CIO ASSOCIATION OF CANADA

A CIO ASSOCIATION OF CANADA REPORT

GEOPOLITICAL IMPACTS OF CYBERSECURITY ON THE PRIVATE SECTOR

Dr. Thomas P. Keenan, FCIPS, I.S.P., ITCP, University of Calgary
in collaboration with
Ron Murch, I.S.P., ITCP, University of Calgary

In partnership with:

DARKTRACE

Unintended Consequences of Widespread Adoption of "Anytime, Anywhere" Information

The Internet has its roots in geopolitical dynamics. It was first envisioned in 1966 as ARPANET - a United States Department of Defense project to enable remote access to computers. At the height of the Cold War, there was serious national security concern about how to maintain strategic communications in the event that another nation disabled portions of the national communications network. Today, the technology of the Internet has made possible the vision that Bill Gates put forth at the COMDEX conference in 1990 when he spoke about "Information at Your Fingertips[1]." The Internet enables almost anyone with a cell phone to connect to any computer, anywhere and copy, edit, or delete any digital asset. It has also opened the door to a world full of unauthorized users, who, through error or, more commonly, malice, seek to get at those digital assets. In addition to criminals, sometimes working in large teams, the perpetrators can include nation states, industry competitors, and ideologically-driven organizations and individuals, all of whom want to focus in on your proprietary digital materials and most likely inflict a world of hurt directly on you.

The Pointy End of the Cybersecurity Spear

If you have information or other digital assets to protect, you are quite possibly staring at the pointy end of the cybersecurity spear. Who's on the other end? You may never find out. But consider this disturbing chronology:

- Over ten years ago, in 2010, a computer worm called Stuxnet[2], was discovered in the Iranian nuclear facility at Natanz. It was intended to cause physical damage to Siemens centrifuges in that facility that were used in nuclear enrichment processes. It has never been conclusively proven, but it is widely accepted, that Stuxnet was created by American and Israeli intelligence agencies to stop or slow Iran's nuclear armament program[3].
- In 2014 and 2015, as part of the conflict in Crimea, Russia engaged with Ukraine in a variety of cyberwarfare attacks[4] that interrupted telecommunications and electrical power to the Ukraine, interfered with elections, and generally caused societal havoc[5].
- Also in 2015, a cyberattack was carried out on the U.S. Office of Personnel Management[6] and the sensitive personal data of an estimated 22 million Americans was exfiltrated[7]. The attack was attributed to the Chinese military and then, in 2017, Equifax was attacked by a similar group. In 2020 four members of the Chinese military were formally charged[8] with that 2017

cyberattack on Equifax. Then, in 2018, Starwood Hotels suffered a similar attack by a similar group. The US indictment covered nine offenses.

- In 2016, the US Election was tampered with[9] and in 2018, twelve Russians were charged in connection with those activities[10].
- During the siege of the U.S. Capitol building on January 6, 2021, intruders were seen rifling through the desks of several Senators, photographing documents. Perhaps even more troubling is the disappearance of a laptop computer belonging to Speaker Nancy Pelosi. While we don't know exactly what was on her laptop, the FBI is investigating the possibility that someone was trying to sell it to Russia[11].
- In a chilling reminder of how exposed our critical infrastructure is to cyberterrorism, the SCADA system at a drinking water treatment plant in Florida was hijacked on February 6, 2021, with the unidentified invaders increasing the level of sodium hydroxide (lye) in the water to poisoning levels[12].

The Whole World Wants in on the Action

The idea that computers and networks could be weaponized to attack other technological targets wasn't a huge concern for the first two decades of the Internet. Now, we're about 35 years and substantial technological development later. As mentioned above, in addition to the United States, the Chinese, the Russians, the Iranians, the North Koreans, and others, have all engaged in launching malware – but not as experiments. They are deadly serious about engaging in cyber warfare to promote their ideologies and are equally serious about industrial espionage to gather intellectual property for the benefit of their nation's commercial interests. The global adoption of the Internet for governmental, economic, and personal benefit, along with the extremely widespread use of unregulated social media, and the variety of inexpensive devices for data storage and connectivity, have all contributed to vastly increased opportunities and elevated risks for competitive and combative cyber-attacks. Highly-specialized technical programming/hacking tools also mean that these attacks can be disguised and obscured – sometimes for very long periods of time. The risks to the target organizations and societies are quite high – both from a financial and even a life-or-death perspective.

"Business Risk?" you say? Enter the CISO.

The official role of a Chief Information Security Officer (CISO) can be traced back to 1995 when Steve Katz[13] joined Citicorp/Citigroup and was appointed CISO there. The emerging field of cybersecurity was still in its infancy but was seen as necessary to

prevent unauthorized access. Since that first "organizational" recognition by Citicorp in 1995 – that cybersecurity was an important organizational function worthy of executive-level responsibility – the field has grown massively, from the perspectives of both the "bad guys" and the "good guys".

The CISO Division of the CIO Association of Canada

In 2019, the CIO Association of Canada established its CISO Division to enable CISOs to network, share ideas, offer CISO support and learn from each other. It provides a primary, common destination for CISOs and security leaders to congregate and participate in strategic initiatives. In a series of on-line sessions held in September and October 2020, the CISO Division focussed on the geopolitical implications for cybersecurity. This article summarizes the important content and implications of those sessions. Then, within three days of FireEye's announcement of the "SolarWinds incident"[14] in mid-December, the CISO Division also quickly organized focussed, collaborative discussions to help CISOs respond to that specific incident by sharing their knowledge, expertise, and experiences. While the full recordings of these sessions are restricted to "members only", summaries are available publicly on the CIO Association website at ciocan.ca

Darktrace Shares their Insights with CIOs

As with a previous series of CIO Association CISO discussions which focussed on Identity Management[15], these discussions were held under Chatham House Rule, so no speakers other than the presenters are identified by name, title or corporate affiliation. That said, we can all gain from their considerable collective wisdom about how to anticipate, prevent, detect, and respond to cybersecurity events that might be motivated by more global geopolitical dynamics and events.

The sessions were led by David Masson, Director of Enterprise Security for Darktrace and moderated by Martin Kyle, Chief Information Security Officer (CISO) for Payments Canada. They were held as videoconference conversations in which approximately twenty of Canada's top CISOs explored the implications of various geopolitical dynamics and events – both in distant countries and closer to home – and what lessons could be gleaned from the actions and impacts that their colleagues had experienced.

These sessions would later prove to be quite prescient as on December 13, less than 8 weeks later, FireEye announced that it had detected the SolarWinds intrusion in its systems and attributed that to a foreign nation state attack. Then, on January 6, 2021, as the United States was formalizing the results of its Presidential Election, there was an attack by a large and vigorous mob on the Washington Capitol Building that resulted

not only in the deaths of five people, but also several concerning cybersecurity-related incidents – including the disappearance of Speaker Pelosi's laptop mentioned above.

Whodunit? – The Vexing Problem of Attribution

Masson shared some of his experience and insights into the dynamics of an orchestrated cyberattack and the motivations behind it.

If someone attacks you, it's just human nature to want to know all the details:

- Who did it?
- Why did they do it?
- How did they do it?
- Were there vulnerabilities that should have been patched?
- Did I somehow invite this through bad practices?
- What harm did the intruder cause?

Experts generally agree that the first two questions are usually the least important. Unless it's a competitor or someone with a grudge against you or your firm, the who and the why is a lot less important than the what and the how.

The discussions quickly highlighted a number of best practices, including:

- The value of vigilance and highly-reliable intrusion detection processes.
- The key role that broad user education and training play in prevention
- The need for responsive and up-to-date regulatory and legislative frameworks within which to operate
- The value of knowledgeable and supportive corporate governance.

After some discussion, the main conclusion from this initial session was that we can't rely on the legislative and regulatory agencies to protect us – they cannot respond quickly enough. An organization needs to maintain a very reliable and up-to-date inventory of its digital and other information-based assets, and deliberately factor protection of them into its organizational risk management planning. In some cases, very valuable assets (like trade secrets) should not even be in digital form.

What About Emerging Technologies??

The second session started with a poll to see who had already experienced a "machine-speed" attack. A majority, 57%, of the CISOs attending said "Yes". And, in a second poll later in the session, 45% indicated that they had experienced a "Zero Day" attack.

David Masson described how "the bad guys" are now using Artificial Intelligence (AI) and Machine Learning (ML) to craft automated attacks on selected targets. Along with

high-performance computing available to almost anyone now, AI/ML enables skillful composition of very realistic and believable phishing emails aimed at collecting legitimate user credentials. Once the intruders gain access, these technologies make it possible and relatively easy to enable automatic surveillance and cataloguing of the target organization's network-accessible resources leading to exfiltration of assets. According to Masson, the only way to detect an AI attack is to have AI looking for it by analyzing, in real time, the behavioural usage patterns of legitimate users to detect unusual behaviours and identify potential infiltrators.

The discussion then turned to the characteristics of nation state attacks – how to identify them and what to do? These attacks are often well-funded and very patient – what Masson described as "low and slow". The sort of activity that is highly skilled, very technical, and not easily detected. The known habits of some countries are that they are patient – they are playing a "high-stakes, long game" scenario – and they often use tools that have been leaked by/from other countries to help disguise their activities (like the NSA tools leaked by Shadow Brokers in 2017[16]).

Nation State Interests

The last session in the three-part CIOCAN series continued an open and very frank exploration of nation state attacks. If you might be tempted to think that you or your organization doesn't need to be concerned about these issues, you might want to think again. The conversation in this session raised some important issues of direct concern to Canadian business organizations. Many of these were recently reflected in "Private firms can't protect us from digital attacks. Government must step in" – a recent article published on ZDNet on February 18[17]. There was also a detailed exploration of the collaboration involved in taking down the Trickbot malware[18]. This attack enabled a zombie computer network and posed a major ransomware threat to banking and other systems. Several organizations from the US Cyber Command to Microsoft collaborated closely in this counteroffensive.

Some of the insights and lessons learned from the SolarWinds incident are presented in another report on the CIOCAN website[19]. While attribution is difficult, many experts believe that SolarWinds had its origins with the Russian SRU intelligence agency. Even more worrisome is the suggestion by Microsoft CEO Brad Smith that SolarWinds attacks are continuing. In a February 14, 2021 interview with 60 Minutes, Smith called SolarWinds "the largest and most sophisticated attack the world has ever seen." Smith estimated that creating this malware involved more than 1,000 developers and that attacks are ongoing[20].

Masson highlighted the potential challenges involved with the merging of Information Technologies (IT) and Operational Technologies (OT). This convergence presents a significant risk vector for very damaging attacks on an organization's operating environment by using their externally-exposed IT networks – and this includes direct consequences for its customers and supply chain. It wasn't long before we had a stark example of the potential for serious societal impacts. The attacks on the SCADA system of a Florida water treatment plant[21], revealed on February 8, are yet another example of these risks – bringing together Information Technology (IT) and Operational Technology (OT). In the past, industrial control was often carried out by specialized systems, running some variety of the UNIX operating system. Now, for economic and functional reasons, organizations are moving to "common, off the shelf" OT solutions, such as the Windows operating system. However, companies may not be doing such a great job of making those systems and procedures as safe and secure as may be necessary under current global conditions.

The US Cybersecurity and Infrastructure Security Agency's (CISA) advisory notice about the Florida case noted that the plant was still running the Windows 7 operating system, support for which ended on January 4, 2020[12]. They recommend ensuring that an organization is running the latest, fully patched software. However, industry representatives point out that upgrading certain field devices can be difficult or even impossible, in which case they may need to be replaced

These are some of the key findings from the CISA's report on this incident. They are well worth heeding:

> The FBI, CISA, EPA, and MS-ISAC [all United States agencies – the Federal Bureau of Investigation, the Cybersecurity and Infrastructure Security Agency, the Environmental Protection Agency, and the Multi-State Information Sharing and Analysis Center] have observed corrupt insiders and outside cyber actors using desktop sharing software to victimize targets in a range of organizations, including those in the critical infrastructure sectors. In addition to adjusting system operations, cyber actors also use the following techniques:
>
> - Use access granted by desktop sharing software to perform fraudulent wire transfers.
> - Inject malicious code that allows the cyber actors to
>   - Hide desktop sharing software windows,
>   - Protect malicious files from being detected, and

    - Control desktop sharing software start-up parameters to obfuscate their activity.
- Move laterally across a network to increase the scope of activity.

So, What's an Organization to do?

For CISOs, one of the learnings from the Darktrace wisdom shared in these sessions is that vigilance and good cybersecurity practices are a crucial aspect of managing general business risk and an important investment in your organization's reputation and future. Other important points include paying attention to an early understanding of risk, deliberately identifying potential threats, having robust detection for possible exposure, and knowing, in advance and in detail, what your initial response plan is.

There were three main takeaways for the CISOs to take back to their organizations:

1. There is an emerging significance of third-party risk endemic in the software supply chain (Brad Smith's comments in that Microsoft interview illustrate this[20].) This is an enormously significant threat, and we may not be able to contain it once it is let loose. It's a real Pandora's Box because so many interrelationships are involved. It may even come back to bite the original attackers because they will undoubtedly be using some of the same supply chain elements that they originally infected. So much for the principle of six degrees of separation. Very scary.

2. The geopolitical implications/dynamics mentioned below that we are seeing emerge in unusual ways. (Both the FireEye and the Capitol attacks have already been highlighted.) How will your organization monitor these sorts of dynamics and factor the implications of geopolitical events and dynamics into your Business Risk Management planning? Your Board of Directors will be accountable. Are you acting reasonably?

3. Perhaps most importantly, geopolitical implications swing both ways. Companies also have responsibilities to think seriously about the potential implications their activities and products might have for geopolitical dynamics. One good example comes from Strava – a company that collects data from personal fitness tracker devices and provides personalized feedback that helps to visualize an individual's activity patterns[22.] These maps can be aggregated to provide group and population analyses. Tracking one's general fitness and activity patterns can be very beneficial at a personal level. However, when presented in meaningful group formats, the implications may be very different. The US Military is quite

concerned that these "heat maps" of US Military personnel's walking and fitness activities while on base, provide a detailed layout of the specific base[23]. These present a disclosure of base layout and security information that could have national security implications. A simple web search can disclose some good images available for US Military bases[24]. What might be the responsibilities of Strava if this sort of data, already available on the Internet (as shown above), exposes classified military base layouts?? A good perspective on this is provided by Jordan Keenan about 27 minutes into his presentation on The Age of Surveillance Capitalism for the PSICC Conference, February 2, 2021[25].

Perhaps the most important lesson that we can all learn is the need for constant cybersecurity vigilence. The "bad guys" are well-funded, well-organized, and have access to amazing tools, both the publicly available ones like Wireshark and Shodan, and the highly-specialized ones that are sold, traded, and offered "as a service" on the Dark Web. As has often been observed, they just need to find a single gap in cybersecurity, while system defenders need to plug every gap, or risk an embarrassing, costly or even lethal security breach.

Cybersecurity has attracted some of the best minds in the world, on both sides of the battle, and that's what makes it such a fascinating and ever-changing field.

REFERENCES:

[1] https://www.youtube.com/watch?v=tWd8DxLfDek

[2] https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html

[3] https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html

[4] https://www.wired.com/story/russian-hackers-attack-ukraine/

[5] https://www.wired.com/story/russian-hackers-attack-ukraine/

[6] https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html

[7] For details see https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html and https://abcnews.go.com/Business/wireStory/us-charges-chinese-military-hackers-equifax-breach-68884240.

[8] https://abcnews.go.com/Business/wireStory/us-charges-chinese-military-hackers-equifax-breach-68884240

[9] https://www.bbc.com/news/world-us-canada-44825345

[10] https://www.bbc.com/news/world-us-canada-44825345

[11] https://www.businessinsider.com/riley-june-williams-given-new-charges-accused-stealing-pelosi-laptop-2021-1

[12] https://us-cert.cisa.gov/ncas/alerts/aa21-042a

[13] https://hmgstrategy.com/network/people/steve-katz

[14] https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

[15] https://tinyurl.com/yy9slwoh

[16] https://arstechnica.com/information-technology/2019/05/stolen-nsa-hacking-tools-were-used-in-the-wild-14-months-before-shadow-brokers-leak/

[17] https://www.zdnet.com/article/private-firms-have-failed-to-protect-our-digital-lives-we-need-the-government/?ftag=TRE-03-10aaa6b&bhid=60749362&mid=13272081&cid=716686221

[18] https://thehackernews.com/2020/10/trickbot-computer-virus.html

[19] https://www.ciocan.ca/if-they-can-hack-the-pentagon/

[20] https://www.zdnet.com/article/microsoft-solarwinds-attack-took-more-than-1000-engineers-to-create/?ftag=TRE-03-10aaa6b&bhid=60749362&mid=13269687&cid=716686221 also https://www.cbsnews.com/news/solarwinds-hack-russia-cyberattack-60-minutes-2021-02-14/

[21] https://www.techrepublic.com/article/fbi-secret-service-investigating-cyberattack-on-florida-water-treatment-plant/?ftag=TREa988f1c&bhid=27422464833382622327483595162663&mid=13263873&cid=1510455862

[22] https://www.strava.com/about

[23] https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/

[24] https://duckduckgo.com/?q=strava+map+us+military&atb=v162-1&iax=images&ia=images

[25] https://psimcc.ca/data2021/DPW21replay