




May 3, 2022

Challenge yourself with our [Cyber Security Superhero](#) quiz!

[REGISTER](#) for Security Day – May 10, 2022!

This past week's stories:

-  [Cybersecurity authorities list top 15 flaws exploited in 2021](#)
 -  [Purported Elgin County data posted online by ransomware group: cyber threat expert](#)
 -  [Canadian businesses scrambling to defend against cyberattacks uptick](#)
 - [What cyber insurance companies want from clients](#)
 - [Israel wants cyber 'Iron Dome' system to fight off attacks, minister says](#)
 - [India to require cybersecurity incident reporting within six hours](#)
 - [German wind farm operator confirms cybersecurity incident](#)
 - [In an interconnected world, everyone is responsible for cybersecurity](#)
 - [How cyber security history repeats itself](#)
 - [Trinidad: Ministry of National Security warns of increased malicious cyber-activity](#)
 - [Europe is bracing itself for cyber warfare, but is it ready?](#)
 - [Fortinet: 80% of breaches attributed to cybersecurity skills gap](#)
-

Cybersecurity authorities list top 15 flaws exploited in 2021

The cybersecurity authorities of the U.S., Australia, Canada, New Zealand and the U.K. have published a list of the 15 biggest vulnerabilities exploited in 2021.

The list includes Log4Shell (CVE-2021-44228), REST API authentication bypass (CVE-2021-40539), ProxyShell (CVE-2021-34523), ProxyShell (CVE-2021-34473), ProxyShell (CVE-2021-31207), ProxyLogon (CVE-2021-27065), ProxyLogon (CVE-2021-26858), ProxyLogon (CVE-2021-26857), ProxyLogon (CVE-2021-26855).

<https://www.itworldcanada.com/post/cybersecurity-authorities-list-top-15-flaws-exploited-in-2021>

Click above link to read more.

[Back to top](#)

Purported Elgin County data posted online by ransomware group: cyber threat expert

The cybersecurity incident that has left Elgin County's website and email system down since the start of the month may have been the result of a ransomware attack involving a notorious Russia-based ransomware syndicate, Global News has learned.

A cyber threat expert says data purporting to belong to the county was posted to the website of the ransomware group Conti on Monday, possibly shedding new light on the "technical disruption" that has been plaguing the county for the last several weeks.

<https://globalnews.ca/news/8788980/elgin-county-data-ransomware-crime/>

Click above link to read more.

[Back to top](#)

Canadian businesses scrambling to defend against cyberattacks uptick

Canada's governor-general and foreign ministry, hospitals, and an airline: a litany of latest cyberattacks has uncovered poor defenses against hackers, notwithstanding warnings to be greater vigilant because of Russia's invasion of Ukraine.

Last week, Canada and 4 other Western international locations, which includes America, warned that Russia become making ready to launch large cyberattacks against Ukraine's allies in in retaliation for assist for Kyiv and sanctions imposed on Moscow.

<https://www.bolnews.com/latest/2022/04/canadian-businesses-scrambling-to-defend-against-cyberattacks-uptick/>

Click above link to read more.

[Back to top](#)

What cyber insurance companies want from clients

Cyberattacks are a fact of life. Every organization — in fact, anyone with an internet account — has been targeted in some manner, from a phishing email to DDoS website attacks to malicious account takeovers.

Just as a company purchases insurance to protect from physical theft and other potential loss and damages, organizations need to add protection against the financial aftermath of a cyberattack.

<https://www.cybersecuritydive.com/news/what-cyber-insurance-companies-want-from-clients/621359/>

Click above link to read more.

[Back to top](#)

Israel wants cyber 'Iron Dome' system to fight off attacks, minister says

Israel's government on Monday ordered communications firms to step up their cyber security efforts in the wake of a rise in attempted hacking attacks.

New regulations are currently being implemented in which mandatory and unified standards will have to be met, the Communications Ministry and Israel's National Cyber Directorate said.

<https://globalnews.ca/news/8802906/israel-cybersecurity-iron-dome-system/>

Click above link to read more.

[Back to top](#)

India to require cybersecurity incident reporting within six hours

The Indian government has issued new directives requiring organizations to report cybersecurity incidents to CERT-IN within six hours, even if those incidents are port or vulnerability scans of computer systems.

This requirement was promoted by India's Computer Emergency Response Team (CERT-In), who states it has identified specific gaps causing difficulties in security incident analysis and response, and to address them, it needs to impose more aggressive measures.

<https://www.bleepingcomputer.com/news/security/india-to-require-cybersecurity-incident-reporting-within-six-hours/>

Click above link to read more.

[Back to top](#)

German wind farm operator confirms cybersecurity incident

German wind farm operator Deutsche Windtechnik confirmed that it was hit with a cyberattack earlier this month, becoming the latest in a string of German energy providers to face disruptions from a cybersecurity incident.

In a statement, the company said its IT systems were targeted by a cyberattack on the night between April 11 and 12.

<https://therecord.media/german-wind-farm-operator-confirms-cybersecurity-incident-after-ransomware-group/>

Click above link to read more.

[Back to top](#)

In an interconnected world, everyone is responsible for cybersecurity

Cybersecurity threats are looming everywhere. As the Internet of Things grows, so too does the attack surface for malicious actors to take advantage.

With Russia's recent invasion of Ukraine, cybersecurity experts are warning of sophisticated attacks against infrastructure. With the stakes getting higher and the avenues for attack becoming more plentiful, understanding how to prevent an attack is key.

<https://federalnewsnetwork.com/cybersecurity/2022/05/in-an-interconnected-world-everyone-is-responsible-for-cybersecurity/>

Click above link to read more.

[Back to top](#)

How cyber security history repeats itself

In late October 2021, the European Union Agency for cyber security (ENISA) published its Threat Landscape Report. Now, in its ninth edition, this report should be considered the primary source material for IT professionals serious about addressing cyber threats and mitigating cyber risk.

This is true irrespective of whether you have a technical or corporate risk background. It's a subject that could easily fill a book, but let's focus instead on three issues raised by the report. Ignore them at your peril.

<https://www.itpro.co.uk/security/367550/how-cyber-security-history-repeats-itself>

Click above link to read more.

[Back to top](#)

Trinidad: Ministry of National Security warns of increased malicious cyber-activity

The Ministry of National Security's cybersecurity arm has warned that the country is facing a sharp increase in malicious cyber activity over the past two months and police are urging those affected to come forward with reports of these incidents.

The warning was made one day after Massy Stores confirmed that it was the target of a cyberattack and, based on this, the Trinidad and Tobago Cyber Security Incident Response Team (TT-CSIRT) has urged all entities to adopt a heightened state of awareness.

<https://www.nationnews.com/2022/05/01/trinidad-ministry-national-security-warns-increase-malicious-cyber-activity/>

Click above link to read more.

[Back to top](#)

Europe is bracing itself for cyber warfare, but is it ready?

When the systems of three oil and transport companies in Europe and Africa were brought down on February 2, 2022, Europe was preparing for a coming war in Ukraine and the impact of tensions on the Russian border were beginning to be felt in global energy markets.

The cyberattack sparked a wave of anxiety that a war in Ukraine would quickly expand online, with critical infrastructure at risk. Less than a week after the attack on SEA-Invest, and just eleven days before

Russian troops crossed the border into Ukraine, the European Central Bank warned banks in Europe to brace themselves for a wave of Moscow-sponsored cyberattacks.

<https://www.euronews.com/my-europe/2022/05/02/europe-is-bracing-itself-for-cyber-warfare-but-is-it-ready>

Click above link to read more.

[Back to top](#)

Fortinet: 80% of breaches attributed to cybersecurity skills gap

The cybersecurity skills shortage not only continues to give C-level executives a migraine, but the gap can also be linked to many breaches, Fortinet's recent report found.

For the report, Fortinet surveyed more than 1,200 IT and cybersecurity leaders from 29 different locations. The company found that 80% of surveyed organizations experienced at least one breach they could attribute to the cybersecurity skill gap, and 64% of those breaches resulted in revenue loss, recovery cost, and other financial damages.

<https://www.sdxcentral.com/articles/news/fortinet-80-of-breaches-attributed-to-cybersecurity-skills-gap/2022/04/>

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.



Security News Digest

Information Security Branch



OCIO

Office of the
Chief Information Officer