# Focus On...

*Helping you bring your organization into focus.™*

September 2020 • Volume 10, Issue 9

# CYBER

## Cyber Risks Emerging from COVID-19—Part 3

**In the last two issues, Focus Audits brought you excerpts from RiskSpotlight's Deep-Dive report on the cyber risks emerging from COVID-19. Below, we continue with the third and final excerpt.**

***COVID-19 related cyber risk examples - Part 2***

- Cyber criminals gain access to bank's IT systems and issue fraudulent SWIFT instructions to transfer money to overseas bank accounts
- Cyber criminals targeting employees working remotely without adequate security protection on their devices, to steal information or use their devices to access their organization's network
- Increase in "Zoombombing" incidents which involved criminals exploiting the default settings on the popular video chat app Zoom, to breach and disrupt online meetings
- Fake sign-in pages for video conferencing software such as Zoom
- Cyber criminals providing mobile apps to track COVID-19 information. Downloading such apps on mobile phone infects the phone with malware and may share personal/sensitive information with criminals.
- Cyber criminals may breach mobile apps being deployed by governments globally for contact tracing
- Ransomware attacks against the financial services firms
- Cyber criminals threatening firms with a large scale DDoS attack if they do not pay a ransom
- Increase in "watering hole" cyber incidents which involve cyber criminal creating website containing coronavirus related information and infecting the website with malware that is downloaded to victims' IT system without their knowledge
- Cyber criminals setting fake websites to sell coronavirus related fake products such as testing kits and personal protection equipment (e.g. face masks, gloves)
- Cyber criminals promoting cures and treatments for coronavirus on social media. Clicking on such ads may download viruses or malware.

***Key COVID-19 related cyber risk trends***

- COVID-19 related uncertainties will stay at heightened level until an effective vaccine is found and deployed globally. Expert opinions on reaching such a milestone ranges from Mar 2021 to Jun 2022. Firms will need to identify the relevant COVID-19 related cyber risks and ensure adequate controls are implemented to manage these until we reach the milestone. Cyber criminals will continue to identify new vulnerabilities within humans behavior, processes and IT systems to exploit the COVID-19 related uncertainties. It is critical that firms implement adequate level of monitoring for existing

## Inside This Issue



***Focus Audits will be closed on Monday, September 7, 2020 in observance of Labor Day.***

FOCUS AUDITS™

# CYBER

and emerging cyber risks.

- Economic slowdown due to COVID-19 will result in rise in unemployment levels which may result in rise in number of individuals committing cyber crime particularly in countries with high number of technologically savvy citizens
- Cyber crime tools have become very cheap to purchase and execute resulting in rise in number of first-time criminals utilizing these for making easy money
- Firms are likely to increase adoption of working from home/remote working/distributed working practices compared to pre-crisis levels. This changes the cyber threat landscape for the firms and will require them to implement appropriate risk treatment measures.
- Firms are likely to increase adoption of cloud technologies to host their IT systems compared to the pre-crisis levels. This also changes the cyber threat landscape for the firms and will require them to implement appropriate risk treatment measures.
- Firms will face cost cutting pressures in response to weakening of economies globally due to COVID-19 related factors. Such pressures may force firms to reduce their investments in cyber risk controls during a period when the level of cyber risk exposure is expected to increase significantly.

***Key COVID-19 related cyber risk alerts and updates***

- (May 14, 2020) - A report by VMware highlights that from the beginning of Feb to end of Apr 2020, attacks targeting the financial sector have grown by 238%. Same report also highlights that ransomware attacks against the financial sector have increased by 9x from the beginning of Feb to end of Apr 2020 - Link
- (April 21, 2020) - UK's National Cyber Security Centre (NCSC) launched a new service to allow citizens to report suspicious emails amid wave of scams seeking to exploit the fear of COVID-19
- (April 8, 2020) - Joint guidance issued from UK's NCSC, US Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) on how to deal with COVID-19 related malicious cyber activity
- (March 27, 2020) - Europol issued a report titled "Pandemic profiteering: how criminals exploit the COVID-19 crisis". The report highlights how the criminals have used the crisis to carry out social engineering attacks, namely phishing emails through spam campaigns and more targeted attempts such as business email compromise
- (March 20, 2020) - FBI issued alert on rise in fraud schemes related to COVID-19. Covers phishing and fake emails
- (March 17, 2020) - UK's National Cyber Security Centre (NCSC) issued guidance to help organizations manage the cyber security challenges of increased home working
- (March 14, 2020) - Cyber security experts from Okta, Microsoft and Clearsky Cyber Security came together to form the COVID-19 Cyber Threat Intelligence (CTI) League. CTI league is an invitation-only group which aims to protect the world from cyber security threats during the pandemic. Since the groups formation, over 1,400 volunteers from 76 countries and 45 sectors have joined the CTI's ranks
- (March 2020) - Over 3,000 cyber expert volunteers from around the world formed the COVID-19 Cyber Threat Coalition to fight cyber attacks exploiting the COVID19 pandemic
- (March 6, 2020) - European Central Bank (ECB) urged the financial institutions to plan for the cyber risks related impacts of COVID-19 pandemic. ECB highlighted potential rise in cyber fraud attacks targeting both employees and customers in its letter
- (February 25, 2020) - The Australian Signals Directorate's Australian Cyber Security Centre (ACSC) issued information on DDoS threats against Australian organizations, primarily in the banking and finance sector
- (February 11, 2020) - World Health Organization (WHO) published an alert warning about cyber criminals exploiting the COVID-19 pandemic scenario by posing as WHO to launch phishing and malware attack
- (January 2020) - IBM X-Force discovered wave of COVID-19 related phishing scams targeting various regions in Japan to spread Emotet with intention of stealing financial information from victims

***Source: RiskSpotlight Deep-Dive, May/June 2020***


# CYBER

## Ransomware Red Flags: 7 Signs You're About to Get Hit

***Caught off guard by a ransomware attack? Security experts say the warning signs were there all along.***

It's every security pro's nightmare: Your company has been hit with ransomware, and every machine and server has been encrypted.

Shocked? Likely, but security experts say the warning signs were there all along. Misdirected DNS requests, bad VPN reboots, and Active Directory login failures should have been setting off alarms that a ransomware attack was in progress.

It doesn't have to be this way. According to Tarik Saleh, a senior security engineer and malware researcher at DomainTools, mitigation efforts begin with evaluating how vulnerable your company is to exploits. For example, are you leaving databases exposed on the public Internet?

And once attackers are in your network, you have anywhere from 48 hours to 12 days before they pull the trigger.

What key warning signs should you be on the lookout for as you develop a ransomware mitigation plan?

1. **Active Directory Will Show Multiple Login Failures**—Monitor Active Directory for login failures. For example, if you see three login failures in a row on RDP servers, that's a surefire sign the network has been attacked. The same holds for administrative login failures. Because companies didn't have time to prepare for COVID-19, and it looks like working from home will go on for the foreseeable future, it's time to develop a safe list of good IP addresses.
2. **Brute-Force Attacks Will Hit the Network**—Look for brute-force attacks on RDP systems. Once in the network, attackers typically look for additional passwords. You also need to watch for unusual file-copying activity, especially of .bat, .zip, .txt, and other common files. It's not common for one account to copy files to and from multiple user accounts or devices. Watch for the use of the Windows Backup Administration Tool wbadmin.exe to delete system backups.
3. **Phishing Emails Land With Strange Domains**—Watch for emails that come in with strange domain names that have never been in the company's environment .
4. **The Network Starts Making a String of Questions About a Single Machine**—Attackers typically start by gaining access to one machine, where they search for information and ask questions that everyday users wouldn't normally pose. Attackers will want to try to find out what else is on the network and what they can access.
5. **Security Tools Are Being Used in Environments They Weren't Assigned To**—Once attackers have admin rights, they will try to disable security software using applications created to assist with the forced removal of software, such as Process Hacker, IObit Uninstaller, GMER, and PC Hunter. These types of tools are legitimate, but if a specific tool is showing up on a system for which it's not assigned, then something is wrong.
6. **Unusual Time Stamps Appear on VPN Connections**—Be on the lookout for anomalous time stamps on VPN connections. If the organization has normal levels of traffic between 9 a.m. and 5 p.m. PT, and then all of a sudden there's traffic with IP addresses from Russia or Mozambique at 2 a.m., that should set off warning signs. You also need to figure out what attackers are trying to access. In addition, watch out for bad reboots on VPN concentrators.
7. **Traffic Is Suddenly Redirected to Questionable Places on the Dark Web**—Normal network traffic should never get redirected to a TOR site. The average user probably doesn't know what that is in the first place, let alone would have any business on a TOR network. Also watch out for unusual DNS requests. If the requests are heading back to known malware sites, that's potentially a problem and the network could get infected.

***Source:*** ***Steve Zurier, 08/28/2020***


# FINANCE

## Transition to Community Bank Leverage Ratio (CBLR) Framework

In response to the direction provided in the CARES Act, the federal regulatory agencies, on April 23, 2020, jointly issued an interim final rule providing revisions to the CBLR framework. The interim rule reduced the minimum leverage ratio for the CBLR. On August 21, 2020, the federal agencies issued a new final rule ("2020 final rule") related to the CBLR effective October 1, 2020.

The previous final rule on the CBLR issued in November of 2019 established a 9.0% minimum leverage ratio for qualifying community banking organization ("Banks or Bank") in 2020 to be considered well capitalized. In addition, the 2019 final rule established a two-quarter grace period for Banks that temporarily fall below the minimum requirement. In response to the CARES Act, the minimum Leverage Ratio for the CBLR was reduced from 9.0% to 8.0% in April of 2020.

Under the 2020 final rule, Banks must have a leverage ratio equal to or greater than 8.0% beginning in the second quarter of calendar year 2020. Subsequently, Banks must have a leverage ratio greater than 8.5% through calendar year 2021 and greater than 9.0% thereafter. The 2020 final rule also includes the two-quarter grace period for Banks that temporarily fail to meet any of the qualifying criteria, providing that Banks will generally still be deemed well capitalized during the grace period so long as the Banks maintain a leverage ratio within 1.0% below the minimum leverage ratio.

The final rule does not make any changes to the other qualifying criteria in the community bank leverage ratio framework.

The agencies are maintaining the 2019 final rule's requirement that the grace period will begin as of the end of the calendar quarter in which the Bank ceases to satisfy any of the qualifying criteria (so long as the Banks maintain a minimum leverage ratio required for the applicable grace period) and will end after two consecutive calendar quarters. For example, if an electing Bank, which had met all qualifying criteria as of March 31, 2020, no longer met one of the qualifying criteria as of May 15, 2020, and still had not met the criteria as of the end of that quarter, the grace period for the Bank would have begun as of the end of the quarter ending June 30, 2020 and could continue through the quarter ending September 30,2020. The Bank would need to comply fully with the CBLR for the quarter ending December 31, 2020. In the event that the grace period extends into a period where the higher minimum leverage ratios are required, the Bank would be subject to the higher minimum requirements for the applicable period.

| Calendar Year | CBLR Leverage Ratio Requirement | Minimum Leverage Ratio During Grace Period |
|---|---|---|
| 2020 | 8.0% | 7.0% |
| 2021 | 8.5% | 7.5% |
| 2022 | 9.0% | 8.0% |


# COMPLIANCE

## Joint Statement on Enforcement of BSA/AML Requirements

On August 14, the federal banking agencies issued a Joint Statement on Enforcement of Bank Secrecy Act/Anti-Money Laundering Requirements updating their existing enforcement guidance to enhance transparency regarding how they evaluate enforcement actions that are required by statute when financial institutions fail to meet Bank Secrecy Act/Anti-Money Laundering obligations. The statement focused particularly on compliance provisions of the Federal Deposit Insurance Act (FDIA) and Federal Credit Union Act (FCUA).

The statement addresses how the agencies evaluate violations of individual components or "pillars" of the BSA/AML compliance program. Under the FDIA and FCUA, the Agencies are directed to implement rules regarding and examine institutions' compliance with BSA/AML requirements, which includes having a program which (1) is reasonably designed to assure and monitor the institution's compliance with the requirements of the BSA and its implementing regulations and (2) have, at a minimum, the following components or pillars:

- A system of internal controls to ensure ongoing compliance with the BSA
- Independent testing for BSA/AML compliance
- A designated individual or individuals responsible for coordinating and monitoring BSA/AML compliance
- Training for appropriate personnel
- A Customer Identification Program with risk-based procedures that enable the institution to form a reasonable belief that it knows the true identity of its customers

The institution must also have risk-based procedures for ongoing customer monitoring.

The Agencies will issue a cease and desist order for the following failures:

1. Failure to establish and maintain a reasonably designed BSA/AML Compliance program, taking into account risks posed by the business and changes to operations.

2. Failure to correct a previously reported problem with the BSA/AML Compliance program.

However, an Agency will not typically issue a cease and desist order for failure to correct a BSA/AML compliance program problem unless the problems subsequently found by the Agency are substantially the same as those previously reported to the institution. For problems which require a significant amount of time to remediate, the Agencies may not issue an order if the institution has made significant progress since the previous finding.

The Agencies may also take other formal or informal actions for failures such as a violation of SAR regulations, record keeping or other reporting requirements.

This Statement is an example of regulatory bodies' increasing focus on the design and effectiveness of controls to mitigate actual risks within an institution's business, and the expectation that institutions will continuously test, update and improve their controls. The Statement provides specific categories and examples of BSA/AML program failures that typically would (or would not) result in a cease and desist order.


# AWARENESS

## Online Security for Kids

**Background**
Kids' lives are online more than ever, from socializing with friends and interacting with family to online learning and education. As parents we want to make sure they do so in a safe and secure manner. However, this is hard as many of us never grew up in such an online environment like this. Below we cover key steps on how you can help kids make the most of online technology safely and securely.

**Education / Communication**
First and foremost, make sure that you foster good open communication with your children. Far too often parents get caught up in the technology required to block content or what mobile apps are good or bad. No parental control technology is perfect, and some have privacy concerns due to the data they collect. Ultimately this is not a technology problem but a behavior and values problem. Teach your kids to behave online as you would in the real world. A good place to start is to create a list of expectations with your kids. Here are some to consider (these rules should evolve as kids get older):

- Times when they can or cannot go online and for how long.
- Types of websites and/or games they can access and why they are or are not appropriate.

- What information they can share and with whom. Children often do not realize what they post is permanent and public, or that their friends may share their secret with the world.
- Who they should report problems to, such as strange pop-ups, scary websites, or if someone online is being creepy or a bully.
- Treat others online as they would want to be treated themselves.
- People online may not be who they claim to be, and not all information is accurate or truthful.
- What can be purchased online and by whom, to include in-game purchases.

Consider tying these rules to their academic grades, completion of chores, or how they treat others. Once you decide on the rules, post them in the house. Even better, have them review and sign the document; that way, everyone is in full agreement. The earlier you start talking to your kids about your expectations, the better.

Not sure how to start the conversation? Ask them what apps they are using and how they work. Put your child in the role of teacher and have them show you what they are doing online. Keeping communication open and active is the best way to help kids stay safe in today's digital world.

For mobile devices, consider a central charging station somewhere in your house. Before your children go to bed at night, have all mobile devices placed at the charging station, so your children are not tempted to use them when they should be sleeping.

**Security Technologies and Parental Controls**
There are security technologies and parental controls you can use to monitor and help protect your kids. They typically provide capabilities to enforce usage limits or hours as well as content protections. These solutions tend to work best for younger children. Older kids not only need more access to the Internet but often use devices that you do not control or cannot monitor, such as those issued by school, gaming consoles, or devices at a friend's or relative's house. This is why communicating with your kids about your expectations and the dangers that exist on the internet is so important.

**Leading by Example**
Set a good example as parents or guardians. When your kids talk to you, put your own digital device down and look them in the eye. Consider not using digital devices at the dinner table and never text while driving. Finally, when kids make mistakes, treat each one as an experience to learn from instead of engaging in an immediate disciplinary action. Make sure they feel comfortable approaching you when they experience anything uncomfortable online or realize they themselves have done something wrong.

***Source: Chris Pizor, Principal SANS Instructor, Curriculum Lead for USAF cyber training***
***SANS Security Awareness***



Focus Audits, LLC
11301 N. US Hwy. 301
Ste. 105
Thonotosassa, FL 33592
(813) 638-8565
www.FocusAudits.com