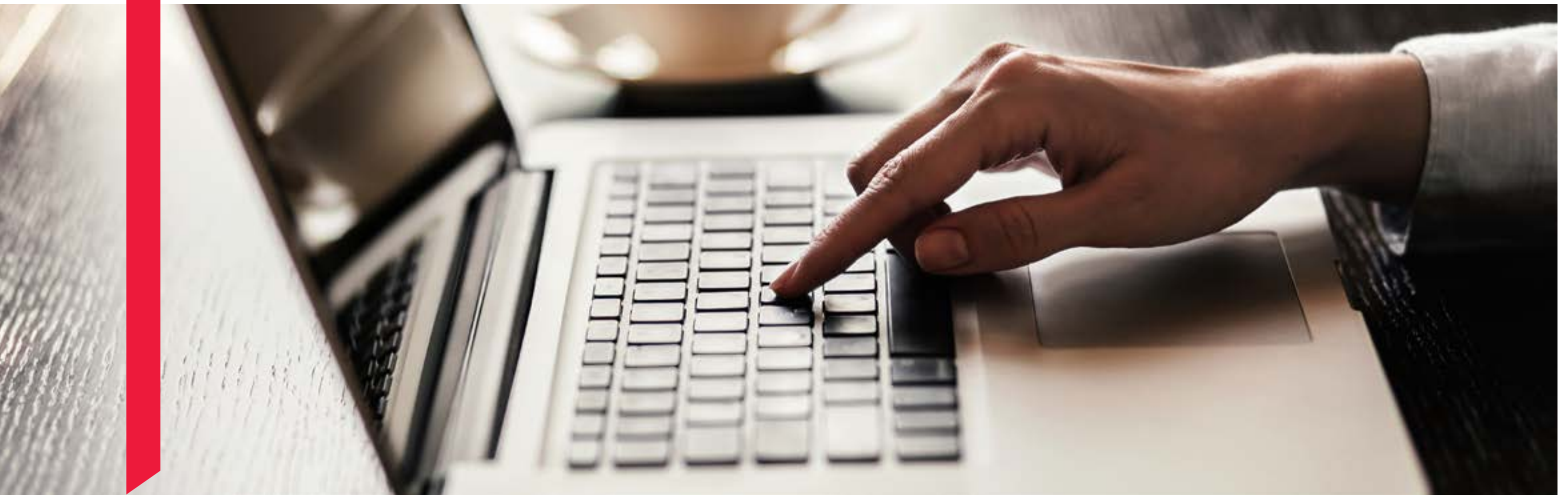

AUGUST 2019

HOW TO PREVENT AN EQUIFAX-TYPE DATA BREACH IN YOUR COMPANY

The Equifax cybersecurity data breach first came to light almost two years ago. Yet the passage of time hasn't dimmed its power. It still ranks as something of a corporate ghost story - a nightmare tale of data lost and brand damaged.

Unlike ghost stories, the Equifax breach is all too real. It battered the company's stock price and its reputation. It also affected more than 143 million people around the world, including 19,000 Canadians.

The Equifax aftermath

This past spring, the Office of the Privacy Commissioner of Canada completed its investigation of the breach and released its findings. Both the U.S. and Canadian companies, it said, had failed in their privacy obligations.

Concerns included "poor security safeguards; retaining information too long; inadequate consent procedures; a lack of accountability for Canadians' information and limited protection measures offered to affected individuals after the breach."

There are some important questions that have been raised as a result of the breach. Why were Equifax servers accessible to anyone on the internet? Why were default passwords used? How did the Equifax security team fail to act on obvious weaknesses in their security strategy?

What is clear is that Equifax's information security program had insufficient oversight, incentive, and reporting requirements to maintain an effective security position.

What to do

Equifax's policies and security controls fell far short of operational procedures needed to monitor and mitigate risk, and to maintain an effective cybersecurity program. The following controls, which are a subset of a cybersecurity control framework, are some of the primary controls that Equifax could have adopted to keep its data safe.

1. **Security Architecture**

   Start with standard network perimeter design to mitigate against the classic attacks including:

   - Internet facing firewalls multiple zones for web, application and data servers
   - VLAN segmented internal networks dependent on business need

2. **Security Controls**

   Implement robust access control procedures such as:

   - Use two-factor authentication, especially for all privileged access accounts
   - Periodically review accounts and permissions
   - Enhance the access control with newer technology such as an identity access management solution

3. Extra Protection for Valuable Data

   Valuable data should be protected by measures beyond the standard security precautions. Measures must include:

   - Encryption of databases and communications sections
   - Behavioral analysis of system and file access logs
   - Enhanced monitoring

4. Patching and Vulnerability Testing

   A Patch Management Program will reduce the vulnerability issues on your network. Vulnerability assessment is essential even with a patch management program in place to ensure effective protection.

Think strategically

Organizations need to shift from focusing on individual security threats to establishing best practice and embedding information security behaviors that mitigate cybersecurity risks with robust preventive and detective controls. One of the best ways to establish an effective cybersecurity program is to comply with industry-leading cybersecurity frameworks. The two primary frameworks are System and Organization Controls (SOC) for Cybersecurity and the National Institute of Standards and Technology (NIST).

REQUEST A FREE CONSULTATION

How to select your cybersecurity compliance partner

BDO has extensive knowledge of cybersecurity compliance frameworks and can help your company assess your current cybersecurity position and then establish and maintain a continuously secure environment. We can assist you with understanding your most critical cybersecurity gaps and provide recommendations and remediation support in order for your company to be able to protect its data.

You want a cybersecurity compliance partner that can work closely with you and tailor their approach to meet your unique needs and business requirements. It is critical to develop a solution that fits with the organization's resources and needs, which includes leveraging existing templates and expertise to accelerate the process, identifying potential issues at the planning stage and understanding the expectations of the end users. Contact us today for a preliminary assessment of your business requirements.

TO LEARN MORE, CONTACT YOUR LOCAL BDO OFFICE OR:

Sam Khoury, CPA, CITP, CRISC
Partner, Advisory Services
National Financial services Leader
416-369-6030
skhoury@bdo.ca

Vivek Gupta, MBA, CISA
National Cybersecurity Leader
416-369-7867
vgupta@bdo.ca

ABOUT BDO

One of the nation's leading accounting firms, BDO Canada provides assurance, accounting, tax, and advisory services. As a member of the BDO international network, which spans more than 150 countries and 1,400 offices, BDO provides seamless and consistent cross-border services to clients with international needs.

ABOUT BDO'S FINANCIAL SERVICES PRACTICE

The Financial Services industry is a changing landscape, marked by regulatory reform, disruptive technology, and new service delivery channels. And BDO is dedicated to helping our clients not only navigate in this landscape, but succeed in it, too. Our services, ranging from governance, risk and compliance to business process reviews and more, are tailored to meet the unique needs of financial services organizations.

www.bdo.ca/financial-services