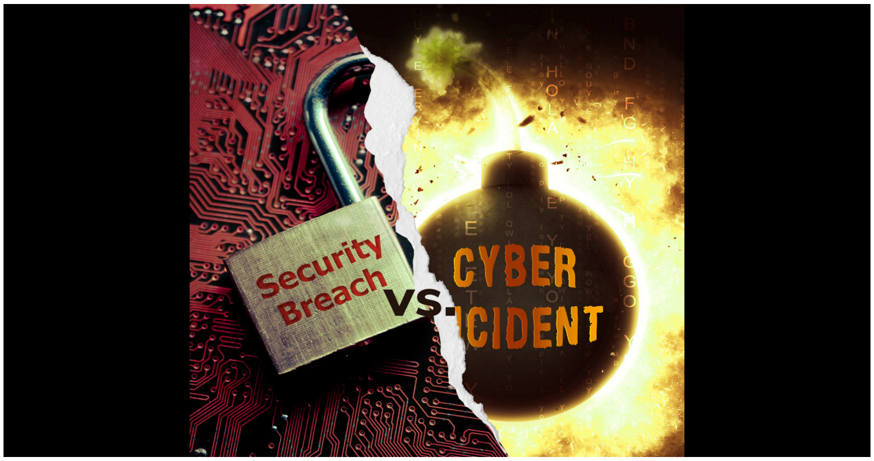
idea LOGICAL

LOGICAL TALK · JUNE 2021 EDITION



What Is the Difference Between Security Incident And Security Breach?

During the pandemic, three in 10 Canadian organizations have seen a spike in the volume of cyberattacks. Sensitive customer and business information are constantly at risk.

Cyberattacks like phishing, spear phishing, malware, ransomware are evolving and getting successful with each attack. A successful cyberattack for a hacker means a business is compromised, leaving devastating aftereffects.

"Today, every business, regardless of its size, should have a Disaster Recovery & Business Continuity Plan," says the president of Idealogical - Andre Vittorio.

Usually, the terms "security incidents" and "security breaches" are referred to in the news media. But, the two words have two different meanings. Understanding the difference between a Security Incident and Security Breach will help you craft an appropriate response plan.

It is essential to understand the difference between a Security Incident and Security Breach to recognize your business needs.

What is the difference between Security Incident vs. Security Breach?

A security incident refers to a violation of an organization's security policy. The violation can happen in the form of an attempt to compromise confidential business and/ or personal data. In contrast, a security breach involves unauthorized access to any data or information.

For example, if a cybercriminal has been successful in deploying malware to your system, just the presence of malware can be referred to as a security incident. However, if the malware was successfully able to cause damage to your system, it is referred to as a security breach.

But just the presence of malware in your system does not constitute as a security breach.

Your Disaster Recovery & Business Continuity Plan must include details on actions for cyber incidents and cyber breaches.

What is a Security Policy?

Cybersecurity is no more just a concern for management and IT departments. Each employee of an organization plays a role in protecting IT systems and data. A Cybersecurity Policy sets usage and behavioural standards for employees, which acts as a guiding principle on using technology internet and other IT systems.

A cybersecurity policy includes does and doesn't like encryption of email attachments, clicking on links, sharing passwords etc.

Idealogical Joins Canadian Chamber Of Commerce in Strengthening Cybersecurity Measures In Canada

The Canadian Chamber of Commerce has newly launched Cyber.Right.Now Campaign in an effort to enhance federal focus on cybersecurity for budget 2022.

The Chamber has recognized Idealogical's effort towards protecting small and medium-sized businesses across GTA from cyberattacks as a responsible managed service provider. As a result, Idealogical has been invited to be one of the select few organizations across Canada to help the Chamber guide the federal government in the right direction towards its cybersecurity investment efforts in 2022.

Upon receiving the invitation, the president of Idealogical shared, "I am thrilled to represent the small business on this important decision-making table. Even though Idealogical is not a cybersecurity firm, we make every effort to protect our clients as their trusted IT service providers."

"For cyber right now campaign, my objective would be to attract the committees focus on supporting small businesses with benefits in terms of financial relief for tools and training that will help the businesses to continue operations with peace of mind of security."

Objectives of the Cyber. Right. Now. Campaign

The Chamber recognizes that Canadians are lucky that our country has a strong cybersecurity foundation in place, with a number of significant global companies calling Canada home.

While the recently released 2021 federal budget did dedicate significant investments in cybersecurity to secure government IT infrastructure, it made no specific commitment to help Canadian businesses boost their cybersecurity measures.

At the same time, our most direct competitors in the US, Israel, and the UK are investing billions. Small and mid-sized Canadian organizations, in particular, are in need of greater cybersecurity threat awareness, protection, and training to utilize the full suite of tools at their disposal to keep Canadians safe from bad actors.

Canada is well-positioned on cybersecurity, but our global competitors are moving fast. Increased investment in cybersecurity stands to benefit communities across Canada from both job creation and from improved Canadian cybersecurity accessibility and protection.

Together we can champion technology made in Canada, by Canada, for Canadians and the rest of the world.

Superstar Of The Month - Luv Bakshi

I feel humbled; it has been an amazing journey so far. The support of the team and my colleagues has always been phenomenal and kept me motivated in managing work and clients in the best possible manner.

I thank the entire Idealogical team for the encouragement as a newcomer, where it never felt like I just started. This award and recognition would put a thrust to my pace to work harder and exceed expectations!!