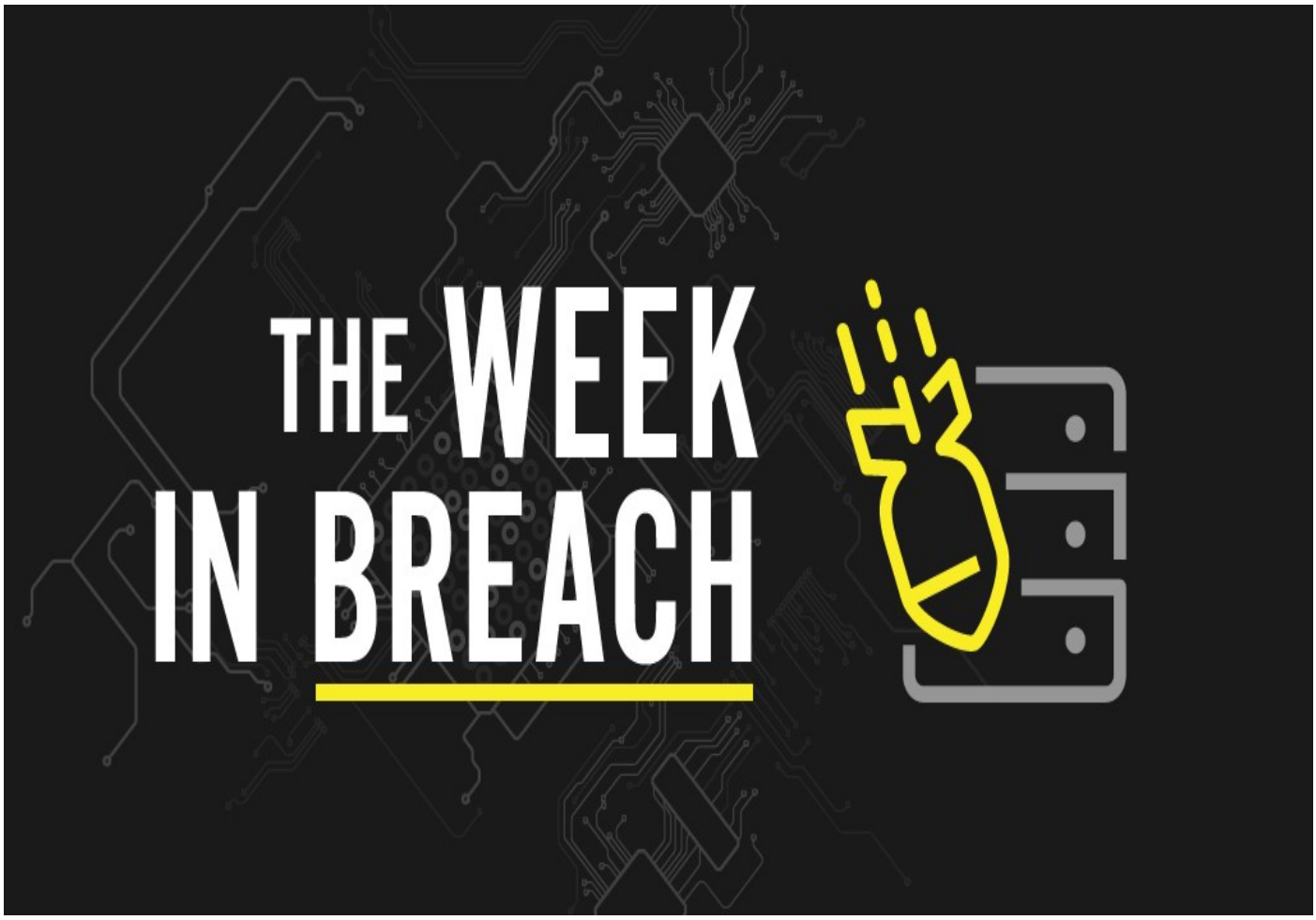
The Week in Breach News: 02/16/22 – 02/22/22

DenBe Computer Consulting
Connecting Business

February 22, 2022 by Dennis Jock



OpenSea's phishing flood just keeps getting worse, Britain's NHS is ensnared in a new data exposure drama thanks to a supply chain snafu and Baltimore officials fall for a BEC trap plus how nation-state cybercrime is threatening your clients right now.

Meyer Manufacturing Co. Ltd.

https://www.securityweek.com/cookware-distribution-giant-meyer-discloses-data-breach

Exploit: Ransomware

Meyer Manufacturing Co. Ltd.: Cookware Manufacturing & Distribution

Risk to Business: 2.177= Severe

Meyer Manufacturing Co. Ltd recently filed a data breach notification disclosing a ransomware attack that impacted employees of its distribution arm. Bleeping Computer reports that this attack is the work of the Conti ransomware group. In its disclosure, Meyer said the initial incident occurred in October 2021 but was not discovered until December 2021. The attack affected Meyer and its subsidiaries, including Hestan Commercial Corp.,

Risk to Business: 1.919= Severe

Employee personal information was snatched in this incident including their first and last name, address, date of birth, gender, race or ethnicity, Social Security number, health insurance information, medical information, driver's license, passport or government-issued identification

Customers Impacted: Unknown

How It Could Affect Your Business: *Data that can be used to falsify identities is a valuable commodity on the dark web and cybercriminals never stop looking for soft targets that enable them to steal it.*

The City of Baltimore

https://www.infosecurity-magazine.com/news/baltimore-conned-out-of-375k/

Exploit: Business Email Compromise

The City of Baltimore: Municipality

Buckle up because this is a saga. A report just released by the Office of the Inspector General (OIG) details a business email compromise disaster that ended up costing the city of Baltimore more than $375,000. In this incident, bad actors managed to change the bank details kept on file for a vendor who had an agreement with Baltimore's Mayor's Office of Children and Family Success (MOCFS). The cybercriminals contacted both MOCFS and Baltimore's Bureau of Accounting and Payroll Services (BAPS) asking to have the vendor's banking information updated to send payments to a different bank account at another financial institution. BAPS ultimately complied with the fraudster's change request, then began sending electronic payments to the new address. You know how this one ends up. Ultimately, cybercriminals made off with $376,213.10. The vendor was not named, but the report noted that cybercriminals had gained access to the vendor's email accounts through a phishing attack.

Customers Impacted: Unknown

How It Could Affect Your Business: Business email compromise is the most dangerous cybercrime according to FBI IC3, 64x worse than ransomware. This is why.

The Internet Society (ISOC)

https://thecyberwire.com/newsletters/privacy-briefing/4/33

Exploit: Misconfiguration

The Internet Society (ISOC): Non-Profit

Risk to Business: 2.776 = Moderate

Cybersecurity researchers recently announced the discovery of a trove of information belonging to ISOC in an unsecured Microsoft Azure blob. The blob was reported to contain contained millions of files with personal and login details belonging to ISOC members. ISOC has secured the blob but there's no telling how long that data was exposed for or who may have seen it.

Risk to Business: 1.282= Moderate

The member data exposed includes members' full names, preferred language, the account ID, donation history, login credentials, social media tokens, email and street addresses, genders and similar personal information.

Customers Impacted: Unknown

How It Could Affect Your Customers' Business*: Human error aka employee negligence is the biggest cause of a data breach because it's what makes things like this happen.*

Expeditors International

https://www.bleepingcomputer.com/news/security/expeditors-shuts-down-global-operations-after-likely-ransomware-attack/

Exploit: Ransomware

Expeditors International: Logistics & Freight Forwarding

Risk to Business: 1.364 = Extreme

Expeditors International was hit by a ransomware attack over the President's Day holiday weekend that has resulted in the company being forced to shut down most of its operations worldwide. First announced by the company on Sunday night, Expeditors International warned that services and systems may be offline until they can restore them from backups. The incident could snarl supply chains globally. Expeditors International handles warehousing and distribution, transportation, customs and compliance at 350 locations worldwide.

Customers Impacted: Unknown

How it Could Affect Your Customers' Business *Supply chain disruption has been the name of the game for cybercriminals and freight forwarders on land and on the sea have been constantly targetted lately*

OpenSea

https://www.cnbc.com/2022/02/20/nft-marketplace-opensea-is-investigating-a-phishing-hack.html

Exploit: Phishing

OpenSea: NFT Trading Marketplace

Risk to Business: 1.282=Extreme

Online NFT marketplace OpenSea has been embroiled in controversy after a cyberattack cost investors their NFT. There's been a lot of back-and-forth on this one. A phishing attack perpetrated on the platform's users is purportedly to blame for the incident that has so far left more than 30 of its users unable to access their NFTs, although some claims have been made on Twitter pointing to a flaw in the platform's code. Reports say that the attacker has made somewhere between $1.7 – 2 million in Ethereum from selling some of the stolen NFTs. An estimated 254 tokens were stolen

Individual Impact: No information about consumer/employee PII, PHI or financial data exposure was available at press time.

Customers Impacted: Unknown

How it Could Affect Your Business *Phishing is a danger to any business in any industry, and it can do massive damage as well as cost a fortune.*