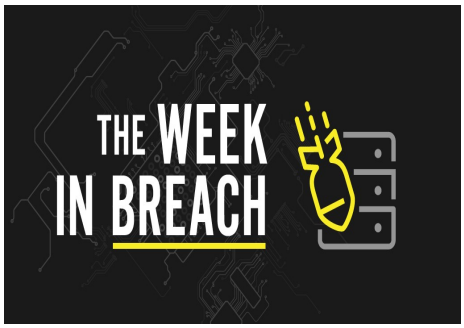
# THE WEEK IN BREACH NEWS: 11/03/21— 11//21

DenBe Computer Consulting
Connecting Business

November 10, 2021 by Dennis Jock




Canada's biggest cyberattack ever disrupts Newfoundland and Labrador healthcare, ransomware is the real villain at Diamond Comic Distributors, phishing wreaks havoc at a defense contractor plus a look at the big benefits of high cyber resilience from the new 2021 IBM Cyber Resilient Organizations Study.

---

If your business isn't using our ***Dark Web Monitoring Services*** please call us for a free scan and to discuss setting up this cutting edge monitoring service for you!

Not ready to talk yet? Visit our website to get your ***FREE Dark Web Scan.*** You will get a free, no obligation scan sent to your inbox within 24hrs. ***Visit today: www.denbeconsulting.com***

# Diamond Comic Distributors

https://bleedingcool.com/comics/diamond-comic-distributors-targeted-by-ransomware-attack/

**Exploit**: Ransomware

**Risk to Business: 1.417= Severe**

It's a bird, it's a plane, it's a ransomware attack at Diamond Comic Distributors. The Baltimore-based company, the exclusive distributor of DC and Image Comics and a publishing outlet for dozens of small-press comics publishers, suffered a ransomware attack last Friday that took down the company's website and customer service platforms all weekend into Monday. Diamond said in a statement that it did not anticipate that any customer financial data had been impacted by this event. Investigation and recovery is underway with some functions already restored.

**Individual Impact**: No consumer PII or financial data loss was disclosed in this breach as of press time.

**Customers Impacted:** Unknown

***How It Could Affect Your Business:*** *Ransomware can cost companies a fortune from operational disruption alone even if no data is snatched, not to mention incident response costs.*

# Electronic Warfare Associates (EWA)

https://www.msspalert.com/cybersecurity-news/electronic-warfare-associates-ewa-data-breach-email-phishing-incident-details/

Exploit: Phishing

**Risk to Business: 1.822=Severe**

A phishing attack that snared an employee is the suspected cause of a breach at defense contractor Electronic Warfare Associates (EWA). The company is a major provider of specialized software for the US defense establishment including the Pentagon, the Department of Defense (DoD), the Department of Justice (DoJ) and the Department of Homeland Security (DHS). EWA's investigation determined that an attacker broke into an EWA email account in August 2021 after a phishing operation. The intrusion was uncovered when the attacker attempted a wire transfer. Employee PII was exposed and concern

**Individual Risk: 1.703=Severe**

EWA has admitted that the attackers snatched files with certain personal information including name and Social Security Number and/or drivers' license number for an undisclosed number of EWA employees, but no further information was given.

**Individual Impact**: No consumer PII or financial data loss was disclosed in this breach as of press time.

**Customers Impacted:** Unknown