May 31, 2022

Challenge yourself with our Cyber Security Superhero quiz!

This past week's stories:

- **Calgary charity hit by data breach says it responded appropriately despite client concerns**
- **Cyber attack downs Regina Public Schools' computer systems**
- **Canadian healthcare provider issues data breach warning after server hack**
- **State of Cybersecurity Report 2022 names ransomware and nation-state attacks as biggest threats**
- **Cyberattacks likely to rise in wake of Ukraine War. This is what Estonia learnt from Web War One**
- **Three-quarters of security pros believe current cybersecurity strategies will shortly be obsolete**
- **Human error is a main cause for cyber security breaches, Verizon report finds**
- **The human toll: examining the impact of breaches on the public**
- **China offering ten nations help to run their cyber-defenses and networks**
- **JBS Foods cyber attack highlights industry vulnerabilities to Russian hackers**
- **How failing to prioritize cyber security can hurt your company**
- **New 'GoodWill' ransomware forces victims to donate money and clothes to the poor**
- **Evolving cybersecurity at the speed of threats**

Calgary charity hit by data breach says it responded appropriately despite client concerns

A Calgary charity has confirmed to Global News it was the victim of an email data breach last fall.

Now, one of its former clients wants to know why it took so long to be alerted.

The Calgary Urban Project Society (CUPS) sent an email to Michael Friesen on Wednesday to inform him that a staff member's email account had been hacked and some of his personal information may have been put at risk. That information included his driver's license, bank statements and rent report.

https://globalnews.ca/news/8872996/calgary-charity-data-breach/

Click above link to read more.

Back to top

Cyber attack downs Regina Public Schools' computer systems

Regina Public Schools has confirmed that what it described as a "network-wide incident" earlier this week is in fact a cyber security attack.

There's no word on the nature of the attack but the school district confirmed it has affected a large number of its computer systems.

On Tuesday, Regina Public Schools said the incident meant all internet-based systems such as email and other education tools were offline.

https://www.cbc.ca/news/canada/saskatchewan/regina-public-schools-cyber-attack-1.6467451

Click above link to read more.

Back to top

Canadian healthcare provider issues data breach warning after server hack

Canadian healthcare service provider Scarborough Health Network (SHN) has warned that a data breach may have exposed patient healthcare records.

In a breach notice, SHN explained that its IT staff noticed unusual activity on its systems on January 25.

After containing the problem and calling in help from external IT forensics experts, a subsequent investigation discovered that a "subset of data" on a number of SHN's servers had been accessed by unauthorized parties.

https://portswigger.net/daily-swig/canadian-healthcare-provider-issues-data-breach-warning-after-server-hack

Click above link to read more.

Back to top

State of Cybersecurity Report 2022 names ransomware and nation-state attacks as biggest threats

Ransomware is the biggest concern for cybersecurity professionals, according to results of the Infosecurity Group's 2022 State of Cybersecurity Report, produced by Infosecurity Europe and *Infosecurity* Magazine.

This attack vector was voted as the biggest cybersecurity trend (28%) by the survey respondents (including CISOs, CTOs, CIOs and academics), marking a significant change from the previous report in 2020, where ransomware did not break the top three. This follows surging ransomware incidents in 2021, with ransom demands and payments growing significantly last year. A number of these attacks have also impacted critical industries, for example, taking down the US' largest fuel pipeline.

https://www.infosecurity-magazine.com/news/2022-state-industry-report/

Click above link to read more.

Back to top

Cyberattacks likely to rise in wake of Ukraine War. This is what Estonia learnt from Web War One

Russia's war on Ukraine is not just being fought with bombs but bytes too, causing nations to now ramp up their cyber defence capabilities.

One country they can learn a lot from is Estonia. The nation, which shares a border with Russia, was one of the first to come under attack from this modern form of hybrid warfare 15 years ago.

https://www.euronews.com/next/2022/05/26/cyberattacks-likely-to-rise-in-wake-of-ukraine-war-this-is-what-estonia-learnt-from-web-wa

Click above link to read more.

Back to top

Three-quarters of security pros believe current cybersecurity strategies will shortly be obsolete

On Tuesday, Crossword Cybersecurity Plc, a cybersecurity solutions company, released a new report demonstrating that UK companies are increasingly worried about cyber-attacks. In the survey of more than 200 CISOs and senior cybersecurity professionals, 40% of respondents said that their current cybersecurity strategy will likely be outdated in just two years. A further 37% said this would happen in three years.

The ever-increasing number of cyber-attacks coupled with constant tech innovation means companies must continuously update their cybersecurity strategies. More than three-fifths (61.4%) of participants marked themselves as "fairly confident" in their ability to thwart cyber-attacks.

https://www.infosecurity-magazine.com/news/security-pros-cybersecurity/

Click above link to read more.

Back to top

Human error is a main cause for cyber security breaches, Verizon report finds

The 2022 Verizon Data Breach Investigations Report has been released and the study provides an analysis of security breaches and attack vectors from the last year.

The data breach report analysed more than 5212 breaches and 23,896 security incidents. The main findings from the annual report were that cyber attackers have four key paths to enterprise estates including credentials, phishing, exploiting vulnerabilities and malicious botnets.

https://www.businessleader.co.uk/human-error-is-a-main-cause-for-cyber-security-breaches-verizon-data-breach-report-finds/

Click above link to read more.

Back to top

The human toll: examining the impact of breaches on the public

The world is in need of a reminder that the detrimental impacts of cyberattacks are not felt solely by faceless corporate behemoths. Cyberattacks affect real people every day. Yet, the impact on these individuals is rarely our focus. Society — and major media outlets — remain fixated on the consequences for business (e.g., dips in stock price, loss of brand deals or partnerships and leadership changes). But the impact on human lives is often found below the fold, if at all, and rarely brought to light.

https://www.forbes.com/sites/forbestechcouncil/2022/05/27/the-human-toll-examining-the-impact-of-breaches-on-the-public/?sh=1f46cc8d49a1

Click above link to read more.

Back to top

China offering ten nations help to run their cyber-defenses and networks

China has begun talking to ten nations in the South Pacific with an offer to help them improve their network infrastructure, cyber security, digital forensics and other capabilities – all with the help of Chinese tech vendors.

Newswire *Reuters* broke the news of China's ambitions after seeing a draft agreement that China's foreign minister Wang Yi is reportedly tabling on a tour of Pacific nations this week and next.

https://www.theregister.com/2022/05/27/china_south_pacific_tech_assistance/

Click above link to read more.

Back to top

JBS Foods cyber attack highlights industry vulnerabilities to Russian hackers

Australia's food supply is uniquely vulnerable to cyber attacks, the director of a national cybersecurity firm warns, as he calls for the industry to raise its standards on the anniversary of the JBS ransomware hack.

JBS Foods, the world's biggest meat processor, was held ransom by Russian-based hackers for $US11 million last year.

https://www.abc.net.au/news/2022-05-30/food-industry-cyber-attack-russia-hacking-risk/101110386

Click above link to read more.

Back to top

How failing to prioritize cyber security can hurt your company

Businesses around the world depend on technology to function and thrive. However, along with this growth, the risk of being hacked is increasing. To avoid the potentially crippling consequences

of these cyber attacks, CISOs (Chief Information Security Officers) need to be aware of cyber attacks, which could come in the form of breaches of data, malware attacks, cyber espionage, and online phishing, or other threats. In addition, CISOs should prioritize their cyber risks so that the organization can take steps to mitigate those risks and mitigate potential harm as effectively as possible. This article explores several strategies for identifying and prioritizing cyber risks affecting your organization.

https://www.analyticsinsight.net/how-failing-to-prioritize-cyber-security-can-hurt-your-company/

Click above link to read more.

Back to top

New 'GoodWill' ransomware forces victims to donate money and clothes to the poor

Cybersecurity researchers have disclosed a new ransomware strain called GoodWill that compels victims into donating for social causes and provide financial assistance to people in need.

"The ransomware group propagates very unusual demands in exchange for the decryption key," researchers from CloudSEK said in a report published last week. "The Robin Hood-like group claims to be interested in helping the less fortunate, rather than extorting victims for financial motivations."

https://thehackernews.com/2022/05/new-goodwill-ransomware-forces-victims.html

Click above link to read more.

Back to top

Evolving cybersecurity at the speed of threats

Organizations all over the world have accelerated their digital transformation agenda multifold since the advent of the COVID-19 pandemic. Today, businesses are leveraging new-age technologies like cloud computing, AI & ML, and big data to achieve scalability of operations. However, in this era of digitization and virtualization of business operations, the ever expanding and constantly changing threat landscape is a major challenge.

https://cio.economictimes.indiatimes.com/news/digital-security/evolving-cybersecurity-at-the-speed-of-threats/91913418

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