Higginbotham™

Lead with values and value leads.

HiggCyber Solutions

$10.5 trillion

Cost of cybercrime by 2025

43%

Of breaches are attacks on small to mid-size businesses

1.2 billion

Predicted increase in internet users from 2019 to 2025

25,575 records

Average size of data breach

1 in 3

Data breaches involves a small business

The Increasing Threat of Cyber Risk

Cybersecurity is not just an IT issue. As our world becomes increasingly connected through technological advancements, cyber-attacks are advancing, too. Cybercriminals exploit your security weaknesses through a variety of methods including hacking, malware, ransomware, social engineering and even human error – something as harmless as an employee clicking a link in an email could lead to a sophisticated cyber-attack.

The repercussions from a cyber-related incident can be expensive and detrimental to your organization – **loss of revenue, reputation damage, loss of clients, lawsuits and compromised business information** are just a few of the damages you could face following a cyber-attack. Unfortunately, even the most vigilant companies are vulnerable.

To invest in the future of your company, invest in a cybersecurity strategy.

Higginbotham's Approach

As cyber threats continue to advance, organizations need solutions to manage their evolving vulnerabilities to cyber risk. With Higginbotham, you'll get comprehensive risk management cyber services tailored to your business:

- Best practices
- In-depth cyber risk assessments
- Incident response planning (steps to be taken in the event of a breach)
- Insurance policy design and implementation
- Strategic vendor partnerships

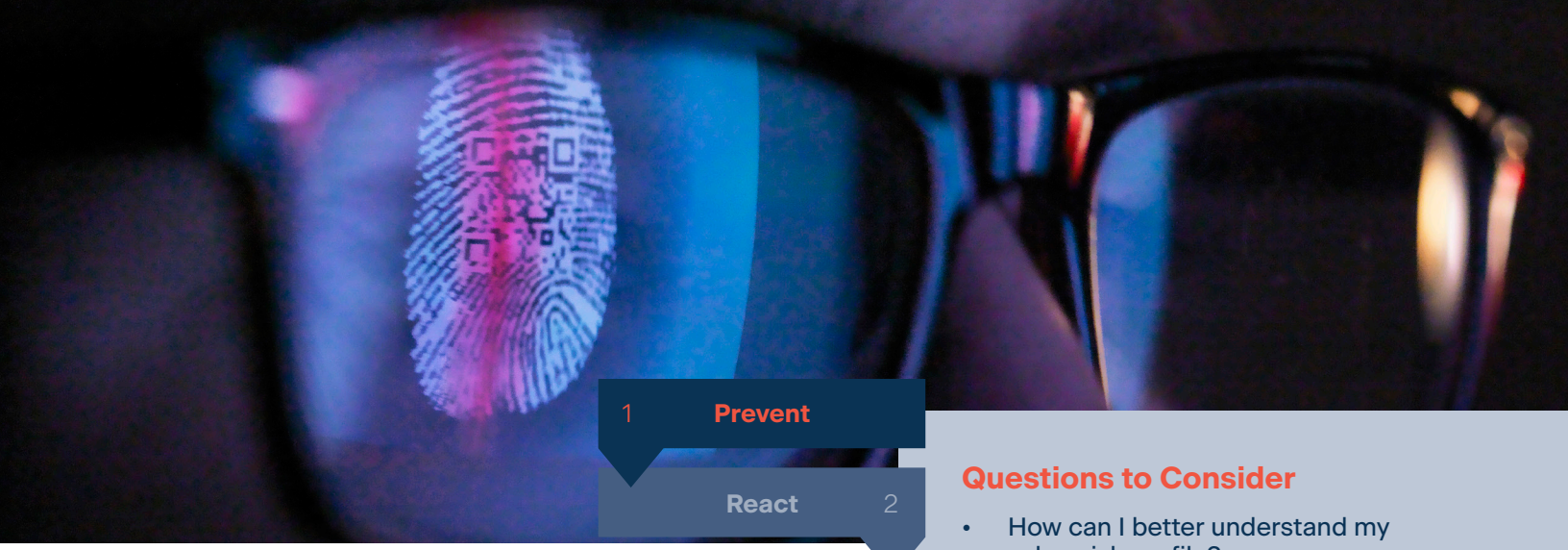
A good cyber risk management plan protects your capital, preserves your reputation and enables growth. That's what Higginbotham's Cyber Solutions is here to do. We advise you with the best protection to help reduce exposures for your unique business operations and needs. Because while insurance is our something, our customers are our everything.

Our Process

1 **Prevent**

React

3 **Recover**



Prevent

Our network of professionals work with you to assess your vulnerabilities, educate your workforce on cyber risk, consult on enhanced security protocols and recommend a tailored solution for incident response.

Assess

To gage your cyber risk and an event's potential impact on your business, we offer in-depth assessments. This helps identify your key vulnerabilities, ensuring cyber risk strategies and technological solutions tailored to your business objectives. We provide practical solutions to reduce risk, achieve business goals and help ensure a cyber resilient organization.

Educate

There are certain things you can do to safeguard your organization – like educating yourself and your employees on cyber risk. With our vendor partners, we use experience, incident data and assessment tools to host educational webinars on current cyber topics to keep you up to date on the growing cybersecurity industry.

Recommend

Once assessment is completed, we assist in developing a tailored cybersecurity strategy. This includes best in class cybersecurity insurance policies as well as response plans to mitigate loss in the event of a cyber-attack or breach. We leverage our deep industry partnerships, utilize specialists in forensics, claims and legal to understand your risk and create mitigation strategies.

Questions to Consider

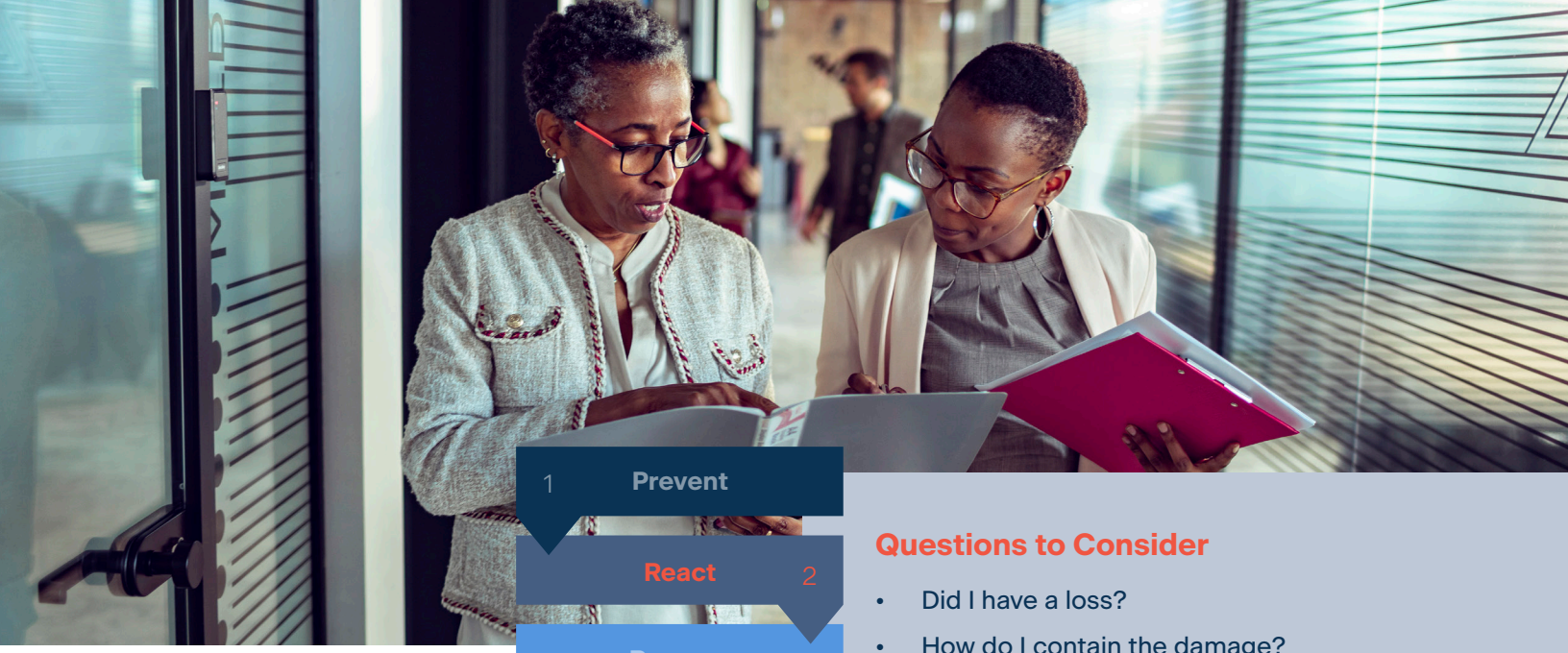
- How can I better understand my cyber risk profile?
- What can my employees do to help defend against a cyber-attack?
- How effective are my current cyber defense mechanisms?
- Does my cyber insurance appropriately cover my risk?

Added Services

We have strategic vendor partnerships that offer additional Cyber Advisor services to our clients. These value-added services alleviate the weight of feeling unprepared for a cyber-attack and remove the financial burden of employing a full-time cybersecurity professional. These services provide guidance and advisory on the cybersecurity matters important to you.

Additional services include:

- Quick Glance Report to provide a quick, cost-efficient report to identify and assess potential cyber threats.
- In-depth IT Risk Assessment to collect and consolidate exposures and risk factors for your organization.
- Collaboration meetings with senior management and other key leaders to answer critical questions and provide consultation on your company's ongoing cybersecurity efforts.
- Developing and implementing basic security strategies, investing in security solutions and remediating vulnerabilities identified during penetration testing.



1 Prevent

React 2

3 Recover

React

When a cyber-attack occurs, immediate action is critical – the decisions you make after an event can have lasting implications on your business – so we work quickly to engage in incident response support.

Engage

In the moments following a cyber-attack, your Higginbotham's Cyber Solutions team stands ready to react. We engage forensic teams, legal support and other professionals to provide the specific expertise needed to restore operations. We'll also send claim notification to your insurers and review your policy and facts of the incident to determine relevant coverage.

Detect

We investigate the incident to identify the cause and extent of the attack within your organization so you can work to prevent the same kind of attack from happening again. It's also important to find out who was affected by the breach – including employees, customers or third-party vendors – we assess the severity of the data breach.

Respond

We arrange an incident call with a pre-approved breach response attorney. The attorney will also work with you to preserve and protect potentially relevant information and documentation.

Questions to Consider

- Did I have a loss?
- How do I contain the damage?
- What happened to cause the incident?
- Who do I need to notify?
- Do I need to report this to law enforcement?
- How do I create a crisis communication program?

1 Prevent

React 2

3 Recover

Recover

It's important to effectively recover the lifeline of your business quickly and reliably. We work with you post-loss to mitigate the damage, notify affected individuals and recover your data to get you back to normal business operations. To help you get the full benefit of your cyber insurance coverage, we also serve as your advocate with your insurance carrier and third party experts for a fair and prompt settlement.

Mitigate

Following a cyber-attack, it's vital to limit the damages and minimize exposures. This can include isolating all or parts of the compromised network, filtering traffic, keeping data encrypted, restricting employee access to sensitive information and requiring multi-factor authentication. You can also consider keeping different workplace networks separated to prevent cybercriminals from gaining full access after attacking a single network.

Questions to Consider

- How do I get back up and operational?
- How do I communicate the cyber breach to impacted parties?
- How can I prevent a cyber-attack from happening again?

Notify

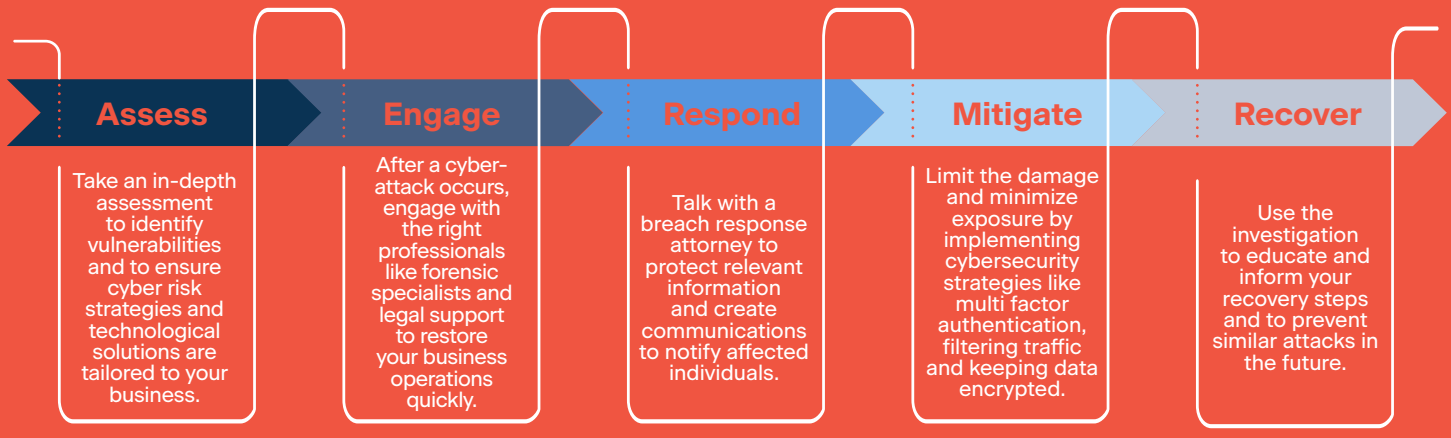
Communication is key – full and immediate disclosure of cyber-attacks is imperative. We have the resources to help you quickly prepare legal response and communications to notify affected individuals, regulators and law enforcement.

Recover

Once our post-attack investigation is complete, we'll use it to educate and guide your organization's recovery steps. When we clearly identify the root cause or discover any additional vulnerabilities, we can implement preventive security measures to prevent similar attacks. The evolving nature of cyber risk requires you to continuously monitor your risk— and adapt.

HiggCyber Solutions

Cyber-attacks happen to businesses of all sizes – your hard work, customer loyalty, reputation and assets are at stake. A fully integrated, comprehensive solution to create a cyber-savvy workforce and resilient systems should be a priority. Navigating cybersecurity solutions can be overwhelming, but Higginbotham's Cyber Solutions will be with you every step of the way.



Sources

[1]*The Mobile Economy 2021 Report*, by the Global System for Mobile Communications
https://bit.ly/3iwO7kA

[2]*Cyber Attack: What to Do After a Security Breach*, by AmTrust Financial
https://bit.ly/2VDrYrY

[3]*7 Ways to Prepare For and Recover from Cyber Attack Crisis Situations*, by Edward Segal for *Forbes*
https://bit.ly/3xQ9J0o

[4]*Cybersecurity Insurance*, from the Cybersecurity and Infrastructure Security Agency
https://bit.ly/2TYE2DN

[5]*Cyberattacks on the rise: What to do before and after a cyberattack or data breach*, by Steve Symanovich for *NortonLifeLock*
https://nr.tn/3hDV0jS

[6]*What to do before and after a cybersecurity breach?* By Gurpreet Dhillon for Virginia Commonwealth University Kogod School of Business
https://bit.ly/3B8ONUP

[7]*How to Recover from a Cyber Attack*, by Traci Spencer for the National Institute of Standards and Technology U.S. Department of Commerce
https://bit.ly/3kb7Szz

[8]*Recovering From a Destructive Cyber-attack*, by Dell Technologies
https://bit.ly/3kfIc4W

[9]*After the Attack - Eight Steps to Take Immediately Following a Law Firm Data Breach*, by Innovative Computing Systems
https://bit.ly/3kfr0ME

[10]Cybercrime to Cost the World $10.5 Trillion Annually By 2025, by Steve Morgan for *Cybercrime Magazine*
https://bit.ly/3wDyXxG

[11]*2020 Cost of a Data Breach Report* by IBM
https://ibm.co/3r8DQxH

[12]IBM Study Shows Data Breach Costs on the Rise; Financial Impact Felt for Years, by IBM
https://ibm.co/3hEddOd

[12]*15 Small Business Cyber Security Statistics That You Need to Know*
https://bit.ly/37ud4H1

higginbotham.com

headquarters
500 W. 13th Street
Fort Worth, TX 76102

p (800) 728-2374

HIGG-BR-12368