ITL #323 Brand protection: a cybersecurity checklist

— 1 month, 2 weeks ago

Cyber-attacks and data breaches can be incredibly damaging. Organizations must get on top of managing the risk. By David Eisenstadt.

The growing cyber siege on corporate Canada is causing management leadership to spend more time, money and concerted efforts to defend against cyber-attacks and data breaches. While no sector of the economy is immune, the real estate industry might become an appealing target.

At tcgpr in Canada, we work closely with our IPREX Global Communication partner, SDI, based in Washington, DC., where Tom Davis and Frank Platsis lead their Cybersecurity, Privacy and Data Security practice.

Based on our collective experience, it is important to diagnose your company's risk of becoming the next victim of a crippling cybersecurity threat, so you'll need to have answers to these questions.

Does your organization have a CISO?

Is there someone who is directly and visibly responsible for your organization's information security program? If so, you are addressing the primary issue.

But having someone on board with the formal title of chief information security officer (CISO) is the gold standard. The CISO should be a member of the executive management team and have the authority, accountability and tools to get the job done. Not having a CISO is seen as a significant vulnerability, and will be a major problem if your company does suffer a breach.

Have your company's data "crown jewels" been identified and are they protected properly?

Among the data proprietary to every company, there is some high value data — the "crown jewels" — that must be given the highest level of protection. Whether intellectual property, business plans, privileged information on potential mergers and acquisitions or board proceedings, it is critical that those assets are identified and management fully understands where they reside, who can access them and how they are protected.

To paraphrase Sun Tzu, prior to understanding the intentions and capabilities of your enemies, you must first "know yourself."

Is there a comprehensive plan for managing a cyber-attack that poses the threat of crisis?

Businesses need to have their policies and procedures for managing responses to a crisis documented in an integrated plan. The intent of the plan is to set forth the process that will be used to mitigate the damage from a data breach and minimize recovery time. The plan should cover notification and activation of the response management team and include clear escalation procedures in terms of who needs to be informed and when. It is important that all key business functions — operations, legal, IT, security, regulatory, HR, compliance and PR be represented on the team. The roles and responsibilities of each function should be clearly detailed in advance.

Full appreciation of cyber risk includes understanding how cybersecurity and physical security may intersect. A company's chief information security officer and chief security officer should work together with other corporate leaders, to assess risk holistically. The integration of cyber and physical security will become even more significant with the rapid growth of the Internet of Things — devices that communicate with each other and the Internet via wireless connections — and reliance on legacy technology to thwart cyber offensives.

Is your board of directors conversant with your approach to managing cyber risk?

Even if your board is not demanding such information, management should regularly explain to the board its ongoing assessment of cybersecurity risks and articulate its plan to address them. To fulfill their fiduciary oversight responsibilities, it is important that boards identify governance responsibilities for cybersecurity. Will these responsibilities reside at the full board or a subcommittee such as the audit or risk committees? It is important that companies set the appropriate tone at the highest levels.

Are you evaluating your plan through exercises?

Exercises are designed to support the development of a robust response capability, train team members in their roles and responsibilities, and evaluate the policies and procedures in the response plan. Using a range of cyber scenarios you can enhance capabilities by stress-testing response and recovery plans and build a more cyber-resilient enterprise. Exercises ought to be conducted regularly to include pentesting (https://searchsecurity.techtarget.com/definition/penetration-testing) from a technical perspective and tabletops to address decision-making.

Lessons learned from these exercises should be incorporated back into the comprehensive plan, which by necessity will be a "living document" to stay apace with new and emerging threats.

Does your response plan detail how communications will be handled in the event of a cyber-attack?

One critical asset sure to be imperiled by a cyber-attack is your corporate reputation. How effectively you communicate will either raise or lower the cost to your reputation and consumer and shareholder confidence.

Your response plan should identify what stakeholders would be affected, what concerns each stakeholder group will have, and how those concerns will addressed. It should make clear who will communicate on behalf of the company, and what communications tools will be used.

It must also define how internal communications will be handled, for your employees will not only have concerns, but will be seen as “voices” of the company. Consider conducting a dress rehearsal of a data breach notification that includes the CEO and CISO. CEOs must master the ability to strategically communicate the technical complexities of cyber risk in plain English, whereas CISOs must be savvy in communicating their know-how from a management and business perspective. Translation is key.

What’s your exposure to third party suppliers?

Third-party suppliers present unique risks to any organization. They often provide portals into a company's technology platforms that attackers may exploit. Your response planning should include assessing cyber risks presented by third-party vendors and subcontractors to ensure they meet appropriate cybersecurity standards.

Are you creating an internal culture of cybersecurity?

Educating your employees about best practices in cybersecurity is one of the most effective ways to reduce your company’s risk profile. Every organization should have a training program that helps employees understand how to avoid falling victim to schemes that attempt to use them to create unauthorized access to your data. Employees should clearly understand their obligations to protect data, as well as best practices in using email, web browsing, using social networks and employing their mobile devices.

It’s 2019. Isn’t it time to get with the program?

The author

David Eisenstadt is Founding Partner of tcgpr.com, the Toronto-based Canadian Partner of IPREX (https://iprex.com/) Global Communication.

Email

deisenstadt@tcgpr.com (mailto:deisenstadt@tcgpr.com)

Website

http://www.tcgpr.com/ (http://www.tcgpr.com/)

The Author

David Eisenstadt (/news/itle/author/David%20Eisenstadt/)

David Eisenstadt is Founding Partner of tcgpr.com, the Toronto-based Canadian Partner of IPREX Global Communication.

mail the author (mailto:deisenstadt@tcgpr.com)
visit the author's website (http://www.tcgpr.com/)

Forward, Post, Comment | #IpraITL (https://twitter.com/search?q=%23IpraITL&src=typd)

We are keen for our **IPRA Thought Leadership essays** to stimulate debate. With that objective in mind, **we encourage readers to participate in and facilitate discussion.** Please forward essay links to your industry contacts, post them to blogs, websites and social networking sites and above all give us your feedback via forums such as IPRA's LinkedIn group. A new ITL essay is published on the IPRA website every week. Prospective ITL essay contributors should send a short synopsis to IPRA head of editorial content Rob Gray email (mailto:editor@ipra.org)

← ITL #322 Intercontinental prospects: navigating the uncharted waters of global agency procurement (/news/itle/itl-322-intercontinental-prospects-navigating-the-uncharted-waters-of-global-agency-procurement/)

ITL #324 - The consumer is your co-driver: social media amplification strategies → (/news/itle/itl-324-the-consumer-is-your-co-driver-social-media-amplification-strategies/)

Comments

ALSO ON IPRA

IPRA and Pakistan extend co-operation: 25 October 2017, London, United Kingdom

1 comment • 2 years ago

Hasan Zuberi — On behalf of Council of PR Pakistan, I would like to thank the IPRA for all their cooperation and interest in development of PR sector in Pakistan. My sincere thanks and regards to the whole IPRA team especially the President Mr. Bart de Vries, and the Sec Gen Mr. Philip Sheppard.Hasan Zuberi
Founder President
Council of PR Pakistan

ITL #308 A big step beyond messaging: the importance of communicators challenging business

2 comments • 5 months ago

ipra — _____

ITL #257 The importance of trust in brand loyalty: building customer relationships through doing good

1 comment • a year ago

Waqas Kazmi — Hi Anne Bahr,It's a nice read. I love the idea of ME to WE and this post helped me to understand that how a brand can strategize its policies to win TRUST while supporting society at large.i think that small and medium brands (market wise) are unable to adapt this ME to WE policy either due to weak organizational vision or lack of financials. The point is if brands understand and implement this approach that will not only portray brand's image positively that led to profits but bring a massive positive change in underprivileged societies as well.Thanks for this wonderful post!

ITL #207 Indian pharma: managing reputational risk in the digital era

1 comment • 2 years ago

abhinav kanchan — Very well written piece and immensely thoughtful. Complex things said simply is the hallmark of good communication. I agree with Seema's views, good preparation and anticipating things will be helpful.

(https://www.ipra.org/golden-world-awards/2019-gwa-gala/)

(/news/itle/become-an-author/)

AUTHORS

Search

ARCHIVE

2019

2018

2017

2016

2015

2014

2013

2012

2011

2010

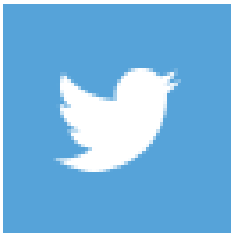
2009

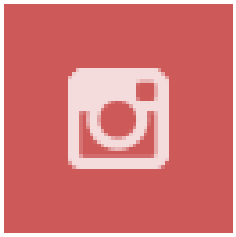
2008

2007

2006

FOLLOW IPRA:






(https://twitter.com/ipraofficial) (https://www.facebook.com/ipraofficial) (https://www.instagram.com/ipraofficial/) (https://www.linkedin.com/groups/689597)

Tweets by @ipraofficial

IPRA
@ipraofficial

Why are some public figures able to survive and sometimes even thrive despite repeatedly causing offence? Read the latest Thought Leadership Essay by Gerry McCusker at ipra.org

Embed View on Twitter

Golden World Awards (/golden-world-awards/winners)
2019 GWA Gala (/golden-world-awards/2019-gwa-gala/)
2019 GWA Judges (/golden-world-awards/judges/)
2019 Rules & Dates (/golden-world-awards/rules/)
2019 FAQ (/golden-world-awards/faq/)
Categories (/golden-world-awards/categories/)
GWA Winners (/golden-world-awards/winners/)
GWA Gala 2018 (/golden-world-awards/gwa-gala-2018/)
GWA Gala 2017 (/golden-world-awards/gwa-gala-2017/)
GWA Gala 2016 (/golden-world-awards/gwa-gala-2016/)

Member Services (/accounts/login)
Member Login (/accounts/login)
Join IPRA (/member-services/join-ipra/)
Find a PR Professional (/member-services/find-a-pr-professional/)
Member Directory (/member-services/member-directory/)
Code of Conduct (/member-services/code-of-conduct/)
PR Books (/member-services/pr-books/)
PR Training (/member-services/pr-training/)
Payment Options (/member-services/payment-options/)
Renew Membership (/member-services/join-ipra)
Gold Paper (/member-services/gold-paper/)

Governance (/governance/board/members/)
Board (/governance/board/members/)
Contact (/governance/board/contact/)
Privacy Policy (/governance/privacy-policy/)

News (/news/itle)
Thought Leadership Essays (/news/itle/)
IPRA and the UN (/news/ipra-and-the-un/)
Charter for Media Transparency (/news/charter-for-media-transparency/)
Press Room (/news/press-room/)
Arabic Website (http://www.ipra-ar.org)

Events and Conferences (/events-and-conferences/events)
Events (/events-and-conferences/events/)
World Congress Johannesburg 2015 (/events-and-conferences/world-congress-johannesburg-2015/)

History (/history/ipras-story/)
IPRA's Story (/history/ipras-story/)
People (/history/people/)
Associations (/history/national-associations/)
Press Freedom (/history/press-freedom/)
Origin of Ethics (/history/origin-of-ethics/)

IPRA
Suite 5879
POB 6945
London W1A 6US
P: (Phone) +44 1634 818308

email (mailto:info@ipra.org)