How to Develop a Cyber Attack Incident Response Plan – A List of Key Considerations

Prepared by:
Wendy Hulton
Dickinson Wright

LORMAN®
Published on www.lorman.com - July 2018

INTRODUCING

Lorman's New Approach to Continuing Education

ALL-ACCESS PASS

The All-Access Pass grants you UNLIMITED access to Lorman's ever-growing library of training resources:

- ☑ **Unlimited Live Webinars** - 120 live webinars added every month
- ☑ **Unlimited OnDemand and MP3 Downloads** - Over 1,500 courses available
- ☑ **Videos -** More than 1300 available
- ☑ **Slide Decks -** More than 2300 available
- ☑ White Papers
- ☑ Reports
- ☑ Articles
- ☑ ... and much more!

Join the thousands of other pass-holders that have already trusted us for their professional development by choosing the All-Access Pass.

Get Your All-Access Pass Today!

SAVE 20%

Learn more: www.lorman.com/pass/?s=special20

Use Discount Code Q7014393 and Priority Code 18536 to receive the 20% AAP discount.

*Discount cannot be combined with any other discounts.

HOW TO DEVELOP A CYBER ATTACK INCIDENT RESPONSE PLAN – A LIST OF KEY CONSIDERATIONS

Written by Wendy Hulton – 5/16/18
Original content comes from the Canada-U.S. Business Law Blog – www.canada-usbizlawblog.com

Along with my colleagues on the Dickinson Wright Cybersecurity Team, I recently attended the Incident Response Forum in Washington, D.C. The Forum, sponsored by Dickinson Wright, brought together the top government cyber-prosecutors and cyber-investigators, attorneys and experts who specialize in data breach response. These experts discussed the most important and timely data breach response topics. After sitting all day in a room full of cyber experts – I am completely certain that it is a question of "when" not "if" we are all going to suffer cyber incident(s).

I want to share some of the key insights from the Incident Response Forum as the lessons are important for all business and legal counsel to consider:

- It is vital that legal professionals be involved both before, for preemptive steps, and acting as the quarterback during an incident response. While breaches frequently make headlines, experts say the number of incidents that actually lead to lawsuits is relatively low often because of the involvement of experienced legal counsel.

- Be prepared for the legal and compliance aftermath of a data breach including governmental investigations and litigation, as well as the almost endless list of potential civil liabilities after a cyber attack.

- Appointing the right experts is critical. My colleague, Justin Root led an informative panel at the Forum on "How to assess and choose an incident response forensic vendor." It goes without saying that use of the wrong people and/or investigation method during the first 72 hours can be fatal to a successful investigation.

- Collect artifacts, remnants and fragments in the aftermath of a data breach. The information gathered during forensic analysis, enables legal and compliance professionals to manage efforts to detect additional attempts by the attacker to regain access and get closer towards containment of the attack.

- Prepare an analysis of cyber concerns for Incident Response teams, which typically cross borders and are global in nature. Take into consideration the EU's General Data Protection Regulation (GDPR), evolving policies of major social media platforms and strategy for attempting to maintain attorney client privilege globally.

- Research and create best practices for handling the insurance issues arising after a data breach and current issues in the cyber insurance market, an area which legal and compliance professionals will need to understand during an incident response.

- Research and create best practices for protecting the attorney-client privilege as it applies to the work product from digital forensic investigators and other consultants responding to a data breach.

As you have probably heard, PIPEDA's mandatory breach notice provisions are coming into force in November and we will be

blogging about what you need to do to stay out of trouble after our next post on the EU's General Data Protection Regulation (GDPR).

In the meantime, do you think businesses are prepared to meet the challenge of cyber attacks? What are your key concerns about managing and preparing for cyber attacks? If you have any comments and opinions on our blog post, please leave them on my Linkedin page linkedin.com/in/wendyhulton, or on the Dickinson Wright Canada, LinkedIn or Twitter page.

About the Author:

Wendy Hulton is a Partner in Dickinson Wright's Canadian Employment Law Group. She provides employment law advice to a wide range of employers on a variety of workplace issues, including discipline and wrongful dismissal matters, workplace privacy, human rights management and litigation and health and safety issues. In addition, she provides advice on cannabis, dietary supplements, natural health products, foods, drugs, cosmetics, medical devices and a wide range of consumer products. Wendy can be reached at 416-777-4035 or whulton@dickinsonwright.com and you can visit her bio here.