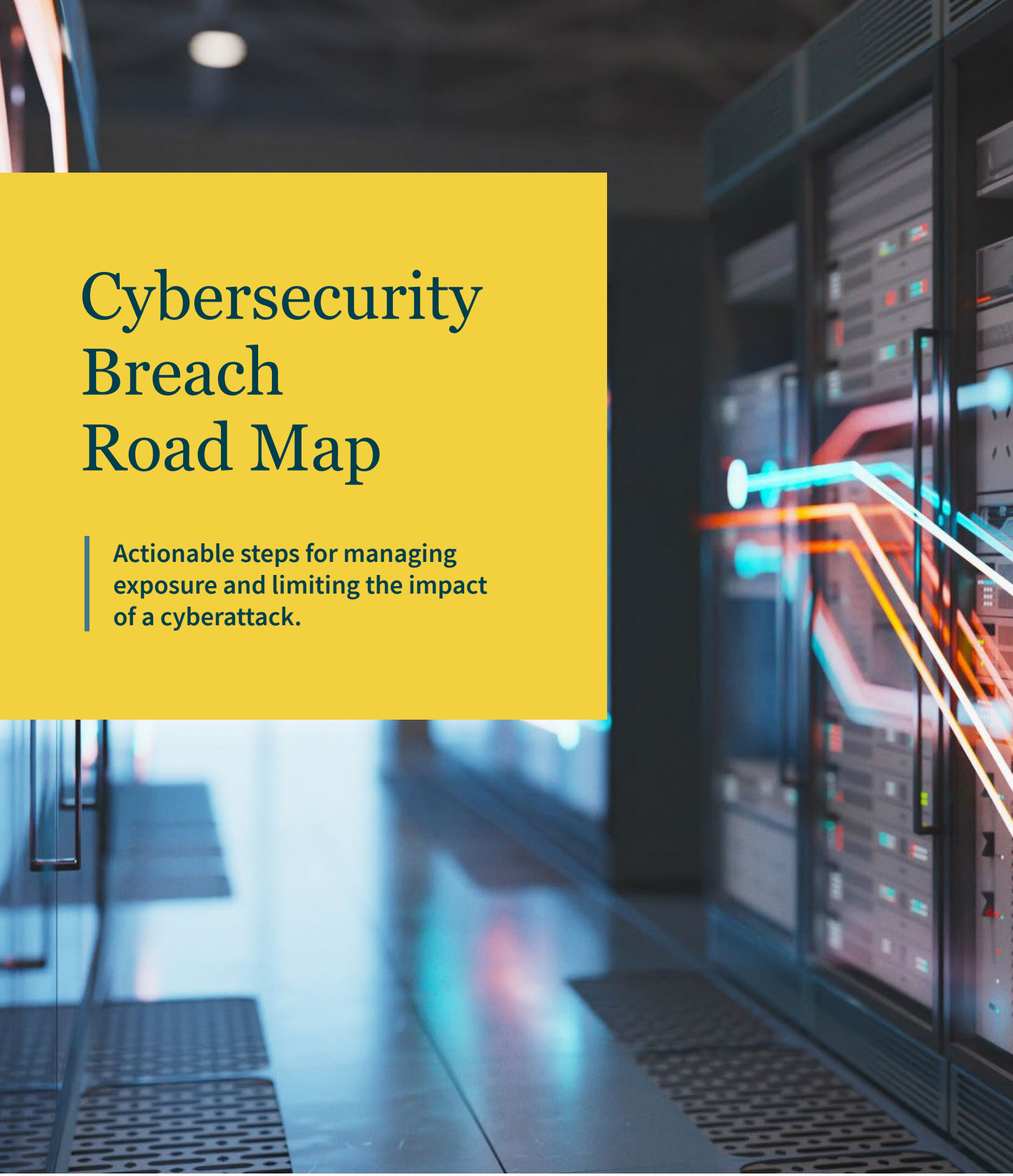

Cybersecurity Breach Road Map

Actionable steps for managing exposure and limiting the impact of a cyberattack.

Managed risk is your reward

Today's interconnected digital world brings vulnerability to the increased risk of cyber fraud, theft, and abuse. According to the Cybersecurity and Infrastructure Security Agency (CISA), 47% of all American adults have had their personal information exposed by cybercriminals during company breaches. These cyberattacks are inevitable — it's not a matter of if your organization is attacked, but when. And in the event of an attack, an effective response within the first 24-hours is critical.

You can only respond appropriately if your organization is prepared. A defined response plan allows you to react seamlessly, protecting your company's data, assets, and activity. If you prepare proactively and practice periodically, you will be ready to execute the plan when the attack strikes.

Organizations of all sizes face resource and planning limitations that can make it difficult to create and adhere to a cyber crisis plan. This cybersecurity breach road map and checklist is designed to give you the essential steps necessary to mitigate an attack within the first 24-hours — so you stay compliant and ensure you're back to business as quickly as possible after an attack.

Learn more about MGO's Technology Practice

Taking steps to prepare your IT structure before an attack is the best **possible protection.**

Key activities

Have an IT / cybersecurity consultant perform a cyber and information security assessment.

- **Identify key threats**
- **Assess regulatory compliance**
- **Review / plan cyberinformation governance**
- **Perform network assessment**
- **Provide security architecture plan**

Keys to a secure IT structure

Taking steps to prepare your IT structure before an attack is the best possible protection.
To assess your readiness, review the following:

Assess the maturity of your cybersecurity framework

- Have you developed and implemented IT policies, procedures and processes based on a governance models such as the U.S. National Institution of Standards and Technology (NIST) 800-171?
- Have you identified and prioritized cybersecurity risks and vulnerabilities?
  - Cybersecurity and IT assessments should be performed at least annually, but as needed.

Have you implemented the following six key IT controls?

1. Multi-factor Authentication (MFA)
2. Critical data is segmented
3. Follow the principle of Least Privilege to grant IT administrative and super user access right
4. System patches are kept current
5. Backups are available for all your critical systems and data
6. Network scans to identify network and cloud blind spots are regularly performed

Establish a team dedicated to monitoring risks

- Oftentimes in an organization, IT security is seen as an expense because it doesn't drive revenue. Being proactive can save a significant amount of capital in the long run if you fortify your systems against an attack.

Identify who oversees security governance

- Who coordinates the security activities of your entity to ensure that security information and decisions are communicated and enforced to achieve data integrity, availability, and confidentiality?

Know your cyber insurance

- Review your cyber insurance regularly to make sure the policies provide the right level of coverage for your organization.
- Verify that the policies you have support data recovery and cover the costs of business disruption.

Designate responsibility

- Assign appropriate responsibilities to different members of your cyber and IT teams.
- Develop Incident Response Plans and perform tabletop exercises regularly.

Back up data

- Back up your data regularly (we suggest daily).
- Ensure your backups are storied somewhere safe, reliable, and separate from the original system.
- Test the backups periodically to ensure if something happens, you can bring your organization back online within the first 24-hours.

Build and coordinate a "dream team"

Cybersecurity incidents require an all-hands-on-deck response to protect valuable assets. Your identified cyber response leader will need to coordinate representatives from several different functions to assess and limit the impact and move forward. Key parties to involve and prepare for collaboration include the following.

The affected business unit

Depending on where the breach occurs, you'll need to determine what you can shut down or pause to protect the rest of the organization. If it is consumer facing, you will need to plan accordingly

In-house and outside counsel

Did the attack involve bad actors or pirates demanding money? Was it a ransom attack? It is against the law to pay these hackers, so you will have to call your legal team for guidance and potentially involve the FBI.

Your cyber insurance company

This group will conduct an investigation to determine the details of the attack and make a conclusive assessment.

Human resources and legal

Your legal team will need to make decisions about how to handle the external aspects of the attack.

Public relations, customer relations, and investor relations

Getting ahead of the news cycle regarding the attack is crucial, and so is letting those affected know. Public relations can help you spin the news in the best possible light, so it doesn't affect your company's reputation or bottom line. Customer relations can work directly with your customers to ensure their needs and fears are addressed. And investor relations can do the same with your investors, who will understandably be concerned.

Board of directors

The board of directors helps you steer the ship of your organization. Thus, it's crucial they understand any risks or exposures in your organization and have the opportunity to provide guidance

Chief Information Security Officer

By leading the development of your organization's overall cybersecurity strategy and program, this person ensures the strategy is aligned with your business goals every step of the way, including after an attack. Typically, they will be the point person when communicating the situation to those who need to know, like the board and investors.

Application leader

This position works directly with the chief information security officer, ensuring the company's security operation is seamless and up to date.

Architecture leader	In collaboration with the chief information security officer and applications leader, the architecture leader will make sure the company's enterprise architecture and IT strategy are aligned.
Infrastructure and operations leader	This leader implements the operation of your company's security program.
Chief information officer	The chief information officer is a liaison between the security team and the rest of the organization so the entire company understands the importance of its cybersecurity strategy and plan.
Technical team	Your "boots on the ground" operation — they design, implement, and run the security architecture in your organization, as well as make sure it is updated based on new threats and risks.
Security and risk management leader	With a finger on the pulse of potential risks and breaches, this leader finetunes the cybersecurity program, folding it into the company's overall risk and compliance program so it becomes a priority before an attack

Cyberattacks are inevitable — it's not a matter of if your organization is attacked, but when.

Key response stages

First 24 Hours

1. Isolate and investigate
2. Segment your network
3. Inform those affected

1 Isolate and investigate

Once a breach has been identified your team must immediately limit the damage and investigate what went wrong.

Tasks include:

- Quickly identify the systems and data affected
- Isolate the compromised technology for future investigations
- Take the affected equipment offline
- Update credentials so hackers cannot utilize the old ones to get in
- Identify what went wrong, where your potential weak spots are, and how to avoid future breaches
- Secure the systems and patch vulnerabilities — because the only thing worse than one breach is multiple breaches
- Survey the damage with a snapshot or copy the authorities can later review, or quarantine it once it has been partitioned from the rest of your network
- Launch your designated incident response team, which will perform an immediate internal investigation to determine the overall impact on your critical business functions
- Utilize their findings to identify the attacker and tighten additional security as needed

Supporting activities

Work with a qualified IT / cybersecurity consultant to create a Security Road Map designed to protect your system. Your road map must include a detailed plan for identity and access management.

If you have concerns about your current system, you can have penetration testing performed to identify vulnerabilities ahead of a potential attack

2 Segment your network

Stop a breach in its tracks.

Tasks include:

- Develop and implement a network segmentation policy
- Segment your network based on data sensitivity using firewalls, access control lists (ACLs), or virtual LANs (VLANs) to control the spread of a potential cyberattack
- Segmentation will make it easier to monitor network traffic and detect threats in a timely manner
- In the event of a security breach, shut down the affected segment instead of taking your entire network offline

Supporting activities

Collaborate with a cyber / information security consultant to ensure your network architecture supports safe segmentation.

3 Inform those affected

Know who to contact — and how.

Tasks include:

- Identify and maintain a succinct list of groups who need to know about the breach within the first 24-hours, including law enforcement, your legal counsel, the board of directors, the incident response team, and cyber insurance. They are your first line of defense.
- Define how you will notify the end users (the individuals whose information or data is directly impacted) after the breach due to required confidentiality.
- Ensure no weaknesses or exposures are exposed immediately following the attack to prevent other hackers from attempting to capitalize on your vulnerability.

Supporting activities

A qualified IT / cybersecurity consultant can help guide the essential hours following an attack with a detailed Incident Response Plan. The plan will include an assessment of third party vendor risks, which can help you get a head start on potential vulnerabilities.

Days 2-30

1. Return to “business as usual”
2. Work with a forensic team
3. Retain audit logs

1 Return to “business as usual”

As soon as you are confident you’ve isolated the incident, you’ll want to allow your teams to get back to work to reduce the overall negative impact of the attack.

Tasks include:

- Define any manual, non-automatic procedures your team will need to implement during or after an attack — before a breach occurs
- Ensure they are in place, ready to be deployed so when the time comes to use them, you know what to do
- Create a 24-hour response plan for these manual procedures

Supporting activities

Ahead of an attack it is essential to have a Business Continuity Management Plan so you have steps and procedures in place to safely return to business.

2 Work with a forensic team

Depending on the extent of the attack, you may need professional support for responding to and documenting the breech.

Tasks include:

- Contact your cyber insurance and security service providers
- Review their findings which will include preserved data, logs who had access to what, and verification of compromised information
- Use the forensic report they have compiled to take remedial measures as needed

3 Retain audit logs

Follow the breadcrumbs at the information level.

Tasks include:

- Verify your audit logs are functioning — if not, you may not be able to figure out what happened retroactively
- Retain the audit logs in the system so you can respond appropriately within the first 24-hours of the breach
- Set the logs to retain for six months to a year

* 47%

of all American adults have had their personal information **exposed by cybercriminals during company breaches**

* In the event of an attack an **effective response is critical within the first**

24 hours

Be prepared

Executing an effective cybersecurity risk assessment is critical to understanding how to mitigate an attack. Whether you are leveraging the best practices in this road map proactively or in the wake of a breach, taking initiative is key to ensure your organization prioritizes agility and resilience in this ceaselessly changing digital age.

Along with our unique cybersecurity service model, our Technology team can help your organization minimize risk and optimize performance. Contact us to empower your organization with leading-edge technology solutions engineered to protect confidentiality, integrity, and availability of your critical data, all tailored to your needs.

Connect with us

Reach out to our Cybersecurity Services team today to find out how we can help you.

www.mgocpa.com

mgo.