Bank of Botetourt

October 2022

Business Continuity Planning

Have you ever wondered how your business would continue to serve customers with critical products and services after a disaster? Do you know what those critical products and services are? Do you know what processes must continue within your operations to provide these essential products and services?

DISASTERS HAPPEN… IS YOUR BUSINESS READY?

Disasters happen; a risk assessment will help identify which disasters an organization is most vulnerable to. Disasters occur from unpredictable events, such as natural disasters, extreme weather, fires, floods, pandemics, and cyberattacks. A business continuity plan (BCP) provides a business of any size the opportunity to answer the questions stated above, identify risks, document mitigating procedures, quickly access contact information.

The three key elements of a BCP are ***resilience, recovery, and contingency***. Elements of resilience include data and system redundancies, maintaining a surplus capacity, and cross-training employees on critical processes. After a disaster, restoring an organization is vital, and prioritizing the most important systems and processes for business recovery is crucial. Strategies for recovery may include systems and applications, third party agreements, and additional inventories. The contingency plan includes procedures for external situations such as leasing emergency office or factory space, hardware replacement, and damage assessments.

A PLAN TO RECOVER

A BCP documents how a business will address the loss of facilities, personnel availability, and information technology systems. While developing a BCP, it is important to understand what functions are most critical to supporting essential activities. This process is called business impact analysis, and it identifies the period in which specific functions

Continued on Page 2

Member FDIC

EQUAL HOUSING LENDER

Connect with us!

(540) 591-5000

must be restored (e.g. 24 hours, 3 days, 1 week, 1 month). Once this is understood, the organization can begin developing the BCP to include plan activation procedures, internal and external communications, alternate facilities, and delegation of authority. The plan should also include employee and vendor contact lists for quick reference and be immediately available in the event of a disaster.

PRACTICE YOUR PLAN

After developing the BCP, remember to practice regularly, at least annually. A simulated disaster tabletop exercise is a good test for a BCP and can identify improvement opportunities for the overall plan.

The development of a BCP can be an overwhelming task. But it is an essential task. There are resources available. FEMA provides a Small Business Continuity Plan Template, which is available online here.

The SBA also provides resources on how to get started on your BCP.

Three Key Components of a Business Continuity Plan

How quickly you bounce back after a disaster may depend on how well you plan before it.

Data is one of, if not the most, important resources for any organization. And, protecting it from disaster, whether intentional or accidental, is no longer optional. As we have mentioned in our previous post, keeping an up to date BCP and DRP is a crucial component of your disaster recovery and business continuity strategy. Here are the components of a healthy BCP.

1. Recover personnel

Successful BCPs are built from the top down. This means that your first step getting buy-in and support from top management. Once this is in place, assign a dedicated person to manage the process and assemble a team comprising a member of each critical business department in your organization. Within your team, there should also be a chain of command; in other words, “who is doing what, where and when” and “how and where the relevant participants can be reached”.

2. Recovery procedure

The recovery procedure is that part of your BCP that outlines the strategies for business functionality. This strategy should identify and prioritize critical business assets such as equipment, the IT system (including network diagrams), contact lists, etc. In order to ensure your BCP is capable of protecting these assets, identify the potential risks and threats to those assets and compile a system that will assist you in recovering from a critical event or natural disaster.

3. Data backup

Statistics show that approximately 23% of organizations that fall prey to cyber-attacks lose business opportunities as a direct result of data loss. You should therefore have a proper backup strategy as part of your BCP. There are two types of backups that you must consider when designing your backup strategy: on-site backup and off-site backup. On-site can use tape drives, external hard drives and are easier to access than off-site backup. Off-site backup and the need for it have been discussed in part 3 above. You should furthermore include the following company documents in your backup plan: financial documentation (such as bank statements, tax records etc.), a list of fixed assets and legal documents such as copies of agreements, policies, memoranda of understanding, insurance documents, etc.

Sources: Mars Bank, Developing a Business Continuity Plan; Robert Kellerman, Stage2Data

7 Best Practices for Social Media Security and Privacy

Social media provides a world of opportunities for an organization or individual to promote and expand a brand. A powerful form of communication that uses the internet, social media can provide any organization with a strong global presence. Because these platforms have billions of users across the world, many organizations view social media as a vital tool in reaching a large number of potential prospects, customers, partners, employees, and advocates all at once.

Ultimately, social media platforms enable an organization's representatives and its followers to have interactions that involve sharing information, exchanging feedback, and creating content.

How to Protect Against Threats on Social Media Platforms
Social media can increase brand awareness and engagement with the public. It allows for a generally less-expensive form of advertising in a non-traditional way. There are many types of social media, from blogs to photo-sharing sites to instant messaging or video-sharing portals and more.

That said, as with almost every form of new technology, social media does come with its own set of challenges too. One drawback for those using social media is that it can put users at risk because it can open pathways that are insecure or tunnel beneath traditional cybersecurity.

How Does Social Media Affect Security?
There are five social media-related cyber threats to be aware of and to protect against. They include the following:

1. Social Engineering
Social engineering refers to a wide range of attacks that leverage human interaction and emotions to manipulate a target. Such an attack attempts to fool victims into giving away sensitive information or compromise corporate security.

A social engineering attack typically involves multiple steps. The attacker will research the potential victim, gather information about them, and then use this newly acquired data to bypass security protocols. Then the attacker works on gaining the target's trust before finally manipulating them into divulging sensitive information or violating security policies.

Obviously, Thanks to its casual nature, social media provides a social engineer with an avenue to naturally engage with the potential victim or organization to push them for information that can then be used to help launch an attack.

2. Phishing
In a phishing attack, usually via an email or an online message, the cyber criminal baits the potential victim(s) by trying to entice them into clicking on a malicious link or opening a malicious attachment. If the attacker uses social media to establish a rapport or relationship with their target, it will be easier to build the trust necessary to get them to click on malicious links or enter sensitive private information into an online form.

Cyber criminals also apply pressure on their potential victim(s) by creating a sense of urgency or appealing to their curiosity. "Act now before it's too late…" is the epitome of the kind of encouragement an attacker uses on their target to get them to either click on a malicious link or provide private information via a form.

3. Malware
The malicious links promoted in social media lead to malware. Malware is the portmanteau of malicious software. There are many different types of malware, such as viruses, trojans, spyware, and ransomware. Cyber criminals use malware to access devices and networks to steal data and take control of systems, create botnets, cryptojack, or damage systems.

4. Brand Impersonation
Another risk created by social media is when an individual or group tries to impersonate a well-respected company or brand to trick victims (employees or individuals) into providing confidential and valuable information that can be used by social engineers to hack systems and networks. In addition to harming the victims who fall for such impersonation tactics, brand impersonation can also damage the reputation of the organization being impersonated.

5. Catfishing
When a person takes information and images from another to create a fake identity and then uses this false identity to victimize an individual on a social media platform, it is known as catfishing. The catfisher usually uses a fake identity to trick targeted individuals into associating with them or doing business online with the goal of stealing from the victim or humiliating them, or both.

7 Social Media Security Best Practices
The best practices for addressing social media threats include these seven strategies:

1. ***Enable MFA.*** Multi-factor authentication is a security measure that protects individuals and organizations by requiring users to provide two or more authentication factors to access an application, account, or virtual private network (VPN). This adds extra layers of security to combat more sophisticated cyberattacks even after credentials or identities have been stolen, exposed, or sold by third parties.
2. ***Do not re-use passwords.*** Use a different password for every account. This prevents other accounts from being easily accessed if one account is hacked. Use a password management tool to keep track of various passwords and make sure passwords are not easy to guess.
3. ***Regularly update security settings across platforms.*** Stay on top of social media platform security options to ensure they are always current and set at the most stringent level.
4. ***Narrow down connections to reduce unknown threats.*** Be wary of the types of individuals and entities that you are connecting with on social media platforms. Carefully review every connection, and don't affiliate with those that appear disingenuous or suspicious.
5. ***Monitor social media for security risks.*** Stay aware of the threat news on specific social media platforms and respond accordingly. If you learn of vulnerabilities or hacking incidents, attend to your accounts and address issues that could lead to breaches or hacks.
6. ***Learn what a phishing attack looks like.*** Be diligent and educate yourself on the latest types of phishing attacks going around, and always be skeptical when someone reaches out to you uninvited via a social media platform or email.
7. ***Look out for spoofs of your account.*** Keep an eye out for brand impersonation attempts, report violations to the social media platform administrators immediately, and inform your followers as well.

Source: ***Fortinet***