

2021

# CYBER TRENDS

---

What the Year Holds for  
Both Cyber Insurers and  
Risk Managers Alike

By Wesley Robinson  
Risk Advisor

# With seemingly few warning signs to inform companies how and when a big loss will happen or what malware will start wreaking havoc next, here are the top trends that cyber insurers and risk managers alike will have to confront in 2021 and beyond.

According to one cybersecurity research firm, the average annual cost of worldwide data breaches will surpass \$5 trillion dollars<sup>1</sup> by 2024, an increase from the current \$3 trillion dollars a year. In a world that is increasingly under attack by cybercriminals, one would think that this number would begin to plateau or decrease as industries gear up to defend themselves, especially for a risk that has been steadily growing since the advent of the internet over 30 years ago. However, as the claims data continues to evolve, it paints a stark picture of the landscape.

To accurately assess the level of claims activity, Lloyds of London, who is responsible for insuring approximately a quarter of global cyber risks, is now requiring all participating insurers to make it clear which policies are responding to cyber, hence eliminating any “silent cyber” claims that could potentially be skewing their data and making the risk more difficult for actuaries to properly price. Meanwhile, ratings agency AM Best has argued that the growth in cyber claims may be understated, pointing out that companies are, in some cases, not reporting claims as they are unaware that they have purchased the coverage or are utilizing captives or unlicensed insurers. In their estimation, claims have doubled since 2017 to a total number of 18,000<sup>2</sup> per year in the US insurance market. Similarly in Canada, over the first 6 months of 2020, insurers reported cyber loss ratios of 499%<sup>3</sup>. Insurers are not only suffering “death by a thousand cuts” as frequency of claims skyrockets but are also more vulnerable than ever to large losses that have the potential to wipe out the entirety of their cyber premium. One of the largest losses in Canada in 2020 was Desjardins, a breach of their systems costing the bank \$108 million<sup>4</sup> to date.

With seemingly few warning signs to inform companies how and when a big loss will happen or what malware will start wreaking havoc next, here are the top trends that cyber insurers and risk managers alike will have to confront in 2021 and beyond.


## 1. THE CONTINUED GROWTH OF MULTI-CLOUD COMPUTING

The cloud computing industry is projected to grow from a total industry size of US \$371 billion<sup>5</sup> in 2020 to

US \$832 billion by 2025. This equates to a compound annual growth rate of 17.5% per year over the next five years. Convenience for consumers has been the main selling point of the cloud computing industry. However, as we are now finding out, this convenience comes at the price of making our data more vulnerable to a single hacking attack than ever before. Sometime between the months of March and June 2020, Software as a Service (SaaS) provider SolarWinds Corp. was breached by Russian hackers. Although this attack appeared to be a very deliberate attempt to gather valuable information on the five branches of the US military - all of whom used SolarWinds - it caught over 18,000 companies in the crossfire. According to Insurance Business Canada, initial estimates put the total insurable costs of this breach as high as \$115 million<sup>6</sup>, with other sources putting the breach costs in the billions given the fact that most companies were completely unaware of the vulnerabilities before January 2021.

## 2. CRYPTO-JACKING

With all the recent chatter around cryptocurrency and the historic high valuation of the world’s most well-known and popular cryptocurrency Bitcoin<sup>7</sup>, crypto-jacking has steadily grown into an industry of its own. Crypto jacking is the illicit use of someone else’s computer to mine cryptocurrency and is often implemented by having a victim click on a malicious link to unwittingly download crypto mining code, or by infecting a website with code that automatically mines cryptocurrency when opened on a victim’s browser. Many of these viruses will automatically spread to other computers via worming software and may also have scripts that check to see if the device is already infected with a form of crypto mining software, at which point said script will disable that software and begin mining for itself. While these codes do not do any outright damage to a victim’s computer and do not usually exfiltrate any valuable data, companies do incur costs with slowed productivity as the computers their employees work on slow down. The resources of IT professionals are then overwhelmed with the task of diagnosing and rooting out the source of lagging networks. With cryptocurrency gaining popularity,



and the cost of crypto-jacking software as low as \$30<sup>8</sup> to get started, this is an attack vector that isn't going anywhere as criminals weigh the benefits of a money-making method that is much lower risk than deploying ransomware.

### 3. ATTACKS ON ESSENTIAL INFRASTRUCTURE

In addition to being the year of COVID-19, 2020 will also be known as the year when cyber-criminals proved to have no shame in their choice of targets. 2020 saw the world's first indirect human death resulting from a ransomware attack on the Duesseldorf University Hospital<sup>9</sup> in Germany, when a patient requiring urgent medical care had to be re-routed to a hospital more than 30 km away from her original destination due to hospital authorities having their hands full with ransomware. Not long after this attack, another hacker was thwarted in their attempts to poison the drinking water of Oldsmar<sup>10</sup>, Florida by drastically increasing the amount of sodium hydroxide in the water, a chemical most often used to control water acidity but that can be dangerous to humans when consumed in high enough concentrations. Cyber security groups and government agencies have been warning for years that State sponsored hacking armies<sup>11</sup> or rogue cybercriminals are aware of the vulnerabilities and the opportunities presented to them by industrial control systems and are going to continue to test the waters of hacking essential infrastructure. According to a 2020 report<sup>12</sup> on the cyberthreat to the global energy system, cybersecurity research firm Dragos listed eleven hacking groups that specifically target and research vulnerabilities in electrical utilities and other energy infrastructure. The intent of these groups is to cause supply chain disruptions, prolonged outages, as well as damage to equipment or human beings. With political tensions in areas such as the Middle East remaining high in 2021, expect these attacks to continue and expect insurers to take a close look at the war and cyber terrorism coverage offered to their clients.

### 4. RANSOMWARE AS A SERVICE

In a world where Ransomware is one of the most common ways for cybercriminals to monetize a breach, Ransomware-as-a-Service can only be described as a pandemic within a pandemic. There are over 25<sup>13</sup> distinct hacking groups who have been involved in the selling of ransomware code for other cybercriminals to use. These groups create ransomware packages for sale to other criminals on the dark web, and by doing so, transfer the risk of being caught to other cybercriminals who see ransomware as one of the easiest attack vectors. The adoption of this business model is helping to fuel the rise of ransomware, turning 2020 into a year where there was a 40%<sup>14</sup> surge in global ransomware attacks, and the sale of ransomware shows no signs of slowing down 2021.

### 5. THE IMPACT OF COVID-19

With the onset of the COVID-19 pandemic, many companies were forced to switch very rapidly to a work-from-home environment. According to a 2020 report on the worldwide state of the cybersecurity job market, 30%<sup>15</sup> of respondents noted that their organizations made the move to a remote workforce in just a single day, with only 16% of respondents saying they had more than a week to make this shift. The pandemic compressed the timeline to secure a remote work environment from months to a matter of days, and cybercriminals took note. While the cybersecurity workforce struggled against these tight timelines, COVID-19 also put pressure on companies who struggled to make ends meet in a locked down economy, meaning that many cybersecurity professionals working in these organizations were impacted by budgetary constraints. Compound this with the fact that cybersecurity spending is often deemed a non-essential expense for companies in the best of times, and it is easy to see how 2020 created a perfect climate for cybercrime to flourish. Cybercrime cost the world more than \$1 trillion dollars in 2020<sup>16</sup>, up 50% since 2018 and equating to 1% of global gross domestic product.



## 6. THE CONTINUED SHORTAGE OF CYBERSECURITY PROFESSIONALS

According to a 2020 report by ISC2, a leading industry group in the field of cybersecurity, there is an estimated workforce gap in cybersecurity professionals of over 3.1MM<sup>15</sup>. In North America alone, this gap was approximately 370,000 professionals. Although globally the gap did shrink in 2020, this was largely driven by the reduced average demand across most industry segments, a demand directly attributable to a global economy that shrank somewhere between 4% to 5% in 2020<sup>17</sup>. Compare this somewhat bleak landscape to the lucrative environment that cybercriminals find themselves in, and the problem becomes one where high-quality talent is attracted to the other side of the ethical boundary. Cyber criminals are earning up to \$2MM<sup>18</sup> a year and Cybercrime is nearly invisible to law enforcement, with under 5% ever being apprehended for their crimes. The cybersecurity industry will have to grapple with the incentives that are currently in place for talented professionals who can choose to work for a corporation, or potentially earn more money working for themselves on the wrong side of the law.

## 7. INTERNET OF THINGS (IOT)

The current world population hovers around 7.8 billion people<sup>19</sup>, with the United Nations predicting an eventual population plateau at around 11 billion people<sup>20</sup>. Compare this to the now 20.6 billion internet connected devices in the world, and we can see that the number of devices, wearable technology, smart homes, and the like outnumber people on this planet 2.6 to 1. These numbers do not consider that there is still an area of the world that is not internet connected, and therefore this number is going to continue to grow exponentially as developing countries catch up to the Western world. What does this mean for the world of cybersecurity? It means that the landscape for attacks and number of targets is larger and more widespread than ever before. We are not just talking about technology that people would immediately consider as dangerous if hacked, such as a self-driving car. Companies who manufacture these cars are incredibly cognizant of hackability and

have built lifetime software updates into their support system. So, although a self-driving car is hackable, the companies responsible for protecting you while in your car are aware of the risk and are doing everything they can to stay ahead of the criminals. On the other hand, companies that traditionally manufactured hardware such as Samsung and LG are now dipping their toes into the IoT industry and have not made it clear how they intend to protect your network from hacking attempts. This includes whether these companies plan to patch in necessary software updates<sup>21</sup> for the life of your devices to protect you and your information. Criminals will always pick the easiest route into your network, whether that is to exploit your information or spread denial of service attacks to a broader audience. The new lowest common denominator might be your smart fridge in 2021!

## 8. INCIDENT RESPONSE IS KEY

According to IBM's 2020 Cost of a Data Breach Report<sup>22</sup>, companies who had previously tested their incident response could save \$2 million on average in the event of a cyber breach, compared to their peers who had no incident response strategy or hadn't tested their plan prior to a breach occurring. The average time to identify and contain a breach was 280 days and almost 40% of costs incurred were more than a year after an attack happened. For risk managers, insurers, and cybersecurity experts alike, these statistics point to the fact that saving time when responding to a cyber incident should be a top priority. When a company responds quickly and contains a breach in less than 200 days, they can expect an additional \$1 million dollars in savings compared to companies who are still handling a breach 200 days and onward. When you consider that the global average total cost of a data breach was \$3.86 million dollars in 2020 (\$8.64 million for US Companies), any amount of savings that a company can achieve in the event of a breach should be seriously considered. Partnering with the right risk managers, cyber brokers, and insurers will ensure an organization's incident response costs are minimized in a worst-case scenario.



---

**LOCAL TOUCH. NATIONAL STRENGTH.™**

*Contact a member of your Iridium Team with any questions you have regarding cyber coverage.*

**[irsnvacord.com](http://irsnvacord.com) | 855.585.9654**

## REFERENCES

1. Cybersecurity breaches to increase nearly 70% over the next 5 years. (2019, October 01). Retrieved April 26, 2021, from <https://www.securitymagazine.com/articles/91019-cybersecurity-breaches-to-increase-nearly-70-over-the-next-5-years>
2. Best's market segment report: Profitability less certain in u.s. cyber insurance market as new risks emerge. (2020, July 21). Retrieved April 26, 2021, from <http://news.ambest.com/presscontent.aspx?refnum=29635&altsrc=9>
3. Malik, A. (2020, November 27). Two options for Cyber INSURERS dealing with huge loss ratios. Retrieved April 26, 2021, from <https://www.canadianunderwriter.ca/insurance/two-options-for-cyber-insurers-dealing-with-huge-loss-ratios-1004200249/>
4. Desjardins data breach cost \$108 million, BANKING Co-op says | CBC News. (2020, February 26). Retrieved April 26, 2021, from <https://www.cbc.ca/news/business/desjardins-breach-cost-1.5476855#:~:text=The%20Desjardins%20Group%20says%20last,the%20co%2Doperative%20%24108%20million.>
5. Cloud computing industry to grow from \$371.4 billion in 2020 to \$832.1 billion by 2025, at a CAGR of 17.5%. (2020, August 21). Retrieved April 26, 2021, from <https://www.globenewswire.com/news-release/2020/08/21/2081841/0/en/Cloud-Computing-Industry-to-Grow-from-371-4-Billion-in-2020-to-832-1-Billion-by-2025-at-a-CAGR-of-17-5.html>
6. Adriano, L. (2021, January 15). SolarWinds trojan hack could cost Cyber insurers CA\$115 MILLION. Retrieved April 26, 2021, from <https://www.insurancebusinessmag.com/ca/news/cyber/solarwinds-trojan-hack-could-cost-cyber-insurers-ca115-million-243640.aspx#:~:text=15%20Jan%202021-,SolarWinds%20trojan%20hack%20could%20cost%20cyber%20insurers%20CA%24115%20million,and%20forensic%20services%2C%20experts%20project.>
7. Browne, R. (2021, February 16). Bitcoin surges to new record as major firms flock to crypto. Retrieved April 26, 2021, from <https://www.cnn.com/2021/02/15/bitcoin-btc-price-hits-a-record-high-of-nearly-50000.html#:~:text=The%20world's%20largest%20cryptocurrency%20by,a%20price%20of%20around%20%2449%2C167.>
8. Nadeau, M. (2021, March 11). What is cryptojacking? How to prevent, detect, and recover from it. Retrieved April 26, 2021, from <https://www.csoonline.com/article/3253572/what-is-cryptojacking-how-to-prevent-detect-and-recover-from-it.html>
9. Cimpanu, C. (2020, September 17). First death reported following a ransomware attack on a German hospital. Retrieved April 26, 2021, from <https://www.zdnet.com/article/first-death-reported-following-a-ransomware-attack-on-a-german-hospital/#:~:text=The%20Duesseldorf%20hospital%20was%20unable,caused%20by%20a%20ransomware%20attack.>
10. Hacker tries to poison water supply of Florida city. (2021, February 08). Retrieved April 26, 2021, from <https://www.bbc.com/news/world-us-canada-55989843>
11. Sullivan, B. (2016, September 22). What is PLA Unit 61398 and who are the five Chinese hackers? Retrieved April 26, 2021, from <https://techmonitor.ai/what-is/what-is-pla-unit-61398-and-who-are-the-five-chinese-hackers-4271980>
12. North American Electric Cyber Threat Perspective (Publication). (n.d.). Dragos. Retrieved April 26, 2021, from <https://www.dragos.com/wp-content/uploads/NA-EL-Threat-Perspective-2019.pdf>.
13. Ransomware-as-a-service: The pandemic within a pandemic. (n.d.). Retrieved April 26, 2021, from <https://www.intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/>
14. Ryuk ransomware behind one third of ALL ransomware attacks in 2020. (2020, November 03). Retrieved April 26, 2021, from <https://www.helpnetsecurity.com/2020/11/03/ryuk-ransomware-2020/>
15. Cybersecurity Professionals Stand Up to a Pandemic (Publication). (n.d.). International Information System Security Certification Consortium. doi:<https://www.isc2.org/-/media/ISC2/Research/2020/Workforce-Study/ISC2ResearchDrivenWhitepaperFINAL.ashx?la=en&hash=2879EE167ACBA7100C330429C7EBC623BAF4E07B>
16. Cybercrime costs the world more than \$1 trillion, a 50% increase from 2018. (2020, December 07). Retrieved April 26, 2021, from <https://www.helpnetsecurity.com/2020/12/07/cybercrime-costs-world/>

## REFERENCES (CONTINUED)

17. World economic Outlook UPDATE, June 2020: A crisis like no other, an Uncertain Recovery. (2020, June 01). Retrieved April 26, 2021, from [https://www.imf.org/en/Publications/WEO/Issues/2020/06/24/WEOUpdateJune2020#:~:text=A%20Crisis%20Like%20No%20Other%2C%20An%20Uncertain%20Recovery,-Read%20full%20report&text=Global%20growth%20is%20projected%20at,Economic%20Outlook%20\(WEO\)%20forecast.](https://www.imf.org/en/Publications/WEO/Issues/2020/06/24/WEOUpdateJune2020#:~:text=A%20Crisis%20Like%20No%20Other%2C%20An%20Uncertain%20Recovery,-Read%20full%20report&text=Global%20growth%20is%20projected%20at,Economic%20Outlook%20(WEO)%20forecast.)
18. Greig, J. (2020, March 12). Cybercriminals raking in \$1.5 trillion every year. Retrieved April 26, 2021, from <https://www.techrepublic.com/article/cybercriminals-raking-in-1-5-trillion-everyyear/#:~:text=Some%20cybercriminals%20can%20bring%20in,in%20more%20than%20%242%20million.>
19. Current world population. (n.d.). Retrieved April 26, 2021, from <https://www.worldometers.info/world-population/>
20. Growing at a slower PACE, world population is expected to reach 9.7 billion in 2050 and could peak at nearly 11 billion around 2100 | UN DESA Department of economic and social affairs. (n.d.). Retrieved April 26, 2021, from <https://www.un.org/development/desa/en/news/population/world-population-prospects-2019.html>
21. Bhartiya, S. (2017, March 03). Your smart fridge may kill you: The dark side of IoT. Retrieved April 26, 2021, from <https://www.infoworld.com/article/3176673/your-smart-fridge-may-kill-you-the-dark-side-of-iot.html>
22. 2020 Cost of a Data Breach (Publication). (n.d.). IBM. doi:<https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/>