IT Insights

Four Questions You Should Be Asking About Cyber Security

Big data breaches continue to make the news, but how much risk does the average company face?

THE GLOBAL AVERAGE COST OF CYBER CRIME INCREASED BY MORE THAN 50% FROM 2016 TO 2018, which is a staggering reality. In spite of increases in global cybersecurity investments, experts estimate that 1 billion people fell prey to a security breach in 2017.

While you cannot completely guarantee your safety, you can take steps to avoid becoming a victim. You can also invest in early detection of breaches so that you can stop the theft of data as soon as possible. The best place to start is understanding where your strengths and weaknesses lie. Begin by asking yourself the following four questions:

Do I know what data to secure?

WHAT MAY SEEM LIKE A SIMPLE QUESTION CAN BE ANYTHING BUT. Before you can move forward with new or improved security measures, you must first know what data you should be securing. What information do you take, control and provide? Who does the taking, controlling and providing? To figure it out, it can be helpful to create an inventory of key security information:

- **THE ACTIVITY:** List the business activities where you collect, use, store, or transmit data
- **THE ACTIVE PARTY:** List the person (or role) who comes into contact with the data
- **THE RESPONSIBLE PARTY:** List the person (or role) responsible for the data
- **WHO HAS ACCESS:** List which people (or roles) should have access to the data
- **THE DATA PROPERTIES:** List what type of data is being collected

Creating an inventory of critical information assets and their usage will help you see where your security measures should be targeted. Without this information, you have no way of knowing whether you have secured all critical information assets. This information will also come in handy when you're performing a risk assessment: you immediately know where your riskier assets are.

weaver
Assurance • Tax • Advisory

Do I know how to prevent attacks?

PREDICTABLY, YOUR IT DEPARTMENT WILL PLAY A KEY ROLE IN PREVENTING CYBER ATTACKS. Securing the company's computers and networks is the first step. This phase includes basic measures such as installing antivirus and firewall software, requiring two-factor authentication, patching systems in a timely manner and backing up information reliably.

The IT department may also be charged with enforcing security measures unrelated to technology, like restricting access to certain rooms in the building, or promptly reporting missing electronic equipment. Does your IT department understand their responsibilities? How do you support their efforts?

But, the responsibility for security does not lie solely with the IT department. Ultimately, all employees are responsible for keeping company data secure. Consider the following employee actions outside of IT's purview:

- Using unapproved applications and cloud services
- Leaving sensitive documents unattended
- Falling prey to phishing scams
- Clicking on e-mail links or opening attachments that load malware onto the user's device

Even the best of employees can make these mistakes if they lack adequate security training. Are employees aware of your organization's goals for protecting data, and are they trained on how to help meet those goals?

> "The responsibility for security does not lie solely with the IT department. **Ultimately, all employees are responsible for keeping company data secure.**"

Will I know how to detect a breach?

DETECTING A BREACH EARLY CAN LESSEN THE PROBABILITY OF WIDESPREAD HARM, so it's important your detection techniques be top-notch.

- **DETECT WITH TECHNOLOGY**
  What internal resources are you using to detect a breach? Make sure that your detection tools are updated; even systems that are a year old may be obsolete. Modern Security Incident and Event Monitoring (SIEM) tools are able to identify deviations from the norm, by using either a rules-based approach or a method that detects relationships and correlations, and then aggregate that data to highlight statistically significant findings. A good SIEM tool should provide simple and clear reports so that your management team can interpret the information and take action.
- **DETECT WITH PERSONNEL**
  As we rely on technology more and more each year, the human factor can be overlooked. But, it shouldn't be. The people who work for you can be a great asset. In fact, they are often called the "human firewall" because they are the first ones to sound the alarm when something looks amiss. However, in order for them to be effective, they need to be adequately trained. Are employees familiar with what areas are most at risk? And don't forget about your IT personnel. Do you provide them opportunities to inform all staff about new and unique security threats to watch out for?
- **DETECT WITH THIRD PARTIES**
  Hiring a third party to help you in your assessment can offer an entirely new viewpoint. The easiest way is to hire a company to perform an independent security assessment for you. A professional can perform penetration testing to see how well you are preventing attacks and can subsequently monitor whether the attempted attack was successful. You may also be able to utilize a third party by hiring a fractional Chief Information Security Officer. If your entity does not have the means to hire such a leader full-time, consider hiring one part-time. They can provide much-needed insight to help you reach your goals.

How will I recover after a breach?

RECOVERING FROM A BREACH BEGINS AND ENDS WITH A SUREFIRE RESPONSE PLAN. An incident response plan is your roadmap to follow; it outlines the immediate steps to take following a breach. Your response plan should look different from any other company's because your plan should address the risks that are uniquely yours. However, all response plans should have some of the following characteristics:

- **THEY SHOULD OUTLINE DIFFERENT SCENARIOS.**
  Take the time to think through how you would respond to each type of attack. You want to be prepared for anything.
- **THEY SHOULD BE FLEXIBLE.**
  Finding the perfect mix between a plan that's specific and flexible will be your challenge. You want your plan to be rigid enough to provide you with step-by-step instructions when you need it, but flexible enough to help you tackle any problem that's thrown your way.
- **THEY SHOULD OUTLINE COMMUNICATION PLANS.**
  Often, communicating the breach – to your employees, shareholders, vendors, customers and competitors – can be overwhelming. Select one point person to handle all communications. They should be able to answer employees' questions, inform affected vendors, and notify clients. Make sure each group is given a consistent message.
- **THEY SHOULD EXPLAIN WHEN TO CONTACT THE PROFESSIONALS.**
  External professionals – like lawyers and forensics specialists – will be your lifeline in the event of a breach. Before an incident occurs, find a lawyer with experience in cyber breaches and establish that relationship, whether or not you choose to keep them on retainer. Similarly, you will want to select a qualified cyber forensics specialist. When the time comes, the forensics specialist can assess the extent of the breach and can work with you and your lawyers to take action.

Once you've created the response plan, run a fire drill to see how well it works. What did you leave out? Is there a way for you to respond more quickly?

Keep asking questions.

THE MORE YOU QUESTION YOUR CYBERSECURITY READINESS, THE MORE YOU WILL IMPROVE. Asking these sorts of questions within your organization is a great tool for you to employ routinely. Taking a step back to look at your operations with a new gaze is a great way to stay on top of the ever-changing landscape that is cybersecurity.

About Weaver's IT Advisory Practice

Weaver's IT advisory services group focuses on delivering performance-enhancing consultations that address your IT and business agendas. We work directly with CIOs and others to create a more risk-aware, effective IT organization that can drive process efficiencies throughout your company and better support and deliver transformational business change. Specific services we provide include:

- Application controls review
- Business continuity/disaster recovery
- Cloud computing assessment
- Data analytics
- Data privacy
- Information security and vulnerability assessment
- ISO27001 reviews
- IT audit
- IT governance and organizational effectiveness
- IT risk assessment
- Pre- and post-implementation application reviews
- System and Organization Controls (SOC) reporting

CONTACT US

Brian Thomas, CISA, CISSP, QSA
Partner-In-Charge, IT Advisory Services
brian.thomas@weaver.com

weaver
Assurance • Tax • Advisory