Focus On...

Helping you bring your organization into focus.™

July 2020 • Volume 10, Issue 7

CYBER

Cyber Risks Emerging from COVID-19

Over the next several issues, Focus Audits will bring you excerpts from RiskSpotlight's Deep-Dive report on the cyber risks emerging from COVID-19. Be sure to look out for our monthly newsletter emails to read the full report!

Why COVID-19 provides an ideal environment for cyber criminals?

- Many people are experiencing a global scale pandemic and disruption to society/ economic activity for the first time resulting in significantly high level of uncertainties in their professional and personal contexts.
- Many governments globally have announced large scale financial support programs to help organizations and individuals affected by the COVID -19 pandemic. The design and implementation of these programs were fast-tracked resulting in movement of significantly large amount of funds within the financial system in a short period of time. This provides cyber criminals with once in a lifetime opportunity particularly when the level of oversight and due diligence is weaker than normal.
- Many people are working from home for the first time and hence may not be fully aware of potential cyber threats related to working remotely.
- Many organizations had to quickly react to government lockdown decisions and hence may not have had adequate time to adjust their processes, systems and controls to protect against cyber threats associated with large scale remote working.
- Many people are worried about the safety of their family and themselves. This has created high level of fear and uncertainties that may result in irrational behaviors. Many people are also actively browsing the internet for information about COVID-19 and protection measures exposing them to cyber threats.
- Many people are also receiving communications from certain organizations for the first time (e.g., WHO, local governments, government health departments, local hospitals). This provides cyber criminals with opportunities to impersonate these organizations for their phishing campaigns.
- Many people solely relying on digital channels (e.g., emails, Zoom calls, WhatsApp) for communication with family, friends and work colleagues due to government lockdowns thus increasing the likelihood of coming across malicious websites, links and messages.
- Many people have been forced to use digital channels for their daily activities for the first time (e.g., online shopping) and hence may not be fully aware with common cyber frauds.
- Excessive amount of COVID-19 information in the media making it very difficult to separate genuine information from malicious information laced with cyber threats.

Inside This Issue

FOCUS AUDITS™

CYBER

Key COVID-19 related cyber risk statistics - Part 1

- In May 2020, Barracuda Networks global survey (Link) reported that:
  - 41% of respondents have cut cybersecurity budgets due to COVID-19 related financial pressures
  - 46% of respondents have encountered at least one cyber security incident since shifting to a remote working model during the COVID-19 crisis
  - 49% of respondents said they expect to see a data breach or cyber security incident in the next month due to remote working
  - 51% of respondents said their workforce is not proficient or properly trained in the cyber risks associated with remote working
  - 56% of respondents plan to continue widespread remote working even after the COVID-19 crisis is over
- In May 2020, Action Fraud (UK) reported that 2,057 victims have lost over $5.7M to coronavirus-related scams. They have received 11,206 reports of coronavirus-related phishing emails - Link
- In May 2020, Kaspersky published a report on analysis of DDoS attacks in Q1-2020. The report highlighted that there was a 80% increase in number of attacks in Q1-2020 vs. Q1-2019 - Link
- In May 2020, Kaspersky survey (Link) highlighted the following:
  - 73% of employees have not received any IT security awareness training from their employers since they transitioned to working from home due to COVID-19
  - 68% of respondents are using personal devices to work from home
  - 50% of companies that allow employees to work using personal devices do not have policies in place to regulate how these devices are used
- In May 2020, cyber security company Darktrace reported that UK home workers experienced 60% increase in malicious email traffic in six weeks since UK's lockdown began in March - Link
- In May 2020, Singapore police reported a total of 151 phishing scams between April 7, 2020 and May 7, 2020, up from a monthly average of 20 in the first three months of this year - Link
- In May 2020, Mimecast published a report (Link) highlighting cyber risk trends over the first 100 days of the pandemic:
  - Increase of 35.16% in malware detections
  - Increase of 55.8% in blocking of URL clicks
  - Increase of 26.3% in scam detections
  - Increase of 30.3% in impersonation detections
  - Over 60,000 COVID-19 related malicious domains were registered

Source: RiskSpotlight Deep-Dive, May/June 2020

FINANCE

"Flying Blind Into a Credit Storm"

This headline from the Wall Street Journal (WSJ) article on June 29th reflects the concern by financial institutions about the distressed credit conditions in the U.S. economy. Many lenders have pulled back sharply on lending to U.S. consumers and businesses during the coronavirus crisis. One reason cited is that they can't tell who is creditworthy. Millions of Americans are out of work and behind on their loans. But, in many cases, the missed payments aren't reflected in their credit scores, nor are they uniformly recorded on borrowers' credit reports.

The confusion stems from a provision in the government's coronavirus stimulus package. The law doesn't allow lenders to report borrowers that chose to defer debt payments as past due to credit-reporting companies. For the three months ended May 31, 2020, Americans deferred debt payments on more than 100 million accounts, according to TransUnion. This sign of widespread financial distress has lenders guessing about all of the debt held by American households.

The Federal Reserve reported that the biggest U.S. banks could be saddled with as much as $700 billion in loan losses in a prolonged downturn. "Without accurate information, their only option is to pull back on credit," said Michael Abbott of consulting firm Accenture PLC. "Banks don't know who is going to pay and who isn't. It's like flying blind into a credit storm."

Banks started tightening their underwriting standards in March, when the first wave of coronavirus layoffs began. By early April, banks reported an increase in minimum credit-score requirements for credit card applications and tighter lending standards for all consumer-loan categories. Loan originations have fallen sharply, a result both of the tightening and a decline in consumer demand.

Pre-pandemic, deferrals were used rarely for most types of consumer debt and were usually confined to areas hit by natural disaster. Now, a staggering number of consumers around the U.S. are in deferral, leading lenders to question credit scores and if a borrower in deferment has fallen on tough times or is simply taking advantage of debt relief options.

Lenders are looking for additional data that will help them figure out which applicants are a safe bet and who's likely to run into financial trouble. Some are considering such things as the use of cellphone data that show unemployment office visits or the review of cash flow in deposit accounts to better assess risks to their borrowers.

The major credit-reporting companies have been in discussions with lenders about additional data sets that could help identify hidden risks. The conversations involve innovations to pinpoint applicants who fall short of lenders' credit-score cutoffs but are likely to pay back their loans.

TransUnion officials reported that the coronavirus has "thrown existing models off". Considering the potential for regulatory compliance issues and increased model risk, lenders should be hesitant and careful using these new credit reporting innovations, particularly when used to deny credit to applicants.

Source: ***WSJ / June 29, 2020***

COMPLIANCE

CFPB Issues Interim Final Rule Regarding Loss Mitigation Options for Homeowners Impacted by COVID-19

The Consumer Financial Protection Bureau (CFPB or Bureau) issued an interim final rule (IFR) on June 23, 2020 that temporarily permits mortgage servicers to offer to borrowers impacted by the coronavirus (COVID-19) pandemic certain loss mitigation options based on the evaluation of an incomplete loss mitigation application.

The Coronavirus Aid, Relief, and Economic Security Act (CARES Act) provides forbearance relief for consumers with federally backed mortgage loans, but the statute does not specify how borrowers receiving CARES Act forbearances must repay the forborne payments. This omission creates uncertainty for stakeholders as to how borrowers must repay these amounts when CARES Act forbearances expire. As many initial forbearance periods were set at 90 days earlier this spring, many of the forbearances will expire in June or July 2020.

The mortgage industry has developed different options for borrowers to repay the payments that were forborne under the CARES Act. For example, the Federal Housing Finance Agency (FHFA), Fannie Mae, and Freddie Mac may permit some borrowers to defer repayment of the forborne amounts until the end of the mortgage loan. The Federal Housing Administration (FHA) has a similar program. These programs require the servicer to collect only minimal information from the borrower before offering the option.

Summary of the Interim Final Rule
The IFR makes it clear that servicers do not violate Regulation X by offering certain COVID-19-related loss mitigation options based on an evaluation of limited application information collected from the borrower. Normally, with certain exceptions, Regulation X would require servicers to collect a complete loss mitigation application before making an offer. Due to the particular needs of mortgage servicers and borrowers during the COVID-19 pandemic, the Bureau is amending Regulation X to temporarily permit mortgage servicers to offer certain loss mitigation options without obtaining a complete loss mitigation application. Servicers may offer eligible loss mitigation options to a borrower experiencing a financial hardship due, directly or indirectly, to COVID-19 and who has received a payment forbearance program, including one offered pursuant to Section 4022 of the CARES Act, or who has had other principal and interest payments that are due and unpaid as a result of a financial hardship due, directly or indirectly, to COVID-19.

The CFPB's amendment conditions eligibility for the new exception on the loss mitigation option satisfying three criteria.

First, the loss mitigation option must permit the borrower to delay paying certain amounts until the mortgage loan is refinanced, the mortgaged property is sold, the term of the mortgage loan ends, or, for a mortgage insured by FHA, the mortgage insurance terminates. These amounts include, without limitation, all principal and interest payments forborne under a qualifying COVID-19-related payment forbearance program. These amounts also include without limitation all other principal and interest payments that are due and unpaid by a borrower experiencing financial hardship due, directly or indirectly, to COVID-19. For purposes of this criterion, the term of the mortgage loan means the term of the mortgage loan according to the obligation between the parties in effect when the borrower is offered the loss mitigation option.

Second, any amounts that the borrower may delay paying through the loss mitigation option do not accrue interest; the servicer does not charge any fee in connection with the loss mitigation option; and the servicer waives all existing late charges, penalties, stop payment fees, or similar charges promptly upon the borrower's acceptance of the loss mitigation option.

Third, the borrower's acceptance of the loss mitigation offer must resolve any prior delinquency. The Bureau states that these criteria provide important protections for borrowers and are intended to align with the COVID-19 payment deferral option announced by FHFA and other similar programs, including FHA's COVID-19 standalone partial claim.

The IFR also provides servicers relief from certain requirements under Regulation X that normally would apply after a borrower submits an incomplete loss mitigation application. Once the borrower accepts an offer for an eligible program under the IFR, the servicer need not exercise reasonable diligence to obtain a complete application and need not provide the acknowledgment notice that is generally required under Regulation X when a borrower submits a loss mitigation application.

The IFR is effective on July 1, 2020, and comments must be received within 45 days after publication in the Federal Register.

Source: ***Lexology.com***

AWARENESS

What is Ransomware?

Ransomware is a type of malicious software (malware) that is designed to hold your files or computer hostage, demanding payment for you to regain access. Ransomware has become very common because it is so profitable for criminals.

Like most malware, ransomware starts by infecting your computer, most often when you open an infected attachment or click on a malicious link in a phishing email. Once ransomware infects your computer, it encrypts files on your hard drive – possibly even your entire hard drive – or anything else connected to your computer, so you can no longer access your files. It then informs you that the only way you can recover your files is to pay the cybercriminal a ransom (thus the name ransomware). Sometimes, the criminals also threaten to release your files publicly if you don't pay the ransom. The criminals may demand payment in the form of untraceable digital currency, such as Bitcoin. If you pay the ransom, the criminals might give you access to your files, but there are no guarantees. Sometimes they will even take your money and still leave your computer infected without you knowing it or keep asking for more money.

Protect Against the Infection

You can protect your computer against a ransomware infection the same way you protect it against other forms of malware. Here are three key steps:

Update Your Systems and Software: Cyber criminals often infect computers or devices by taking advantage of unfixed bugs (known as vulnerabilities) in your software. The more current your software is, the fewer known vulnerabilities it has, and the harder it is for cyber criminals to infect them. Therefore, make sure your operating systems, applications, and devices have automatic updating enabled.

Enable Anti-Virus: Use up-to-date anti-virus software from a trusted vendor. Such tools are designed to detect and stop malware. However, anti-virus cannot block or remove all malicious programs, and usually it cannot recover your files after a ransomware infection. Cyber criminals are constantly innovating, developing new and more sophisticated infection tactics that can evade detection. In turn, anti-virus vendors are constantly updating their products with new capabilities to detect malware. In many ways it has become an arms race, with both sides attempting to outwit the other.

Be Vigilant: Cyber criminals often trick people into installing ransomware and other forms of malicious software through phishing email attacks. For example, a cybercriminal might send you an email that looks legitimate and contains an attachment or a link. Perhaps the email appears to come from your bank or a friend. However, if you open the attached file or click the link, you could activate malicious code that infects your computer. If a message creates a strong sense of urgency or seems too good to be true, it could be an attack. Be vigilant – cyber attackers play on your emotions. — Common sense is often your best defense.

Back Up Your Files Before the Infection

Since it's impractical to assume that you'll always be able to prevent an infection, your best defense against ransomware is backups. If you have a backup of your important documents and other files, you have the option of recovering from backup instead of paying the ransom. It's important that you use some type of automated backup that regularly backs up all your files and that you test your restore procedures to make sure you can recover them if the need arises. There are numerous simple Cloud and local backup solutions that you can install on your computer that will securely and regularly back up all your files for you.

Source: Lenny Zeltser, CISO at Axonius , Guest Editor
SANS Security Awareness

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