Cyber Roundup – April 2021

By Thomas J. DeMayo, Principal, Cybersecurity and Privacy Advisory

It may be that numbers don't lie, but in the cyber world they sure can engender trepidation. Cybercrime is constantly on the rise and the costs associated with it are expected to be $6 trillion in 2021. The largest ransomware demand to date is $50 million. Every individual and every business – private, public, governmental – can be targeted. As Cyrus Vance Jr., Manhattan District Attorney, said in 2010: *The Internet is the crime scene of the 21st Century.* Our Cybersecurity team can help you ramp up your security.

Key Cyber Events

The following is a rundown of what happened during the month of March 2021. We welcome your comments, insights and questions.

- **In a report by Cybersecurity Ventures, it is noted that the global cybercrime cost is estimated to increase to $10.5 trillion by 2025.** On average, the global cost of cybercrime increases 15% each year. To help place the cost in perspective, they further noted that with an estimated cost of cybercrime at $6 trillion in 2021, that would place the costs as the third largest economy after the United States and China.

- **Enterprise security camera solutions provider, Verkada, suffered a breach that resulted in cyber criminals gaining access to 150,000 customer video archives.** Impacted customers included major names such as Tesla, Cloudflare, and Equinox. The hack is believed to have occurred as a result of administrative credentials exposed on the internet through publicly available listings.

- **A breach of Astoria Company, LLC, a lead generation company that collects information on consumers in the market for car loans, medical insurance, or payday loans, resulted in the exposure of 300 million user records.** Twenty million of those records breached included highly sensitive information such as a SSN, bank account information and medical information. The breach was the result of a developer flaw that resulted in the administrative web login page automatically populating the username and password of an administrator.

  Tom's Takeaway: When we think of a cyber breach, many of us associate it with a sophisticated "hack" by a cybercriminal. This serves as a reminder that sometimes it is as simple as the "remember me" feature of a web session. As the world becomes more digital, and more and more developers enter the market place, teaching and enforcing secure program development will be key. Equally as important, will be the system development lifecycles implemented by companies to identify security issues before they reach the public.

- **The California State Controller's office became a victim of a phishing attack.** The attack resulted in unauthorized access by the cyber criminals and the theft of SSNs and other sensitive information on the state's multi-thousand work force. The cyber criminals further leveraged the stolen information to phish 9,000 more state workers and other contacts.

- **The FBI released a Private Industry Notification alerting state and local governments to have increased awareness related to business email compromise scams.** The FBI noted that government entities are being targeted by cyber criminals impersonating vendors and suppliers. Millions have been lost over the past two years with losses ranging from $10,000 up to $4 million.

Tom's Takeaway: No different than a commercial business, a government entity needs to make a decision on where they want to allocate a finite set of funds. No different than a commercial business, a government entity is a prime target by cyber criminals. For a government entity, strong cyber controls are not only a matter of protecting the information of its constituents, but could also result in a matter of life safety. Local government entities are strongly encouraged to evaluate the strength of its cyber program ***independently***. Leverage the assessment to evaluate the effectiveness of cybersecurity spend to ensure the finite resources are allocated effectively and optimally. As a firm, we specialize in local government entities. If you need assistance, we can help.

- **In a report by Barracuda Networks, it was noted that phishing attacks have increased 26% after the release of COVID-19 vaccines.** The prominent type of phishing scams leveraged brand impersonation of the major vaccine suppliers. Other scam premises consisted of the following:
  - Early access to the vaccine in exchange for payment.
  - The submission of personal information to check for vaccine eligibility.
  - Employee impersonation requesting assistance while they are getting the vaccine.
  - Human Resource impersonation noting that vaccines are available for employees.
- **Consistent with the past year, ransomware events dominated the headlines.** The following is a summary of major ransomware attacks:
  - In an effort to increase the pressure on victimized companies to pay, ransomware operators have resorted to reaching out to journalists and impacted business partners and customers to place pressure on the victimized company to pay the ransom in order to protect the stolen data.
  - IT managed service provider, CompuCom, is estimating that losses as a result of ransomware will exceed $20 million. The company provides IT-related services to major companies such as Citibank, Home Depot, Target, and Wells Fargo.
  - In a study by Palo Alto Networks, it was noted that ransomware payments continue to increase, averaging $115,123 in 2019 and up to $312,493 in 2020. The highest requested ransom was $30 million in 2020, up from $15 million in 2019.
  - Payroll and HR software provider, PrismHR, suffered a ransomware attack. The attack impacted 200 of their clients across the U.S., potentially impacting payroll processing.
  - The FBI released a warning to schools in the U.S. and UK of increased targeting by the PYSA (a strain of ransomware) operators.
  - Computer maker, Acer, suffered a ransomware attack in which the cyber criminals are demanding $50 million from the company, the highest ransom demand to date.

Contact Us

Thomas J. DeMayo, Principal, Cybersecurity and Privacy Advisory
CISSP, CISA, CIPP/US, CRISC, CEH, CHFI, CCFE

PKF O'Connor Davies, LLP
665 Fifth Avenue, New York, NY, 10022
212.867.8000 or 646.449.6353 (direct)
tdemayo@pkfod.com

www.pkfod.com

About PKF O'Connor Davies

PKF O'Connor Davies, LLP is a full-service certified public accounting and advisory firm with a long history of serving clients both domestically and internationally. With roots tracing to 1891, fourteen offices in New York, New Jersey, Florida, Connecticut,

Maryland and Rhode Island, and more than 800 professionals, the Firm provides a complete range of accounting, auditing, tax and management advisory services. PKF O'Connor Davies is ranked 27th on *Accounting Today*'s 2020 "Top 100 Firms" list. It is also ranked among the top 20 best accounting employers to work for in North America by *Vault*.

PKF O'Connor Davies is the lead North American representative in PKF International, a global network of legally independent accounting and advisory firms located in over 400 locations, in 150 countries around the world.

Our Firm provides the information in this e-newsletter for general guidance only, and it does not constitute the provision of legal advice, tax advice, accounting services, or professional consulting of any kind.