

Cyber Security Presentation



BakerHostetler



M. Scott Koller

Partner

BakerHostetler

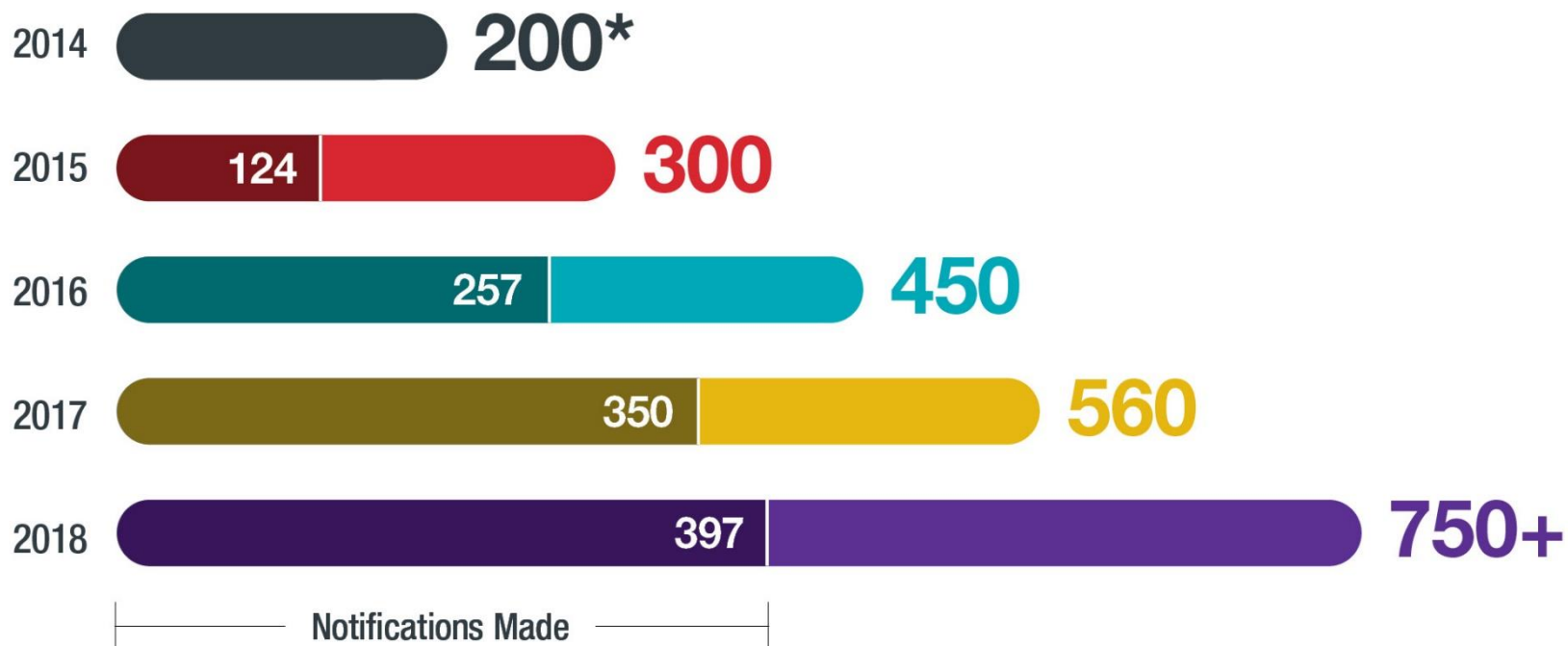
Data Privacy Group

310.979.8427

mskoller@bakerlaw.com

- Chambers Global ranked & Legal 500 ranked Privacy and Data Protection practice
- BTI Cybersecurity Powerhouse (2020)
- Privacy and Data Protection “Practice Group of the Year” by Law360 in 2013, 2014, 2015, & 2018
- 70+ attorneys specializing in privacy and data security law nationwide
- 3,500+ incidents handled (1,000+ in 2019 alone)
- 200+ incident response training workshops and tabletops
- 400+ regulatory investigations
- 100+ privacy and data security class actions

Numbers of Incidents



Not all incidents require notification – over four years, notice was provided in 53% of incidents.

*Not all data sets mentioned were measured in the 2014 DSIR Report, our first edition.

750+

Incidents in 2018



U.S. Breach Notification Law Interactive Map

bakerlaw.com/BreachNotificationLawMap

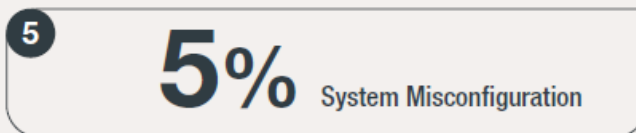
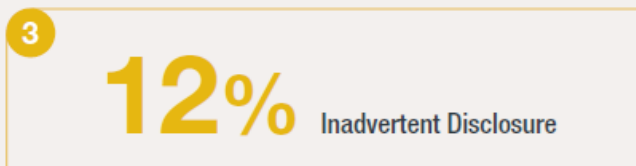
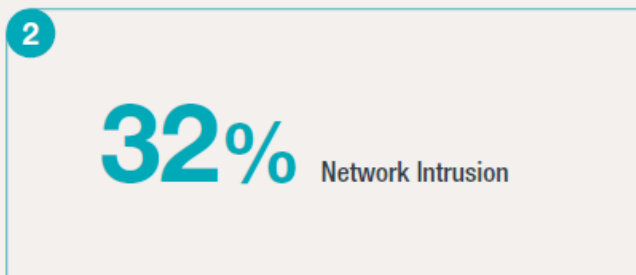


EU GDPR Data Breach Notification Resource Map

bakerlaw.com/EUGDPRResourceMap

Incident Causes

Top 5 Causes



What Happens Next After Phishing



31%
Office 365
Account Takeover

8%
Wire Transfer

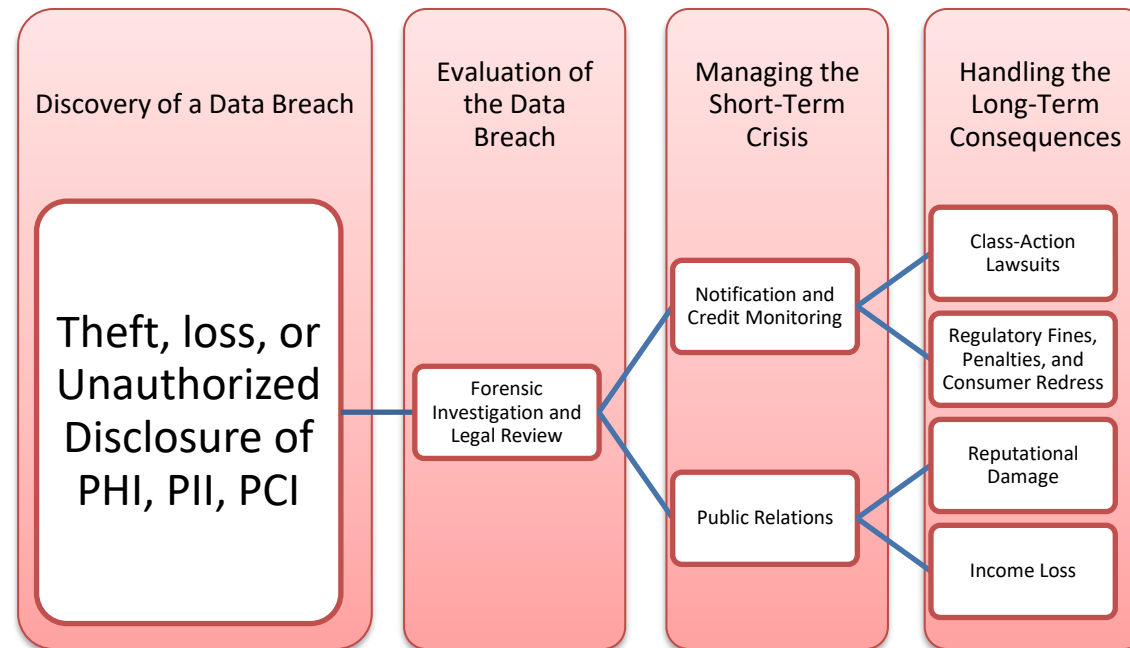
24%
Ransomware

7%
Theft of Data

13%
Network Intrusion

1%
Espionage

A Simplified View of a Data Breach



Incident Response Timeline

Incident Response Timeline (median)

12

Days

Occurrence to Discovery

3

Days

Discovery to Containment

34

Days

Time to Complete Forensic
Investigation

38

Days

Discovery to Notification

LILY HAY NEWMAN

SECURITY 04.23.2018 08:55 PM

Atlanta Spent \$2.6M to Recover From a \$52,000 Ransomware Scare

Whether to pay ransomware is a complicated—and costly—calculation.



Ryuk gang estimated to have made more than \$150 million from ransomware attacks

Most of the Ryuk gang's "earnings" are being cashed out through accounts at crypto-exchanges Binance and Huobi.



Image: QuinceCreative

The operators of the Ryuk ransomware are believed to have earned more than \$150 million worth of Bitcoin from ransom payments following intrusions at companies all over the world.

\$18.8 million

Largest ransom demand
in 2019

\$5.6 million

Largest ransom paid in 2019
(2018 largest was \$250,000)

\$302,539

Average ransom payment
amount (2018 average
was \$28,920)



encryption key received
after payment made



payment made by third party
for the affected organization

73%

of the time organization restored from backup
or managed without paying ransom

6%

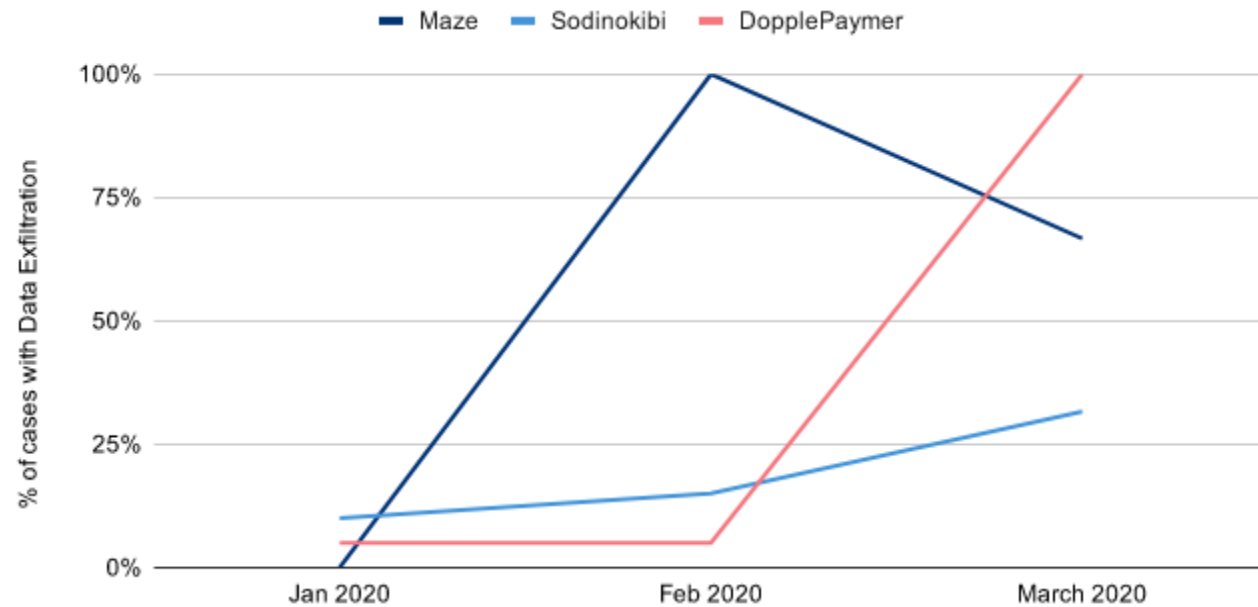
of incidents involved unauthorized access or
acquisition of data resulting in notification
to individuals

Ransomware Epidemic

Cases with data exfiltration

8.7%

Data Exfiltration Rates



Data exfiltration, where data is downloaded from victim computers and is threatened to be released publicly, became a prevalent tactic during ransomware attacks in Q1 2020. This was a big change from the previous quarter where it was virtually non-existent.

Office of Foreign Assets Control

- On October 1, 2020, the U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) issued an advisory regarding ransom payments and the risk of sanctions associated with such payments.



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments¹

Date: October 1, 2020

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is issuing this advisory to highlight the sanctions risks associated with ransomware payments related to malicious cyber-enabled activities. Demand for ransomware payments has increased during the COVID-19 pandemic as cyber actors target online systems that U.S. persons rely on to continue conducting business. Companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in

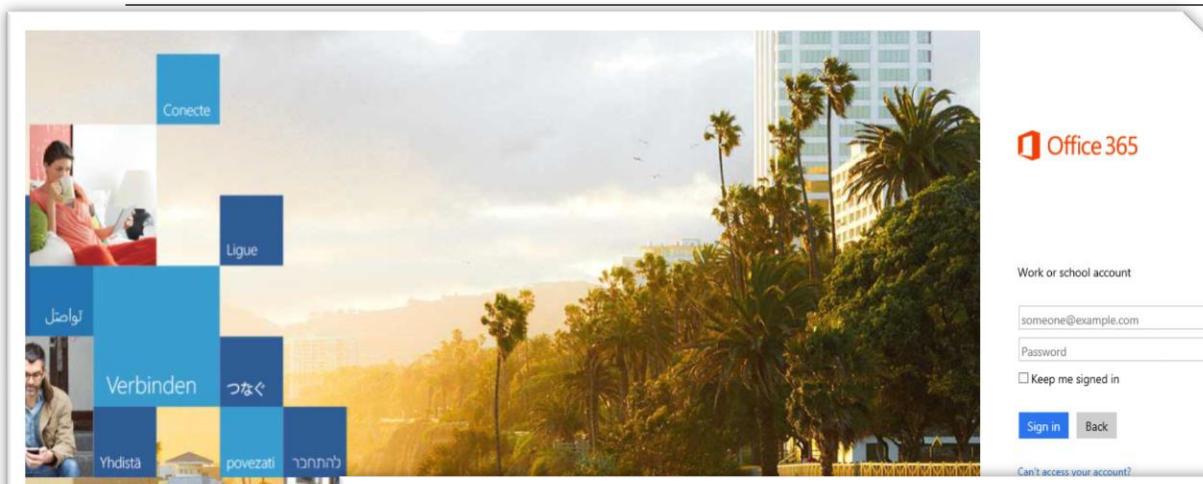
Key Takeaways

- The U.S. Government disfavors payments of ransom, but there is no general ban.
- Payments to sanctioned individuals and/or entities, however, can result in significant penalties and applications for licenses to make such payments will be handled with a presumption of denial, which may be based on U.S. policy interests alone.
- Cooperating with law enforcement is critical. The U.S. Government benefits because it can gather more information about these threat actors to help with prosecution. Although our clients are generally working with law enforcement, we are hearing that many companies are not reporting these incidents to the FBI. OFAC's guidance is pushing companies to work with the FBI more closely. The benefit to the company is the threat information sharing, which could also include information about the origin of the threat actor. In addition, OFAC has identified early and continuing cooperation with law enforcement as a "significant mitigating" factor in an enforcement context.

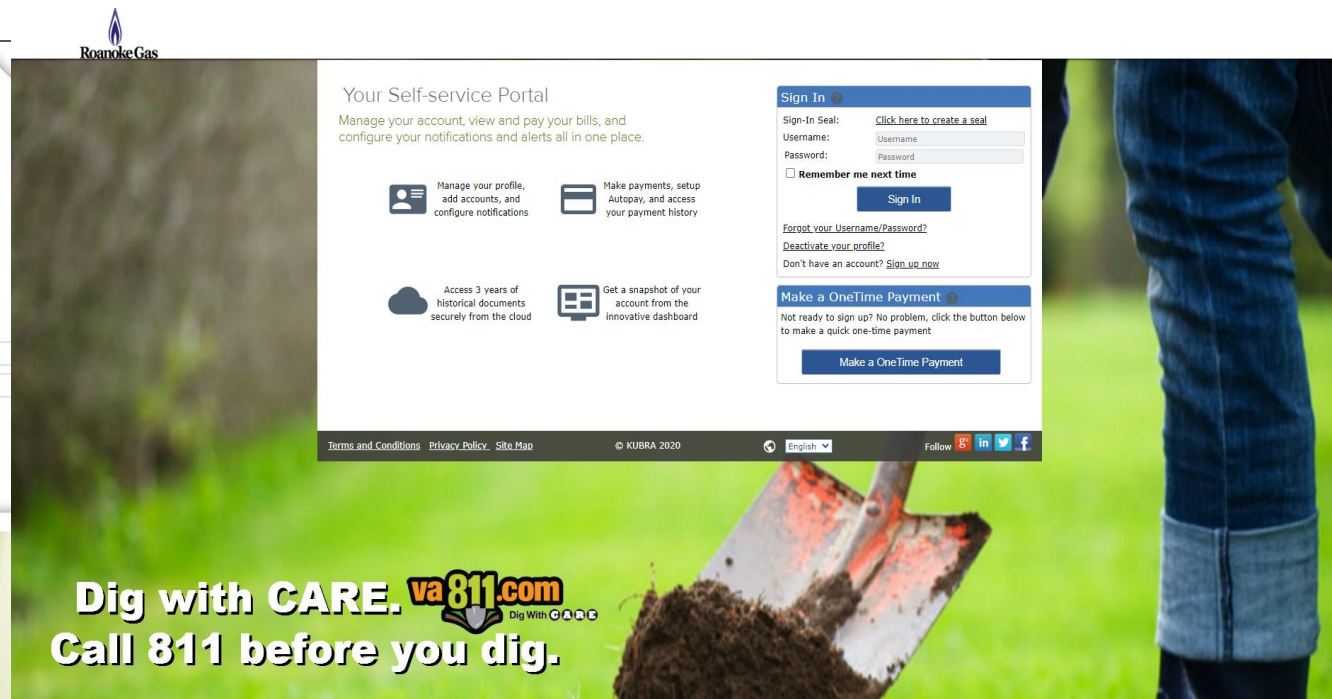
Take Action: Address Ransomware Risk

- ▶ Guard against phishing, address security gaps caused by limited utility of antivirus against banking trojans like Trickbot and Emotet, and secure remote access (e.g., open RDP ports).
- ▶ Enable MFA for the organization and any service providers with remote access.
- ▶ Evaluate your business continuity and disaster recovery plans and how they integrate with your incident response plan.
- ▶ Look at your strategy for backups. Current backups, segmented from production systems and easily accessed, can help you avoid business interruption without paying a ransom.
- ▶ Understand your insurance resources. Think through the hourly impact of downtime in the event you have to decide whether, when, and how much ransom to pay.
- ▶ Ransomware attacks can also involve access to data that triggers notification obligations – contractual and legal. In the rush to restore systems, some organizations wipe and reimage devices without preserving evidence, which complicates the ability to determine what occurred after the attacker gained access to the network before ransomware was deployed.

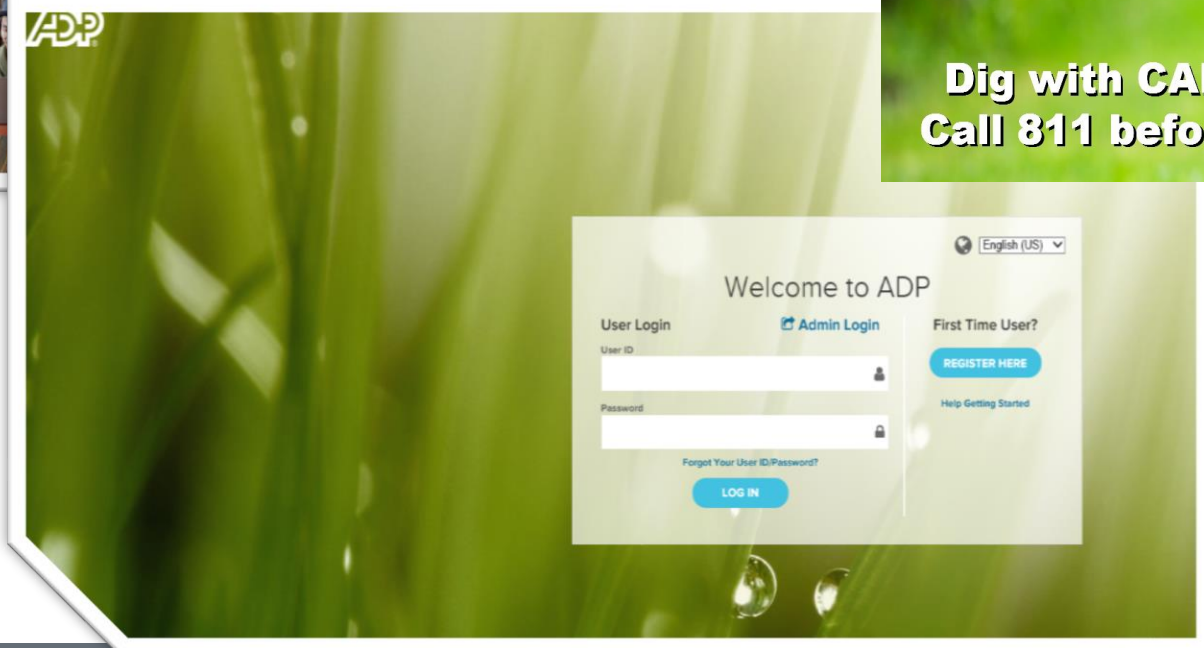
Account Takeovers



Office 365 login page. The page features a background image of palm trees and a building. On the left, there is a grid of blue and white squares with text in various languages: "Conecte", "Ligue", "تواصل", "Verbinden", "つなぐ", "Yhdistä", "povezati", and "لتواصل". The main content area includes the Office 365 logo, the text "Work or school account", a "Work or school account" checkbox, a text input field for "someone@example.com", a "Password" input field, a "Keep me signed in" checkbox, and "Sign in" and "Back" buttons. A link "Can't access your account?" is at the bottom.



Roanoke Gas self-service portal. The page has a green background with a shovel digging up soil. The header includes the "Roanoke Gas" logo. The main heading is "Your Self-service Portal" with the subtext "Manage your account, view and pay your bills, and configure your notifications and alerts all in one place." Below this are four service icons: "Manage your profile, add accounts, and configure notifications", "Make payments, setup Autopay, and access your payment history", "Access 3 years of historical documents securely from the cloud", and "Get a snapshot of your account from the innovative dashboard". On the right is a "Sign In" form with fields for "Username" and "Password", a "Remember me next time" checkbox, and a "Sign In" button. Below the form are links for "Forgot your Username/Password?", "Deactivate your profile?", and "Don't have an account? Sign up now". At the bottom right is a "Make a OneTime Payment" button. The footer contains "Terms and Conditions", "Privacy Policy", "Site Map", "© KUBRA 2020", a language dropdown set to "English", and social media icons for YouTube, Instagram, LinkedIn, Twitter, and Facebook.



ADP login page. The page has a green background with a close-up of a plant stem. The ADP logo is in the top left. The main heading is "Welcome to ADP". There are two login options: "User Login" and "Admin Login". The "User Login" section has a "User ID" input field, a "Password" input field, a "Forgot Your User ID/Password?" link, and a "LOG IN" button. The "Admin Login" section has a "First Time User?" checkbox, a "REGISTER HERE" button, and a "Help Getting Started" link. A language dropdown is set to "English (US)".

Dig with CARE. **va811.com**
Dig With CARE
Call 811 before you dig.

Business Email Compromise

Over 70%

of the email account access incidents in 2019 resulted in notification to individuals and regulators



of notifications involved a population of under 10,000



had more than one incident in 2019

30+ days longer

to notify than median time to notification for all incidents due to “e-discovery process” to find personal information and match to a mailing address



Business Email Compromise

Take Action:

Prevent Account Access and Wire Transfers

- ▶ Properly implemented MFA significantly reduces risk.
- ▶ Pair MFA with a properly configured Office 365 tenant or G Suite, which includes disabling legacy protocols (e.g., IMAP and POP3) that do not support modern authentication, adjusting SPF/DKIM/DMAR, IP blacklisting where possible, setting alerts for “impossible logins” and creation of forwarding rules, and enabling appropriate logging.
- ▶ If it is not there it cannot be taken. Use good governance and retention practices to limit what is sent by email and how long emails are retained.
- ▶ Employee training and awareness – not just training on phishing and social engineering but also the proper use of MFA (if you are not attempting to log in, do not hit “Accept”).
- ▶ Use good out-of-band verification protocols for changing wire instructions.

“Reasonable Security”

- **Align to a security framework** – such as NIST CSF. Many of the other items listed below are identified as components of one of these security frameworks.
- **Do risk assessments** – identify critical assets, threats, and vulnerabilities. Use assessment to prioritize cybersecurity roadmap/maturity plans. .
- **Know your environment** – if you do not know what devices you have you cannot defend them (e.g., avoids scenarios where you deploy an endpoint tool but it does not get provisioned on every device and then those are the devices that are first compromised).
- **Know what data you have and where it resides** – if you do not know what data you have and where it resides, you are not likely to implement appropriate measures (or even know when there is unauthorized access to it). A data inventory is also part of complying with the new obligations under CCPA and is part of a GDPR compliance program.
- **Multifactor authentication** – enable MFA where you can, especially for Office 365 (and disable backwards compatible apps that do not support MFA/modern authentication) and any other cloud based application where logging in provides access to sensitive data (e.g., payroll services like ADP – apply MFA at least for HR admin users).
- **Manage cloud assets** – address access rights for cloud resources (make sure that they are not set to public access where anyone that knows the url can see what is in the bucket).
- **Endpoint security** – deploy an endpoint tool that goes beyond signature-based AV detection. Examples are FireEye’s HX agent, CrowdStrike’s Falcon, Carbon Black, Tanium, or Cylance.
- **Encryption** – encrypt portable devices (e.g., laptops, USB drives), sensitive data at rest (e.g., payment card numbers, SSNs), and passwords for online accounts (do not just hash).
- **Patch management** – use a tool for patching and evaluate patching cycle.
- **Logging and log monitoring** – use a SIEM and have a SOC (internal or outsourced) to provide 24/7 monitoring of logs and alerts. Talk to security firm that does forensic investigations about log retention and details to log (this identifies evidence sources that enable them to be more precise in their investigation).
- **Phishing** – use an email filter to reduce the amount of phishing emails that get through (e.g., Proofpoint, Mimecast, FireEye’s ETP)
- **Security awareness training** – design and implement a program that teaches employees about phishing and social engineering. Test phishing exercises are pretty common.
- **Vendor management** – build a program that appropriately vets vendors (e.g., marketing cannot just sign up someone – other disciplines should be involved including legal and security), negotiate appropriate contractual protections and rights (you can build a data security addendum you add to vendor agreements to cover your core terms/needs), and oversee vendors after selection.
- **Business continuity** – ransomware has become very problematic. Have good backups that are readily available and not stored on each host they are a backup of.

Questions?

M. Scott Koller

Partner at Baker Hostetler
11601 Wilshire Boulevard | Suite 1400
Los Angeles, CA 90025-0509
T +1.310.979.8427
mskoller@bakerlaw.com

