



Cybersecurity Update

December 10, 2020

WILK AUSLANDER | *As*

Natalie Shkolnik, Esq.

Partner at Wilk Auslander LLP
212-981-2294
nshkolnik@wilkauslander.com



Experience in cybersecurity matters, judgment enforcement, commercial and securities litigation, government and regulatory investigations, and cross-border issues.

Mark S. Piazza

4A's SVP - Business Intelligence & Insight Group
212-850-0760
mpiazza@4as.org





WHAT DOES COVID-19 MEAN FOR CYBERSECURITY?

- The shift to working remotely due to the pandemic has had major consequences for cybersecurity.
- Now that employees are using more devices and different kinds of devices, including personal devices, malign actors' "attack surface," or the range of opportunities to steal data, has expanded. There are now major vulnerabilities that did not exist before COVID.
- The FBI reported on April 16, 2020, that the number of complaints about cyberattacks has increased to as many as 4,000 per day, a 400% increase from pre-COVID levels.
- McAfee Labs, the threat research division of the antivirus software company, observed an average of 419 malware threats per minute in Q2 2020, a 12% increase over Q1 2020.

DEFINING THE BIGGEST RISKS

- Malware is any program or file that harms a computer, such as a virus.
- Ransomware is one type of malware – it is when the malign actor infects a system and disables it until the owner pays a ransom, sometimes millions of dollars.
 - Attacks can cause downtime, data leaks, intellectual property theft and data breaches.
 - Ransomware attacks now account for one third of all cyberattacks.¹
 - Attackers demand payment by cryptocurrency such as bitcoin.

Oops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send \$300 worth of Bitcoin to following address:
1Mz7153HMuxXtuR2R1t78mGSdzaAtNbBWx
2. Send your Bitcoin wallet ID and personal installation key to e-mail
wowsmith123456@posteo.net.

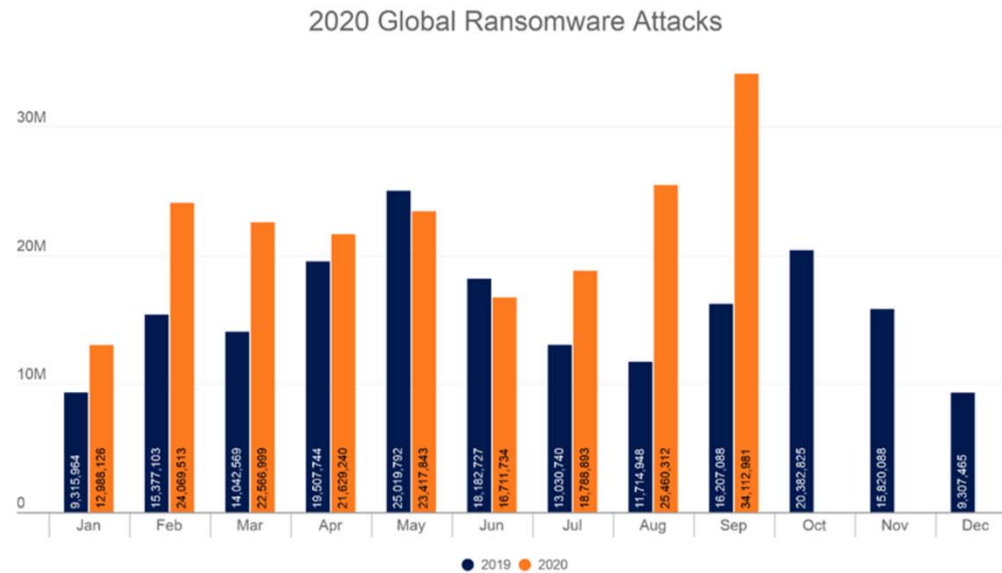
2



DEFINING THE BIGGEST RISKS – continued

- Phishing is common, and can introduce ransomware and other kinds of malware to a computer or network. Phishing is when a malign actor sends an email that looks reputable in order to induce the recipient to reveal personal information or click on an attachment or link that will infect the computer with malware.
 - As of September 1, 2020, in almost half of ransomware cases, the attackers gained access through the remote access systems, either through phishing emails or exploiting the system's vulnerabilities.³
- Business email compromise is almost as common as ransomware. In these attacks, hackers impersonate an executive authorized to make wire transfers or other decisions, and induce the target to transfer the money or confidential information to them.
 - For example, the FBI reported on April 6, 2020, that a bank received an email allegedly from the CEO of a company requesting that a previously-scheduled transfer of \$1 million be moved up and the recipient account changed due to the pandemic and quarantine precautions.

THE NUMBERS: RANSOMWARE ATTACKS, 2019-2020



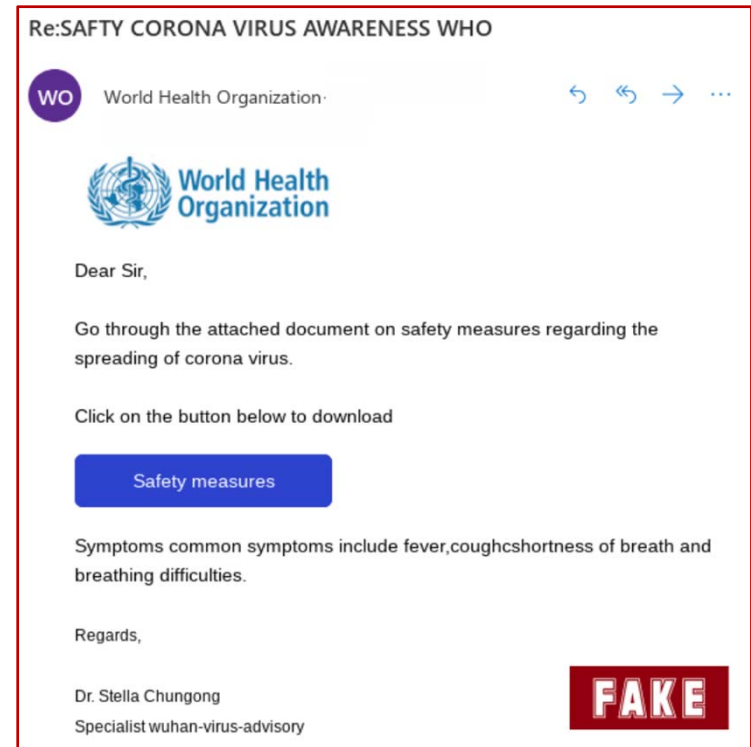
SONICWALL

www.sonicwall.com

Ransomware attacks have generally been more common in 2020 than in 2019, with a significant increase in August and September 2020. September 2020 totals exceeded 34 million.⁴

COVID-SPECIFIC ATTACKS

- The government's efforts to respond to the pandemic have created new opportunities for bad actors, such as phishing attacks aimed at coronavirus stimulus check fraud. On August 15, 2020, the Canadian government revealed that a cyberattack had stolen COVID relief payments out of almost 10,000 accounts.
- Other examples include malware that looks like COVID information or work-from-home resources. One strain of ransomware is using files with "coronavirus" in the name so that they look important.



COVID-SPECIFIC ATTACKS – continued

- Or, hackers may send emails disguised as government emails or charity solicitations. The FBI has recently warned that scammers are posing as charities. By clicking on the links in such messages, users may download harmful viruses or other malware.⁶

Washington, D.C.
FBI National Press Office
(202) 324-3691

[Twitter](#) [Facebook](#) [Email](#)

October 14, 2020

FBI Warns of Potential Charity Fraud Associated with the COVID-19 Pandemic

Many Americans want to help during the COVID-19 pandemic by contributing to charities, but the FBI is warning that scammers also want to help—they want to help themselves to your money.

Nationwide, the FBI and other law enforcement agencies have received reports of scammers fraudulently soliciting donations for individuals, groups, and areas affected by COVID-19. They are leveraging the COVID-19 pandemic to steal your money, your personal information, or both. Don't let them.

Charity scams often occur when a scammer poses as a real charity or uses the name of a real charity to get money from you.

Be careful about giving money to any charity calling you for donations and be wary if you get a call about a donation pledge that you don't remember making. Remember, you can't always believe your caller ID. Scammers often spoof organizations' phone numbers. It's always best to research the organization telephone number yourself and call direct to verify. Do not be pressured or rushed to donate. That is a strong indicator of a scam.

Similarly, if you receive an email purporting to be from a charitable organization, do not click on links. These could be attempts to download viruses onto your computer or cell phone. Watch out for charity names which sound very similar to well-known charities, as well as email addresses that are not consistent with the charity soliciting donations. Instead, search for the charity using an internet search engine to ensure you're connected to the actual charitable organization.



PROFESSIONAL SERVICE COMPANIES ARE FREQUENT TARGETS

- Lessons learned from data breaches across all industries are transferable. While anyone on the internet can be the target of a cyberattack, professional service companies are frequent targets.
- Grubman Shire Meiselas & Sacks: On May 7, 2020, hackers targeted an entertainment law firm that provides legal services to many high-profile individuals including Madonna, Tom Cruise, Bruce Springsteen, and Lady Gaga. Around 756 GB of data was leaked, including contracts, contact information, personal correspondence, and non-disclosure agreements made with ad agencies and modeling firms. The hackers reportedly were paid \$365,000 so far, but have demanded \$42 million.
- Online marketing company View Media suffered a data breach in September 2020 in which the contact information of 39 million U.S. users was left on a publicly accessible Amazon Web Services (AWS) server.

'View Media' Exposed 39 Million User Records on Unprotected AWS Database

By [Bill Toulas](#) / September 3, 2020



PROFESSIONAL SERVICE COMPANIES ARE FREQUENT TARGETS

- Australian graphic design firm Canva was attacked on May 24, 2019. Malign actors accessed usernames, emails, and passwords for 139 million users.

Canva 'working around the clock' to investigate data breach

[James Walker](#) 28 May 2019 at 14:50 UTC
Updated: 29 May 2019 at 08:07 UTC

Data Breach

Attack against graphic design site said to impact 139 million users

- Other media companies including BuzzFeed, Facebook, Sony, and the Washington Post have also experienced cyberattacks.



COMPANIES OWE DUTIES TO THEIR EMPLOYEES, NOT JUST THEIR CUSTOMERS

- Employees' data should be just as secure as customers' data.
- Dittman v. University of Pittsburgh Medical Center⁷
- Sackin v. TransPerfect Global, Inc.⁸
- Hapka v. CareCentrix, Inc.⁹
- Limits: Need evidence that the breach caused damages.
- Written policies should clearly explain the duty.

November 26, 2018 12:00 AM

Judge rules UPMC should have protected employee data

RACHEL Z. ARNDT  



A STRONG CYBERSECURITY PROGRAM

Zero-Trust Architecture: “Never trust, always verify.”

- Implement multi-factor authentication. This may reduce your risk by 40 percent.¹⁰
- Assess every device that accesses your company’s network, whether or not it is a company device, to determine its trustworthiness.
- Network segmentation: users should be given access only to the extent needed to perform their jobs.
- All activity must be logged and monitored.
- Regular penetration testing and risk assessments.
- Use a virtual desktop infrastructure (VDI).
- Whichever remote access system you use, ensure it is secure.



A STRONG CYBERSECURITY PROGRAM – continued

The following measures complement zero-trust architecture:

- Have a written incident response communications plan.
 - Duties and responsibilities for every phase of response, from detection to negotiations with law enforcement to recovery of the data.
 - Regular security reporting to the board.
 - In the event of a security event, immediate notice to the CEO.
 - In the event of a breach, immediate notice to the CEO and the designated first response team.
- Continuously train employees on the threats they face, including by testing users with phishing simulations and working with specific employees to help them understand best practices.
- Encourage remote workers to use best practices at home, such as changing their default WiFi passwords and regularly checking for software updates for their routers.
- Purchase cyber insurance.



A STRONG CYBERSECURITY PROGRAM – continued

Assess your long-term cybersecurity needs.

- What devices, tools, platforms, and staffing does your IT department need to protect a remote workforce?
- Does your equipment need to be updated?
 - Case study: In July 2019, Lenovo, a computer and technology company, confirmed that a vulnerability in one of its older network-attached storage drives had caused a leak of 36TB of data, or over 3 million files, including significant amounts of financial information.
- Are your vendors as protected as you are?
 - Case study: Focus Brands Inc., a restaurant franchising group, reported a data breach in October 2019 due to a hacking of their point of sale (PoS) vendor.
- Reevaluate your company's data backup and disaster recovery plans, including how your IT team can physically access a server room without exposure to COVID.
- Consider transitioning to cloud storage.
- Ensure your cybersecurity program is sufficiently funded to work as intended and considered as part of budget planning.



A STRONG CYBERSECURITY PROGRAM: LESSONS LEARNED FROM RECENT DATA BREACHES AND ENFORCEMENT ACTIONS

Case Study: Anthem, Inc.

- 2014 data breach of healthcare insurance provider compromised the personal information (including names, addresses, and Social Security numbers) of 78.8 million customers.
- The company settled with a multi-state coalition for \$39.5 million in penalties and fees on September 30, 2020. The company also settled a class action for \$115 million on August 15, 2018.
- Anthem agreed to implement a comprehensive security program that incorporates principles of zero trust architecture, and to maintain a written response plan to prepare for and respond to security events.
- Anthem agreed to several specific security requirements, including logging and monitoring of the network, anti-virus maintenance, access controls and two-factor authentication, encryption, risk assessments, penetration testing, and employee training, among others.



A STRONG CYBERSECURITY PROGRAM: LESSONS LEARNED FROM RECENT DATA BREACHES AND ENFORCEMENT ACTIONS

Case Study: NotPetya

- NotPetya caused \$10 billion in damages, to banks, energy companies, government officials, and other companies, including a multinational advertising and PR firm.
- Examples:
 - Pharmaceutical company Merck suffered damages of roughly \$870 million.
 - FedEx's European subsidiary TNT Express suffered damages of roughly \$400 million.
 - Shipping company Maersk suffered damages of roughly \$300 million.
- At the time of attack some of Maersk's servers were still running a Windows operating system that was no longer supported.
- IT executives at Maersk pushed for a revamp that included network segmentation, and the changes were approved and budgeted. However, the success of the revamp was not made a performance indicator for the IT department, and it was never implemented.



A STRONG CYBERSECURITY PROGRAM: LESSONS LEARNED FROM RECENT DATA BREACHES AND ENFORCEMENT ACTIONS

Case Study: Bombas

- Bombas, a sock manufacturer, suffered a breach on September 27, 2014. Unauthorized intruders inserted software code designed to steal payment information and accessed names, addresses, and credit card information of almost 40,000 cardholders.
- Bombas did not notify consumers until May 2018.
- Settlement reached June 6, 2019, with the New York Attorney General:
 - \$65,000 in penalties.
 - Agreed to enhance employee training on compliance with New York's data breach notification law.



A STRONG CYBERSECURITY PROGRAM: LESSONS LEARNED FROM RECENT DATA BREACHES AND ENFORCEMENT ACTIONS


Case Study: Dunkin’

- Beginning in early 2015, hackers compromised tens of thousands of customers’ online accounts through “credential stuffing.” Dunkin’ took no action after a third-party app developer repeatedly alerted the company to the attacks.
- Settlement reached September 15, 2020, with the New York Attorney General:
 - \$650,000 in penalties
 - Dunkin’ remediated affected customers and agreed to maintain reasonable safeguards to protect against future credential stuffing attacks.



THE STOP HACKS AND IMPROVE ELECTRONIC DATA SECURITY ACT (SHIELD ACT)

- Applies to any business around the country that owns or licenses the private information of New York residents – not just New York businesses.
- Every company with employees in New York must comply with the SHIELD Act, at least with respect to its employees, because every employer has “private information” about its employees.
- Private information means:
 - A user name or email address in combination with a password or security question and answer that provides access to an online account or
 - Personal information (any information concerning a natural person that can be used to identify the person, i.e., name, number, personal mark, or other identifier) in combination with certain data elements



THE STOP HACKS AND IMPROVE ELECTRONIC DATA SECURITY ACT (SHIELD ACT) – continued

Breach Notification Provisions

- A “breach” now includes unauthorized access, rather than solely unauthorized acquisition or exfiltration of data
- In the event of a breach, the business must provide a notice to any resident of New York whose private information was accessed or acquired. The notice must be made “in the most expedient time possible” and include, among other things, the information believed to have been accessed or acquired

Reasonable Safeguards Provisions

- Administrative safeguards
- Technical safeguards
- Physical safeguards



OFFICE OF FOREIGN ASSETS CONTROL (OFAC)

- OFAC administers economic and trade sanctions. OFAC sanctions generally apply to U.S. persons (in some instances, to non-U.S. entities owned or controlled by a U.S. entity) and transactions cleared through the U.S. financial system.
- OFAC's October 1, 2020 advisory warned that because hackers may be on the "Specially Designated Nationals" (SDN) list, or have a sanctions nexus, companies that facilitate ransomware payments (such as banks, cyber insurance firms, and companies involved in incidence response) may risk violating sanctions laws.
- WannaCry ransomware attack in May 2017:
 - This attack infected approximately 300,000 computers in at least 150 countries and caused damages estimated at hundreds of millions, if not billions, of dollars to companies, hospitals, and government entities.
 - WannaCry was linked to a cybercriminal organization known as the Lazarus Group, which in turn was linked to North Korea. Lazarus Group and two of its subgroups were designated in September 2019.
- OFAC sanctions are a matter of strict liability.
- Full and timely cooperation is important.



RANGE OF PENALTIES FOLLOWING CYBERSECURITY ISSUES VARIES WIDELY

| | |
|---|---|
| SHIELD Act data breach notification provisions | \$5,000, or \$20 per failure to notify with a maximum penalty of \$250,000. |
| SHIELD Act reasonable safeguards provisions | \$5,000 per violation. |
| OFAC penalty | Penalties vary widely. So far, civil penalties settled by OFAC in 2020 have ranged from \$5,000 to \$7.8 million. |
| Settlements with Attorneys General or class actions | Settlements vary widely. The New York Attorney General settled with Bombas for \$65,000, and with Anthem (as part of a multi-state coalition) for \$39.5 million. |



CYBERSECURITY INSURANCE

Consider whether your policy covers:

- Forensic investigation costs
- Business interruption costs
- Crisis management expenses
- Costs of notifying clients
- Costs of PR firms and lawyers to address reputational and legal consequences
- Data restoration costs
- Cost of the ransom (in the event of a ransomware attack)
- Regulatory penalties

Red flags:

- Sub-limits
- Low limits
- Does not cover employees
- Does not cover fines
- Exclusions
- Does not cover prior acts



HOW CAN YOU PROTECT YOURSELF, YOUR EMPLOYEES AND YOUR CLIENTS

Wilk Auslander Advises Clients on Cybersecurity Risks and Legal Requirements

Design, draft, and implement key policies to prevent the risk of an attack and of a subsequent government enforcement action:

- Information security policy reasonably designed to protect personal information.
- Training guides for employees: ensure that employees know and can protect against the biggest risks.
- Incident response plan, covering all phases of cybersecurity preparedness and response.

IMPLEMENTING EFFICIENT AND SENSIBLE PREVENTION MEASURES DESIGNED TO MITIGATE YOUR CYBERSECURITY RISKS IS THE SINGLE MOST IMPORTANT STEP YOU CAN TAKE TO AVOID SUBSEQUENT LITIGATION AND ENFORCEMENT MEASURES. NOW IS THE TIME TO IMPLEMENT THOSE MEASURES WITH THE GUIDANCE OF APPROPRIATE COUNSEL.



HOW CAN YOU PROTECT YOURSELF, YOUR EMPLOYEES AND YOUR CLIENTS – continued

Wilk Auslander Advises Clients During and After Cyberattacks

“First Responder” in the event of an attack:

- Partner with cybersecurity forensic experts.
- In conjunction with the forensic experts, negotiate with the attacker and assist with paying any ransom.
- Partner with IT cybersecurity specialists to strengthen the company’s safeguards.
- Interface with law enforcement.
- Partner with PR professionals.

Post-crisis fallout:

- Advise on duty to notify customers.
- Serve as legal counsel in the event of litigation or investigation by state and federal enforcement.
- Implement the terms of any settlement.
- Work with each client to formulate and execute the right strategy.



4A'S PROFESSIONAL LIABILITY INSURANCE

- Basic Policy coverage includes:
 - Traditional media perils – defamation and copyright & trademark infringement
 - “All Risk” advertising services liability
 - Misstatements or errors in the content of an agency’s work
 - Claim mitigation expense
- Optional coverage:
 - Business operations of ad agency
 - Technology services errors & omissions liability
 - Cyber liability & cyber-claim expense reimbursement



4A'S PROFESSIONAL LIABILITY ENDORSEMENTS

- Data security and privacy – protects against:
 - Accidental release, theft or loss of damage to protected data
 - Transmitting/receiving malicious code via insured's computer system
 - Unauthorized access or use of computer system that results in denial or disruption of online services or computer systems
- Crisis management & computer system extortion:
 - Forensic investigation & legal expense reimbursement
 - Fraud response
- Technology services errors & omissions liability – covers claims from:
 - Computer system design, internet activities including ISP services, search engines or web portal services
 - Provision of electronic publishing or maintaining web-conferencing, web casting, online forums or b-boards, chat rooms, etc.
 - Website development, design, programming, website hosting, etc.



4A'S PROFESSIONAL LIABILITY ENDORSEMENTS

- Social engineering – protects against loss of money due to “Larceny by Trick”
- Ransomware attack & loss expense
- Regulatory action defense – coverage for alleged violations of national, state and local privacy laws & regulations
- Business interruption coverages
 - Pays loss of net profit and extra expense due to computer system or service disruption or failure caused by cyber attack
 - Public relations services to repair image, reputation, etc., following a covered claim
- Loss control services include:
 - Axis eRisk Hub
 - Panel counsel pre-vetted providers



FINAL NOTE

Remember that this presentation is not an exhaustive discussion, or a substitute for legal advice, and it may not be applicable to all situations. Contact an attorney for legal advice.

Natalie Shkolnik, Esq.

Partner at Wilk Auslander LLP

212-981-2294

nshkolnik@wilkauslander.com



SOURCES

- 1 Kroll: <https://www.infosecurity-magazine.com/news/ransomware-tops-2020-threat/>;
Positive Technologies: <https://www.techrepublic.com/article/ransomware-accounts-for-a-third-of-all-cyberattacks-against-organizations/>
- 2 Wikipedia: <https://commons.wikimedia.org/w/index.php?curid=60473519>
- 3 Kroll: <https://www.infosecurity-magazine.com/news/ransomware-tops-2020-threat/>
- 4 2020 SonicWall Cyber Threat Report:
<https://www.securitymagazine.com/articles/93769-ryuk-ransomware-responsible-for-one-third-of-all-ransomware-attacks-in-2020/>
- 5 FTC.gov
- 6 FBI.gov
- 7 196 A.3d 1036 (Pa. 2018)
- 8 278 F. Supp. 3d 739 (S.D.N.Y. 2017)
- 9 No. 16 Civ. 2372, 2016 WL 7336407 (D. Kan. Dec. 19, 2016)
- 10 Coveware: <https://www.coveware.com/blog/reduce-ransomware-risk-by-90-for-free-in-one-day>