





April 26, 2022

Challenge yourself with our [Spring Cleaning](#) quiz!

[This past week's stories:](#)

-  [Why healthcare data is the latest cyber battlefield](#)
-  [Sunwing deals with delays for third day, blames cyber breach](#)
-  [Local municipality still struggling to recover from 'cyber security incident'](#)
-  [Hackers sneak 'more eggs' malware into resumes sent to corporate hiring managers](#)

 [Ransomware attacks target more than 4 in 5 Canadian businesses](#)

[FBI Warns of BlackCat Ransomware That Breached Over 60 Organisations Worldwide](#)

[Cybersecurity threats and trends 2022](#)

[Top data breaches and cyber attacks of 2022](#)

[FBI warns ransomware attacks on agriculture co-ops could upend food supply chain](#)

[Hackers claim to target Russian institutions in barrage of cyberattacks and leaks](#)

[Microsoft's \\$15 billion cybersecurity business is giving investors new reason for optimism](#)

[Organizations face cybersecurity debt for not prioritizing cybersecurity](#)

Why healthcare data is the latest cyber battlefield

Every industry and all organizations are vulnerable to breaches and hacks.

Healthcare companies, however, are four times more likely to be targeted than any other industry. Patient data, rich with personal health and financial information, is highly lucrative to a hacker. According to Becker's Hospital Review, the patient's medical information can be worth between 10 and 40 times more than a credit card number on the black market.

There is no immunity or vaccine to prevent a breach, hack or ransomware attack; you must think of a cyber break-in in terms of when it might happen versus if it happens.

<https://www.cpacanada.ca/en/news/pivot-magazine/2022-04-25-cybersecurity-risks>

Click above link to read more.

[Back to top](#)

Sunwing deals with delays for third day, blames cyber breach

A technical problem at Sunwing Airlines that continues to ground flights is being blamed on a data security breach at the company's third-party provider.

"A system that is up and running all the time, which never fails, was hacked," said Sunwing President Mark Williams. "They had a cyber-breach and they've been unable to get the system up."

<https://www.ctvnews.ca/canada/sunwing-deals-with-delays-for-third-day-blames-cyber-breach-1.5868952>

Click above link to read more.

[Back to top](#)

Local municipality still struggling to recover from 'cyber security incident'

Elgin County officials and politicians remain tight-lipped about the cyber disruption that's rendered its government website and email system inactive for weeks, but say they're optimistic it will be back online soon.

"It's been difficult," said Sally Martyn, Central Elgin mayor and member of Elgin County council.

"We haven't had any email or anything for quite a while now. But I know they've been working around the clock to get everything fixed."

<https://www.thestar.com/news/canada/2022/04/20/local-municipality-still-struggling-to-recover-from-cyber-security-incident.html>

Click above link to read more.

[Back to top](#)

Ransomware attacks target more than 4 in 5 Canadian businesses

In March 2021, tech firm Acer was faced with paying one of the largest ransomware demands known to date: a price tag of US\$50 million for the return of the global computer manufacturer's stolen data.

The dramatic extortion by cybercriminals captured headlines. But ransomware attacks happen every day to every size of company.

<https://www.theglobeandmail.com/business/adv/article-ransomware-attacks-target-more-than-4-in-5-canadian-businesses/>

Click above link to read more.

[Back to top](#)

Hackers sneak 'more_eggs' malware into resumes sent to corporate hiring managers

A new set of phishing attacks delivering the more_eggs malware has been observed striking corporate hiring managers with bogus resumes as an infection vector, a year after potential candidates looking for work on LinkedIn were lured with weaponized job offers.

"This year the more_eggs operation has flipped the social engineering script, targeting hiring managers with fake resumes instead of targeting jobseekers with fake job offers," eSentire's research and reporting lead, Keegan Keplinger, said in a statement.
Link

<https://thehackernews.com/2022/04/hackers-sneak-moreeggs-malware-into.html>

Click above link to read more.

[Back to top](#)

FBI warns of BlackCat ransomware that breached over 60 organisations worldwide

The U.S. Federal Bureau of Investigation (FBI) is sounding the alarm on the BlackCat ransomware-as-a-service (RaaS), which it said victimized at least 60 entities worldwide between as of March 2022 since its emergence last November.

Also called ALPHV and Noberus, the ransomware is notable for being the first-ever malware written in the Rust programming language that's known to be memory safe and offer improved performance.

<https://thehackernews.com/2022/04/fbi-warns-of-blackcat-ransomware-that.html>

Click above link to read more.

[Back to top](#)

Cybersecurity threats and trends 2022

Over the past few years, cybersecurity has become a widespread priority. The emerging security threats for individuals, companies, and even the government, have placed the information security sector on high alert. Unfortunately, the technology we have right now has become both an advantage and disadvantage for cybercriminals. As people continue to strengthen their security, they are also improving their sophisticated methods for their cyberattacks. Now that most sectors have shifted to remote due to the COVID-19 pandemic, cybercriminals were given more opportunities for large-scale cyberattacks. Unfortunately, in 2020 and 2021, cyber threats were at their peak with the new techniques and tactics proven effective by these cybercriminals.

Now that most sectors have shifted to remote due to the COVID-19 pandemic, cybercriminals were given more opportunities for large-scale cyberattacks. Unfortunately, in 2020 and 2021, cyber threats were at their peak with the new techniques and tactics proven effective by these cybercriminals.

<https://latesthackingnews.com/2022/04/25/cybersecurity-threats-and-trends-2022/>

Click above link to read more.

[Back to top](#)

Top data breaches and cyber attacks of 2022

Regrettably, cyberattacks and breaches are big business – bad actors with an endless stream of nefarious motives populate the internet, ready to pounce on insecure data and immature security practices.

There's no shortage of attacks and breaches, and that can make it hard to manage if you like to keep up with the latest security news.

<https://www.techradar.com/features/top-data-breaches-and-cyber-attacks-of-2022>

Click above link to read more.

[Back to top](#)

FBI warns ransomware attacks on agriculture co-ops could upend food supply chain

Ransomware operators are eyeing attacks on large networks of farmers, called agriculture cooperatives, during make-or-break planting and harvest seasons, when they are likely most desperate to pay, according to the Federal Bureau of Investigation.

A new advisory details previous attempts by threat actors since 2021 to disrupt agricultural co-op operations, including a Lockbit 2.0 attack on a critical farming supplier, and a July 2021 breach of a business management software company serving several agricultural cooperatives. Some of the attacks were successful and resulted in a production slowdown, the FBI says.

<https://www.darkreading.com/attacks-breaches/fbi-warns-agriculture-about-ransomware-attacks-timed-to-planting-harvest-seasons>

Click above link to read more.

[Back to top](#)

Hackers claim to target Russian institutions in barrage of cyberattacks and leaks

Hackers claim to have broken into dozens of Russian institutions over the past two months, including the Kremlin's internet censor and one of its primary intelligence services, leaking emails and internal documents to the public in an apparent hack-and-leak campaign that is remarkable in its scope.

The hacking operation comes as the Ukrainian government appears to have begun a parallel effort to punish Russia by publishing the names of supposed Russian soldiers who operated in Bucha, the site of a massacre of civilians, and agents of the F.S.B., a major Russian intelligence agency, along with identifying information like dates of birth and passport numbers. It is unclear how the Ukrainian government obtained those names or whether they were part of the hacks.

<https://www.nytimes.com/2022/04/22/us/politics/hackers-russia-cyberattacks.html>

Click above link to read more.

[Back to top](#)

Microsoft's \$15 billion cybersecurity business is giving investors new reason for optimism

In January 2021, Microsoft CEO Satya Nadella revealed the size of the software company's security business for the first time. The number was big.

Nadella told analysts on an earnings call that the operation had reached \$10 billion in annual revenue and was "up more than 40%" year over year. In other words, it was outpacing every other major Microsoft product.

<https://www.cnn.com/2022/04/26/microsoft-15-billion-security-unit-gives-investors-reason-for-hope.html>

Click above link to read more.

[Back to top](#)

Organizations face cybersecurity debt for not prioritizing cybersecurity

When organizations accelerate their digital transformation due to the pandemic two years ago, many did not prioritize cybersecurity. In fact, organizations were focused mostly on ensuring business continuity and avoiding any disruptions to productivity.

As the pandemic continued, investments in tech became long-term, with the focus on providing seamless and agile working operations. Companies adopted newer technologies to remain relevant. However, there was one problem, cybersecurity remained an afterthought.

<https://techwireasia.com/2022/04/organizations-face-cybersecurity-debt-for-not-prioritizing-cybersecurity/>

Click above link to read more.

[Back to top](#)

Click [unsubscribe](#) to stop receiving the Digest.

The Security News Digest (SND) is a collection of articles published by others that have been compiled by the Information Security Branch (ISB) from various sources. The intention of the SND is simply to make its recipients aware of recent articles pertaining to information security in order to increase their knowledge of information security issues. The views and opinions displayed in these articles are strictly those of the articles' writers and editors and are not intended to reflect the views or opinions of the ISB. Readers are expected to conduct their own assessment on the validity and objectivity of each article and to apply their own judgment when using or referring to this information. The ISB is not responsible for the manner in which the information presented is used or interpreted by its recipients.

For previous issues of Security News Digest, visit the current month archive page at:

<http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/security-news-digest>

To learn more about information security issues and best practices, visit us at:

<https://www.gov.bc.ca/informationsecurity>

OCIOSecurity@gov.bc.ca

The information presented or referred to in SND is owned by third parties and protected by copyright law, as well as any terms of use associated with the sites on which the information is provided. The recipient is responsible for making itself aware of and abiding by all applicable laws, policies and agreements associated with this information.

We attempt to provide accurate Internet links to the information sources referenced. We are not responsible for broken or inaccurate Internet links to sites owned or operated by third parties, nor for the content, accuracy, performance or availability of any such third-party sites or any information contained on them.

