WebsterBank®

How to Limit Losses From a COVID-19 Cyber Attack
Your Guide to Best Practices

In Part One of this content series we offered advice on how businesses can protect their operation from COVID-19 related cyber attacks.

In Part Two, we'll focus on how you can mitigate losses should one occur.

You put proper safeguards in place. You educated employees about the latest cyber crimes and phishing schemes. You required security awareness training for all staff. You even strengthened the security of your workflows and internal controls.

And still it happened. Your business was hacked by cyber criminals.

Unfortunately, it's not surprising. Cyber criminals are devising more sophisticated and insidious tactics, using advanced phishing scams and conducting more attacks via smartphone.

- According to anti-virus provider, McAfee, 480 new high-tech threats are introduced every minute.
- The Federal Bureau of Investigations (FBI) says that the number of cyber crimes reported has quadrupled since the COVID-19 pandemic. Not only do many of them take advantage of others goodwill or interest to help in these trying times, but they also use social engineering techniques to get individuals to perform a seemingly normal or routine action in such a way that it exposes them to a scam.

Perhaps even more startling than the number of attacks is the damage caused by them. In fact, the latest research shows that falling victim to just one cyber attack can be absolutely devastating for business owners and executives:

- On average, cyber attacks cost businesses of all sizes **$200,000**[1].
- **60 percent**[2] of those that are victims of a cyber attack go out of business within six months after the incident.

The question is…what can you do to recover?

[1] National Cyber Security Alliance, 2015

[2] Hiscox Cyber Readiness Report, 2019

Act quickly to limit losses.

Following your business continuity plan and any contingency plans you have established will make it easier for you to respond after a crisis. If you don't have one, connect with your IT, legal or accounting partners for ideas and input; additional framework information is available here:

In fact, according to the IT information website, Comparitech, four out of five or about **80 percent of businesses recovered from a cyber attack within 24 hours**… when they had a disaster recovery plan already in place.

Not only will the plan chart the step-by-step procedures you need to take to get essential business functions up and running after a crisis, it outlines roles and responsibilities as well as:

- Calling trees to communicate with senior leaders, lawyers, IT staff, internet providers, accountants, insurance brokers and other key personnel
- How to assess the extent of the damage
- What alternative operating procedures should be established
- What/when/who should communicate to staff and customers
- How to deal with the legal impact, such as reporting the cyber crime to law enforcement
- Instructions for restoring server, data, and access backups.
- How to access funds and bank accounts

Review your cyber liability insurance program.

Consider having cyber insurance, as it is an important part your organization's security controls and contingency plans. Coverage can offset recovery costs after a cyber-related loss data breach, fraud or financial loss in three broad categories:

1. liability for a data breach or loss

2. reimbursement to pay for cost to investigate, notify stakeholders, etc.

3. regulatory fines, penalties and settlement costs

However, all policies are not the same and not all policies cover all cyber risks and losses. So don't simply assume "We're covered for this." Notify your trusted insurance professional about your situation and check that you're indeed covered for the losses you may be experiencing, such as:

- critical system breakdown/ Internet outage
- cyber theft
- damaged/lost files
- virus or denial of service attack
- phone system failure
- power outage
- ransom of key files and computers
- privacy breach
- damage to data
- costs/income loss from business interruption

Understand what is irreplaceable.

Nothing is more important than the good will and reputation of your company. But unfortunately that's the one exposure that is difficult to fully restore after a cyber fraud or data breach, even if you have insurance coverage. Remember, having insurance allows you to transfer your risk, not eliminate it entirely.

Recognize that you need levels of mitigation.

Once you have recovered from a cyber incident, it's important to re-evaluate and adjust your plan. Get your team together to discuss what worked and what didn't. Was there a step missing from your plan? Could your security controls be even stronger? Closing gaps in your business continuity plan and incident response plan, and running practice drills using your new insights are key to protecting your company . . . if, and when, it experiences another cyber incident and loss.

Also, keep in mind that some of the best solutions for protecting your business are no-cost and low-tech, like confirming both suspicious transactions and messages with a simple phone call.

From a banking standpoint, consider an approach that builds security in layers, such as:

- services that give you important status updates on your accounts. For example, Positive Pay services warn you about potential check or electronic debit fraud and inform you of account activity you need to double-check.
- a more detailed review of your account set-up and cash-flow processes to mitigate the impact of cyber fraud.

To help make sure you have secure controls in place and are incorporating some of the latest best practices for fraud management in your plan, review this list on a regular basis with your business recovery team.

By next year, cyber crime is expected to cost the world $6 trillion. Now, more than ever, it's important to ensure that your business could recover—and survive—if it suffers from fraud or targeted cyber attack.

> “The losses that can be incurred from data breaches are best mitigated by investing in cyber security insurance, yet only 15% of U.S. businesses have this type of insurance.”
>
> *Source:*
> *U.S. Better Business Bureau*

See how Webster Bank can help you set up internal controls and payment account structure to mitigate fraud risk. https://public.websteronline.com/node/7666

The opinions and views in this guide are those of the authors, and are not intended to provide specific advice or recommendations for any individual. All loans are subject to the normal credit approval process.

EQUAL HOUSING LENDER

WebsterBank®