The Conference Board of Canada

Zero-Day Vulnerabilities

Briefing August 2019

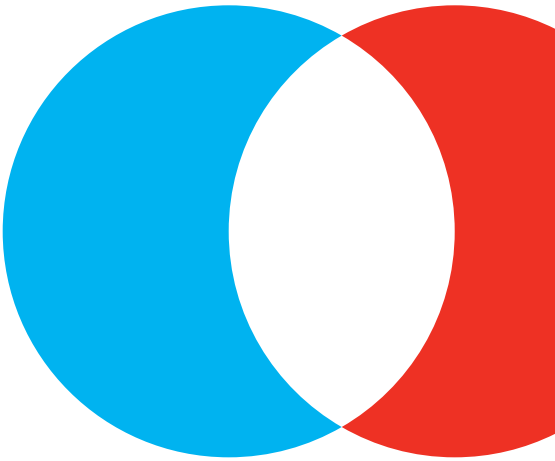
Acknowledgements

This briefing was prepared by Rachael Bryson, Senior Research Associate, and Dr. Vanessa Thomas, Senior Research Associate. Stacey Noah, Associate Director of Information Technology, The Conference Board of Canada, provided an internal review. The Conference Board of Canada relies on external reviews to provide constructive, candid comments on most of our reports. Thank you to Daniel Craigen, Director of Carleton University's Global Cybersecurity Resource, for taking on this task.

This briefing was funded by the Cyber Security Council.

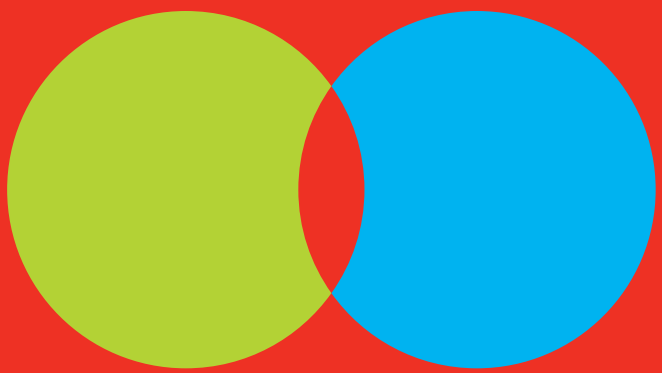
Any omissions in fact or interpretation remain the sole responsibility of The Conference Board of Canada.

Contents



Zero-Day Vulnerabilities

Executive summary



Zero-day vulnerabilities—weaknesses in computer code that are not publicly known and can be or are being exploited by malicious actors—are an ongoing concern for individuals and organizations.

As zero-day attacks continue to have major effects and consequences,[1] we must consider best practices and technical assessments to make sense of zero-day challenges and prevention strategies. The unique nature of zero-day vulnerabilities is that they cannot be consistently predicted, and there is often very little, if anything, that organizations can do in terms of prevention.[2] Additionally, much of the activity around zero-day vulnerabilities takes place on the black market.[3] These factors contribute to a limited amount of up-to-date analysis, difficulties verifying evidence, and limited data availability about the frequency, nature, and scope of future zero-day vulnerabilities. Despite these challenges, there are steps organizations can take to mitigate the impacts of such attacks.

This briefing aims to offer a clear definition of zero-day vulnerabilities and their threat environment and to identify and explain some of the key challenges surrounding zero-day vulnerabilities and responding to them. We conclude by offering five recommendations that can help organizations mitigate, although not eliminate, the effects of these vulnerabilities and attacks:

1. Develop and enforce good cyber-hygiene habits across your organization.
2. Build your organization's cyber resilience.
3. Build cooperation and information-sharing among your organizational communities.
4. Monitor zero-day vulnerability markets.
5. Invest in "bug bounty" programs.

Not all organizations will be able to implement these five recommendations; this is especially understandable in the case of the last two recommendations. Organizations should work with their internal security, technical, and legal experts to determine which of our recommendations are most attainable.

1 Ablon and Bogart, *Zero Days, Thousands of Nights*.
2 Last, "Forecasting Zero-Day Vulnerabilities."
3 Ablon and Bogart, *Zero Days, Thousands of Nights*.

What is a zero-day vulnerability?

A zero-day vulnerability is a type of bug or weakness in software code that can be exploited and is not publicly known.[1,2]

Within the security industry, there are slight variations in defining what "counts" as a zero-day vulnerability. For example, according to Emery, a "zero-day vulnerability is a vulnerability that is found before the software manufacturer has discovered it, or, if the manufacturer has discovered it, before the manufacturer can take action to correct it."[3] This definition aligns with Norton Security's, which states that a zero-day is "a newly discovered software vulnerability. Because the developer has just learned of the flaw, it also means an official patch or update to fix the issue hasn't been released."[4] Both of these definitions are restrictive because they account only for a software developer's or manufacturer's discovery of the vulnerability; however, other people and organizations can discover a zero-day.

A vulnerability is still considered to be "zero day" if it is known to other individuals or entities and the public is not aware of it. For example, government security agencies, the original software developers, and third-party information technology (IT) security firms may know of a zero-day vulnerability long before it becomes public knowledge.[5] There is also a marketplace for these vulnerabilities where hackers will buy knowledge of the vulnerability so they can exploit it.

The questions of public knowledge and exploitability are key: zero-day vulnerabilities "have been known about [publicly] for zero days."[6] In this sense, there have been zero days to develop a solution to, or to patch, the vulnerability.[7] This is the key differentiator between zero-day vulnerabilities and other software vulnerabilities. Flaws or errors are frequently found in software code, programs, or operating systems.[8] Companies will provide updates to their software that include patches to fix these vulnerabilities. The onus then rests with the customer to install these updates, or risk leaving known security gaps open for exploitation.[9]

1 Jardine, *Global Cyberspace Is Safer Than You Think*.
2 Bilge and Dumitras, "Before We Knew It."
3 Emery, "Zero-Day Responsibility."
4 Norton, "Zero-Day Vulnerability."
5 Emery, "Zero-Day Responsibility."
6 Baylon, Brunt, and Livingstone, *Cyber Security at Civil Nuclear Facilities*.
7 Jardine, *Global Cyberspace Is Safer Than You Think*.
8 Norton, "Zero-Day Vulnerability."
9 Jardine, *Global Cyberspace Is Safer Than You Think*.

In medicine, vaccines can only be developed for diseases and viruses we know exist. Similarly, for software, patches can only be developed for flaws or errors that we know exist.

A **zero-day attack** is when a zero-day vulnerability is exploited by a hostile entity before there is much, if any, awareness of the risk. Because the vulnerability is not publicly known, and likely unknown by the original code source or manufacturer, there is no patch available for it.[10] For these reasons, zero-day vulnerabilities offer an advantage to would-be attackers. Sun and others write that "[the] information asymmetry between what the attacker knows and what the defender knows makes zero-day exploits extremely hard to detect."[11] Before software developers and/or third-party IT security firms are even aware of the vulnerability, or while they are trying to develop a patch to fix it, they may be hit with an attack seeking to exploit it.

The challenge of zero-day vulnerabilities

Zero-day vulnerabilities present a challenge to individuals and organizations. In medicine, we can develop vaccines only for diseases and viruses we know exist. The same is true for software; patches can only be developed for flaws or errors that we know exist. Zero-day vulnerabilities can affect any "internet-connected device, network component or piece of software."[12] Our growing demand for connectivity will lead to an increase in the potential points of vulnerability and opportunities to exploit flawed code. The inability to act to protect oneself will be exacerbated by several key challenges: the availability and speed of patches, the commodification of zero-day vulnerabilities, and information-sharing.

Availability and speed of patches

Zero-day vulnerabilities may be made public either by the discoverer or because a major malware attack has occurred; they are rarely announced by a manufacturer.[13] Once a zero-day vulnerability is known, many manufacturers race to develop patches that will address the problem.[14] However, some manufacturers—depending on the industry and business model—are not as dedicated to addressing their code's issues. Others, including manufacturers of certain types of Internet of Things (IoT) devices

10 Bu, "Zero-Day Attacks Are Not the Same as Zero-Day Vulnerabilities."
11 Sun and others, "Towards Probabilistic Identification of Zero-Day Attack Paths."
12 Ohio State University, The, "What Is a Zero-Day Exploit?"
13 Baylon, Brunt, and Livingstone, *Cyber Security at Civil Nuclear Facilities*.
14 Clark and others, "Familiarity Breeds Contempt."

(e.g., medical devices or in-home products), might have few options for deploying a patch.[15,16]

To revisit the medical analogy, vaccines require time to develop and implementation is imperfect: it takes time to roll out vaccines, and some people may choose not to get vaccinated. In software, a patch is like a vaccine. Patches take time for software companies to develop and rollouts of patches are time-consuming. In some cases, patches are imperfectly applied.

A company may have limited motivation or feel there is limited economic benefit for them to develop a patch for two reasons. First and foremost, a patch can be expensive to develop. Second, software companies know that implementing a patch can be an imperfect process and that users may not apply the patch as quickly as possible. This means they will still be exposed to an attack and still blame the company for the issue.

The development time for patches is also a significant factor in combatting zero-day attacks. It is possible that code originators or manufacturers may be the first to learn of a zero-day vulnerability and may have time to develop a patch and send out updates to users. However, once a zero-day vulnerability is known by a "black hat" (malicious) actor, or is publicly known, reusable malware can be deployed with much greater speed and effect than a patch can be developed and deployed.[17]

Commodification of zero-day vulnerabilities

The potentially catastrophic effects of zero-day attacks have given rise to a complex marketplace for information about zero-day vulnerabilities.[18,19] Because they are rare, zero-day vulnerabilities are also extremely valuable.[20] An article in the *International Journal of Computer, Information Science and Engineering* indicates "that a major percentage of discoverers, a majority in some cases, are unaffiliated with the software developers and thus are free to disseminate the vulnerabilities they discover in any way they like."[21] This has contributed to the commodification of zero-day vulnerabilities on black markets.

A legitimate, regulated market exists for information on zero-day vulnerabilities. There are two kinds of information sellers: "white hats," who are not-for-profit driven and may be security experts who seek to share information to prevent zero-day attacks;[22] and discoverers, who will seek rewards or "bug bounties" but who are not hackers or other potential exploiters. Buyers may consist of original software developers and third-party security service providers. These organizations will have strict procedures to follow when someone wants to disclose a zero-day vulnerability and transactions are documented, although the seller may remain anonymous.[23]

15 Zou, "IoT Devices Are Hard to Patch."
16 Simpson, Roesner, and Kohno. "Securing Vulnerable Home IoT Devices With an In-Hub Security Manager."
17 Bradshaw, *Combatting Cyber Threats*.
18 Egelman, Herley, and van Oorschot, "Markets for Zero-Day Exploits."
19 Bradshaw, *Combatting Cyber Threats*.
20 Jardine, *Global Cyberspace Is Safer Than You Think*.
21 Algarni and Malaiya, "Software Vulnerability Markets."
22 Emery, "Zero-Day Responsibility."
23 Algarni and Malaiya, "Software Vulnerability Markets."

Discovering a zero-day vulnerability requires significantly more skill than exploiting it, thus allowing discoverers to benefit financially without carrying out a cyber attack themselves.

Finding a zero-day vulnerability typically requires a high level of skill, and prices of upwards of US$100,000 can be commanded on the legitimate market for proven zero-days.[24] Google's Vulnerability Reward Program currently offers between US$100 and US$31,337 for proven vulnerabilities.[25] Facebook's Bug Bounty Program offers a minimum of US$500 and does not list a maximum reward amount;[26] and Microsoft offers up to US$250,000.[27]

These prices can also be commanded on the black market—an unregulated market where discoverers will sell information on zero-day vulnerabilities to individuals who may use them to launch a zero-day attack.[28] Discovering a zero-day vulnerability requires significantly more skill than exploiting it, thus allowing discoverers to benefit financially without carrying out a cyber attack themselves.[29]

While some zero-day vulnerabilities are being exchanged and sold in the legitimate and black markets, evidence suggests that they are being sold in increasing numbers to state intelligence agencies. A number of studies suggest that some states openly carry out this practice; others indicate that state intelligence agencies may be operating in the black market, attempting to prevent sales to malicious actors or to acquire knowledge of these vulnerabilities for their own purposes.[30,31] This represents a significant grey area, as there are no legislative frameworks that cover state ownership responsibilities concerning this information.[32]

Information-sharing

Government ownership of information about zero-day vulnerabilities presents an additional challenge in this space, as there is no requirement on the part of state security agencies to disclose these vulnerabilities to code originators, manufacturers, or the public.[33] Bradshaw explains[34] that states have a very clear motive for wanting exclusive access to this information:

> **States view the Internet as a new domain, which has led them to develop their own malware and scripts for exploiting other states, and to hoard zero-day vulnerabilities. The quest for geopolitical power and a strategic military advantage over another state's cyber defences is sometimes at odds with the state's responsibility to ensure public safety and secure cyberspace, because developing new exploits or leaving old vulnerabilities unaddressed creates risk in the system.**

24 Egelman, Herley, and van Oorschot, "Markets for Zero-Day Exploits."
25 Google, "Google Vulnerability Reward Program (VRP) Rules."
26 Facebook, "Information."
27 Warren, "Microsoft Will Now Pay Up to $250,000 for Windows 10 Security Bugs."
28 Emery, "Zero-Day Responsibility."
29 Algarni and Malaiya, "Software Vulnerability Markets."
30 Emery, "Zero-Day Responsibility."
31 Algarni and Malaiya, "Software Vulnerability Markets."
32 Jardine, *Global Cyberspace Is Safer Than You Think*.
33 Ibid.
34 Bradshaw, *Combatting Cyber Threats*.

Calls for enhanced regulation of this market and mandatory disclosure to the private sector have emerged because of both the risks that zero-day vulnerabilities pose to individuals, organizations, and national security and the potential benefits of early warning to the private sector. However, significant challenges remain in determining how to balance regulation with national security and how to expand a regulatory framework in a space that is significantly populated by cybercriminals.[35]

The 2018 Conference Board of Canada briefing *Building Cyber Resilience* recommended that organizations adopt a five-pillar model for building cyber resilience: Prepare, Protect, Detect, Respond, and Recover.

Strategies for mitigating zero-day vulnerabilities and attacks

How can organizations protect themselves in this complicated space, where the threat of zero-day vulnerabilities, by their very definition, cannot be avoided? Our research has identified five key recommendations to help organizations prepare for and mitigate the impacts of zero-day vulnerabilities and attacks.

1. Develop and enforce good cyber-hygiene habits across your organization.

Good cyber hygiene encompasses many of the basics of corporate cyber security and can help limit the general cyber incidents an organization may have. Some of these measures include implementing phishing training programs for employees; having standards for personal online behaviours on work devices; securing personal (or "bring your own") devices or isolating their access to a separate network; and making software updates mandatory. Accepting software updates and patches is emphasized, as they could include valuable fixes for recently discovered zero-day vulnerabilities that your organization may not yet be aware of.[36]

35 Emery, "Zero-Day Responsibility."
36 Norton, "Zero-Day Vulnerability."

2. Build your organization's cyber resilience.

Cyber resilience is defined as "an organization's ability to limit the impact of cyber disruptions, maintain critical functions, and rapidly re-establish normal operations following a cyber incident."[37] Cyber resilience goes beyond cyber security in that it acknowledges that the likelihood of an organization experiencing a cyber incident is virtually inevitable. This shift in thinking from building firewalls to keep everything out to building better business continuity practices for the eventuality of a cyber incident is crucial to improving organizational preparedness for dealing with zero-day vulnerabilities and attacks.

In July 2018, The Conference Board of Canada published *Building Cyber Resilience*, a briefing meant to clarify the definition of "cyber resilience," outline a framework for building cyber resilience, and identify recommendations for employing the framework. It recommended that organizations adopt a five-pillar model for building cyber resilience: Prepare, Protect, Detect, Respond, and Recover. This framework is based on the National Institute of Standards and Technology (NIST) framework for cybersecurity resilience.[38]

3. Build cooperation and information-sharing among your organizational communities.

As numerous community organizations[39] and academics[40] have recognized, software developers and manufacturers would benefit from building partnerships across their communities. These partnerships could facilitate information-sharing and help improve the protection available to software users.

Organizations could also engage with the Computer Security Incident Response Team (CSIRT) community. CSIRTs are informal networks of security experts who cooperate to leverage their specialized skills to prevent, detect, and respond to Internet security incidents. These teams can even be formalized and used to conduct incident analysis and undertake "information sharing and dissemination, and skills training."[41]

Belonging to a networked community, whether formally or informally, could be a major advantage in receiving information on newly discovered zero-day vulnerabilities, and would be helpful should an organization be hit by a zero-day attack.

37 Bryson, *Building Cyber Resilience*.
38 NIST, "Cybersecurity Framework."
39 Information Systems Security Association, "About ISSA."
40 Solansky and Beck, "Enhancing Community Safety and Security."
41 Bradshaw, *Combatting Cyber Threats*.

4. Monitor zero-day vulnerability markets.

Make sure your organization is aware of when new zero-day vulnerabilities enter the legitimate or black markets and that you are protected against known vulnerabilities. Organizations without sufficient internal resources to monitor these marketplaces, or that are hampered in their efforts to monitor black markets in particular, can leverage third-party information security companies that offer this monitoring service.[42] Additionally, NIST maintains the National Vulnerability Database,[43] which is just one of several open source databases that lists known vulnerabilities—including already-published zero-day vulnerabilities.

5. Invest in "bug bounty" programs.

A study out of the University of California, Berkeley, has found that vulnerability reward programs—also called "bug bounty programs"—are an "economically efficient mechanism for finding vulnerabilities, with a reasonable cost/benefit trade-off." Programs that encourage discoverers to disclose found vulnerabilities for set prices can be "[more] cost effective than hiring expert security researchers to find vulnerabilities."[44]

These programs should be designed as legitimize financial reward systems and should be transparent in their structure and requirements.[45,46] If successful, vulnerability reward programs can give organizations time to address bugs before they are discovered by another party and possibly exploited. It is interesting to note that one study found that "researchers will often responsibly disclose bugs even if the organization the bug applies to does not have a bug bounty program." They may offer organizations time to address the vulnerability before making it public. This incentivizes the code originator or manufacturer to act quickly.[47]

If designing and implementing a "bug bounty" program is beyond the resources or expertise of your organization, consider partnering with other organizations that share the same concerns. For example, engage a third-party information security company that has a record of purchasing zero-day vulnerability information as a way to improve the overall security of their clients. Returning to the medical analogy, this would be akin to joining a health insurance program that had a history of procuring vaccines for similar ailments.

42 Algarni and Malaiya, "Software Vulnerability Markets."
43 NIST, "National Vulnerability Database."
44 Finifter, Akhawe, and Wagner, "An Empirical Study of Vulnerability Rewards Programs."
45 Ibid.
46 Emery, "Zero-Day Responsibility."
47 Ohio State University, The, "What Is a Zero-Day Exploit?"

Appendix A
Bibliography

Ablon, Lillian, and Andy Bogart. *Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits*. Santa Monica, CA: RAND Corporation, 2017.

Algarni, Abdullah M., and Yashwant K. Malaiya. "Software Vulnerability Markets: Discoverers and Buyers." *International Journal of Computer, Information Science and Engineering* 8, no. 3 (2014): 480–90.

Baylon, Caroline, Roger Brunt, and David Livingstone. *Cyber Security at Civil Nuclear Facilities: Understanding the Risks*. London: Chatham House, 2016.

Bilge, Leyla, and Tudor Dumitras. "Before We Knew It: An Empirical Study of Zero-Day Attacks in the Real World." In *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, 833–44. New York, NY: ACM, 2012. Accessed July 24, 2019. https://doi.org/10.1145/2382196.2382284.

Bradshaw, Samantha. *Combatting Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity*. Waterloo, ON, and London, U.K.: Centre for International Governance Innovation and Chatham House, 2015.

Bryson, Rachael. *Building Cyber Resilience.* Ottawa: The Conference Board of Canada, 2018.

Bu, Zheng. "Zero-Day Attacks Are Not the Same as Zero-Day Vulnerabilities." *Fireeye*, April 24, 2014. Accessed July 24, 2019. https://www.fireeye.com/blog/executive-perspective/2014/04/zero-day-attacks-are-not-the-same-as-zero-day-vulnerabilities.html.

Clark, Sandy, Stefan Frei, Matt Blaze, and Jonathan Smith. "Familiarity Breeds Contempt: The Honeymoon Effect and the Role of Legacy Code in Zero-Day Vulnerabilities." In *Proceedings of the 26th Annual Computer Security Applications Conference*, 251–60. New York, NY: ACM, 2010. Accessed July 24, 2019. http://doi.acm.org/10.1145/1920261.1920299.

Egelman, Serge, Cormac Herley, and Paul C. van Oorschot. "Markets for Zero-Day Exploits: Ethics and Implications." In *Proceedings of the 2013 New Security Paradigms Workshop*, 41–46. New York, NY: ACM, 2013. Accessed July 24, 2019. http://doi.acm.org/10.1145/2535813.2535818.

Emery, Alek Charles. "Zero-Day Responsibility: The Benefits of a Safe Harbor for Cybersecurity Research." *Jurimetrics: The Journal of Law, Science & Technology* 57, no. 4 (Summer 2017): 483–503.

Facebook. "Information." 2018. Accessed July 24, 2019. https://www.facebook.com/whitehat.

Finifter, Matthew, Devdatta Akhawe, and David Wagner. "An Empirical Study of Vulnerability Rewards Programs." In the *Proceedings of the 22nd USENIX Conference on Security*, 273–88. Berkeley, CA: USENIX Association, 2013.

Google. "Google Vulnerability Reward Program (VRP) Rules." 2018. Accessed July 24, 2019. https://www.google.com/about/appsecurity/reward-program/.

Information Systems Security Association (ISSA). "About ISSA." 2016. Accessed July 24, 2019. https://www.issa.org/page/AboutISSA.

Jardine, Eric. *Global Cyberspace Is Safer Than You Think: Real Trends in Cybercrime*. Waterloo, ON, and London, U.K.: Centre for International Governance Innovation and Chatham House, 2017.

Last, David. "Forecasting Zero-Day Vulnerabilities." In *Proceedings of the 11th Annual Cyber and Information Security Research Conference*, 13:1–13:4. New York, NY: ACM, 2016. Accessed July 24, 2019. http://doi.acm.org/10.1145/2897795.2897813.

NIST. "Cybersecurity Framework." Accessed July 24, 2019. https://www.nist.gov/cyberframework.

—. "National Vulnerability Database." Accessed July 24, 2019. https://nvd.nist.gov/.

Norton. "Zero-Day Vulnerability: What It Is, and How It Works." n.d. Accessed July 24, 2019. https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work-30sectech.html.

Ohio State University, The. "What Is a Zero-Day Exploit?" n.d. Accessed July 24, 2019. https://cybersecurity.osu.edu/cybersecurity-you/avoid-threats/what-zero-day-exploit.

Simpson, Anna Kornfeld, Franziska Roesner, and Tadayoshi Kohno. "Securing Vulnerable Home IoT Devices With an In-Hub Security Manager." In *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 551–56. Kona, HI: IEEE, 2017.

Solansky, Stephanie T., and Tammy E. Beck. "Enhancing Community Safety and Security Through Understanding Interagency Collaboration in Cyber-Terrorism Exercises." *Administration & Society* 40, no. 8 (2009): 852–75.

Sun, Xiaoyan, Jun Dai, Peng Liu, Anoop Singhal, and John Yen. "Towards Probabilistic Identification of Zero-day Attack Paths." In *2016 IEEE Conference on Communications and Network Security (CNS),* 64–72. Philadelphia, PA: IEEE, 2016.

Warren, Tom. "Microsoft Will Now Pay Up To $250,000 for Windows 10 Security Bugs." *The Verge*, July 26, 2017. Accessed July 24, 2019. https://www.theverge.com/2017/7/26/16044842/microsoft-windows-bug-bounty-security-flaws-bugs-250k.

Zou, Xu. "IoT Devices Are Hard to Patch: Here's Why—and How to Deal With Security." *TechBeacon*. Accessed July 24, 2019. https://techbeacon.com/security/iot-devices-are-hard-patch-heres-why-how-deal-security.

Where insights meet impact

Zero-Day Vulnerabilities

Rachael Bryson and Vanessa Thomas

To cite this : Bryson, Rachael, and Vanessa Thomas. *Zero-Day Vulnerabilities*. Ottawa: The Conference Board of Canada, 2019.

The Conference Board of Canada

Publication 10405
Price: Complimentary
conferenceboard.ca