Focus On...

Helping you bring your organization into focus.™

August 2020 • Volume 10, Issue 8

CYBER

Cyber Risks Emerging from COVID-19—Part 2

Last month, Focus Audits brought you the first part of this series, which included excerpts from RiskSpotlight's Deep-Dive report on the cyber risks emerging from COVID-19. Below, we continue with Part 2.

Key COVID-19 related cyber risk statistics - Part 2

- In Apr 2020, Palo Alto Networks Threat Intelligence Team released research highlighting: -
  - ◊ 116,357 coronavirus-related new domains were registered between Jan and Mar 2020 (around 1,300 per day). Of these 2,022 were identified to be malicious and 40,261 were identified to be "high-risk"
  - ◊ 656% rise in average daily number of malicious COVID-19 themed domains from Feb to Mar 2020
- In Apr 2020, Australian Cyber Security Centre (ACSC) published a cyber threat report revealing:-
  - ◊ It disrupted over 150 malicious COVID-19 related websites in collaboration with Google, Microsoft and Australian telecommunication services providers over a period of one month starting from 10Mar2020
  - ◊ It also received more than 95 reports about Australians targeted by scams and online frauds to steal their money or personal details during the same period
- In Apr 2020, Google reported that it blocked 18 million COVID-19 related phishing emails per day in second week of Apr 2020. This was in addition to the 240 million COVID-19 themed spam messages sent to Gmail accounts everyday
- In Apr 2020, VMware Carbon Black revealed their analysis of cyber risk trends amid COVID-19 highlighting:
  - ◊ Increase in cyber attacks targeting financial institutions by 38% between Feb 2020 and Mar 2020
  - ◊ Increase in COVID-19 related ransomware attacks by 148% from their baseline levels in Feb 2020
  - ◊ 52% of all cyber attacks recorded were financial related attacks
- In Apr 2020, ISACA survey highlighted that only 51% of technology professionals and leaders are highly confident that their cybersecurity teams are ready to detect and respond to rising cybersecurity attacks during COVID-19. Only 59% respondents said their cybersecurity team has the necessary tools and resources at home to perform their job effectively
- In Mar 2020, Barracuda Networks reported that phishing emails have spiked by 667% in Mar 2020 compared to Feb 2020. Of the COVID-19 phishing attacks, 54% were classified as scams, 34% as brand impersonation attacks, 11% blackmail and 1% as business email compromise

Inside This Issue

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

FOCUS AUDITS™

CYBER

COVID-19 related cyber risk examples - Part 1

- Employees receiving phishing emails telling them that they could choose to be furloughed by signing in to a certain website
- Employees receiving phishing emails with instructions to click on a link to add benefit payments to their next payroll
- Employees receiving phishing emails from government department or employer seeking personal information for registration to benefit payment program
- Employees receiving phishing emails from their IT department with instructions and link to download new software
- Employees receiving phishing emails to reset virtual private network (VPN) accounts
- Employees receiving fake reports on fellow colleagues infected with COVID-19 asking victims to enter their credentials to see the details in the report
- Employees receiving phishing emails from company chief executive requesting them to donate to a health charity
- Cyber criminals using trusted brand names like World Health Organization (WHO) or US Centers for Disease Control and Prevention (CDC) to send COVID-19 themed emails in order to get victims to click on malicious links or attachments
- Cyber criminals impersonating emails that are generated by file sharing sites such as OneDrive or SharePoint. The links in these emails directs the victims to a phishing site.
- Finance team members receiving phishing emails containing information relating to tax rebates or COVID-19 related financial grant by the government
- Finance team members targeted with Business Email Compromise (BEC) fraud
- Banks receiving request by cyber criminals, impersonating as clients, to change recipient account details for certain payments due to regular bank accounts becoming inaccessible due to COVID-19 related factors
- Cyber criminals hacking supplier email-ids and misleading firms to change payment instructions for due invoices

Source: RiskSpotlight Deep-Dive, May/June 2020

Cyber Security and Cyber Resilience, The Difference

What's the difference between cyber security and cyber resilience – and why does resilience matter?

Cyber security – keeping them out
Cyber security is a series of measures focused on preventing hackers penetrating your IT systems. While implementing basic cyber security best practice will prevent the great majority of attacks, even with your defenses are up, hackers can find holes when the landscape changes.

Cyber resilience – responding when they get in
If we work based on "not if, but when" with a cyber-attack, the importance of cyber resilience comes into play.

Definitions tend to describe a cyber resilient organization as one that will be able to respond and recover from a cyber-attack, keep operating through it (very important) and eventually get back on track and be more capable of withstanding future disruption. Cyber resilience also involves things like business continuity management.

One of the reasons for the emergence of 'cyber resilience' lies with the realistic view that for all the defenses an organization might have in place, there is still a likelihood that they'll suffer an attack.

However, what makes cyber resilience so mission critical **is the ability to remain operational during such an event.**

But is the distinction that simple?

CYBER

Is cyber security a stand-alone process with cyber resilience following (as if they are two separate things), or does cyber resilience include cyber security? Opinions differ. If you research coverage of the link between the topics, you'll mainly find a linear relationship. Many articles start by discussing cyber security, and then move on to cyber resilience.

The World Economic Forum, in their post "Cyber resilience: everything you need to know" talk about cyber security as 'binary' – 'either something is secure or it isn't'. They also say that there is a difference between the access control of cyber security and the more strategic, long-term thinking that cyber resilience should evoke.

However, if we look at the US National Institute for Standards and Technology (NIST) Cyber Security Framework, an internationally recognized and respected framework of activities, outcomes and references that detail approaches to aspects of cyber security, cyber resilience covers five stages – **Identify, Protect, Detect, Respond and Recover.**

The **"Identify"** stage is described as to **"Develop the organizational understanding to manage cyber security risk to systems, assets, data, and capabilities."** So, in the NIST context, cyber security is a stage of the wider process of cyber resilience.

Cyber resilience is a broader process which includes cyber security. Both terms start with 'cyber' but, in terms of scope, cyber resilience would seem to **exceed** cyber-security.

So**, why does cyber resilience matter?**

A severe cyber-attack can have consequences in terms of delivery of services should systems be put out of operation. If your organization is part of critical national infrastructure, the impact of a security breach could be big.

Steps towards cyber resilience
So, how do you get there? Your cyber security resilience activities will almost certainly encompass one or more standards, schemes or models with which you need to be certified or comply.

The comprehensive path to cyber resilience comes through a cyber-security program ***which includes an assessment of your existing resilience.*** We also look at your security governance, policies, standards, processes and procedures, and appropriate levels of awareness training for staff and users.

We use well established cyber risk management principles guided by widely accepted best practice to help you design and implement your program. This includes the NIST Cyber Security Framework, SANS Critical Security Controls and the Cybersecurity Resilience Review.

Cybersecurity	Cyber Resilience
Definition: procedures followed, or measures taken to ensure the safety of a state or organization	Definition: the capacity to recover quickly from difficulties; toughness
Technologies and processes designed to protect an organization from cybercrime	Technologies and processes designed to keep delivering intended services in spite of cyber incidents
Works to reduce the risk of cyber attacks and to protect the organization from cyber theft/espionage	Works to ensure continuity on a wider scope, comprising cybersecurity and business requirements
Can work effectively without compromising the usability of other systems	Requires organization-wide culture shift the normalizes and embeds security best practices
Includes a business plan to resume operations in the event of a successful attack	Requires the organization to become agile and adaptable in the face of cyber-attacks and incidents

FINANCE

Examiner Guidance For Assessing Safety and Soundness

On June 23, 2020, the federal agencies jointly issued "Interagency Examiner Guidance for Assessing Safety and Soundness Considering the Effect of the COVID-19 Pandemic on Institutions." While the agencies will continue to evaluate financial institutions under the appropriate rating system, such as CAMELS, examiners will also assess management's responsiveness to the COVID-19 impact and distinctive stresses resulting from the pandemic. The following are highlights and interpretations from the concise 11-page document.

Effectiveness of Institution's Assessment of Risk
Examiners are expected to evaluate management's assessment of risks including any additional risks and exposures related to the effects of the pandemic. Most notably, examiners will review management's assessment of credit risk and asset quality estimates. The institution's risk assessments should also include the pandemic's effects on the institution's earnings prospects, capital adequacy, funding, liquidity, operations, and sensitivity to market risk. Examiners will determine whether an institution's assessments of risk are sufficient in scope and content, given the localized impact of the pandemic. From a regulatory viewpoint, the quality and documentation of enterprise risk assessments have never been more important.

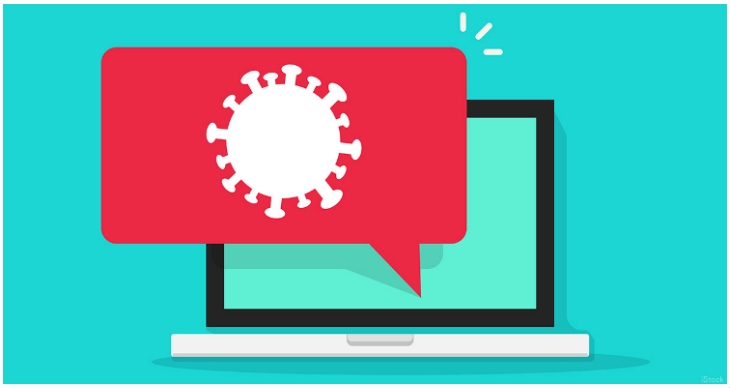
Asset Quality
It should be no surprise that asset quality is a major area of focus for current examinations. The severe hit to the economy and massive wave of dislocated workers absolutely increased the degree of credit risk in the operating environment. Government stimulus programs and assistance from lenders and landlords helped cushion the blow but may have only delayed the real default rate from this credit crisis. Many lenders continue to be "flying blind in a credit storm." Financial institution management teams are very much aware of the rising credit risks but have been hesitant or unable to take mitigating actions with their borrowers. Big banks have confirmed this situation by announcing much larger than normal loan loss provisions.

Examination scopes will be adjusted with respect to the most significantly affected portfolios. Examiners will be looking to see if management has been able to identify substantially affected credits and any additional loss exposures through an objective assessment of credit risk both internally and through the independent loan review process.

Examiners will be considering underlying credit risk attributes such as a) the classification of credits, b) credit risk review process, c) new loan origination standards, d) loan modifications and payment deferrals, e) non-accrual loans, f) the ALLL analysis, and g) real estate valuations.

Management
Examiners will be expected to evaluate the reasonableness and effectiveness of management's response to the pandemic. Areas of specific focus include a) operational risks, b) the quality of ongoing independent risk management and audit activities, c) the impact on earnings, d) liquidity management, and e) changes in the institution's interest rate risk profile.

Focus Audits offers clients a full range of enterprise level and specific risk management services.



COMPLIANCE

US Banking and Consumer Regulators Ramping Up LIBOR Transition Focus

On July 1, 2020, the Federal Financial Institutions Examination Council (FFIEC) issued a statement highlighting the financial, legal, operational and consumer protection risks that financial institutions will need to address as they prepare to transition away from LIBOR. The discontinuation of LIBOR will affect nearly every financial institution, though larger institutions and those engaged materially in capital markets activities will face a more substantial impact.

According to the FFIEC's statement, institutions should first identify risks in their own on- and off-balance sheet assets and contracts that reference LIBOR, including derivatives, commercial and retail loans, investment securities and securitizations, including but not limited to consumer protection-related risks.

Following an identification of key risks and dependencies, institutions should quantify their LIBOR exposure. This quantification should also include an assessment of the viability of existing contract fallback language. For contracts with inadequate fallback language, institutions need to develop a remediation strategy. To limit additional exposure, institutions should also discontinue the origination or purchase of LIBOR-indexed instruments.

In planning for the transition, institutions should consider the various legal, operational and other risks associated with various consumer financial products that reference LIBOR. Any replacement rate not already included in fallback language may impact consumers, increase reputation risk and result in legal exposure to institutions and the financial industry. Transition plans should, among other things, identify affected consumer loan contracts, highlight necessary risk mitigation efforts and address development of clear and timely consumer disclosures regarding changes in terms.

While there is a recognition that the supervisory focus itself will depend on the size and complexity of each institution's LIBOR exposures, examiners expect all institutions to have transition plans and risk management processes in place.

Financial institutions of all kinds need to take recent statements by regulators seriously. Indeed, many financial institutions have already designed transition-related infrastructure and formulated plans. But having plans is not the same as actually executing them. There needs to be a full understanding of how to properly mitigate the various legal and other risks that arise from such tasks as executing contract amendments, communicating with customers and counterparties and responding to inquiries from regulators.

***Source:** Shearman & Sterling*

AWARENESS

Virtual Conferencing Safely and Securely

What is Virtual Conferencing?
With so many of us now working from home, you are most likely finding yourself remotely connecting with your co-workers using virtual conferencing solutions like Zoom, Slack, or Microsoft Teams. Your family members - perhaps even your children – may also be using these same technologies to connect with friends or for remote learning. Regardless of why you are connecting, here are key steps you can take to make the most of these technologies safely and securely.

Attending a Virtual Conference
If you will be attending a virtual conference, here are five key steps.

1. **Update the Software:** Make sure you are always using the latest version of the conferencing software. The more recent and updated your software, the more secure you will be. Enable automatic updating and quit your program when done, so it can check for the latest updates the next time you restart.
2. **Configure Audio / Video Settings:** Set your preferences to mute your microphone and turn off your video when joining a meeting and enable them only when you want. Consider placing a webcam cover or tape over your computer's camera to ensure privacy when you're not actively broadcasting. Remember: if your camera is on, everyone can see what you are doing even when you are not talking.

3. **Double-Check What's Behind You:** If you want to enable your webcam, be aware of what's behind you. Ensure you do not have any personal or sensitive information visible behind you during a call. Some video conferencing software lets you blur or use a virtual background, so people cannot see what is behind you.
4. **Don't Share Your Invite:** The invite link is your personal ticket to enter the meeting. Even if a trusted co-worker needs the link, it's much better they ask the conference organizer for their own invite.
5. **Do Not Record:** Do not take screenshots of or record the conference call without permission. You could accidentally share very sensitive information if those screenshots or recordings become public.

Hosting a Virtual Conference
If you will be hosting a virtual conference, here are some additional steps you should take.

1. **Require a Password:** To protect the privacy and security of your conference and control who can join, protect your meeting with a password. This way only people who have the conference password can join the event.
2. **Review Attendees:** Review the people attending your event. If there is someone you do not know or cannot identify, have that person confirm their identity. If you have any concerns, or if someone is being rude or disruptive, remove them from the conference. Many solutions offer the option to lock the conference once it has begun, so no one else can join unless you let them in. Another option may be to initially place people in a virtual waiting room, so you can approve who joins the call.
3. **Inform if Recording:** If you intend to record the event (and have permission to record), be sure to inform everyone on the conference ahead of time.
4. **Sharing Your Screen:** If you will be sharing your computer screen at any point, be sure to first close all other applications and remove any sensitive files from your computer's desktop. Also disable any pop-up notifications. This helps ensure you don't accidently share sensitive or embarrassing information while sharing your computer screen. Another option is to consider sharing just the program you want to show instead of sharing your entire computer screen.

These technologies are a fantastic tool and, in many ways, represent the future of how we will work, collaborate, and communicate with others. These simple steps will go a long way to ensure you safely and securely make the most of them.

Source: Lodrina Cherne, Principal Security Advocate, Cybereason
SANS Security Awareness

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