DIGITALLY SPEAKING

# HACK ATTACK

## PROTECTING CORPORATE REPUTATION WHEN YOU HAVE BEEN DIGITALLY EXPOSED

**What do AshleyMadison.com, The RCMP, Sony, Home Depot, Apple, Target, United Airlines and Jeep Cherokees all have in common? They were all hacked in 2015 by cyber criminals who compromised the privacy, credit card information and safety of billions of people, worldwide.**

Hackers have exposed millions of cheating spouses, breached Canadian government computers to access classified national security documents, stopped vehicles on the highway by hijacking their computer systems, and used malicious software to infect computers and spy on people through their own webcams.

It is compelling proof that no matter how big a company is, or how sophisticated its IT department, every organization is vulnerable. With the proliferation of companies using cloud-based technology to make company data even more digitally accessible, the risks of a breach have escalated substantially and communicators need to be prepared.

It is estimated that in 2013, hackers cost the global economy more than $400 billion a year—$3 billion in Canada alone—affecting companies in all sectors. It is becoming a major issue because Canada is the second-largest target in the world for cybercrime according to Intel Security's 2014 report, Net Losses: Estimating the Global Cost of Cybercrime. In fact, the Canadian government alone has invested $240 million over the past five years to guard against similar threats both foreign and domestic.

In the UK, 93 per cent of large companies and 87 per cent of small businesses reported a cyber breach in the past year, and the financial and reputational costs of recovery are astronomical. Case in point: humbled U.S. retailer Target estimated that their 2013 data breach cost the company $420 million.

> "CANADA IS THE SECOND-LARGEST TARGET IN THE WORLD FOR CYBERCRIME."
>
> **Source:** Net Losses: Estimating the Global Cost of Cybercrime. Intel Security, June 2014

**Communicators must be prepared**

Most tech security experts agree that it's no longer a question of if your organization will be hit by a cyber-attack, but when. So as communicators, it is absolutely crucial to assess how prepared your organization is to combat a digital disruption and start planning. As the guardians of reputation for our organizations and clients, it is essential that professional communicators are prepared to respond to this type of a crisis.

In my reputation risk work with CEOs across North America, I have seen firsthand the disconnect between the C-suite and technology. Thanks in part to these high-profile attacks and the emergence of online reputation threats, executives are starting to proactively invest resources to be better prepared.

They realize just how vulnerable their companies have become. In fact, Intel Security's Canadian survey also revealed that only 23 per cent of CEOs believe their companies are very well prepared for cyber-attacks.

Based on nearly 20 years of experience developing crisis and reputation strategies for companies small and large, here are my six hack attack crisis survival tips:

1. **The plan:** Prepare and annually test a comprehensive hacker crisis communications response plan with well-defined, unambiguous messaging, policies and processes that clearly outline decision-making authority and enable rapid-response capabilities based on various cyber-attack scenarios.
2. **Communication:** Ensure that your crisis response team has 24/7 access to the plan, contact information and a channel to connect as a group remotely within minutes to ensure decision makers can assess the risk level, activate the plan and hit the ground running.
3. **Never over-promise:** The temptation among the C-suite will be to reassure employees, customers and other key stakeholders that you have secured your systems and have returned to business as usual. Be forewarned; if you make a public pronouncement that you have secured your systems to prevent this from happening again, you have just challenged the hackers to prove you wrong. Every technology is vulnerable.
4. **Training and resources:** The crisis response team, IT staff, and rank-and-file employees must all be properly trained and clearly understand their roles to prevent and manage a hack attack. Smart companies already have consultants on retainer to manage both the technology side of the data breach and the reputational damage it will cause. Timing is crucial and, to mitigate losses, you want to surround yourself with a team of experts who know what they are doing.
5. **Technology:** Your organization must invest in critical firewall and related security technologies, and then communicators should collaborate closely with IT to create enterprise-wide awareness among employees to minimize threats such as malware from suspicious emails that access a computer and the network.
6. **Media preparedness:** Ensure your spokespeople, ideally subject-matter experts, have been thoroughly media trained on camera. The communications team must be available to coach and adapt pre-approved crisis plan messaging to match the current and evolving circumstances as more information becomes available. Timing is crucial. Your organization needs to get ahead of the story to frame the conversation and appear as transparent and informative as possible.


ABOUT
**HEATH APPLEBAUM, ABC, BA, MCM, OCGC**

Heath Applebaum, ABC, BA, MCM, OCGC, is the owner of Echo Communications Inc. a reputation management consulting company based in Toronto. Heath has developed and led crisis and reputation strategies for dozens of clients from start-ups to multinational companies over the past 17 years. He is also an Accredited Business Communicator, Gold Quill winner, and industry thought leader who has spoken at more than 50 industry conferences around the world.


TOP