THE WEEK IN BREACH NEWS: 12/02/20 – 12/08/20

DenBe Computer Consulting
Connecting Business

December 9, 2020 by Dennis Jock

This Week in Breach News: Egregor ransomware is flying high in retail, manufacturing & staffing around the world, and Amazon phishing scams are even more of a holiday menace than usual to businesses this year.

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***

Greater Baltimore Medical Center

https://www.securityweek.com/greater-baltimore-medical-center-hit-ransomware-attack

Exploit: Ransomware

Greater Baltimore Medical Center: Hospital

Risk to Business: 1.622 = Severe

A ransomware attack left Greater Baltimore Medical Center (GBMC) scrambling after many of its systems were knocked offline, impacting patient care. Procedures scheduled for 12/07/20 had to be rescheduled. Backups and workarounds enabled the hospital to keep functioning as the attack was investigated and mitigated. Recovery is ongoing.

Individual Risk: No personal or consumer information was reported as impacted in this incident.

Customers Impacted: Unknown

How it Could Affect Your Customers' Business: Ransomware is increasingly being used as a way to cause operational disruptions instead of just snatching data, complicating its impact.

AspenPointe

https://www.bleepingcomputer.com/news/security/healthcare-provider-aspenpointe-data-breach-affects-295k-patients/

Exploit: Unauthorized Database Access

AspenPointe: Healthcare Non-Profit

Risk to Business: 1.613 = Severe

AspenPointe has disclosed a large data breach that exposed personally identifying information (PII) of patients working with non-profit organizations that it manages including participants in its mental health and substance misuse programs. The unauthorized access took place in early September 2020 and it's unclear how much data was stolen. AspenPointe is a nonprofit funded by Medicaid, state, federal, and local government contracts, as well as donations, that manages 12 organizations providing care and counseling in Colorado.

Individual Risk 1.820 = Severe

Patients may have had extensive personal and private information exposed including PPI like their date of birth, Social Security number, Medicaid ID number, date of the last visit (if any), admission date, discharge date, and/or diagnosis code. AspenPointe is providing those affected by the data breach IDX identity theft protection services including "12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services."

Customers Impacted: 295,617

How it Could Affect Your Customers' Business: Data breaches at any business are bad news, but at a business like this, it's a nightmare. Not only will AspenPointe have to deal with the corporate fallout, but regulators are also going to come calling with fines as well, making this incident extra expensive.

Philabundance

https://www.phillyvoice.com/philabundance-cyberattack-theft-1-million-dollars/

Exploit: Business Email Compromise

Philabundance: Hunger Relief Non-Profit

Risk to Business: 2.017 = Severe

Hunger relief charity Philabundance got bilked by BEC scammers at the worst possible time. The charity, which fed 54,700 Philadelphians weekly in 2019, is now feeding 134,800 people each week. This incident occurred when the organization paid a construction bill of over $923,000 for a new $12 million facility built in North Philly for its Community Kitchen program, only to discover that they'd paid scammers instead. It's believed that the con was enabled by a hack on the charity's computer systems in July that enabled scammers to divert legitimate email from the construction company and replace it with their own fakes. Philabundance says that daily operations will not be impacted by the incident, but it remains a huge problem for this organization at a time when so many Americans rely on programs like this to keep their families fed.

Individual Risk: No personal or consumer information was reported as impacted in this incident.

Customers Impacted: 134,800 Philadelphians daily

How it Could Affect Your Customers' Business: Business email compromise scams are some of the thorniest problems that every business faces. Good regularly refreshed security awareness training will help employees spot and stop BEC scams.

Kmart

https://threatpost.com/kmart-egregor-ransomware/161881/

Exploit: Ransomware

Kmart: Retail Store Chain

Risk to Business: 1.802 = Severe

Already beleaguered retailer Kmart did not need the extra complications that came with the Egregor ransomware attack that was delivered to their door. The incident has encrypted devices and servers connected to the company's networks, knocking out back-end services and corporate operations functions. Retail stores are operating normally and no consumer impact has been reported.

Individual Risk: No personal or consumer information was reported as impacted in this incident.

Customers Impacted: Unknown

How it Could Affect Your Customers' Business: Ransomware is a disaster for any business, but it's an especially cruel problem for a non-profit these days.

Alaska Division of Elections

https://www.juneauempire.com/news/113000-alaskan-voter-ids-exposed-in-data-breach/

Exploit: Hacking

Alaska Division of Elections: State Agency

Risk to Business: 2.336 = Severe

An election-time data breach involving voter registration information was recently disclosed in Alaska. State and federal officials say that the election process was not impacted, but voter data was obtained for more than 100K Alaskan voters. Officials suspect nation-state hackers may be involved.

Individual Risk 2.114 = Severe

The database snatched included some PII like birth dates, driver's license or state identification numbers, the last four digits of social security numbers, full legal names, party affiliation, and official mailing addresses.

Customers Impacted: 113,000 voters

How it Could Affect Your Customers' Business: Nation-state hacking is an especially serious problem for government agencies and infrastructure targets. Adding extra security with MFA and similar tools helps combat this risk.