The state of Cyber-risk and IT-security risk management: Questions for corporate directors

By Josée Morin, Eng., MBA, CDir., jo.morin@videotron.ca

The following is a generic list of questions that to help corporate directors evaluate the state of of Cyber-risk and IT security risk management in a business that is starting to implement a structured risk management approach. There may be risks that are not covered in this list or questions that do not apply to your situation.

Key data assets

1. What are the key data assets that we own, that are the most central to our business (meaning that if those data were stolen, it would cause the most harm and monetary loss)? For example:

    - Business plans and merger and acquisition strategies and discussions
    - Contracts with customers, suppliers, partners
    - Employee login credentials
    - Facility information
    - R&D information including new products development and IP
    - Information about key business process
    - Source code
    - List of employee, customers, suppliers, contractors
    - Client data

2. Can we put evaluation the losses that would be incurred if the key data assets are stolen, in dollars and other impacts?

3. Where do each of the key data assets reside, and if online on which systems?

4. Do we own these key data assets or do we host it for our customers?

5. How are the key data assets accessed, who has permission to access them?

6. Do we have legal, regulatory and contractual obligations regarding the key data asset, to ensure we are protecting it and reporting incidents? If so, what are they? How do we make certain we comply?

Key IT systems

7. What are the IT systems that are central to conducting our business (meaning that if we lost access to these systems, we would have difficulty doing our day to day business and or we would lose important revenue)? For example:

   - Customer relationship management (CRM)
   - Contract management
   - Email
   - Enterprise Ressource Planning (ERP)
   - On-line store

8. Can we put evaluation the losses that would be incurred if the IT systems are not available, in dollars and other impacts?

9. Do we have Service Level Agreements with users, or availability metrics, for those systems, what are they, historically do we meet them?

IT Infrastructure security

10. Who oversees cyber and infrastructure security?

11. Can you describe our IT security infrastructure? How current and effective is it?

12. How do we protect each of the systems where the key data assets and key IT systems are hosted?

13. Do we monitor these systems 24-7? With on-call employees?

14. How often do we test our protection infrastructure to guarantee its functionality?

15. Can we detect attacks and/or intrusions? Have we in the past (give statistics) ? How do we report it and to whom?

16. Do we detect malicious code, unauthorized mobile code, etc?

17. Do we have policies and procedure established for data security and do we verify they are known enforced? For example:

    - restricting user installation of application
    - ensuring patches are installed
    - updating software applications
    - restricting user privileges
    - restricting physical access
    - having power outage contingencies in place and tested
    - promptly removing access for terminated employee

- collecting only the required personal information
- ensuring that development and testing environment is separated from the production environment
- destroying and purging old data no longer required
- recording and monitoring all logs
- monitoring all network traffic
- using data encryption
- performing ongoing reiterative backups and testing them
- establish the parameters by which you allow BYOD
- securing the cloud

18. What is the budget and resources we spend on protecting our data including detecting and responding?

19. Are our employees aware of cyber security risks and of the role they should play to protect data including their security responsibilities? How often do we train them?

20. Are our third-party suppliers aware of cyber security risks and of the role they should play to protect data including their security responsibilities?

21. Do we monitor information about emerging threats, legislation, new technology and methods? What do we do to stay up to date?

22. What operational metrics are currently tracked by IT? By management?

Response plan and insurance

23. Do we have a recovery plan if our business systems go down (disaster recovery plan)? Is it up to date? How frequently do we test it is working?

24. Do we have a response plan and recovery plan if our data gets hacked? Does it include lessons learned, PR management, communication of breach? How often do we test it?

25. Do we have insurance for business interruption? business systems breach or cyber security breach?