BUSINESSCLASS
KNOWLEDGE • SEMINARS • INSIGHTS

Blakes

Incident Response Plan Checklist

LITIGATION & DISPUTE RESOLUTION

Catherine Beagan Flood
Partner
Direct: 416-863-2269
cbe@blakes.com

Ryder Gilliland
Partner
Direct: 416-863-5849
ryder.gilliland@blakes.com

INFORMATION TECHNOLOGY

Sunny Handa
Partner
Direct: 514-982-4008
sunny.handa@blakes.com

Christine Ing
Partner
Direct: 416-863-2667
christine.ing@blakes.com

PRIVACY

Wendy Mee
Partner
Direct: 416-863-3161
wendy.mee@blakes.com

Birch Miller
Partner
Direct: 403-260-9613
birch.miller@blakes.com

CAPITAL MARKETS

Ross McKee
Partner
Direct: 416-863-3277
ross.mckee@blakes.com

Every business should have a plan detailing how to respond to a possible cybersecurity incident. The plan should not be too long or too short, otherwise it will not be useful if an incident occurs. Here is a step-by-step checklist on how to create an effective incident response plan:

Step 1: Draft It

- ☐ Response team members
- ☐ How will the response team be contacted? (include alternative methods in case company email is compromised)
- ☐ Who will contact the cybersecurity insurer?
- ☐ Who to notify and when (e.g., board, customers, regulators, law enforcement, etc.)
- ☐ Back-end technological response options, including third parties to hire if necessary
- ☐ How to document actions taken
- ☐ How to preserve privilege over the investigation
- ☐ Identify a sole team member to speak to the media
- ☐ How to reduce the risk of litigation
- ☐ What global considerations are there? (e.g., different laws/practices with respect to personal information and privacy)

Step 2: Test It

- ☐ Run a simulation, evaluate your company's response, adjust the plan
- ☐ Document simulation results and responses to be able to prove you take cybersecurity seriously
- ☐ Provide opportunities for cross-functional teams — legal, IT and top executives — to get to know each other and educate each other on respective cybersecurity expertise
- ☐ Designate leaders to implement the plan (e.g., IT head for technology response, legal for communication with the board, executives, etc.)

Step 3: Line Up Third Parties

- ☐ Establish agreements with vendors in advance (e.g., PR, forensic, outside counsel, etc.)

Step 4: Keep It Fresh

- ☐ Update the plan periodically; it will not be helpful if, for example, the plan requires the head of IT to be contacted but that person no longer works there