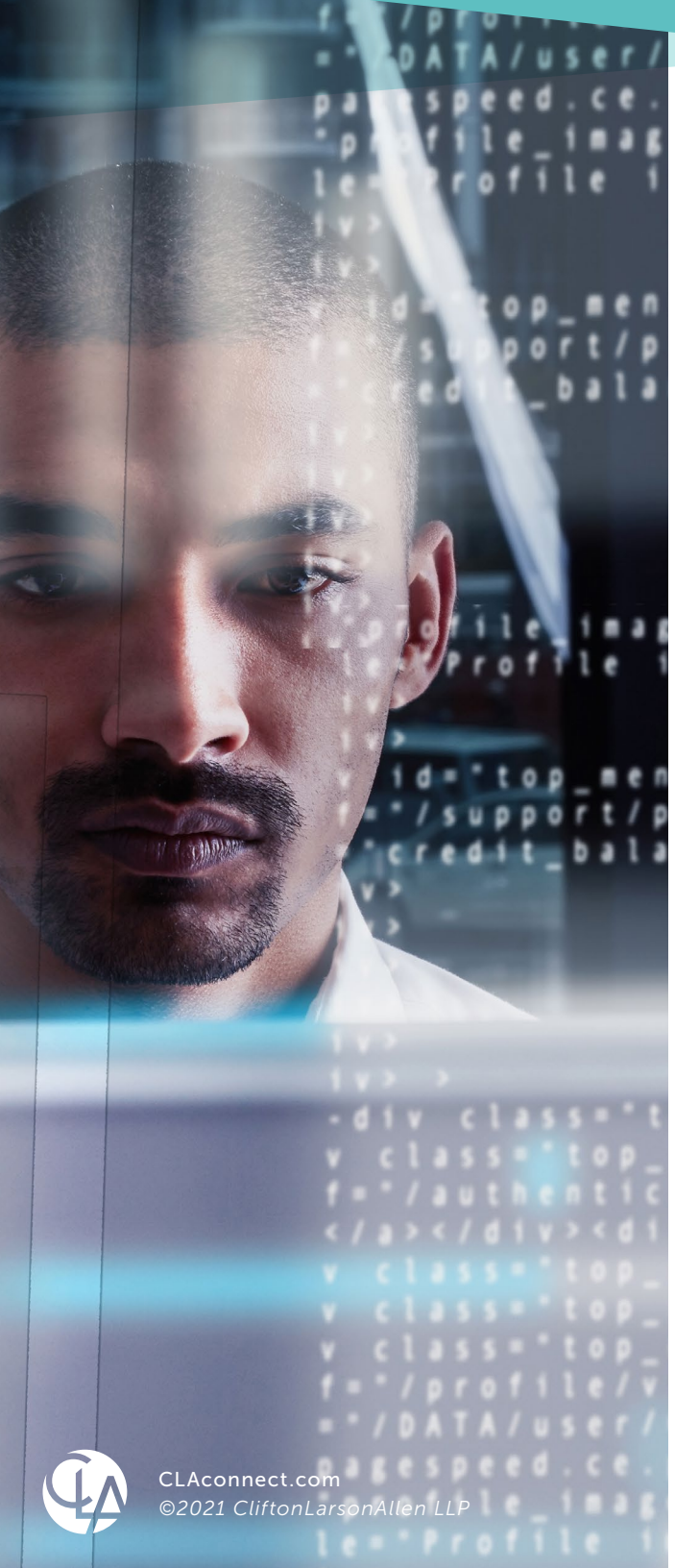
Four Steps to Conducting a Threat Assessment

Among the first things an organization should do to enhance its cybersecurity, protect its network, and safeguard its data is to conduct a threat assessment. This process will help determine:

- Which assets need the greatest protection
- Where your digital infrastructure is most vulnerable
- How to create and implement a cybersecurity policy
- How to develop cyber awareness training for employees

This white paper outlines the four basic steps that can help you prevent data breaches, cyber assaults, and ransomware attacks — and how to mitigate their impact should one occur. And while no assessment can guarantee total digital security, it can put you on a path that can help save your organization money, grow client trust, and build confidence in your network.



Step One: Prioritize Which Assets Need Protection

The first step to securing sensitive information is to evaluate exactly what data needs to be protected. This will vary depending on your business or organization, but typically includes the following:

- **Customer data —** This is largely associated with financial data (credit cards, credit reports, tax forms) but also includes any data that can be linked to a specific individual to aid in identity theft. This is commonly referred to as personally identifiable information, or PII.
- **Protected health information (PHI) —** If you operate in health care or have access to health care data via a client, there are very strict laws about keeping that data secure, and noncompliance can result in a large fine.
- **Personal Identifiable Information (PII) —** Employee data such as social security numbers, HR reports, background information.
- **Business information —** Think of any information that would be harmful or pose a risk to you if a competitor or someone outside your organization obtained it. Some of these items pose significant legal risk, such as trade secrets, financial information, or supplier records.

Once you've determined what information needs to be protected, you can then map out where that information is stored within your organization, who has access to it, and how to lock down those systems.

Additionally, if it hasn't been done already, create backups of business-critical data in a secure location. Back up these files on a regular basis so, in the event of an attack, these documents will be as up to date as possible. Don't forget to test restoring from these backups to verify you can access the files in a timely manner if an incident should occur.

Research present cyber threat landscape for your industry

It's important to research threats specific to your own business environment. While threats are always evolving, looking at the threat landscape can help you learn from others' mistakes and better anticipate methods attackers will be using.

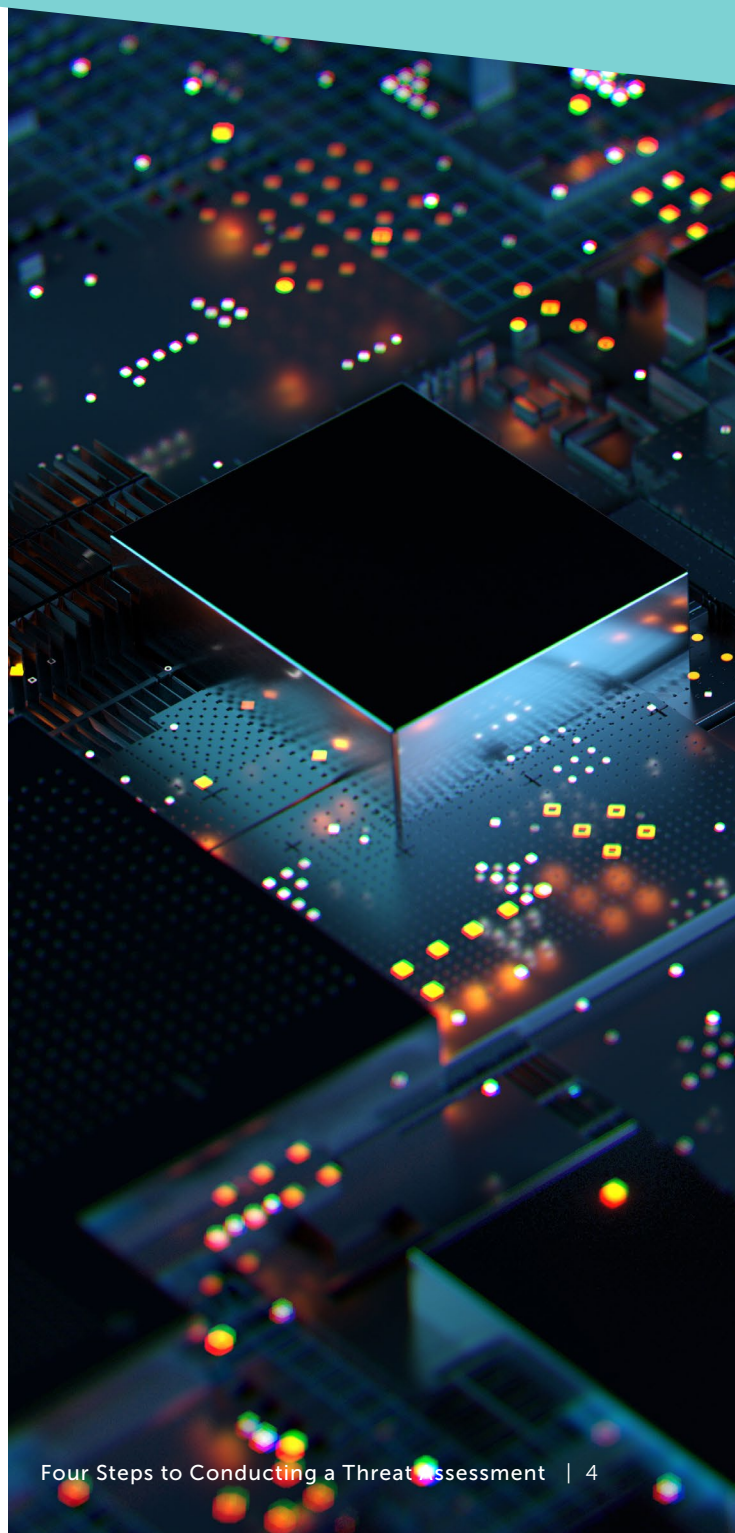
On a general level, you'll want to look at any information on recent attacks. There are many resources online that publish yearly reports with the most current cyber news.

As you research recent cyber attacks, ask yourself:

- What companies are being targeted?
- Who are their customers?
- What industries do they operate in?
- How did the attack occur?
- What is the cyber threat readiness state of my organization?

For added insight, look to your competitors. Chances are, if a hacker is targeting your competitors, they pose a threat to you as well. Research the volume of companies in your space that have had their security breached in the last few years, what data the attacker was targeting, and what methods they used to breach the system.

Of course, this step should be repeated regularly as security breach tactics change over time.



Step Two: Identify Network Vulnerabilities

Once you have an understanding of your at-risk data, where it lives within your system, and the present threat landscape, the next step is to evaluate how secure your current infrastructure is.

To get the most out of this process, remember that system vulnerabilities generally follow the 80/20 rule — meaning that 80% of the risk can be attributed to 20% of your vulnerabilities.

As such, start with the key foundational items that will make the most impact in a short period of time. Begin with assessing the high-risk data you identified in step one and evaluate vulnerable entry points a hacker can use to access it.

You should also consider how your employees' user habits impact your overall security posture. For example, you might have a secure Wi-Fi network in your offices, but do you have employees that work offsite? If that's the case, check that any sensitive documents are located behind a firewall and protected by a VPN.

This process is also a good opportunity to limit employee access to sensitive information to just key personnel.

Cybersecurity assessments

To understand the depth of your cyber exposure and readiness state, you'll probably want to work with a cybersecurity professional to obtain a cybersecurity assessment. A cyber professional can have more visibility into what's going on "under the hood" of your security infrastructure to see what may leave you vulnerable to an attack. Depending on your needs, your cyber professional may recommend you have one or more of the following assessments done:

Vulnerability assessment	This process looks across your organization's computer networks, systems, hardware, applications, and other key elements within your IT infrastructure to assess risk and rank your vulnerability to being compromised. The assessment should provide a ranking of the most critical vulnerabilities and a remediation plan.
Phishing assessment	Phishing attacks are a common method hackers use to infiltrate your ecosystem — are you sure your employees can recognize a phishing attempt? If not, you may benefit from a phishing assessment. Here, a realistic phishing attempt is simulated to your employees, and their response is monitored and documented.
Social engineering assessment	Like a phishing assessment, a social engineering assessment simulates different types of social engineering attempts to your employees to see how susceptible they might be to a hacker's tricks. This helps establish a baseline of your employees' cyber awareness and sets up the foundation of what still needs training.
Penetration testing	If you think you've been able to remediate most of the known vulnerabilities on your own, you might consider a penetration test. Here, a cyber professional will attempt to access your systems, applications, or wireless network through a controlled breach. You'll be able to see how a hacker got inside and what they were able to access.
Dark web scan	The dark web is an unindexed, mostly unreachable part of the internet and has grown to be a hotspot for cybercriminals to buy and sell personal information or sensitive business information. A dark web scan provides additional information as to whether or not your business information has been compromised and is being made available to cybercriminals and competitors.

Once you've identified and assessed your vulnerabilities, it's important to develop an action plan to start locking those items down. If you work with a cyber professional for some or all of these action items, you have been proactive in developing a cyber risk mitigation strategy that is designed to remain current and address the continuing threats to your system.

Step Three: Creating a Cybersecurity Policy

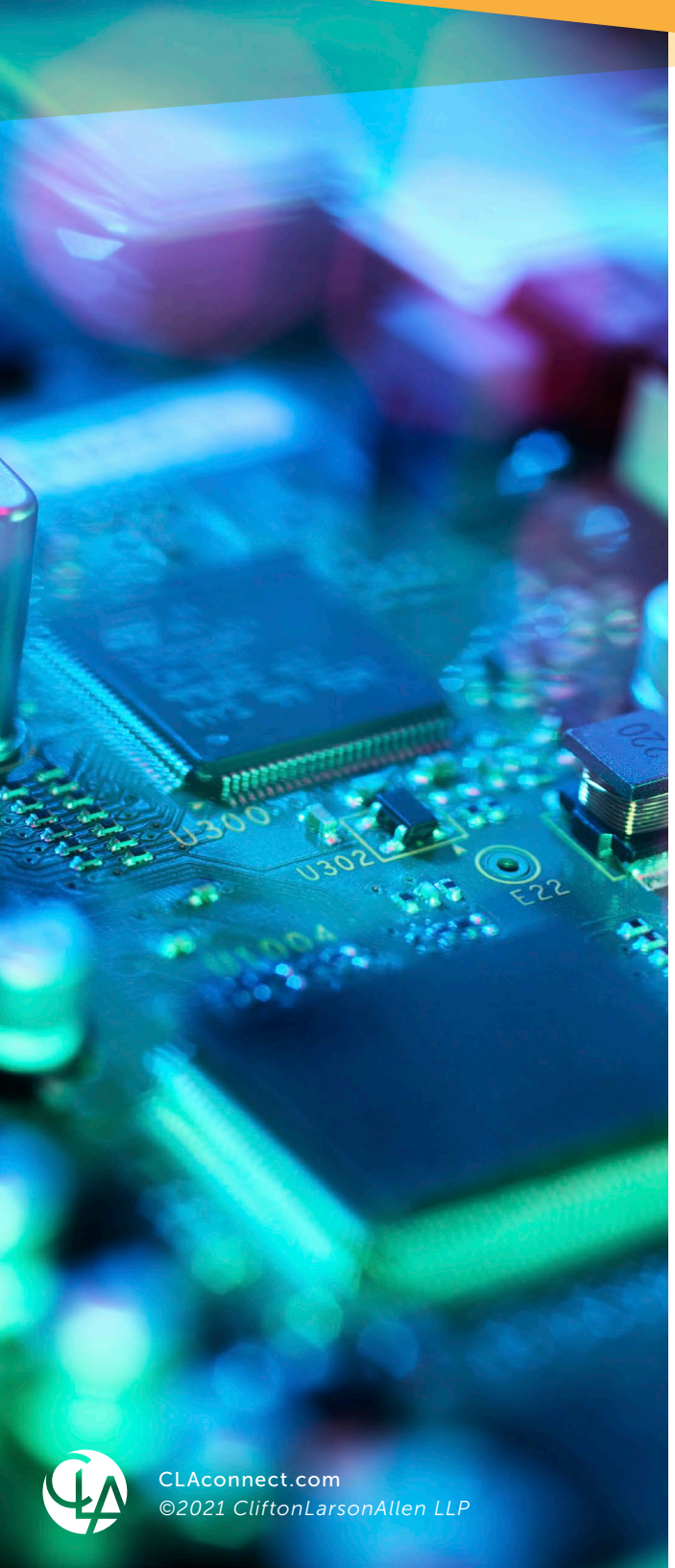
Build your team

Once you have identified and assessed your cybersecurity framework and associated vulnerabilities, it's important to create a written cybersecurity policy designed to keep your systems secure.

This policy should be well-documented, providing clear communication on the procedures needed to deploy and monitor end-to-end security across the organization.

To create a cybersecurity policy that truly protects all areas of your business, you'll need to collaborate across several departments. Each area of your business comes with its own unique cyber risks — and getting input and buy-in from various departments is key to success. Some important players in this process should include:

Board/leadership team	Of course, key organizational leaders should be included in the process so they can clearly communicate these policies from the top and affirm that they align with business goals.
IT team	If you have an internal IT team, they should also be included so they can closely monitor system updates, detect abnormal activities, and create clear standards around hardware and software usage.
Legal team	This team can provide input on current privacy, security, and data usage laws both nationally and internationally to verify that your organization is compliant with these terms and understands the implications for noncompliance in the event of a breach.
HR team	Human resources can put together a plan to clearly communicate the final policy for managers and employees. Additionally, they can work this into new-employee onboarding strategy and exit strategy for when an employee leaves the company.
Risk management team	Whether you have an internal audit team or use an external firm such as CLA, you need an independent compliance oversight function. Your risk management team can assist you in performing periodic operational, network, and privacy reviews; provide insight on acceptable monitoring procedures; and develop an understanding of your cyber insurance coverage with your internal business risk team or insurance broker.



Formulate your policy

As far as creating the actual policy, look at the procedures you executed to identify and assess your cyber profile in the previous sections. Consider how you can create a defined, easily repeatable process that will make security a part of your organization's culture.

Most importantly, this policy should be able to be expanded upon in the future. Because the threat landscape is always changing, your policy should grow with and reflect present threats.

Depending on how many internal resources you have, this is another step you may want to work on with an outside cybersecurity professional. A cyber professional can assist with creating a well-rounded cybersecurity policy, or take a more hands-on approach to your cyber health for the long term.

If your company has a smaller IT team or limited access to cyber skillsets internally, outsourcing some of the more technical work can reap higher benefits in the long run.

Some examples of outsourced cyber services include:

- Virtual Chief Information Security Officer (vCISO)
- Ongoing security threat detection and monitoring
- Dark web monitoring
- Vendor and third-party management

Even if your organization has the most comprehensive policy and vigilant employees, the security of your data is still only as safe as the third-party vendors you use. If your vendor gets hacked, you can still suffer huge consequences. A cyber professional can help you develop a risk management strategy to verify all third-party vendors have proper security protocols in place before you start developing a business relationship with them.

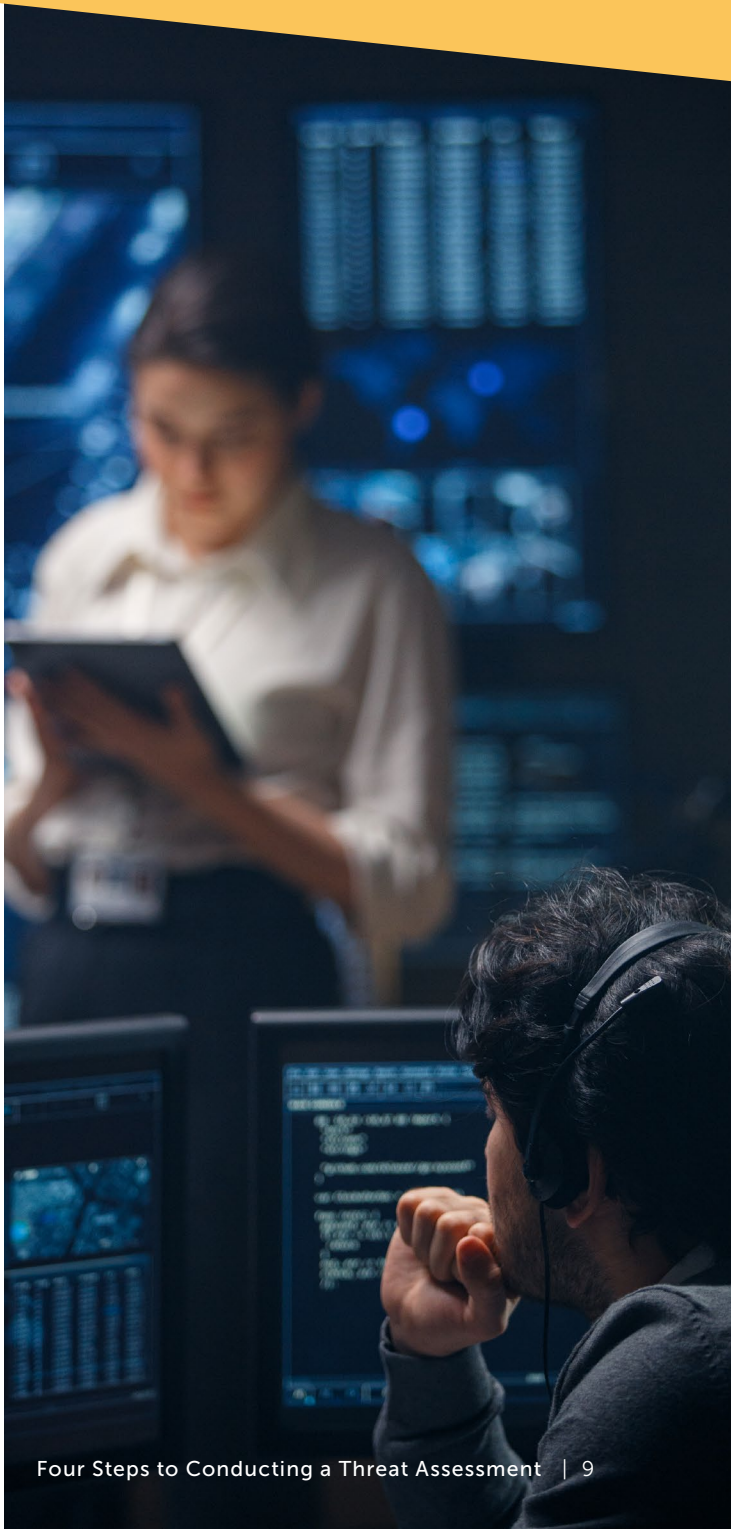
Create an incident response plan

Another vital element of a cybersecurity policy is a well-defined incident response plan in the event of a data breach.

When a cyber attack occurs, there is a very small window of time to properly identify and lock down systems before the hacker causes even more damage. As such, having clear steps in place before this happens lessens the overall response time.

This plan should include the following steps and define who is responsible for completing each of them:

- How you plan to contain the scale of the attack
- What information do IT and security teams need to gather about the attack (how the system was infiltrated, what data was exposed, what else could still be at risk, etc.)
- What legal risks have resulted from the attack and what process to take to report it
- Internal and external communication strategy
- Revisiting existing policy and expanding to help prevent future incidents



Step Four: Awareness Training for Employees

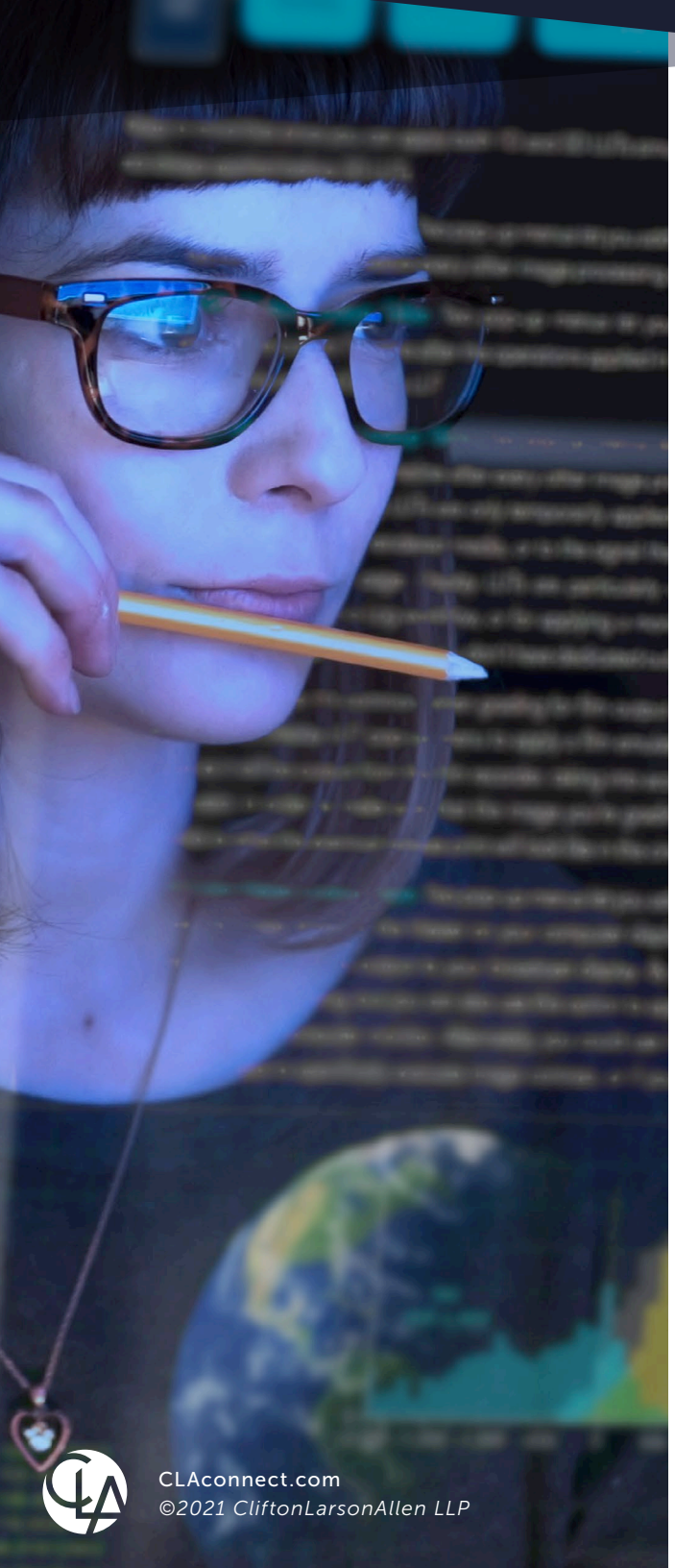
Conduct cybersecurity employee training

When it comes to your organization's cyber health, you're only as strong as your weakest links. You can have the most airtight policies in place, but it only takes one employee clicking on a phishing link to have your data compromised. Cybercriminals out there know this — which is why training your employees on proper cybersecurity awareness and procedures is so vital.

Cyber awareness training should be an ongoing initiative in your organization. A training strategy can be developed internally using cross-collaboration between leadership, IT, legal, and HR. However, it's often more effective to bring in an outside trainer with an established criteria rather than recreate the wheel.

Regardless of which you choose, these trainings must strike a balance between engaging and informing — so your employees will be able to retain what they've learned. Additionally, you must be able to measure the results of these trainings to see where your employees' cyber awareness stands before and after to determine if the training is effective. Lastly, be sure to document the training and results, as this may mitigate some of the legal risk if a successful attack occurs.

If you are looking to hire an outside team to conduct the trainings, it's important to know that all courses are not created equal. Some courses might be outdated and not reflect the current threat landscape. When evaluating potential trainers, look to an organization that has hands-on experience dealing with cybersecurity threats. These professionals will often have the most cutting-edge understanding of how threats occur and what employees need to know to stay safe. An ideal cyber awareness training program goes beyond a one-size-fits-all approach. Look for a team that can customize the program based on your employees' current awareness levels and the specific risks your industry is facing.



What to Look For in a Professional Cybersecurity Team

Final thoughts

Prioritize securing your systems against an attack. The reality is not if you'll be targeted — it's a matter of when. Proactively investing in your cyber health today can help prevent irreversible damage down the line.

We hope that this guide provides the building blocks you need to begin creating a culture of cybersecurity within your organization.

If you have any questions on what's been covered or would like to speak to one of our CLA cyber professionals about helping with your cybersecurity initiatives, click the button below to contact us, and we can work together to take steps to protect your business from a data breach.

TALK WITH AN ADVISOR

CLAconnect.com

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING