain issues when conducting cyber breach investigations. These areas of regulatory focus offer some guidance to institutions on where they might concentrate their cyber breach prevention and management efforts. That said, decisions about which initiatives to prioritize will vary across institutions depending on their individual circumstances.

We have found that when considering a cyber breach, regulators often ask what institutional measures are in place in respect to some or all of the following:

- An overall institutional plan for protecting the security of electronic records and preventing cyber breaches (in particular, whether there is a well thought-out plan, whether the plan is reviewed and updated regularly, and whether the institution is checking for compliance);
- Employee training on cyber breaches, both generally and through simulated cyberattacks;
- Backups of electronic records (for example, how often backups are conducted, whether backup files are stored securely offline, or what their retention period is);
- The use of antivirus software, including real-time and regularly scheduled scans;
- Software and operating systems updates (of note, many IT experts consider software updates to be “low hanging fruit” that are inexpensive, are easy to deploy, and significantly enhance overall system security);
- Email systems that identify and quarantine potentially risky external emails and attachments;
- User privileges that grant information access rights based on user roles (“role-based access”) and that grant only the minimum level of access required for a user to carry out their role;
- Active content limitations that limit users’ ability to run computer code embedded in documents.

Hospitals and other health information custodians are encouraged to consider and be prepared to respond to such questions, and to view these different information security measures as forming a cybersecurity “baseline” to work toward.

In addition to asking about preventive measures in place at the time of a cybersecurity incident, regulators often want to know about organizations’ responses to the incidents themselves. Regulators may ask about such issues as:

- The steps taken to immediately contain the cyberattack (for example, disconnecting infected networks from the internet, disconnecting infected machines from the network, locking down shared network drives);
- What electronic information was affected by the cyberattack, how it was affected, and whether the institution was able to limit or prevent access to the information at issue.

These areas of focus suggest that institutions may wish to focus their initial response efforts and resources on containment of any breach before shifting to the fact-finding process.

We would recommend that institutions consider some or all of the following additional breach management steps, depending on the nature of the incident:

- Notifying essential health-care partners, such as other hospitals in the same electronic health record network;
- Notifying insurers and internal or external legal counsel;
- Considering whether an outside cyber forensics expert would be helpful to the investigation process (a decision best made in consultation with legal counsel);
- Sending notification to any applicable regulators (another scenario in which seeking legal advice first is strongly advised);
- Drafting a cyber breach response plan, which considers such issues as containing the breach, removing the ransomware from the infected system, and recovering the data from backup systems.

Every security incident is unique, and the appropriate steps needed to prevent, contain, and handle cyber breaches will vary across institutions based on numerous considerations. Using the above considerations as a general guideline, however, can help an institution maintain a consistent and effective approach.

By

Ira Parghi

Expertise

Cybersecurity, Privacy & Data Protection, Health Care & Life Sciences

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 725 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749